

新機能	4
CCC 5の新機能	5
Carbon Copy Cloner 5 Release Notes	12
Credits	32
Carbon Copy ClonerとAPFSについて知っておくべきこと	34
APFSボリュームグループと動作するには	38
Carbon Copy Cloner 3.5 から Carbon Copy Cloner 5にアップグレードするには	41
Carbon Copy Clonerのシステム要件	44
CCCを購入するには	46
Bombich Software 販売条件とよくある質問	47
アップグレードしてCarbon Copy Cloner 5を購入するには	50
30日間の無料お試し期間について教えてください。	52
Carbon Copy Clonerの価格と購入方法を教えてください。	53
今CCCの代金を支払っても、将来のアップデートでまた支払う必要がありますか。	55
CCCの1つのライセンスを家族で複数のMacに使用できますか。	56
教育機関向けの特別割引はありますか。	57
ボリュームライセンス契約を提供していますか。	59
CCCをプレゼントとして贈ることはできますか。	61
どうしてCCCはMac App Storeにないのですか。	62
電話でのサポートに対応していますか?	63
CCCをダウンロード、インストール、登録するには	64
Carbon Copy Clonerのダウンロードとインストールの方法を教えてください。	65
CCC 4からCCC 5にアップグレードするには	68
CCCの登録コードを手動で入力するには	69
Carbon Copy Clonerの古いバージョンをダウンロードできますか。	74
ワンクリックでCCCを登録するには	75
登録情報の適用に問題がありますか。	77
CCCの1つのライセンスを家族の複数のMacに使用するには、どうすればいいですか。	79
おっと! そのライセンスコードは正しくありませんよ...	81
I already purchased CCC but can't find my registration code. Can you send it to me?	84
Migrating CCC tasks from one system to another	85
CCCの使用開始準備をするには	86
バックアップドライブを選択するには	87
コピー先ディスクをmacOSのインストール用に準備するには	91
Mac OSをアップデートするための最善策	104
CCCを使用するには	108
最初のバックアップを設定するには	109
起動可能なバックアップを検証またはテストするには	115
バックアップから復元するには	118
バックアップのスケジュールを設定するには	125
スケジュールしたタスクを変更するには	129
CCCのメニューバーアプリケーションを使ってバックアップタスクをモニタリングするには	133
メール通知を設定するには	139
最後のバックアップがいつ実行されたかを確認するには : タスク履歴	144
既にコピー先ボリュームにあるデータを保護するには : Carbon Copy Cloner SafetyNet	148
ディスクセンター	153
Appleの Recovery HDパーティションをクローンするには	156
APFSボリュームでスナップショットを活用する	159
シンプルモード	170
Notes for VoiceOver users	173
CCCとそのヘルプツールにフルディスクアクセスを許可するには	174
macOSのシステムボリュームをApple Software Restoreを使ってクローンするには	177
データボリュームのバックアップを作成および復元するには	180
使用例	182

ハードドライブ全体を新しいハードドライブまたは新しいコンピュータにクローンしたいのですが。	183
データをTime Capsule、NAS、またはその他のネットワークボリュームにバックアップしたい	185
Restoring an item from a hidden folder	187
Cloning one external hard drive to another external hard drive	192
Folder-to-Folder Backups	195
Backing up and restoring Finder's Trash	200
Refining the scope of a backup task	201
トラブルシューティング	202
macOS Big Sur Known Issues	203
macOS Catalina Known Issues	206
ヘルプが必要な時はどうすればいいですか。	212
ヘルプ！クローンが起動しません！	214
CCCを最新に保つには	225
CCCをアンインストールするには	227
Antivirus software may interfere with a backup	229
CCCはどのような条件を使って、ファイルを再コピーする必要があるかどうかを判断しますか？	232
"CCC found multiple volumes with the same Universally Unique Identifier"	234
Finder or App Store finds other versions of applications on the backup volume	236
Launchpad ignores settings created while booted from another volume	237
"The task was aborted because a subtask did not complete in a reasonable amount of time"	238
Troubleshooting slow performance when copying files to or from a network volume	240
Where can I find CCC's log file?	242
Why can't I eject the destination volume after the backup task has completed?	243
Why does Finder prevent me from viewing the home folder on my backup when it's attached to another Mac?	246
Some third-party storage drivers may cause hardware misbehavior	249
APFSの複製に関するトラブルシューティング	251
Coping with errors caused by APFS filesystem corruption	254
ハードウェアに関連する問題を識別してトラブルシューティングするには	255
高度な使用例	259
バックアップタスクからファイルとフォルダを除外するには	260
高度な設定	266
Performance Suggestions	273
FileVault暗号化で作業するには	276
Some files and folders are automatically excluded from a backup task	279
Performing actions Before and After the backup task	283
Restoring non-system files	289
Backing up to a disk image	290
Restoring from a disk image	294
I have a full-volume backup in a folder or a disk image, but I don't have a bootable backup. How can I restore everything?	296
Using Carbon Copy Cloner to back up to/from another Macintosh on your network	298
A caveat for backing up to a remote Macintosh that has no user logged in	306
Restoring from a backup on a remote Macintosh	307
タスクを整理する	308
I want to defragment my hard drive	310
Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks	311
Backing up databases on OS X Server	313
Backing up large files, mounted disk images, and Virtual Machine containers	315
CCC SafetyNet フォルダの自動管理	316
"My disk is already formatted APFS or HFS+, why am I getting this warning?"	319
Backing up to/from network volumes and other non-macOS-formatted volumes	321
A closer look at how CCC determines the "bootability" of a destination volume	326
Cloning Coach Configuration Concerns	329
スケジュールしたタスクの実行条件を設定するには	332

Modifying CCC's Security Configuration	335
Creating a separate task to prevent VM container versions from bloating the SafetyNet	336
Outgoing network connections made by CCC	337
When I boot from my backup, Little Snitch reports that its rules have been replaced by a different version. Why, and how can I avoid this?	339
Limitations of online-only placeholder files	341
What is CCC's Privileged Helper Tool?	343
Downgrading an APFS-formatted Fusion volume from Mojave	345
よくある質問	347
用語集	348
コピー先のディスクの使用状況がソースと一致しません。CCCがコピーしていないファイルがありますか。	354
I want to back up multiple Macs or source volumes to the same hard drive	356
Can I run a backup while I'm using my computer? If I have open files, will they be backed up?	358
アプリケーションが異なる動作をしたり、クローンしたボリュームのシリアル番号を要求します。CCCがなにか見つけられませんか。	359
1台のコンピュータをバックアップし、そのクローンを使用して別のコンピュータを復元できますか?	361
I have a clone created by another application. Will CCC recognize that data, or will it want to recopy everything?	364
CCCはBootCamp (Windows) パーティションをバックアップできますか。	365
Can I use Carbon Copy Cloner to clone a Time Machine backup?	367
CCCからコピー先がいっぱいという報告がありました。この問題を回避するにはどうすればいいですか。	368
Frequently Asked Questions about encrypting the backup volume	371
Frequently asked questions about scheduled tasks	376
Frequently asked questions about the Carbon Copy Cloner SafetyNet folder	379
Frequently Asked Questions about cloning Apple's "Recovery HD" partition	383
Can I run backup tasks while my system is on battery power?	385
Can I run my backups more frequently than Hourly?	386
System problems can lead to a failure to install CCC's helper tool	387
レガシーSafetyNetフォルダは、スナップショットがコピー先で有効の場合、使用されません	388
Why does CCC say that my Mac is booted from a backup volume?	390
CCCとmacOS Catalinaについてのよくある質問	391
CCCとmacOS 11についてのよくある質問	401

新機能

CCC 5の新機能

Carbon Copy Cloner 5は、高度なユーザ向けのより高度なカスタマイズ機能、よりスマートでより動的なデフォルト設定、及び初心者向けの特別なヘルプを提供しています。何か素敵なものがみんなに用意されています。それでもまだ新機能について頭を抱えるようなことがあるなら、どうぞ遠慮なく [こちらまでお問い合わせください](http://bombich.com/ja/software/gethelp) <<http://bombich.com/ja/software/gethelp>>。

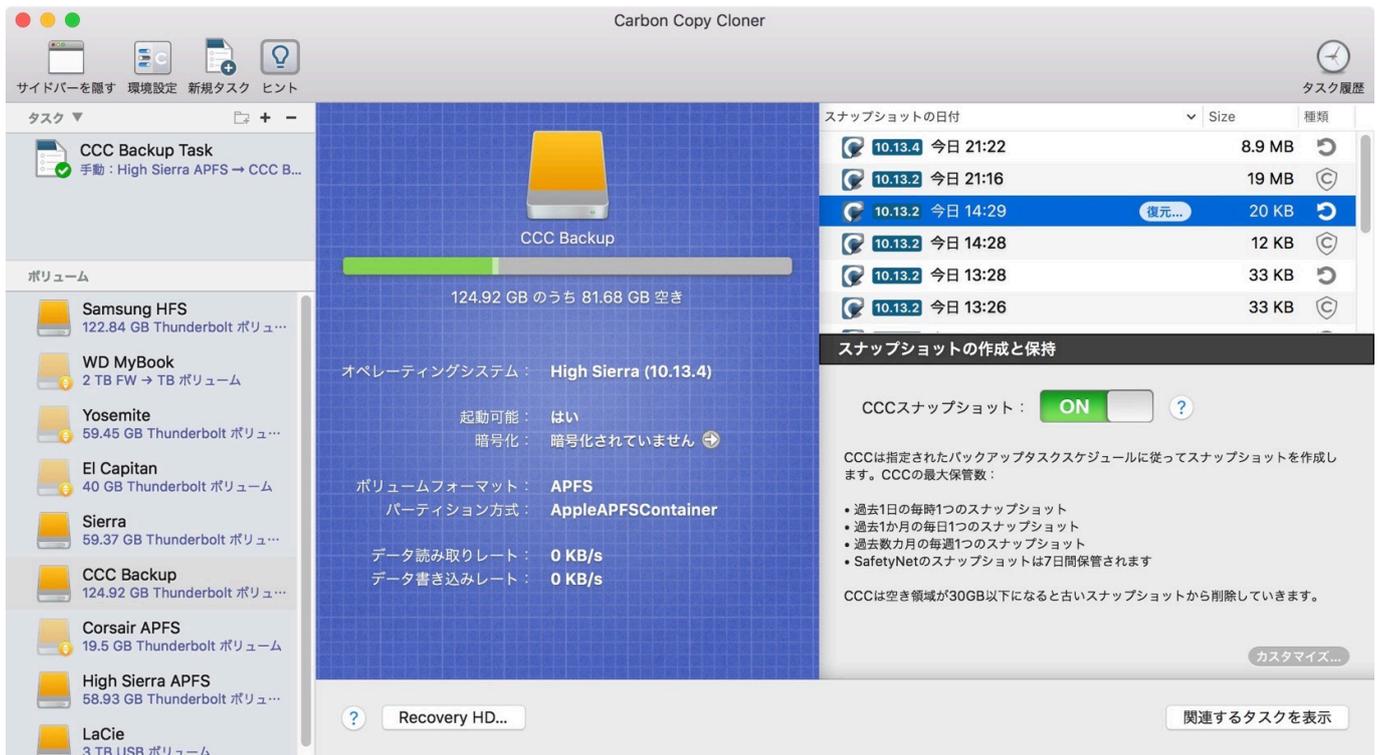
CCC 5.1の新機能

APFSスナップショットがついたバックアップをバージョン化

新しくCCCはAppleの新しいAPFSファイルシステムのスナップショット機能を利用して、その時点 (point-in-time)での復元をサポートします。また、CCCは macOS対応の初めての包括的なスナップ

ショット管理ユーティリティ

でもあります。CCCのデフォルト設定は道理に適った値ですが、CCCがスナップショットを作成する頻度と、時間経過と共にどのようにスナップショットを保持するかを正確に指定することができます。クリック1つでスナップショットの内容をブラウズでき、特定のスナップショットを削除したければ、それを選択して “Delete” キーを押すだけです。CCCは特定のボリュームのそれぞれのスナップショットをそのサイズと一緒に表示します。複数のスナップショットを選択すると、合わせたサイズを表示します。APFSボリュームのスナップショットにこれほどの洞察を提供するユーティリティは他にありません。



The screenshot shows the Carbon Copy Cloner application window. On the left, there's a sidebar with a task list and a volume list. The main area displays the configuration for a backup task named 'CCC Backup Task' on a 'High Sierra' volume. It shows a progress bar for the backup and system information like 'オペレーティングシステム: High Sierra (10.13.4)'. On the right, there's a 'スナップショットの日付' (Snapshot Date) table and a 'スナップショットの作成と保持' (Snapshot Creation and Retention) section.

スナップショットの日付	Size	種類
10.13.4 今日 21:22	8.9 MB	🔄
10.13.2 今日 21:16	19 MB	🛡️
10.13.2 今日 14:29	20 KB	🔄
10.13.2 今日 14:28	12 KB	🛡️
10.13.2 今日 13:28	33 KB	🔄
10.13.2 今日 13:26	33 KB	🛡️

スナップショットの作成と保持

CCCスナップショット: ON ?

CCCは指定されたバックアップタスクスケジュールに従ってスナップショットを作成します。CCCの最大保管数:

- 過去1日の毎時1つのスナップショット
- 過去1か月の毎日1つのスナップショット
- 過去数か月の毎週1つのスナップショット
- SafetyNetのスナップショットは7日間保管されます

CCCは空き領域が30GB以下になると古いスナップショットから削除していきます。

関連ドキュメント

- APFSボリュームでスナップショットを活用する <<http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes>>

タスクフィルタを定義する新しいインターフェース

バックアップタスクからフォルダを1つか2つ除外することは、CCCにとって大変だったことはありません。しかし、より複雑なフィルタに関しては難関がありました。そこで、多くの要望にお答えして、以下の新しい機能を追加しました：

- CCCはソース上のファイルが消費する容量を計算できます。タスクから項目を除外する、またはパターンに基づいて項目を除外するためのカスタムフィルタを追加する場合、CCCはそれぞれのフォルダの保護された合計サイズ(と累積)を報告します。
- 新しく、タスクフィルタはデフォルトですべてを除外します。これにより、バックアップタスクに含まれる必要のある項目のみを指定できるようになりました。これは、CCCがデフォルトですべてを含めて、バックアップタスクから除外する項目を指定するという、というデフォルト動作とは反対です。
- フィルタの読み込み、書き出しができます。さらに、バックアップタスクのためにソースを変更すると、CCCは新しくタスクフィルタをリセットしたいかどうかを確認するようになりました(単純にリセットするのではなく)。
- カスタムフィルタとグローバルフィルタの効果は明らかです。
- QuickLookパネルが、選択したファイルのプレビューを表示します。
- コンテンツを、名前、変更日、またはサイズで並べ替えることができます。
- 項目を選択してから、同じ親フォルダの中の別の項目のチェックボックスをShift+クリックすると、その間にあるすべての項目を選択または選択解除できます。
- どうしてもというなら、CCCにゴミ箱をコピーさせることもできます。そのためのチェックボックスを追加しました！

名前	変更日	サイズ	保護されています	デフォルトのフィルタ動作
Macintosh HD	昨日 17:59	60.88 GB	60.85 GB	
.DS_Store	2017/06/12 11:12	10 KB	10 KB	
.file	2016/02/25 17:50	0 KB	0 KB	
.localized	2014/05/10 18:44	0 KB	0 KB	
.Freshes	2017/05/31 12:24	0 KB	0 KB	
bin	2016/05/02 22:54	5 MB	5 MB	
etc	2015/10/19 21:46	11 バイト	11 バイト	
home	2017/05/31 12:29	0 KB	0 KB	
installer.failurerequests	2015/08/22 22:35	313 バイト	313 バイト	
private	2016/02/01 14:28	2.26 GB	2.26 GB	
sbin	2016/05/02 22:54	2.3 MB	2.3 MB	
tmp	2015/10/19 21:46	11 バイト	11 バイト	
usr	2015/10/21 14:37	1 GB	1 GB	
var	2015/10/19 21:46	11 バイト	11 バイト	
アプリケーション	2017/04/24 13:29	36.38 GB	36.38 GB	
システム	2016/05/02 22:54	12.12 GB	12.09 GB	
ユーザ			15.4 MB	
ライブラリ			9.09 GB	
.localized			0 KB	
Application Support			3.36 GB	
Audio			376.6 MB	
Bundles			2.9 MB	
Caches			0 KB	
ColorPickers			0 KB	
ColorSync			151 KB	
Components			0 KB	
Compositions			0 KB	
Contextual Menu It			0 KB	
CoreMediaIO			2.8 MB	
Desktop Pictures			433.6 MB	
.localizations	2015/08/24 23:44	58 KB	58 KB	
.orderedPictures.plist	2015/08/24 23:35	2 KB	2 KB	
.thumbnails	2015/08/24 23:35	973 KB	973 KB	
Abstract.jpg	2015/08/24 23:34	15.2 MB	15.2 MB	
Antelope Canyon.jpg	2015/08/24 23:34	10.5 MB	10.5 MB	
Bahamas Aerial.jpg	2015/08/24 23:34	9.6 MB	9.6 MB	
Beach.jpg	2015/08/24 23:34	10.5 MB	10.5 MB	
Blue Pond.jpg	2015/08/24 23:34	9.5 MB	9.5 MB	



カスタムフィルタのルール

*.webtmp ファイル拡張子のフィルタ 除外

Library/Caches サブパスのフィルタ 除外

除外する項目を定義

デフォルトですべてがコピーされます。ここで選択解除した項目はコピーされません。ソースに追加された項目をコピーするためにフィルタに変更を加える必要はありません。

ソースのオプション

Finderのゴミ箱をコピーしない

コピー先オプション

除外したファイルを削除

ルートレベルの項目を保護

凡例

含まれていない項目

部分的に除外

完全に除外

部分的に除外-(カスタムルール)

完全に除外-(カスタムルール)

除外されている、無効-(CCCルール)

よりスマートになったSafetyNet

新しく、CCCのSafetyNet削除設定はタスクがコピーする必要のあるデータ量に合わせて自動的に調整するようになりました。コピー先にバックアップタスクを実行するための十分な空き容量がない場合、CCCはSafetyNetフォルダの削除に戻ってから、コピーを再開します。コピー先に制限されたオーバーヘッドがあるせいでSafetyNet機能が実行不可能な場合、その機能を無効にすることをお勧めします。

リモートMacの設定を単純化

リモートMacintoshにバックアップするための設定手順が非常にシンプルになりました。新しく、CCCはリモートログインサービスが有効になっているローカルネットワーク上のMacを表示するブラウザを表示するようになりました。認証の際に、CCCはOSバージョンの詳細(互換性を判断するために)、とボリュームとファイル/フォルダ

のリストを取得します。これにより、リモートホストアドレスの仕様とソース/コピー先へのパスを単純化できるようになります。この機能はタスクフィルタにも同様に拡張できます。そこでは、リモートMacのソースにある特定の項目を除外するよう選択できます (CCC v4よりもリモートMacの復元がずっとシンプルになります)。

タスクのグループ化

多くのユーザからタスクを整理するためにもっと高度な方法を、とのご要望がありました。そこでCCC v5では、整理機能と実行時間の動作の両方を備えたタスクグループを追加しました。

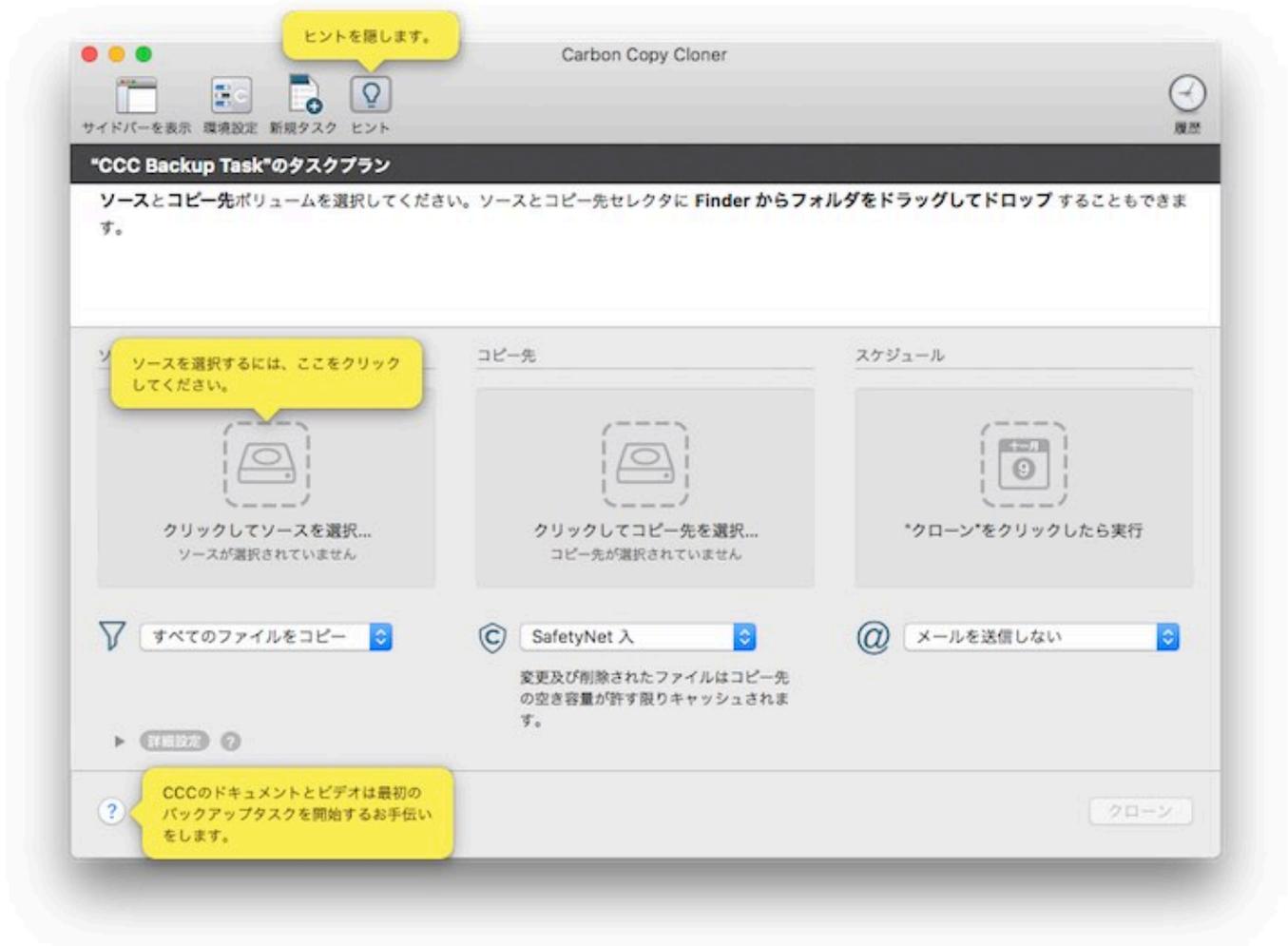


The screenshot shows the Carbon Copy Cloner application window. On the left, there is a sidebar with a 'タスク' (Tasks) section containing a list of tasks: CCC Backup Task, Daily Tasks (selected), Bootable Backup, Photos Backup, RAID Backup, and Work Files. Below this is a 'ボリューム' (Volumes) section listing various storage volumes like Macintosh HD, Sierra, Photos, etc. The main area is titled 'タスクグループ "Daily Tasks"' and contains instructions on how to manage tasks within a group. Below the instructions, there is a summary box showing 'タスクの数: 3' and '最近完了したタスク: RAID Backup (2017/06/28 12:12)'. To the right, there is a 'グループスケジュール' (Group Schedule) section with a calendar view. The calendar shows tasks scheduled for specific days and times: Bootable Backup on Sunday, Photos Backup on Wednesday, Friday, Saturday, and Sunday, and RAID Backup on Sunday. A 'クローン' (Clone) button is visible at the bottom right.

最もシンプルな形としては、タスクグループはタスクを論理的に整理することができます。しかし、タスクグループをスケジュールすることもできます。これで、一連のタスクを指定した順番でより簡単に実行できるようになりました。そこには優れたパワーと柔軟性があります。グループ内の個別のタスクをスケジュールして、グループから独立して実行できる上に、グループのスケジュールでも実行することができます。CCCはそこで起きる競合も処理します。例えば、タスクがグループ経由ですでに実行中の場合は、そのタスクはその独自のスケジュールをスキップします。タスク指定のポストフライト電源管理設定がある場合、それらは統合されます。グループ内で実行する最後のバックアップタスクを終えると、CCCはシステムをスリープ/再起動/終了します。

設定ガイド

新しく、CCCは“吹き出し”に役立つヒントを表示するようになりました。これらのヒントは様々なユーザインタフェースの要素の目的を説明します。最初の起動時に、これらのヒントがいくつか表示され、最初のバックアップタスクの設定を案内します。それが完了すると、メニューバーから“ヒント”を切り替えると、ヒントの一覧が表示されます。



復元ガイド

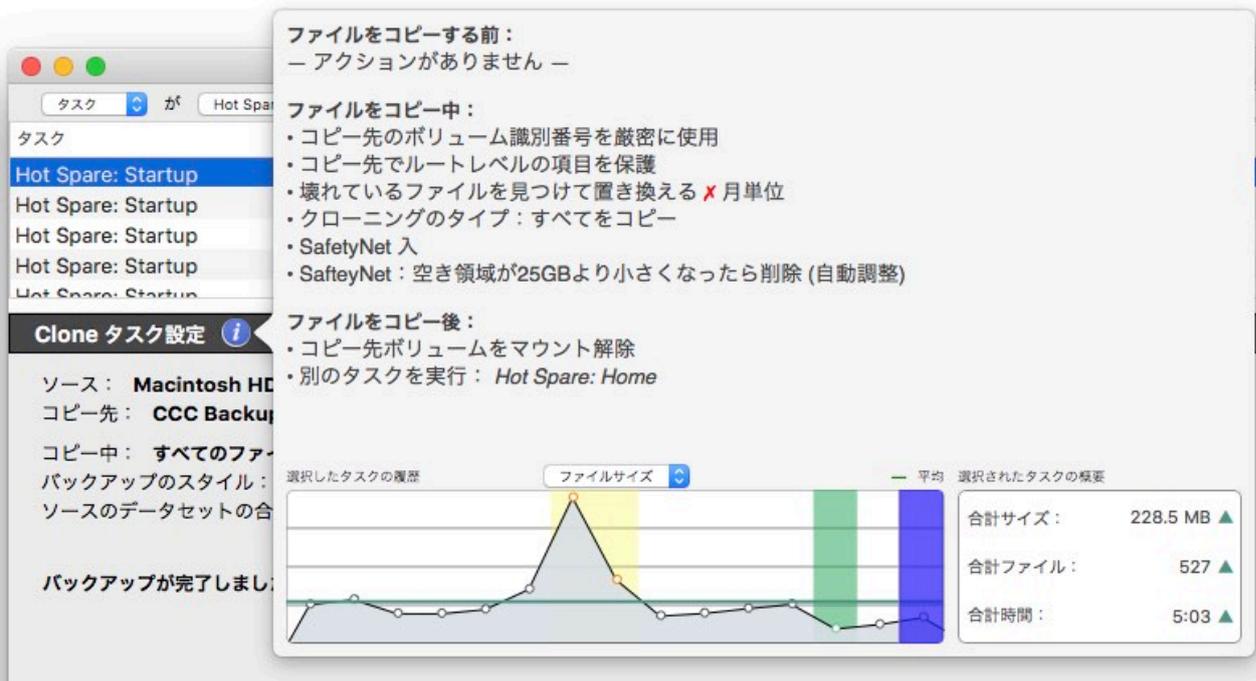
CCCは、お使いのMacが以前CCCのコピー先ボリュームであったボリュームから起動されかどうかを判断することができます。起動時にこれが確認されるとすぐに、CCCが開き、復元ガイドを表示します。復元ガイドでは、CCCは新しい復元タスクを作成し、起動ディスクをソースとして選択してから、コピー先の選択と（オプションで）復元タスクから項目を除外する手順を案内します。“ヘルプ”ボタンをクリックすると、復元に関するドキュメントとビデオに進むことができます。

新しいスケジュールオプション

タスクを今後決まった時間に1度実行するようスケジュールすることができます。その実行が終わると、そのタスクは“クローンボタンをクリックした時のみ”実行する、元の状態に戻ります。また、時間ごとの実行時間の制限を追加しました。例えば、タスクが実行される時間を5PMから7AMに制限することができます。時間ごとの制限を使用すると、タスクは指定された実行時間外に開始されません。また、タスクが指定された終了時間を過ぎてても実行中の場合は停止されます。

タスク履歴の動向

CCCのタスク履歴ウィンドウは新しく動向グラフを提供します。動向グラフはタスクがこれまでどのように実行されているか、タスクが実行される度に幾つのファイルまたはどれくらいのデータがコピーされたかを表示します。これまでこれらの情報はすべてタスク履歴ウィンドウからアクセスできましたが、グラフにすることで、これまでの動向や考えられる設定の問題などを視覚化して、問題が発生した場合に識別するのが簡単になります。



その他の改良点

私たちのTo-doリストは尽きることがありません。また、CCCを向上させるためのすばらしいフィードバックがユーザーの皆様から次々と送信されてきます。次にご紹介するのはCCC v5に追加された改良点のほんの一部です：

- SafetyNetについてたくさんの質問をいただきます。そこで新しくSafetyNetのポップアップメニューに“ SafetyNetとは？”の項目が追加されました。
- タスクを名前、終了状況、最後の実行日、次の実行日、または手動で並べ替えることができます。
- コピー先セレクトに視覚的なディスクの使用状況インジケータが追加されました。
- ボリュームをクリックすると (例えば、ソースまたはコピー先セレクトから) 、そのボリュームをマウントまたはマウント解除、あるいはFinderに表示できます。
- ソースとコピー先の選択内容を“ソース/コピー先を選択”してリセットできます。
- CCCのユーザーエージェントが新しく、メインアプリケーションで定義されたスケジュールでアップデートを確認するようになりました。
- クローン操作のお手伝いをする案内メッセージのいくつかが統合されシンプルになり、初心者ユーザーにも親しみやすくなりました。
- “壊れているファイルを見つけて置き換える”の設定が新しく、1週間に1度、または1か月に1度に制限できるようになりました。このシンプルな変更により、多くのユーザーがタスクの不必要な複製を持つ必要がなくなりました。
- タスクの読み込みと書き出し <<http://bombich.com/ja/ja/kb/ccc5/migrating-ccc-tasks-from-one-system-another>>が可能になりました。

CCC 4からアップグレードするには

CCC 4からCCC 5にアップグレードする手順をこれ以上簡単にすることはできないでしょう。CCC 5を開くだけで、CCC v4のタスクを自動的にアップデートします。30日間製品の様子をみた後、CCC 4を使い続けたい場合には、CCC 4を再度開き、ダウングレードのオプションを選択してください。CCC 4は元々のCCC v4のタスクをもう1度読み込み、すべてをCCC v5を試す前の状態にします。

関連リソース

- CCC 5をダウンロード <<http://bombich.com/ja/software/downloadccc.php?v=latest>>



- CCC 4をダウンロード <<http://bombich.com/ja/download#ccc4>>
- Carbon Copy Cloner 3.5 から Carbon Copy Cloner 5にアップグレードするには
<<http://bombich.com/ja/ja/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5>>

Carbon Copy Cloner 5 Release Notes

Carbon Copy Cloner 5.1.25

February 2, 2021

- Fixed an issue that was causing "On Reconnect" tasks to not run when the destination volume was remounted (affecting Catalina and Big Sur volumes).
- Fixed an issue in which the destination volume could be set as the current startup disk at the end of a task on systems with System Integrity Protection disabled.
- Made a handful of VoiceOver-related adjustments.
- Fixed the positioning of CCC's Preferences window, it had a tendency to wander downwards.
- Fixed the appearance of the update notification window in the user agent when Dark Mode is used.
- Fixed an issue in the Task Filter window in which items within a folder would appear to be excluded or re-included automatically as changes were made to that folder in the Finder.
- When applicable, the Backblaze /Library/Backblaze.bzpkg/bzdata/bzvolssystemvolume/bzvolid.xml file is now removed at the end of a Full Volume Clone to avoid a "safety freeze" when booting from a Big Sur backup.
- Attempting to clone a Big Sur volume into another volume in the current startup disk's APFS container is now disallowed (because it always fails). CCC offers some better alternatives instead.

Carbon Copy Cloner 5.1.24

December 16, 2020

- Fixed an issue in which CCC was not presenting custom volume icons in the sidebar and source/destination selectors.
- Fixed an issue in which CCC's main window was occasionally not showing task progress for a running task.
- Fixed the functionality of the "Manage snapshots on {volume name}" contextual menu item on the source and destination selectors.
- Improved some error handling when performing a full volume clone with Apple's APFS replication utility.
- Adjusted postflight disk image ejection. We found some cases where CCC had no trouble unmounting the destination disk image, but the eject request initially failed because it was "busy". Patiently waiting a few more seconds avoids a case where the disk image couldn't be remounted (e.g. when the task runs next) without manually ejecting the disk image.
- Resolved a logistical annoyance on Big Sur that can occur if a task is configured to run "On reconnect", the destination volume is a volume group, the Data volume is encrypted (note that the System volume is not encrypted on Big Sur), and CCC has not been given the password to that volume. CCC now instead waits for the Data volume's mount event as a trigger to these tasks.
- Time Machine backup volumes are now explicitly disallowed as source or destination selections on Big Sur. We're not planning to offer support for cloning to or from volumes that are flagged as Time Machine volumes.
- The "task started" notification now indicates the user-facing name of the source volume rather than the name of the Data sibling.
- CCC now breaks a cycle in which two tasks can volley back and forth, erring out because their destination folders are absent. This occurs when both tasks are configured to "Defer if another task is writing to the same destination", and both tasks are configured to back up to a folder on the same NAS volume.
- Addressed a few cases where CCC wasn't requesting the password for an encrypted volume (again, because the System volume on Big Sur is no longer encrypted when FileVault is enabled).
- Fixed an issue that could cause an ASR restore of a read-only disk image to fail. CCC also will automatically scan read-only disk images for ASR when configured to create a read-only disk image.
- Addressed an issue in which tasks were errantly getting marked "Task requires review".

- Fixed an issue regarding restores of Data volume snapshots on Big Sur.
- Made a few tweaks to work around ASR failures that can occur when the destination APFS container has remnants of an older OS.
- Addressed an issue with the CCC update mechanism in which the application doesn't automatically re-open when clicking the "Install and Relaunch" button on macOS Big Sur. The fix won't be realized until you apply the next update after this one, so if this issue was affecting you, you may still have to manually re-open CCC after applying this update.

Carbon Copy Cloner 5.1.23

November 24, 2020

Bootable backups on macOS Big Sur

CCC can now make bootable backups of a Big Sur startup disk on Intel-based Macs. Support for System volume cloning on Apple Silicon Macs is disabled for now because [Apple's APFS replication utility does not currently work on that platform](http://bombich.com/kb/ccc5/macOS-big-sur-known-issues#asrbrokenarm) [<http://bombich.com/kb/ccc5/macOS-big-sur-known-issues#asrbrokenarm>](http://bombich.com/kb/ccc5/macOS-big-sur-known-issues#asrbrokenarm) . When Apple fixes that, we'll post an update to CCC that restores support for making bootable backups on Apple Silicon Macs.

CCC is a native application on Apple Silicon and is 100% compatible with Apple Silicon Macs. CCC will automatically proceed with a Data Volume backup when backing up an APFS Volume Group on Apple Silicon Macs — that's a complete backup of your data, applications, and system settings. If you would like to make your Apple Silicon Mac backup bootable, you can [install Big Sur onto the CCC Data Volume backup](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#installmacos) [<http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#installmacos>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#installmacos) . Please keep in mind, however, that [your CCC backup does not have to be bootable for you to be able to restore data from it.](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate) [<http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate>](http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate)

Please take a moment to review the following resources related to macOS Big Sur:

- [macOS Big Sur Known Issues](http://bombich.com/kb/ccc5/macOS-big-sur-known-issues) [<http://bombich.com/kb/ccc5/macOS-big-sur-known-issues>](http://bombich.com/kb/ccc5/macOS-big-sur-known-issues)
- [Frequently asked questions about CCC and macOS 11](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-11) [<http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-11>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-11)
- Made several cosmetic adjustments specific to macOS Big Sur.
- Fixed an issue in which "On reconnect" tasks wouldn't run (i.e. when the destination volume is remounted) if the source is a Big Sur startup disk.
- Fixed an issue with unlocking and mounting encrypted APFS volume groups on Big Sur.

Carbon Copy Cloner 5.1.22

October 16, 2020

- Fixed an issue in which CCC was unable to access a new secret Apple data store in a folder named "searchparty" that was added in macOS 10.15.7.
- Added a global exclusion for a "com.apple.mediaanalysisd" temporary items folder whose content was leading to stalls on macOS 10.15.7.
- Improved the error message that is presented when CCC is unable to copy the Catalina System volume due to a lack of Full Disk Access (or more precisely, due to the inconsistent manner in which the system grants full disk access to an application's helper tool).
- Fixed a math issue regarding the application of a task time limit when the task starts shortly before midnight and the time limit starts at midnight.
- Made a couple small improvements to the messaging around some exceptional conditions in the Remote Mac setup window (e.g. lack of Full Disk Access on the remote Mac, using an "@" character in a hostname).
- The "If the source or destination is missing" UI in the scheduler is now made available to tasks that are part

of a scheduled task group.

- This update includes many changes to accommodate Apple's next OS, macOS "Big Sur". Please take a moment to review the following resources prior to upgrading to macOS Big Sur:
 - [Frequently asked questions about CCC and macOS 11](http://bombich.com/kb/coc5/frequently-asked-questions-about-coc-and-macos-11) <<http://bombich.com/kb/coc5/frequently-asked-questions-about-coc-and-macos-11>>
 - [macOS Big Sur Known Issues](http://bombich.com/kb/coc5/macos-big-sur-known-issues) <<http://bombich.com/kb/coc5/macos-big-sur-known-issues>>
 - [Best practices for updating your Mac's OS](http://bombich.com/kb/coc5/best-practices-updating-your-macs-os) <<http://bombich.com/kb/coc5/best-practices-updating-your-macs-os>>

Carbon Copy Cloner 5.1.21

August 10, 2020

- Added an exclusion for a system cache folder that has been causing some stalls, affecting primarily 10.15.6 users.
- Addressed an error related to the copying of a "SystemKey" file on a Catalina startup disk.
- Addressed an issue affecting the bootability of Yosemite and El Capitan backups.

Carbon Copy Cloner 5.1.20

July 21, 2020

- In macOS 10.15.6, Apple has resolved the [firmlink creation issue that was introduced in macOS 10.15.5](http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered) <<http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered>>. This update to CCC removes the workaround that we added in CCC 5.1.18 to address that issue. For 10.15.6 users, CCC will now revert to using its own file copier for establishing new bootable backups. 10.15.5 users will be encouraged to apply the 10.15.6 update, although the aforementioned workaround will still work for 10.15.5 users.

Carbon Copy Cloner 5.1.19

June 17, 2020

- This update addresses a handful of failure conditions of Apple's APFS replication utility which CCC is using temporarily in response to a bug that Apple introduced in macOS 10.15.5. We have also improved the task configuration workflow for new backup tasks, and we've added some documentation around this functionality: [Cloning macOS System volumes with Apple Software Restore](http://bombich.com/kb/coc5/cloning-macos-system-volumes-apple-software-restore) <<http://bombich.com/kb/coc5/cloning-macos-system-volumes-apple-software-restore>>, [Creating and restoring data-only backups](http://bombich.com/kb/coc5/creating-and-restoring-data-only-backups) <<http://bombich.com/kb/coc5/creating-and-restoring-data-only-backups>>, [Troubleshooting APFS Replication](http://bombich.com/kb/coc5/troubleshooting-apfs-replication) <<http://bombich.com/kb/coc5/troubleshooting-apfs-replication>>.
- Orphaned System volumes are now handled more proactively when selected as a source or destination. Orphaned System volumes arise when you either delete or erase the "Backup - Data" volume in Disk Utility without deleting/erasing the whole volume group when prompted. System volumes are unsuitable for user data, but some folks manage to get data onto them anyway (it doesn't help that Finder allows you to copy data to them). CCC can now help you migrate content from an orphaned System volume source, and will insist that you erase an orphaned System destination before proceeding with a task.
- CCC no longer excludes 1Password by default. We added the exclusion in light of [a recommendation by the folks at Agile software](https://support.1password.com/extra-copies-found) <<https://support.1password.com/extra-copies-found>>, however we got some feedback that people would prefer to exclude this manually, if at all.
- The Backblaze ".b2vol" folder is now removed from the root of the destination volumes at the end of an initial APFS replication. This should resolve issues in which Backblaze has identification issues after an initial clone is performed.

Carbon Copy Cloner 5.1.18

May 29, 2020

- Addressed an issue that Apple introduced in 10.15.5 (FB7706647) that will prevent CCC from establishing an initial backup of a macOS Catalina system volume.
- Starting in 10.15.5, CCC will no longer back up a macOS Catalina System volume to a disk image destination (i.e. a sparseimage or sparsebundle disk image file). We're making this change reluctantly, unfortunately we just can't get reliable results when using Apple's proprietary utility with disk images.
- Added a green checkmark emoji to the subject of "task completed successfully" emails.
- Improved upon the previous attempts to suppress VirusBarrier attached-but-not-mounted disk images in CCC's sidebar.
- When backing up to a OneDrive or Dropbox folder, CCC will no longer replace online-only placeholder files with a non-placeholder from the source unless the two files' modification dates differ. This resolves an issue in which a user flags a OneDrive/Dropbox folder as "online only" and CCC replaces the placeholders with real files, causing OneDrive/Dropbox to re-upload the content.
- Addressed an issue in which some sparse files were getting copied during every backup. In some cases this led to a noticeable performance degradation.

Carbon Copy Cloner 5.1.17

May 12, 2020

- Creating a new task via the CCC menubar application now works more consistently.
- Addressed a small logistical change introduced in macOS 10.15.4 that could lead to (harmless, but annoying nonetheless) errors while archiving the Preboot helper volume in a macOS Catalina volume group.
- Addressed a small UI error that occurred when strict volume identification is disabled for a task and a matching volume is present. The issue was specific to APFS volume groups.
- If a scheduled task was missed due to an encrypted volume being physically absent, CCC will now run that task and unlock the applicable volume when the device reappears. Previously the task would only run when the volume was unlocked by the user (and thus mounted), but now CCC will unlock the volume if a scheduled task was missed, or if the task is configured to run when the source or destination reappears.
- Resolved an issue in which CCC would report that it was unable to delete a snapshot on a rotational startup disk while the system was busy defragmenting boot files (another treat bestowed upon us by Apple's 10.15.4 update!).
- Resolved an issue introduced in CCC 5.1.16 that would cause CCC to fail to perform a task whose destination is a disk image on the startup disk.
- Unmounted disk images that some application left attached (VirusBarrier, I'm looking at you) are no longer listed in CCC's sidebar.
- When enabling the "Find and replace corrupted files" setting for a task that specifies an encrypted APFS volume group as the destination, CCC now presents a dialog requesting the password to that volume (if CCC doesn't already have it). This resolves a situation where the task would fail if CCC is unable to unlock and mount the destination Data volume.
- If CCC establishes a connection to an SMTP server, but the server never responds to CCC's "EHLO" reply, CCC will retry the connection.
- Fixed a crash that can occur in CCC's file copier while looking for case conflicts (only applicable if the source is case-sensitive and the destination is not).
- Support for extended attributes is now disabled by default when the user selects a network volume (or a folder on a NAS volume) as the source or destination to the task. You're welcome to re-enable extended attribute support, but we have found that most NAS devices offer exceptionally poor support for extended attributes, and that disabling them is the best default configuration.

Carbon Copy Cloner 5.1.16

March 31, 2020

- macOS 10.15.4 introduced a small timing issue that can occur when CCC attempts to delete the transient source snapshot at the end of the backup. This error is harmless, and the snapshot is removed automatically later, but this update adds a more aggressive method of removing the snapshot.
- macOS 10.15.4 also introduced a change that can cause trouble for setting up a remote Macintosh source or destination. This update resolves an error indicating that the remote Macintosh could not be reached during the initial setup.
- Fixed a dead end that can occur when a backup task encounters an error that calls for aborting the backup task (e.g. due to a stall, or when the destination volume pops offline in the middle of the task).
- Improved the reliability of the option to reveal an APFS Data volume in the Finder (via the volumes table contextual menu or via the Source/Destination selectors).
- Minor improvement to the handling of sparse files on APFS volumes. Also improved progress indication while copying particularly large sparse files.
- Made a small adjustment to the handling of BoxCryptor volumes.
- The "Defer if another task is writing to the same destination" setting now considers other volumes in the same APFS volume group to be the same destination. This addresses cases where one task is configured with the System volume as the destination (a standard configuration for a bootable backup) and another task is configured to back up to a folder on the Data sibling of the same volume (also a standard configuration for a folder-to-folder backup).
- Improved case conflict detection in cases where the source or destination is a member of an APFS volume group.
- In cases where a task is configured to back up to a disk image on a NAS volume, and the diskimages-helper service dissents the unmount request for the underlying NAS volume at the end of the task, CCC now terminates the offending process to make a followup unmount request more effective.
- The option to suppress the destructive task warning is now reset when resetting a task to default settings.
- Addressed some minor errors related to archiving the source APFS helper partitions that can occur if the source is a read-only device (e.g. a read-only disk image).
- Addressed an issue in which the startup disk setting would be set to the current startup disk when running a backup task (e.g. in cases where the current startup disk is not actually set as the startup disk selection in the Startup Disk Preference Pane).
- Remote Mac: If CCC's RSA key pair should become corrupted, CCC will now deal with the authentication failures more gracefully.
- Addressed a logic error that can lead CCC to restore items to the root of the selected destination volume rather than to a designated folder on that volume when restoring from a Data volume snapshot.
- Fixed an issue in which tasks that were flagged for review because the HFS+ destination will be converted to APFS were not presenting an APFS conversion dialog if the destination device was not attached.

Carbon Copy Cloner 5.1.15

February 4, 2020

- Added a timeout mechanism to volume unmount requests. The DiskArbitration service should never fail to reply to an unmount request, but we've been seeing those incidents more frequently lately.
- Made some additional tweaks to HFS+ to APFS conversion that should make it more robust.
- Addressed an issue in which an "On reconnect" task would not run when the source or destination was reconnected if the source or destination is a folder on a Data volume in an APFS volume group.
- CCC will now disable Spotlight by default on the destination when making a bootable backup of a macOS Catalina System volume.
- The "task finished with errors" email subject now leads with a "warning" emoji so it's more easily distinguishable from non-erring tasks.
- Fixed a logic issue that caused a selected Task Group to not be marked as selected in the View menu. Fixed a similar issue that caused the "Run Now" menu option in the File menu to be disabled for task groups.

- Fixed some dead ends in the CCC command-line utility that can be encountered when CCC's helper tool has not yet been installed, or when tasks have not yet been saved.
- Fixed a localization issue related to the thousands grouping separator used in numbers presented in various windows, including the Task History window.
- Errors that are produced by Disk Utility on a remote Mac regarding the failure to load unsigned plugins will no longer cause CCC to fail to produce a volume list when configuring a backup task to or from a remote Mac.
- Addressed an issue in which some pre and postflight scripts failed to run, supposedly due to the lack of a shell interpreter line.
- Added more specific handling of a scenario in which Disk Utility fails to create an APFS volume group when a T2 Mac is booted from an encrypted volume.
- Fixed a couple user interface sizing and placement anomalies.
- Improved the accuracy of the "Total data size" value reported in the Task Filter window when an APFS volume group is selected as the source.
- Fixed an issue in which the "Total data size" value that was being reported in the Task History window was incorrect (too low) in cases where the data set had very, very few modified items.
- CCC will no longer add the "About this folder.rtf" file to the SafetyNet folder if "OneDrive" appears anywhere in the folder path. This should avoid complaints from OneDrive that arise due to its 1980s-esque failure to deal with files whose names start with a space character.

Carbon Copy Cloner 5.1.14

November 14, 2019

- Authentication errors that occur when failing to mount the destination Data volume are now handled correctly (i.e. you'll get a "Reset Password" prompt instead of a generic error).
- CCC no longer avoids rebuilding the dynamic linker shared cache on Macs with less than 4GB of RAM. We found that this resolved system performance issues in the past, but now it only exacerbates system performance issues on these anemic systems when running macOS Catalina.
- CCC will now disallow the conversion of an HFS+ formatted Drobo volume to APFS because Drobo does not currently support APFS. This does not prevent you from reformatting a Drobo volume yourself and selecting it as a destination for a Catalina bootable backup, but CCC is no longer going to perform the task that places the Drobo volume in an unsupported configuration. If you want to use your Drobo device as a bootable backup, you should share that feedback with Drobo.
- Catalina: Added a "Reveal Data Volume" button to the source and destination selector when the applicable volume is a mounted System volume.
- Catalina: CCC's Cloning Coach now warns that a FireWire-attached destination is not bootable on Catalina+ (Apple no longer supports this configuration).
- Catalina: Errors encountered during the System volume backup will no longer cause the Data volume backup to fail, and the errors are now presented with more helpful advice.
- High Sierra+: Fixed an issue that resulted in non-bootable clones when specifying a volume other than the current startup disk as the source.
- The task selection in CCC's sidebar is retained more reliably.
- Fixed a logic issue that caused CCC's restart or shutdown requests to fail when no user is logged in.
- Catalina: Addressed a issue where an "On reconnect" task would fail to run when the destination volume was reconnected in cases where the source is the startup disk and the System volume had been replaced entirely during a system software update.
- CCC now works around volume unmount interference caused by CleanMyDrive. That product can still cause trouble for Disk Utility, however, so consider disabling that software if you're having trouble with an HFS+-to-APFS conversion, for example.
- Addressed an issue in which the source and destination selections might not be cleared out in Simple Mode.
- Fixed an issue in which CCC would report that it was unable to collect the details about the underlying volume when selecting a folder on a volume within a volume group, and when that underlying volume's name had a non-ASCII character (e.g. "CCC Backup - Données").

Carbon Copy Cloner 5.1.13

October 17, 2019

- Made an adjustment to how CCC copies the contents of the System volume when that volume is getting updated to avoid removing any content from the destination System volume that doesn't belong there. While it is inappropriate to ever have content on the destination System volume (CCC, for example, would not allow you to configure a task in that manner), Finder allows the modification of that volume, so conceivably someone could copy content to that volume without realizing the error. In general, you should avoid storing anything on your macOS backup volume that is unrelated to the source volume. If you want to store other content on your backup disk, [create a dedicated volume for that content <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#dedicatedvolume>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#dedicatedvolume) .
- CCC detects a couple more error conditions that are commonly encountered during APFS conversion on macOS Catalina and either works around them to make the conversion succeed or presents them with more accurate advice.

Carbon Copy Cloner 5.1.12

October 10, 2019

- Fixed an issue in which folders in the Task Filter window were missing a disclosure triangle, making it difficult to exclude subfolders.
- Improved OneDrive and Dropbox placeholder file detection.
- If you've deleted a Catalina System volume from a destination volume group, CCC now allows the selection of the orphaned Data volume as a destination, and will recreate the volume group as necessary.
- Made a couple small adjustments that should make HFS+-to-APFS conversions more reliable, particularly for slower destination devices.
- CCC 5.1.10 addressed an issue in which a remote Mac could go to sleep between CCC's archive management and file copying requests, but we found that change to be inadequate. This update improves upon that fix.
- Fixed a race condition in which the sort criteria popup menu in the Task History window wasn't getting populated if the task history window was opened very soon after launching CCC.
- Added "files copied" to the history output of the CCC command-line tool.
- When backing up to a disk image on a network volume, postflight unmounting of the network volume is now a little more reliable in cases where the diskimages-helper service is being stubborn.
- When CCC creates a System volume on the destination, the new System volume is now formatted as case-sensitive if the sibling Data volume is formatted as case-sensitive.

Carbon Copy Cloner 5.1.11

August 30, 2019

- Relaxed the restriction related to cloning a newer OS than what the Mac is currently booted from. CCC issues a warning, indicates clearly that the destination may not be bootable, but now you're welcome to proceed in this scenario if you have a particular need to create a non-bootable backup of the source system.
- Fixed an issue in which you'd be prevented from backing up to a new disk image stored on the startup disk.
- Fixed the "Open Disk Utility" and "Open Terminal" menu items in the Utilities menu for Catalina users.
- Addressed an edge case in which CCC would errantly report that it was unable to bless the destination because it's in the same APFS container as the current startup disk.
- Fixed some quirky behavior of the email password text field in the Preferences window.
- Addressed a couple errant Cloning Coach messages.
- Addressed a race condition that could cause the CCC User Agent to lose its connection to CCC's privileged helper tool after applying an update to CCC. This would lead to an empty task list in the CCC menubar, a

lack of task started/finished notifications, and a failure to present the mini task progress window.

- Addressed an issue in which CCC would not create the APFS helper partitions on an APFS destination when restoring from an HFS+ volume, resulting in a non-bootable volume.

Carbon Copy Cloner 5.1.10

August 20, 2019

This update offers qualification against macOS 10.15 Catalina, but also includes improvements for pre-Catalina OSes, so we recommend this update for all CCC 5 users. Please follow [macOS Catalina Known Issues](http://bombich.com/kb/ccc5/macOS-catalina-known-issues) <<http://bombich.com/kb/ccc5/macOS-catalina-known-issues>> for information on issues related to the new OS.

Changes not specific to macOS Catalina

- Addressed an issue introduced in 10.14.6 that prevents the removal of snapshots via CCC's Disk Center (it does not affect the automated removal of snapshots that occurs when backup tasks run).
- Corrected the read/write rate calculation for non-APFS-Fusion volumes.
- Added a button to reveal the password that you're typing into the Email Settings password panel.
- Changed the encoding of postflight emails that are sent by CCC to "quoted printable" (from UTF-8) to address an obscure edge case on some systems.
- CCC no longer automatically enables snapshot support on APFS-formatted volumes unless CCC can positively determine that the underlying device is an SSD. We have been underwhelmed by the performance of APFS on rotational devices, particularly with snapshot-related activities. Users are still welcome to manually enable snapshot support on any volume — simply click on the volume in CCC's sidebar and flip the switch to "on".
- CCC offers more helpful advice in cases where snapshot creation fails due to the destination being a slow, rotational device and also in cases where encryption conversion is preventing the creation of snapshots.
- CCC's privileged helper tool now proactively verifies the code signature of any client that attempts to connect to the helper. This resolves a potential vulnerability in which an application masquerading as CCC could make requests to CCC's helper tool.
- Modification of the name of a source or destination is detected and presented as a review item to the user. Previously we were simply marking the task dirty, and many users found that behavior disconcerting.
- CCC now proactively warns against cloning a volume whose operating system is newer than what the Mac is currently booted from.
- Addressed an issue in which a remote Mac could go to sleep between CCC's archive management and file copying requests.
- Failure to mount an encrypted volume attached to a remote Mac is now handled with a password request and the task's destination specification is updated accordingly.
- Addressed some minor accessibility annoyances in the CCC License window. Added a proper accessibility label to the task status icon in the Task History window.

Catalina-specific changes

- CCC will make bootable backups of macOS Catalina startup volumes. For most people, that's all you need to know, and you don't have to make any changes to your current tasks to accommodate the upgrade. The logistics of booting macOS are a bit more complicated in macOS Catalina, but we've risen to the challenge, CCC supports it 100%, and nearly all of these complications are dealt with automatically.
- macOS Catalina requires APFS, it cannot be backed up to a volume formatted with Apple's legacy HFS+ format. When cloning a macOS Catalina system volume, CCC will inform you of this requirement and request your permission to allow conversion of an HFS+ formatted destination to APFS. When you proceed with the task, CCC will automatically convert the destination to APFS (when possible).
- When you upgrade to macOS Catalina, any existing backup tasks that reference your startup disk and a non-APFS destination volume will be disabled and flagged for review. If any scheduled tasks are disabled in this manner, CCC will be opened automatically on startup and these concerns will be raised to your

attention.

- CCC will automatically create System and Data volumes on the destination as required to support APFS volume groups.
- When selecting an APFS volume group member as a source (i.e. your current startup disk), CCC will automatically copy the contents of both the System and Data volumes to the corresponding System and Data volumes on the destination. No special configuration is required for this, you will simply choose a single source and destination as you have in the past.
- CCC's task filter automatically accommodates source volumes that have a System/Data bifurcation.
- CCC fully supports encrypted source and destination APFS volume groups. If you have enabled FileVault on your bootable backup, CCC can automatically unlock and mount both members of the destination volume group as required for your scheduled backups. Please take note, however, of [a kernel panic issue that we have reported to Apple <http://bombich.com/kb/coc5/macOS-catalina-known-issues>](http://bombich.com/kb/coc5/macOS-catalina-known-issues) that can occur when mounting encrypted volume groups.
- When mounting and unmounting a volume that is a member of a volume group (either by clicking on the volume in CCC's Source/Destination selectors, or by right-clicking on the volume in CCC's sidebar), CCC will automatically apply that action to both members of the volume group.
- Tasks configured to unmount the destination at the end of the task will automatically unmount both members of a destination volume group.
- When backing up an APFS volume group to a disk image, CCC automatically creates System and Data volumes as required on the destination disk image, and copies the source volume group members accordingly.
- CCC has special handling of snapshot retention policies for APFS volume groups. The snapshot retention policy for both group members will be configured via the Data volume member.
- CCC will never create snapshots on source System volumes. These volumes are already read-only so a snapshot is not required. Considering that software updates may delete the snapshots or the System volume altogether, creating snapshots on the source System is futile.
- CCC will only create snapshots on a destination System volume when changes have been made to the source (i.e. when you apply system updates). As such, time-based retention of System volume snapshots is not very applicable. Instead, CCC will retain every snapshot of System volumes and will only remove System snapshots when the free space limit of the retention policy is exceeded.
- CCC lists the OS version and now also the build number associated with both System and Data volumes in the snapshots table.
- CCC offers great flexibility for restoring from System and Data volume snapshots. For example, you can restore from a newer Data volume snapshot and an older System volume snapshot, allowing you to downgrade the System without losing newer data. However, care should be taken when restoring System and Data volume snapshots that are associated with different OS versions, we don't yet know the implications of mixing these.
- Added a "Reveal in Finder" contextual menu item to the Volumes table so that users can reveal the Data volume in the Finder. That's key if you wanted to access something at the root level of that volume, e.g. the `CCC SafetyNet` folder.
- CCC no longer limits its requests for full disk access to times that you're saving a task that references the current startup disk. On macOS Catalina, we need full disk access to have access to external volumes and network volumes, so we pretty much need it any time you want to make a backup.
- When selecting a macOS Catalina System volume as the source, CCC's Source selector shows the cumulative disk usage of the System and Data volumes (because that's the value that reflects what will be copied). To see the individual disk usage of each volume separately, you can click on those volumes in CCC's sidebar.

New unsupported configurations in macOS Catalina

- Copying macOS Catalina system volumes to or from a Remote Macintosh is not a supported configuration, nor will CCC copy the contents of a System volume to a subfolder on a locally-attached volume. The logistics of producing a bootable copy of the bifurcated system are too complex to manage on or from a remote Mac, so we're only going to support making bootable backups of macOS at the root-level of locally-attached volumes.

- Selecting the startup disk of a remote Macintosh as a destination is no longer supported. This rarely works in the way you'd hope it will, typically it just produces lots of errors. You may still select a subfolder on the remote Mac's startup disk as long as it is a writable folder.

Carbon Copy Cloner 5.1.9

May 16, 2019

- Fixed an issue that could lead CCC to incorrectly conclude that a GoogleDrive volume is not mounted or present.
- Improved disk read/write rate calculations for APFS Fusion volumes.
- Minor adjustment to the analysis of permissions errors that occur when trying to access OneDrive placeholder files.
- We've received several reports of long stalls in the "Cleaning up" phase when backing up to a disk image; particularly when that disk image resides on a NAS volume. In most cases this was the result of a filesystem stall while the filesystem was attempting to create a snapshot. Snapshot support is now disabled by default for CCC-created APFS-formatted disk images. You're welcome to enable snapshot support on a disk image manually if you prefer that; double-click the disk image to mount it, then click on the mounted disk image volume in CCC's sidebar to manage the snapshot creation and retention preferences for that volume.
- Minor adjustment to the handling of locked files when trying to create hard links.
- Fixed an edge case in which the "Secure CCC's Scripts Folder" function was not removing non-root-user write privileges on shell scripts.
- The task history sort attribute is now retained as a preference.

Carbon Copy Cloner 5.1.8

February 26, 2019

- When creating a new disk image on a Mojave+ system, CCC will now create APFS-formatted disk images if the source volume is APFS-formatted. All snapshot functionality afforded to APFS-formatted volumes will apply to APFS-formatted disk images as well.
- Hard drives from a popular vendor ship with a rogue "is a bundle" flag set on the root folder. When cloning this volume to a folder, the rogue flag is preserved on the destination folder, which causes the Finder to treat it like a file, making it awkward to see the items that were copied. CCC now strips this rogue flag from the root folder of the selected destination to avoid the annoying result.
- Adjusted the handling of 0-byte "placeholder" files (e.g. Dropbox, GoogleDrive, OneDrive "online only" files) to avoid lengthy delays. These delays were particularly notable when working through Dropbox folders.
- Total snapshot disk usage is presented more prominently in the Disk Center.
- When cloning to an ExFAT or FAT32 volume, custom volume icons are now preserved at the destination.
- Addressed errors that could occur while trying to create hard links in locked folders.
- Resolved an error that can occur when creating read-only disk images on SMB network volumes. Due to a bug in macOS Mojave, sparseimage disk images cannot be created on SMB NAS volumes. Rather than creating a sparseimage intermediate disk image, CCC will now create a sparsebundle intermediate disk image.
- CCC's "trust but verify" case-sensitivity check is now applied to "ufsdExtFS" volumes as well, after getting confirmation from a user that these volumes incorrectly report themselves as case-insensitive, when in fact they are case-sensitive.
- To protect against unauthorized modifications, CCC now requires that pre- and postflight scripts are owned and writable only by the system administrator, and that all parent folders of the scripts are owned and writable only by the system administrator. A new "Secure CCC's Scripts folder" option is available in the Utilities menu to help meet these new requirements.
- Fixed some UI issues around the visibility of the pre/postflight script interface elements.
- Fixed an issue in which other tasks within a group would start to run after the following events: a) start task

- group, b) stop task group before all tasks complete, c) manually run one of the tasks within the group.
- Fixed an issue in which CCC would errantly report that a destination lacked support for files larger than 4GB.
- Hourly run time limits that have a start or end time at midnight will be applied a little more gracefully, e.g. a task that starts a few seconds prior to midnight will be allowed to run with a midnight start time limit.
- Fixed a password decoding issue that could cause problems while configuring a task with the Remote Macintosh option if the administrator's password on the remote Mac contained 3-byte characters (e.g. €).
- Tasks that failed due to the source or destination being missing will no longer get a "failed" badge in the Tasks table if the task is also configured to not send error notifications when the source or destination is missing. Likewise, the Task Plan will now indicate this condition specifically, rather than offering a generic "Errors occurred during the last run" message.

Carbon Copy Cloner 5.1.7

December 13, 2018

- CCC will now proactively warn about configurations specific to T2 Macs that will produce non-bootable results, and configurations that will lead to problems with enabling encryption or modifying Startup Security settings.
- Addressed an issue in which a Mojave-running remote Macintosh would fail (inconsistently) to correctly validate the code signature of CCC's file copier, thus causing backups to the remote Mac to fail.
- Apple cache files that have been found to degrade task performance are now excluded from backup tasks by default.
- CCC can now distinguish between a volume that is encrypted vs. a volume that has FileVault enabled. This is a subtle difference that is only apparent on T2-based Macs. CCC will no longer ask for a password for encrypted volumes that are not FileVault protected.
- The "Shut down if previously off" setting is now allowed on a non-scheduled task as long as that task is part of a scheduled group.
- Improved compatibility with VeraCrypt volumes.

Carbon Copy Cloner 5.1.6

October 12, 2018

- Improved the handling of Microsoft OneDrive, Google Drive File Stream and Dropbox placeholder files. Please note that if you're using any of these services, files that are marked as "online only" cannot be backed up. [Learn more here <http://bombich.com/kb/ccc5/limitations-online-only-placeholder-files>](http://bombich.com/kb/ccc5/limitations-online-only-placeholder-files).
- When showing the sidebar, the left side of the window will no longer get place under the Dock if the user has the Dock placed on the left side of the screen.
- Updated the default snapshot retention policy that gets applied to the startup disk. The default settings are now more conservative, so fewer snapshots will be retained on the startup disk. Note that you must apply the new default settings if snapshots are already enabled for your startup disk.
- When deleting the last task, the new task that's created to replace it is now named "CCC Backup Task" (rather than "Untitled") and it is no longer marked "edited" by default.
- Final Cut Pro "fcpbundle" files are now treated as ordinary folders in the Task Filter window, allowing the user to exclude items within these bundles files from the backup task.
- Addressed an edge case scenario where the permissions of the root folder of the destination could be set to values that prevent the logged-in user from accessing that volume.

Carbon Copy Cloner 5.1.5

September 17, 2018

- CCC now proactively prompts Mojave users to grant Full Disk Access to CCC and its helper tool so CCC

can back up all of the user's Application Data.

- Minor improvement to the handling of sparse files.
- When connecting to a remote Mac via the Remote Macintosh option in the Source and Destination selectors, a timeout that might occur due to a firewall or other Remote Login configuration problem is now greeted with more helpful advice (rather than reported as an "internal error").
- Changes to a custom filter expression or rule type now causes the task to be marked as edited.
- CCC now excludes the Dropbox ".dropbox.cache" folder. This folder's volatile content not only contains a bunch of garbage that shouldn't be backed up, but attempting to do so provokes a conflict between Dropbox and various anti-virus applications.
- Fixed the handling of a failure to mount an encrypted volume when clicking on the source or destination selector if the source or destination was a folder on that volume and CCC lacked the password for that volume.
- Fixed an issue in which CCC was sending two email notifications for a task that exceeds a run time limit.
- Fixed an issue in which a task group might run immediately when adding tasks to it.
- The email body template field in CCC's Preferences window now explicitly disallows macOS from performing 'smart quote' replacements. Such replacements resulted in corruption of the tokens in non-English locales, leading to the presence of the tokens in the resulting emails, rather than the substituted text (e.g. "##Nome dell'operazione##" instead of "Backup CCC").

Carbon Copy Cloner 5.1.4

July 27, 2018

- Some performance enhancements added to the previous version of CCC could occasionally lead to errors affecting tasks that specify a remote Macintosh source. This update modifies those performance enhancements to avoid those errors.
- Errors related to being unable to access Apple-private folders in the user home folder are now suppressed.
- Fixed a crashing issue that occurs when clicking on the source or destination selector. This only affects El Capitan users when VoiceOver is enabled.
- Added an option to the 'ccc' command-line utility to print schedule information in CSV format.

Carbon Copy Cloner 5.1.3

July 17, 2018

- Fixed an issue that would prevent CCC's User Agent from finding updates to CCC.
- Minor improvements to error handling related to creating snapshots.
- Animations are now reduced for 10.12+ users that are using the "Reduce motion" setting in the Accessibility preference pane.
- Improved performance of the "Find and replace corrupted items" checksumming pass on systems that have exceptionally fast storage.
- Fixed a edge-case couple crashing issues.

Carbon Copy Cloner 5.1.2

May 21, 2018

- Addressed a couple more minor, edge case issues related to unmounting a source snapshot at the end of the backup task.
- Fixed an error that occurred when selecting a folder on a remote Macintosh as a source or destination if that folder's name started with a space character.
- Fixed an issue that caused support request submissions to fail (i.e. via the "Ask a question about CCC" menu item in CCC's Help menu).
- Fixed a date math error that occurred when trying to adjust the initial fire date after a time zone change

occurred.

- Fixed a drawing anomaly that occurred when selecting multiple rows in the Snapshots or Related Tasks tables.

Carbon Copy Cloner 5.1.1

May 4, 2018

- The "Use strict volume identification" setting has always been disabled when the destination lacks a unique identifier (because the setting isn't applicable in that case). Now we also uncheck that box in those cases to avoid any confusion about whether that setting will be applied.
- Minor adjustments to the timing of snapshot creation on the source at the beginning of the task. These accommodate archiving of the source volume's helper partitions and also resolve potential conflicts when several tasks are started simultaneously that use the same source volume.
- The postflight destination unmount subtask is no longer skipped when a task is aborted due to a time limit overrun.
- Fixed an issue related to manually mounting an encrypted source or destination volume (when clicking on the source/destination selector).
- Fixed a cosmetic issue in which custom filters with multiple suffixes (e.g. '*.tar.gz') would appear to not be applied to matching files in the Task Filter window, despite actually matching those files during task run time.

Carbon Copy Cloner 5.1

April 24, 2018

- Added support for creating a snapshot on an APFS-formatted source at the beginning of the backup task. This snapshot is then mounted and used as the source for copying files. By using a read-only volume as the source, we avoid rare, but potential conflicts that can occur during the backup task if files are modified while being copied.
- CCC's SafetyNet feature is now built on top of APFS snapshots when the destination is an APFS volume and snapshot support is enabled for that volume.
- CCC will create a snapshot on APFS destination volumes at the end of a backup task to establish a point-in-time restore point.
- CCC offers a highly-tunable snapshot retention policy that allows you to define how long snapshots will be retained (hourly, daily, weekly), and also allows you to define a minimum amount of free space to retain on the volume.
- CCC's Disk Center offers detailed insight into the snapshots that CCC and Time Machine have created on your APFS volumes. Quickly see how much space those snapshots are consuming, and delete one or many snapshots with the press of a button.

Carbon Copy Cloner 5.0.9

February 15, 2018

- This update implements a workaround for [a serious flaw that we've discovered in macOS](http://bombich.com/blog/2018/02/13/mac-os-may-lose-data-on-apfs-formatted-disk-images) [that can lead to data loss when using an APFS-formatted disk image](http://bombich.com/blog/2018/02/13/mac-os-may-lose-data-on-apfs-formatted-disk-images). If you're running macOS High Sierra, please apply this update and review any tasks that back up to a disk image on a network volume. Note: this flaw applies to APFS disk images only — ordinary APFS volumes (e.g. your SSD startup disk) are not affected. Disk images are not used for most backup task activity, they are generally only applicable when making backups to network volumes.

Carbon Copy Cloner 5.0.8

February 5, 2018

- Fixed an issue introduced in CCC 5.0.6 in which CCC was mishandling the encoding of a network volume whose username or hostname contained special characters (e.g. "some%20user@Airport%20Base%20Station.local"). That led to errors mounting the affected network volume during an automated backup task.
- Errors related to creating a Recovery HD archive are now suppressed if those errors are the result of the user stopping the backup task while CCC was creating the Recovery HD archive.

Carbon Copy Cloner 5.0.6

January 30, 2018

- We made some improvements to the postflight option that unmounts the destination volume. If the destination is an encrypted volume, the volume will now be immediately locked when unmounted (negating the need for a separate postflight script as referenced in our blog). If the destination is an ordinary volume and the only partition on an external device, the destination device should be more likely to spin down the disk.
- Improved the efficiency of copying sparse files on APFS volumes. Sparse files appear larger than the amount of data they actually contain. In the wild, we've seen sparse files used by VMWare.
- Notifications prompting you to reattach a missing source/destination will now be revoked when the task starts to run next (e.g. when you attach the missing disk).
- Fixed a subtle timing issue that occurs when a scheduled task with an hourly run time limit starts a couple seconds early. A task with such a limit would previously have stopped immediately, claiming that it was running outside of its allowed time window.
- The remote Macintosh option now handles IPv6 addresses more gracefully.
- Addressed an edge-case scenario in which CCC would set overly-restrictive ownership/permissions settings on the destination root folder.
- The Task Filter window now correctly shows the application of a system items exclusion filter when the destination is a NAS volume that is not currently mounted.
- Fixed a behavior problem in the Task Filter window that arose after refreshing the size of a folder that had excluded items.

Carbon Copy Cloner 5.0.5

December 11, 2017

- Fixed a scheduling issue in which tasks would not be scheduled for the original start time hour (in local time) after a time zone switch and a restart.
- Progress indication during a "Backup with Health Check" is no longer errantly indeterminate.
- Addressed an issue that was introduced by the 10.13.2 update which causes Remote Macintosh setup to fail with an internal error.
- Fixed an issue in which CCC was unable to mount the source for an HFS+ Recovery HD cloning task.
- Custom port numbers are now supported for AFP and SMB hosts.
- The task outlook table now correctly displays the run times for tasks configured to run weekly with a repeat interval greater than 1.
- Fixed an issue in which some tasks were getting errantly marked with a "task failed" badge.
- Clicking on a task finished notification will now open the CCC application and select the relevant task.
- Fixed an issue in which a backup task involving a remote Mac would stall if the source or destination volume on the remote Mac was not available.
- ZFS volume mount notifications are now handled more effectively.
- The CCC command line application will now exit immediately after starting a task group.

- Made some minor improvements to CCC's task database that should make it more resilient to corruption.
- Fixed a minor window sizing issue specific to Yosemite and the dialog that is produced when disabling the SafetyNet setting.
- Suppressed an errant error message produced by High Sierra that can occur when converting a sparse disk image to a read-only format.

Carbon Copy Cloner 5.0.4

November 2, 2017

- Fixed the resolution of the task badge on Retina displays on High Sierra.
- When creating a disk image, the disk image is now formatted as APFS if the source is an APFS volume. CCC also creates the Preboot and Recovery volumes on these disk images so that they can be restored using Disk Utility (in addition to being restorable via CCC).
- Items marked as hidden now stay reliably hidden on an HFS+ destination on High Sierra.
- Addressed an issue in which a task that specifies a remote Macintosh as the source or destination would re-try the connection too aggressively if the remote host was unavailable.
- Fixed the free space indicator for APFS volumes when viewing a volume's details in CCC's sidebar.
- Implemented an alternative key installation method for cases where the remote Macintosh cannot accept files via scp.
- Improved the drawing of the task outlook table when viewing a task group.
- Minor enhancements to the CCC command-line utility.
- The source/destination contextual menu items now more consistently refer to the underlying volume for a disk image, and mounting/unmounting the underlying network volume for a disk image now works. Also tweaked the subtitle offered when an underlying network volume is not mounted. Previously it said "{sharepoint}" is missing', now it says "{sharepoint}" is not mounted'.
- The "Show Details" button in CCC notifications that are presented as alerts now correctly opens the Task History event in CCC.
- CCC now handles an undocumented Keychain Services error code that was occurring when CCC was trying to open its keychain for the first time (i.e. before the keychain yet exists). This resolves an issue that some High Sierra users might have encountered when trying to save a password to CCC's keychain.
- Addressed an issue in which a backup task could stall while "Cleaning up" if the task was configured to unmount the destination volume, and Spotlight was dissenting the volume unmount.
- Minor improvements to the Task Trend chart in the Task History window.

Carbon Copy Cloner 5.0.3

September 29, 2017

- Addressed an issue in which task history events weren't getting recorded for a subset of backup tasks.
- Improved the performance of CCC's archive pruning utility.
- Fixed an issue in which CCC may not have presented a dialog to update the HFS+ Recovery HD volume on the destination when the source is an APFS volume.
- Fixed a window resizing issue affecting the "New disk image" Save panel for High Sierra users.
- Fixed issue affecting Yosemite users in which custom filters in the Task Filter window were hidden despite the custom filter table being shown.
- Fixed an issue in which the setting to skip weekend days was getting disabled for tasks configured to run on a daily or weekly basis.

Carbon Copy Cloner 5.0.2

September 21, 2017

- Added a menu option to clear CCC's entire Task History.

- Added Stop Loading, Reload, Make Text Larger, and Make Text Smaller buttons to the Documentation tab of CCC's Help window.
- Added a couple more ways to rename tasks and groups, because a lot of people were having trouble with this. Previously the semantics were similar to that of the Finder, e.g. click on the text of the title, or select the task and press the Return key to make the text editable. Now you can double-click a task in the task list to make the title text editable, or you can right-click on the text and choose the option to rename the task.
- Tasks listed in the CCC menubar application are now sorted in the same manner as defined in the Tasks table of the main application. The same is now true for the View menu in the main application.
- The run time order for grouped tasks is now considered when sorting the Tasks table by next run time.
- Fixed the "failed to set global attribute" error on first launch for upgrading users.
- Fixed a bug that could cause a spin if a CCC v4 imported task had been configured to run weekly, only on Sunday, and also with a runtime limit that prevented it from running on weekends.
- Fixed a condition in which CCC would report that an error occurred while updating the dynamic linker shared cache and kernel extension cache (it wasn't an error, it was just new debug information).
- Resolved some edge cases that caused remote Macintosh authorization setup to fail.
- Connection reset errors (e.g. remote host drops the connection) now cause a remote Mac task to be restarted.
- Imported v4 tasks with a remote Mac destination are no longer prevented from copying system items (i.e. because we don't yet know the destination filesystem).
- Fixed an errant cloning coach message that said the destination on a remote Mac wouldn't be bootable because it wasn't the root of a volume.
- Fixed the source/destination label in cases where the item is a remote Mac. The label wasn't updating consistently, and sometimes was left at the stub text.
- Addressed some cases where CCC would consistently prompt the user for a guided setup when a task with "restore" in its name is present and specifies the current startup disk as the destination, or when the relevant destination volume is named "Macintosh HD".
- Guided Setup and Guided Restore is now disabled if VoiceOver is active. Some VoiceOver users found that these bubble tips were stealing VoiceOver's focus, making task setup more challenging.
- Fixed an issue in which CCC would become unresponsive if you configured a daily or weekly task to start at 7AM, and then checked the box to apply an hourly runtime limit.
- System files are now excluded if the source has an OS older than 10.13 and the destination is APFS. Added a Cloning Coach message to explain the limitation.
- APFS as a system destination is only supported when the running system is 10.13+.
- Fixed the abbreviation for "Monday" that was incorrectly translated in German to "Monat" (rather than "Mo").
- Increased the threshold for system uptime at the time of CCC load to 90 for determining whether the system just restarted. This accommodates slower systems that would otherwise skip a task that was missed while the system was off.
- Write failures on NAS volumes are now more consistently presented as showstoppers that cause the task to fail rather than individual file errors in an otherwise-successful backup task.
- Added some tolerance to the hourly run time limits such that tasks firing a few seconds before the limit window will be allowed to run.
- Fixed an issue in which running a task group could lead to an inability to sleep the system.
- Tasks that are both disabled and suspended now correctly get the "activate/leave suspended" dialog.
- A task can now be moved back outside of a group if there is only one group present and all tasks are part of that group.
- Enabled expansion tooltips for the task name in the task outlook table.
- Fixed an issue in which the destination APFS Preboot volume was not getting properly populated when using an HFS+ source volume.
- The Preferences window is no longer moved to the main screen if its on the secondary screen and the secondary screen is positioned below the main screen.
- Improved some dialog behavior for tasks configured to run on source/destination reconnect, that also are configured to prompt before proceeding and issue a periodic reminder. The CCC User Agent now revokes a reminder prompt if you attach the affected disk before dismissing the reminder prompt.
- Made some minor modifications to CCC's global exclusions list that resolves a startup delay when booting from the backup volume.

- "Delete a SafetyNet folder" now accepts any item that is in the Trash.
- The "Auto adjust" setting being disabled will no longer cause the advanced settings view to be expanded if the SafetyNet is set to Off.
- Fixed an errant Cloning Coach message that said file metadata would not be preserved on a disk image on a network volume.
- Cancelling out of the filter window without making changes will no longer leave the task in the edit state.
- System folders are no longer excluded when copying to or from a folder on the startup disk.
- Fixed a software update issue in which CCC might check for updates on startup if the update interval was set to never check.
- Fixed the calculation of a task's elapsed time as noted in the Task Plan.

Carbon Copy Cloner 5.0

August 24, 2017

- New interface for defining task filters:
 - CCC can calculate the amount of space consumed by the files on the source. If you exclude items from the task or add custom filters to exclude items based on patterns, CCC will report the total protected size of each folder (and cumulatively).
 - The task filter can now exclude everything by default, allowing you to specify only what items should be included in the backup task. This is in contrast to the default behavior in which CCC includes everything by default, allowing you to specify what is excluded from the backup task.
 - Filters can be imported and exported. Additionally, when you change the source for your backup task, CCC will now ask you whether you want to reset the task filter (rather than simply resetting it).
 - The effects of custom and global filters are immediately apparent.
 - A QuickLook panel shows a preview of the selected file.
 - Contents can be sorted by name, modification date, or size.
 - You can select an item, then Shift+click on the checkbox for another item within the same parent folder to select/deselect all of the items in between.
 - If you really want to, you can have CCC copy your Trash. There's a checkbox for that now!
- CCC's SafetyNet pruning settings will now automatically adapt to the amount of data your tasks need to copy. If a backup task runs out of space on the destination, CCC will revisit the pruning of the SafetyNet folder, then resume copying.
- The SafetyNet pruning feature is now available for Remote Macintosh destinations.
- The setup procedure for backing up to a remote Macintosh has been greatly simplified.
- Task filters can be configured for Remote Macintosh source volumes with the same ease as locally-attached volumes.
- Tasks can be sorted by name, exit status, last run date, next run date, or manually.
- Tasks can be placed into groups for organizational purposes, and also to be run collectively as a group.
- A new Guided Setup feature offers initial task configuration tips for first-time users.
- Upon detecting that your Mac is booted from a CCC backup volume, CCC will present a new Guided Restore option. In the guided restore, CCC will create a new restore task, select the startup disk as the source, then present coaching tips that guide the user through selecting the destination and (optionally) excluding items from the restore task.
- Tasks can be scheduled to run once at a particular time in the future. After that run, the tasks will revert to run "only when I click the Clone button".
- Hourly runtime limits allow the user to limit a task to running only between 5PM and 7AM, for example. Hourly limits will prevent a task from starting if it's outside the specified run time, and if the task runs past the allowed end time, the task will be stopped.
- CCC's Task History window now offers a trend chart. The trend chart shows how your tasks are performing over time, and how many files/how much data gets copied each time your task runs.
- The destination selector offers a visual disk usage indicator.
- You can right-click on a volume (e.g. in the source/destination selectors) to mount or unmount that volume, or to reveal it in the Finder.
- The source and destination selections can be reset to "Choose a source/destination".

- The CCC User Agent will now check for updates on the schedule defined in the main application.
- Some of the the Cloning Coach messages have been aggregated and simplified to seem less daunting to novice users.
- The "Find and replace corrupted files" setting can now be limited to run once per week or once per month.
- Tasks can be imported and exported, making it simpler to migrate task settings to a second Mac.

Carbon Copy Cloner 4.1.24

October 30, 2018

Carbon Copy Cloner 4.1.23

June 21, 2018

Carbon Copy Cloner 4.1.22

May 21, 2018

Carbon Copy Cloner 4.1.21

February 12, 2018

Carbon Copy Cloner 4.1.20

October 25, 2017

Carbon Copy Cloner 4.1.19

September 12, 2017

Carbon Copy Cloner 4.1.18

August 16, 2017

Carbon Copy Cloner 4.1.17

July 19, 2017

Carbon Copy Cloner 4.1.16

June 27, 2017

Carbon Copy Cloner 4.1.15

May 19, 2017

Carbon Copy Cloner 4.1.14

May 11, 2017

Carbon Copy Cloner 4.1.13

January 12, 2017

Carbon Copy Cloner 4.1.12

December 8, 2016

Carbon Copy Cloner 4.1.11

December 6, 2016

Carbon Copy Cloner 4.1.10

September 16, 2016

Carbon Copy Cloner 4.1.9

June 14, 2016

Carbon Copy Cloner 4.1.8

June 6, 2016

Carbon Copy Cloner 4.1.7

February 2, 2016

Carbon Copy Cloner 4.1.6

December 3, 2015

Carbon Copy Cloner 4.1.5

December 2, 2015

Carbon Copy Cloner 4.1.4

September 1, 2015

Carbon Copy Cloner 4.1.3

May 19, 2015

Carbon Copy Cloner 4.1.2

May 6, 2015

Carbon Copy Cloner 4.1.1

May 5, 2015

Carbon Copy Cloner 4.1

April 28, 2015

Carbon Copy Cloner 4.0

October 1, 2014

Carbon Copy Cloner 3.5.3

October 22, 2013

Carbon Copy Cloner 3.5

July 20, 2012

Carbon Copy Cloner 3.4

July 20, 2011

Carbon Copy Cloner 3.3

September 21, 2009

Carbon Copy Cloner 3.2

March 18, 2009

Carbon Copy Cloner 3.1

March 24, 2008

Carbon Copy Cloner 3.0

September 18, 2007

Carbon Copy Cloner 2.3

October 23, 2003

Carbon Copy Cloner 2.0

November 19, 2002

Carbon Copy Cloner 1.0

January 18, 2002

Credits

CCC includes, in source or binary form, the following open source projects.

vsdbutil and hfs.util

Carbon Copy Cloner contains portions of source code available under the Apple Public Source License. That code may be downloaded by clicking the links below.

- [vsdbutilmain.c](https://opensource.apple.com/source/diskdevcmds/diskdevcmds-332.11.5/vsdbutil.tproj/vsdbutilmain.c.auto.html) <<https://opensource.apple.com/source/diskdevcmds/diskdevcmds-332.11.5/vsdbutil.tproj/vsdbutilmain.c.auto.html>> (View our modifications: [vsdbutil.h](http://bombich.com/software/opensource/vsdbutil.h) <<http://bombich.com/software/opensource/vsdbutil.h>> and [vsdbutil.c](http://bombich.com/software/opensource/vsdbutil.c) <<http://bombich.com/software/opensource/vsdbutil.c>>)
- [hfsutil](https://opensource.apple.com/source/hfs/hfs-226.1.1/hfsutil/) <<https://opensource.apple.com/source/hfs/hfs-226.1.1/hfsutil/>> (Our only modification is #define HFSUIDSUPPORT 1 in [hfsutilmain.c](#))

View the APSL 2.0 license <<https://www.opensource.apple.com/apsl>>

rsync

Carbon Copy Cloner also includes, independently in binary form, rsync version 3.0.6. rsync is made available under the GNU General Public License. Per the license requirements, the source code and my modifications may be downloaded via the links provided below. This modified software is provided at no cost and with no warranty, also per the GNU GPL.

- Download the complete rsync 3.0.6 project <<https://rsync.samba.org/ftp/rsync/src/rsync-3.0.6.tar.gz>>
- Download the rsync 3.0.6 patches <<https://rsync.samba.org/ftp/rsync/src/rsync-patches-3.0.6.tar.gz>>
- Download the diff file (diff between 3.0.6 + [crtimes.diff, fileflags.diff, log-checksum.diff, and backup-dir-dels.diff] and my modifications) <<http://bombich.com/software/opensource/rsync3.0.6-bombich20190114.diff>>
- View the GNU GPL <<http://bombich.com/software/opensource/COPYING.txt>>

Carbon Copy Cloner is not a derivative work of rsync. Rsync is called in binary form only. You can access the build of rsync that is included with CCC via the application bundle: right-click on the CCC application icon, choose "Show Package Contents", then navigate to Contents > MacOS > rsync.

Sparkle

Carbon Copy Cloner leverages [Sparkle](http://sparkle-project.org) <<http://sparkle-project.org>> for handling software updates. Sparkle is Copyright (c) 2006 Andy Matuschak and licensed under the following terms:

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT

HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

[View the complete license for Sparkle, including external attributions](http://bombich.com/software/opensource/SparkleLicense.txt)
<<http://bombich.com/software/opensource/SparkleLicense.txt>>

skpsmtplib

The SimpleSMTP framework included with CCC is a derivative work of the [skpsmtplib](https://code.google.com/p/skpsmtplib/) project. skpsmtplib is licensed under the MIT license:

The MIT License (MIT)

Copyright (c) 2008 Skorpiostech, Inc. All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

CocoaFob

We leverage [CocoaFob](https://pixelespressoapps.com) <<https://pixelespressoapps.com>> for license generation and verification in Carbon Copy Cloner. CocoaFob is distributed under the [BSD License](http://www.opensource.org/licenses/bsd-license.php) <<http://www.opensource.org/licenses/bsd-license.php>>, Copyright © 2009-2015, PixelEspresso. All rights reserved. The following statement pertains to CocoaFob:

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Carbon Copy ClonerとAPFSについて知っておくべきこと

AppleはmacOS High Sierraで新しいファイルシステムを導入しました。そこで当然のこととして、Carbon Copy Clonerがこれをどのように扱い、この新しい変更がバックアップにどのような影響をもたらすのか心配されていることでしょう。“ファイルシステムとは何か？”という疑問もあるかもしれませんが、そこから始めましょう。そして徐々に技術的な詳細に移りましょう。

- [ファイルシステムとは何ですか？](#)
- [どうしてAppleは新しいファイルシステムを導入したのですか？](#)
- [使っているMacをHigh Sierra \(またはそれ以降\) にアップグレードすると、自分の起動ディスクはAPFSに変換されますか？](#)
- [HDDで最初にHigh Sierraにアップグレードして、その後SSDにクローンした場合、SSDはAPFSに変換されますか？](#)
- [OSのアップグレードが私の起動ディスクをAPFSに変換した場合、私のバックアップディスクに何かする必要がありますか？APFSとして消去する必要がありますか？](#)
- [CCCを使ってAPFS起動ディスクを別のMacにクローンできますか？](#)
- [CCCは暗号化されたAPFSボリュームをサポートしますか？](#)
- [APFSには“クローン”機能があると聞きました。それはCCCがしていることと同じですか？](#)
- [バックアップディスクのディスク使用状況がソースディスクのディスク使用状況と一致しないのはなぜですか？](#)
- [APFSの新しいスナップショット機能はバックアップ方法においてどんな役割を果たしているのですか？](#)
<<http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes>>
- [macOS Catalinaのこれらの "{volume name} - データ" ボリュームは何ですか？](#)
<<http://bombich.com/ja/ja/kb/ccc5/working-apfs-volume-groups>>

ファイルシステムとは何ですか？

ファイルシステムはMacのソフトウェアでおそらく最も重要な部分でしょう。また、最も明らかな箇所の1つと言えます。少なくとも正しく動作しているかどうかという点において。すべてのユーザとすべてのアプリケーションはファイルシステムを使用します。ファイルシステムはハードドライブのファイルのすべての記録を保ち、整理します。また、どのユーザとアプリケーションがそれらのファイルにアクセスできるかを判断します。ファイルシステムはファイル数とそれらのファイルが消費している容量も記録しています。ファイルを検索、ファイルを開く、ファイルを移動する、ファイルを保存する、ファイルを削除する、そのたびに、そのアクションを実行しているのがファイルシステムです。

どうしてAppleは新しいファイルシステムを導入したのですか？

Appleのレガシーファイルシステム、HFS+は、約20年間うまく動作してきました。そして、Appleはその間一貫して改良を続けてきました。例えば、Appleは拡張属性、ファイルシステムの圧縮、ファイルシステムのジャーナリング、およびフルディスク暗号化のサポートを追加しました。これらすべての新しい機能は、新しいオペレーティングシステムの機能と歩調を合わせ、ファイルシステムの信頼度を上げるために追加されました。しかし、そのファイルシステムは当初Mac OS 8のために作成され、プラターベースのハードドライブのためにデザインされました。ストレージの技術は過去20年で大きく様変わりし、HFS+を修正することでそれらの変更についていくことはますます困難になりました。新しいiOSと新しいストレージ技術のチャレンジを満たすために、AppleはApple File System、つまり“APFS”をHigh Sierraで導入しました。

使っているMacをHigh Sierra (またはそれ以降) にアップグレードすると、自分の起動ディスクはAPFSに変換されますか？

macOS High Sierraにアップグレードすると、すべてのフラッシュストレージ設定のあるシステムは自動的に変換されます。ハードディスクドライブ (HDD) のあるシステムとFusion Driveは、macOS High SierraではAPFSに変換されません。Mojaveにアップグレードする際、HDDとFusionボリュームもAPFSに変換されます。 [APFSへの移行から逃れることはできません <https://support.apple.com/en-us/HT208018>](https://support.apple.com/en-us/HT208018)

HDDで最初にHigh Sierraにアップグレードして、その後SSDにクローンした場合、SSDはAPFSに変換されますか？

macOS High SierraまたはMojaveを実行している場合、HDDまたはSSDのどちらも自動的にAPFSに変換されません。しかし、SSDにクローンする前にSSDをAPFSとして消去することを選択できます。High SierraおよびMojaveでCarbon Copy Cloner 5を使用する場合、APFSもHFS+もどちらも有効なコピー先フォーマットです。macOS Catalinaのシステムボリュームのバックアップを作成する場合、CCCはコピー先ボリュームをHFS+からAPFSに自動的に変換します [<http://bombich.com/ja/kb/ccc5/working-apfs-volume-groups#convert>](http://bombich.com/ja/kb/ccc5/working-apfs-volume-groups#convert)。但し、ユーザからの明示的な承認が与えられている場合に限りです。

OSのアップグレードが私の起動ディスクをAPFSに変換した場合、私のバックアップディスクに何かする必要がありますか？APFSとして消去する必要がありますか？

macOS High SierraまたはMojaveにアップグレード後バックアップディスクに何もする必要はありません (そしてまた、macOS Catalinaでも、CCCはコピー先を自動的にAPFSに変換するので、コピー先ボリュームに何もする必要はありません)。APFSフォーマットされたHigh SierraまたはMojaveの起動ボリュームのHFS+バックアップを持つことは差し支えありません。それは将来の復元で、APFSフォーマットされたボリュームにさえも問題なく機能します。バックアップディスクがSSDの場合、またはコピー先の消去を計画している場合は、APFSとして消去することを強くお勧めします。

Mojaveを実行しています。HDDコピー先をAPFSとして消去することは可能ですか？コピー先でAPFSを使用する利点はありますか？

コピー先ボリュームをいずれにせよ消去するつもりであれば、そのボリュームをAPFSとしてフォーマットすることをお勧めします。

回転式ディスクのAPFSの列挙パフォーマンスは、同じハードウェア上のHFS+よりもまだ圧倒的に劣っています [<http://bombich.com/ja/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>](http://bombich.com/ja/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives) が、その一方でHFS+よりもAPFSを選択する利点がいくつかあります。例えば、APFSコピー先はその時点 (point-in-time) の復元を可能にするスナップショットを保管することができます。また、APFSボリュームは [スパスファイル <http://bombich.com/ja/ja/kb/ccc5/glossary-terms#s>](http://bombich.com/ja/ja/kb/ccc5/glossary-terms#s)

をサポートするので、APFSフォーマットされたボリュームにバックアップする際、名前の比較の問題 (例えば、ソースのAPFSボリュームのファイルに“é”のようなUnicode文字が含まれている場合)

に遭遇する可能性が少なくなります。また、HFS+ 暗号化されたボリュームからT2

Macを起動することはできません。ですから、T2

Macを使用していて、バックアップの暗号化が必要な場合、APFSを使用する必要があります。

CCCを使ってAPFS起動ディスクを別のMacにクローンできますか？

macOSのアップグレードをインストールすると

、お使いのMacにmacOSインストーラがファームウェアのアップグレードを適用します

[<https://support.apple.com/en-us/HT208020>](https://support.apple.com/en-us/HT208020)。このファームウェアアップグレードはクローンのプロセスの一部にはなれません。macOSインストーラのみがMacintoshをアップグレードして、APFSをサポートできます。まだmacOSインストーラからファームウェアアップグレードを受け取っていないMacintoshにAPFSボリュームをクローンしようと試みても、そのMacintoshはAPFSボリュームから起動することはできません。MacがmacOSインストーラからファームウェアアップグレードを受け取ると、MacはCCCの起動可能なバックアップからAPFSに起動できるようになります。しかし、macOSのメジャーアップグレードはすべて、新しいオペレーティングシステムの使用を許可するために新しいファームウェアアップグレードを必要とする可能性がありますので、注意してくだ

さい。

また、これはターゲットディスクモードを実行中のMacintoshにも適用されますので、注意してください。インストーラを使って1台のMacをHigh Sierra (またはそれ以降) にアップグレードすると、2台目のMacをターゲットディスクモードに起動できません。2台目を最初のものに接続してから、High Sierra (またはそれ以降) をターゲットディスクモードでMacにクローンしてください。必要なファームウェアアップグレードはターゲットディスクモードで起動されたMacには適用できません。macOSインストーラを2台目のMacで実行する必要があります。2台目のMacがmacOSインストーラを経由してファームウェアアップグレードを受け取ると、最初のMacをターゲットディスクモードで起動されている2台目のMacにクローンできます。

CCCは暗号化されたAPFSボリュームをサポートしますか？

はい、CCC 5は暗号化されたAPFSボリューム (別名: FileVault暗号化) とクローンできます。但し、CCCは暗号化の処理には一切関与しませんので注意してください。暗号化はボリュームの機能で、ファイルを書き込むツールの機能ではありません。起動ディスクでFileVaultを有効にしている場合、起動ディスクのファイルは暗号化されます。それらのファイルは、アプリケーションによって開かれた際に、ファイルシステムによりその場で暗号化されます。同様に、FileVaultをコピー先ボリュームで有効にしている場合 (例えば、バックアップから起動中、環境設定のセキュリティパネルを経由して)、コピー先のファイルは暗号化されます。CCCはそれらのファイルを暗号化する必要はありません。ディスクに書き込まれていく時にファイルシステムによってその場で暗号化されます。

APFSには“クローン”機能があると聞きました。それはCCCがしていることと同じですか？

いいえ。APFSのクローン機能はCCCが実行するクローンとはまったく無関係です。

APFSのクローンは、余分な空き領域を消費することなく、**同じボリュームに** ファイルのコピーを即座に作成します。ファイルをクローンする際、ファイルシステムはデータのコピーを作成しません。むしろ、そのファイルに最初のファイルから独立して修正できる第2のリファレンスを作成します。この2つのファイルは、同一のまま残るファイルの一部のディスクで領域を共有します。しかし、どちらかのファイルに加えられた変更内容はディスクの異なる部分に書き込まれます。APFSのファイルのクローンはファイルのコピーを同じボリュームに作成する時のみ動作します (例えば、Finderでファイルまたはフォルダを複製する場合)。一般的にCCCはボリューム間でファイルをコピーしますので、APFSのクローンはその種のタスクには適用されません。

覚えておくべき重要な点は、APFSのファイルクローンは起動ディスクの領域を節約できるということです。一方、CCCのクローンはソースディスクに問題が起きた場合にデータを保存して置けるということです。これらはまったく異なる目的を果たしています。APFSのファイルクローンはバックアップを作成するという点とはまったく関係がありません。

バックアップディスクのディスク使用状況がソースディスクのディスク使用状況と一致しないのはなぜですか？

CCCの**グローバル除外** <<http://bombich.com/ja/ja/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task>> はSafetyNet機能と同様に、過去のディスクの使用状況においてこれまで正当な違いをもたらしてきました。しかし、前述のAPFSのファイルクローン機能は、この懸念に新しい側面を追加しました。APFSのファイルクローン機能がソースボリュームで領域を節約する一方で、これらの領域節約はファイルを別のボリュームにコピーする際に必ずしも適用できないことがあります (というのはAppleは1つのファイルが別のファイルのクローンであるかどうか

かを私たちが判断するための手

段を提供しないからです)。さらに悪いことには、**Finderはファイルのディスク使用状況を正確に表示しません**

<<https://youtu.be/KggyuL8mED0>>

。Finderは1つのファイルが別のファイルのクローンであるかどうかを考慮に入れませんが、Appleはこの判断をする方法を提供しないからです)。ですから、Finderはそれぞれのファイルとフォルダの合計サイズを計算し、ディスクの容量よりもはるかに高い合計値を表示します。

MacのディスクをAPFSに変換した場合、ソースとコピー先のディスク使用量は決して合計されないため、ソース

とコピー先を比較するための信頼できる測りにはならないということを理解してください。

追加情報

- ビデオ： CCCの起動可能なバックアップを使用して、High SierraからSierraにダウングレードするには <<https://www.youtube.com/watch?v=UMvSfDTaLwY?t=9m44s>>
- バックアップボリュームをmacOSのインストール用に準備するには <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>>
- ビデオ： macOS High Sierraでディスクユーティリティと動作してCCCのバックアップディスクを準備するには <<https://youtu.be/oEfqfMf2z9k>>
- CCCのバックアップをテストするには <<http://bombich.com/ja/ja/kb/ccc5/how-verify-or-test-your-backup>>

ヘルプが必要な時は

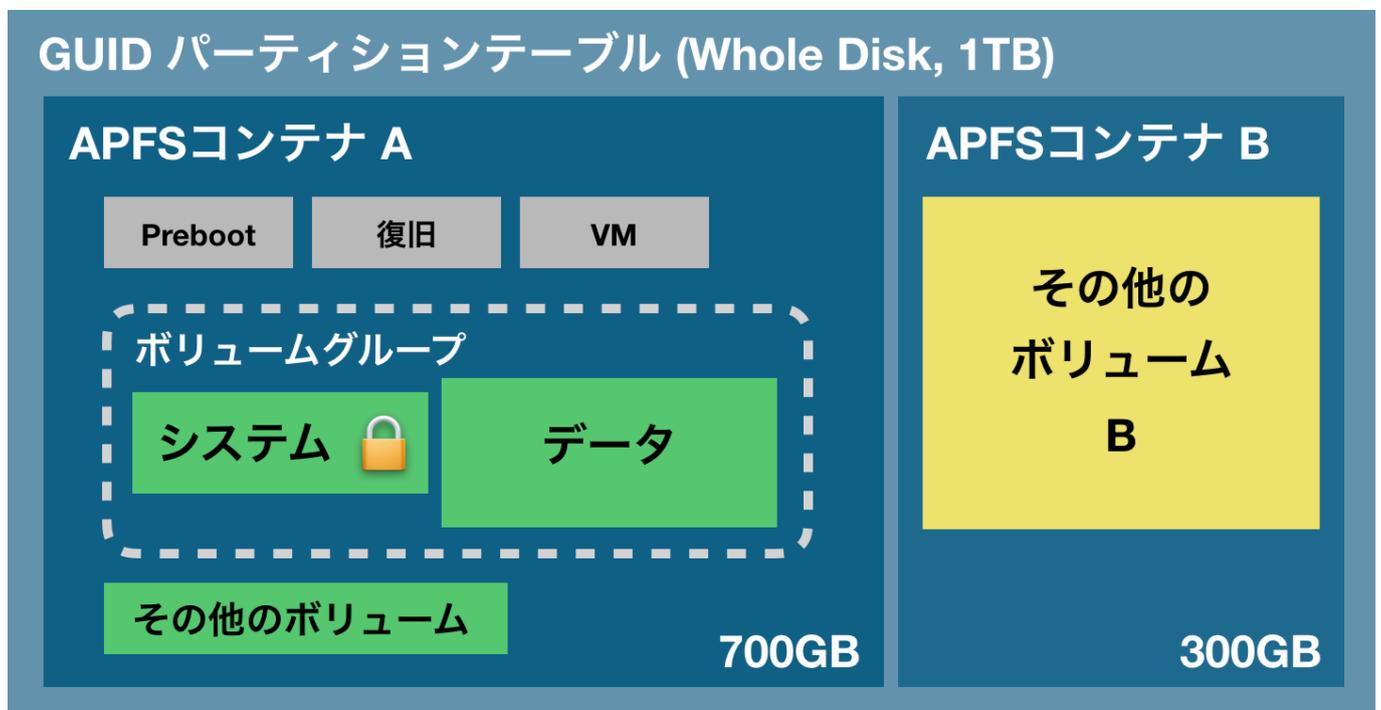
行き詰まったり、何かアドバイスが必要な場合は、CCCから直接お問い合わせいただけます。CCCの“ヘルプ”メニューから“質問する”を選択して、ヘルプデスクまで質問をお寄せください。

APFSボリュームグループと動作するには

数年前、AppleがAPFSファイルシステムを紹介したとき、次の新しい概念と一緒に登場しました: APFS コンテナです。すべてのAPFSボリュームは1つのコンテナの中にあり、そのコンテナはディスクのパーティションスキームの中にあります。コンテナ内のすべてのボリュームはコンテナで利用可能なスペースを共有します。別のAPFSコンテナはお互いのスペースを共有しません。

macOS High Sierraで、Appleはボリュームに **役割** の概念を追加しました。その時点では、役割は3つだけで、大部分は平均的ユーザが気付くものではありませんでした: Preboot、復旧、そしてVM (仮想メモリ) です。これらの役割により、システムが特定のボリュームを特定の目的に識別できるようになり、その後ボリュームを特定の方法で扱えるようになります (例えば、上記の役割を持つ任意のボリュームをデフォルトで非表示にしたり、またデフォルトでマウントしないようにできます)。

以下の記述でこれらのAPFSの概念を説明しましょう:



パーティションスキームは物理的ディスク全体を網羅します。パーティションスキーム内には1つ以上のAPFSコンテナを作成でき、それぞれのコンテナ内には1つ以上のAPFSボリュームを作成できます。過去のパーティションとは異なり、コンテナ内のすべてのボリュームはコンテナに割り当てられたスペースを共有します。上の例では、3つのグレーのヘルパーパーティション、システムとデータボリューム、そして“その他のボリューム”、それらすべてがその700GBのストレージにアクセスできます。しかし、“その他のボリューム B”は別のコンテナにあるので、コンテナ“A”のボリュームとスペースを共有しません。通常、ディスクはこのようにパーティションされていませんが、例えば、同じディスクにある起動ディスクのクローンを維持したい場合 (例、デバロッパがテスト目的で)、それが必要になります。

新しい概念: APFSボリュームグループ

macOS Catalinaで、AppleはAPFSファイルシステムにもう1つの新しい概念を紹介しました: **ボリュームグループ** です。これはAPFSコンテナ内のボリュームを概念的にグループ化したもので、新しいサブ構造ではありません。また、AppleはAPFSボリュームに利用できる役割の数を大幅に広げました (現在16のユニークな役割があります)。Catalinaにアップグレードすると、現在使用中のmacOSシステムボリュームは名前が変更されます。例えば、“

Macintosh HD - Data”にです。その役割は**データ**に設定され、その後、新しいボリュームが**システム**の役割と共に起動ディスクのAPFSコンテナに追加され、同時にデータボリュームと共にグループ化されます。そのグループ内の2つのボリュームは、特別な絆を共有し、Finderから、およびそれぞれのボリュームのファイルシステムから特別な扱いを受けます。ユーザの視点から見ると、これら2つのボリュームは1つの、統合されたボリュームとして扱われます。しかし、ディスクユーティリティを見ると、2つのボリュームは異なる、別個の項目として表示されます。

読み出し専用のシステムボリューム

おそらく、macOS

Catalinaで

の最大の変更を1つ

挙げるなら、システムボリュームが起動

時にマウントされる方法、つまり**読み出し専用**

ということです。ボリュームを読み出し専用に変更することで、攻撃者がmacOSのシステムボリュームのコンテンツに変更を加えることが不可能になります。だからと言って、お使いのMacがすべての考え得る攻撃から100%安全という訳ではありません。むしろ、それらの危険に対する防御の1つと考える方が良いでしょう。

macOS Big Surより、Appleは暗号で封印された “署名付きのシステムボリューム”

<https://developer.apple.com/news/?id=3xpv8r2m>

を

導入

して、シ

ステムボリューム

の保護を拡張しました。システムボ

リュームが起動時にマウントされることが**完全になくなり**

、代わりに、システムボリュームのスナップショットがマウントされ、起動ディスクとして使用されています。そのスナップショットは読み出し専用で、完全にイミュータブルです。

データボリューム

データボリュームはシステムボリュームの読み出し/書き込みの“影”と考えることができます。データボリュームにはすべてのユーザデータ (例、ホームフォルダ、他社製アプリケーション等) が含まれていますが、同時に、読み出し専用ボリュームに存在できない握りのシステムコンポーネントも含まれています。例えば、AppleはSafariをデータボリュームに配置しています。おそらく、より頻繁にアップデートできるからでしょう。現在の起動ディスクのデータボリュームは、システムの特別なマウントポイントにマウントされています。FinderからMacintosh HD > システム > ボリューム > {データボリューム名} と進むと、見つけられます。そこで目にするのは、システムボリュームのルートレベルのフォルダのレプリカです。これらのフォルダ内には、まだ書き込み可能なシステムコンポーネントがすべてあります。しかし通常、これらの項目はFinderに表示されません。というのは、Finderは2つのボリュームのコンテンツを視覚的に1つにして、1つのボリュームとして表示するからです。また、Finderがデータボリュームをその他すべてのボリュームの横にリスト表示することはありません。つまり、**データボリュームはマウントされていますが、非表示です。**

Firmlinksと絆を築くには

1つの統合されたボリュームで

あるという幻想を解き放つために、AppleはAPFSにFirmlinks

のサポートを追加しました。名前が暗示する通り、Firmlinkは概念的にソフトリンクとハードリンク間を繋ぎます

。しかし、おそらくその説明でそれらがより明確になる訳ではありません (ソフトリンクとハードリンクに精通し

ている人でさえも!)。Appleは、Firmlinkを2つのファイルシステム間の“双方向ワームホール”と説明しています。“

ユーザ”フォルダを例にとって見てみましょう。システムボリュームのルートレベルにある“ユーザ”フォルダは、実

際データボリュームのルートレベルにある“ユーザ”フォルダを指すFirmlinkです。システムボリュームの“/Users”フ

ォルダに進んでみると、実際データボリュームの“/Users”フォルダのコンテンツが表示されます。同様に、もしデ

スクトップのフォルダを見ているとして (つまり、データボリュームのコンテンツを見ている)、数レベル上に

進むとします。“ユーザ”フォルダの親に到達した時には、見ているのはもはやデータボリュームではなく、むしろ、そのFirmklinkによってシステムボリュームのルートレベルに転送されています。

macOS Catalinaにはシステムボリュームのさまざまなフォルダを、データボリュームの書き込み可能なフォルダにリンクする20ちょっとのFirmklinkがあります。興味があるなら、Firmklinkの全リストを起動ディスクの“/usr/share/firmlinks”から閲覧できます。

アプリケーションフォルダとFinderのおふざけ

Firmlinksはほぼ明白でわかりやすいですが、1つ実に顕著な例外があります。それはアプリケーションフォルダです。システムボリュームのルートレベルにあるアプリケーションフォルダは、データボリュームのルートレベルにあるアプリケーションフォルダへのFirmklinkです。しかし、起動ディスク > システム > ボリューム > データ > アプリケーション、と進むと、アプリケーションの大部分がそこにはないのに気が付くでしょう。しかし、システムボリュームのアプリケーションフォルダを見ると、それらはすべてそこにあります！ここでFinderがちょっとした魔法を使います。読み出し専用のシステムアプリケーションフォルダは、実はシステムボリュームの、システム > アプリケーション、と進んだ場所にあります。そして、Finderでアプリケーションフォルダを開くと、そのフォルダの集合体とデータボリュームのルートレベルのアプリケーションフォルダが表示されています。平均的ユーザにはこれが期待通りの動作で、それは素晴らしいことです。しかし、この同じ集合体はお使いのMacの現在の起動元ではない、他のシステムボリューム (例、お使いのバックアップディスク) に適用されていないことに気が付くでしょう。それらのボリュームで、表示されているシステムボリュームのルートレベルのアプリケーションフォルダを開くと、データボリュームのルートレベルのアプリケーションフォルダへのFirmklinkのコンテンツのみが表示されます

(例、Appleのアプリケーションは無く、サードパーティのアプリケーションとSafariのみ)。

しかし、安心してください。すべてのアプリケーションはバックアップされています！それらはバックアップボリュームの、システム > アプリケーション、にあります。

関連ドキュメント

- CCCを最初に行うとき、CCCは起動可能なバックアップディスクに何をしますか？ <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#convert>>
- 私の暗号化されたバックアップボリュームは自動的にAPFSボリュームグループに変換されますか？ <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversionencrypted>>
- CCCとmacOS Catalinaについてのよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina>>
- FileVault暗号化で作業するには <<http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption>>
- バックアップボリュームの暗号化についてのよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>>
- Carbon Copy ClonerとAPFSについて知っておくべきこと <<http://bombich.com/ja/ja/kb/ccc5/everything-you-need-know-about-carbon-copy-cloner-and-apfs>>

Carbon Copy Cloner 3.5 から Carbon Copy Cloner 5にアップグレードするには

Carbon Copy Cloner 5をインストールするには

Carbon Copy Cloner 5をまだインストールしていない時に、3.5からアップグレードするようにメッセージが表示された場合は、Carbon Copy Cloner

5を手動でダウンロードしてインストールできます。図解での説明は、[Carbon Copy Clonerのダウンロードとインストールの方法を教えてください。](http://bombich.com/ja/ja/kb/ccc5/how-do-i-download-and-install-carbon-copy-cloner) <<http://bombich.com/ja/ja/kb/ccc5/how-do-i-download-and-install-carbon-copy-cloner>>をご覧ください。

タスク移行アシスタント

Carbon Copy Cloner 3.5 またはそれ以降でスケジュールタスクを作成してある場合、Carbon Copy Cloner 5をはじめて開くと、タスク移行アシスタントが表示されます。CCCの **ファイル**メニューから **タスクの移行**を選択して、タスク移行アシスタントを表示することもできます。

それぞれのタスクをクリックして、CCC

5との互換

性を確実にするため

にCCCがタスクに加える変更についての注意事項を確認してください。**読み込む**のコラムから、CCC 5に移行したいタスクの横にあるボックスにチェックマークを付け、**読み込む** をクリックしてください。

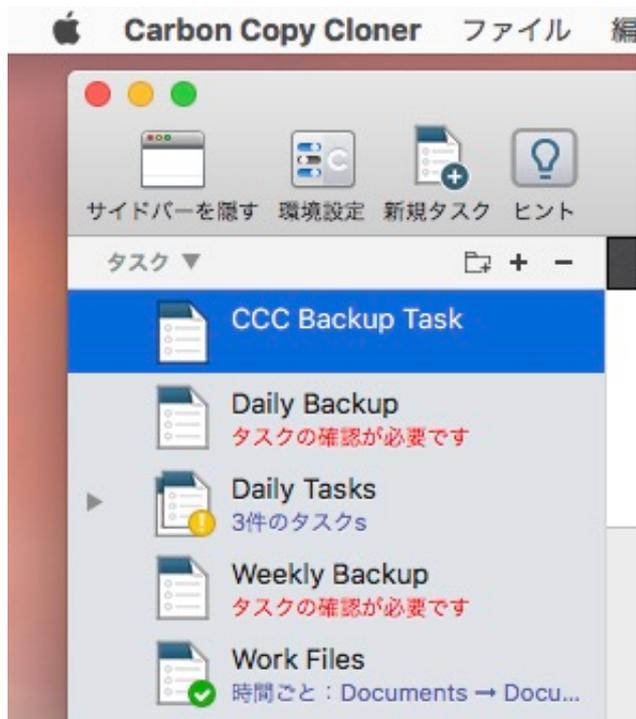
注意：CCC 5に移行されたタスクは、CCC 3.5では無効になります。

1つ以上の古いタスクを読み込まずに即座に完全に削除するには、それらのタスクを選択して(Command+クリックで複数のタスクを選択)、Delete キーを押してください。



読み込まれたタスクは確認が必要です

タスクの移行が完了すると、これらのタスクは確認が必要です、というメッセージがCCCから表示されます。サイドバーのタスクをそれぞれクリックして、設定を確認してください。タスクが希望通り設定されていれば、**保存** をクリックするか、CCCの **ファイル** メニューから **保存** を選択してください。



古いバージョンのCarbon Copy Clonerをアンインストールするには

タスク移行アシスタントを経由してタスクを読み込むと、CCCは古いバージョンのCCCをアンインストールするよう、30日リマインダーを自動的にスケジュールします。このリマインダーが表示されるのを待つことができますが、CCCの **ファイル** メニューから CCC 3.x..をアンインストールを選択して古いバージョンのCCCを即座にアンインストールすることもできます。



Carbon Copy Clonerのシステム要件

システム要件

- OS X 10.10 Yosemite
- OS X 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra
- macOS 10.14 Mojave
- macOS 10.15 Catalina
- macOS 11 Big Sur

古いバージョンのOSを使用しているユーザの方々に古いバージョンのCCC <<http://bombich.com/ja/download>>をまだご利用いただけます。これらの古いバージョンは現在活発に開発されることはなくなり、サポートもケースバイケースでのみ提供されます。

サポートされている設定

- macOS 10.10から10.12の起動可能なバックアップには、HFS+フォーマットされたボリュームが必要です
- macOS 10.13 High SierraおよびMojaveの起動可能なバックアップには、APFSまたはHFS+フォーマットされたボリュームが必要です
- macOS 10.15 Catalinaおよびそれ以降の起動可能なバックアップには、APFSフォーマットされたボリュームが必要です
- APFSソースおよびコピー先ボリュームはmacOS 10.13 High Sierraおよびそれ以降でのみサポートされています
- ユーザデータのバックアップは、非Appleフォーマット (例: 非HFS+ またはAPFS) のファイルシステムでサポートされているものもあります
- Firewire²、Thunderbolt、およびUSBエンクロージャ³のSSDおよびハードディスクドライブ¹
- CCCは、OS X 10.10 Yosemite (またはそれ以降) を正式にサポートするApple Macintoshでのみサポートされます
- 少なくとも1024x768の解像度が必要です

1 : APFSは回転数が7200RPMより遅いHDDで使用すると、パフォーマンスが劣ります

2 : macOS

Catalina、およびそれ以降はFireWire接続されたデバイス経由でMacを起動することをサポートしていません

3 : すべてのハードドライブエンクロージャがmacOSを起動できるとは限りません。ハードドライブをCarbon Copy Clonerとの使用に準備するには <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>> および [ヘルプ!](#) を参照してください。クローンが起動しません <<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot>>

をご参照ください。これらの制限はデバイスがMacを起動できる能力に関して適用されるものです。これらすべてのデバイスは一般的なバックアップには適しています。

サポートされていない設定

- CCCは、フォーマットされていない、またはマウントされていないデバイスに (または、デバイスから) クローンしません。ソースおよびコピー先にはmacOSに認識され、Finderで表示できるファイルシステムが必要です
- Windowsシステムファイルのクローンはサポートされた設定ではありません <<http://bombich.com/ja/ja/kb/ccc5/can-ccc-back-up-my-bootcamp-windows-partition>>
- CCCは光メディア (例 : CD-ROM や DVD-ROM) には直接バックアップしません
- WebDAV、FTP、NFS、およびその他の“クラウド” コピー先はサポートされていません
- macOS Mojave、およびそれ以降はRAIDデバイスから起動できません

- CCCは、2台のMacを同期しておくための双方向同期を目的にデザインされていません。よって、これはサポートされていない設定です。
- CCCで一括デプロイメントを実行することはサポートされていません。Appleはこの種のデプロイメントを推奨していません <<https://support.apple.com/en-us/HT208020>>ので、その他のリソースをこちらから提供しています <<https://help.apple.com/deployment/macOS>>。また、考慮すべき代替の解決法 <<https://twocanoes.com/products/mac/mac-deploy-stick>>もあります。
- お使いのハードドライブでAppleによってサポートされているmacOSのバージョンのクローンのみをサポートできます。例えば、2008 MacProでCatalinaを実行させるお手伝いはできません。同様に、出荷時にCatalinaを搭載している2019 MacBook ProにMojaveをクローンさせることはできません。Appleがサポートしていないなら、弊社もサポートできません。

CCCを購入するには

Bombich Software **販売条件とよくある質問**

- [CCC 5 \(または 4\)の購入方法は？](#)
- [返金の条件について教えてください。](#)
- [ヘルプが必要ですか。](#)
- [販売条件は何ですか。](#)
- [CCC はどのように発送されますか。](#)
- [利用できる支払い方法は？](#)
- [発注書を受け付けますか。](#)
- [消費税、付加価値税やその他関税などの税金がかかりますか。](#)
- [e-コマースに使用されているセキュリティについて教えてください。](#)
- [W-9 フォームはどこからダウンロードできますか。](#)
- [よくある質問](#)

CCCの購入方法は？

Bombich Software製品は弊社の[オンラインストア](http://bombich.com/ja/store) <<http://bombich.com/ja/store>> から直接購入できます。オンラインストアはe-コマースのパートナーFastSpring <<http://www.fastspring.com>> により管理されています。

個人ユーザ向けライセンスの払い戻し返還コードは、一部のコンサルタントおよび再販業者から利用できることもあります。認可を受けた再販業者の一覧は、[ライセンスの払い戻しページ](https://cccreseller.com/redeem) <<https://cccreseller.com/redeem>> をご覧ください。

ライセンスはこれまでのバージョンのCCCに有効です (例えば、CCC 5のライセンスを購入すれば、CCC 4を使用できます)。CCCの購入に関する詳細は、[Carbon Copy Clonerの価格と購入方法を教えてください。](http://bombich.com/ja/ja/kb/ccc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it) <<http://bombich.com/ja/ja/kb/ccc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it>> をご覧ください。

払い戻しの条件について教えてください。

購入前にこの製品がお客様のニーズを満たすものであるかを検証するために使用できる [Carbon Copy Clonerの全機能を搭載した 30 日間無料お試しバージョン](http://bombich.com/ja/download) <<http://bombich.com/ja/download>> を提供していますので、ご購入後の返金請求に対してはそれぞれの状況に応じて対応させていただきます。最低15%の手数料がかかることがありますのでご注意ください。払い戻しの請求は、購入後30日以内に[セールス担当](mailto:sales@bombich.com?subject=Refund%20Request) <<mailto:sales@bombich.com?subject=Refund%20Request>> までご連絡ください。

ヘルプが必要ですか。

CCCに技術的な問題が起きた場合、喜んで問題解決に取り組み、CCCを続けて使用していただけるよう最大限努力します。サポートチケットを開くには、Carbon Copy Clonerの[ヘルプメニュー](#)からCCC [について質問する...](#) (英語) を選択してください。

販売条件は何ですか。

すべての製品は、それぞれの製品に含まれている特定のライセンス契約に合意することで提供されます。

CCC はどのように発送されますか。

弊社のすべての製品は電子的にのみ配信されます。物理的な製品が配送されることはありません。ソフトウェアはこちらの[ダウンロードページ](http://bombich.com/ja/download) <<http://bombich.com/ja/download>> からいつでもダウンロードでき、その後登録キーがメールでお客様に送信されます。

購入の領収書と登録番号は、電子フォーマットでのみ提供されますので、ご注文が処理された後にメールで送信される送り状をプリントしていただくか、安全な場所にアーカイブしておかれることをお勧めします。この送り状は購入証明書となり、テクニカルサポート、将来のアップグレード、および特別割引などの際に必要となります。

利用できる支払い方法は？

オンラインストア <<http://bombich.com/ja/store>>

からいただいたご注文には以下のお支払い方法がご利用いただけます。オンラインストアはe-コマースのパートナー、FastSpring <<http://www.fastspring.com>>により管理、決済されています。すべての支払い方法がすべての国で利用できるとは限りませんので、ご了承ください。

クレジットカード：マスターカード、ビザ、ディスカバー、アメリカンエキスプレス、および JCB 各社のクレジットカードをご利用いただけます。

小切手およびマネーオーダー

：法人または個人用小切手を受け付けます。小切手およびマネーオーダーのご利用に関しては、各国によって異なりますのでご注意ください。このオプションが支払い手続きの画面に表示されない場合、お住まいの国でこのオプションを利用することはできません。メンテナンスなど、購読タイプの製品には小切手を使用できません。

PayPal (ペイパル)：ペイパルアカウントからのお支払いをご利用いただけます。

Amazon ペイメント：Amazon

ペイメントからのお支払いをご利用いただけます。

このオプションが支払い手続きの画面に表示されない場合、お住まいの国でこのオプションを利用することはできません。

別のお支払い方法：特定の国と地域では、Giropay、iDEAL、Sofort、WebMoney、およびAlipayをご利用いただけます。このオプションが支払い手続きの画面に表示されない場合、お住まいの国でこのオプションを利用することはできません。

発注書 (PO) を受理しますか。提示したPO条件を承諾していただけますか。

お客様の内部記録のために請求書に発注書 (PO) 番号を参照として付けさせていただきます。しかし、発注書 (PO) を支払方法として受け付けたり、一般的に発注書 (PO) に付随する利用条件を承諾することはありません。お支払いの処理が済むまでの間、全機能を搭載した30日間の無料お試し期間を提供しています。

弊社は標準的な**エンドユーザ使用許諾契約** <<http://bombich.com/ja/software/CCCEULA.rtf>>

をすべてのお客様に提供することで低価格を維持していますので、商業信用を提供していません。すべてのお客様に対して請求日当日にお支払いいただくことが弊社の支払条件です。全額のお支払いを確認後、ライセンスを発行し、メールで送信させていただきます。詳細は弊社の **セールス部門** <<mailto:sales@bombich.com>> までお問い合わせください。

消費税、付加価値税やその他関税などの税金がかかりますか。

輸入する国の裁量により該当する関税が適用され、それらはお客様に支払い義務があります。これらの費用はお支払い手続きの最後に追加され、製品を選択する段階の画面で表示されるものではありません。

e-コマースに使用されているセキュリティについて教えてください。

オンラインストアで使用している e-コマースは、FastSpring <<http://www.fastspring.com>> により提供されています。

[FastSpringのプライバシーポリシーをご確認ください](http://www.fastspring.com/privacy.php) <<http://www.fastspring.com/privacy.php>>。

W-9 フォームはどこからダウンロードできますか。

弊社が直接販売を管理することはありません。すべての販売は、信頼する再販業者のパートナー、Fastspringを通じて行われます。

[Fastspringの W-9 フォーム <http://www.fastspring.com/w9.pdf>](http://www.fastspring.com/w9.pdf)

よくある質問

- 30日間の無料お試し期間について教えてください。 <<http://bombich.com/ja/ja/kb/ccc5/how-does-free-30-day-trial-work>>
- Carbon Copy Clonerの価格と購入方法を教えてください。 <<http://bombich.com/ja/ja/kb/ccc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it>>
- 今CCCの代金を支払っても、将来のアップデートでまた支払う必要がありますか。 <<http://bombich.com/ja/ja/kb/ccc5/if-i-pay-ccc-now-will-i-have-pay-future-updates>>
- アップグレードしてCarbon Copy Cloner 5を購入するには <<http://bombich.com/ja/ja/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5>>
- CCCの1つのライセンスを家族で複数のMacに使用できますか。 <<http://bombich.com/ja/ja/kb/ccc5/can-i-use-one-license-ccc-on-multiple-macs-in-my-household>>
- 教育機関向けの特別割引はありますか。 <<http://bombich.com/ja/ja/kb/ccc5/do-you-offer-academic-discount>>
- CCCをプレゼントとして贈ることはできますか。 <<http://bombich.com/ja/ja/kb/ccc5/can-i-give-ccc-gift>>
- ボリュームライセンス契約を提供していますか。 <<http://bombich.com/ja/ja/kb/ccc5/do-you-offer-volume-licensing-program>>
- どうしてCCCはMac App Storeにないのですか。 <<http://bombich.com/ja/ja/kb/ccc5/why-isnt-ccc-on-mac-app-store>>
- 電話でのサポートに対応していますか。 <<http://bombich.com/ja/ja/kb/ccc5/do-you-offer-telephone-support>>

アップグレードしてCarbon Copy Cloner 5を購入するには

CCC 3.5または4 のライセンスをCCC 5で使用できますか。

いいえ。CCC 5は新しいライセンスが必要です。しかし、CCC 4のライセンスを2017年5月22日以降に購入された場合は、CCC 5のライセンスを無料で贈呈致します

。2017年5月22日より前に個人用ライセンスとProライセンスを購入された場合は、アップグレード価格をご利用いただけます。

2017年5月22日以降にCCC 4のライセンスを購入しました。CCC 5の無料ライセンスを取得するにはどうすればいいですか。

CCC 5を最初に開くと、ご使用のCCC 4のライセンスの詳細を使用して、新しいライセンスの取得を試みます。これが問題なく完了すると、新しいライセンスと新しいライセンスをCCC 5に適用するための詳細が指定されたメールに送信されます。この処理が実行されない場合(例えば、インターネットに接続できないため)、[弊社ウェブサイトからライセンスを取得してください](http://bombich.com/ja/forgot) <<http://bombich.com/ja/forgot>>。

どのライセンスがオンラインアップグレード価格の対象になりますか？

CCC 3.5およびCCC 4の家庭向けおよびProライセンスが以下のアップグレード価格の対象です:

CCC 1、2、3、または3.3をご使用の場合.....割引は提供されません。
CCC 3.5の個人および家庭向け、またはプロライセンス.....25%割引。
CCC 4の個人および家庭向け、またはプロライセンス.....50%割引。

企業および団体向けライセンス (数量ライセンスプログラム) は[現在のそれぞれの価格帯](http://bombich.com/ja/store/corporate) <<http://bombich.com/ja/store/corporate>>

の25%オフのアップグレード割引の対象となります。企業および団体向けライセンスをお持ちの場合は、カスタムアップグレードプランを提供させていただきますので、[弊社までお問い合わせください](mailto:sales@bombich.com)

<<mailto:sales@bombich.com?subject=CCC%20Upgrade%20Quote%20Request>>

。メンテナンスを購入されていて、それが現在有効な場合、アップグレードは無料です。

アップグレード価格の対象でないのはどのライセンスですか。

部署またはサイトライセンスのようなレガシーライセンスはアップグレード価格の対象ではありません。

教育機関向け割引をアップグレード価格に適用できますか。

いいえ。アップグレード価格に追加の割引を適用することはできません。

CCC

5のライセンスをアップグレード価格で購入するにはどうすればいいですか。

CCC 4の登録済みコピーを使用している (または、使用していた) 場合は、CCC 5をダウンロードして、開いてください。CCC 5はCCC 4のライセンスを認識して、アップグレードの対象かどうか



かを確認します。この自動システムがそのライセンスがアップグレード対象であると判断すると、CCCはクーポンコードを取得して、自動的にApp内購入に適用します。

CCC 3.5をアップグレードしたい場合は、

弊社ウェブサイトからアップグレード価格のリクエストを送信してください

<<http://bombich.com/ja/store/upgrade>>。CCC 4のApp内からのアップグレードに問題が生じた場合にも、

アップグレード価格のリクエストフォーム <<http://bombich.com/ja/store/upgrade>>

を使用できます。アップグレードの購入に関してご質問や問題がある場合は、[こちらからお問い合わせ](#)

<<mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>>ください。

企業および団体向けライセンスをお持ちの場合は、カスタムアップグレードプランを提供させていただきますので、[弊社までお問い合わせください](#)

<<mailto:sales@bombich.com?subject=CCC%20Upgrade%20Quote%20Request>>。

使っているMacがCCC 5には古すぎます。CCC 5のライセンスを購入した場合、そのライセンスでCCC 4または3.5が動作しますか。

もちろん！CCC 5のライセンスを購入された場合、そのライセンスはCCC

3.5.7、またはそれ以降で認識されます。後でMacをアップグレードした場合、CCC 5にアップグレードしてCCC 5ライセンスの使用を開始できます。

追加情報

- CCC 5の新機能 <<http://bombich.com/ja/ja/kb/ccc5/whats-new-in-ccc>>
- Carbon Copy Clonerのシステム要件 <<http://bombich.com/ja/ja/kb/ccc5/system-requirements-carbon-copy-cloner>>
- Carbon Copy Cloner 3.5 から Carbon Copy Cloner 5にアップグレードするには <<http://bombich.com/ja/ja/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5>>
- セールスサポートに問い合わせる <<mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>>
- CCCをダウンロード <<http://bombich.com/ja/download>>



30日間の無料お試し期間について教えてください。

ご購入前に30日間無料でCCCの完全な機能をお試しいただけます（お試し期間に無効になる機能はありません）。この期間を利用してCCCの自動化された、増分バックアップ機能を体験し、起動可能なバックアップを作成してください。

Carbon Copy Clonerの最新で最強のバージョンをダウンロードしてください <<http://bombich.com/ja/download>>。

Carbon Copy Clonerの動作や機能に関するご質問はお試しバージョンをご使用中も、ご購入後もCarbon Copy Clonerの **ヘルプ** メニューのCCC **について質問する... (英語)** からどうぞ。

Carbon Copy Clonerの価格と購入方法を教えてください。

価格

Carbon Copy Cloner 5 の個人用ライセンスは\$39.99 USDです。(別途地方税が適用されます) 国によっては、異なるお支払い方法を利用できるように、現地通貨で事前に設定された価格で提供することがあります。その他の国々では、USD (米ドル) を購入の時点での為替レートで換算して現地通貨価格を割り出します。

購入

企業および団体 のお客様は、**企業向けストア** <<http://bombich.com/ja/store/corporate>> からシングルワークステーションライセンス、ボリュームライセンス、およびPro (技術者) ライセンスをご購入いただけます。

Bombich Software製品は弊社の**オンラインストア** <<http://bombich.com/ja/store>> から直接購入できます。オンラインストアはe-コマースのパートナー**FastSpring** <<http://fastspring.com>> により管理されています。Carbon Copy

Clonerの

発送は電子的な送

信のみです。物理的な製品が配送されることはありません。ソフトウェアは **ダウンロードページ**

<<http://bombich.com/ja/download>>

からいつでもダウンロードできます。万が一登録キーを失くした場合には、メールで再発送するようにCCCの中からリクエストを送信できます。

個人ユーザ向けライセンスの払い戻し返還コードは、一部のコンサルタントおよび再販業者から利用できることもあります。認可を受けた再販業者の一覧は、**ライセンスの払い戻しページ** <<https://cccreseller.com/redeem>> をご覧ください。

アップグレード価格

CCC 3.5 または 4.0 の個人用ライセンスを所有しておられる場合、CCC 5のご購入の際に割引を提供しています。

CCC 1、2、3、または3.3をご使用の場合.....割引は提供されません。

CCC 3.5を所有している場合.....25%オフ。

CCC 4を所有している場合.....50%オフ。

割引の適用については**アップグレードページ**から詳細をご覧ください <<http://bombich.com/ja/store/upgrade>>。

注意: 5月22日から8月21日の間にCCC 4を購入された場合は、既にCCC 5の無料ライセンスをお持ちです。 **こちらからご利用ください** <<http://bombich.com/ja/forgot>>。

追加情報

- Carbon Copy Clonerのアップグレードを購入するには <<http://bombich.com/ja/ja/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5>>
- Carbon Copy Cloner 3.5 から Carbon Copy Cloner 5にアップグレードするには <<http://bombich.com/ja/ja/kb/ccc5/upgrading-from-carbon-copy-cloner-3.5-carbon-copy-cloner-5>>
- セールスサポートに問い合わせる <<mailto:sales@bombich.com?subject=Upgrade%20Eligibility%20Question>>

今CCCの代金を支払っても、将来のアップデートでまた支払う必要がありますか。

アップデートが小さな改良や修正からなる場合(例: 不具合の修正、バージョン5.0から5.1への移行など)、ライセンス契約されているユーザにはアップデートは無料で提供されます。

しかし、時にはアプリケーションに非常に大きな変更をもたらす新しいバージョンを発表することがあります。このようなアップグレードは新しいバージョン番号で区別され(例: バージョン4から5へ移行)、新しい機能や特徴が搭載され、新しいオペレーティングシステムのサポートが含まれます。このプロセスには、リサーチやデザイン、開発、およびテストに多大な時間と労力を費やします。従って、これらのリリースは大部分の商業ソフトウェアのように扱われます。現在ご利用中のユーザにはアップグレード価格が提供されます。アップデートの購入を辞退された場合、前のバージョンを古いオペレーティングシステムで使用し続けることができます。

現在有効のソフトウェアメンテナンス合意のあるボリュームライセンス契約のお客様は、追加料金なしで有料アップグレードをご利用いただけます。

但し、古いバージョンのCCCが無期限にサポートされるわけではありませんので、ご注意ください。現在サポートされているバージョン、まもなくサポートが打ち切られる予定のバージョンを検索するには、[ダウンロードページ](http://bombich.com/ja/download) <<http://bombich.com/ja/download>>をご覧ください。

現在のアップグレードの価格オプションについての詳細は、[Carbon Copy Clonerの価格と購入方法を教えてください。](http://bombich.com/ja/ja/kb/ccc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it) <<http://bombich.com/ja/ja/kb/ccc5/how-much-does-carbon-copy-cloner-cost-and-how-can-i-purchase-it>>をご覧ください。

CCCの1つのライセンスを家族で複数のMacに使用できますか。

はい、[CCC ライセンス <http://bombich.com/ja/software/CCCEULA.rtf>](http://bombich.com/ja/software/CCCEULA.rtf)

は、個人的、非商業目的で所有、管理されているコンピュータにCarbon Copy Clonerをインストールして使用することを許可します。CCCを商業目的、または機関、団体で使用する場合は、[企業向け <http://bombich.com/ja/store/corporate>](http://bombich.com/ja/store/corporate) または [教育機関向け <http://bombich.com/ja/edu>](http://bombich.com/ja/edu) ライセンスの購入オプションをご利用ください。

CCC 5のライセンスはCCC 3.5.7及びCCC

4にも対応できます。ご家庭で複数のMacを所有していて、その中にCCC

5の要件を満たしていないものがある場合、CCC 3.5.7、CCC 4、CCC

5を搭載するすべてのMacに同じライセンスを使用できます。CCCのすべての利用可能なバージョンはいつでも [ダウンロードページ <http://bombich.com/ja/download>](http://bombich.com/ja/download)

からダウンロードできます。ライセンスが見つかりませんか。CCC内から直接、または [弊社ウェブサイトから <http://bombich.com/ja/forgot>](http://bombich.com/ja/forgot) 登録キーを要求してください。

複数のMacでライセンスを使用する場合の詳しい情報は、[家族で複数のMacでCCCを使用するには <http://bombich.com/ja/ja/kb/ccc5/how-do-i-use-one-license-ccc-on-multiple-macs-in-my-household>](http://bombich.com/ja/ja/kb/ccc5/how-do-i-use-one-license-ccc-on-multiple-macs-in-my-household) をご覧ください。

教育機関向けの特別割引はありますか。

教育機関向けに25%オフの特別割引を提供しています。

対象は誰ですか。

Bombich Software

教育機関向けの特別割引を受けるには、教育機関のエンドユーザとしての資格を有する必要があります：

- 認可されたK-12の学校（幼稚園、小中学校、及び高校）、または高等教育機関に現在従事する教職員、またはスタッフで、かつ有効な教育機関用メールアドレスを持つ方。
- 認可された高等教育機関に在学中で有効な教育機関用のメールアドレスを所有している学生。

対象は何ですか。

CCCの家庭向けライセンス、ワークステーションライセンス、Proライセンス、およびボリュームライセンスの新規購入は教育機関向け特別割引の対象です。現在のライセンス所有ユーザはアップグレードの購入に割引が提供されませんが、教育機関向け割引を追加で利用することはできません。

個人用に購入する場合どうすればいいですか。

1. 弊社の [教育機関向け特別割引の検証ページ](http://bombich.com/ja/edu) <<http://bombich.com/ja/edu>> に進み、クーポンコードをお客様の教育機関用のメールアドレスに送信されるようにしてください。
2. お受け取りになられた“個人用に購入”のリンクを使ってCCCを購入してください。

*教育機関向け自動割引の資格のある教育機関のメールアドレスの一覧を維持しています。お客様のドメインが一覧にない場合でも、割引を受け取ることはできますが、手動で認証プロセスを完了していただく必要があります。手動認証が必要な場合、お手続きの手順はメールで送信いたします。

教育機関用に購入する場合どうすればいいですか。

1. 弊社の [教育機関向け特別割引の検証ページ](http://bombich.com/ja/edu) <<http://bombich.com/ja/edu>> に進み、クーポンコードをお客様の教育機関用のメールアドレスに送信されるようにしてください。
2. お受け取りになられたメールにある“教育機関向けに購入”のリンクを使って、CCCをご購入ください。

*教育機関向け自動割引の資格のある教育機関のメールアドレスの一覧を維持しています。お客様のドメインが一覧にない場合でも、割引を受け取ることはできますが、手動で認証プロセスを完了していただく必要があります。手動認証が必要な場合、お手続きの手順はメールで送信いたします。

*利用できるお支払い方法についてのご質問は sales@bombich.com <<mailto:sales@bombich.com>> までメールでお問い合わせください。

他に何か知っておくことはありますか。

利用規約

個人的使用

：個人でご使用になる場合、教育機関向けエンドユーザの資格を持つ方はそれぞれ、バージョンごとおよび教育機関用メールアドレス1件ごとにCCCライセンスを1つ購入いただけます。Bombich Softwareは、Carbon Copy Clonerを教育機関向け割引価格でご購入いただく前に、その機関に従事している、あるいはその機関の学生である証明をご提示いただく権利を有するものとします。この証明には学校の認定証、教職員身分証明書、学生証明書

、および/またはメールアドレスの検証が含まれます。

教育機関による使用

：CCCが教育機関の使用に購入された場合、1件のコピー制限の条件は適用されませんが、Bombich Softwareは1機関による購入数を制限する権利を有するものとします。Bombich Softwareは、Carbon Copy Clonerを教育機関向け割引価格でご購入いただく前に、その機関に従事している証明をご提示いただく権利を有するものとします。この証明には学校の認定証、教職員身分証明書、学生証明書、および/またはメールアドレスの検証が含まれます。

価格には地方税または地域の関税は含まれません。Bombich Softwareは、いかなる時も独自の自由裁量でこの割引の提供を変更、割引の取り消し、注文の解約をする権利を有するものとします。

質問がある場合、どうすればいいですか。

sales@bombich.com <mailto:sales@bombich.com> までメールでお問い合わせください。

ボリュームライセンス契約を提供していますか

○

はい、ボリュームライセンス契約はお客様の団体の資金節約をお手伝いします。

Carbon Copy

Clonerの複数のユーザ向けライセンスの特別価格を提供しています。ボリュームライセンス契約はCarbon Copy Clonerライセンスを5つ以上ご購入の方にはどなたでもご利用いただけます。ボリュームライセンス契約には以下の同意が含まれます：

- 標準小売り価格の割引
- 簡単に管理できるよう、お客様のすべてのCarbon Copy Clonerライセンスを1つのライセンスキーにまとめています
- ソフトウェアメンテナンスオプション

ボリュームライセンスについての詳細は、[ボリュームライセンスとメンテナンスについての同意書](http://bombich.com/ja/software/CCCVolumeLicenseandMaintenanceAgreement2014.pdf)
<<http://bombich.com/ja/software/CCCVolumeLicenseandMaintenanceAgreement2014.pdf>> [をご覧ください](#)

製品の発送とご注文について

Carbon Copy Clonerボリュームライセンスは、ダウンロードによってのみご提供します。物理的な箱に梱包されたソフトウェアの複製を発送することはありません。

ボリュームライセンスのご注文、または見積もり価格のご請求に際しては、弊社の[Corporate Store](http://bombich.com/ja/store/corporate)
<<http://bombich.com/ja/store/corporate>>

をご

利用くだ

さい。教育機関向けライセンスの割引についての詳細、または教育機関向け割引でのご注文は、[教育機関向け価格](http://bombich.com/ja/edu)
<<http://bombich.com/ja/edu>>

をご覧ください。既

存のボリュームライセンスに追加ライセンスを購入したい場合は、弊社の[セールス担当までメール](mailto:sales@bombich.com?subject=Add%20Volume%20License%20Seats%20to%20CCC%20License)

<<mailto:sales@bombich.com?subject=Add%20Volume%20License%20Seats%20to%20CCC%20License>>

でお見積もりをお問い合わせください。

ソフトウェアメンテナンス

ボリュームライセン

スにはソフトウェアメンテナンスを含め

るオプションが提供されています。このオプションを利用すると、メンテナンス契約をお支払い後、Carbon Copy Clonerのすべてのアップデートに伴うサービスが無料になります。メンテナンス契約は Carbon Copy

Cloner

ボリュームライセンスの発送メールに添付されたリンクからいつでもキャンセルできます。詳細は、[Carbon Copy Cloner メンテナンス利用規約](http://bombich.com/ja/software/maintenanceterms2014.pdf) <<http://bombich.com/ja/software/maintenanceterms2014.pdf>> [をご参照ください](#)。

販売条件

販売条件に関する情報は、[販売条件およびよくある質問](http://bombich.com/ja/sales-terms-and-conditions) <<http://bombich.com/ja/sales-terms-and-conditions>>
をご参照ください。

Carbon Copy Clonerが教育機関向け割引でライセンスを提供した場合、そのライセンスは、生徒の教育のみを目



的として組織、運営されている認可を受けた K-12の教育機関（または同等の）、あるいは高等教育機関に籍のある学生、教授、先生、および職員のみが利用できるものとします。さらに、ボリュームライセンス契約にはポータブルまたは家庭で使用する権利は含まれていません。

ご質問は [こちらまでメールでお問い合わせください <mailto:sales@bombich.com>](mailto:sales@bombich.com)。



CCCをプレゼントとして贈ることはできますか

。

はい。オンラインギフトストア <<http://sites.fastspring.com/bombich/product/ccc?option=gift>>をご利用ください。

CCCの登録は購入時に使用されたお名前とメールアドレスに関連付けられますので、[オンラインギフトストア](http://sites.fastspring.com/bombich/product/ccc?option=gift) <<http://sites.fastspring.com/bombich/product/ccc?option=gift>> でプレゼントの受取人を指定することができます。領収書が注文者にメールで送信され、プレゼントの受取人には即座にライセンス情報が送信されます。



どうしてCCCはMac App Storeにないのですか。

Mac App StoreをCCCの発送ルートの1つとして加えることができれば素晴らしいのですが、Appleが要求するポリシーと合致しない特定クラスのアプリケーションがあります。Appleがこれらのポリシーを変更しない限り、macOSの起動可能なバックアップを作成できるユーティリティをMac App Storeで見ることはないでしょう。このポリシーについて [Apple にフィードバックを送信](#) [<https://www.apple.com/feedback/>](https://www.apple.com/feedback/) することはできますが、AppleのフィードバックページからMac App Storeが欠落していること、この件に関するAppleの断固とした立場から判断して、このポリシーが変更されることは期待できません。

電話でのサポートに対応していますか？

お客様からの電話に対応しているサポートスタッフはおりません。

2002年よりカスタマーサポートを提供するに当たって、オンラインで問題を送信していただくことから始まるサポートのプロセスが、より効率的でより高いクオリティを提供できると判断しました。Carbon Copy Clonerのヘルプメニューから直接サポートリクエストを送信していただくと、リクエストと共にお客様のログ(同意していただいた場合)が送信され、お使いのCCCの固有の設定と遭遇されているエラーメッセージを分析することができます。“これが動かなくて困っている”という以外の情報がないリクエストが送信されることがよくあります。その程度の詳細でも大丈夫です。CCCのログを早急に確認した後、問題を解決するための手順を注釈付きのスクリーンショットを付けて、迅速に対応させていただきます。それでもまだ問題が継続する場合に、電話または画面共有によるサポートが有益であると思われる場合には、それらのサポートを手配させていただきます。

すべてのサポートリクエストに、営業日の1日以内にBombich Softwareのサポートチームから回答を差し上げるべく最善を尽くしています。オンラインサポートはアメリカ東部時間の月曜日から金曜日、午前9時から午後5時まで、英語で対応しています。

関連ドキュメント

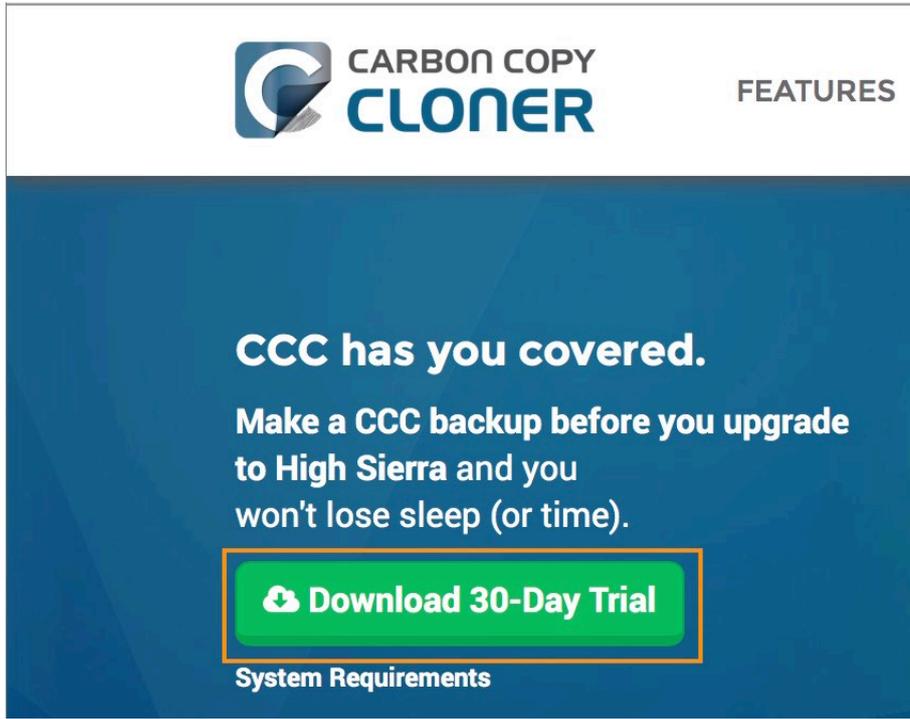
- ヘルプを取得するには <<http://bombich.com/ja/ja/kb/ccc5/how-do-i-get-help>>
- 会社概要 <<http://bombich.com/ja/about>>

CCCをダウンロード、インストール、登録するには

Carbon Copy Clonerのダウンロードとインストールの方法を教えてください。

このチュートリアルビデオをYouTubeで見る <<https://www.youtube.com/watch?v=vi1p-aM0gxc>>

bombich.com **ウェブサイトを開く**



The screenshot shows the Carbon Copy Cloner website. At the top left is the logo with the text 'CARBON COPY CLONER'. To the right of the logo is the word 'FEATURES'. Below this is a dark blue banner with white text that reads: 'CCC has you covered. Make a CCC backup before you upgrade to High Sierra and you won't lose sleep (or time).' In the center of the banner is a green button with a white download icon and the text 'Download 30-Day Trial'. Below the button, the text 'System Requirements' is visible.

<https://bombich.com> <<https://bombich.com>> を開き Downloadをクリックします。

ダウンロードが完了するのを待ち、ダウンロードフォルダのCCC Zipアーカイブを開く



ダウンロードが完了したら、ダウンロードフォルダのCCC Zipアーカイブを開き、CCCのアーカイブを解除します。

CCCを開き、アプリケーションフォルダに移動する



アプリケーションフォルダに移動

をクリックしてください。これで他のアプリケーションと同様にCCCがアプリケーションフォルダに保管されます。注意：アプリケーションフォルダに古いバージョンのCCCが既にある場合、CCC 5はそれを上書きしません。そして、このメッセージも表示されません。それで大丈夫です。というのは、CCC 3のタスクの移行が進み(可能であれば)、CCC 3がアンインストールされた後、CCCは自ら移動するメッセージを表示します。

(オプション) CCCをDockに追加する



CCCをDockに追加するには、アプリケーションフォルダからDockにドラッグしてドロップしてください。

CCC 4からCCC 5にアップグレードするには

CCC 4内のアップグレードインターフェースからCCC 5をダウンロードすると、CCC 5がMacにダウンロードされ、CCC 4の横に配置されます。CCC 5を最初に開くと、全機能搭載の30日間お試しバージョンが始まります。この期間を利用してCCC 5を評価してください。CCC 5を購入する準備ができたなら、CCCを開いた時に表示される“お試し”ウインドウが購入ボタンをクリックしてください。

“古いバージョンのCCCのライセンスをすでに持っています。CCC 5のアップグレードを支払う必要はありますか。”

はい、CCC 5は有料アップグレードです。しかし、CCC 3または4のライセンスはアップグレード価格に適用される可能性があります。[こちらから適格性を確認してください](http://bombich.com/ja/store/upgrade)
<<http://bombich.com/ja/store/upgrade>>。

“CCC 5のアップグレードを購入しないと決めた場合、CCC 4にダウングレードできますか。”

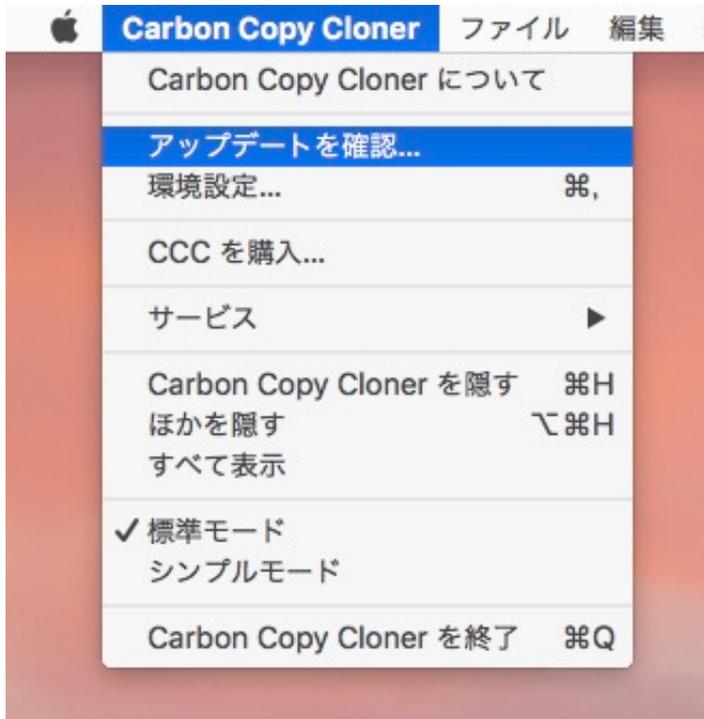
はい、CCC 4にダウングレードすると、アップグレード以前のタスクの状態を復元します。CCC 4がまだアプリケーションフォルダにある場合は、CCC 4を開き、**ダウングレード**のオプションを選択してください。ウェブサイトからCCC 5をダウンロードして、CCC 4のコピーを置き換えた場合、[ウェブサイトからCCC 4を再度ダウンロード](http://bombich.com/ja/download#ccc4)
<<http://bombich.com/ja/download#ccc4>>してください。

追加情報

- アップグレードしてCarbon Copy Cloner 5を購入するには <<http://bombich.com/ja/ja/kb/ccc5/purchasing-upgrade-carbon-copy-cloner-5>>
- 30日間の無料お試し期間について教えてください。 <<http://bombich.com/ja/ja/kb/ccc5/how-does-free-30-day-trial-work>>
- CCC 5の新機能 <<http://bombich.com/ja/ja/kb/ccc5/whats-new-in-ccc>>
- Carbon Copy Cloner 5 のシステム要件 <<http://bombich.com/ja/ja/kb/ccc5/system-requirements-carbon-copy-cloner>>
- Carbon Copy Cloner 5 リリースノート <<http://bombich.com/ja/ja/kb/ccc5/release-notes>>
- Carbon Copy Cloner 5についてのご質問、または問題の報告 <<http://bombich.com/ja/software/gethelp>>

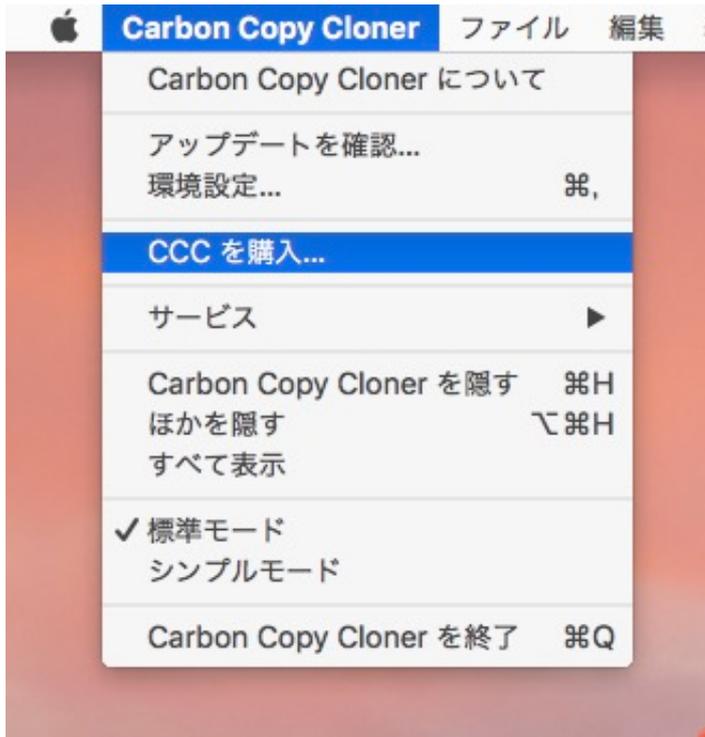
CCCの登録コードを手動で入力するには

CCCを起動してアップデートを確認



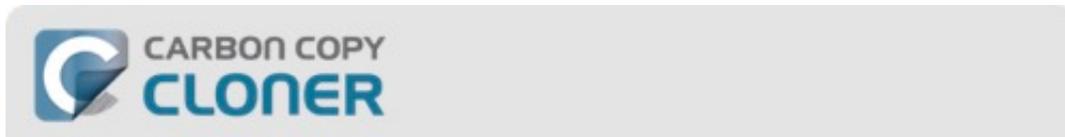
未登録のコンピュータからCCCを起動します。Carbon Copy Cloner > アップデートを確認...と進み、CCCの最新バージョンが実行中であることを確認してください。

登録ステータスを確認



起動したら、Carbon Copy Cloner >
登録情報を表示...と進み、コンピュータの登録ステータスを確認してください。

未登録のCCC



Carbon Copy Cloner へようこそ

Carbon Copy Cloner をお試し頂きありがとうございます！ご購入前に CCC の全機能を30日間お試しいただけます。この期間を使って、CCC の自動化されたインクリメンタルなバックアップ機能を調査したり、起動可能なバックアップを作成したり、デジタルライフに必要なデータを新しいハードドライブに移すなどして、心配のタネを取り除いて下さい。

すでにライセンスを持っています ➡

試用

CCC を購入

試用期限は、2017/07/20 8:38 です

CCCが未登録の場合、Carbon Copy Cloner

へようこそ

の登録画面が表示されます。以前にCCC

を購入したことがある場合は、**すでにライセンスを持っています**をクリックしてください。

登録コードをコピーしてペーストする



Carbon Copy Cloner の登録

名前
メールアドレス
ライセンスキー

登録を取得する

戻る

登録者

試用期限は、2017/07/20 8:38 です

登録メールからそのままお名前、メールアドレス、ライセンスキーをコピーしてペーストしてください。

注意

：別の名前、メールア

ドレス、およびライセンスキーを使用すると、無効と表示されます。**登録する**をクリックしてください。

正確に入力されたコード

CCCの登録が問題なく完了すると、“ご登録いただきありがとうございます!”の画面が表示されます。



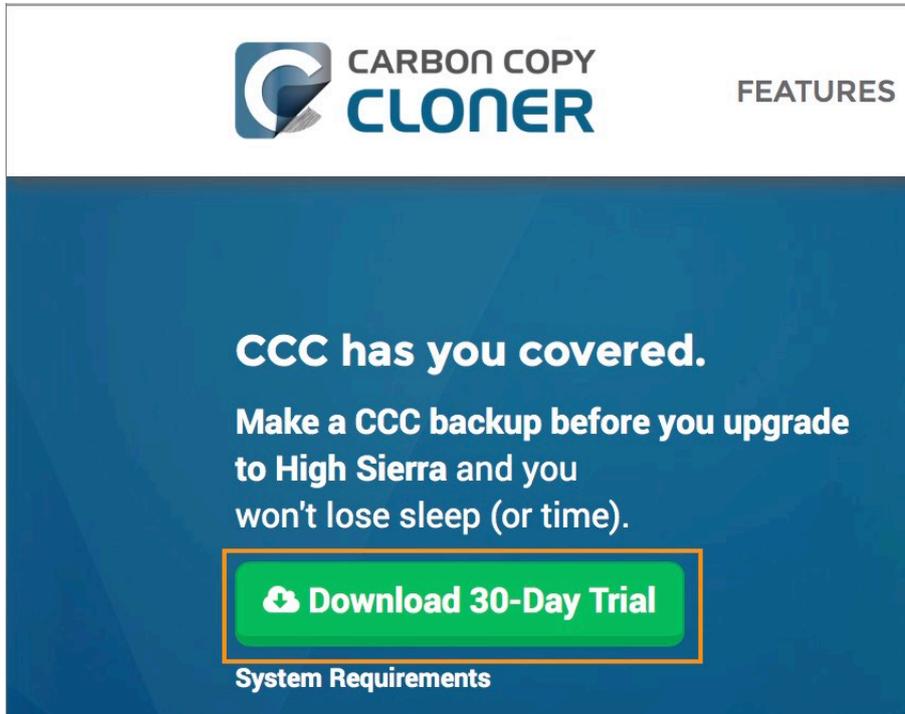
Carbon Copy Clonerの古いバージョンをダウンロードできますか。

古いバージョンのCCCは、こちらからダウンロードできます：<https://bombich.com/download>
<<http://bombich.com/ja/download>>

CCC 4 及び CCC 3.5 のライセンスは販売していません。CCC 4 及び CCC 3.5を使用するには、CCC 5 のライセンスをご購入ください。CCC 5のライセンスはCCC 4およびCCC 3.5の登録に使用できます。

ワンクリックでCCCを登録するには

Carbon Copy Clonerをインストールして起動する



The screenshot shows the Carbon Copy Cloner website. At the top left is the logo with the text 'CARBON COPY CLONER'. To the right of the logo is the word 'FEATURES'. Below this is a dark blue banner with white text that reads: 'CCC has you covered. Make a CCC backup before you upgrade to High Sierra and you won't lose sleep (or time).' Below the text is a green button with a white download icon and the text 'Download 30-Day Trial'. At the bottom of the banner, the text 'System Requirements' is visible.

ワンクリック登録が作動するには、まず最初にCarbon Copy Clonerをインストールして起動する必要があります。CCCをダウンロードするには、<https://bombich.com> <<https://bombich.com>> を開き、Downloadボタンをクリックしてください。

登録メールを開く

Carbon Copy Cloner

Registration name: Your Name
Registration email: Your Email Address
Registration code:

Number of licenses: [1]

Registering Carbon Copy Cloner

Please resist the temptation to type in that really long registration code. If you're reading this email on your Mac and you already have CCC installed*, just click on this great big button:



[Click Here to Register CCC](#)

We suggest that you do this right now, while you're online. As long as you already have CCC installed on your Mac, clicking the magic button should instantly apply the registration settings to CCC. If you don't already have Carbon Copy Cloner installed, do this first:

1. [Download the latest version of CCC \[Alternate\]](#)
2. Double-click the downloaded zip file and drag the Carbon Copy Cloner icon into your Applications folder.
3. Launch Carbon Copy Cloner, then go back to this email and click the registration button above to apply your registration settings

*** Not on your Mac right now?** If you want to apply this registration code to another Macintosh covered under the same license, drag the big registration button to your Desktop, then distribute the bookmark file to the other Macs and open it there.

登録メールを開き、[こちらをクリックしてCCCを登録](#) をクリックします。以上！完了です！

トラブルシューティング：万が一、OS Xがcom.bombich.ccc.licで始まるインターネットアドレスを認識できないため、Safariが、com.bombich.ccc.lic://blah-blah-blahを開くことができません”

のようなメッセージが表示された場合、(1) CCCがダウンロードされていること、(2) 登録設定を適用しようとするMacでCCCが開いていること、を再確認してください。既にCCCが開いていて、それでもこのメッセージが表示されるようでしたら、[手動で登録情報を入力する <http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code)か、または弊社まで [お問い合わせ <http://bombich.com/ja/software/gethelp>](http://bombich.com/ja/software/gethelp) ください。

登録情報の適用に問題がありますか。

よくある質問

- [登録情報を取得するにはどうすればいいですか。過去にCCCを購入しましたが、今回別のユーザアカウントで使いたいのですが。](#)
- [登録情報を取得できない場合どうなりますか。](#)
- [登録設定を適用しようとボタンをクリックすると、ブラウザに、この奇妙なURLを開くことはできません、と表示されます。](#)
- [登録設定を適用するためにボタンをクリックすると、Firefoxが“コンテンツが壊れていますというエラー”を表示します。どうしてですか。](#)
- [CCCをワンクリックで登録するにはどうすればいいですか。](#)
- [CCCの登録コードを手動で入力するにはどうすればいいですか。](#)
- [まだ解決できない問題があります。ヘルプが必要ですが、どうすればいいですか。](#)

登録情報を取得するにはどうすればいいですか。CCCを購入しましたが、未登録と表示されません。

CCCを過去に購入したことがあるのに、購入を促すメッセージが表示された場合、弊社のウェブサイトから登録情報を取得することができます <<http://bombich.com/ja/forgot>>

。C

CCを購

入時に使用した

メールアドレスを入力いただ

と、そのメールアドレスに登録情報を送信します。

メールの中のボタンをクリックすると、すぐにCCCを登録できます（登録コードをコピーしてペーストする必要はありません） <<http://bombich.com/ja/ja/kb/coc5/how-register-ccc-in-one-click>>。

登録コードはライセンス

購入時に提供されたお名前とメールアドレスに直

結しています。

メールアドレスまたは名前が間違っ

ライセンス情報が正確に適用されていることを確認するには、ライセンスメールを開き、“こちらをクリックしてCCCを登録”をクリックすると自動的に設定が適用されます（必要であれば、CCCをリンクを開く時に使用するアプリケーションとして選択してください）。

登録情報を取得できない場合どうなりますか。

この問題が起きるにはいくつか理由があります。例えば、元々CCCを購入した時に使用したメールアドレスにアクセスできなくなっている場合、どのメールを使用したか覚えていない場合などです。もし登録情報を自動的に取得できない場合、過去の購入を検証する必要があります。その場合、[登録アシスタントのリクエストを送信](http://bombich.com/ja/forgot?found=0) <<http://bombich.com/ja/forgot?found=0>> してください。できるだけ迅速に対応いたします。

登録設定を適用しようとボタンをクリックすると、ブラウザに、この奇妙なURLを開くことはできません、と表示されます。

送信されたメールから“こちらをクリックしてCCCを登録”をクリックした後、“macOSが com.bombich.ccc.lic で開始されるインターネットアドレスを認識できないため、Safariは com.bombich.ccc.lic://blah-blah-blahを開くことができません。”のようなメッセージを受け取った場合、それはCCCがまだこれらのURLを処理するアプリケー

ションとして登録されていないことを意味します。一般的にCCCは、CCCが起動される時にURLハンドラとして登録されますので、CCCをダウンロードしたら必ず、登録設定を適用したいMacで開いてください。既にCCC (3.5 またはそれ以降) を開いていて、それでもこのメッセージが表示される場合、[登録値を手動で入力するには](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code) [<http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code)、または [問い合わせる](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code) [<http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code)、または [問い合わせる](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code) [<http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code) をご利用ください。

CCCをワンクリックで登録するにはどうすればいいですか。

ワンクリック登録を画像付きのステップバイステップで解説しています。ご覧ください。
[<http://bombich.com/ja/ja/kb/ccc5/how-register-ccc-in-one-click>](http://bombich.com/ja/ja/kb/ccc5/how-register-ccc-in-one-click)

CCC の登録コードを手動で入力するにはどうすればいいですか。

手動で登録する方法を画像付きのステップバイステップで解説しています。ご覧ください。
[<http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code)

まだ解決できない問題があります。ヘルプが必要ですが、どうすればいいですか。

喜んでお手伝いします。 [この登録アシスタントフォーム](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code)からお問い合わせください
[<http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code>](http://bombich.com/ja/ja/kb/ccc5/how-manually-enter-ccc-registration-code)。できるだけ早急に問題が解決するようお手伝いします。

CCCの1つのライセンスを家族の複数のMacに 使用するには、どうすればいいですか。

CCCライセンス契約は、Carbon Copy Clonerをお客様が非商業目的で個人的使用のために所有または制御するコンピュータにインストールして使用することを許可します。CCCを商業目的または企業や団体に使用している場合でも、この記事の説明を適用することができますが、必ず弊社の[企業及び教育機関向けのライセンスオプション](http://bombich.com/ja/store/corporate) <<http://bombich.com/ja/store/corporate>>を確認して、ライセンス契約に従って使用してください。

まず未登録のMacにCCCをインストールして開く

登録設定の適用を試みる前にもう1台のMacにCCCをダウンロード

<<http://bombich.com/ja/software/downloadccc.php?v=latest>>

してください。CCCを開き、CCCが自動的にアプリケーションフォルダに移動するまでお待ちください。詳しいインストール方法はこちらからどうぞ：[Carbon Copy](#)

[Clonerのダウンロードとインストールの方法を教えてください。](#) <<http://bombich.com/ja/ja/kb/ccc5/how-do-i-download-and-install-carbon-copy-cloner>>

オプション 1：未登録のMacでメールをチェックできる場合

メールを開き、CCCの登録メールを見つけてください。“こちらをクリックしてCCCを登録”のリンクをクリックしてください。詳細は、[ワンクリックでCCCを登録するには](#) <<http://bombich.com/ja/ja/kb/ccc5/how-register-ccc-in-one-click>>

をご参照ください。登録メールが見つかりませんか。[弊社ウェブサイトから新しい登録キーを要求してください](#) <<http://bombich.com/ja/forgot>>。

オプション 2：未登録のMacでメールをチェックできない場合

1. 既に登録済みのMacで登録メールを開きます。

登録設定を別のMacに適用するには、[こちらをクリックしてCCCを登録](#)のボタンまたはリンクを購入確認のメールからデスクトップにドラッグしてください。

Registering Carbon Copy Cloner

Please resist the temptation to type in that really long registration code. If you're reading this email on your Mac and you already have CCC installed*, just click on this great big button:

Click Here to Register CCC

Click Here to Register CCC
<https://mew.bombich.com/li...RB-XNPZ8-WC3NL-CEMAF-8K8M>

We suggest that you do this right now, while you're online. As long as you already have CCC installed on your Mac, clicking the magic button should instantly apply the registration settings to CCC. If you don't already have Carbon Copy Cloner installed, do this first:

1. [Download the latest version of CCC \[Alternate\]](#)
2. Double-click the downloaded zip file and drag the Carbon Copy Cloner icon into your Applications folder.
3. Launch Carbon Copy Cloner, then go back to this email and click the registration button above to apply your registration settings

*** Not on your Mac right now?** If you want to apply this registration code to another Macintosh covered under the same license, drag the big registration button to your Desktop, then distribute the bookmark file to the other Macs and open it there.

2.登録リンクをデスクトップにドラッグ



リンクをデスクトップにドラッグすると、ブックマークファイルがデスクトップに表示されます。

3.転送してダブルクリック



このファイルをメール、フラッシュドライブ、ファイル共有、クラウドストレージなどを利用して未登録のMacに転送し、そこからCCCの登録設定を適用してください。

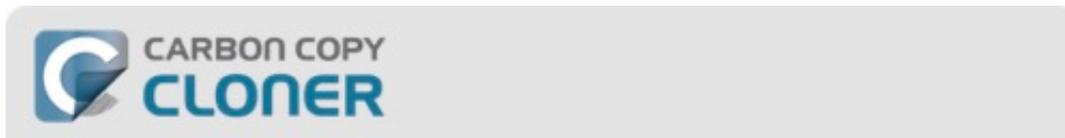
おっと! そのライセンスコードは正しくありませんよ...

CCCを起動しようとした時にこのウィンドウが表示された場合

一般的に2つの問題が考えられます。

1. 1つは、お名前、メールアドレス、登録コードが購入時に指定された情報と正確に一致しない場合。お名前とメールアドレスは登録メールのものと**正確に**一致する必要があります。
大文字/小文字の区別もあります! 一致しないと、ライセンスは無効と表示されます。
2. もう1つは、実行中のCCCのバージョンが破損しているために、<https://bombich.com/download>
<<http://bombich.com/ja/download>>から新規コピーをダウンロードして置き換える必要がある場合があります。

CCCに入力された情報を確認するには、**戻る**をクリックしてください。



おっと! そのライセンスコードは正しくありませんよ...

タイプミスを防ぐため、お客様にお送りしたメール内の"CCCで登録設定に申し込む"のリンクをクリックしてください。

助けて!

戻る

CCC を購入

試用期限は、2017/07/20 12:08 です

登録の詳細

登録メールを開いて、表示されている情報が**正確に**一致するか確認してください。確認が済んだら**登録**をクリックしてください。



ご登録いただきありがとうございます！

Carbon Copy Cloner 5

名

name@email.com

メールでライセンスを取得

ライセンスを変更

閉じる

I already purchased CCC but can't find my registration code. Can you send it to me?

Yes, you can [request via our website <http://bombich.com/forgot>](http://bombich.com/forgot). If you're getting a message about a trial and you have already purchased CCC, or if you have any other questions or concerns about your registration, you can [retrieve your registration code here <http://bombich.com/forgot>](http://bombich.com/forgot).

Migrating CCC tasks from one system to another

If you wish to migrate your tasks from CCC on one system to CCC on another system, follow these steps:

1. Choose Export All Tasks from CCC's File menu.
2. Specify a name for the exported settings file and a location where to save it.
3. Transfer the exported settings file to another Mac.
4. Install CCC onto the other Mac
5. Double-click the exported settings file.
6. As prompted, review the task settings and reset the source/destination selections as necessary.

Note that CCC uses a unique identifier to positively identify your source and destination volumes. While your other Mac may have a "Macintosh HD" volume and a "Backup" volume, those volumes will appear very different to CCC on the second Mac. Simply reselect those new volumes in CCC's Source and Destination selectors to update the task for your additional Mac.

Also note that CCC's keychain is not transferrable between Macs. If you migrate CCC tasks to a new Mac, you will have to re-supply CCC with any applicable volume, disk image, or SMTP passwords.

Recovering tasks from a backup

Many people find that "cleaner" applications will aggressively remove CCC's tasks and preferences. If you have lost all of your backup tasks but you have a full backup of your startup disk, you can recover your tasks from the backup with these steps:

1. Quit CCC if it is running.
2. Choose Computer from the Finder's Go menu.
3. Click on your startup disk (often named Macintosh HD)
4. Navigate to /Library/Application Support/
5. Move the com.bombich.ccc folder to the Trash (note: doing so will remove any saved tasks on that volume).
This folder may not be present, and that's OK.
6. Open a new Finder window (e.g. File > New Finder Window).
7. Choose Computer from the Finder's Go menu.
8. Click on the backup disk
9. Navigate to /Library/Application Support/
10. Copy the com.bombich.ccc folder to /Library/Application Support/ on your startup disk.
11. Open the Activity Monitor application (Applications > Utilities)
12. Choose All Processes from the View menu
13. Find and quit the com.bombich.ccchelper application.
14. Open CCC — your tasks should now be restored.

Note that you may have to activate suspended tasks, and/or reselect the source or destination volumes in your tasks.

Also, please note that you must move the com.bombich.ccc application support folder that is located in the root-level Library folder (e.g. Macintosh HD > Library, NOT Macintosh HD > Users > USERNAME > Library). If you're looking in your home folder, you're in the wrong place.

CCCの使用開始準備をするには

バックアップドライブを選択するには

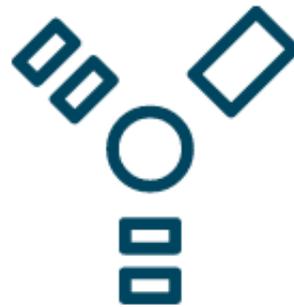
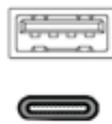
USB、Firewire、それともThunderbolt？



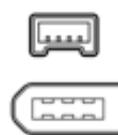
Thunderbolt



USB



Firewire



多くのハードドライブエンクロージャはFirewire、USB、Thunderbolt、またはハードドライブをコンピュータに接続するためのインターフェースを組み合わせて持っています。これらのインターフェースはバックアップおよびデータの保護には充分です。

一般的に複数のインターフェースオプションを提供するエンクロージャを購入することをお勧めします

(例：Thunderbolt+USBなど)。お使いのMacがUSB 3.0をネイティブにサポートしない場合（例えば、2012年より古いもの）、USBデバイスがMacを起動する可能性はありますが、パフォーマンスはMacの内蔵ハードドライブよりもかなり遅いものになります。

Catalinaを使用している場合

:FireWire接続したデバイスからMacを起動することについてAppleはサポートを終了しました。FireWireデバイスへのバックアップは問題ありませんが、起動可能なバックアップが必要な場合は、USBまたはThunderbolt経由でMacに接続できるデバイスを使用する必要があります。

推奨ハードドライブ

ハードドライブエ

ンクロージャのほとんどは、バック

アップになら問題ありません。ただし、[起動可能なデバイスとしては機能しないものもあります](#)

<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#knownissues>

。それぞれのエンクロージャとMacのどの組み合わせがうまくいく、うまくいかない、という完全なリストをここで紹介するのはほぼ不可能です。しかし、お勤めがあるかと尋ねられることがよくあるので、ここに私たちがテストした中で良い結果が得られたハードドライブエンクロージャのリストをご紹介します。パフォーマンスと価格には相伴うものがあります。USBのみ対応のデバイスを選んだ場合、2015年以前のMacはそのデバイスから起動する時、遅くなります。USB-Cを搭載したMacは、USB-C (USB 3.1) 搭載のハードドライブからうまく動作します。エンクロージャ内のディスクがSSDである場合は特にうまく動作します。

USB 3.1、第2世代ポータブル外部SSD

これらのデバイスは適度な量の

ストレージと優れたパフォーマンスを提供します。以下は起動可能なバックアップデバイスのお勧めです:

Oyen Digital U32 Shadow External SSD USB-C (1-4TB) <<https://amzn.to/2CVG23q>> (UK <<https://alteredimagesltd.com/product/u32-shadow-dura-usb-c-rugged-portable-ssd/>>)

Oyen Digital MiniPro Dura USB-C (USB 3.1) Rugged (1-4TB) <<https://amzn.to/2KjWNe5>>

USB 3.1、デスクトップ外部ハードドライブ (メカニカルドライブ)

Oyen Novus 外付け USB-C Rugged デスクトップハードドライブ (2TB-16TB) <<https://amzn.to/2YroF40>>

Thunderbolt、デスクトップ外部ハードドライブエンクロージャ (ディスクなし)

HighPoint RocketStor RS5212 Thunderbolt Storage Dock <<https://www.bhphotovideo.com/c/product/985459-REG/highpoint52122baythunderbolt10gbsstorage.html/BI/20458/KBID/15280/kw/HIRS5212/DFP/d10-v21-t1-x451315>>

Oyen Novus 外付け USB-C Rugged デスクトップハードドライブエンクロージャ <<https://amzn.to/2GPwNE1>>

USB 3.1、外部エンクロージャ (ディスクなし)

Oyen Digital MiniPro Dura 2.5" SATA to USB 3.1 外付けハードドライブ/SSD エンクロージャ <<https://amzn.to/2PdKc0m>>

むき出し HDD (SATA) 500GB - 6 TB

これらのドライブは“裸”なので、外付けとして使用するには、エンクロージャまたはドックが必要です

WD Black Performance 内蔵ハードドライブ - 7200 RPM Class、SATA 6 Gb/s、256 MB Cache、3.5" <<https://www.amazon.com/Black-4TB-Performance-Hard-Drive/dp/B00FJRS6FU/&tag=bombich-20&creative=9325&linkCode=as2&creativeASIN=B07G3LYX3M&linkId=0561481c219dc81a5c076d88092b4ffa>>

推奨できません

エンクロージャを購入する前に、必ず、そのデバイスに関連する [周知の互換性の問題](http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#knownissues)

<<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#knownissues>>

がないか確認してください。しかし

、ここでは一般的なアドバイスと、非常によく使われている

が、macOSの起動可能なバックアップディスクとしてはうまく機能しないことが知られているデバイスをいくつか紹介します。

シングル磁気記録方式を使用するディスクは避ける

数年前、Seagateは回転式ハードドライブのストレージ容量を増加させるために [シングル磁気記録方式](https://www.seagate.com/tech-insights/breaking-areal-density-barriers-with-seagate-smr-master-ti/)

<<https://www.seagate.com/tech-insights/breaking-areal-density-barriers-with-seagate-smr-master-ti/>> を導入しましたが、書き込みパフォーマンスが犠牲になりました。これらのデバイスでは、特にAPFSのパフォーマンスは相当悪化すると思われます。多くの製造元は最近まで、自社製のデバイスのSMRの使用について、必ずしも率直というわけではありませんでした。SMRを利用するデバイスには以下のものが含まれています:

- これらのSeagate製ディスク <<https://www.seagate.com/internal-hard-drives/cmr-smr-list/>>
- これらのWestern Digital製ディスク <[https://blog.westerndigital.com/wp-content/uploads/2020/04/20200422WDSMR\\$KUs1Slide.pdf](https://blog.westerndigital.com/wp-content/uploads/2020/04/20200422WDSMR$KUs1Slide.pdf)>
- これらの東芝製ディスク <<https://toshiba.semicon-storage.com/ap-en/company/news/news->

[topics/2020/04/storage-20200428-1.html](https://bombich.com/ja/topics/2020/04/storage-20200428-1.html)>

5400RPM 回転式 HDD、別名 “スリム型”、“ポータブル”、または “2.5” ハードドライブ”:

これらのディスクは安価で、人気があります。

しかし残念ながら、APFSは回転式ディスクでは良いパフォーマンスをしないことがわかっています

<<http://bombich.com/ja/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>>

。そして、そのパフォーマンスはこれらの “遅いものの中で最も遅い” 回転式ディスクでは、受け入れ難いものです。以下のディスクはこれらの遅いデバイスの例です。

macOSの起動可能なバックアップにこれらを使用することは推奨できません:

- Seagate Backup Plus Slim ポータブルドライブ
- Western Digital My Passport Ultra Portable
- LaCie Mobile Drive
- G-Technology G-DRIVE Mobile USB 3.0対応 外付けポータブルハードドライブ

上記のいずれかのデバイスを所有している場合、APFSではなく、そのデバイスをAppleの古い “Mac OS 拡張 (ジャーナリング)” を使ってフォーマット <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x#chooseformat>> して、データのためのバックアップ <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable>> に使用できます。

Samsung T5 Portable SSD および Transcend StoreJet SSD [High Sierra および Mojave 限定]:

Samsung T5 Portable SSD および Transcend StoreJet SSDは小型の便利なデバイスですが、それらにHigh SierraまたはMojaveがインストール

され、APFSフォーマットされている場合、[起動プロセスの最初に長い遅延を引き起こす](#)

<<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#knownissues>> という報告が多く寄せられています (弊社にも、一般的にインターネットでも)。この遅延は外部SSDからMacを起動しようとする場合にも、さらにはその内部ディスクからMacを起動する場合にさえも起こる可能性があります。特に、外部SSDを主要な起動ディスクとして使用する場合、またはMacを頻繁に再起動する傾向がある場合には、これら2つの外部SSDをHigh SierraおよびMojaveと使用することは避けるよう推奨します。

macOS Catalina、およびそれ以降: Samsung T5 Portable SSDはmacOS Catalinaでは良い結果が出ていることが確認されています。弊社の内部テストでは100%成功をおさめ、弊社の結果を裏付ける報告も数件届いています。

USBメモリスティック、およびSDカード:

回転式ストレージよりも速いと思われるフラッシュストレージですが、USBメモリスティックおよびSDカードは一般的にかなり遅いと言えます。バックアップするデータ量が相当多量な場合、これらのデバイスの使用は推奨できません。さらに、[起動ディスクの起動可能なバックアップの作成には絶対に推奨しません](#)

<<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#knownissues>> 。

Western Digital My Passport HDD

Western Digital My PassportエンクロージャからmacOS Catalinaを起動できないMacがある

<<http://bombich.com/ja/ja/kb/ccc5/macos-catalina-known-issues#wdbootability>>

ことが弊社に数件報告されています。

バックアップボリュームはどれくらい大きくなりますか?

バックアップボリュームはコピーをしたいデータ量と最低でも同じである必要があります。このボリュームに定期的にバックアップする計画をしているのであれば、最優先のルールは、バックアップボリュームは初回にバックアップする予定のデータ量よりも最低50%大きいこと、です。こうすると、データ量の適度な増加や変更および削除されたファイルの一時的なアーカイブにも対応できます。

取り替えのきかない重要なデータには、バックアップタスク専用のボリュームを確保しておくことを強くお勧めします。

他のどこにも存在しないバックアップボリュームにデータがある場合、それはバックアップされていません！Carbon Copy Clonerとの使用にボリュームを対象とする場合、何らかの正当な理由でいくつかのファイルが削除されてしまうリスクが常に伴います。CCCはデータが喪失されることから保護するためのオプションや警告を提供します。しかし、CCCの誤った使用や、提供される機能を誤って理解したことで起きるデータの喪失を防ぐことはできません。

ネットワークアタッチストレージ (NAS) にバックアップするには

NASデバイスは最近人気を集めています。ワイヤレスバックアップの利便性を魅力的に感じる人が多いようです。しかし、ユーザフィードバックから判断すると、NASデバイスを主要なバックアップとして頼ることは次のいくつかの理由でお勧めできません：

- NASデバイスへの書き込みパフォーマンスは、一般的に、最善でも、USB 2.0 HDDへの書き込みと同等
- WiFi経由でアクセスしたNASのパフォーマンスは、平均的なローカル接続のハードドライブに比べて10から100倍遅くなる
- NASデバイスのデータの整合性を定期的に検証することは、ネットワークパフォーマンスの理由で実現が困難
- WiFiバックアップはネットワーク接続とmacOSのネットワークファイルシステムのクライアントと同等の信頼性しかない
- ネットワークファイルシステムのファイルシステムトランザクションは、ローカルに接続されたファイルシステム上でのファイルシステムトランザクションよりもさらに多くのオーバーヘッドを伴うため、データセットに多くのファイルがある場合、非常に長いバックアップウィンドウにつながる (例：> 250K ファイル)
- マウント中、または基になるNASボリュームの空き領域に制限を受けている時、ネットワーク接続が頻繁に喪失されると、ディスクイメージのファイルが最終的に壊れることがあります。Time Machineからネットワークボリュームのバックアップを削除または再作成するよう推奨された場合、基になる問題が同じです。ディスクイメージをマウントできない場合にも、同じ提案ができます。

主要なバックアップには、USBまたはThunderboltハードドライブを入手して、起動可能なバックアップをローカルに接続されたディスクに作成することを推奨します。

万が一Macの起動ディスクが失敗した場合、

ローカルの起動可能なバックアップはずっと

シンプルで信頼性が高く

、復元が簡単です。ネットワークボリュームのディスクイメージからオペレーティングシステムを復元するロジスティクスは、機能する起動ディスクがないとかなり複雑です。機能する起動ディスクを提供することこそが、CCCの強みであり、バックアップの問題を解決することになります。

特に推奨しないNASデバイス

Western Digital MyCloud

Home

：このNASデバイスの“Home”モデルは、ストレージに安全にアクセスするためにWDプロプライエタリソフトウェアの使用を必要とします。SMB経由で直接ストレージにアクセスしたければ、ゲスト権限でのみ利用できます。[ユーザレポート <https://community.wd.com/t/use-my-cloud-home-with-finder-without-wds-app/216769/4>](https://community.wd.com/t/use-my-cloud-home-with-finder-without-wds-app/216769/4) WDのソフトウェアを使用中のストレージパフォーマンスは、SMB経由のゲストアクセスに比べて平均以下です。他のユーザからは、Western Digitalのソフトウェア経由でマウント中、macOSはストレージにディスクイメージを作成またはマウントできない、という報告を受けています。

コピー先ディスクをmacOSのインストール用に準備するには

注意：この操作は指定されたディスクのすべてのデータを消去します

Appleのディスクユーティリティを起動

Finderウィンドウを開き、**アプリケーション > ユーティリティ** と進み、**ディスクユーティリティ**をダブルクリックします。



残りのステップは実行中のオペレーティングシステムにより大幅に異なります。Appleのメニューから**このMacについて**を選択して現在ご使用のOSを確認してから、以下の選択をしてください。

- [macOS 11Big Sur、10.15 Catalina、10.14 Mojave、および10.13 High Sierra](#)
- [macOS 10.12 SierraおよびOS X 10.11 El Capitan](#)
- [OS X 10.10 Yosemite](#)

Big Sur、Catalina、Mojave、およびHigh Sierraでの手順

このチュートリアルビデオをYouTubeでご覧ください <<https://youtu.be/narMTq3d58>>
ディスクユーティリティの使用についての詳しいチュートリアル
<<https://www.youtube.com/watch?v=oEfqfMf2z9k>>

すべてのデバイスを表示

デフォルトで、ディスクユーティリティはお使いのデバイスの非常に単純化された表示を提供します。残念ながら、これではバックアップディスクのパーティションを変更するために選択する必要があるデバイスが隠れてしまいます。

ディスクユーティリティで他のことをする前に、“表示”メニュー、またはディスクユーティリティのツールバーの“表示”のポップアップボタンか**すべてのデバイスを表示**を選択してください。



コピー先ディスクを選択する

CCCタスクのコピー先として使用したいディスクをクリックして選択します。このディスクは起動ディスクと同じであることはできません。

新しいディスクの名前には製造元の名前が含まれていることがよくあります (例: WD My Book 111D Media...)。起動ディスクには製造元のシリアル番号がタイトルに含まれていることがよくあります (例: TOSHIBA MK50...)。ディスクのボリュームの1つではなく、**ディスク**を選択するように、特に注意してください

。デバイスを正しく初期化するには、ディスク全体を選択する必要があります。お使いのディスクがFusionデバイスの場合、代わりにその中の“コンテナ”を消去してもかまいません。



指定されたディスクですべてのボリュームをマウント解除する

ディスクユーティリティは、ボリュームを消去しようとする時、マウント解除に問題を起こすことがあります (例:

Spotlightがマウント解除の要求を妨げる)。ディスク上の任意のボリュームの横にある“取り出す”ボタンをクリックして、ディスクを消去する前にブリエンプティブにそれらをマウント解除してください。

指定されたディスクを消去する

ディスクユーティリティのツールバーから**消去** ボタンをクリックして、ディスクの名前、フォーマット、パーティション方式を設定してください。好きな名前をつけてください。但し、スキームはGUIDパーティションマップと設定してください。スキーム オプションが表示されない場合は、2ステップ戻って、ディスク上のボリュームの1つではなく、ディスクデバイス全体を選択してください。

コピー先ボリュームのフォーマットを選択する

お使いのコピー先デバイスが5400RPM (またはそれより遅い) 回転式HDDの場合：

(例：“スリム型”バックアップデバイス、2.5" ディスク)

APFSはこれらのデバイスのためにはデザインされていません <<http://bombich.com/ja/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>>ので、

macOS起動パフォーマンスは劣る可能性があります <<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#performance>>

。これらのデバイスをAPFSとしてフォーマットして、起動可能なバックアップを試みることはできますが、デバイスのパフォーマンスがあまりにも遅くて実用的でないなら、Mac OS **拡張**

(**ジャーナリング**)をフォーマットとして選択することを推奨します。Big SurまたはCatalinaの起動ディスクのバックアップを作

成したい場合、コピー先の

ファイルシステムがAPFSに変換されるのを避けるために、**データみのバックアップを作成** <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable>>

することを推奨します。

Big

Sur、Catalina、およびMojave

の場合：起動ディスクをバックアップしている場合、またはmacOSの別のインストールをバックアップしている場合、APFS を選択してください。APFS (**暗号化**)

を選択しないでください。バックアップボリュームから起動中、FileVaultを有効にする

<<http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption>>ことでバックアップを暗号化できます。

High Sierra: APFSおよびMac OS **拡張 (ジャーナリング)**

のどちらもシステムをバックアップするフォーマットとして利用できます。Appleの推奨を反映して

<<https://support.apple.com/en-us/HT208033>>

、お使いのデバイスがSSDで、macOSのバックアップに使用される場合、またはT2に基づくMacをバックアップしていて、バックアップで暗号化を有効にするつもりである場合は、APFS

を選択することを推奨します。コピー先デバイスがスピンドラターベースのデバイス (例：ハードディスクドライブ、またはHDD)、または10.13より古いオペレーティングシステムをバックアップする場合は、Mac OS **拡張**

(**ジャーナリング**)を選択してください。

コピー先の名前、フォーマット、パ

ーティションスキームの設定を終えたら、**消去**ボタンをクリックしてください。

ボリュームグループを消去

の選択が与えられたら、そのオプションを選択してボリュームグループ全体を消去してください。



パーティションを追加 (オプション)

複数のソースボリュームをこの同じバックアップディスクにバックアップする場合、パーティションを作成することで整理しておくことができます。バックアップボリュームをAPFSとしてフォーマットした場合は、そのボリュームを選択して、ディスクユーティリティの“編集”メニューから“APFSボリュームを追加...”を選択してください。別のフォーマットを選択している場合は、バックアップボリュームを選択してから、ディスクユーティリティのツールバーにある“パーティション”をクリックしてください。

これで、新規ハードドライブは、Carbon Copy Clonerによって作成されたバックアップを受け入れる準備ができました！

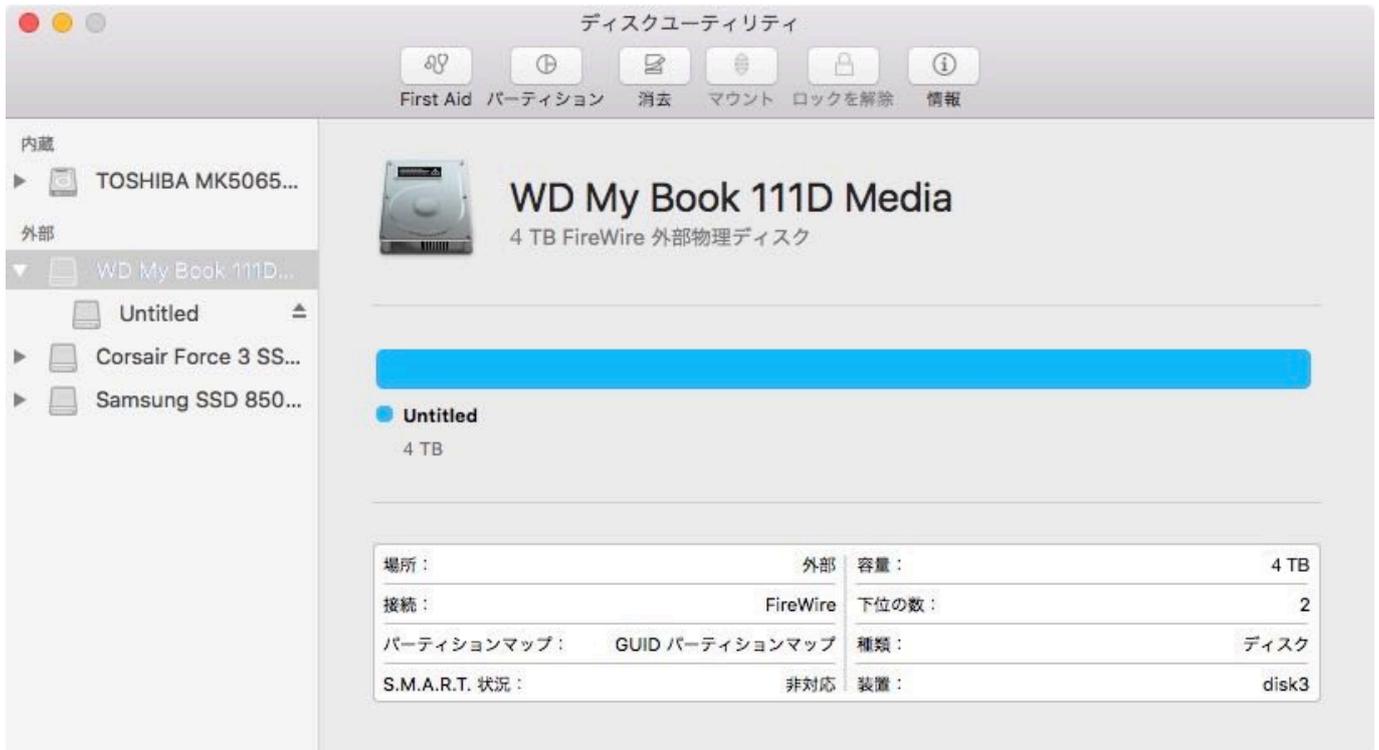
El CapitanおよびSierraの手順

[このチュートリアルビデオをYouTubeでご覧ください <https://www.youtube.com/watch?v=3AUXkwaVVFQ>](https://www.youtube.com/watch?v=3AUXkwaVVFQ)

コピー先ディスクを選択する

CCCタスクのコピー先として使用したいディスクをクリックして選択します。このディスクは起動ディスクと同じであることはできません。

新しいディスクの名前には製造元の名前が含まれていることがよくあります (例: WD My Book 111D Media...)。起動ディスクには製造元のシリアル番号がタイトルに含まれていることがよくあります (例: TOSHIBA MK50...)。



指定されたディスクを消去する

ディスクユーティリティのツールバーから消去 ボタンをクリックして、ディスクの名前、フォーマット、パーティション方式を設定してください。名前にはなんでも好きな名前を使えますが、フォーマットはMac OS 拡張 (ジャーナリング)と、パーティション方式は GUID パーティションマップと、設定してください。その後、消去ボタンをクリックします。



Time Machineを使用しない

使用しないをクリックしてください。Time MachineとCCCの両方のバックアップに同じバックアップディスクを使用しても構いませんが、そうする場合、Time Machineバックアップに専用のパーティションを使用する必要があります。そうしないと、Time Machineはバックアップボリュームにある利用可能なスペースをすべて使用するので、CCCはそのバックアップボリュームを使用できなくなります。



これで、新規ハードドライブは、Carbon Copy Clonerによって作成されたバックアップを受け入れる準備ができました！

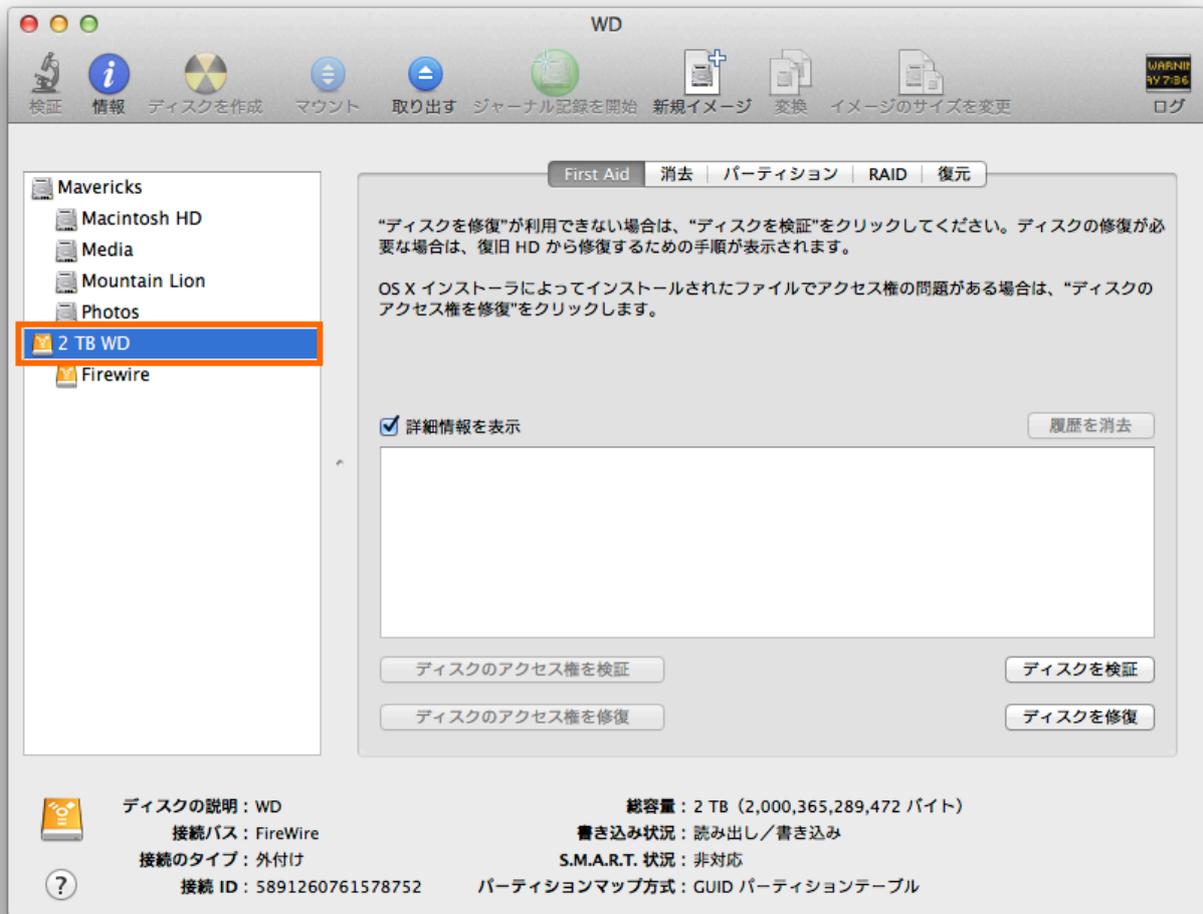
Yosemiteでの手順

このチュートリアルビデオをYouTubeでご覧ください <<https://www.youtube.com/watch?v=WZ1sstRdWjk>>

コピー先ディスクを選択する

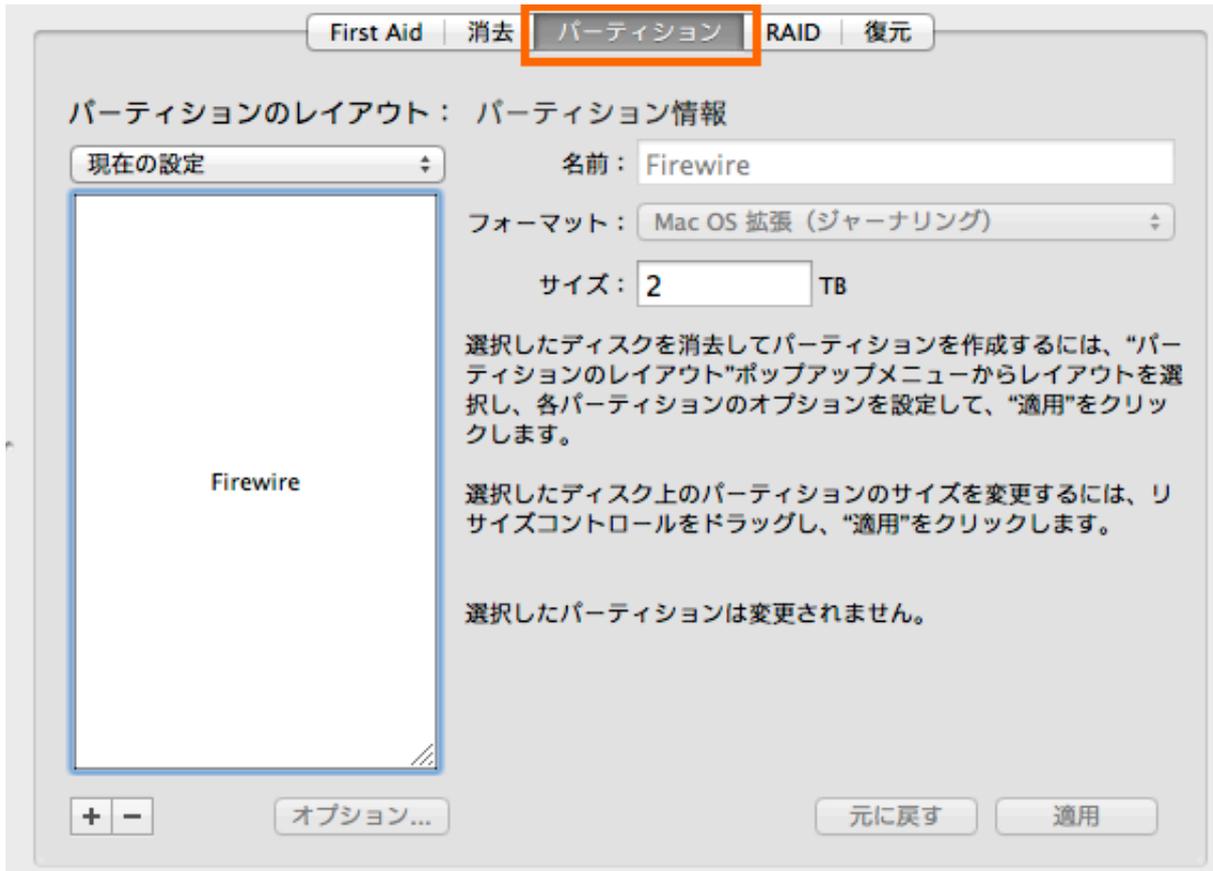
CCCタスクのコピー先として使用したいディスクをクリックして選択します。このディスクは起動ディスクと同じであることはできません。

新しいディスクの名前にはストレージ容量と製造元の名前が含まれていることがよくあります (例: 500.07 GB WD My Passp...)。起動ディスクには製造元のシリアル番号がタイトルに含まれていることがよくあります (例: 320.07 GB TOSHIBA MK3255GSXF メディア)。

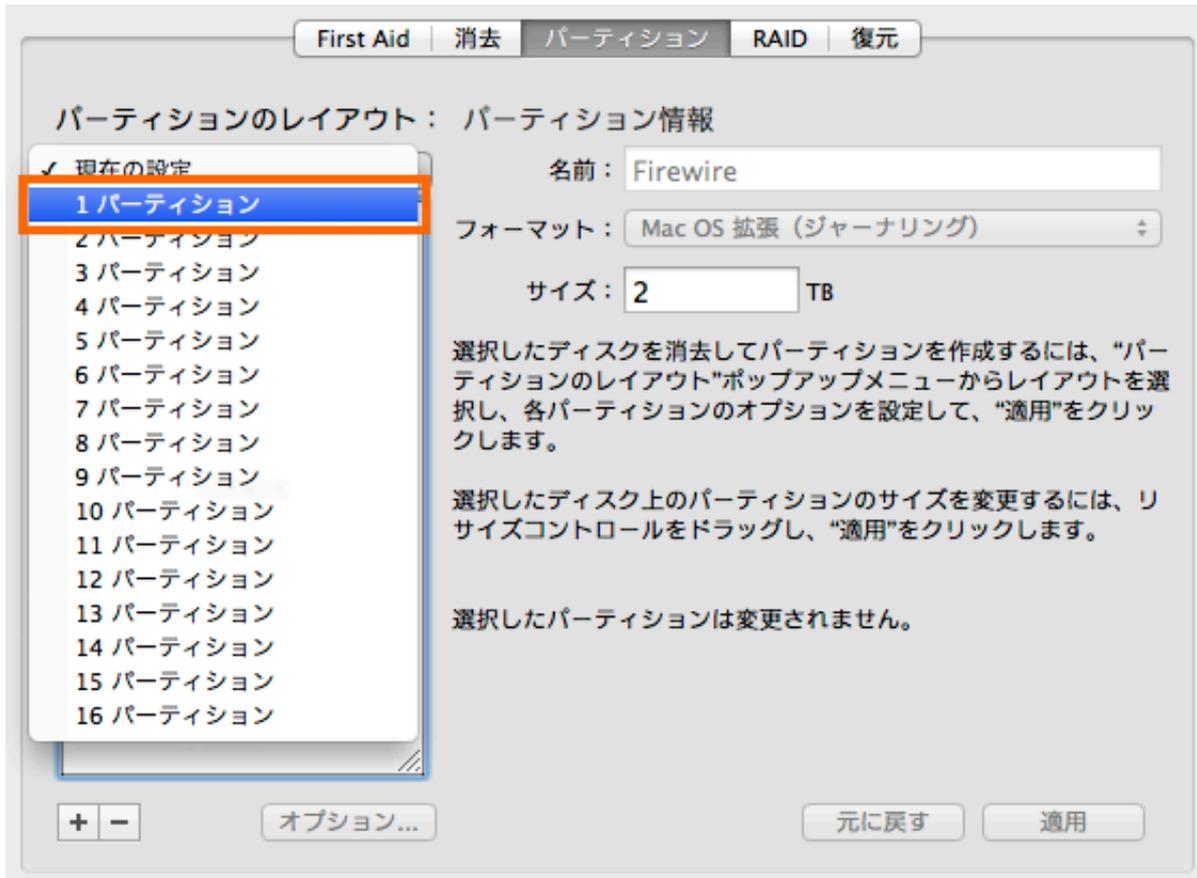


ディスクのパーティションを作成する

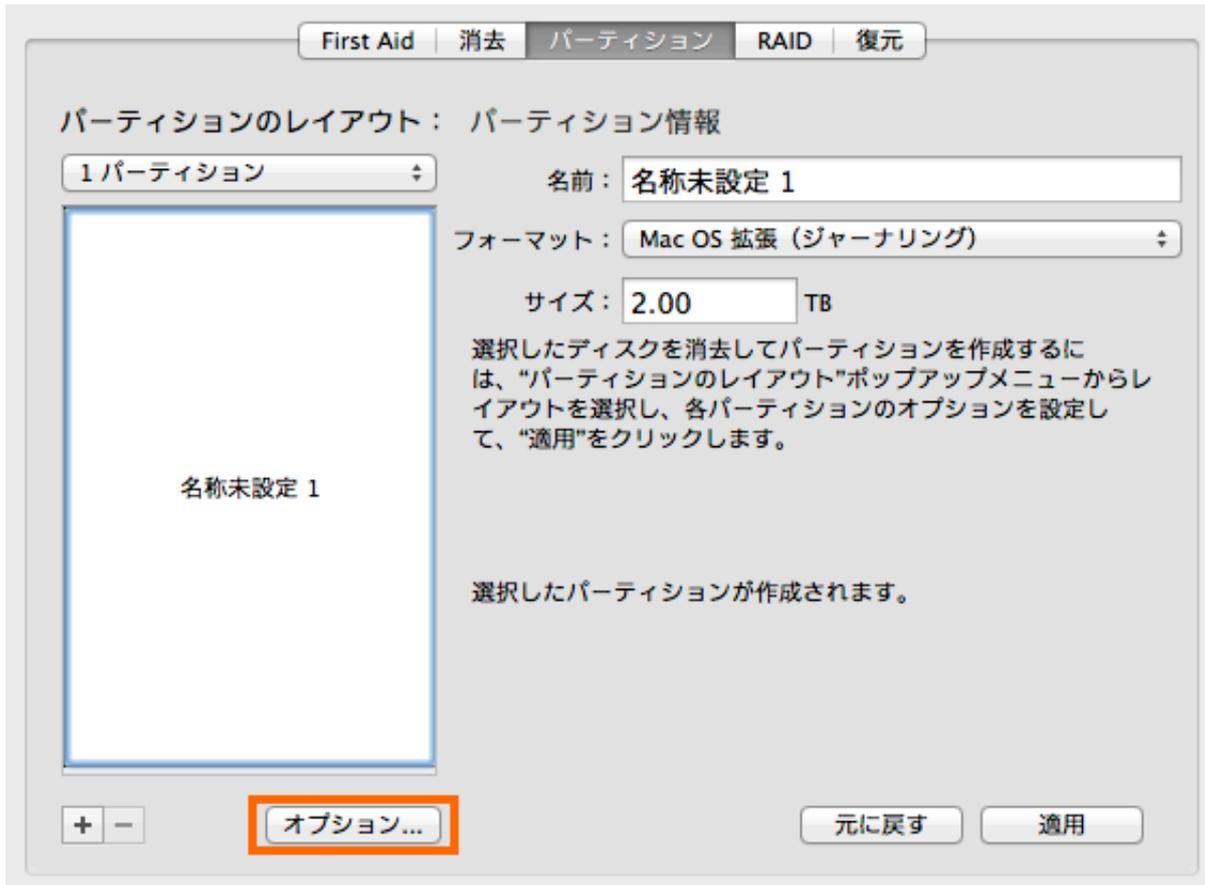
パーティション タブをクリックします。



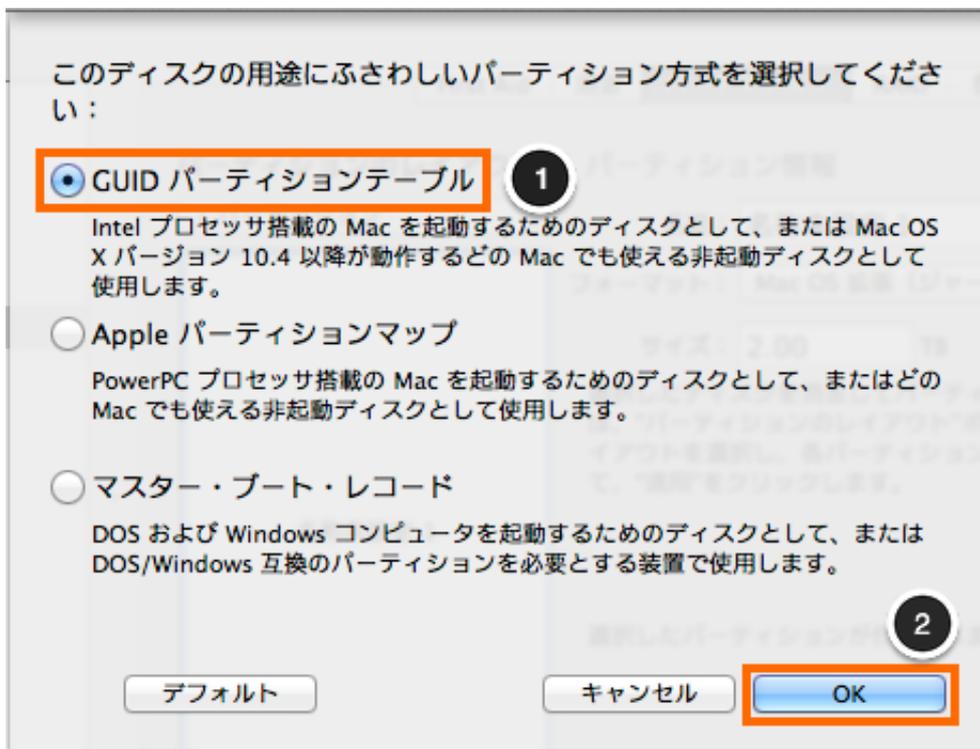
パーティションレイアウトポップアップメニューから 1
パーティションを選択します (必要であれば増加してください)。



オプションをクリックします。



GUID パーティションテーブルを選択し、OKをクリックしてください。

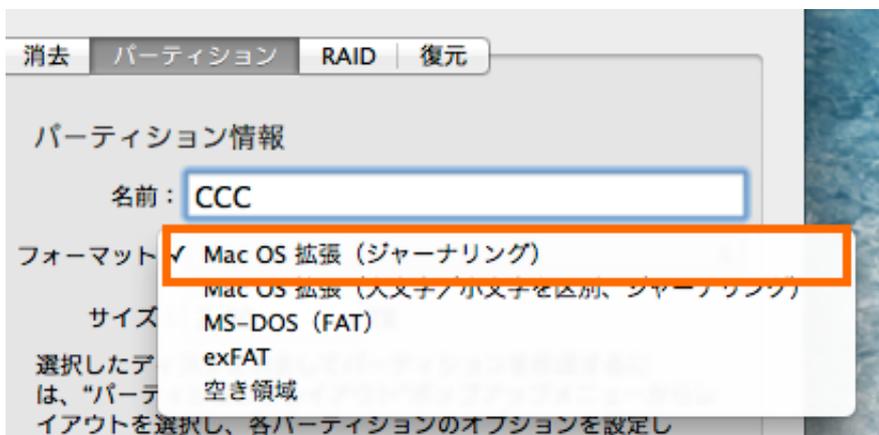


ボリュームに名前をつける

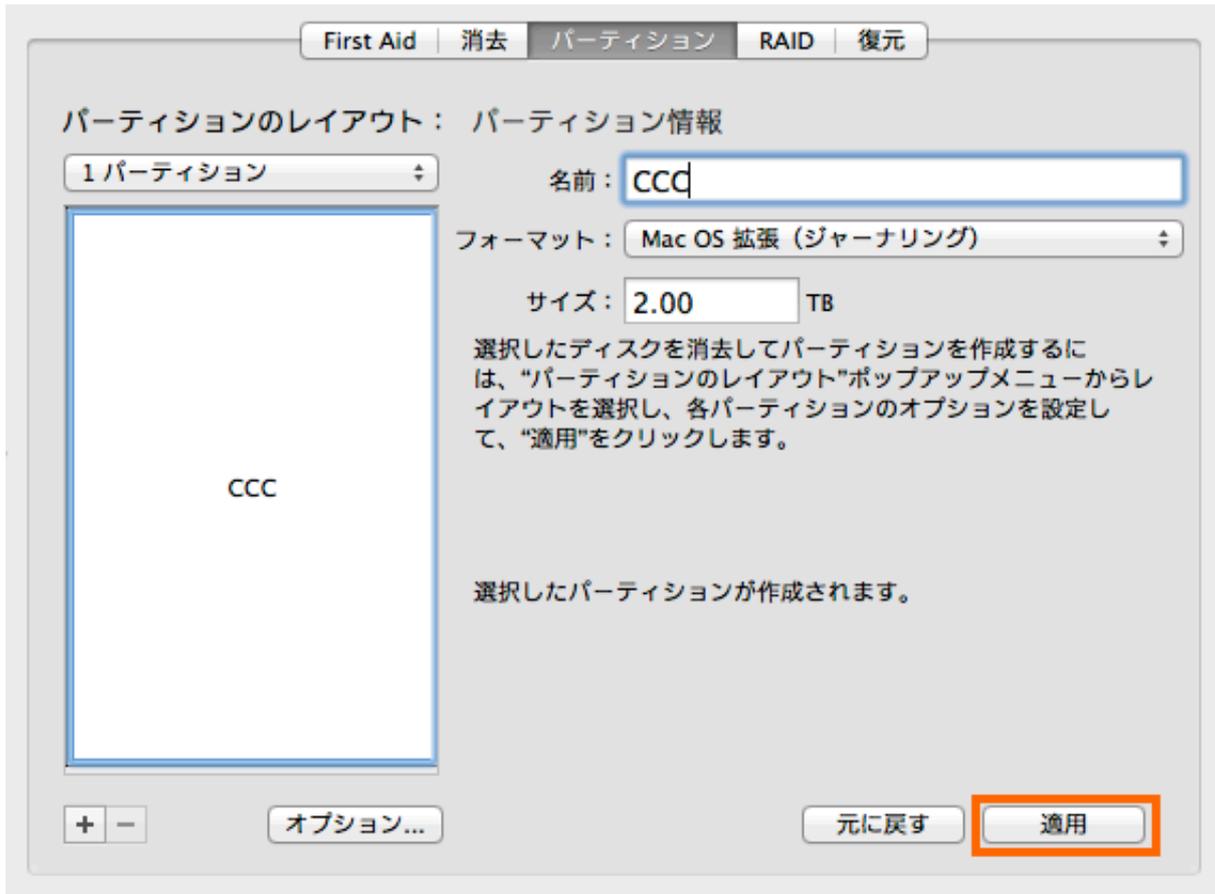


ボリュームをフォーマットする

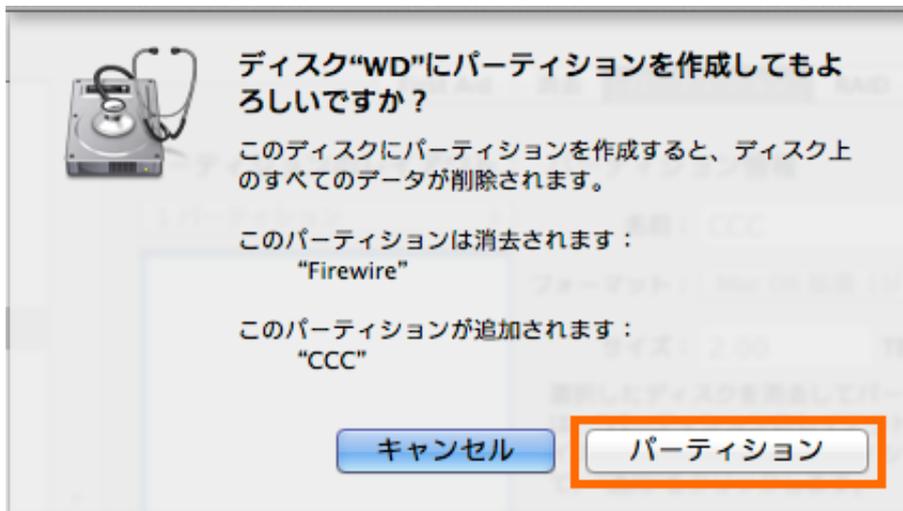
Mac OS 拡張 (ジャーナリング) をパーティションフォーマットのポップアップメニューから選択します。



適用をクリックしてください。



正しいディスクが選択されていることを確認してください。このステップは選択したディスクからすべてのデータを削除します。パーティションをクリックします。



ここから、OS固有ではない[残りの説明にスキップしてください](#)。

関連ドキュメント

- "ディスクは既に HFS+ にフォーマットされているのに、なぜこの警告が表示されるのですか？"
<http://bombich.com/ja/ja/kb/ccc5/my-disk-already-formatted-hfs-why-am-i-getting-warning>
- ビデオ：新規 / 追加のパーティションを作成するには (OS X 10.10、およびそれ以前)



<<https://www.youtube.com/watch?v=XQG6-OJiv3s>>

- サードパーティファイルシステムのサポート(例 : NTFS、FAT32)

<<http://bombich.com/ja/ja/kb/ccc5/backing-up-tofrom-network-volumes-and-other-non-hfs-volumes>>

Mac OSをアップデートするための最善策

すでに最新のmacOSを実行中でCCCを開くのに問題がある場合、[CCCの最新バージョンをダウンロード](http://bombich.com/ja/software/downloadccc.php?v=latest)
<<http://bombich.com/ja/software/downloadccc.php?v=latest>> しているか確認してください。

Appleが次のメジャーOSを発表しました。アップグレードにワクワクしていますよね！でもその準備はできていますか？OSのアップグレードはワクワクするような新機能、より良いパフォーマンス、バグの修正、などが搭載されていますが、と同時に時間や生産性の低下など代価を払うことがあります。OSをアップグレードしてしまった後に、重要なサードパーティ

アプリケーションや周辺機器が正しく動作しない、
しかも

前のバージョンのOSにダウングレードするのは不可能

だと気が付いた時には本当に途方に暮れてしまうでしょう。しかし、完全に、起動可能な、アップグレード前のMacのバックアップがあれば、その心配はありません。

Macをアップグレードするべきですか？

メジャーなシステムアップグレードは往々にして破壊的なことがあります。従って、それらの適用に関しては、常に非常に保守的なアプローチを推奨しています。以下の点を考慮してください：

- 自分のMacはアップグレードが必要か？
- アップグレードに心ひかれる機能が含まれているか？
- このアップグレードは自分のMacのパフォーマンスを向上させるか、それとも下げてしまうか？
- アップグレードすることで、Macを効率的に使用することを妨げていた問題が修正されるか？
- アップグレードを適用後、使用できなくなるソフトウェアがあるか、あるとすればどれか？
- 自分の古くなっているMacにこのアップグレードを適用すると、その陳腐化を早めることにならないか？

アップグレー

ドの結果が喜ばしいもので

はなく、ダウングレードしなければならない場合、も

ちろん**前のOSからのCCCのバックアップを使ってダウングレード** <<http://bombich.com/ja/ja/kb/ccc5/best-practices-updating-your-macs-os#downgrade>>

することも可能です。しかし、この種の処理には時間と労力が必要です。ですから、OSをアップグレードすることで得られる可能性のある利点と、面倒なことが起きる可能性を秤にかけて判断する必要があります。

最後に、仕事やその他の生産性において、Macの有用性に大きく依存しているユーザの皆さんには、OSのメジャーアップグレードをインストールする前に、いくつかのアップデートを待つことを検討するようにお勧めします。最初のリリースはワクワクするものですが、そのワクワクにはリスクが伴います。いち早くアップグレードを採用した人たちが、必然的にその欠点やバグを発見してくれるので、マイナーなOSアップデートで修正されます。

アップグレードの前に起動可能なバックアップを作成する

1. バックアップディスク

クを用意してください。ディスクのお勧めを見たい場合は、[こちらのCCCドキュメント](http://bombich.com/ja/ja/kb/ccc5/how-set-up-your-first-backup)
<<http://bombich.com/ja/ja/kb/ccc5/how-set-up-your-first-backup>>を参照してください。

2. macOSのインストールのためにバックアップボリュームを準備します

<<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>>。

3. CCCをダウンロード <<http://bombich.com/ja/software/downloadccc>> して起動します。

4. ソースセレクトから起動ディスクを選択します。
5. コピー先セレクトからバックアップボリュームを選択します。
6. “クローン” ボタンをクリックしてください。
7. バックアップドライブが起動可能かどうかをテストします <<http://bombich.com/ja/ja/kb/ccc5/how-verify-or-test-your-backup>>
: システム環境設定アプリケーションから起動ディスク環境設定パネルを開き、バックアップディスクを起動ディスクとして選択してから、再開してください。
8. AppleメニューからこのMacについて
を選択して、お使いのMacがバックアップディスクから起動されているか確認してください。
9. システム環境設定アプリケーションで起動ディスクのセレクションをお使いの製品起動ディスクにリセットして、再開します。
10. バックアップディスクをMacから接続
解除して横に置いておきます
。新しいOSを使う決心が着くまで、バックアップディスクがスケジュール済みのバックアップタスクで自動的にアップグレードされるのを避けるためです。

新しいOSにアップグレードする

Mac App Storeから最新のOSをダウンロードして、アップグレードを適用します。

まず、すべてが正しく動作しているか確認してください... それから、バックアップを再開してください

時間を取って、あなたにとって最も重要なアプリケーションを実行してみてください。1週間ほどして、すべてが順調で新しいOSに移行する覚悟ができたなら、バックアップディスクをMacに接続してCCCを開き、同じ設定でバックアップタスクをもう1度実行してください。これは重要なステップです。というのは、一旦バックアップタスクが完了すると、そのバックアップを使って前のOSにダウングレードすることはできなくなります。

ダウングレードする必要がある場合は、以下を実行してください

macOS Catalina (またはBig Sur) から macOS Mojave (またはそれ以前のOS) にダウングレードするには
<<https://youtu.be/aBjk5ghQPfw>>

CCCの起動可能なバックアップを使用して、High Sierra (またはMojave) からSierraにダウングレードするには
<<https://youtu.be/UMvSfDTaLwY?t=9m44s>>

新しいOSでAppleアプリケーションを開く時 (例: メール、連絡先、カレンダー、など)、これらのアプリケーションは即座に、そして不可逆的にそれらのアプリケーションのためのユーザデータをアップグレードするということを念頭に置いておいてください。Mojaveを (例えば) 再インストールして、アップグレードしたユーザデータでいつも通りにすることは単純にできないのです。それらのAppleアプリケーションのCatalinaバージョンは、アップグレードされたデータを使用できないからです。

前のOSにダウングレードする必要がある場合は、アップグレード以前の状態の、完全に起動可能なMacのバックアップが不可欠です。

すべてを効率的に前のバージョンのOSに復元して戻すには、以下を実行してください:

1. CCCのバックアップタスクを一時的に無効にします <<http://bombich.com/ja/ja/kb/ccc5/monitoring-backup-tasks-ccc-menubar-application#disabletasks>>
2. CCCのバックアップディスクをMacに接続します
3. システム環境設定の起動ディスクの設定パネルを開きます
4. バックアップボリュームを起動ディスクとして選択してから、“再起動” ボタンをクリックしてください
5. ディスクユーティリティを開きます
6. オリジナル (アップグレード済み) の起動ディスクをマウント解除します

7. 表示メニューから “すべてのデバイスを表示” を選択します
8. オリジナルの起動ディスクを含むディスクデバイス全体、つまり "Macintosh HD" ボリュームの親を選択します
9. ディスクユーティリティのツールバーから “消去” をクリックします
10. High Sierraよりも古いOSにダウングレードする場合、またはHigh Sierraを使用中のFusionデバイスに復元しようとする場合、OS X拡張(ジャーナリング)フォーマットを使用してくださいそれ以外は、APFSをフォーマットとして使用してください
11. CCCを開きます
12. ソースセレクトからバックアップボリュームを選択します
13. コピー先セレクトからオリジナルの(今は空になった)OSボリュームを選択します
14. デフォルト設定、つまり “SafetyNetをオン” のままにしてください
15. “クローン” ボタンをクリックしてください。

復元の処理が完了したら、システム環境設定で起動ディスクをリセットして、Macを再起動してください。あっという間に前のOSに戻ることができます！

注意：システムが新しいOSを実行中、処理を作成または変更した場合、古いバージョンのファイルが復元されます。残念ながら、新しいOSを使用しながらAppleアプリケーション

(例：カレンダー、アドレスブック、メール、写真、等

)で作成された個人的なデータは、古いOSと互換性を持たない

<http://bombich.com/ja/images/blog/newerphotoslibrarynotbackwardscompatible.png>

ので、その情報を復元することはできません。

“アップグレード前の起動可能なバックアップがありませんが、ダウングレードしたいと考えています。どうすればいいですか？”

起動可能なバックアップがない場合、ダウングレードすることは単純なタスクではありません。また、期待している結果を得られない可能性があります。中には古いシステムアプリケーションが読み取れない項目もあります。例えば、Appleのメール、カレンダーなど、基本的にAppleのアプリケーションはすべてアップグレードされたデータ保存を使用することはできません。古いOSのクリーンインストールで開始する場合、最善のオプションは “ホーム” フォルダのみの復元を試みることです。これは弊社がサポートを提供できる設定ではありません (サポートされている設定にはアップグレード前の起動可能なCCCのバックアップが必要です)。しかし、CCCで以下の手順を使用するとお使いの “ホーム” フォルダを復元することができます：

1. すべてのアプリケーションとすべてのFinderウィンドウを終了してください
2. CCCを開き、新規タスクを作成します
3. ホームフォルダをバックアップディスクからCCCのソースセレクトにドラッグします
4. ホームフォルダを現在の起動ディスクからCCCのコピー先セレクトにドラッグします
5. 高度な設定ボタンをクリックします
6. トラブルシューティングから、アクセス権を保持しないの横にあるチェックボックスをチェックします (これにより、アカウントが古いシステムと新しいシステムで異なる数字のIDを持つことで生じる所有権の問題を回避することができます)
7. “クローン” ボタンをクリックします

復元したいアプリケーションがある場合は、Finderでドラッグ&ドロップするか、またはインストーラからそれらをインストールし直して復元することを推奨します。

この操作は現在ホームフォルダにあるものをすべて置き換えますので、注意してください。既に項目を手動で復元した場合、この操作はそれを取り消しますので、ドラッグ&ドロップして手動でファイルを復元する方法が適切かもしれません。

追加情報

- Carbon Copy ClonerとAPFSについて知っておくべきこと <http://bombich.com/ja/ja/kb/ccc5/everything-you->

[need-know-about-carbon-copy-cloner-and-apfs>](#)

- macOS CatalinaからmacOS Mojaveにダウングレードするには <<https://youtu.be/aBjk5ghQPFw>>
- CCCの起動可能なバックアップを使用して、High SierraからSierraにダウングレードするには <<https://youtu.be/UMvSfDTaLwY?t=9m44s>>
- APFSフォーマットされたFusionボリュームをダウングレードするには <<https://youtu.be/YeQ0N5izTlo>>
- バックアップボリュームをmacOSのインストール用に準備するには <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>>
- ディスクユーティリティと動作してCCCのバックアップディスクを準備するには <<https://youtu.be/narMTq3d58>>
- CCCのバックアップをテストするには <<http://bombich.com/ja/ja/kb/ccc5/how-verify-or-test-your-backup>>

ヘルプが必要な時は

行き詰まったり、何かアドバイスが必要な場合は、CCCから直接お問い合わせいただけます。CCCの“ヘルプ”メニューから“質問する”を選択して、ヘルプデスクまで質問をお寄せください。

CCCを使用するには

最初のバックアップを設定するには

このチュートリアルビデオをYouTubeでご覧ください <<https://www.youtube.com/watch?v=SADf7xp97nE>>

バックアップディスクをコンピュータに接続する

この件に関する追加情報は、バックアップドライブを選択するには <<http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive>> を参照してください。

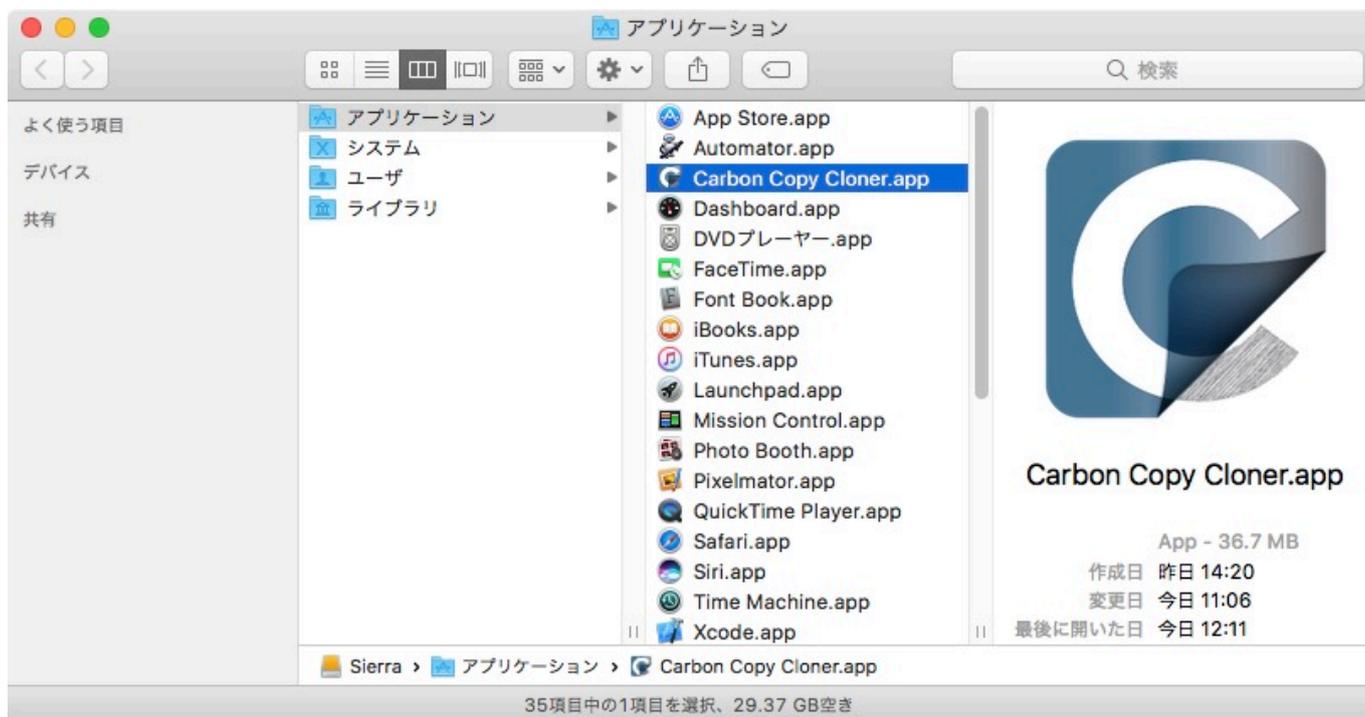
ディスクをフォーマットする

macOSのバックアップのために新規ディスクを使用できるようにするために、まず最初に“ディスクユーティリティ”を使って正しいフォーマットでディスクを初期化する必要があります。

詳しい手順はドキュメントの [macOSのバックアップのためにバックアップディスクを準備するには](http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>> をご参照ください。また、そのチュートリアルビデオをYouTubeで見る <<https://www.youtube.com/watch?v=3AUXkwaVVFQ>> こともできます。

Carbon Copy Cloner を開く

アプリケーション > Carbon Copy Cloner



CCCを初めて開くと、最初のタスク設定の手順を案内されます。案内が必要ない場合は、CCCのツールバーにあるヒントをクリックしてください。

ソースを選択する

ソースの下の点線の四角をクリックして、利用できるソースを表示します。

こちらも参照: ""Macintosh HD"と"Macintosh HD -

Data"の別々のバックアップタスクを作成する必要がありますか? <<http://bombich.com/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#separatetasksCollapse>> "

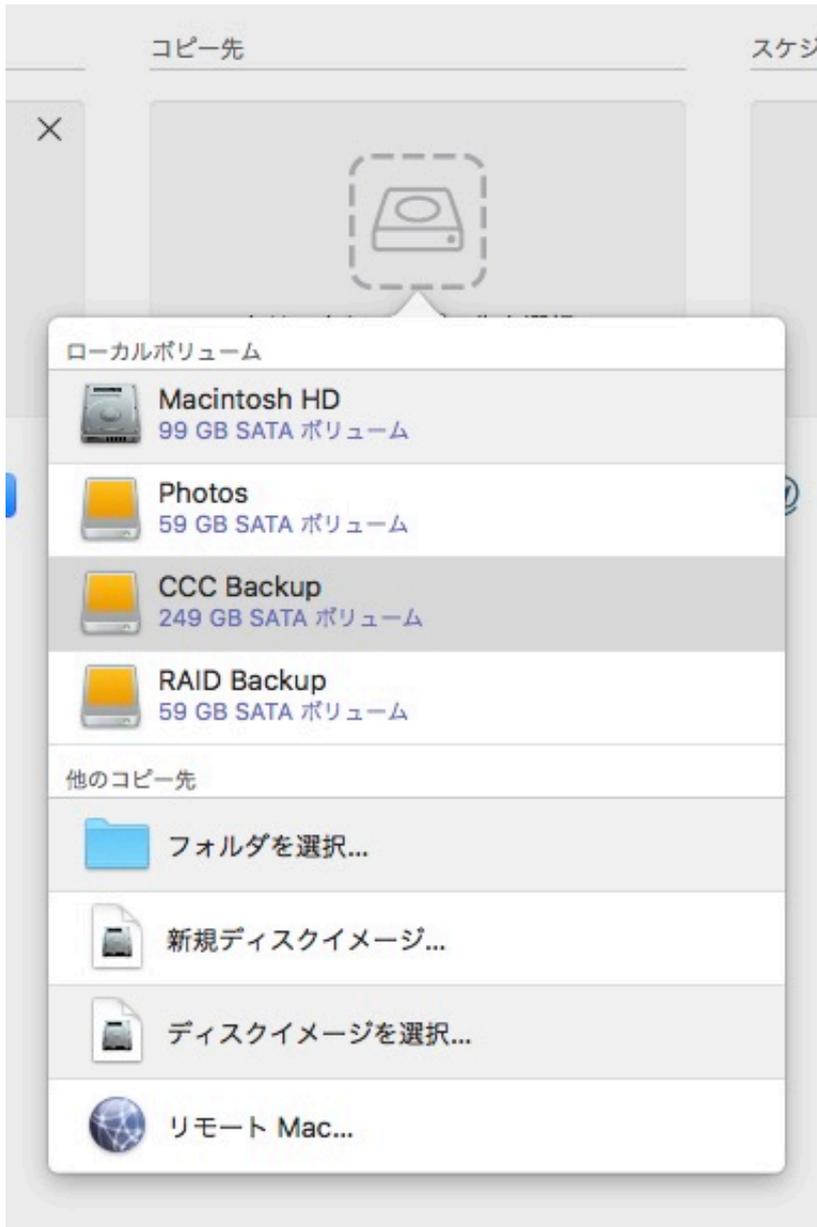


ソースに利用できるボリュームのメニューから起動ディスクを選択します。



コピー先を選択する

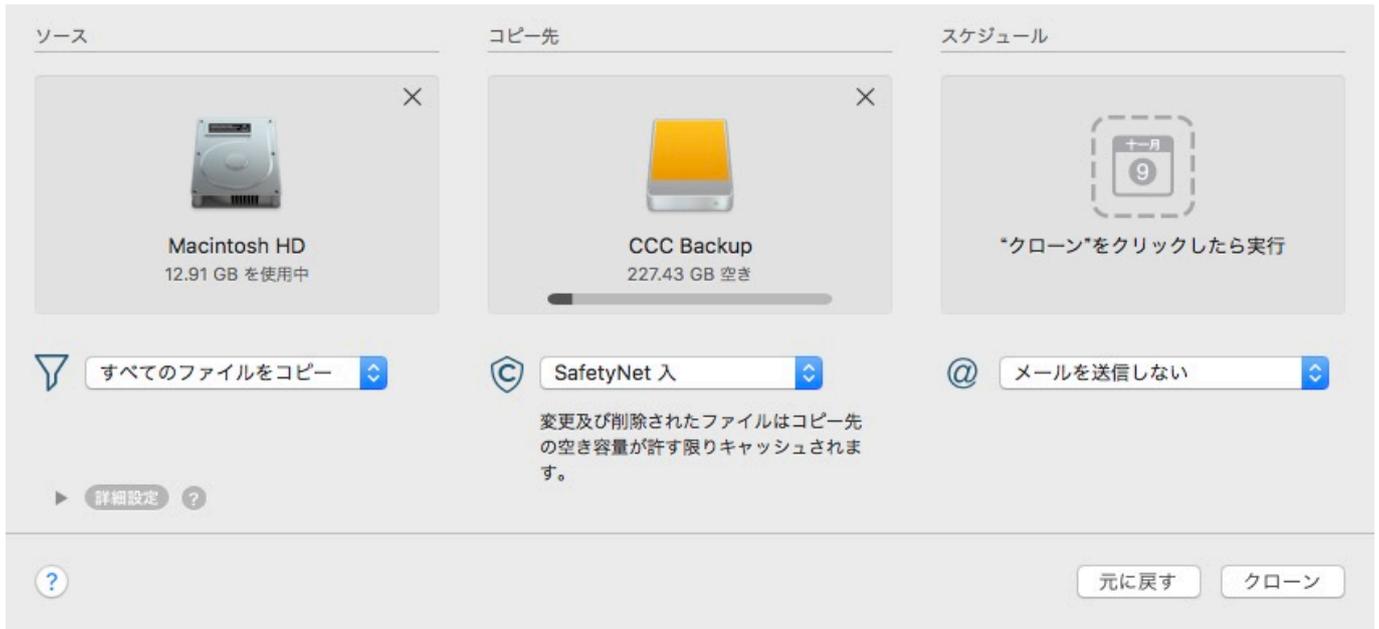
コピー先の下にある点線で囲まれたボックスをクリックして利用可能なコピー先を表示し、コピー先に利用できるボリュームから新規バックアップドライブを選択してください。



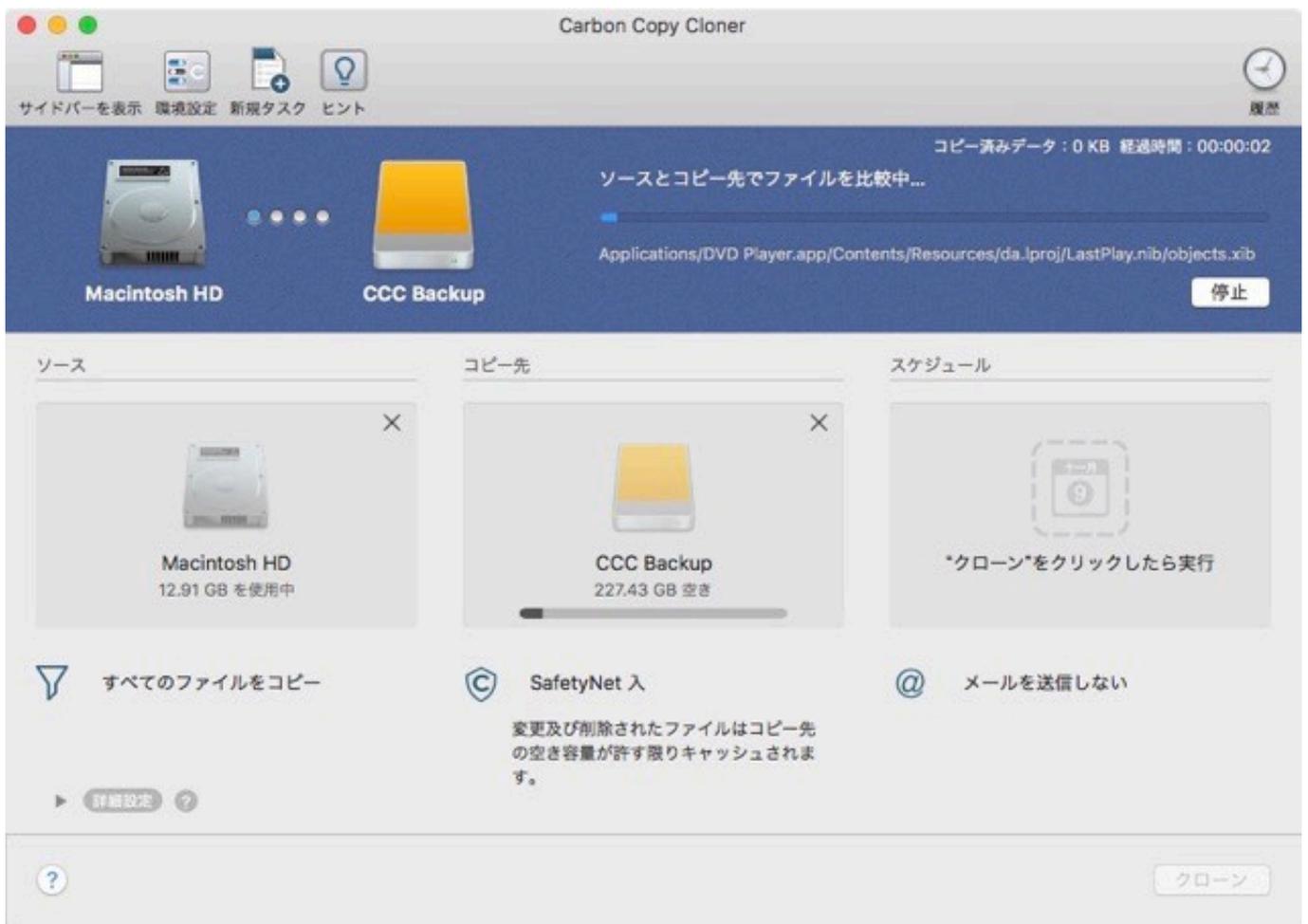
クローンを開始

クローン

をクリックします。バックアップタスクを最初に実行すると、権限ヘルパーツールがインストールできるようにCCCから認証メッセージが表示されます。このヘルパーツールは権限のあるタスク、例えばシステムファイルをコピーするなど、を実行するために必要です。



おめでとうございます！最初のクローンが進行中です！



スマートアップデート

同じバックアップタスクをもう1度実行する場合、CCCは変更された項目のみをコピーします。この動作を実行する特別な

設定はありません。単

にクローンボタンをもう1度クリックするか、バックアップタスクをスケジュールに従って自動的に実行
<<http://bombich.com/ja/ja/kb/ccc5/how-set-up-scheduled-backup>>するように設定してください。

関連ドキュメント

- macOSのシステムボリュームをApple Software Restoreを使ってクローンするには
<<http://bombich.com/ja/ja/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>>
- バックアップを検証またはテストするには <<http://bombich.com/ja/ja/kb/ccc5/how-verify-or-test-your-backup>>
- 使用例 <<http://bombich.com/ja/kb/tags/sample-usage-scenarios>>
- ヘルプを取得するには? <<http://bombich.com/ja/ja/kb/ccc5/how-do-i-get-help>>

起動可能なバックアップを検証またはテストするには

バックアップディスクをコンピュータに接続する 起動ディスクの環境設定を開く

システム環境設定 > 起動ディスク



バックアップボリュームを選択する

左下隅にある鍵ア

アイコンをクリックした後、検証したいバックアップボリュームを選択します。再開をクリックしてください。

このときお使いの起動ディスクが表示されない場合は、Optionキー (Intel Macの場合)、またはパワーボタン (AppleシリコンMacの場合)

を押したままMacを再起動して、起動マネージャから起動ボリュームを選択してください。

Big Surの起動ボリュームのいくつかが環境設定の“起動ディスク”に表示されないことがある
<<http://bombich.com/ja/ja/kb/ccc5/mac-os-big-sur-known-issues#startupdiskprefpane>>



起動ディスクを検証する

Macが再開後、AppleメニューからこのMacについて... を選択します。



バックアップボリュームから起動したことを検証してください。



バックアップをテストする

アプリケーションを数個起動し、データが元の状態のままであることを確認してください。

起動ディスクをリセット

起動ディスクの環境設定パネルで起動ディスクをオリジナルの起動ディスクにリセットしてから（前述の通り）、コンピュータを再開してください。

関連ドキュメント

バックアップの統合性を詳しく検証するには、[高度な設定](http://bombich.com/ja/ja/kb/ccc5/advanced-settings) <<http://bombich.com/ja/ja/kb/ccc5/advanced-settings>> の、[壊れているファイルを見つけて置き換える](#)をご参照ください。

- アプリケーションが異なる動作をしたり、クローンしたボリュームのシリアル番号を要求することがあります。CCCがなにか見つけられませんか。 <<http://bombich.com/ja/ja/kb/ccc5/some-applications-behave-differently-or-ask-serial-number-on-cloned-volume.-did-ccc-miss>>
- “ コピー先のディスクの使用状況がソースと一致しません。CCCがコピーしていないファイルがありますか。 <<http://bombich.com/ja/ja/kb/ccc5/disk-usage-on-destination-doesnt-match-source.-did-ccc-miss-some-files>>
- ヘルプ！クローンが起動しません！ <<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot>>

バックアップから復元するには

Finderでドラッグ&ドロップしてバックアップボリュームから項目を個別に復元すること

<https://youtu.be/n7JgLKyW0> ができます。バックアップディスクから復元したい項目を見つけて、起動ディスクにドラッグして戻すだけです。多数の項目を起動ディスクに復元したい場合は、[フォルダからフォルダ](http://bombich.com/ja/ja/kb/ccc5/folder-folder-backups)
<http://bombich.com/ja/ja/kb/ccc5/folder-folder-backups>

のタスクを設定して、特定のフォルダをバックアップディスクから起動ディスクの特定のフォルダに復元してください。

システムファイル、アプリケーション、またはバックアップのすべてを復元したい場合は、以下のステップに従って、バックアップディスクからMacを起動し、バックアップディスクをMacの内部ハードドライブに復元してください。

バックアップディスクをMacに接続する

USB、またはThunderboltケーブルを使ってバックアップディスクをMacに接続してください。

環境設定 “ 起動ディスク ” を開く

システム環境設定 > 起動ディスク



バックアップボリュームを選択する

ウインドウの下にある南京錠のアイコンをクリックして認証した後、復元に使用したいバックアップディスクを選択してください。再開

をクリックしてください。これでバックアップからシステムが再起動され、バックアップがメインハードドライブにクローンされます。



環境設定の起動ディスクパネルを使用できない場合...

環境設定の起動ディスクパネルから起動ディスクを変更できない場合

(例えば、オリジナルのハードディスクから起動できない場合)、Optionキー (Intel Macの場合)

、またはパワーボタン (AppleシリコンMacの場合)

を押したままMacを起動してください。バックアップディスクが起動ディスクのオプションとして**起動マネージャ**

<<https://support.apple.com/en-us/HT204417>>

に表示されます。起動マネージャの一覧にお使いのバックアップボリュームが表示されていない場合は、

ヘルプ!をご覧ください。CCCのドキュメントの“クローンが起動しません!”

<<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot>>

のセクションに詳しいトラブルシューティングの提案がありますので、ご参照ください。

注意:

バックアップ

ディスクからMacを起動で

きない場合、または新しいiMacにデータを移行する場

合は、“**移行アシスタント**”を使って、データをCCCのバックアップディスクから移行

<<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#migrate>>できます。

復元先にしたいディスクを準備する

ほんの数個の個別ファイルを復元する場合を除いては、バックアップを復元する時には新しくフォーマットされたディスクを使用することをお勧めします。コピー先をフォーマットする全手順は**バックアップディスクをOS Xのバックアップ用に準備する** <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>>

を参照してください。これは、macOS High

Sierra、およびそれ以降を復元する際に特に重要ですので、ご注意ください。

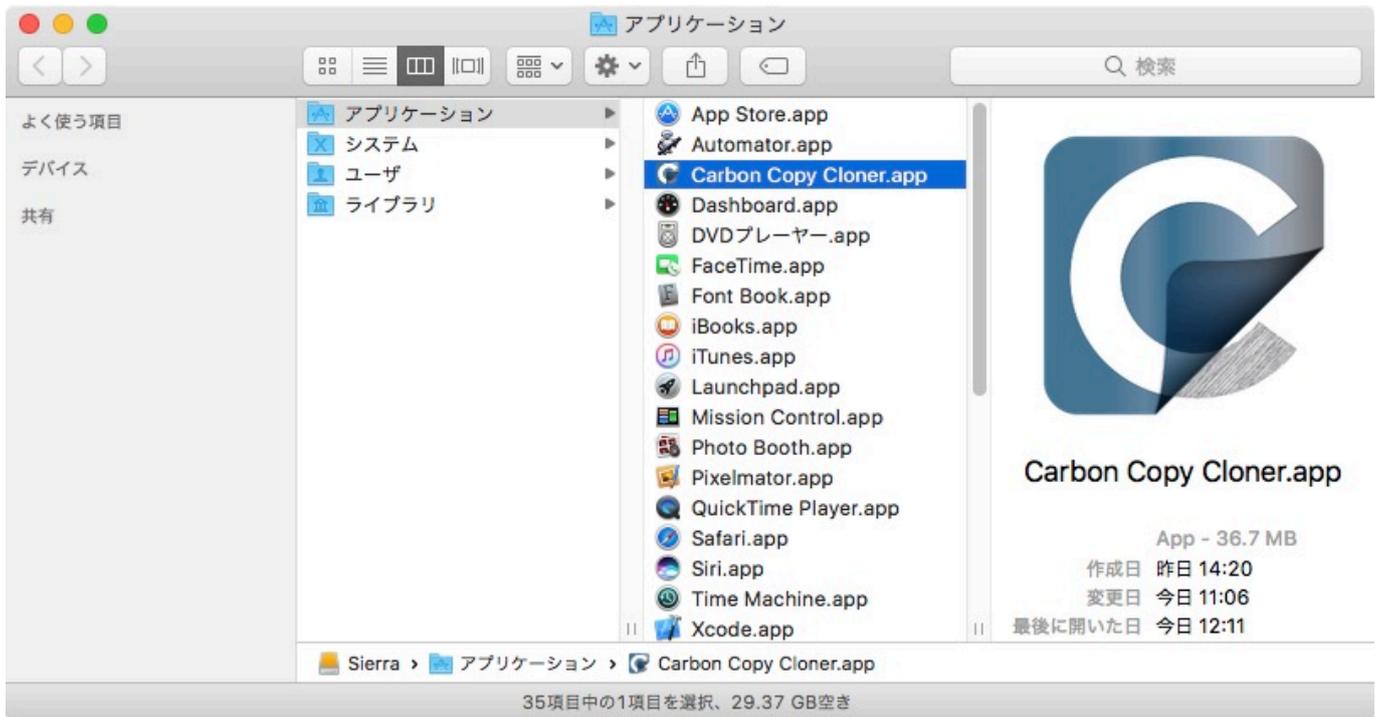
Sierra、およびそれ以降を復元する際に特に重要ですので、ご注意ください。

Carbon Copy Cloner を開く

Macが再起動を完了したら、Carbon Copy Clonerを開いてください。**アプリケーション** > Carbon Copy Cloner

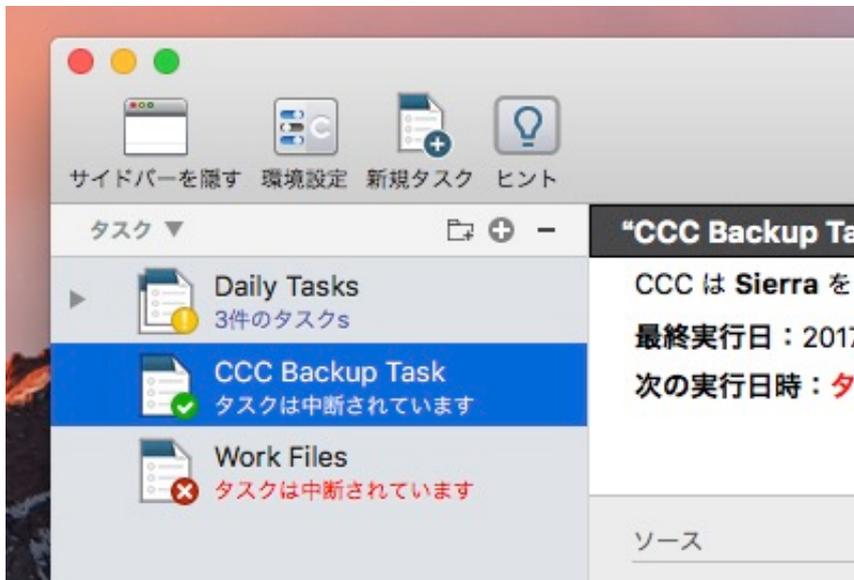
注意: CCCをバックアップボリュームで開くと、CCCは復元タスクの設定を案内する表示が提示されます。それは、ここで紹介する手順と重複します。この提示を辞退する場合、CCCは通常予定されているタスクが中断されていることを示します。提示があった場合、タスクを中断したままにしておけるオプションを選択してください。

同様に、タスクを保存するように指示された場合、“変更を元に戻す”を選択してください。

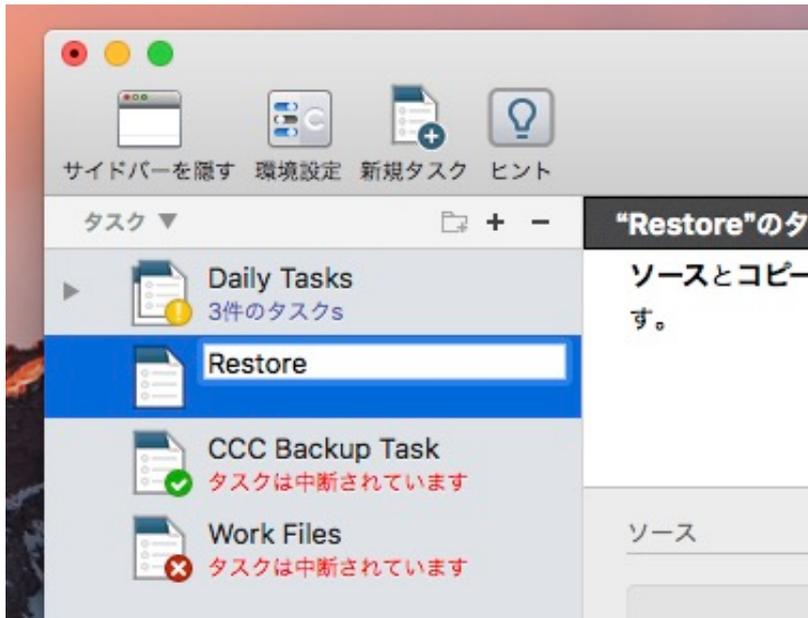


新規タスクを作成する

タスクヘッダの+をクリックします。必要であれば **サイドバーを表示** をクリックしてください。



新規タスクに名前をつけてください。



ソースを選択する

“ソース” の下の点線の四角をクリックして、利用できるソースを表示します。クリックして、バックアップ

ボリューム をソースとして選択してください。Catalina**を使用している場合**

:システムボリュームおよびデータボリュームを復元するために別の復元タスクを作成する必要はありません。CCCが両方のボリュームを復元します。



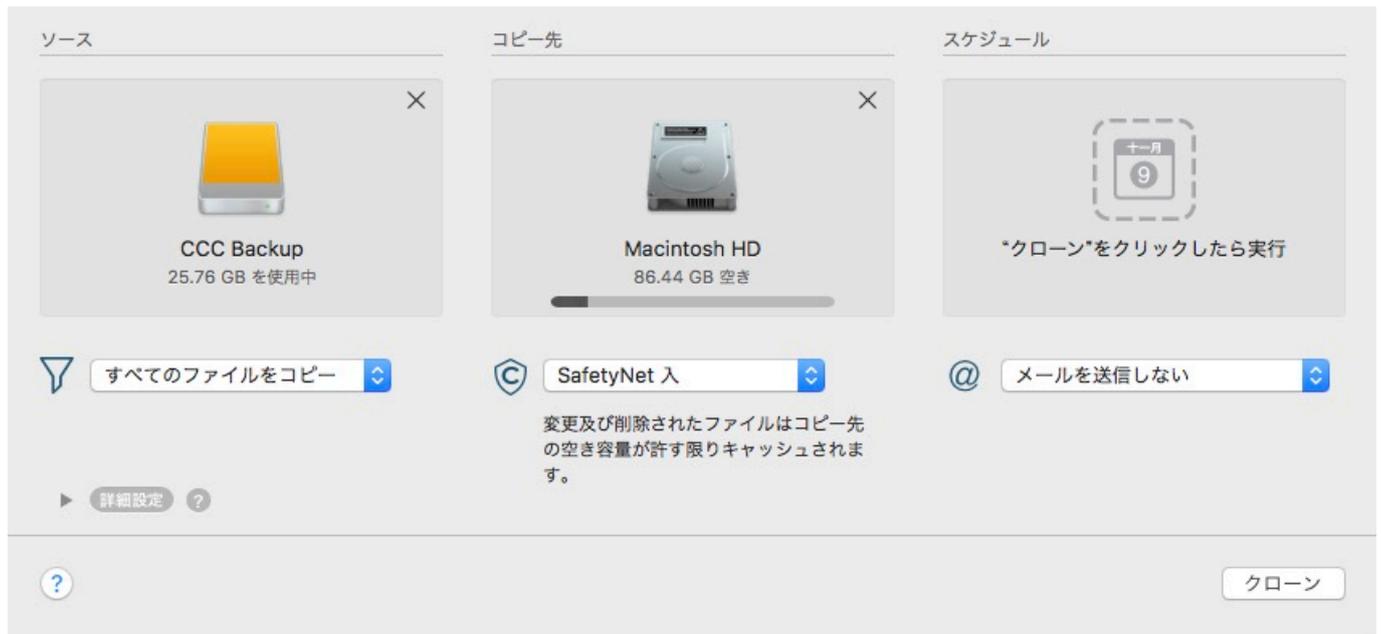
コピー先を選択する

“コピー先”の下**点線の四角**をクリックして利用可能なドライブを表示してください。復元先に指定したい**ボリューム**をクリックして、選択してください。



クローンをクリック

右下の“クローン”ボタンをクリックして、復元タスクを開始してください。



起動ディスクをリセット

クローンを完了後、CCCのユーティリティメニューから**起動ディスク**を選択します。起動ディスクをオリジナルの起動ディスクにリセットしてコンピュータを再起動してください。

復元をテスト

アプリケーションを数個起動し、データが元の状態のままであることを確認してください。

おめでとうございます。これでバックアップからデータの復元ができました！

関連ドキュメント

- ヘルプ！クローンが起動しません！ <<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot>>
- ビデオ：CCCのバックアップから個別のファイルとフォルダを復元するには <<https://youtu.be/nZJgLKyW0>>
- 非システムファイルを復元するには <<http://bombich.com/ja/ja/kb/ccc5/restoring-non-system-files>>
- ディスクイメージから復元するには <<http://bombich.com/ja/ja/kb/ccc5/restoring-from-disk-image>>
- “完全なボリュームのバックアップがフォルダかディスクイメージにありますが、起動可能なバックアップがありません。どうすればすべてを復元できますか？” <<http://bombich.com/ja/ja/kb/ccc5/i-have-full-volume-backup-in-folder-or-disk-image-i-dont-have-bootable-backup.-how-can-i>>

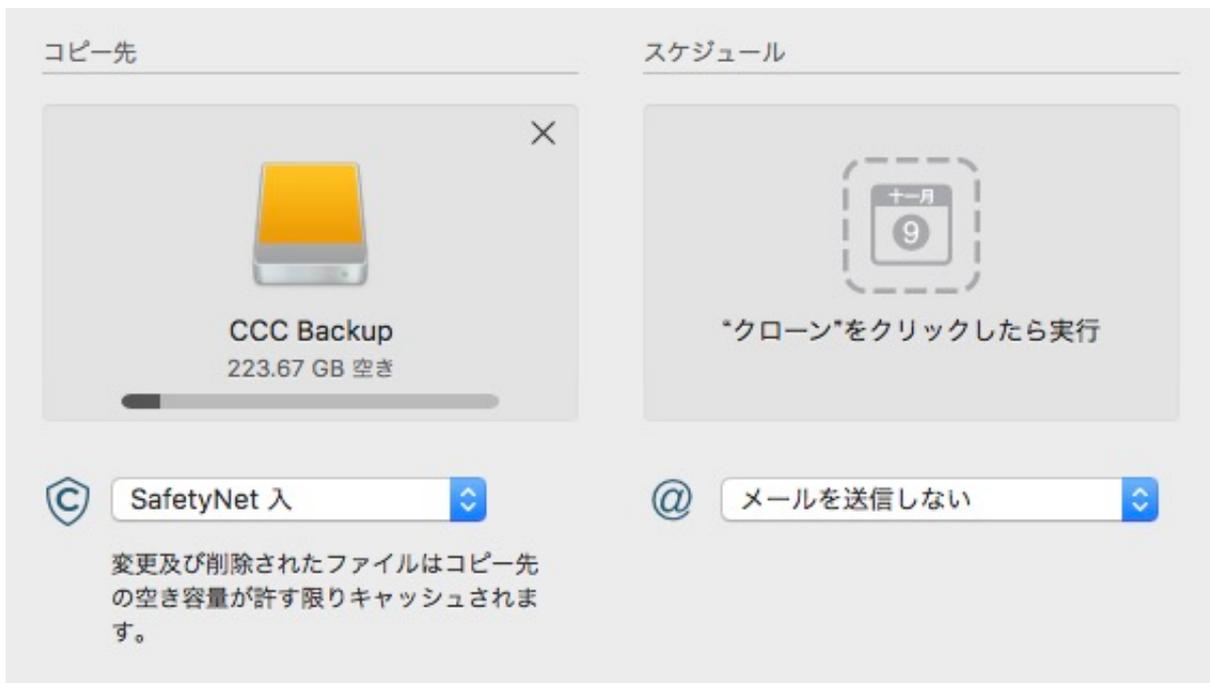
バックアップのスケジュールを設定するには

このチュートリアルビデオをYouTubeでご覧ください <<https://www.youtube.com/watch?v=IHijjbbTiV4>>

タスクを設定

ソースとコピー先

を選択して、今すぐバックアップタスクを実行するかのようにCCCを設定します。スケジュールの下の点線で囲まれたボックスをクリックしてスケジュールオプションを表示してください。



スケジュールを設定する

ドロップダウンメニューからタスクをいつ実行したいか選択してください。タスクを定期的に行いたい場合は、毎時、毎日、毎週、毎月の中から選択してください。ソースまたはコピー先ボリュームがMacに再接続された時にタスクを実行したい場合は、**ソースまたはコピー先が再接続された時**のオプションを選択してください。



スケジュールに希望する変更を加えたら、**完了**をクリックします。

Carbon Copy Cloner

タスクを実行：

日単位

繰り返しの間隔： 1 日

開始時刻： 2017/ 6/20 午後 5:00

次の実行時刻： 明日 午後5:00:00 GMT-4

実行条件

別のタスクが同じ書き込み先には書き込まれている場合、延期

このタスクを実行する条件

今日が週末でなければスキップ

今日が週末であればスキップ

このタスクを実行する時間を制限

午後 7:00 から 午後 7:00

システムのスリープ状態

このタスクを実行しようスケジュールされている時にシステムがオフまたはスリープ状態の場合：

システムをスリープ解除する

ソースまたはコピー先が見つからない場合：

エラー通知を送信しない

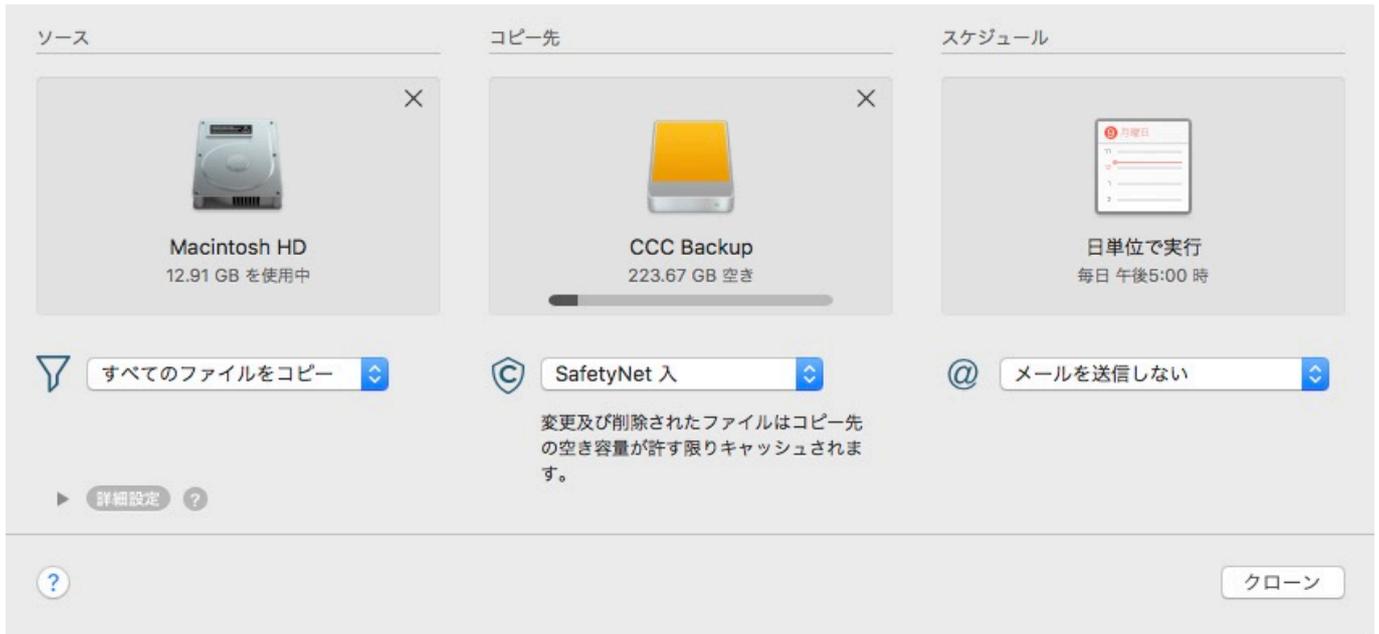
みつからなかったボリュームが再度表示されたらすぐにこのタスクを実行

?

完了

タスクを保存

保存をクリックします。



The screenshot shows the Carbon Copy Cloner (CCC) configuration window. It is divided into three main sections: **ソース** (Source), **コピー先** (Destination), and **スケジュール** (Schedule).

- ソース:** Shows "Macintosh HD" with 12.91 GB in use. Below it is a filter icon and a dropdown menu set to "すべてのファイルをコピー".
- コピー先:** Shows "CCC Backup" with 223.67 GB free. Below it is a shield icon and a dropdown menu set to "SafetyNet 入". A note below states: "変更及び削除されたファイルはコピー先の空き容量が許す限りキャッシュされます。"
- スケジュール:** Shows a calendar icon and the text "日単位で実行 毎日 午後5:00 時". Below it is an @ icon and a dropdown menu set to "メールを送信しない".

At the bottom left, there is a "詳細設定" button with a question mark. At the bottom right, there is a "クローン" button.

スケジュールした日時にバックアップタスクが実行されます！

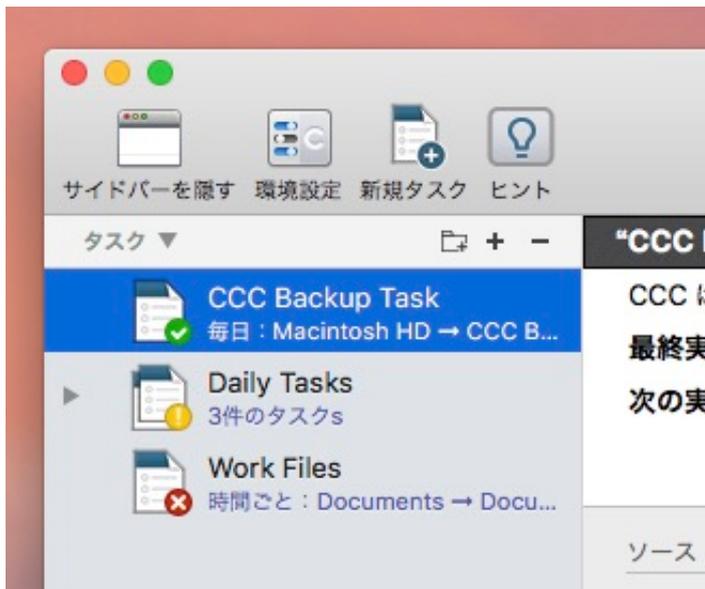
関連ドキュメント

- スケジュールしたバックアップを変更するには <<http://bombich.com/ja/ja/kb/ccc5/how-modify-scheduled-backup>>
- スケジュールしたタスクの実行条件を設定するには <<http://bombich.com/ja/ja/kb/ccc5/configuring-scheduled-task-runtime-conditions>>

スケジュールしたタスクを変更するには

タスクを選択します

変更したい **タスク** を選択します。必要であれば、**サイドバー**を表示をクリックしてスケジュール済みのタスクを表示してください。



スケジュールを変更

スケジュールアイコンをクリックします。

Carbon Copy Cloner

タスクを実行：

日単位

繰り返しの間隔： 1 日

開始時刻： 2017/ 6/20 午後 5:00

次の実行時刻： 今日 午後5:00:00 GMT-4

実行条件

別のタスクが同じ書き込み先に書き込まれている場合、延期

このタスクを実行する条件

今日が週末でなければスキップ

今日が週末であればスキップ

このタスクを実行する時間を制限

午後 7:00 から 午後 7:00

システムのスリープ状態

このタスクを実行しようスケジュールされている時にシステムがオフまたはスリープ状態の場合：

システムをスリープ解除する

ソースまたはコピー先が見つからない場合：

エラー通知を送信しない

みつからなかったボリュームが再度表示されたらすぐにこのタスクを実行

完了

コピーされます。

日単位で実行
毎日 午後5:00 時

メールを送信しない

スケジュールを変更し、完了をクリックしてください。

タスクを実行：

週単位 ▼

繰り返しの間隔： ▼ 週

開始時刻： ▼

曜日
 日曜
 月曜
 火曜
 水曜
 木曜
 金曜
 土曜

次の実行時刻： 明日 午前5:00:00 GMT-4

実行条件

別のタスクが同じ書き込み先に書き込まれている場合、延期

このタスクを実行する時間を制限

▼ から
 ▼

システムのスリープ状態

このタスクを実行しようスケジュールされている時にシステムがオフまたはスリープ状態の場合：

▼

ソースまたはコピー先が見つからない場合：

エラー通知を送信しない
 みつからなかったボリュームが再度表示されたらすぐにこのタスクを実行

?
完了

スケジュールを保存

保存をクリックします。

注意：タスク設定に加えた変更について気が変わった場合、**元に戻す**ボタンをクリックすると、タスクを最後に保存した設定に戻すことができます。

コピー先	スケジュール
 CCC Backup 223.67 GB 空き	 週単位で実行 第 2 週目の [日, 火, 木]
 SafetyNet 入	 メールを送信しない
変更及び削除されたファイルはコピー先の空き容量が許す限りキャッシュされ ます。	
<input type="button" value="元に戻す"/> <input type="button" value="保存"/>	

これで、新規スケジュールに従ってバックアップが実行されます！

CCCのメニューバーアプリケーションを使ってバックアップタスクをモニタリングするには

Carbon Copy Cloner メニューバーアプリケーション

CCCのメニューバーアプリケーションを使用すると、タスクに簡単にアクセスできるので、タスクのステータスを素早く判断したり、どのタスクが実行中かを確認したり、特定のタスクを開始、停止、延期したりできます。



実行中のタスクがありません



1件以上のタスクを実行中です



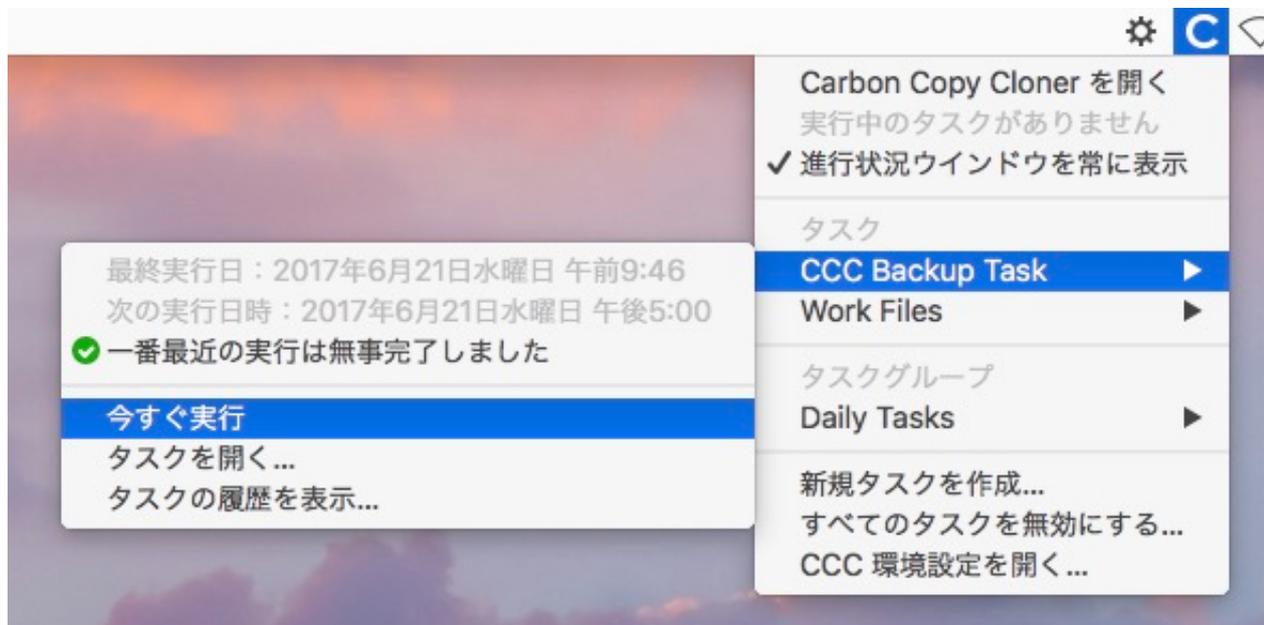
タスクの確認が必要です



すべてのタスクが中断されています

タスクを開始するには

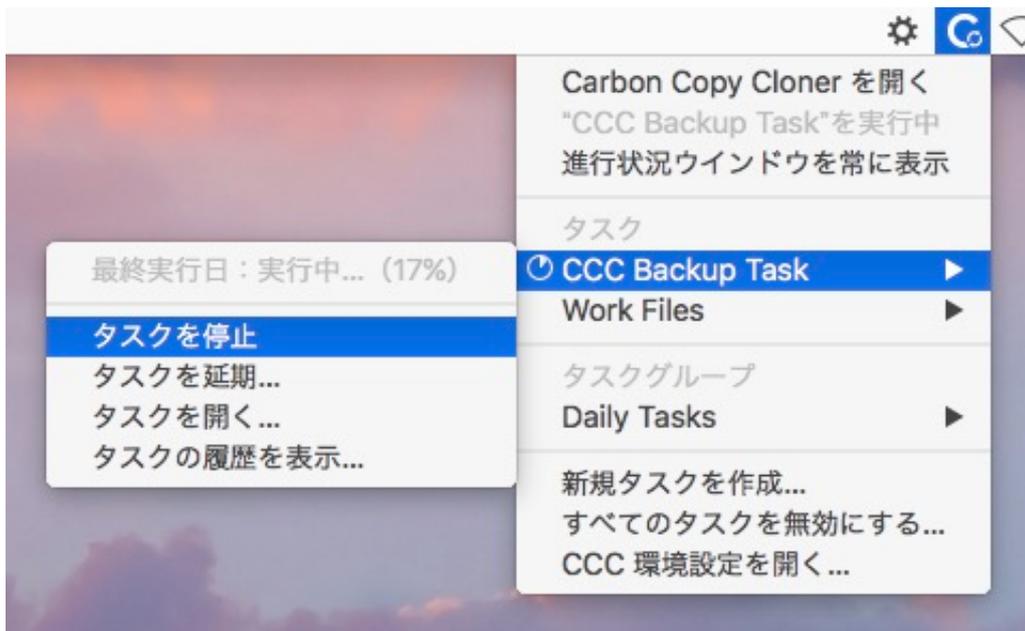
タスクのどれか1つをすぐに実行したい場合、Carbon Copy Clonerのメニューバーアプリケーションをクリックし、そのタスクのサブメニューから**今すぐ実行**を選択してください。



タスクを停止するには

時折、スケジュールしたタスクの1つが都合の悪い時に実行されることがあります。残業中？空港に急がなくてはいけない時？ Carbon Copy Clonerのメニューバーアプリケーションをクリックし、そのタスクのサブメニューから **タスクを停止**

を選択すると、タスクが即座に停止します。



タスクを延期するには

定期的スケジュールされているタスクが実行中にそのタスクを停止し、また近い将来に実行されるのを防ぎたい場合、Carbon Copy Clonerのメニューバーアプリケーションから“タスクを延期”を選択することができます。例えば、バケーションにラップトップを持って行ったとしましょう。しかし、バックアップディスクは念のため家に残して置くことにしたとします。その場合、バックアップボリュームが利用できませんという通知を日ごとや時間ごと送信されるのを避けるために、コピー先ディスクが確実に利用できるまでタスクを延期することができます。



タスクを中断するには

すべてのタスクを中断するには、Carbon Copy Clonerのメニューバーのアプリケーションメニューから**すべてのタスクを中断...**を選択してください。CCCは1時間から1週間の範囲で、中断する期間のリストと、タスクを無期限に中断するオプションを提供します。タスクをもう1度有効にし直すには、Carbon Copy Clonerのメニューバーアプリケーションから**タスクを再度有効にする**を選択するか、CCCを開いて提示があった時に再度有効にし直してください。

注意：個別のタスクを無効

にしたい場合は、タスクのサブメニューから**タスクを開く...**

を選択してください。CCCの中から無効にしたいタスクを右クリックして、タスクを無効にするオプションを選択してください。無効にされたタスクは、CCCのメニューバーアプリケーションのタスクリストに表示されませんので、ご注意ください。また、タスクを中断することとタスクを無効にすることは、別のことですので、注意してください。すべてのタスクを中断して、その後その中断を解除した場合も、それより前に個別に無効にしていたすべてのタスクは無効なままです。

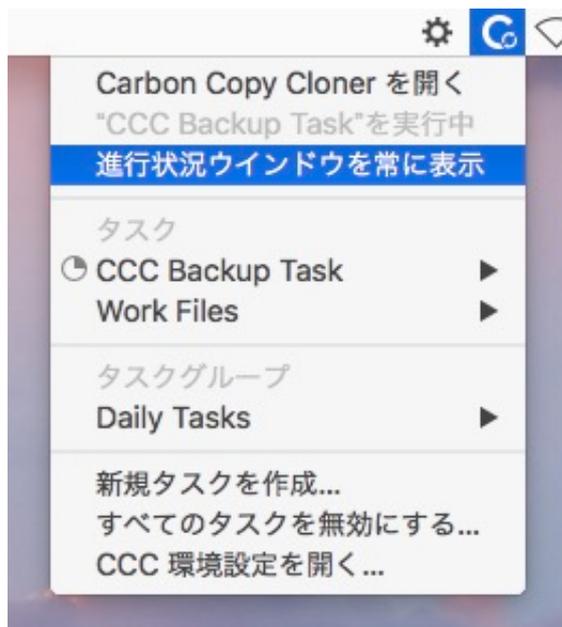


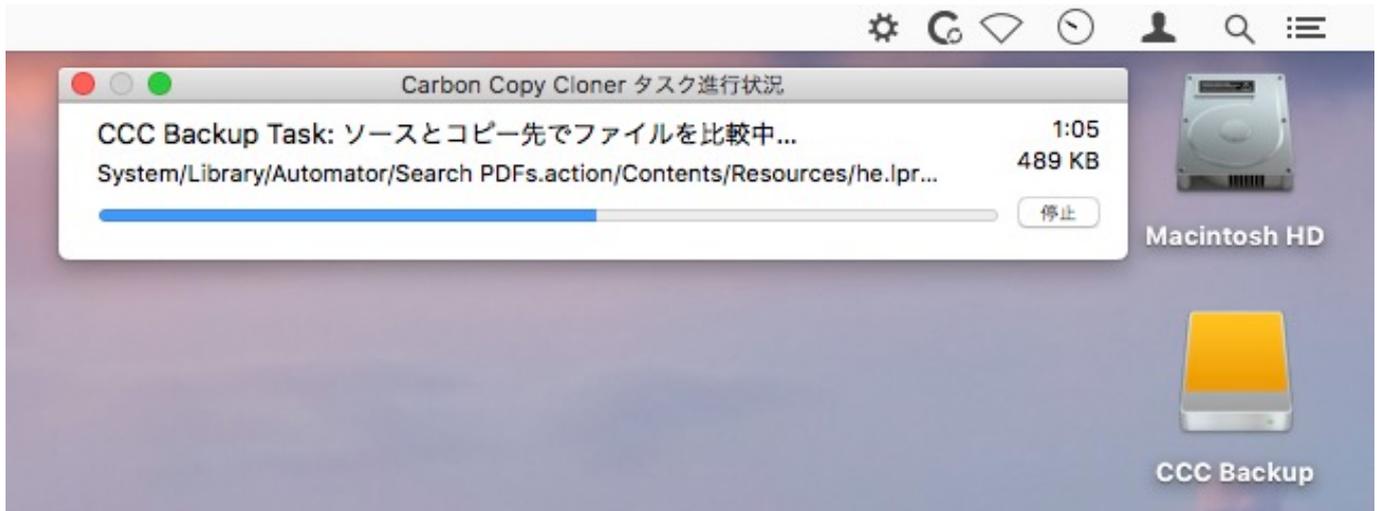
タスクの進行状況を表示するには

CCCのメニューバーアプリケーションには、タスクの進行状況を表示するミニサイズのウインドウがあります。このウインドウには、実行中のすべてのタスクの進行状況の詳細が表示され、実行中のタスクがない時には自動的に非表示になります。こ

のウインドウはデフォルトでは表示されないの

、表示するには常に**進行状況ウインドウを表示**を選択してください。





通知センター

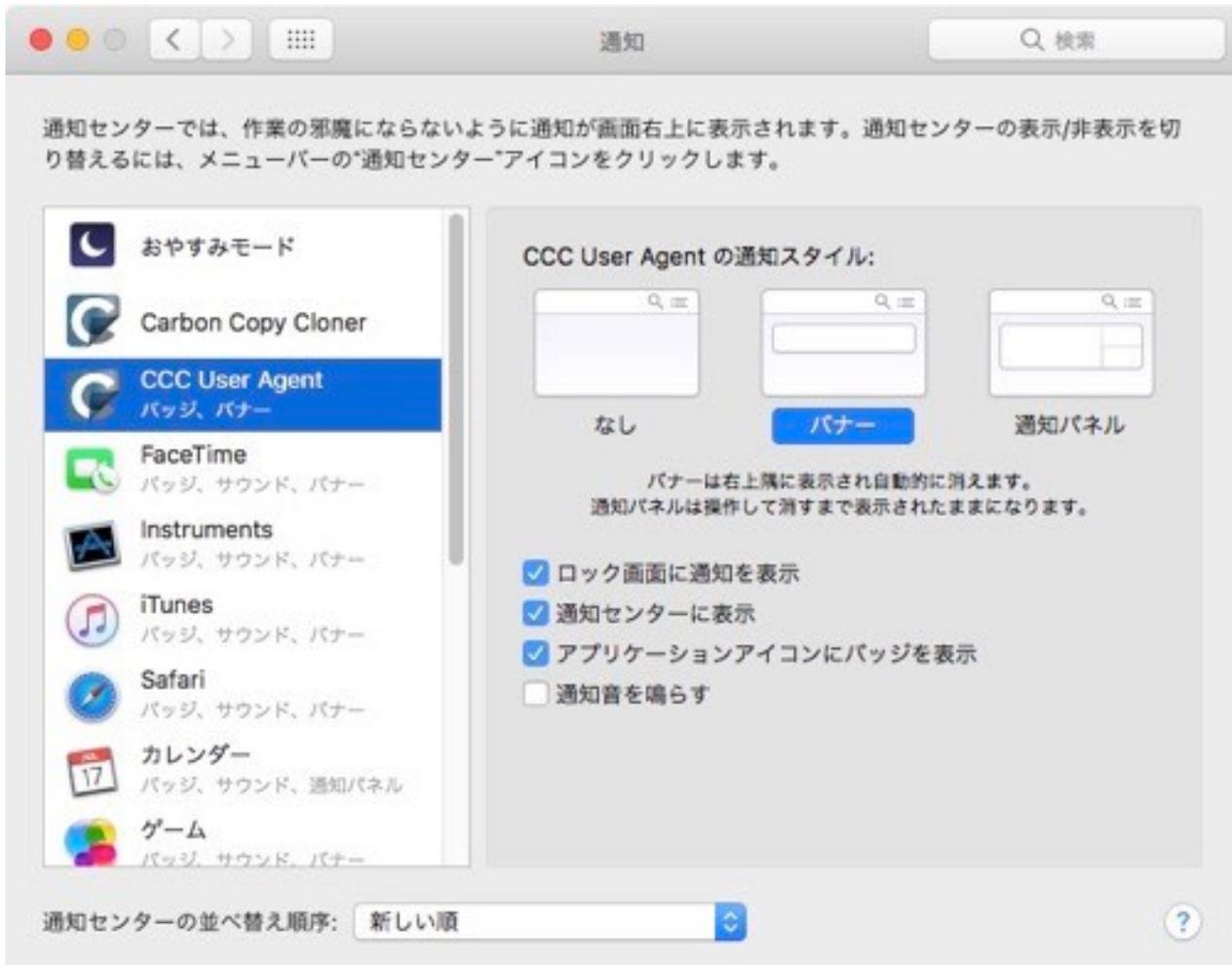
Carbon Copy Cloner は、バックアップタスクの開始と終了時、およびエラーが報告された場合に、macOSの通知センターに通知を送信します。これらの通知は、通知センターの CCC

ユーザエージェント

という名前のアプリケーションに表示されます。CCCの環境設定ウインドウの通知パネルには、タスク開始とタスク終了の通知を無効にするオプションが用意されています。また、エラーが起きた時にCCCのメニューバーアイコンを点滅させるオプションもあります。



macOSの通知センターからこれらの通知の管理方法と表示方法を設定するには、**システム環境設定**アプリケーションの**通知環境設定**パネルを開いて下さい。



古いバージョンのCCCでは、ソースまたはコピー先が見つからない、またはエラーが発生した場合、スケジュールされたタスクはダイアログボックスを表示していました。この設定はCCC 5のどこで見つかりますか？

CCC 5はこれらの通知を通知センターに送信するので、通知センターの環境設定パネルで指定された表示設定の対象となります。デフォルトでは、通知はバナーとして表示され、数秒後自動的に消えます。手動で消すまで画面に表示しておきたい場合は、CCC ユーザエージェントの通知を設定して、警告として表示することができます。

CCC ユーザエージェントを通知センターから削除するには

CCC ユーザエージェント (または、その意味で、すべてのサードパーティアプリケーション) を通知センターのリストから削除したい場合、単純に、通知センターのリストの中からアプリケーションを選択して、“削除”キーを押してください。

CCCユーザエージェントがログイン時に開始するように設定されていない場合、CCCの機能のいくつかは無効になります

CCCのメニューバーアプリケーションは“CCC ユーザエージェント”という名付けられ、CCCアプリケーションファイルの中にまとめられています。ユーザエージェントはCCCアイコンをメニューバーに配置しますが、CCCのバックグラウンドヘルプツールのための他のプロキシのような機能も提供します。以下の機能はCCCのユーザエージェントによって提供されています：

- タスク開始 と タスク終了 の通知

- タスクが完了した時に再起動、またはシステム終了する高度なオプション
- ソースまたはコピー先が再接続された時に実行するよう設定されたタスクに関して：
 - 先に進む前に確認する
 - タスクがしばらく実行されていない場合はリマインダーを送信

CCCのユーザエージェントをログイン時に開くように設定していない場合、上記の機能を確実に実行できません。その結果、それらの機能はユーザエージェントをログイン項目として設定するまで無効になります。CCCのユーザエージェントのログイン項目の設定は、CCCの“環境設定”ウインドウの“通知”からいつでも変更できます。

関連ドキュメント

- [CCCのメニューバーアプリケーションの環境設定を設定するには](#)
- [最後のバックアップがいつ実行されたかを確認するには：CCCタスク履歴](#)
<<http://bombich.com/ja/ja/kb/ccc5/how-find-out-when-backup-last-ran-ccc-task-history>>

メール通知を設定するには

CCCからタスクの結果をメールで受け取りたい場合、まず最初にCCCのメール設定からメール送信のアカウントを設定する必要があります。

1. Carbon Copy Cloner メニューから **環境設定** を選択します (または、ツールバーの **環境設定** ボタンをクリックします)。
2. 環境設定ウインドウのツールバーにある**メール設定**をクリックします。
3. **メールから送信**
のポップアップメニューの中から、メールから読み込まれたアカウントの1つを選択します。それから、詳細を確認してアカウント資格情報を提示されたフォームに入力してください。
4. アカウント情報を入力し終わったら、OK をクリックしてください。

高度なユーザの皆様へ：SMTPサーバがSSLを要求し、**自己署名**のセキュリティ証明書を使用する場合、**証明書チェーンを検証しない**のチェックボックスをチェックしてください。あるいは、サーバのセキュリティ証明書をキーチェーンアクセスアプリケーションの**システム** キーチェーンに追加し、明示的にその証明書を信頼することができます。



[オプション] メールの件名と本文テンプレートを変更する

CCCがタスクの完了を知らせるメールの件名と本文はカスタマイズすることができます。例えば、特定のメールがどのMacから送信されたか知りたい場合、メッセージの件名をカスタマイズできます：

ひろこのiMac: ##タスク名##: ##終了状況##

CCCがメール通知を送信する時、テンプレートの値（二重の#マークで内包された部分）はタスクの属性に置き換えられます：

例) ひろこのiMac : 毎日バックアップ : バックアップは正常に終了しました

利用可能なテンプレートの値の大部分は、既にデフォルトテンプレートに存在します。テンプレートの値を並び替えたり、その回りのテキストを変更したりできますが、二重の#マークで内包されたテキストを変更することはできません。テンプレートの値を追加したい場合：

1. テンプレートの値を配置したい場所、例えば、件名または本文のテキストフィールド、にカーソルを置きます。
2. ポップアップメニューの**テンプレートの値** からテンプレートの値を選択します。
3. **挿入** ボタンをクリックしてください。

件名と本文テンプレートに変更を加え終わったら、**変更を保存**

をクリックします。このテンプレートは、CCCから送信されるすべてのメール通知に使用されます。

追加したいテンプレートの値がありましたら、[こちらまでご連絡ください](http://bombich.com/ja/software/gethelp)

[<http://bombich.com/ja/software/gethelp>](http://bombich.com/ja/software/gethelp) !

テストメールを送信する

ウインドウの下にある **テストメールを送信...** をクリックします。テストメールの送信先のメールアドレスを入力してください。テストメールが送信されたというメッセージをCCCから受け取ったら、受信を確認して、タスク完了時に受け取りたい情報がテンプレートに含まれているか確認してください。

通知レベルを選択

環境設定ウインドウを閉じて、メール通知に追加したいタスクを選択してください。通知には3つのレベルがあります：

- メールを送信しない：CCCはタスク終了後にメールを送信しません。
- 実行されるごとに送信：問題なく完了した場合も、エラーが報告された場合も、タスクの最後にメールが送信されます。
- エラー時のみ送信：タスクを実行中、エラーが起きた時のみメールを送信します。

通知レベルを選択後、タスク完了後に通知を送信するメールアドレスを指定してください。複数のアドレスにメールを送信する場合は、アドレスをコンマで区切り、それぞれのアドレスを入力後、returnキーを押してください。受信者のテキストフィールドには、1度に1件のアドレスのみが表示されます。それぞれのアドレスを表示するには矢印キーを使用してください。

通知レベルと受信者の設定を完了したら、CCCのファイルメニューから **保存** を選択して、設定を保存してください。



App用パスワードを必要とするSMTPサービスを使ってメールを送信するには

CCCはバックグラウンドアプリケーションからメールを送信するので、おそらくログインされているユーザがまったくないとき、CCCは2ファクタ認証をサポートできません。多くのアプリケーションには同様のロジスティックな制約があるので、本来の目的でApp用パスワードを作成したという条件で、大抵のメールプロバイダはこれらのアプリケーションがSMTPサービスを使用することを許可します。例えば、GmailまたはiCloudアカウントを使ってメールを送信しようとした時、“ユーザ名およびパスワードが無効です”、または“認証できませんでした”というエラーに遭遇した場合、App用パスワードを作成することで問題を解決できます。

解決策:iCloudのためのApp用パスワードを作成する

Apple IDアカウントページに進み、CCC専用のApp用パスワードを作成してください:

1. [Apple ID アカウントページ](https://appleid.apple.com/account/home) <<https://appleid.apple.com/account/home>>にサインインします。
2. “セキュリティ”セクションから**App用パスワード**の見出しの下にある**パスワードを生成**...をクリックして、その手順に従ってください。
3. App用のパスワードをCCCの環境設定ウインドウのメール設定パネルにペーストしてください。
4. 注意: ユーザ名には必ず、@mac.com、@me.com、または、@icloud.comのメールアドレスを使用してください。

Appleの参照リンク: [App用パスワードを使う](https://support.apple.com/kb/HT6186) <<https://support.apple.com/kb/HT6186>>

解決策: YahooのためのApp用パスワードを作成する

アカウントセキュリティのページに進み、CCC専用のApp用パスワードを生成してください:

1. [アカウントのセキュリティページ](https://login.yahoo.com/account/personalinfo) <<https://login.yahoo.com/account/personalinfo>>に進みます。
2. ページ下の**アプリパスワードを生成**をクリックします。
3. **アプリを選択**をクリックし、**その他のアプリ**を選択してください。カスタム名として、“CCC”または“Carbon Copy Cloner”と入力します。
4. **一般**ボタンをクリックします。
5. アプリパスワードをコピーして、CCCの環境設定ウインドウの“メール設定”パネルにペーストしてください。注意: パスワードはコピーしてペースト

することをお勧めします。書き移す場合は、スペースが入らないように気をつけてください。パスワードは4つのグループで表記されていますが、実際にスペースはありません。ちょうど16文字あります。

解決策：Gmail専用のAppパスワードを作成する

App用パスワードのページに進み、CCC専用のApp用パスワードを生成してください：

1. **アプリパスワードページ** <<https://security.google.com/settings/security/apppasswords>>に進みます。
2. **アプリを選択** をクリックして**その他 (カスタム名)**を選びます。CCC または Carbon Copy Clonerと入力してください。
3. **一般** ボタンをクリックします。
4. App用のパスワードをCCCの環境設定ウインドウのメール設定パネルにペーストしてください。注意：パスワードは**コピーしてペースト**することをお勧めします。書き移す場合は、スペースが入らないように気をつけてください。パスワードは4つのグループで表記されていますが、実際にスペースはありません。ちょうど16文字あります。
5. 注意：ユーザ名には必ず、@gmail.com のメールアドレスを使用してください。G Suiteアカウントはサポートされていません。

Googleの参照リンク：[アプリパスワードでログイン <https://support.google.com/accounts/answer/185833>](https://support.google.com/accounts/answer/185833)

“ Gmail アカウントはCCCがメール通知を送信することを許可しません ”

Googleはサードパーティアプリケーションの開発者がGoogle Developer アカウントを入手してGoogle所有のAPIに登録することで、Gmail アカウントを使って特別な形式の認証 (OAuth2)を使用することができると強く主張しています。Googleの認証形式ではなく、業界標準の認証メカニズムを使用することを選択した開発者は、不当に“セキュリティに劣る”とみなされ、そのためデフォルトで、Googleはこれらのアプリケーションからの認証リクエストを否定します。さらに傷口に塩をすり込む様に、アプリケーションが業界標準の認証方式を使ってGmailに認証を試みると、リクエストを要求しているアプリケーションは“最新のセキュリティ標準を満たしていません”と言う主旨のメールがGoogleから送信されます。

CCCは絶対的に最新のセキュリティ標準を使用しています。特に、すべてのトラフィックをセキュリティ保護してSMTPサーバに送信するTLSを使用しています。TLSはメール通信をセキュリティ保護する最新のセキュリティ標準であり、そうあり続けています。Google所有の認証メカニズムのサポートを実行するために何日も費やすよりも、貴重な開発時間をCCCの機能向上のために使うことを優先します。それは、ユーザのデータを保護するための核となる機能です。

GmailアカウントはCCCにメールを送信することを許可しないと言うメッセージを受信した場合、以下の2つの選択を提案します：

- **Googleアカウントの2段階認証を有効にする** <<https://accounts.google.com/b/0/SmsAuthConfig>>。
それから [CCC用のアプリのパスワードを作成する](#) [第1に推奨する方法です]

— または —

- **Gmailアカウントの設定を変更** <<http://www.google.com/settings/security/lesssecureapps>>してGoogleを無効にします

あるいは、CCCの環境設定ウインドウのメール設定からGoogle以外のメールアカウントだけを指定することもできます。

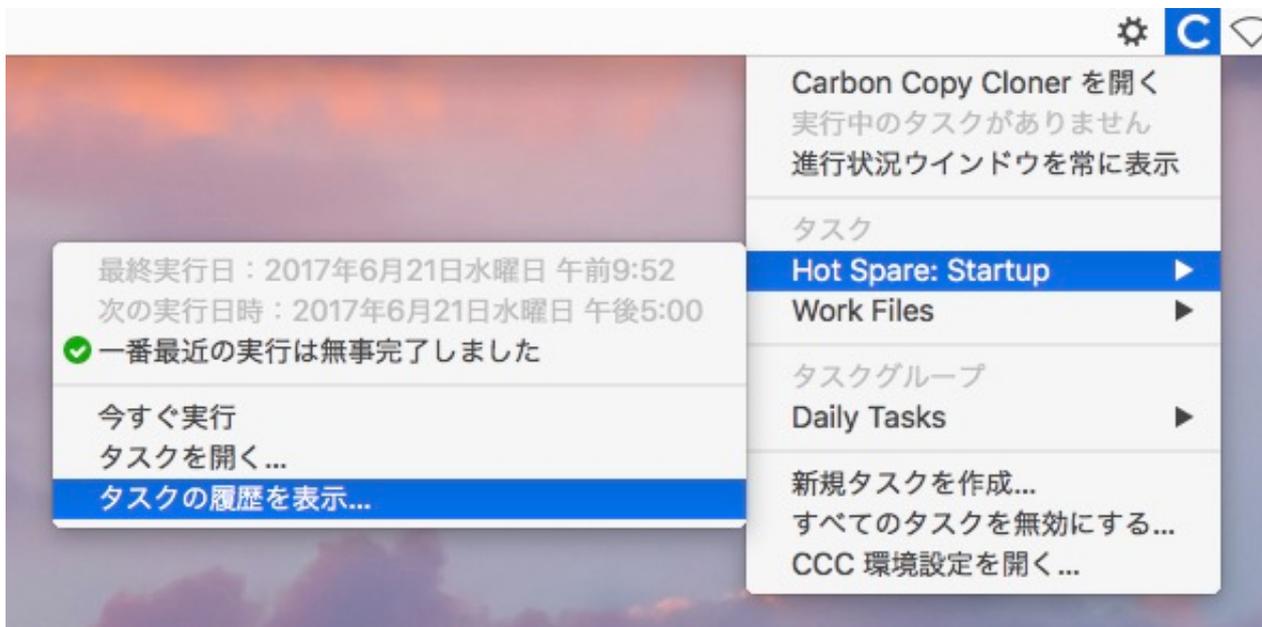
新しいiMacに移行後、SMTP資格情報をアップデートする

SMTP資格情報をCCCに提供すると、CCCはそれらを安全にmacOSキーチェーンファイルに保管します。そのキーチェーンファイルはいくつかの方法でセキュリティ保護されます。それらは、macOSシステム管理者によって

のみ読み込むことができる、CCCによってのみロック解除できる、元々作成されたMacでのみロック解除できる、です。結果として、新しいMacを購入してデータをその新しいMacに移行する場合、CCCのキーチェーンは新しいシステムでは動作しません。また、CCCがメールで通知を送信することはできません。新しいシステムに移行した後、CCCのメール設定を開いて、**編集...** ボタンをクリックしてから、SMTPアカウントの資格情報を再入力してください。

最後のバックアップがいつ実行されたかを確認するには：タスク履歴

最後のバックアップがいつ実行されたかを確認するには、メニューバーにあるCarbon Copy Clonerのアイコンをクリックし、調べたいタスクのサブメニューの上にマウスを移動します。それぞれのタスクのサブメニューはそのタスクが最後に実行された日時、そのステータス、および次の実行予定日時（該当する場合）を表示します。タスク履歴を表示...を選択してCCCを開き、これまでのタスクの実行の詳細を表示してください。



CCCがバックアップタスクを実行するたび、そのタスクの結果と統計情報が記録され、CCCのタスク履歴ウィンドウに表示されます。タスク履歴を表示するには、ツールバーの履歴ボタンをクリックするか、ウィンドウメニューの履歴

を選択してください。タスク履歴ウィンドウでは、タスクイベントをタスク名、ソース、コピー先、または開始時刻でフィルタして整理できます。CCCは最高1000件までのタスク履歴イベントを表示できます。それぞれのイベントはタスクの開始と終了日時、コピーされたデータ量とタスクの全般的なステータスを示します。ステータスインジケータのカラーは以下のように定義されています：

- グリーン：問題なくタスクが完了
- イエロー：タスクは完了しましたが、いくつかのファイルを転送中にエラーが起きました
- レッド：エラーが起きたため、タスクを完了できませんでした
- グレー：タスクがキャンセルされました

エラーが起きた場合、CCCは影響を受けたファイルをリストで表示します。CCCはコピーされたすべてのファイルリストを記録するわけではありません。

タスクの傾向

タスク履歴のウィンドウでタスクイベントを選択すると、下のパネルにある“情報”アイコンをクリックしてタスク設定と統計情報を含むポップオーバーを表示できます。これまでのそのタスクの統計情報を表すグラフが表示されます。キーボードの矢印キーを使うと、タスクイベントを時間を追って見ることができます。タスク設定のすべての変更内容は黄色で強調表示されます。



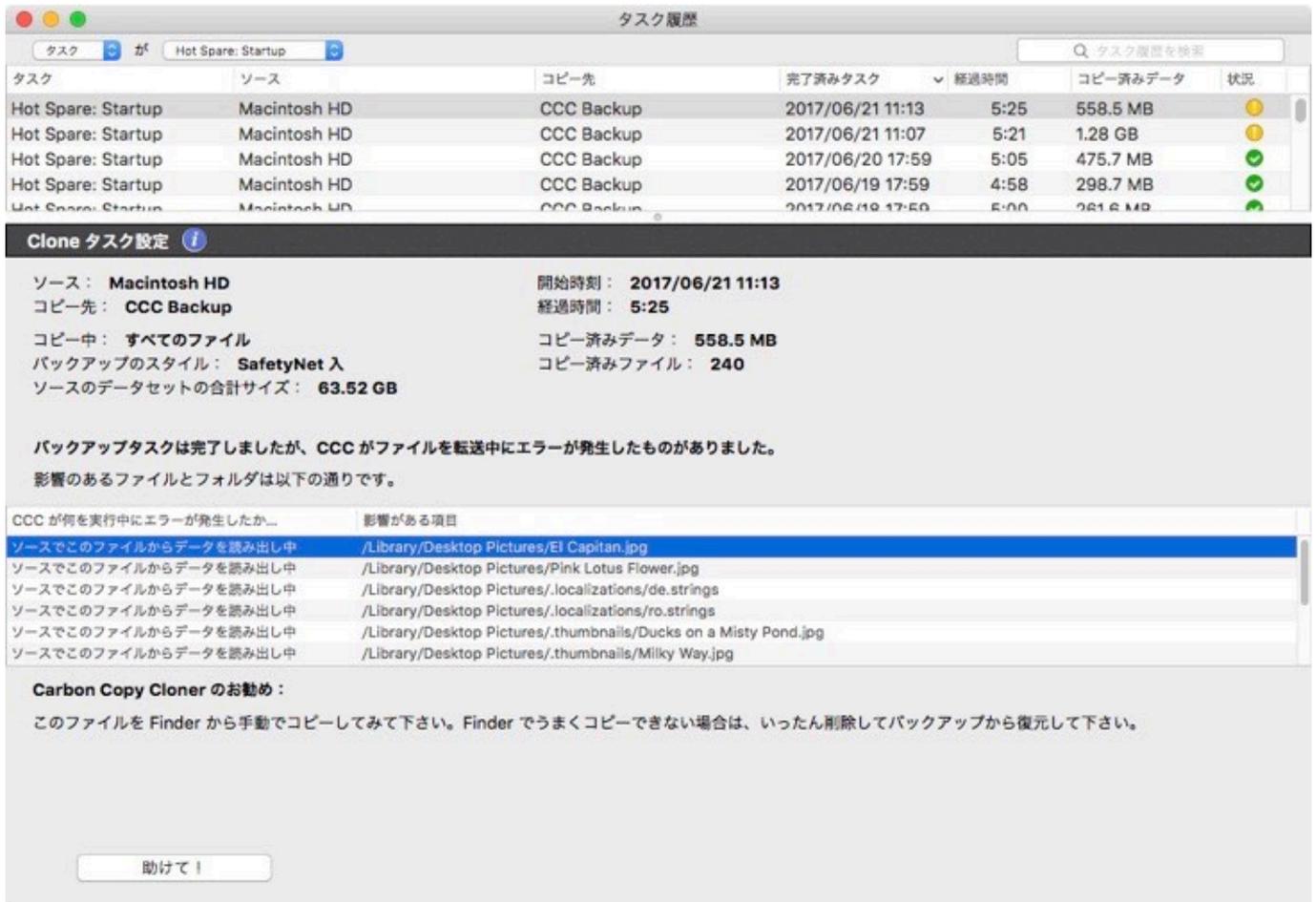
現在選択中のタスクはダークブルーの背景で表に表示されています。イベント

は、エラーで終了した場合は赤い背景で表示されます。何らかのエラーで終了したイベントが別の方法で完了した場合は、イエローの背景で表示されます。バックアップヘルスチェック

(“壊れているファイルを見つけて置き換える”)を使用したイベントはグリーンの背景で表示されます。時間の経過と共にタスク設定に加えられた変更を確認するためにトレンドチャートを閲覧するには、上下の矢印キーを使ってタスクイベントをスクロールしてください。

エラーの報告

Macのハードドライブに影響を与える可能性のあるハードウェアとファイルシステムの問題が数多くあります。ファイルシステムとメディアの損傷はよくあることで、そのエラーが起きるとCCCは専門的なアドバイスを提供します。CCCのタスク履歴ウィンドウは、バックアップタスクの全結果と発生したすべてのエラーの詳細を表示します。CCCはそれらのエラーを列挙し、共通する条件を分析し、わかりやすい言葉で問題を説明し、問題解決のための実用的なアドバイスを提供します。



The screenshot shows the Carbon Copy Cloner task history window. At the top, there's a search bar and a dropdown menu. Below is a table of tasks with columns for Task, Source, Destination, Completion Date, Duration, Data Copied, and Status. The first task, 'Hot Spare: Startup', is highlighted in blue and has a yellow status icon, indicating it failed. Below the table is a section titled 'Clone タスク設定' (Clone Task Settings) for the selected task, showing details like source, destination, backup style (SafetyNet), and data size. A message states that the backup task is complete but an error occurred during file transfer. Below this is a table listing affected files with columns for the error description and the affected item. The first item is '/Library/Desktop Pictures/El Capitan.jpg'. At the bottom, there's a 'Carbon Copy Cloner のお勧め' (Carbon Copy Cloner Recommendation) section with a '助けて!' (Help!) button.

タスク履歴ウインドウはより多くのイベントを一度に表示できるようにサイズ変更が可能です。イベントリストの下の分割線をドラッグすると、エラーメッセージのためのスペースを広げることができます。

影響を受けたファイルリストを書き出すには

エラーの一覧に影響を受けたファイルリストを保存したい場合、影響を受けた項目を選択 (または、Command+A を押して **すべてを選択**) してください。その後、CCCのファイルメニューから**コピー**を選択し (または Command + C)、項目リストをクリップボードにコピーしてください。すべてのエラーが同じではないことにご注意ください。ファイルリストを書き出すと、ファイルごとのコンテキスト情報は残りません。CCCのタスク履歴ウインドウに戻り、コンテキスト情報およびそれぞれのファイルに特定のアドバイスを入手してください。

よくあるエラーについてヘルプを得るには

エラーが起きると、CCCはエラーを分類し、トラブルシューティングのアドバイスを提供します。エラーによっては、CCCはタスク履歴ウインドウの下に役立つヒントのボタンを用意しています。それを使用すると、例えば、ディスクユーティリティに進み、Finderの壊れているファイルを明示します。それぞれのエラーをクリックして、CCCがお勧めするエラー解決法をご参照ください。行き詰まったり、問題に圧倒されたり、CCCのアドバイスで問題が解決しなかった場合には、“助けて!” ボタンをクリックして、問題の概要をBombich Softwareのヘルプデスクまで送信してください。

関連ドキュメント

- “ CCCのログファイルはどこにありますか。 ” <<http://bombich.com/ja/ja/kb/ccc5/where-can-i-find-cccs-log-file>>

CCCのタスク履歴ウインドウからイベントを削除できますか。

タスク

イベントを履

歴表から削除するには、タ

スクイベントを右クリックして、コンテキストメニュー

ーから **削除**

を選択すると、選択したイベントの記録を削除できます。タスク履歴のウインドウからタスクイベントを削除しても、バックアップには影響がありません。単にCCCのタスク履歴ウインドウからイベントを削除することに過ぎません。タスク履歴のイベントを削除するには管理者としてログインする必要があります。

CCC

のタスク

履歴をすべて消去

したい場合は、タスク履歴ウインド

ウを開き、CCCのファイルメニューから **タスク履歴を消去...**を選択してください。

既にコピー先ボリュームにあるデータを保護するには : Carbon Copy Cloner SafetyNet

名前が示す通り、SafetyNetとはコピー先で思いがけなくデータが喪失されるのを防ぐための **安全対策** です。

典型的なバックアップシナリオでは、起動ディスクのバックアップタスク専用のディスクがあり、バックアップディスクの内容がソースのコンテンツと正確に一致することが期待されています。しかし、多くの場合、大容量の3 TBディスクにスペースを見つけて、それを“オーバーフロー”した項目、例えば、大きなビデオファイル、古いもののアーカイブ、iMovieライブラリなど、に使用してしまいます。大容量のディスクをオーバーフローした項目で既に埋めてしまって、それをまたバックアップボリュームとして使用したいと望んでいるのなら、CCCのデフォルト設定が、バックアップディスクの他の項目を破壊することなく、あっという間にバックアップできるようデザインされているということが分かるでしょう。

CCCがコピー先にファイルをコピーすると、コピー先に既に存在するファイル、例えば、バックアップタスクの範囲にあるファイル、ソースに全くない項目などに何らかの影響を及ぼします。CCCはSafetyNetと呼ばれる機能を使用して、3つのカテゴリーに収まるファイルとフォルダを保護します：

- 前回のバックアップタスク以来変更された古いバージョンのファイル
- 前回のバックアップタスク以来ソースから削除されたファイル
- コピー先のルートレベルにしか存在しないファイルとフォルダ

SafetyNetのスナップショット

CCCのスナップショットサポートが有効なAPFSフォーマットされたコピー先ボリュームにバックアップをする場合、CCCのSafetyNet機能はスナップショット経由で実行されます。バックアップタスクの最初に、CCCはコピー先に **SafetyNetのスナップショット** を作成します。このスナップショットは、CCCがそれに変更を加える前のコピー先ボリュームの状態をキャプチャします。CCCがコピー先のアップデートに進む際、即座にファイルを削除して置き換えます (適用対象となる場合)。ファイルはSafetyNetのスナップショットとして保持されているので、スナップショットが削除されるまでそれらのファイルは完全に削除されることはありません。コピー先のルートレベルにしかない項目の保護は、以下に説明する通り、同じままです。

レガシーSafetyNetの動作 : SafetyNet オン

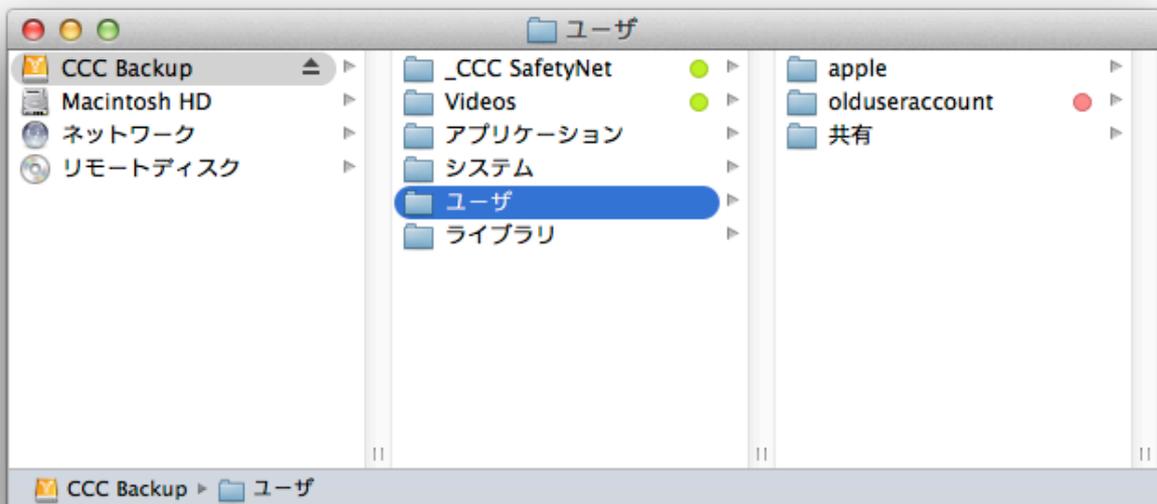
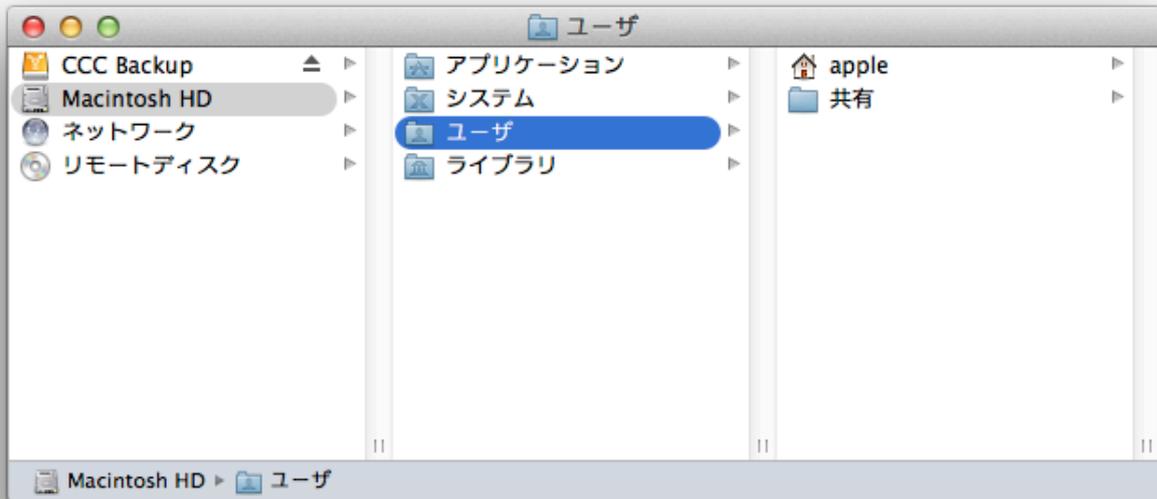
非APFSボリュームにバックアップする場合、またはAPFSのコピー先でスナップショットをオフにしている場合、CCCのSafetyNetはコピー先でフォルダとして実行されます。

Catalina: コピー先のCCC SafetyNetフォルダはどこにありますか？ <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet>>

SafetyNet オン

SafetyNetをオンにすると、CCCは変更された古いバージョン、および前回のバックアップ以来ソースから削除されたファイルをコピー先のルートにある **CCC SafetyNet フォルダ** に配置します。これが“SafetyNet”と呼ばれるのは、この機能がなければ、これらの項目は即座に削除されてしまうからです。SafetyNetは大惨事を防ぎます。CCCはコピー先からこれらの項目を即座に削除してしまう代わりに、項目をスペースが許す限りコピー先に保存しておきます。

3つ目のカテゴリーのファイルとフォルダは、SafetyNetがオンの時、コピー先に放置されます。コピー先のルートレベルにしか存在しないファイルとフォルダは完全に放置されるのです。これがどういう意味が分かりやすく説明しますので、以下の2つのFinderウィンドウを思い浮かべてください：



最初のウィンドウには、通常のアプリケーション、ライブラリ、システム、ユーザフォルダと共に、起動ディスクの内容が表示されています。2番目のウィンドウには、コピー先ボリュームの内容が表示されています。コピー先ボリュームの“ルート”は2番目のウィンドウに表示されています。コピー先ボリュームのルートレベルにはそこにしか存在しない2つの項目があります。“CCC SafetyNet”と“ビデオ”です。もしCCCがこのボリュームをSafetyNetをオンにした状態でアップデートした場合、これらのフォルダは両方ともスクリーンショットで緑にタグ付けされ、CCCに放置されます。しかし、ユーザフォルダはコピー先にしか存在しないわけではありません。つまりソースとコピー先の両方に存在します。結果として、ユーザフォルダの中にある“olduseraccount”(古いユーザアカウント)フォルダはそのまま**放置されない**で、_CCC SafetyNetフォルダに移動します。

コピー先のルートレベルにある項目を保護するには

SafetyNetをオン

の設定には、選択中のコピー先のルートに存在する項目を保護するオプションが含まれています。この機能は、コピー先のルートにのみ存在する項目にかなる変更も加えられないようにデザインされています。上記の例を再び参照すると、例えば、**ビデオ**という名前のフォルダが CCC

バックアップという名前のボリュームにあるとしましょう。CCCの**バックアップ**

ボリューム

をタスクのコピー先と

して選択し、SafetyNetをオンにしたままにし

ておくと、CCCはその**ビデオ**フォルダをその場所に残し、削除することも CCC SafetyNet

フォルダに移動することはありません。

コピー先の“ルート”とは**選択中の**コピー先に対して最初の、または一番上のフォルダを指します。CCC

バックアップ

という名前のボリュームをコピー先として選択した場合、ルートレベルはそのボリュームのルートを指し、そのボリュームをFinderで開いたときにはそれが表示されます(上のスクリーンショットの真ん中のパネルがそうです)。

フォルダをタスクのコピー先として選択する場合、“コピー先のルートにある項目”とは、コピー先として選択した特定のフォルダにある項目を指しています。ボリューム全体のルートのことではありません。フォルダをコピー先として選択すると、そのフォルダの外にあるものはすべて、完全にバックアップタスクの領域外になり、その特定のバックアップタスクから除外されます。

コピー先でルートレベルの項目を保護の設定はSafetyNet 機能に必須ではありません。SafetyNetはオンのままにしておきたいが、ソースからすでに削除された項目をコピー先のルートから削除するようにCCCを設定しておきたい場合、“詳細設定”のボタンをクリックしてから、

コピー先でルートレベルの項目を保護の設定のチェックを外してください。

SafetyNet フォルダのサイズを制限するには

CCCバックアップでSafetyNet機能がオンの時、CCCはコピー先ボリュームの空き容量が 25GB

以下になると、自動的にSafetyNet フォルダの内容を削除するようデフォルト設定されています。CCCは必要に応じて削除制限を自動的に調整します。例えば、25GB以上をコピーするバックアップタスクがある場合、CCCは追加の削除を実行し、削除制限を増大します。

一般的にCCCの削除の動作を調整する必要はありませんが、“高度な設定”からそれぞれのタスクの削除設定をカスタマイズできます。CCCはSafetyNetフォルダのサイズ、SafetyNetフォルダの項目の古さ、およびコピー先の空き容量を元にして削除を提案します。

SafetyNetの空き領域の削除制限の自動調整について

自動調整のオプションが有効になっている場合(デフォルトで有効になっています)、バックアップタスク中コピー先に空き領域が不足してくると、CCCは自動的に空き領域の削除制限を増加します。例えば、削除制限がデフォルトの25GBに設定されていて、バックアップタスクの開始に25GBの空き領域がある場合、タスクの開始時に削除は実行されません。しかし、そのタスクが進むうちに25GB以上のデータをコピーする場合、コピー先はいっぱいになります。その場合、CCCは現在のタスクでコピーされたデータ量か、CCCがコピーしようとしている最後のファイルに必要なデータ量のどちらか大きい方で削除制限を増加します。例えば、CCCが25GBのデータをコピーした場合、削除制限は25GBに増加します。しかし、CCCが40GBのファイルをコピーしたい場合、CCCはそのファイルの25GBを無駄にコピーするのではなく、むしろ、削除制限を即座に40GBに増加して、削除をしてから、タスクを再開します。

最後に、自動調整された値が希望するよりも高い設定になっている場合は、削除制限を手動で変更することもできます。自動調整機能は、SafetyNetの削除をより寛大で詳細すぎないようにデザインされていますが、いつでもより低い値に削除制限をリセットすることができます。

SafetyNet オフ

コピー先を常にソースと一致させておきたい、そして、前回のバックアップ以降変更されたファイルの古いバージョン、またはコピー先から削除されたファイルを残しておく必要がない場合、コピー先セクタの下にある大きなスイッチアイコンを使って、CCCの SafetyNetをオフに設定できます。CCCの SafetyNet機能がオフになると、変更が加えられたファイルの古いバージョンは、アップデートで置き換えられたファイルが問題なくコピー先にコピーされると、削除されます。コピー先のみ存在するファイルは完全に削除されます。コピー先にしか存在しないファイルとフォルダに、削除から免れる特別な保護が与えられることはありません。**この動作の唯一の例外は、CCC SafetyNet フォルダです。CCCはこのフォルダは削除しません。** 前回のタスク実行時に SafetyNet 機能がオンであったため CCC SafetyNet フォルダが作成された場合、その SafetyNet フォルダをゴミ箱にドラッグして捨てることができます。

コピー先のルートレベルの項目を保護

CCCの SafetyNetにはコピー先ボリュームのルートレベルにしかない項目を保護するための重要な機能が含まれています (上記の “ SafetyNet 入 ” の説明を参照してください)。 SafetyNetのポップアップメニューから SafetyNet 切 を選択している時には、**コピー先のルートレベルの項目を保護** の設定が無効になります。 SafetyNetを無効にしたままその設定を使用したい場合は、 **詳細設定** のボタンをクリックして、そのオプションの横のボックスをチェックしてください。

何も削除しない

この設定を使うと、CCCはコピー先から何も削除しません。ファイルがソースではなくコピー先に存在する場合、そのファイルはコピー先にそのまま残ります。CCCがコピー先でファイルをアップデートしている場合、古いバージョンのファイルが CCCの SafetyNetフォルダに移動されます。この設定はソースフォルダとボリュームが素晴らしく整理されている場合に便利です。例えば、プロジェクト名で写真を保管していて、プロジェクトが完了した時に、それらのプロジェクトを全体としてソースから削除したい場合、それらのアーカイブされたプロジェクトがコピー先から削除されるのを避けるために**何も削除しない**の SafetyNet設定を使用できます。

この設定を使用するに当たって1つ注意すべき点：古いファイルはコピー先で累積され、ソースで消費されているよりも多くのスペースを消費します。また、ファイルがうまく整理されていないと、ソースから削除したもののすべてがまだバックアップに残るので、将来の復元が非常に面倒になります。

“ コピー先で項目を置き換えている間にエラーが起きました ”

SafetyNet設定で **何も削除しない** を使用している場合、CCCはコピー先に異なるタイプをもつ項目を置き換えることができません。例えば、エイリアスのあるフォルダを置き換える場合、CCCはエイリアスのファイルをコピーできず、その代わりにエラーが発生します。コピー先から問題の項目を手動で削除するか、または SafetyNet設定の中の他の1つを選択すると、CCCは置き換えを実行することができます。

バックアップボリュームのデータを保護するその他の方法

バックアップボリュームにのみ存在するファイルを移動または削除されたくない場合 (例えば、ファイルがソースデータセットの一部である場合など)、そのデータを保護する方法がもう2つあります。

新しいパーティションをコピー先ハードドライブに追加する

ディスクユーティリティを使用して、既存の HFS+ フォーマットされたボリュームのサイズの変更、および新しいパーティションを APFS コンテナに追加することができます。これらの操作は非破壊的に、つまり、ファイルやフォルダが既存のどのボリュームにあっても消去されることなく、実行することができます。

フォルダにバックアップする

CCCを使って、データをコピー先ボリュームのサブフォルダにバックアップすることができます。コピー先ボリュームのサブフォルダにバックアップすると、CCCのコピーと削除の判断は完全にサブフォルダの範囲で行われます。つまり、サブフォルダの外にある内容はバックアップタスクによって考慮に入れられることも影響を受けることはありません。フォルダをバックアップするには、CCCのコピー先セレクトから “フォルダを選択...” を選択してください。

“その他”のデータをバックアップボリュームに残しておく一般的な考え方

取り替えることができない大切なデータのバックアップタスクには、それ専用のボリュームを確保されることを強くお勧めします。

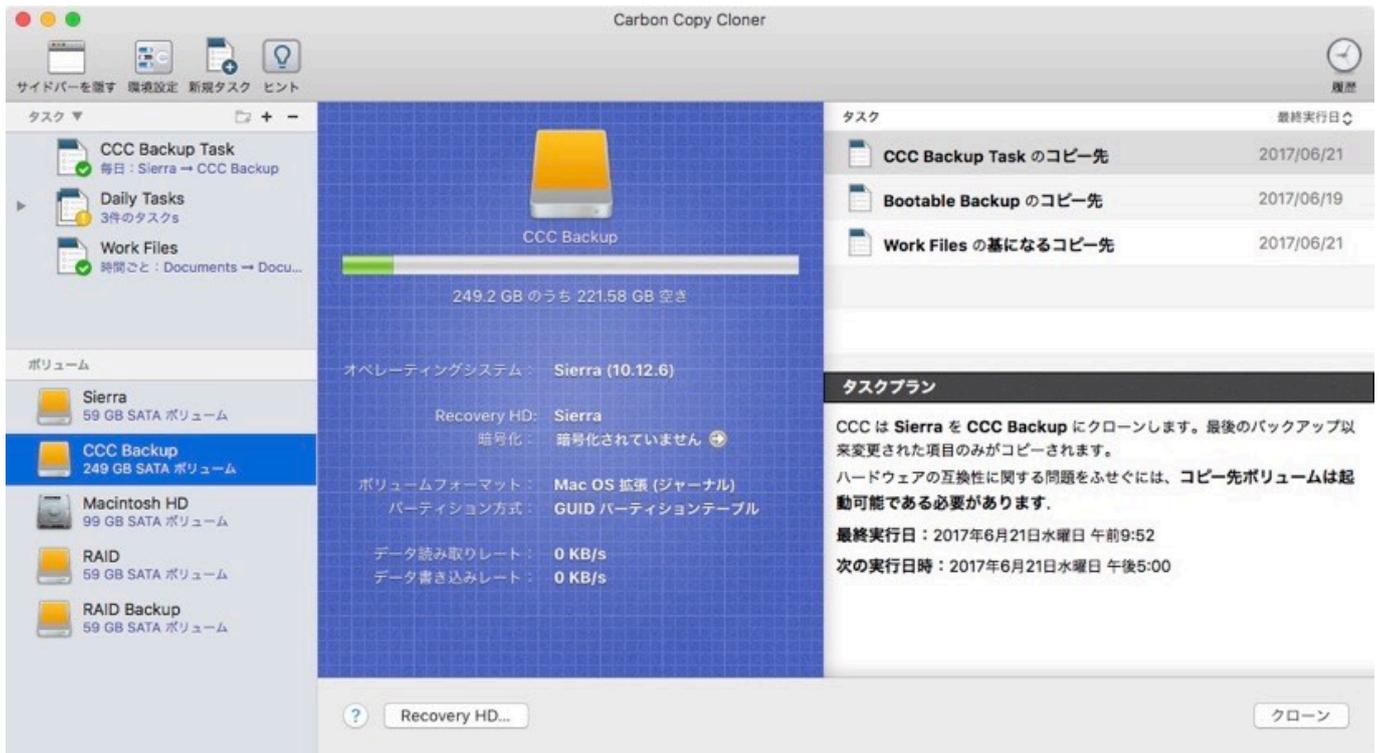
他のどこにも存在しないバックアップボリュームにデータがある場合、それはバックアップされていません！Carbon Copy Clonerとの使用にボリュームを対象とする場合、何らかの正当な理由でいくつかのファイルが削除されてしまうリスクが常に伴います。CCCはデータが喪失されることから保護するためのオプションや警告を提供します。しかし、CCCの誤った使用や、提供される機能を誤って理解したことで起きるデータの喪失を防ぐことはできません。

関連ドキュメント

- Carbon Copy ClonerのSafetyNetについてのよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet>>
- APFSボリュームでスナップショットを活用する <<http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes>>

ディスクセンター

CCCのディスクセンターは、Macにマウントされているローカル接続されたボリュームについての一般的なボリューム情報を表示します。また、これらのボリュームの読み込みと書き出しの速さ、エラーの統計情報も表示されます。CCCのサイドバーからボリュームを選択して（サイドバーが隠れている時はツールバーで“サイドバーを表示”をクリックしてください）、そのボリュームをディスクセンターに表示してください。また、CCCは選択したボリュームに関連するバックアップタスクも表示します。選択したタスクを実行するには“クローン”をクリック、編集するにはタスクをダブルクリックしてください。



基本的なボリューム情報

サイドバーにあるディスクセンターの表は、ローカル接続の、マウント済みボリュームのリストを表示しています。これらのボリュームの1つをクリックすると、ボリューム名、ファイルシステム、容量、ディスクの使用状況、およびそのボリュームに関連するRecovery HDについての情報など（適用される場合）が表示されます。ディスクの使用状況の上にレベルインジケータが表示されています。ディスクの使用量がボリューム容量の70%を超えると、レベルインジケータが黄色に変わり、“大掃除”をする時期であることを示します。ディスクの使用量がボリューム容量の90%を超えると、レベルインジケータが赤色に変わります。特にmacOSのインストールを含むボリュームは、最低10%を空き領域として維持しておくことをお勧めします。起動ディスクがいっぱいになると、macOSの一般的なパフォーマンスが低下し始めます。

APFSボリュームの使用状況インジケータ

CCCのサイドバーでAPFSフォーマットされたボリュームを選択すると、ボリュームの使用状況のインジケータがいくつかの異なるカラーを表示することがあります。緑、黄色、赤は上記と同じ意味です。これらのカラーにはそれぞれ薄い色があり、スナップショットにより消費されているディスク使用量の割合を示しています（これはスナップショットが選択中のボリュームに存在する時のみ適用されます）。薄いグレーは空き容量を示します。濃いグレーは同じAPFSコンテナ内の他のAPFSボリュームが消費しているディスク使用量を示します（ディスクユーティリティに示された“その他のボリューム”と同じです）。

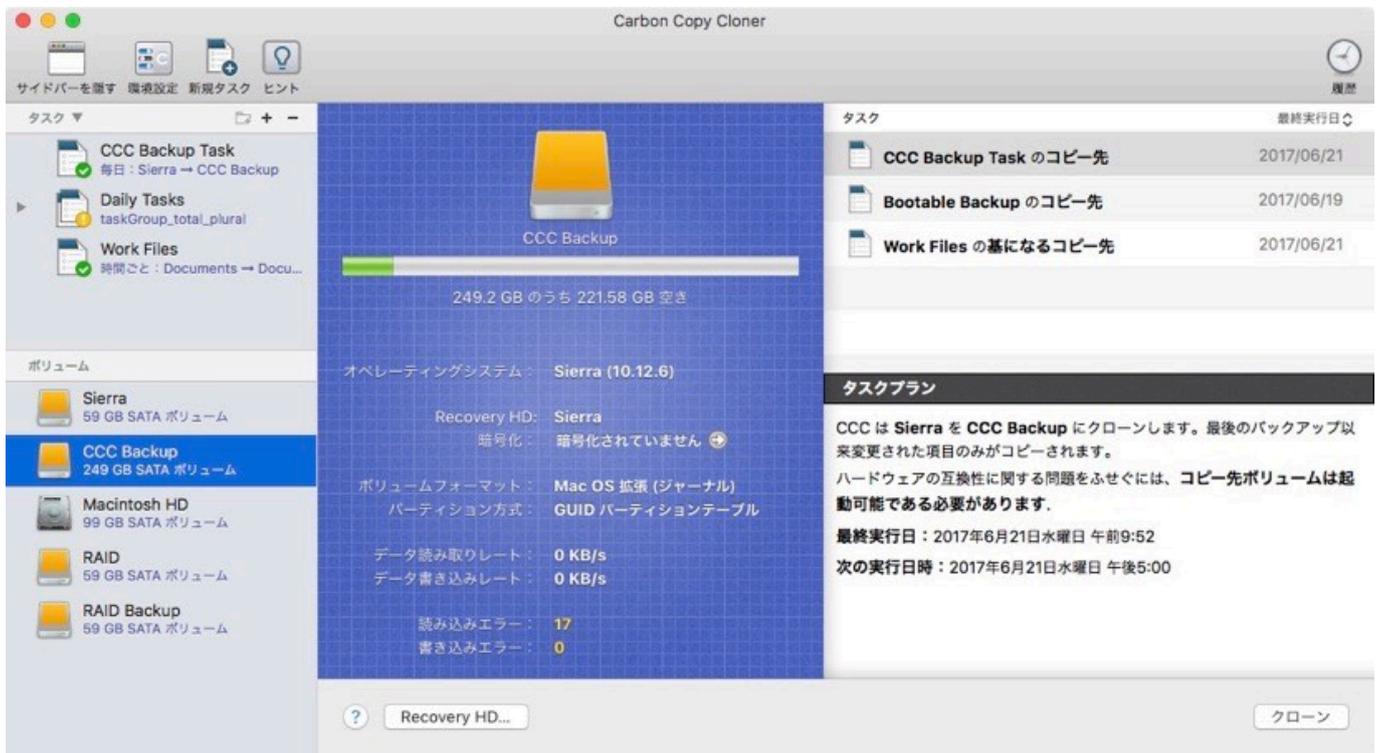
ドライブの統計情報

ディスクセンターは1秒間隔でディスクアクティビティの統計情報をアップデートします。ディスクアクティビティはハードドライブのインタフェースでmacOSにより収集されますので、同じディスクに常駐する複数のボリュームのデータは同一です。データの読み込みや書き出しの速さから、macOSがどれほどの速さでディスクから（またはディスクに）データを読み込んだり、書き出しているかを判断できます。これらの値はバックアップタスクの途中で大幅に変動することに気付くことでしょう。これは極めて普通のことです。書き出しのパフォーマンスは一般的に、多くの小さなファイルをコピーする時は遅くなり、大きなファイルを1つだけコピーする時は速くなります。小さなファイルを数多くコピーしている時には、ソースとコピー先ボリュームで、多くのシークアクティビティが起きています。このシークの動作は、ディスクの理論的なスループットに比べて、全体的なスループットを極端に低下させます。

バックアップタスクが特に遅いと思われる場合は、タスクを停止して、ベースラインディスクアクティビティが何であるかを確認してください。かなりの量のアクティビティがある場合は、アクティビティモニターアプリケーションを使用して、どのアプリケーションがディスクのリソースを過大に使用しているか判断してください。

ディスクエラーの統計情報

読み取りおよび書き出しエラーの統計情報が存在する時、CCCから報告があります：



The screenshot shows the Carbon Copy Cloner interface. The main window displays the 'CCC Backup' task with a progress bar and storage information: '249.2 GBのうち 221.58 GB 空き'. Below this, system details are shown: 'オペレーティングシステム: Sierra (10.12.6)', 'Recovery HD: Sierra', 'ボリュームフォーマット: Mac OS 拡張 (ジャーナル)', and 'パーティション方式: GUID パーティションテーブル'. At the bottom, error statistics are listed: '読み込みエラー: 17' and '書き込みエラー: 0'. On the right, a 'タスク' (Tasks) list shows recent backup runs for 'CCC Backup Task', 'Bootable Backup', and 'Work Files'. A 'タスクプラン' (Task Plan) section provides instructions and execution times for the current task.

読み取り、書き出しエラーは、ディスクがMacに接続されて以降、完了できなかった読み取り、書き出しの試みの件数を示します。壊れたセクターに常駐しているファイルがディスクのファームウェアに自動的に削除されない場合、読み取りエラーがしばしば発生します。このようなファイルはCCCも読み取ることができないので、これらのファイルを読み込めませんでしたという報告がバックアップタスクの最後にCCCから送信されます。読み取りエラーは必ずしもハードドライブのエラーを示唆するものではありません。例えば、この数字は、同一の壊れたファイルの読み取りを複数回試みた場合、確実に上昇します。しかし、一般的に読み取りエラーはバックアップタスクのパフォーマンスを低下させる物理的なハードウェアの問題に関係しています。macOSが読み取りエラーを上手く処理せず、ディスクにアクセスを試みると、システム全体の機能停止につながる場合もあります。

書き出しエラーはより深刻です。書き出しエラーを報告するディスクがある場合、デバイスのハードウェア設定に問題があるか(例：不良なケーブル、ポート、



エンクロージャーなど)、そのディスク自体に問題があると考えられます。

スナップショットの管理

APFSフォーマットされたボリュームが選択されると、CCCはボリュームのスナップショットのリストと、そのボリュームのために設定さ

れたスナップショットの保持に関するポリシーが

表示されます。スナップショットの管理に関する詳しい情報はこちらから

<http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes>。

ディスクユーティリティと [他のサードパーティユーティリティ] からはこのディスクの問題が報告されません。なぜCCCからは報告があるのですか？

読み取り、書き出しエラーの統計情報は低いレベルのストレージドライバーに保管されていて、ボリュームに特有のものではありません。通常読み取りエラーが生じる時、ハードドライブのファームウェアは影響を受けた部分のデータをディスクの別の部分に移動を試みてから、破損した部分をスペアします。それが成功すると、ストレージドライバーの統計情報は最新ではないという可能性が生まれます。

これらの統計情報は、影響を受けたディスクが物理的にMacから接続解除されるか、再起動された時、リセットされます。

関連ドキュメント

- ハードウェア関連の問題を識別してトラブルシューティング <http://bombich.com/ja/ja/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems>
- “メディアエラー”のトラブルシューティング <http://bombich.com/ja/ja/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems#ioerrors>
- AppleのRecovery HDパーティションをクローンするには <http://bombich.com/ja/ja/kb/ccc5/cloning-apples-recovery-hd-partition>
- FileVault暗号化で作業するには <http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption>

Appleの Recovery HDパーティションをクローンするには

このチュートリアルビデオをYouTubeでご覧ください <<https://www.youtube.com/watch?v=6q9xeUjtx8>>

macOSインストーラは“ Recovery HD ” という名前の起動ディスクに隠れたボリュームを作成します。Recovery HD ボリュームの主な目的は、macOSを再インストールする方法を提供することです。macOSボリュームのバックアップを実行時、Carbon Copy Clonerはソースボリュームに関連するRecovery HDボリュームを自動的にアーカイブします。このアーカイブは後で別のRecovery HDボリュームに復元することができます。CCCのディスクセンターは、新規のRecovery HDボリュームをAppleのレガシーファイルシステム、HFS+ <<http://bombich.com/ja/ja/kb/ccc5/glossary-terms#h>> でフォーマットされたボリュームに作成する機能も提供します。

CCCはAPFSフォーマットされたコピー先の特別な“ヘルパー”ボリュームを自動的に管理します

CCCはPrebootおよびRecoveryヘルパーボリュームをAPFSフォーマットされたコピー先ボリュームに作成してアップデートします。以下に説明されているRecovery HDをクローンするタスクは、APFSフォーマットされたコピー先には適用されません。CCCは追加の手順を必要とすることなく、あなたに代わってこれらすべてを代行します。これらのボリュームはディスクユーティリティには表示されませんので、ご注意ください。

起動マネージャーにRecoveryボリュームが表示されないのはどうしてですか？

起動マネージャーはAPFSのRecoveryボリュームを表示しません。Appleはsのインターフェースにそれらを表示しないことを決めました。代わりに、起動時に、“Command+R” (Intel Macの場合) を押すか、パワーボタンを押し続ける (AppleシリコンMacの場合)と、リカバリーモードに起動できます。

通常、バックアップディスクでリカバリーモードに起動することはありませ

で、注意してください。

バックアップから復元したい場合には、Recoveryボリュームではなく、[バックアップから起動](http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup) <<http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup>>します。

バックアップディスクにRecovery HD ボリュームを作成するには？

注意：macOSはRecoveryボリュームへのアクセスを制限します。CCCのRecoveryボリュームを作成または変更するには管理者ユーザとしてログインする必要があります。

以下のシンプルな手順に従ってください：

1. CCCを使用して、起動ディスク（またはmacOSのインストールを含む他のソースボリューム）をバックアップボリュームにクローンします
2. CCCのサイドバーにある**ボリューム**からバックアップボリュームを選択します（CCCのサイドバーを表示するには、CCCのツールバーから**サイドバーを表示**をクリックしてください）
3. ウィンドウの下にある Recovery HD... をクリックします
4. Recovery HD **を作成** ボタンをクリックしてください



新規Recovery HDボリュームを作成するには

注意: Drobo デバイスはダイナミックボリュームのサイズ変更をサポートしませんので ([参照 <http://www.drobo.com/support/updates/firmware/ReleaseNotesFirmwareB800iElite2.0.4.pdf>](http://www.drobo.com/support/updates/firmware/ReleaseNotesFirmwareB800iElite2.0.4.pdf))、Recovery HDボリュームを承認できません。Recovery HDボリュームをDroboデバイスで作成しようとしないでください。

注意: RecoveryボリュームをFusionまたはRAIDボリュームで作成することはできません。Recoveryボリュームをこれらのデバイスで作成する場合、これらの“仮想”ボリュームの作成前に完了する必要があります。詳細は [こちらのCCC Kbase記事 <http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition#fusion>](http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition#fusion) をご参照ください。

Recovery HDボリュームは約 650MBです。新規 Recovery HDボリュームを作成するには、最低 1GBの空き容量があるディスク上のボリュームを選択する必要があります。ドキュメントでは、この選択されたディスクを“ドナー”ディスクと呼んでいます。ドナーディスクでデータに危害が及ぼされることはありません。新規Recovery HDボリュームに空き容量が割り当てられるように、サイズが変更されるだけです。ボタンをクリックして新規Recovery HDボリュームを作成する時、以下の動作が実行されます:

1. ドナーディスクをマウント解除
2. ディスクユーティリティの“ディスクを検証”ツールと同等の動作を実行
3. ドナーボリュームを1GBにサイズ変更
4. 借りた容量1GBを使って、Recovery HD という名前の新規ボリュームを作成
5. 適切なRecovery HD をRecovery HD
ボリュームのアーカイブまたは別のディスク（起動ディスクなど）から新たに作成されたRecovery HD
ボリュームにクローン
6. ドナーボリュームをマウント解除

タスクが完了すると、Recovery HDボリュームはデスクトップにマウントされなくなります。また、ディスクユーティリティに表示されることもなくなります。このRecovery HDボリュームの機能を確認するには、起動時にOptionキーを押したままにしてRecovery HDボリュームを起動ディスクとして選択してください。

注意：Recovery HDのクローンタスクをラップトップで実行する際、タスクが完了するまでMacがAC電源に接続されていることを確認してください。

既存のRecovery HDボリュームをクローンし直すには

関連するRecovery HDボリュームが既に存在するボリュームを選択した場合、CCCから“Recovery HDをクローン”するよう指示されます。Recovery HDボリュームをクローンし直すことが役立つのは、Recovery HDボリュームが無効な場合、または、そのパーティションタイプが無効な場合（そしてそれがデスクトップに表示される場合）です。

既存のRecovery HDボリュームを削除するには

なんらかの理由でバックアップディスクからRecoveryボリュームを削除する必要がある場合があります。Recovery HDボリュームを削除するには：

1. CCCのサイドバーにある**ボリューム**からバックアップボリュームを選択します（CCCのサイドバーを表示するには、CCCのツールバーから**サイドバーを表示**をクリックしてください）
2. ウィンドウの下にある Recovery HD... をクリックします
3. Option キー（**⌥**）を押したままにして、Recovery HDを削除のボタンをクリックしてください。
[VoiceOverを使用する場合：QuickNavを使用して、“キャンセル”ボタンの左にあるRecovery HDを削除... ボタンをクリックしてください]

CCCは、Recovery HDボリュームを削除し、その空き容量をドナーボリュームに割り当てます。このタスクがドナーボリュームを破壊することはありませんが、パーティションの変更をする前にこのボリュームにあるデータをバックアップしておくをお勧めします。

関連ドキュメント

- Appleの“Recovery HD”パーティションをクローンするには、についてのよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition>>
- ディスクセンター <<http://bombich.com/ja/ja/kb/ccc5/disk-center>>
- FileVault暗号化で作業するには <<http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption>>

APFSボリュームでスナップショットを活用する

このチュートリアルビデオをYouTubeでご覧ください <<https://youtu.be/buM2HzDJKU4>>

スナップショットとは何ですか？

スナップショットはAppleのAPFSファイルシステムの新機能で、macOS High Sierraおよびそれ以降で利用できます。スナップショットはハードドライブ上のボリュームのある時点の状態です。スナップショットが取られると、そのスナップショット内のそれぞれのファイルは、たとえそのファイルが削除されても、スナップショットが取られた瞬間のそのままの状況でスナップショットに利用できます。CCCがAPFSフォーマットされたボリュームのスナップショットを定期的を作成するよう設定しておくことで、ファイルの古いバージョンをすばやく復元できます。スナップショットとCCCの起動可能なバックアップを組み合わせることで、Macの古いバージョンのオペレーティングシステムの古いバージョンを復元することさえも可能です！

注意：スナップショットはmacOS High Sierraおよびそれ以降でAPFSフォーマットされたボリュームにのみ利用できます。

包括的なデータ保護の方法としてのスナップショットの役割

バックアップが提供するデータ保護にはいくつかの局面があります。以下に備えて保護：

- 誤ってファイルを削除または変更してしまった場合
- ファイルの悪意的な変更 (マルウェアやランサムウェアなど)
- 機能を後退させるようなOSまたはソフトウェアアップデート
- ハードドライブの問題
- コンピュータの盗難
- 災害による喪失 (例：竜巻、台風、洪水など — オリジナルとバックアップの両方の喪失)

ファイルシステムレベルのスナップショットのサポートはバックアップの戦略を考える上で重要かつ不可欠な要素です。しかし、スナップショットは、別の物理的なハードウェア上にバックアップをするという本当の意味でのバックアップに完全に置き換えられるものではありません。もし起動ディスクが動作しない場合、世界中のどのスナップショットも起動ディスクとデータを復元させることはできません。起動可能なバックアップを外部ディスクに作成しておけば、いつでも即座に作業に戻ることができます。

スナップショット	起動可能なバックアップ	リモートMacintoshへのバックアップ
誤ってファイルを削除してしまった場合 マルウェア/ランサムウェア 不良なOSアップデート ハードドライブの問題 盗難 自然災害による喪失		

バックアップの戦略を考える時、データに与える可能性のあるすべてのリスクを考慮して、それらのリスクが緩和できるか、そしてどのように緩和できるかを判断してください。最小限、ローカルに接続されたハードドライブにバックアップを定期的にスケジュールすることをお勧めします。定期的にスケジュールされたバックアップがあれば、データに与える最も一般的なリスクからうまく保護することができます。

CCCでスナップショットを使用する

SSDデバイスのAPFSボリュームをソースまたはコピー先としてCCCのバックアップタスクに選択した場合、CCCは自動的にそのボリュームでスナップショットのサポートを有効にして、デフォルトの“スナップショット保持のポリシー”をそのボリュームに設定します。

基本的なスナップショットのサポートには、他の設定を追加する必要はありません。CCCは自動的に論理的なデフォルト設定を使ってスナップショットを管理します。

† CCCは起動ディスクではスナップショットのサポートを自動的に有効にしません。起動ディスクのストレージをスナップショットに使用したい場合、そのボリュームのスナップショットのサポートを手動で有効にできます。

回転式HDDデバイスにおけるAPFSおよびスナップショット

CCCはソリッドステートデバイスによってバックアップされたAPFSボリュームに限り、そして、デバイスがソリッドステートデバイスであることをCCCが判断できる時に限って (この判定は外部デバイスではできないことがよくあります)、自動的にスナップショットのサポートを有効にします。APFSフォーマットのHDDデバイスで十分なパフォーマンスが得られない場合、そのボリュームのスナップショットのサポートを無効にして、そのボリュームにあるすべてのスナップショットを削除することを推奨します。また、

[起動ディスクの起動可能なバックアップを作成するためにSSDの購入を検討](#)

<http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive> することをお勧めします。

ソースのスナップショット

ソースボリュームでスナップショットを維持しておく、偶発的なファイルの削除や変更から保護することができます。スナップショットをソースボリュームに残しておく、誤って削除されたファイルを復元したい時にバックアップボリュームを必要としません。しかし、スナップショットを保持しておくことで、時間の経過と共にディスクの使用領域が増えるので、ソースのスナップショットの保持の上限を設定しておくことを推奨します。この推奨は

[CCCが起動ディスクに対して特に重要とするものです](#)

。さらに、スナップショットを保持する方法を考える際、Appleのインストーラが起動ディスクからすべてのスナップショットを削除する可能性があることを忘

れないでください。スナップショットは恒久的なデータストレージの方法ではありません。

バックアップタスクを実行中、CCCは適格なソースボリュームにスナップショットを自動的に作成して、そのスナップショットをバックアップタスクのソースとして使用します。スナップショットは読み出し専用でマウントされるので、バックアップタスクを実行中にファイルに加えられた変更がバックアップタスク中にエラーを引き起こすことはないからです。データのまさしくその時点 (point-in-time) のバックアップを入手できます。ソースボリュームでスナップショットを無効にしている場合 (この方法については以下で詳細をご覧ください)、CCCは一時的なソースのスナップショットをバックアップタスクの終了時に自動的に削除します。

macOS

Catalina、およびそれ以降:

CCCはソースのシステムボリュームにあるスナップショットを[APFSボリュームのグループ](#)

<http://bombich.com/ja/ja/kb/ccc5/working-apfs-volume-groups>

に作成することはありません。これらのボリュームはすでに読み出し専用なので、スナップショットは必要ありません。この例外が唯一適用されるのは、ソースのボリュームグループにある特別なシステムボリュームだけで、“Data” ボリュームには適用されません。ソースの“Data” ボリュームへのスナップショットの作成と保持は、“スナップショット保持のポリシー”の後に続きます。

コピー先のスナップショット

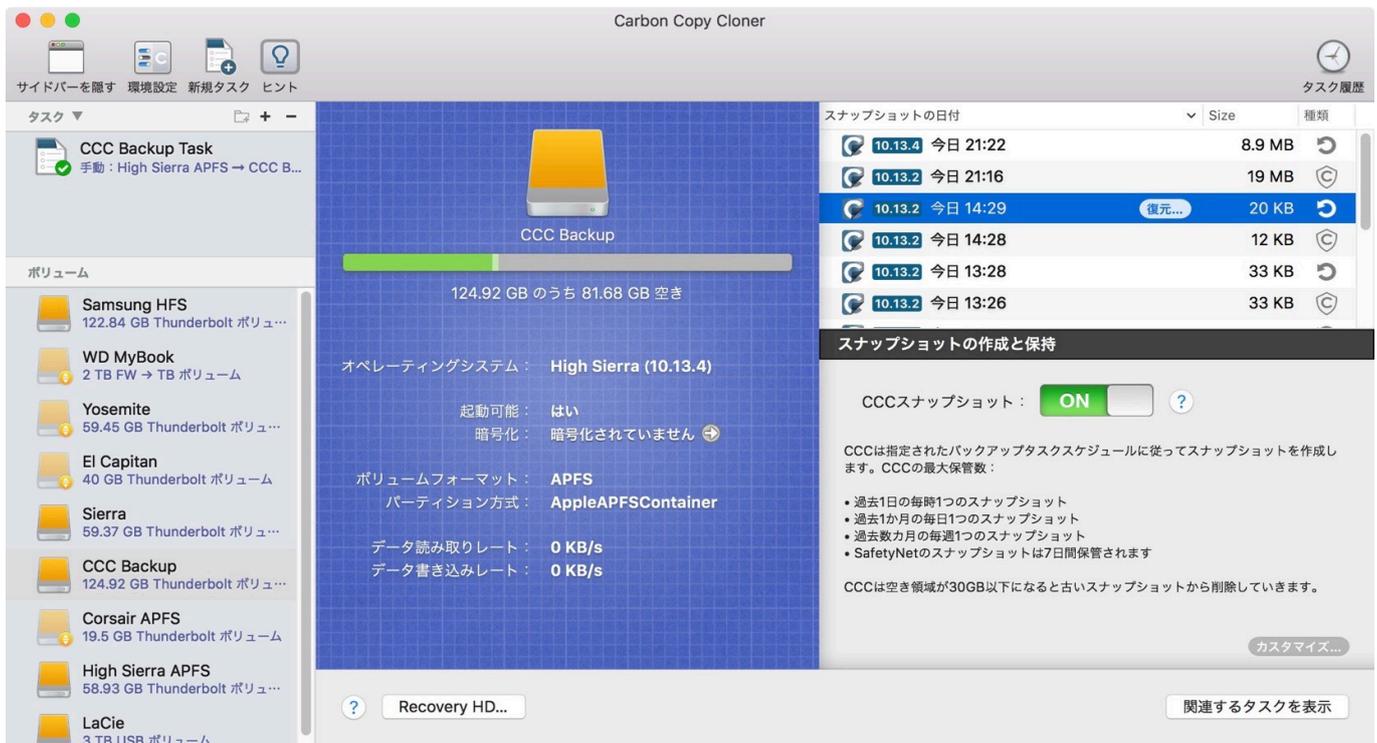
CCCのSafetyNet機能が有効になっている場合、CCCはコピー先の [SafetyNetのスナップショット](#) <http://bombich.com/ja/ja/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet#safetynetsnapshot> をバックアップタスクの開始時に作成します。その後CCCは、そのボリュームの

ために定義されたスナップショット保持ポリシーに従ってコピー先のスナップショットを削除します。バックアップタスクの最後に、CCCはもう1つの“バックアップのスナップショット”を作成します。このもう1つの“バックアップのスナップショット”は、そのバックアップタスクイベントのその時点でのバックアップを定義します。

スナップショットのサポートを切り替え、スナップショット保持ポリシーを設定するには

CCCはスナップショットのサポートを個々のボリュームベースで考えます。スナップショットのサポートは、あるボリューム(またはそのボリュームのフォルダ)がソースまたはコピー先としてCCCのバックアップタスクに選択されると、自動的に有効になります。ソースとコピー先ボリュームでスナップショットのサポートをCCCに自動的に有効にして欲しくない場合は、CCCの環境設定からその操作を無効にすることができます。

ボリュームのスナップショットのサポートまたは保持ポリシーを表示または変更するには、CCCのサイドバーを表示し、サイドバーからボリュームをクリックしてください。CCCは現在ボリュームに存在するスナップショットをすべて表示して、そのボリュームに関する保持ポリシーを表示します。スナップショットのサポートはAPFSボリュームに限定されていることをお忘れなく。非APFSフォーマットのボリュームをCCCのサイドバーで選択しても、スナップショットの設定は表示されません。



The screenshot shows the Carbon Copy Cloner application window. The main area displays the settings for a selected volume, 'CCC Backup'. The volume is a 124.92 GB Thunderbolt volume with 81.68 GB of free space. The operating system is High Sierra (10.13.4), and the volume format is APFS using AppleAPFSContainer partitioning. Read and write speeds are both 0 KB/s. The 'Snapshots' section shows that snapshots are currently turned ON. Below this, there is a list of existing snapshots with columns for date, time, size, and type. A 'Recovery HD...' button is visible at the bottom left, and a '関連するタスクを表示' button is at the bottom right.

スナップショットの日付	Size	種類
10.13.4 今日 21:22	8.9 MB	🔄
10.13.2 今日 21:16	19 MB	🔄
10.13.2 今日 14:29	20 KB	🔄
10.13.2 今日 14:28	12 KB	🔄
10.13.2 今日 13:28	33 KB	🔄
10.13.2 今日 13:26	33 KB	🔄

保持ポリシーのデフォルト設定

- SafetyNetのスナップショットは7日間保持されます†
- 週ごとのスナップショットは空き領域が制約を受けるまで保持されます†
- 日ごとのスナップショットは30日間日保持されます†
- 時間ごとのスナップショットは24時間保持されます
- 空き領域が30GB以下になると一番古いスナップショットから削除されます

† CCCは起動ディスクに対してはより保守的な保持ポリシーを適用します。つまり、SafetyNetのスナップショットは3日間保持されます。週ごとのスナップショットは保持されません。日ごとのスナップショットは3日間のみ保持されます。これらの設定をカスタマイズして、起動ディスクのスナップショットをより長く保持しておくことができますが、それによる起動ディスクの [ディスク使用状況に与える影響を考慮してください](#)。

CCCはバックアップタスクの開始時、および空き領域が制約を受けた場合(コピー先ボリュームで)バックアップタスク中にスナップショットを削減します。保持ポリシーは上記の順に評価されますが、指定された空き領域の制限を達成するために必要であれば、任意のスナップショットが削除される可能性があります。その唯一の例外は、他のアプリケーションで作成されたスナップショットと、現在のバックアップタスク中に作成されたスナップショットです。CCCは現在のバックアップタスクの開始時に作成されたSafetyNetのスナップショットは削除しません。

ボリュームグループのスナップショット保持のポリシー

ボリュームグループ <<http://bombich.com/ja/ja/kb/ccc5/working-apfs-volume-groups>> はグループごとに1つのスナップショットの保持ポリシーで処理されます。ポリシーの設定は、グループのデータメンバーを表示する際に編集できます。CCCは、ソースに変更が加えられた時にのみ(例: システムアップデートを適用した時)、およびmacOS Catalinaでのみ、コピー先システムボリュームにスナップショットを作成します。このように、時間を基にしたシステムボリュームのスナップショットの保持は、あまり適切ではありません。代わりに、CCCはシステムボリュームのすべてのスナップショットを保持し、保持ポリシーの空き領域の制限が超過した場合に限って、システムのスナップショットを削除します。

他のアプリケーションで作成されたスナップショット

スナップショットを削減中、

CCCは他のアプ

リケーションで作成されたスナッ

プショットを削除することは決してありません

。他のアプリケーションで作成されたスナップショットを削除したい場合は、CCCのサイドバーで関連するボリュームをクリックして、削除したいスナップショットを選択してから、“削除”キーを押してください。

CCCのスナップショット保持のポリシーは、スナップショットがそのボリュームで有効な場合のみ適用されます

以前に作成されたCCCのスナップショットを含むボリュームのCCCのスナップショットサポートを無効にすると、CCCはそのボリュームに関しては自動的にスナップショットを削減しません。スナップショットのサポートを無効にしている場合、スナップショットの切り替えボタンの上に表示されているスナップショットを削除して問題ありません。表の中のスナップショットを1つ以上選択してから“削除”キーを押すだけです。

スナップショットの保持ポリシーはどのスナップショットを保持するかを定義するもので、いつ作成されるかを定義するものではありません

CCCはバックアップタスクが実行される時に、そしてバックアップタスクが実行される時にのみ、スナップショットを作成します。CCCはスケジュールされた時以外に、また手動でバックアップタスクを実行する時以外にスナップショットを作成することはありません。このように、“24時間の間、1時間ごとに最高1つのスナップショット”を保存するという保持ポリシーは、前日の分として24のスナップショットがあるということを示唆しているわけではありません。バックアップタスクを日ごとのみに実行するように設定している場合、ソースボリュームとコピー先ボリュームに1つのスナップショットがあるということです。時間ごとのスナップショットが欲しい場合には、バックアップタスクが時間ごとに実行されるよう設定されているか確認してください。

CCCはバックアップを完了するために追加の空き領域が必要であれば、空き領域の制限を上書きします

デフォルトの空き領域の制限は30GBになっていて、通常それぞれのバックアップタスク中、CCCが30GBのデータを確実にコピー先ボリュームに書き込むことができるようになっています。CCCが30GB以上のデータをコピーする必要があり、コピー先にその領域がない場合、CCCは追加のスペースを解放するためにバックアップタスク中スナップショットを追加で削除します。この“緊急”削除が発生した場合、CCCはバックアップタスクイベントに通知を追加して(タスク履歴ウインドウに)、コピー先ボリュームの“スナップショットの保持ポリシー”を確認するよう提案します。

スナップショット保持のポリシーを確認するには:

CCCのサイドバーからコピー先ボリュームをクリック

クして、カスタマイズ

をクリ

ックすると、保持ポリシーの設定をカスタマイズできます。特に変更を検討した方が良い設定は、**"空き領域が xx GBより少ないとき一番古いスナップショットを削除**

"とラベルされているものです。空き領域の制限を確認するには、自分のバックアップタスクが通常30GB以上コピーするかどうかを考えてください(算定するには [CCCの“タスク履歴”ウインドウ](#)

<http://bombich.com/ja/ja/kb/ccc5/how-find-out-when-backup-last-ran-ccc-task-history>

を利用してください)。緊急の削除とそれに伴う通知を回避するためにも、通常コピー先にコピーされるデータ量を保管しておくのに十分なスペースを残す値を指定してください。

バックアップタスクが突然普段よりも多くのデータをコピーしていることに気が付いたら、問題が起きている可能性がないか確認してください。例えば、別のソースを同じコピー先にバックアップするバックアップタスクが2つ以上ある場合、それらのタスクが競合していて、お互いのファイルを削除しているかもしれません。また、コピー先のディスク使用量がソース(スナップショットのディスク使用状況)に比べて異常に多くないかどうかを確認してください。ディスクの使用状況に疑問がある、またはCCCがコピーしているデータ量に説明がつきにくい場合、お気軽にお使いの設定について [詳しく確認をするためにお問い合わせ](#)

<http://bombich.com/ja/software/gethelp> ください。

SafetyNetのスナップショット vs. バックアップのスナップショット

SafetyNetはコピー先ボリュームのデータを保護することを目的としたCCCのユニークな機能です。例えば、あなたが3つのボリュームを持っているとしましょう: Macintosh

HD、バックアップ、写真の3つです。バックアップタスクを作成して、誤って**写真**のボリュームをコピー先として選択してしまった場合、大抵のクローンアプリケーションは単純にコピー先を消去するか、またはそのボリュームのファイルを削除します。後戻りはできません! SafetyNetを有効にしておく、CCCはそれらの項目をコピー先に保持しますが、別のフォルダに分けて入れておくので、必要であれば後で復元できます。

スナップショットが有効になっているボリュームでは、SafetyNetは新しくプリフライトスナップショットとして実装されます。CCCがコピー先に変更を加える前に、CCCはコピー先の“SafetyNetのスナップショット”を作成します。その後、タスクは通常の方法、つまりソースからコピー先にファイルをコピーするという方法で進みます。間違ったコピー先でタスクを設定してしまった、または、ファイルをコピー先ボリュームに配置し、それらがバックアップタスク後無くなっている、ということに後で気づいた場合、それらの項目をSafetyNetのスナップショットからコピー先に復元することができます。

バックアップタスクの終了時、CCCは2つ目のスナップショット、“バックアップのスナップショット”を作成します。この2番目のスナップショットは現在のバックアップイベントのソースの状況を表しています。もしデータをオリジナルのソースまたは置換ディスクに復元し直したい場合は(例えばソースディスクが動作しないため)、バックアップのスナップショットを使ってデータを復元することができます。これは重要なポイントです。一般的にSafetyNetのスナップショットを使用してデータをオリジナルのソースに復元し直すことはありません。SafetyNetのスナップショットはコピー先で誤って削除されたり、変更されたファイルを復元するために使用されます。

要するに、これら2つのポイントを覚えていてください:

-  SafetyNetのスナップショットは **バックアップタスクに関連のない**コピー先にファイルを復元できる
-  バックアップのスナップショットはソースボリュームからのその時点 (point-in-time) のデータを復元する

SafetyNetは自分に必要なものですか? SafetyNetをオフにできますか。または、SafetyNetが使用する領域を制限できますか?

SafetyNetのスナップショットは、間違ったコピー先を選択した、バックアップタスクに関連しないファイルを保存するためにコピー先を使用した、などの設定のミスから保護します。これらのスナップショットには異なる目的があるので、それらはそれぞれ別の保持ポリシーで管理されます。デフォルトで、CCCは1週間を超えているSafetyNetのスナップショットを削除します。コピー先ボリュームがバックアップタスク専用で、そのボリュームに他

のファイルを保存することが決していない場合、SafetyNetの保持値を下げることができます(例、1日か2日などに)。

タスクの設定に問題がない自信があり、コピー先がバックアップタスク専用であり、同時にコピー先に多くのオーバーヘッドがない場合、SafetyNetを無効にする選択をすることもできます。SafetyNetをタスクごとに無効にすることもできますが、コピー先ボリュームのSafetyNetの保持の値をゼロに設定することを推奨します。この設定を使うと、CCCはタスクの最初にSafetyNetのスナップショットを作成しますが、それまでに作成されたSafetyNetのスナップショットはすべて次のタスクが開始される時に削除されます。この設定はコピー先ディスクで多くの余分なスペースを浪費することなく、設定エラーから若干保護することができます。

SafetyNetは安全なメカニズムですが、バックアップボリュームに他のものを保持するための方法ではありません

シートベルトを着

けているからといって、毎日壁に突

っ込んで良いわけではないのと同じです。

バックアップボリュームはバックアップタスク専用にするべきです。

バックアップディスクの余分なスペースを利用したい

場合、[そのディスクにその他のデータを保存するための特別なボリュームを追加 <http://bombich.com/ja/ja/kb/ccc-5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#apfsaddyvolumestartupdisk>](http://bombich.com/ja/ja/kb/ccc-5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#apfsaddyvolumestartupdisk)

するのがよいでしょう。その別のボリュームはCCCの権限外ですので、すべての意図的ではない変更から保護されます。ディスクユーティリティを開いてバックアップディスクを選択し、編集メニューから**APFSボリュームを追加...**を選択してバックアップディスクにボリュームを追加してください。

スナップショットの内容をマウントおよびブラウズするには

スナップショットの内容をブラウズしたい場合、スナップショットの表からブラウズしたいスナップショットを選択して右クリックし、**Finderでブラウズ**を選択してください。または、単純に

スナップショットをダブルクリックしてください

。そうすると、そのスナップショットの内容をいつも通りFinderでブラウズすることができます。スナップショットは読み出し専用でマウントされているので、スナップショットに有害な変更を加えることは不可能です。1つの項目を復元したい場合は、その項目をスナップショットから復元したい場所にドラッグするだけです。スナップショットがマウントされると、“スナップショット”一覧のスナップショットのクリエイターアイコンに緑色の丸が付いて、マウント中であることを示します。

スナップショットの日付	Size	種類
 10.13.4 2018/03/21 21:22	8.9 MB	
 10.13.2 2018/03/21 21:16	19 MB	
 10.13.2 2018/03/21 14:20	20 KB	
 10.13.2 2018/03/21 14:15	12 KB	
 10.13.2 2018/03/21 14:10	33 KB	
 10.13.2 2018/03/21 14:05	33 KB	

1 snapshot: 20 KB
Finderでブラウズ
 削除
 タスクイベントの詳細

注意：デフォルトで、マウントされたスナップショットはFinderにもディスクユーティリティにも表示されないの
 で、通常それらのアプリケーションでスナップショットをマウント解除することはできません。CCCは、スナ
 ップショットの表のスナップショットクリエイターアイコンの上に緑色の小さな丸を配置することでスナップシ
 ョットがマウントされたことを表示します。CCCでマウントされたスナップショットを右クリックして“マ
 ウント解除”のオプションを選択すると、スナップショットを手動でマウント解除できます。しかし、利便性を高めるために、
 CCCはCCCの終了時に、CCCがマウントしたすべてのスナップショットを自動的にマウント解除します。

ディスクイメージから復元するには

CCCにはスナップショットから復元する方法が2つあります。最もシンプルな方法は、CCCのディスクセンターから開始することです：

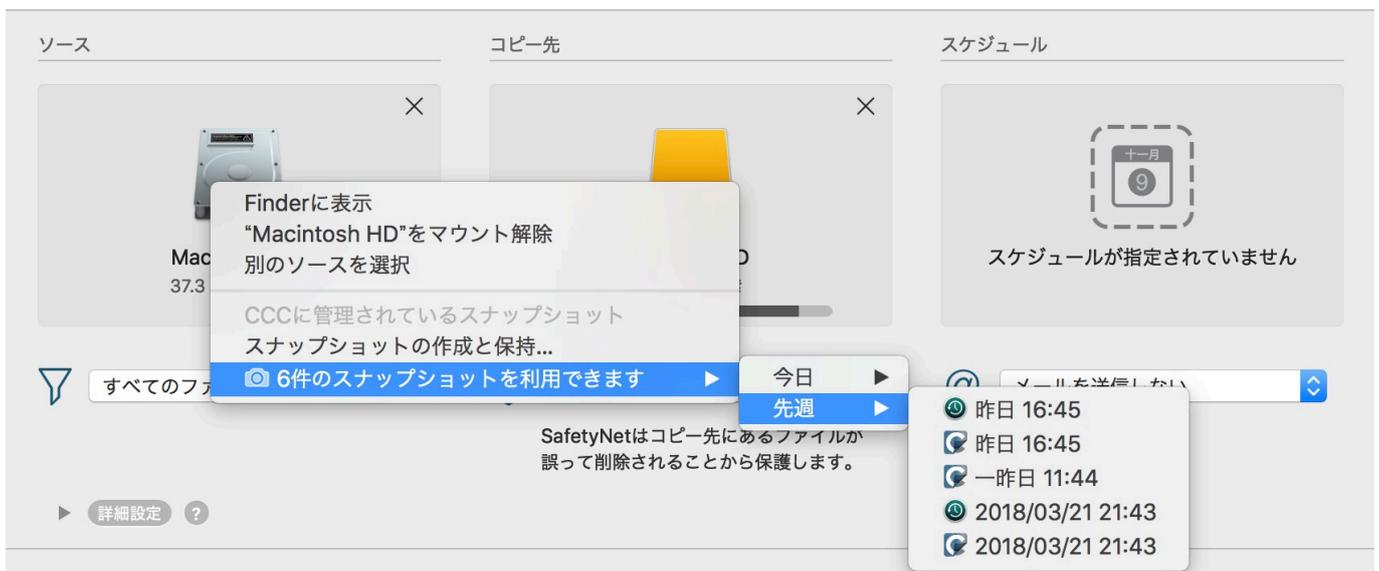
1. CCCのサイドバーからボリュームをクリックし、そのボリュームに利用できるスナップショットのリストを表示してください
2. スナップショットを個別に選択します
3. **復元...** ボタンをクリックします

CCCは新規の復元タスクを作成し、スナップショットをマウントしてバックアップタスクのソースとしてそれを選択します。選択されたスナップショットがSafetyNetのスナップショットの場合、SafetyNetはオリジナルのコピー先ボリュームをコピー先として選択します。選択されたスナップショットがCCCで作成されたバックアップのスナップショットの場合、CCCはオリジナルのソースボリュームをコピー先として選択します。選択されたスナップショットがCCCで作成されていない場合、コピー先セクタをクリックして復元タスクのコピー先を選択してください。また、[復元タスクを特定のファイルとフォルダのセットに制限する](#)

<http://bombich.com/ja/ja/kb/ccc5/excluding-files-and-folders-from-backup-task>よう選択することもできます。

また、復元タスクを手動で設定する際にスナップショットを選択することもできます：

1. 新規タスクを作成します
2. スナップショットを含んでいるボリュームをソースとして選択します
3. ソースセクタをクリックしてコンテキストメニューから特定のスナップショットを選択してください



システムファイルを起動ディスクに復元するには

macOSではmacOSから起動中オペレーティングシステムを変更することは許可されていません。以前のスナップショットからOSを復元したい場合、[CCCのバックアップボリュームからMacを起動](#)
<http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup>
 すると、スナップショットから復元を進めることができます。

APFSボリュームグループをmacOS Catalinaの1組のスナップショットから復元するには

この操作はmacOS Big Surでは利用できません。

AppleはmacOS Catalinaで [ボリュームグループ](#) <http://bombich.com/ja/ja/kb/ccc5/working-apfs-volume-groups> と

このコンセプトを紹介しました。ボリュームグループは、2つ1組のボリュームで成り立ち、1つのボリュームにはオペレーティングシステムのファイルが、もう1つにはユーザのデータが含まれています。CCCは、コピー先のシステムボリューム上のそれぞれのOSバージョンのスナップショットを1つ保持します。そして、ユーザのデータボリュームのスナップショットをコピー先のスナップショット保持のポリシーに従って保持します。スナップショットの一覧には、CCCはスナップショットが作成された時点のOSのバージョンとビルドナンバーを表示します。

スナップショットからAPFSボリュームグループを復元するには、2つの別々の復元タスクを実行する必要があります。まず第1に、バックアップディスクのデータボリュームにあるスナップショットを選択し、“復元”ボタンをクリックしてから、そのスナップショットをAPFSフォーマットされたコピー先に復元してください。第2に、バックアップディスクのシステムボリュームにあるスナップショットを選択し、“復元”ボタンをクリックしてから、そのスナップショットを同じAPFSフォーマットされたコピー先に復元してください。CCCはボリュームグループをコピー先に自動的に作成して、それぞれのスナップショットをコピー先の正しいボリュームに復元する過程を処理します。

- 異なるOSバージョンに関連するシステムおよびデータのスナップショットを復元してもかまいませんが、これらをミックスする意味はまだわかりません。できれば、OSバージョンが一致するシステムおよびデータのスナップショットを復元してください。
- CCCは、ソースのスナップショットがシステムか、データか、どちらのボリュームのスナップショットかを判断して、それぞれをコピー先の正しいボリュームに復元する過程を処理します。スナップショットを正しい場所に導くために特別な手順は必要ありません。復元先にしたいボリュームを選択するだけです。

SafetyNetのスナップショットからファイルをコピー先に復元するには

SafetyNetは偶発的な削除からコピー先ボリュームのファイルを保護するようデザインされたメカニズムです。誤って間違ったボリュームをコピー先として選択した場合、またはソースのデータセットに関連のないコピー先に保存したファイルが無くなっている場合、SafetyNetのスナップショットからコピー先にファイルを復元できます。

- CCCを開いて、CCCのサイドバーから影響を受けるコピー先ボリュームを選択します。
- 適用できるSafetyNetのスナップショットをスナップショットの表から選択してください。
- 復元...** ボタンをクリックします。
- CCCが作成したタスクの設定を確認してから、“クローン”のボタンをクリックしてください。

この復元タスクを続けると、CCCはファイルをスナップショットから、選択されたコピー先にコピーし直します。CCCは、それらのファイルをコピー先に復元するより先に、復元しようとしているファイルが入っているスナップショットを削除できませんので、注意してください。その結果、復元中のすべてのファイルのコピーを収容するための十分な空き領域がコピー先にある必要があります。ファイルをオリジナルのコピー先に復元し直すことは実用的ではない場合があるかもしれません。その場合、先に他のディスクに復旧する必要がある可能性があります。

関連リソース：

- バックアップから復元するには <<http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup>>
- バックアップタスクからファイルとフォルダを除外するには <<http://bombich.com/ja/ja/kb/ccc5/excluding-files-and-folders-from-backup-task>>
- “新しいファイルのために十分な空き容量があるのに、CCCからコピー先がいっぱいだという報告があるのはどうしてですか？” <<http://bombich.com/ja/ja/kb/ccc5/ccc-reported-destination-full.-what-can-i-do-avoid#destinationistightonspace>>

CCCのスナップショット vs. Time Machineのスナップショット

CCCとTime Machineはどちらも指定されたAPFSボリュームでスナップショットを作成することができます。それぞれで作成されたスナップショットはまったく同等です。CCCで作成されたスナップショットとTime Machineで作成されたスナップショットに技術的な違いはありません。Time Machineが有効で、CCCのソースまたはバックアップボリュームをTime

Machineの範囲から特に除外しない限り、Time Machineはそれらのボリュームに独自のスナップショットを自動的に作成したり削除したりします。CCCは復元のために存在するスナップショットについては曖昧なスタンスを持っているので、Time

MachineがCCCのソースとコピー先ボリュームにスナップショットを作成することを許可します。

しかし、CCCとTime Machineの両方に指定したボリュームのスナップショットの作成を許可したいかどうかをよく考える必要があります。異なる保持ポリシーで管理されている重複するスナップショットが害になることはありませんが、おそらく保持スケジュールの効率を下げる結果になるでしょう。しかし、Time Machineはスナップショットを24時間だけ保持するので、問題になるのは1日分のスナップショットに限定されます。

Time Machineのスナップショットを個々のボリュームで無効にするには

CCC内で、あるボリュームのスナップショットのサポートを無効にした後も、そのボリュームのスナップショットがまだ作成されていることは、多くのユーザが気付いています。スナップショットのサポートを無効にすると、CCCがそのボリュームからのスナップショットを作成および削除するかに影響しますが、Time Machineには影響しません。CCCのスナップショットの一覧にはスナップショットを作成したアプリケーションのアイコンが表示されています:

-  Carbon Copy Clonerによって作成されたスナップショット
-  Time Machineによって作成されたスナップショット

Time Machineが指定したボリュームでスナップショットを作成しないようにしたい場合、そのボリュームをTime Machineから除外することができます:

- システム環境設定を開きます
- 環境設定パネルの“Time Machine”を開きます
- ウィンドウの右下にある **オプション...** ボタンをクリックします
- + ボタンをクリックして除外したいボリュームを選択してください

スナップショットと領域の問題：スナップショットを削除するには

当初、スナップショットは本質的に領域を消費しません。スナップショットを作成する際、スナップショットを含むボリュームのディスク使用状況は変化しません。しかし、スナップショットがボリュームのすべてのファイルに参照を保持するため、ファイルを削除する際に領域が解放されません。例えば、100GBのハードドライブに80GBのコンテンツがあるとします。スナップショットを作成し、その後20GBのファイルをゴミ箱に移動してゴミ箱を空にします。結果として生じるディスクの使用量はまだ80GBです。その20GBの領域はスナップショットが削除されるまで解放されません。

この空き領域の動作はスナップショットを特定のボリューム（起動ディスクを含む）で有効にするかを判断する際に考慮すべき重要な要素です。特にハードドライブがいっぱいになっている状態では、スナップショットをそのボリュームで維持することは実用的な解決策ではないでしょう。Time Machineとは対照的に、CCCは特定のボリュームでスナップショットを有効にするか、そしてどのようにそれらのスナップショットを長期間維持するかという点で非常に柔軟性があります。さらに、CCCは特定のスナップショットを簡単に見つけて削除することができます。スナップショットの表から削除したいスナップショットをクリックして“Delete”キーを押すだけです。

注意:

Finderと“情報を見る”ウィンドウは、ボリュームで利用可能な空き領域を計算する際にローカルスナップショットを含みません。 <<https://support.apple.com/en-us/HT204015>>

特定のボリュームでスナップショットが消費している領域を知りたい場合は、CCCのサイドバーからそのボリュームを選択してください。ディスクの使用状況インジケータはスナップショットが消費している領域のパーセンテージを表示します。スナップショットの表にはボリュームのそれぞれのスナップショットのサイズが表示されます。スナップショットのサイズの計算は複雑で動的です。スナップショットを削除すると、隣接するスナップショット

トが消費している領域は、それらのスナップショットがディスク上のファイルの最後の参照ホルダーになるので、変化する可能性があります。これは正常なことです。また、スナップショットのサイズは、そのスナップショットが削除された場合どれだけの領域が解放されるかを示すものであることに注意してください。そのスナップショットによって参照されている総データ量を示すものではありません。

スナップショットのディスク使用量の総量が、個々のスナップショットのディスク使用量を足した合計よりも多いのは、なぜですか？

多くの人がこの差を見たとき、CCCは計算ができないのかと勘違いされるようですが、数字はすべて正確です。スナップショットのディスク使用量の総量は、個々のディスク使用量の合計ではありません。以下のリンクのビデオでその理由が説明されています。

スナップショットおよびディスクの使用状況についての詳細はYouTubeのこのビデオをご覧ください

<https://www.youtube.com/watch?v=4wqAC4YXiaY>

よくある質問

- [保持ポリシーは1時間ごとに1つのスナップショットを保持するとなっています。自分のディスクに時間ごとのスナップショットがもっとたくさんないのはどうしてですか？](#)
- [“CCC SafetyNet”フォルダはどこに行ったのですか？](#)
- [スナップショットを活用するには、HDDバックアップディスクをAPFSとしてフォーマットし直す必要がありますか？](#)
- [時間毎のスナップショットが欲しいのですが、コピー先を1日を通して毎時利用できるわけではありません。どうすればソースボリュームに時間ごとのスナップショットを残すことができますか？](#)
- [APFSフォーマットされたボリュームで暗号化を有効にしたところ、CCCがスナップショットを作成できないというエラーが出るのはどうしてですか？](#)

保持ポリシーは1時間ごとに1つのスナップショットを保持するとなっています。自分のディスクに時間ごとのスナップショットがもっとたくさんないのはどうしてですか？

ディスクにスナップショットを作成するための最大のコントロールとして、CCCはバックアップタスクが実行された時のみスナップショットを作成します (1時間ごとにスナップショットを作成する、設定不可能なTime Machineと比べてこれが特に対照的な点です)。バックアップタスクを日ごと、または週ごとに実行する場合、CCCは時間ごとのスナップショットを生成しません。保持ポリシーは指定された期間 1時間ごとに最高で1つのスナップショットを残します。これは、その期間 1時間ごとに最低1つのスナップショットを残すという意味ではありません。時間ごとにスナップショットを作成したい場合には、時間ごとにタスクを実行するようスケジュールできます。

“CCC SafetyNet”フォルダはどこに行ったのですか？

CCC 5.1より前、CCCはSafetyNet機能が有効な場合、“CCC SafetyNet”フォルダをコピー先ボリュームのルートに作成していました。CCCがコピー先をアップデートすると、ソースに存在しないファイル、またはアップデートされたバージョンで置き換えられたファイルはそのSafetyNetフォルダに移動していました。CCC 5.1、およびそれ以降でスナップショットがサポートされると、スナップショットがコピー先で有効になっている場合、そのフォルダはSafetyNetのメカニズムの一部として使用されなくなります。代わりに、CCCはタスクの開始時にSafetyNetのスナップショットを作成し、その後コピー先のアップデートに進みます。古いバージョンのファイルとソースに存在しないファイルは、コピー先から即座に削除されます (しかしまだ、SafetyNetのスナップショットによって保護されています!)。従って、タスクの終了時にはソースとコピー先が同一になります。

レガシーSafetyNetフォルダを持つAPFSのコピー先ボリュームでスナップショットを有効にしている場合、CCCはまずSafetyNetのスナップショットを作成します。SafetyNetのスナップショットの作成を完了した後 (それにはレガシーSafetyNetフォルダが保持されています)、レガシーSafetyNetフォルダは削除されます。その後、SafetyNetのスナップショットは、コピー先ボリュームのためのスナップショットの保持ポリシーで定義されたSafetyNet保持の対象になります。そのSafetyNetフォルダの内容にアクセスしたい場合は、SafetyNetのスナップショットを選択して、そのスナップショットを右クリックし、Finderに**表示**を選択してください。

SafetyNetを使ってファイルの古いバージョンを復元することに慣れている場合、CCC 5.1ではバックアップのスナップショットがその目的を実行するようデザインされていますので、注意してください。SafetyNetのスナップショットは、コピー先に残っていた何かがバックアップタスクを実行後に喪失した場合にのみ、使用を検討してください。

こちらも参照：[レガシーSafetyNetフォルダは、スナップショットがコピー先で有効の場合、使用されません](http://bombich.com/ja/ja/kb/ccc5/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination)
<<http://bombich.com/ja/ja/kb/ccc5/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>>

時間毎のスナップショットが欲しいですが、コピー先を1日を通して毎時利用できるわけではありません。どうすればソースボリュームに時間ごとのスナップショットを残すことができますか？

CCCはタスクイベント中スナップショットのみを作成します。というのは、スナップショットはバックアップ対策の中の1つで、バックアップに代わるものではないからです。スナップショットは便利ですが、本当のバックアップは、物理的に異なるメディア上にファイルが保護される必要があります。それでも、時間ごとのスナップショットの利便性が気に入っているが、ロジスティックな理由で、コピー先が常に利用できない(例：仕事に出かける、等)ためバックアップタスクを実行できない人もいます。

CCCが時間ごとのスナップショットを特定のボリュームに作成するように設定するには、その同じソースボリュームの1つのフォルダを別のフォルダにコピーする <<http://bombich.com/ja/ja/kb/ccc5/folder-folder-backups>> 新規タスクを設定することができます。その場合何がコピーされるかは、両方のフォルダが同じディスクにある限り、重要ではありません(事実フォルダが空でも構いません)。CCCは、そのボリュームに定義した保持ポリシーに従って、そのボリュームにスナップショットを作成して保持します。

1. 2つの新規フォルダをソースボリュームのどこかに作成して、“ソース”と“コピー先”と名前をつけてください。
2. CCCを開いてツールバーの **新規タスク** をクリックします
3. ソースフォルダをCCCのソースセレクトにドラッグします
4. コピー先フォルダをCCCのコピー先セレクトにドラッグします
5. SafetyNet機能をオフにします
6. 時間ごとに実行するタスクをスケジュールします
7. タスクを保存してください

APFSフォーマットされたボリュームで暗号化を有効にしたところですが、CCCがスナップショットを作成できないというエラーが出るのはどうしてですか？

APFSファイルシステムは、暗号化の変換が進行中、スナップショットを作成しません。しかし、ファイルシステムはこの状況で特定のエラーコードを出さないため、CCCはこのエラー状況をもっと役立つアドバイスと一緒に提示することができない上、変換が完了するまでエラーを表示することもできません。さらに、macOSは特定のボリュームの変換が進行中かどうかを知るためのインターフェースを他社製アプリケーションには提供しません。ですから、CCCには暗号化されたボリュームが現在変換中かどうかはわかりません。ターミナルアプリケーションに `diskutil apfs list` と入力することで、変換の進行状況を見ることができます。

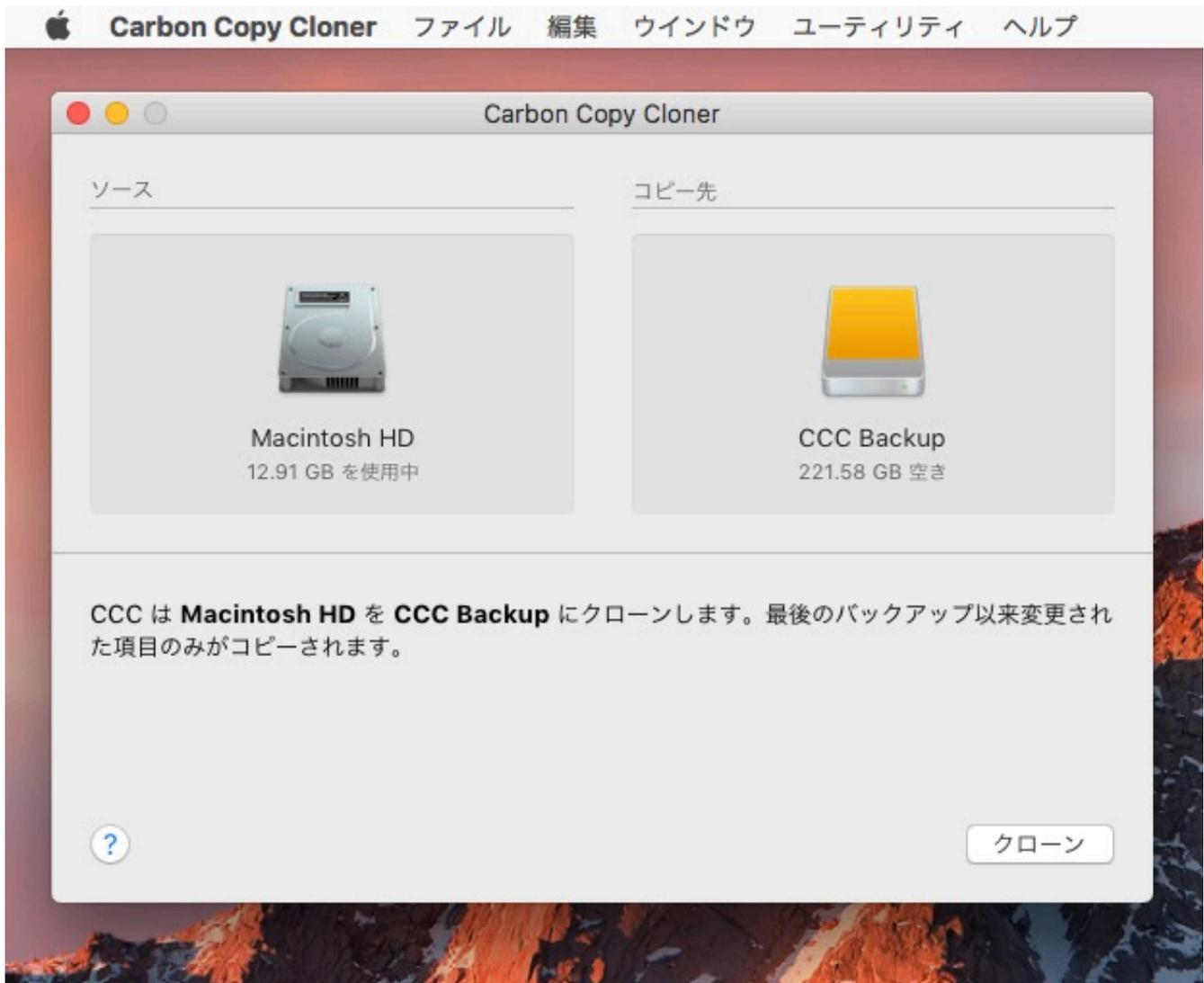
シンプルモード

シンプルモードを使用すると、ユーザインターフェースの要素が軽減され、シンプルになります。サイドバー、ツールバー、スケジュールセレクタ、高度な設定はすべて非表示になり、次の3つの主要なコントロールだけが表示されます：ソース、コピー先、クローンボタン。このシンプルなインターフェースは、あるボリュームから別のボリュームに特定の目的のためだけに基本的なクローンを必要とし、タスクのスケジュールを維持する必要のないユーザに、最適な方法と言えます。シンプルモードを使用するには、Carbon Copy Clonerのメニューから**シンプルモード**を選択してください。



シンプルモードでバックアップタスクを設定するには

1. ソースを選択します
2. コピー先を選択します
3. “クローン” ボタンをクリックします



関連ドキュメント

- OS Xのバックアップにバックアップディスクを準備するには <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>>

ネットワークボリュームを選択できますか？このバックアップをスケジュールする方法は？バックアップタスクから項目を除外できますか？

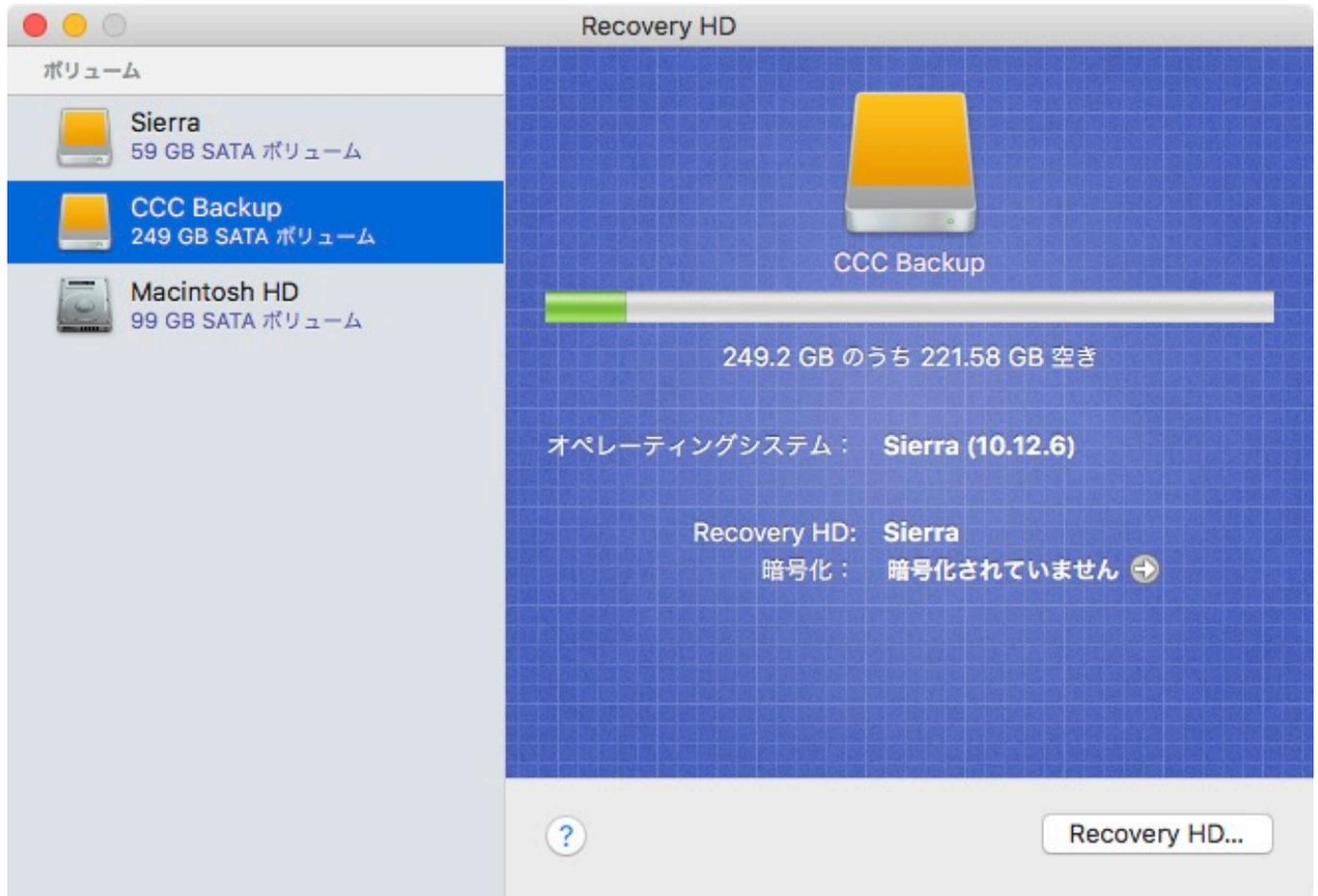
シンプルモードは単純に **基本的な**クローンタスクを目的としています。追加オプションを使用するには、Carbon Copy Clonerのメニューから **標準モード**を選択して標準モードに戻ってください。

参考のために、シンプルモードのタスクは標準モードで作成されたタスクと同じデフォルト設定で実行されます：つまり、SafetyNetは有効に設定されていて、コピー先の空き容量が25GB以下になるとSafetyNetフォルダの内容は削除されます。CCCは必要に応じてこの削除制限を自動的に調整します。シンプルモードでは、ソースとコピー先の選択肢は保存されません。CCCを開くたびにソースとコピー先には何も表示されません。さらに、タスク実行中CCCを開いたままにしておく必要があります。CCCを終了すると、実行中のタスクは停止されます（確認メッセージの表示後）。

Appleの Recovery HDボリュームをクローンするには

注意：この処理およびウインドウは、macOS Catalina、またはそれ以降を実行中のMacには適用することも、利用することもできません。

この過程にはシンプルとは程遠いと言える背景がある一方、この機能はシンプルモードに利用できるべき機能と考えられます。OSをバックアップボリュームにクローンした後、CCCのウインドウメニューからRecovery HDを選択すると、ローカルに接続されたボリュームがリスト表示されている別のウインドウを表示することができます。



バックアップボリュームにRecovery HDを作成するには、左側の表にあるバックアップボリュームをクリックしてから、ウインドウの下にあるRecovery HD...ボタンをクリックしてください。

- AppleのRecovery HDパーティションをクローンするには <<http://bombich.com/ja/ja/kb/ccc5/cloning-apples-recovery-hd-partition>>
- Appleの“ Recovery HD ”パーティションをクローンするには、[についてのよくある質問](http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition) <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-cloning-apples-recovery-hd-partition>>

Notes for VoiceOver users

CCC's main window is divided into three main sections. At the top is a toolbar, and beneath that there is a split pane divided vertically. The view on the left is called the sidebar, the view on the right holds the task configuration view. When you open CCC for the first time, the sidebar is hidden. The sidebar is automatically revealed when you add a new task.

The sidebar is split horizontally. The top half contains a table of backup tasks, the bottom half lists locally-attached volumes on your Mac. When you select a task in the task list, the details of that task are presented in the right pane of the window. Likewise, if you select a volume from the list in the bottom of the sidebar, the details of that volume are presented in the right pane. CCC requires that you save any changes you have made to a task before selecting another task or a volume, so if you switch away from a task that is currently being edited, you will be prompted to save unsaved changes, revert the task to its on-disk state, or cancel the event that would have changed the task selection.

Navigation challenges and solutions

The "Automatically interact when using tab key" setting in VoiceOver Utility > Navigation can make navigation to CCC's task configuration view quite challenging. If you prefer to leave this setting enabled, we recommend that you hide CCC's sidebar to avoid navigation challenges. You can use CCC's View menu to select tasks and volumes (in other words, the contents of the View menu completely replaces the need for the sidebar).

Quick Nav

The Tab key will effectively move your cursor to each control in CCC. With Quick Nav enabled (to enable it, simultaneously press the left and right arrow keys), you can also navigate through non-control user interface elements, such as labels, scroll views and split view dividers. Largely this is quite intuitive, however there is one place where the order of elements as interpreted by the window is not very intuitive. This is only applicable when the sidebar is revealed -- if the sidebar is hidden, focus goes to the source selector, and the following is irrelevant.

Upon launch, CCC places focus on the tasks table. The task configuration view lies to the right of the tasks table, so you would think that you could use the right arrow key to move focus to the task configuration view. However, the tasks configuration view is ordered in front of the tasks table, so you must use the left arrow key to get from the tasks table to the task configuration view. Alternatively, use the Tab key.

Simple Mode

Simple Mode significantly reduces the number of user interface elements -- the sidebar, toolbar, scheduling selector, and advanced settings are all suppressed, leaving the user three primary controls: Source, Destination, Clone button. For users that desire a basic ad hoc clone from one volume to another, this simplified interface is the perfect solution.

CCCとそのヘルパーツールにフルディスクアクセスを許可するには

macOS Mojaveには、特定のアプリケーションデータ (例：メール、メッセージ、Safari、写真) へのアクセスをデフォルトで許可しないという新しいプライバシーの制限が加わりました。これまでもカレンダーや連絡先などのアプリケーションに関連するデータに制限が課されていましたが、これらの以前の制限とは異なり、macOS Mojaveは権限アプリケーション (CCCのファイルコピー機能など) にも同様にこれらの制限を課すようになりました。macOS Catalinaではこれらのプライバシーの変更内容がさらに広く適用され、アプリケーションはいかなる外部ハードドライブおよびネットワークボリュームにもアクセスできなくなりました。

さらに複雑なことには、macOSは、アプリケーションがそのデータにアクセスを試みる時、アプリケーションにアクセスを許可するかをユーザに確認しないということです。その代わりに、事前にアプリケーションを承認するための長い手続きを完了するよう要求されます。その結果、最も貴重なデータをバックアップするために特別にアプリケーションをダウンロードしても、あなたがそのデータへのアクセスを許可するように手続きを完了するまでそのアプリケーションはそのデータをバックアップできません。

CCCとそのヘルパーツールにフルディスクアクセスを前もって許可しておくには、Carbon Copy Clonerメニューから “ CCCにフルディスクアクセスを許可...” を選択してください。



CCCにフルディスクアクセスを許可

アプリケーションデータ (例：メール、カレンダー、メッセージ等) をバックアップするには、CCCとそのヘルパーがそのデータにアクセスできるように許可してください。

- こちらをクリックして“セキュリティとプライバシー”を開く
- カギのアイコンをクリックして変更を許可
- 以下の魚アイコンをフルディスクアクセスの表にドラッグ
- CCCを終了するか質問された時に“後で”を選択



ステップ3でこのアイコンをドラッグ

次回から確認しない

CCCのインストールアシスタントは、上のスクリーンショットが示すように、CCCとそのヘルパーツールにフルディスクアクセスを許可できるように、事前の承認手続きを案内します。まず、ボタンをクリックしてシステム環境設定の “ セキュリティとプライバシー ” のパネルを開きます。CCCは直接 “ プライバシー ” タブに移動して、フルディスクアクセスのカテゴリーを選択します。次に、 “ プライバシー ” ウィンドウの左下のカギアイコンをクリックして、変更を許可してください。次に、CCCのインストールアシスタントから魚のアイコンを “ プライバシー ” ウィンドウの表にドラッグしてください。このアイコンはMac上で、Carbon Copy Clonerのアプリケーションとその権限ヘルパーツールの、2つの別のファイルを表します。そのため、これをプライバシーの表にドロップすると、 “ Carbon Copy Cloner.app ” と “ com.bombich.ccchelper ” の両方がその表に表示されます。CCCのヘルパーツールにフル

ディスクアクセスを許可すると、CCCはインストールアシスタントを終了して、インストールアシスタントを実行する前にしていたタスクを再開します。この時点で、システム環境設定を閉じて構いません。CCCを今すぐ終了するか、後にするかを確認された場合、“後で”を選択することができます。

CCCのクローニングコーチは、CCCのヘルパーツールがデータの一部にアクセスできない場合に警告を表示します

起動ディスクをタスクのバックアップのためのソースとして選択し、かつCCCの権限ヘルパーツールにフルディスクアクセスをまだ許可していない場合、そのタスクを保存または実行する際にCCCのクローニングコーチから注意喚起が表示されます。クローニングコーチから出される“アクセスを許可...”のボタンをクリックすると、CCCは上のスクリーンショットに示されている、インストールアシスタントを表示します。

同様に、CCCの権限ヘルパーツールにフルディスクアクセスを許可しないでバックアップタスクを続け、CCCが何かしらをバックアップできない場合、CCCのタスク履歴ウィンドウで注意喚起のエラーが、“アクセスを許可...”のボタンと共に表示されます。

“Carbon Copy Clonerをフルディスクアクセスのカテゴリに追加しましたが、まだエラーが表示されます”

Carbon Copy Clonerのアプリケーションをフルディスクアクセスのリストに追加することは直感的なようです。残念ながら、アプリケーションが権限ヘルパーツールを利用する場合、Appleのプライバシー対策は直感的な方法では動作しません。高度な権限をもつタスク(例：起動ディスクをバックアップする)を実行するためのAppleのベストプラクティスに従い、CCCはバックアップタスクのすべての局面を管理するために権限ヘルパーツールを利用します。そのため、フルディスクアクセスが必要なのはCCCの権限ヘルパーツール("com.bombich.ccchelper")であって、メインアプリケーションではありません。CCCとそのヘルパーツールにフルディスクアクセスを許可した後、フルディスクアクセスの表は以下のように見えるはずですが：



関連ドキュメント

- CCCの権限ヘルパーツールとは何ですか? <<http://bombich.com/ja/ja/kb/ccc5/what-cccs-privileged-helper-tool>>

手動でCCCの権限ヘルパーツールにフルディスクアクセスを許可

アクセシビリティのために、ドラッグ&ドロップが困難な場合は、以下のステップに従って、CCCの権限ヘルパーツールにフルディスクアクセスを許可してください。

1. システム環境設定の“セキュリティとプライバシー”のパネルを開きます
2. “プライバシー”タブをクリックします
3. 左下のカギのアイコンをクリックして変更を許可します
4. カテゴリの中から **フルディスクアクセス** をクリックします
5. + ボタンをクリックします
6. 起動ディスクのルートレベル (例: Macintosh HD) > ライブラリ > PrivilegedHelperTools と進みます
7. com.bombich.ccchelper を選択します
8. **開く** をクリックしてください

ESET Cyber Securityがプライバシー環境設定パネルと干渉することがある

ESETソフトウェアが環境設定の“セキュリティとプライバシー”の“プライバシー”タブの設定の変更を妨げるという報告を数件受け取っています。“フルディスクアクセス”のカテゴリに項目を追加できない、かつESETをインストールしているという場合は、CCCとそのヘルパーツールにフルディスクアクセスを許可する前に、一時的にESETをアンインストールしてください。CCCにフルディスクアクセスを許可した後、ESETを再インストールすることができます。

私のMacはHFS+フォーマットされたボリュームから起動していて、フルディスクアクセスリストに変更を加えられません

現在の起動ディスクがHFS+フォーマットされている場合、macOSは“プライバシー”のデータベースに変更を加えることを許可しません。バックアップをHFS+フォーマットされたボリュームに作成する前に、CCCにフルディスクアクセスを許可しておかないと、そのボリュームから起動中、CCCにフルディスクアクセスを許可することはできません。その結果、CCCはお使いのユーザデータの大部分を復元できなくなります。以下の方法でこの問題を解決してください:

1. ディスクユーティリティを使用してコピー先ボリュームをAPFSとして消去する
<<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>>
2. macOS Mojaveをダウンロード <<https://itunes.apple.com/us/app/mac-os-mojave/id1398502828?mt=12>>して、macOSをコピー先ボリュームにインストールする
3. 移行アシスタントを使って、データをHFS+フォーマットのバックアップから新しくインストールされたMojaveに移行する

移行が完了したら、CCCを開いて、新しい起動ディスクを元の(オリジナルの)バックアップディスクにバックアップするタスクを設定してください。この時、先に進む前にCCCにフルディスクアクセスを与えておく、今後、再インストールと移行アシスタントの手間を省くことができます。

CCCとそのヘルパーツールにフルディスクアクセスを前もって許可しておくには、Carbon Copy Clonerメニューから“CCCにフルディスクアクセスを許可...”を選択してください。

macOSのシステムボリュームをApple Software Restoreを使ってクローンするには

macOS Big Sur (11.0)以降、システムは暗号で封印された "署名付きのシステムボリューム"

<https://developer.apple.com/news/?id=3xpv8r2m>

にあります。その封印はAppleだけが適用でき、システムボリュームの通常のコピーはAppleのシールがないと起動可能にはなりません。macOS 11のシステムボリュームの機能するコピーを作成するには、Appleのツールを使用してシステムをコピーするか、またはバックアップにmacOSをインストールする必要があります。お使いのMacの起動ディスクの初期の起動可能なバックアップを確立

するために、CCCは独自のファイルコピー機能を使用できません。Big Surの起動ボリュームのクローンを作成するためのバックアップタスクをCCCに設定すると、CCCはAppleのAPFSレプリケータ ("ASR") を使って、初期クローンを作成します。以降のバックアップでは、CCCは独自のファイルコピー機能を使い、MacのDataボリュームから異なる内容のみをコピーします。

最初のバックアップタスクを設定する際に予測しておくべきこと

APFSボリュームグループ (例: macOS Big Surの起動ディスク)

をタスクのソースとして選択し、コピー先がすでに確立されたBig Surボリュームでない場合、CCCは選択中のコピー先の設定内容に応じて、タスクをどのように続けるか、いくつかのオプションを提示します。推奨するのは、1つのボリュームをバックアップタスク専用にしておくことです。というのは、そのボリュームはいずれ起動可能なバックアップを確立するために消去される必要が出てくるからです。

コピー先を消去

このオプションを選択すると、CCCはAppleのAPFSレプリケータを使って、選択中のソースを選択中のコピー先にクローンするようタスクを設定します。タスクを開始すると、コピー先は即座に消去されます。SafetyNetはこの設定には適用されません。ですから、空のボリューム、または、削除されても大丈夫なデータが入っているボリューム (例: 古いバックアップ) が選択されていることを、必ず確認してください。

ボリュームを追加

選択中のコピー先がAPFSフォーマットされたボリュームで、かつ、そのボリュームのコンテナがソースボリュームの完全なバックアップを収容するのに十分な容量がある場合、CCCはコピー先のAPFSコンテナにボリュームを追加するオプションを提供します。このオプションを選択すると、選択中のコピー先は消去されません。代わりに、CCCはコピー先に新しいボリュームを追加して、その新しいボリュームをソースの専用バックアップとして使用します。

データみのバックアップ

選択中のソースの起動可能なバックアップを作成できない、または作成する必要がない、かつ同時に選択中のコピー先を消去したくない場合は、**データのみ**

のオプションを選択できます。このオプションを選択すると、CCCは選択中のソースのデータボリュームをタスクのソースとして選択し、選択中のコピー先は消去しません。このオプションは、既存の暗号化されたバックアップボリュームがあり、それを消去や暗号化しないで使い続けたい場合、便利です。データみのバックアップは起動可能ではありませんが、[これらのバックアップを "移行アシスタント" にソースとして使用することができます](http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#migrate) <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#migrate>> (例:

データをmacOSのフレッシュなインストールに移行する)。

よくある質問

タスクの実行が始まると、コピー先がソースと同じ名前に変更されました。そして、この“ASR DataVolume”ボリュームとは何ですか？

非常に鋭い方なら、Appleのボリュームレプリケータが動作し始めると、コピー先ボリュームの名前が変わることに気が付いていることでしょう。CCCのサイドバーにも追加のボリュームが表示されているかもしれません。これは正常なことです。これらのボリュームは“ボリュームグループ”に集約され、1つのボリュームとして表示されるので、複製が完了すると、CCCはコピー先を元の名前に変更します。

AppleのAPFS複製ユーティリティが失敗し、ASRDataVolume、またはASRNewVolumeが持続されているのを確認した場合、ディスクユーティリティでそれらの痕跡のあるボリュームを削除できます。単純にそれらのボリュームを選択してから、ツールバーの“-”ボタンをクリックしてください。

起動可能なバックアップを作成するには、コピー先を消去する必要がありますか？

お使いのMacがBig Surを実行しているなら、答えは「はい」です。macOS Big Surの時点では、APFSボリュームグループの起動可能なクローンを確立

するために、AppleのAPFSレプリケータを使用することが要求されています。SafetyNet機能を利用できないので、バックアップボリュームに他のデータを保管しておくことは適切ではなくなりました。ボリュームを起動可能なバックアップ専用にしておく必要があります。一旦起動可能なバックアップが確立されると、その後CCCは独自のファイルコピー機能を使って、その後のバックアップタスクでコピー先のDataボリュームをアップデートします。

自分のバックアップディスクを他の目的のためにも使用できますか？

はい。APFSボリュームをコピー先のAPFSコンテナに追加して、その新しいボリュームをCCCの専用バックアップに使用するか、または他のコンテンツのために使用することを推奨します。CCCのバックアップとその他のコンテンツが別のボリュームに保管されている限り、これらは同じ物理的デバイスで平和に共存できます。同様に、コピー先がAPFSフォーマットでなければ、パーティションをバックアップディスクに追加することもできます。例えば、HFS+フォーマットされたボリュームにすでにコンテンツが存在する外部ハードドライブを利用している場合、ディスクにパーティションを追加して、その新しいパーティションをCCCのバックアップに使用できます。

初期のバックアップからコンテンツの一部を除外できますか？

お使いのMacがBig Surを実行している場合は、コンテンツを除外して起動可能なバックアップを作成することは不可能です。初期のバックアップからコンテンツを除外する必要がある場合は、

[データのみバックアップを続ける](http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#create) <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#create>>

ことを推奨します。その後そのバックア

ップを起動可能にしたい場合は、[macOSをバックアップボリュームにインストールしてください](http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#installmacos)

<<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#installmacos>>。

関連ドキュメント

- [コピー先にボリュームまたはパーティションを追加するには](http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#dedicatedvolume) <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#dedicatedvolume>>

私のバックアップディスクにはすでに他のボリュームがあります。それらは消去されますか？

いいえ。“{destination}を消去”のオプションを使って続けると、選択中のコピー先ボリュームのみが消去されます。物理的に同じデバイスにある他のボリュームが影響を受けることはありません。ですが、他のどこにもバックアップされていないデータがあるディスクにバックアップをすることは絶対に推奨しません。それら他のボリュームがまだバックアップされていないのであれば、先に進む前にそのデータをバックアップしてく

ださい。

ボリュームを追加しましたが、その追加のボリュームが結局必要なくなりました。削除できますか？

はい。CCCの“ユーティリティ”メニューから**ディスクユーティリティ**を選択し、削除したいボリュームを選択してください。次に、ツールバーの“-”ボタンを押してそのボリュームを削除してください。

暗号化されたボリュームにクローンできますか？

暗号化されたボリュームをコピー先として選択してもかまいませんが、そのボリュームはいずれ消去され、また、タスクが完了する時点で暗号化されていません。AppleのAPFS複製ユーティリティは、FileVaultをクローンされたボリュームでプリエンティブに有効にすることはありません。コピー先でFileVaultを有効にするには、バックアップボリュームから起動し、環境設定の“セキュリティとプライバシー”でFileVaultを有効にしてください。

関連ドキュメント

- [APFSの複製に関するトラブルシューティング <http://bombich.com/ja/ja/kb/ccc5/troubleshooting-apfs-replication>](http://bombich.com/ja/ja/kb/ccc5/troubleshooting-apfs-replication)
- [FileVault暗号化で作業するには <http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption>](http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption)

データボリュームのバックアップを作成および復元するには

データのためのバックアップはお使いのすべてのデータ、設定、およびアプリケーションの完全なバックアップです

場合によっては、CCCはmacOSの起動ディスクのデータのためのバックアップを作成します。AppleがmacOS Catalinaで導入したAPFSのボリュームグループについて馴染みがない場合には、以下から詳細をご覧ください：

APFSボリュームグループを動作させるには <<http://bombich.com/ja/ja/kb/ccc5/working-apfs-volume-groups>>

データのためのバックアップを作成するために、CCCはそのAPFSボリュームグループ内のDataボリューム全体をコピーします。システムボリューム（その中にはmacOSインストーラによってインストールされた約15GBのみの読み出し専用のシステムファイルが含まれています）、はコピーされません。データのためのバックアップは起動可能ではありませんが、そこにmacOSをインストールすることで、バックアップを起動可能にできます。または、データのためのバックアップをソースとして移行アシスタントに使用できます。

データのためのバックアップを作成するには

場合によっては、CCCはタスクを自動的にデータのためのバックアップに設定することがあります。以下のステップを実行すると、データのためのバックアップを手動で設定することができます。

1. 最終的にバックアップを起動可能にしたい場合は、
[ディスクユーティリティでコピー先ボリュームをAPFSとして消去](http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x#highsierra)
<<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x#highsierra>> してください
2. CCCのツールバーから **サイドバーを表示**のボタンをクリックします
3. CCCのサイドバーからソースセレクトにMacintosh HD - Data ボリュームをドラッグします
4. コピー先セレクトをクリックして、コピー先を選択してください

macOSをデータのためのバックアップにインストールするには

データのためのバックアップが非暗号されたAPFSボリュームにある場合、macOSをバックアップディスクにインストールすることで起動可能にできます。

Intelプロセッサ搭載Mac

1. macOSインストーラをダウンロードして開きます: [[Catalina <https://itunes.apple.com/us/app/macOS-catalina/id1466841314?ls=1&mt=12>](https://itunes.apple.com/us/app/macOS-catalina/id1466841314?ls=1&mt=12)] [[Big Sur <https://itunes.apple.com/us/app/macOS-big-sur/id1526878132>](https://itunes.apple.com/us/app/macOS-big-sur/id1526878132)]
2. ディスクを選択するように促されたら、**すべてのディスクを表示...** をクリックして、お使いのバックアップディスクを選択してください
3. 続けて、macOSをバックアップディスクにインストールしてください

AppleシリコンMac

1. Macをシステム終了してから、起動オプションが読み込まれるまで、パワーボタンを押したままにします
2. “オプション” ボタンをクリック後、“続ける” をクリックしてください
3. Recoveryが読み込まれたら、“macOS Big Surを再インストール” のオプションを選択します
4. 続けて、macOSをバックアップディスクにインストールしてください



移行アシスタントを使ってCCCのバックアップからデータを移行するには

データをCCCのバックアップからmacOSのクリーンなインストールに移行するには、移行アシスタントを利用できます。例えば、起動ディスクが壊れている、または置き換えるのが難しい場合、以下のステップに従ってmacOSを再インストールして、データを復元できます：

1. “ Command+R ” を押したまま(Intel Macの場合)、またはパワーボタンを押し続け (AppleシリコンMacの場合)て、Macを [リカバリーモード <https://support.apple.com/en-us/HT204904>](https://support.apple.com/en-us/HT204904) に起動してください
2. ディスクユーティリティを使って、Macの (新しい) 内部ディスクをAPFS として消去します (詳しい方法は [この Kbase 記事 <http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x#highsierra>](http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x#highsierra) を参照してください)
3. ディスクユーティリティを終了します
4. macOSを再インストール のオプションを選択し、macOSを新しいディスクにインストールします
5. macOSが新しいディスクで最初に起動する際、データを移行するか確認されますので、移行することを承認してください
6. 移行のソースを選択するよう促されたら、CCCのデータのみのバックアップボリュームを選択してください

使用例

ハードドライブ全体を新しいハードドライブまたは新しいコンピュータにクローンしたいのですが。

ハードドライブの正確なクローンを作成するには様々な理由があります。例えば、ラップトップが故障し、修理に出さなければならないとしましょう。その間、別のコンピュータを借りなければならないばかりか、コンピュータ上のデータ、アプリケーション、仕事環境がそっくりそのまま無くなるのです。このような環境の不備は不満がつるばかりか、生産性が損なわれます。コンピュータが修理から戻ってきてからも、貸りたコンピュータで変更されたドキュメントを確認して、自分の元のコンピュータにコピーし直さなければなりません。また、Appleはデータの喪失に責任を負わないため、コンピュータを修理に出す前にデータをバックアップしておくことを勧めています。

このような状況では、ハードドライブの全内容を外部ハードドライブにコピーして、生産性のあるコンピュータの“起動可能なクローン”を作成しておくのが理想的でしょう。そうすれば、この起動可能なクローンから貸りたコンピュータを起動し、自分のコンピュータからのように作業できます（バックアップから別のMacを実行することに関するよくある質問は、以下の関連ドキュメントをご参照ください）。

ハードドライブ全体の、完全でシンプルなバックアップが必要になる時：

1. Carbon Copy Cloner を開きます
2. ソースセレクトからクローンしたいボリュームを選択します
3. コピー先メニューから **正しくフォーマットされたボリューム** <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>> を選択してください
4. “クローン” ボタンをクリックします

将来クローンしたボリュームをアップデートしたい場合、同じタスクを実行（あるいは自動的に実行するようスケジュール）すると、CCCは最後のバックアップ以降変更された項目のみでバックアップをアップデートします。

設定アシスタントまたは移行アシスタントを使用して、CCCのバックアップから新しいMacにデータを移動する

ボリューム全体のクローンを作成するのが理想的と考えられる別のシナリオは、新しいMacを購入し、古いMacから新しいMacにすべてを移動したい時でしょう。しかし、Appleから新しいコンピュータを購入すると、特定のバージョンのmacOSがインストールされていて、さらにハードウェア固有の“ビルド”がインストールされています。新しいMacは、古いMacにインストールされている古いバージョンのmacOSとビルドから起動することができないため、単純に古いMacを新しいMacにクローンしてもうまくいきません。この制限により、設定アシスタントアプリケーション（Macが一番最初に起動する時に実行されます）を使用するか、古いMacから新しいMacに内容を移行できる移行アシスタントアプリケーションを使用することをお勧めします。古いMacのCCCのバックアップから直接移行することができます。設定アシスタントまたは移行アシスタントを使ってユーザアカウントとアプリケーションの移行が完了したら、古いMacで使用していた同じバックアップボリュームにMacをバックアップして、Carbon Copy Clonerを使用し続けることができます。

移行アシスタントとCCC SafetyNet

バックアップボリュームに“CCC SafetyNet”フォルダがある場合、移行アシスタントを使用する前にそのフォルダをゴミ箱に移動して、移行中そのフォルダがコピーされないようにできます。これは、そのフォルダの中に多くのデータがあり、バックアップボリュームよりも小さいディスクに移行している場合、特に重要です。バックアップボリュームにSafetyNetフォルダを保持したい場合、ゴミ箱を空にしないでください。移行アシスタントが完了すると、SafetyNetフォルダをバックアップボリュームのルートに戻すことができます。

Apple Kbase #HT2186 : Macの出荷時に搭載されていたMac

OSを使用するか、互換性のある新しいバージョンを使用してください <<https://support.apple.com/kb/HT201686>>

Apple Kbase #HT204350 : コンテンツを新しいMac [Mavericksおよびそれ以降]に移動

<<https://support.apple.com/kb/HT204350>>

Apple Kbase #HT3322 : 移行アシスタントを使用して別のMacからファイルを転送するには [LionおよびMountain Lion] <<https://support.apple.com/kb/ht3322>>

関連ドキュメント

- 1台のコンピュータをバックアップし、そのクローンを使用して別のコンピュータを復元できますか？
<<http://bombich.com/ja/ja/kb/ccc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer>>

データをTime Capsule、NAS、またはその他のネットワークボリュームにバックアップしたい

Time Capsuleやその他のネットワークストレージアプリケーションは“個人用クラウド”ストレージ共有を提供することで、大変人気を得ています。当然、このストレージはバックアップのコピー先として魅力的に映ります。ケーブル接続なしですべてをバックアップできるという考えに心を奪われそうになるでしょう。事実、このストレージはメディアファイルの共有には非常に適しています。しかし、これらのデバイスに大容量のデータをバックアップするのは、実用的にも物理的な移動の観点からも障害があります。例えば、macOSのシステムファイルをNASにバックアップすることは推奨しません。この設定には、あまりにも多くの移動の問題と信頼性に関する懸念が伴います。以下に、データをネットワークボリュームにバックアップする方法を説明します。その後、この方法が持つ制限とパフォーマンスの予想をご説明します。

起動の可能性 (bootability) について： 起動可能なバックアップを必要とするのであれば、**またはシステムファイルを復元する必要がある** この先1度でもあるとすれば、Macに直接接続された**外部ハードドライブエンクロージャ** <<http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive>> を使用して、起動可能なバックアップを作成する必要があります。

データをネットワークボリュームにバックアップするには

先に進む前

に、お使いのNASボリュームをFinderにマウントしてアクセスできるようにしてください。

ネットワークボリュームへのアクセス権を得るための手順は、macOSヘルプセンターから利用できます。ネットワークボリュームがCCCのソースまたはコピー先メニューに表示されない場合、アクセスしたいストレージデバイスに添付されたドキュメントを参照するか、Finderのヘルプメニューから“ヘルプセンター”(Yosemite以降は“Macヘルプ”)を選択し、“サーバに接続する”を検索してください。

CCCを使ってホームフォルダをNASボリュームにバックアップするには:

1. ソースセレクトから**フォルダを選択**を選択します。
2. ホームフォルダをソースとして選択してください(ショートカット: Commandキー + Shiftキー + Hを押してホームフォルダに移動できます)。
3. コピー先セレクトから**フォルダを選択**を選択してください。
4. NASボリュームに移動してから、**新規フォルダ**をクリックしてこのボリュームに新規フォルダを作成してください。“CCCバックアップ”などと名前を付けてください。“OK”ボタンをクリックしてください。
5. **高度な設定**ボタンをクリックします。
6. より良いパフォーマンスのためには、**拡張属性を保持しない**の横のチェックボックスをチェックしてください。
7. **クローン** ボタンをクリックしてすぐにタスクを実行するか、または後でタスクを実行するようスケジュールしてください。

ネットワークボリュームにバックアップする際のパフォーマンスの予想

“利便性”と“速さ”は通常相伴うものですが、ネットワークボリュームへのバックアップに関しては必ずしも当ては



まるものではありません。バックアップのパフォーマンスを劇的に低下させる要因がいくつかある中で、このバックアップ方法にはその要因が複数含まれています。ネットワークのバックアップが遅いと気づいた場合には、[ネットワークのバックアップのトラブルシューティング](http://bombich.com/ja/ja/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume) <<http://bombich.com/ja/ja/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume>>をお考えください。

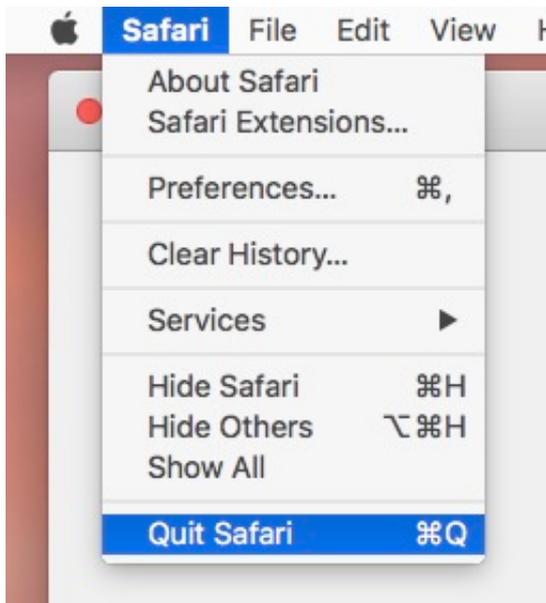
Restoring an item from a hidden folder

This article is primarily written for users running macOS Yosemite or El Capitan. If you are running macOS Sierra or later, simply press Command+Shift+Period (`⇧ .`) to toggle the Finder's display of hidden items, then you can easily navigate to the hidden items in the Finder and restore those items via drag and drop.

Usually it's easiest to restore a single item from your backup by simply dragging it from the backup volume to your original source volume. Sometimes, though, it's not that easy. Suppose, for example, that you have inadvertently deleted all of your Safari bookmarks. The Safari Bookmarks file is stored in a hidden folder within your home directory, and the fact that this folder, and the folder on the backup volume are both hidden makes accessing that file in the Finder quite difficult. The steps below demonstrate how to restore this item from your Carbon Copy Cloner backup volume.

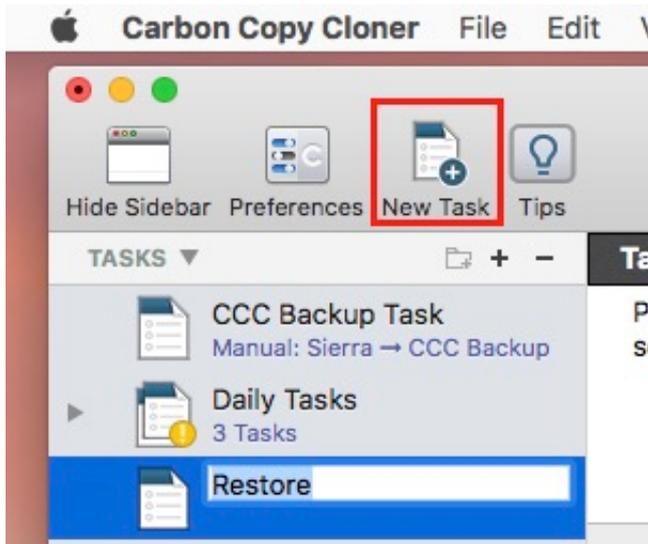
Quit Safari

Before you restore any files that are referenced by a particular application, you should quit that application first.



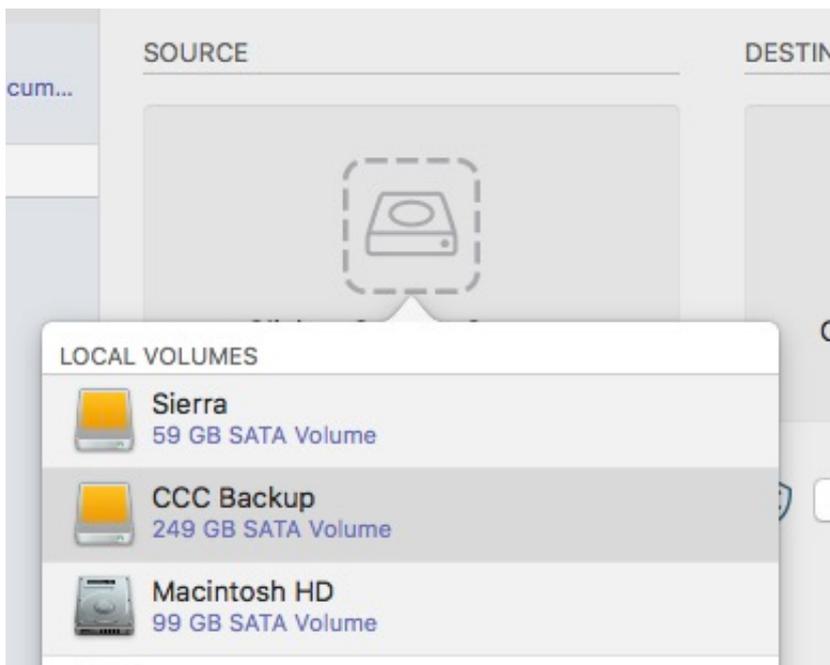
Open CCC and create a new task

Rather than making changes to your usual backup task, click the "+" button to create a new task. You can delete the task when you're done.



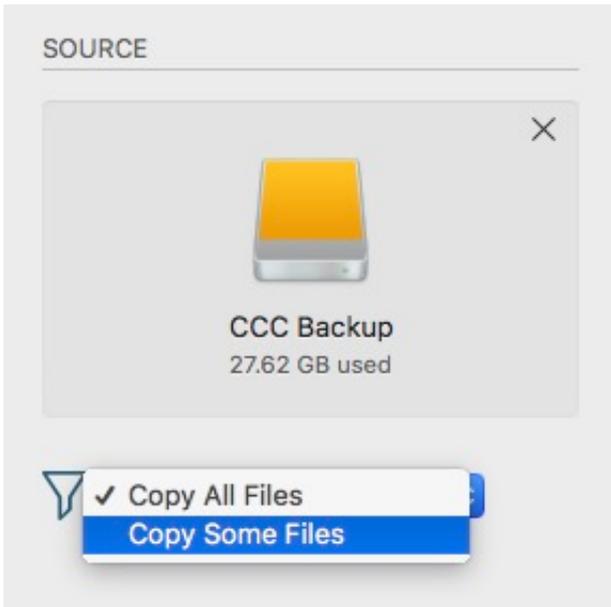
Select your backup volume as the source

Click on the Source selector and choose your backup volume as the source.



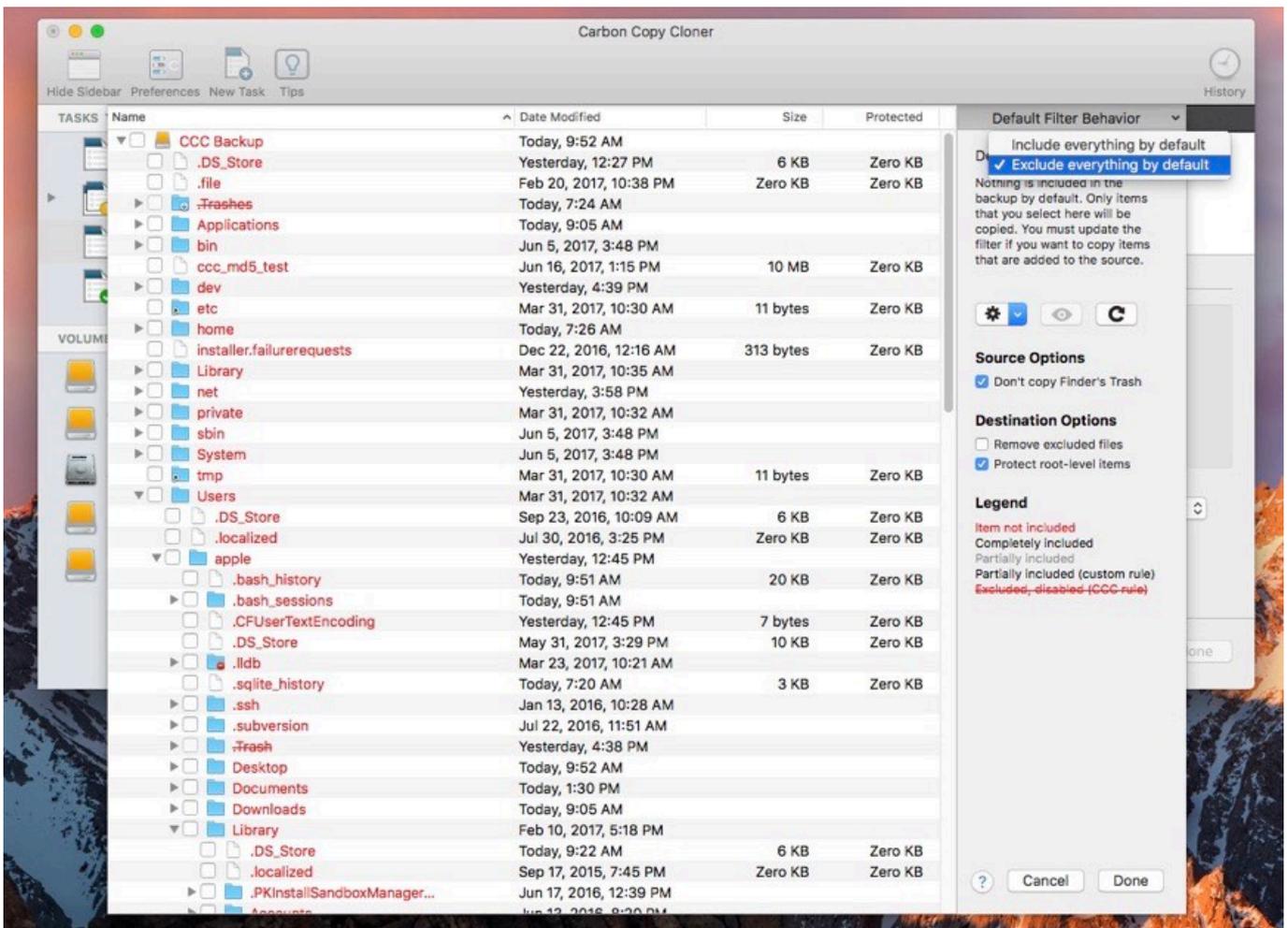
Choose "Some Files..." from the Clone popup menu

We don't want to restore everything, so choose the "Some Files..." option in the Clone popup menu.



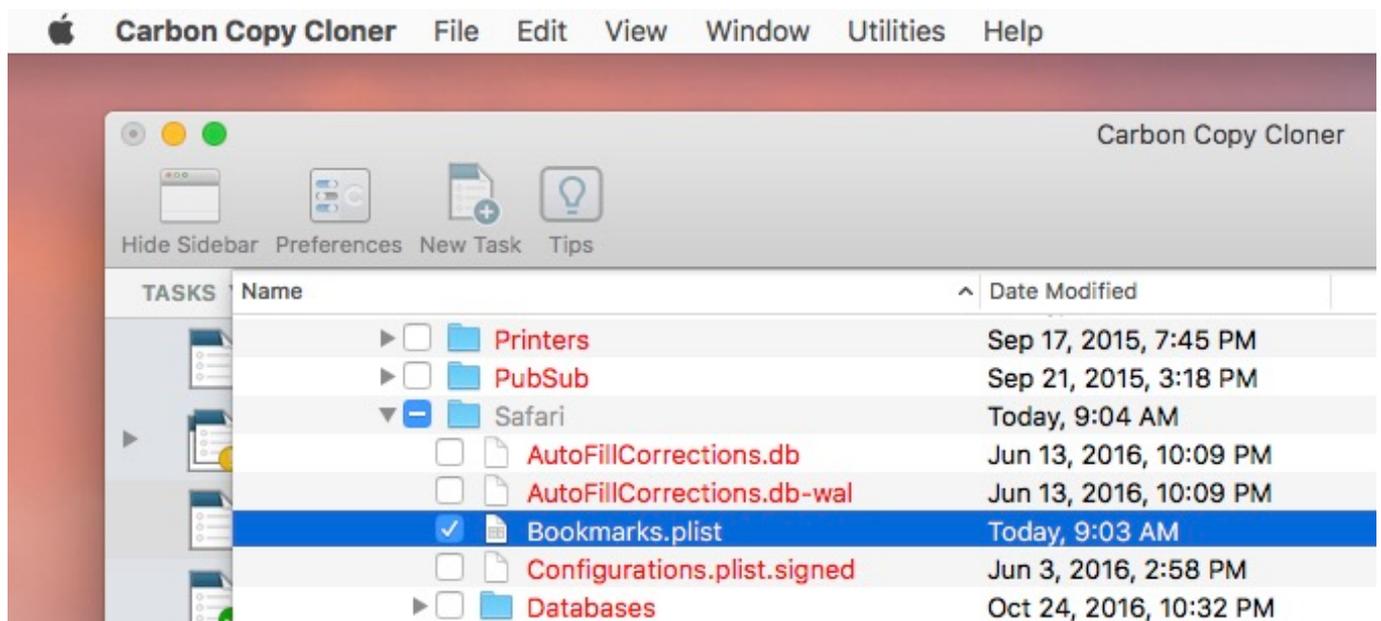
Exclude everything by default

We're only restoring a single item, so change the task filter's default behavior to "Exclude everything by default".



Navigate to the desired folder and select the item you would like to restore

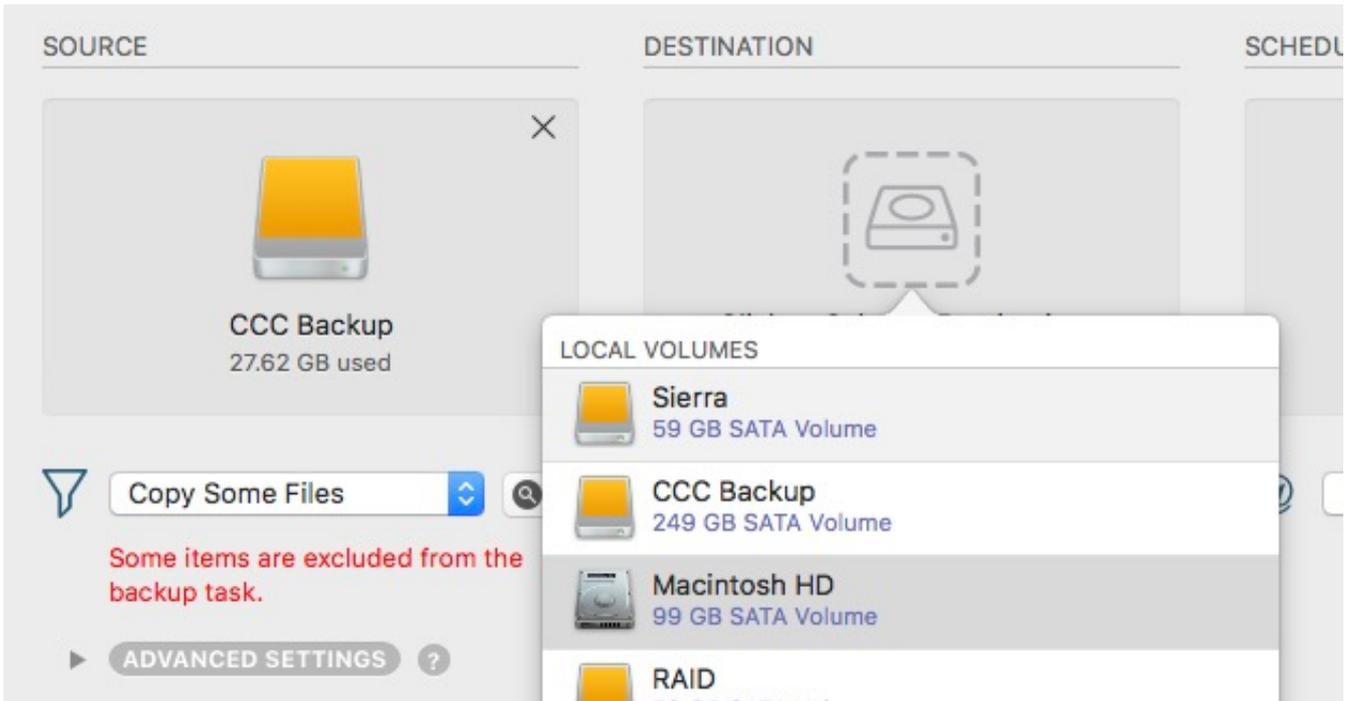
Start opening disclosure triangles next to the folders that you would like to descend into until you reach the item you want to restore. In this case, the path is Users > apple > Library > Safari. The Library folder is hidden in the Finder, but CCC makes it visible here so you can restore items from it.



Check the box next to the item you want to restore. Bookmarks.plist is the file we're trying to restore in this case.

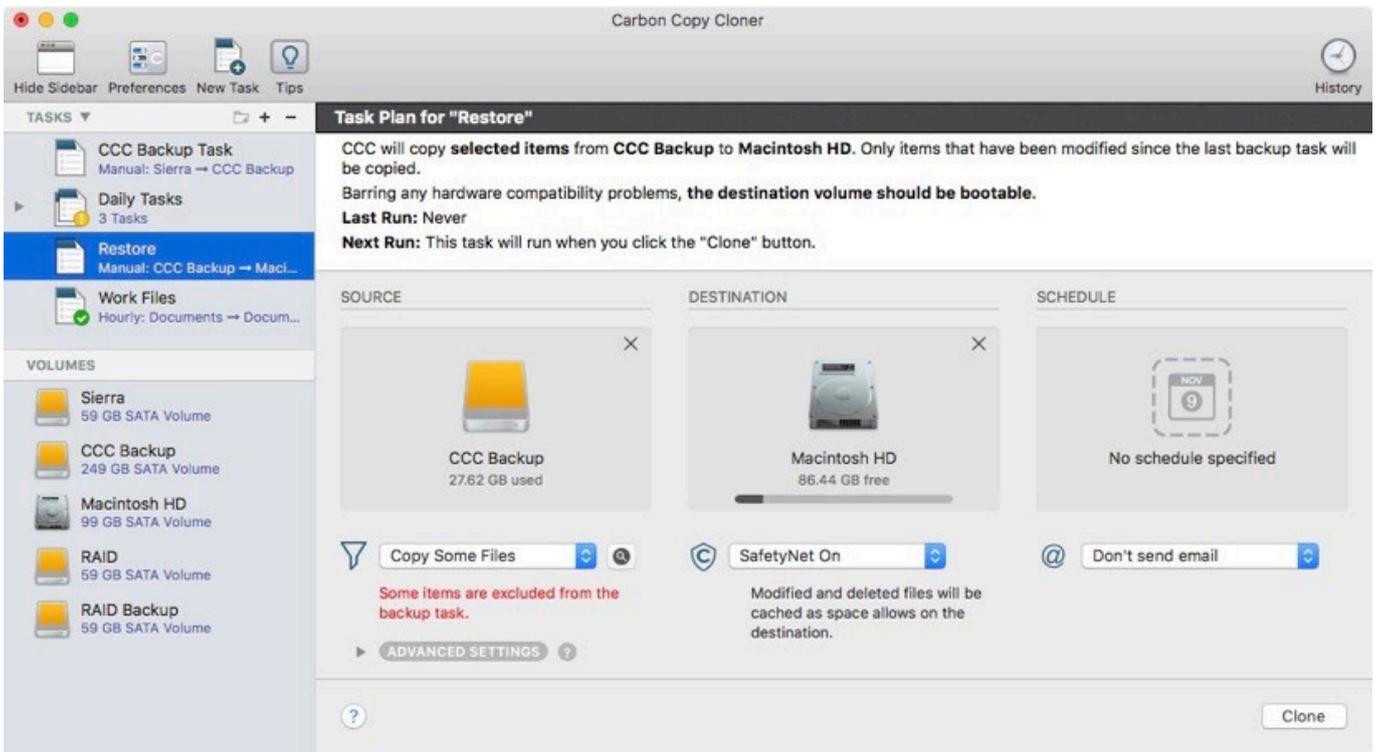
Select the volume to restore to as the destination

In this case, we want to restore the item back to the startup disk, so choose Macintosh HD from the destination selector. When you select your startup disk as the destination, CCC will produce a stern warning about restoring files to the startup disk. To prevent accidentally restoring system files to an active startup disk, CCC will explicitly exclude system files from this restore task. In this case, we can ignore the dialog because we already excluded everything except for the single file.



Click the Clone button

This restore task will go really quickly, and when it's done you can open Safari to verify that your bookmarks have been restored.



Cloning one external hard drive to another external hard drive

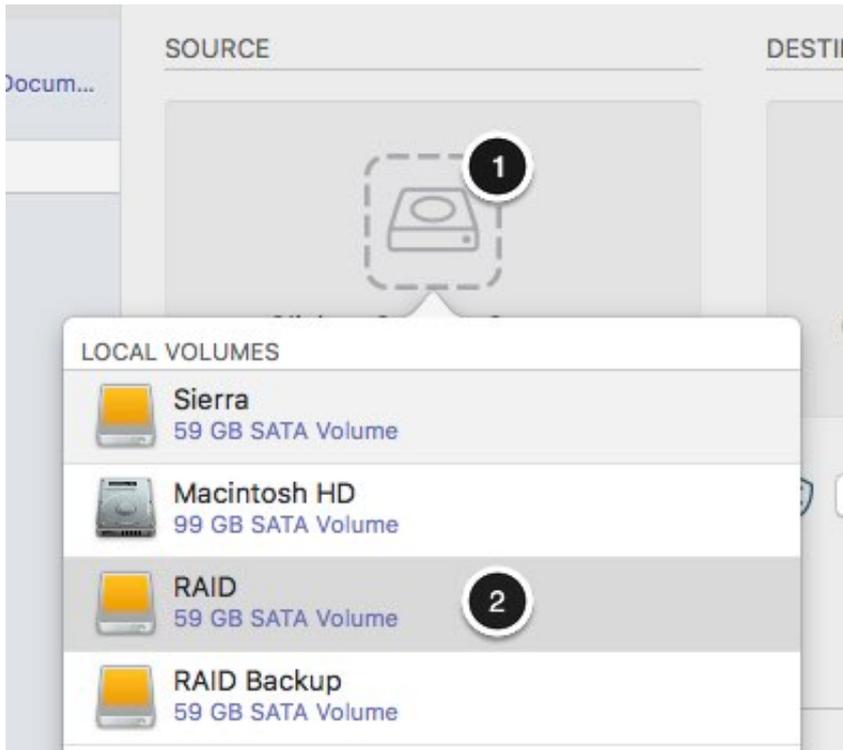
Create a new task

Click on the New Task button in the toolbar to create a new task, then type in a name for the new task.



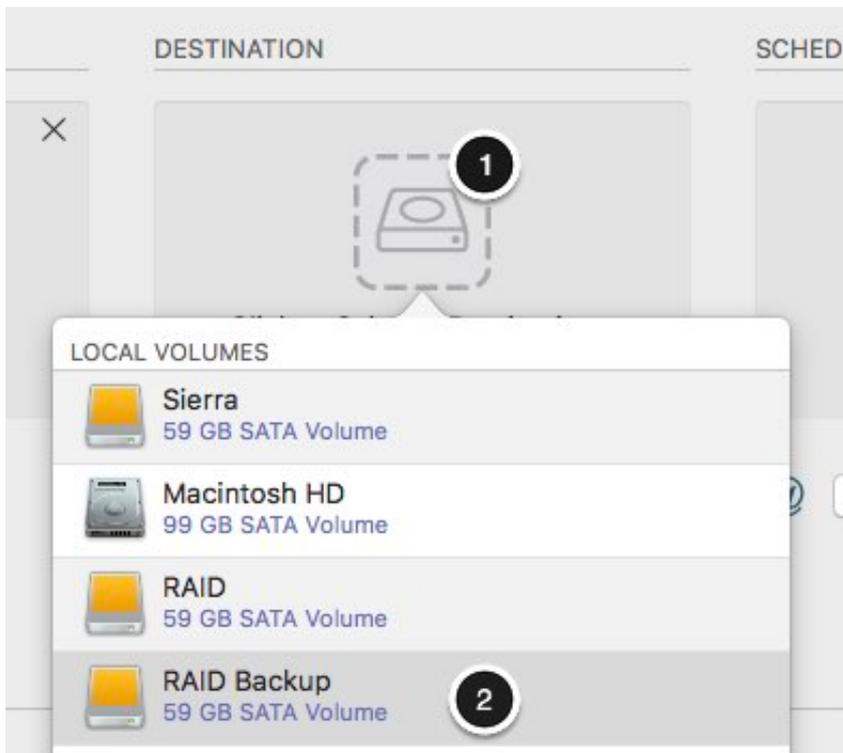
Select a source volume

Click on the Source selector button, then choose the volume that you want to copy files from.



Select a destination volume

Click on the Destination selector button, then choose the volume that you want to copy files to.



Click the Clone button

Click the Clone button to copy files right away, or click the Scheduler selector to configure the task to run on a

regular basis.

Related Documentation

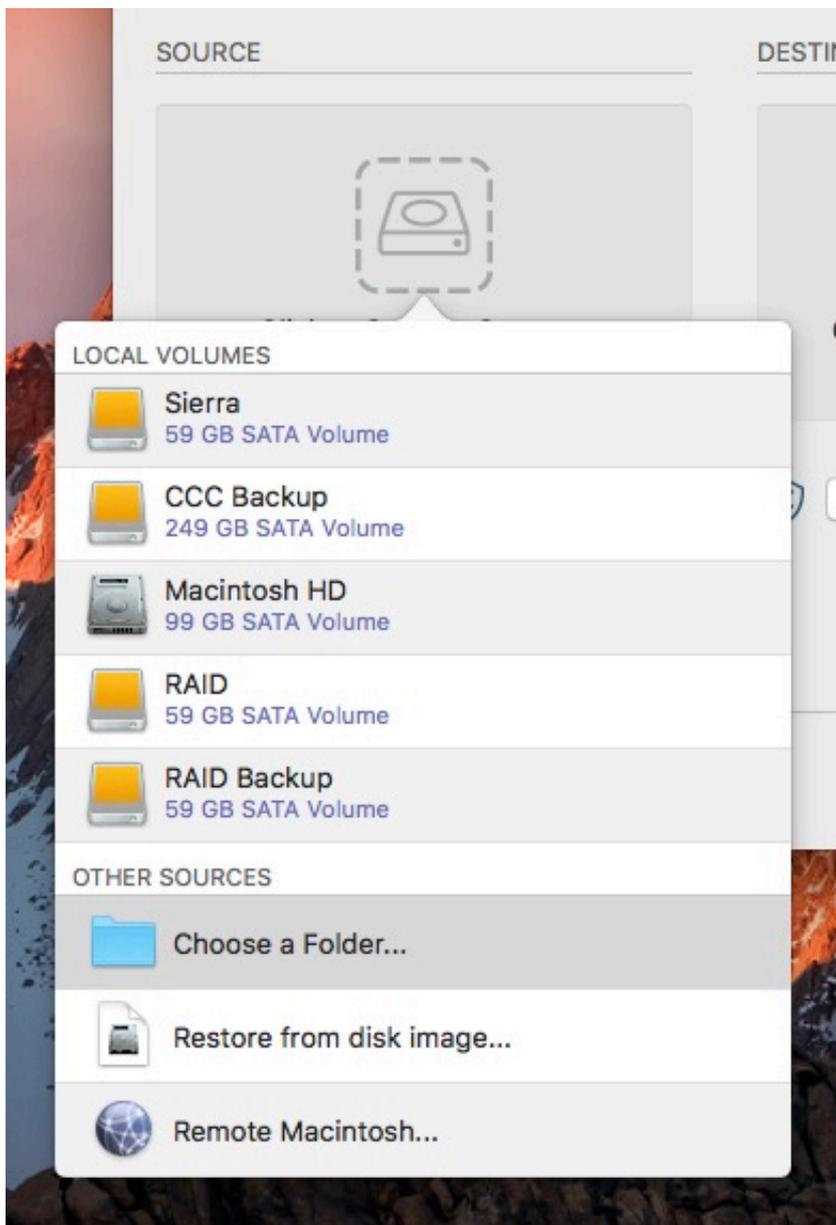
- [How to set up a scheduled backup <http://bombich.com/kb/ccc5/how-set-up-scheduled-backup>](http://bombich.com/kb/ccc5/how-set-up-scheduled-backup)

Folder-to-Folder Backups

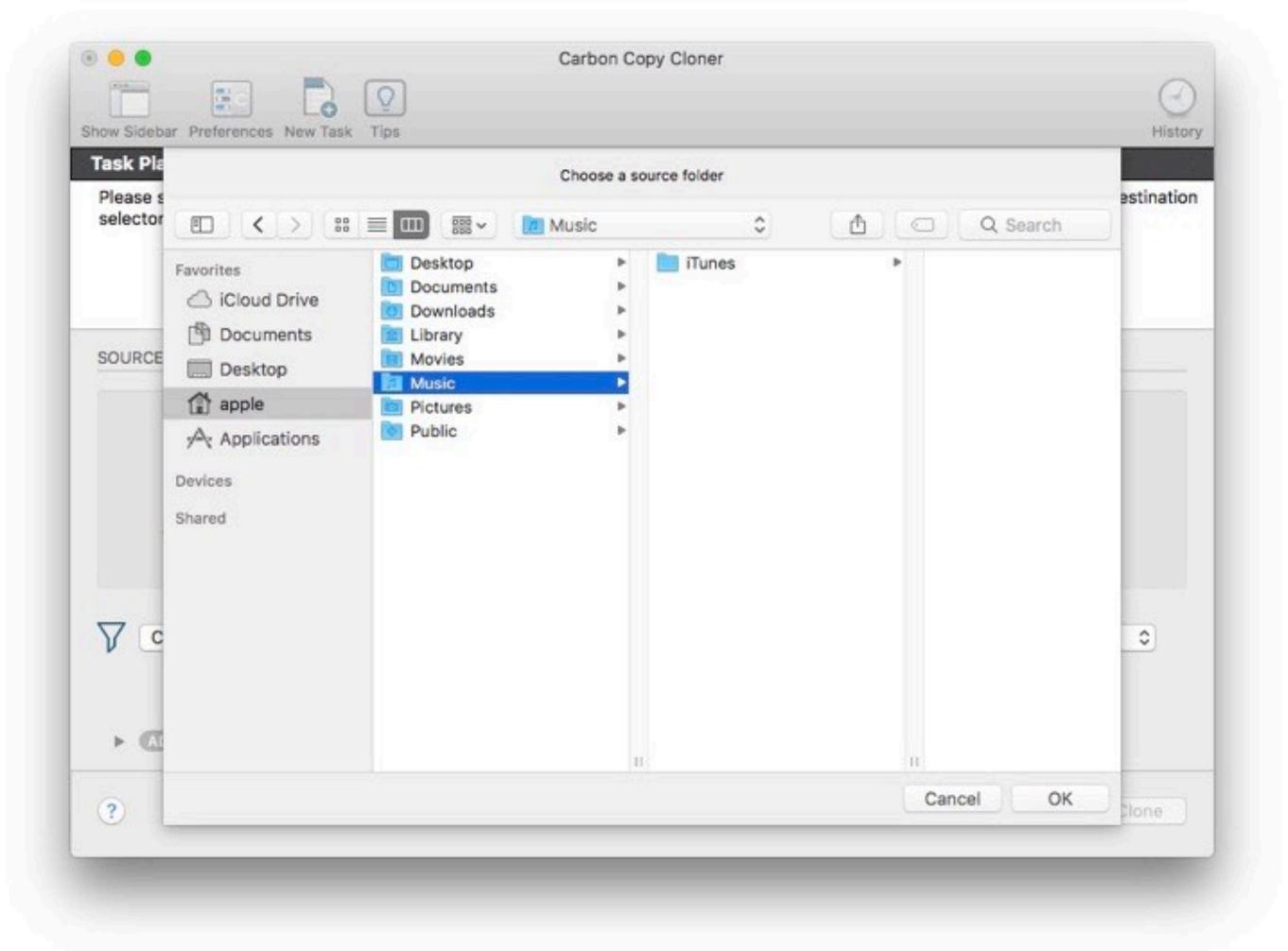
When you select a volume as the source and destination, CCC copies the entire contents of that volume (minus anything you exclude) to the destination volume, preserving the full hierarchy of folders on the source. If you don't want to preserve that hierarchy, you can back up a specific folder from the source to a specific folder on the destination. In this configuration, CCC will copy the contents of the selected folder to the selected destination folder, without the hierarchy up to that source folder.

Choose your source

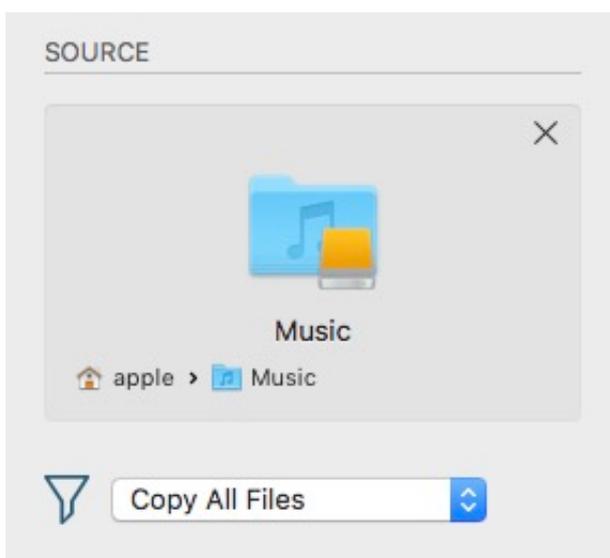
From the Source selector, select Choose a Folder...



Select your source folder and click OK.

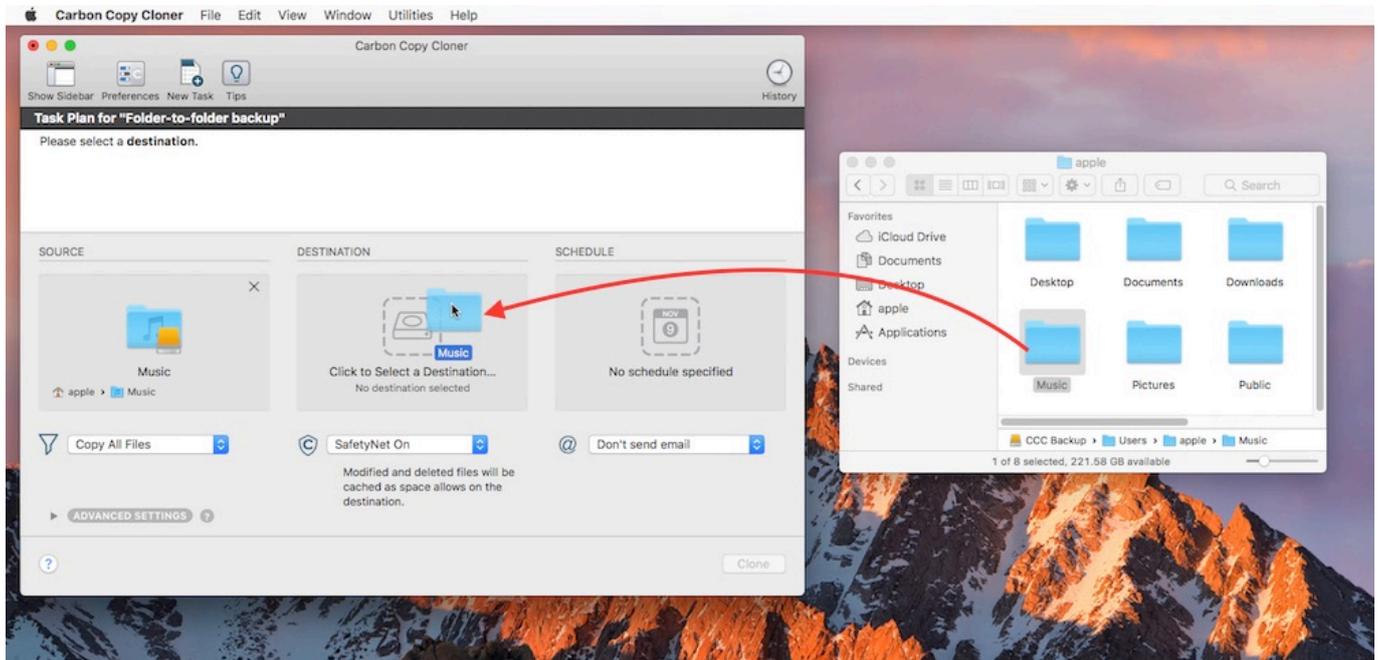


When correctly selected, the Source selector should display a folder icon and a path to the folder beneath it. Note that this path may be truncated but if you mouse over it, individual items will be expanded. You may choose to Copy All Files, the default, or define a task filter by choosing Copy Some Files from the Filter popup menu.

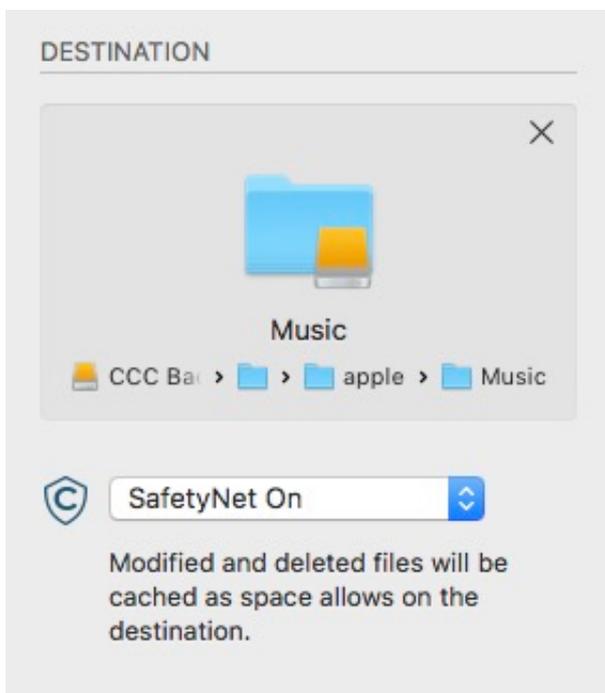


Choose your destination

The steps used to select the source need to be repeated for the destination. CCC also supports drag and drop selection, so we'll demonstrate that here. Find your destination folder in the Finder, then drag it onto CCC's Destination selector.



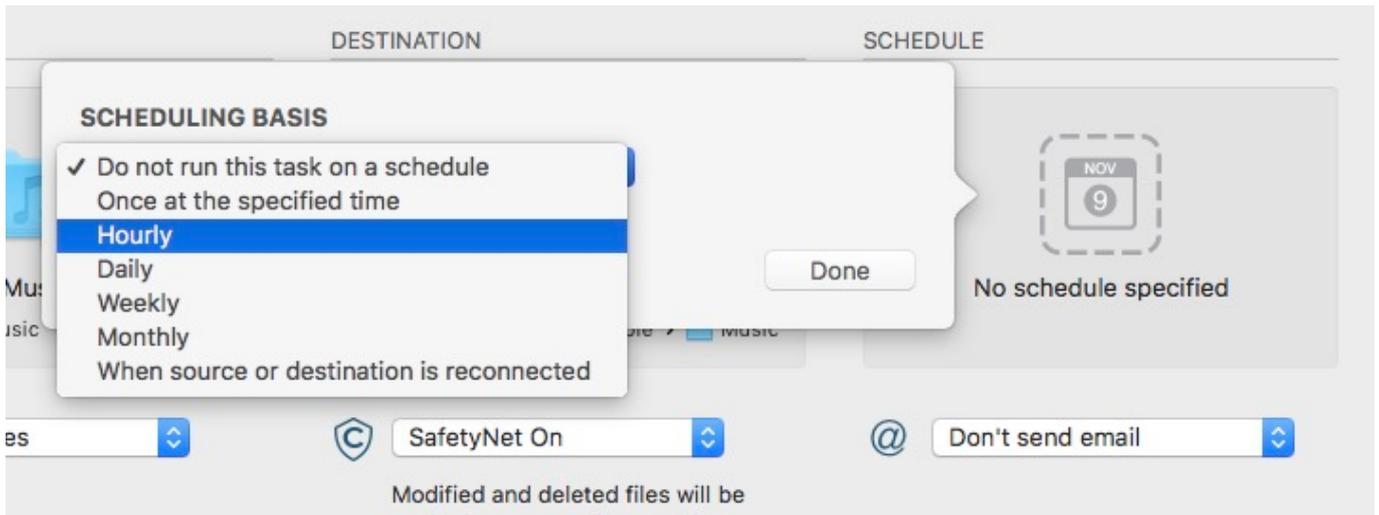
Once you have selected the destination folder, the Destination box should have a folder icon in it with the path displayed beneath it. You may choose to leave SafetyNet on or turn it off. To learn more about SafetyNet, please see [Protecting data that is already on your destination volume: The Carbon Copy Cloner SafetyNet](http://bombich.com/kb/cc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet) <<http://bombich.com/kb/cc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>>.



Schedule the backup

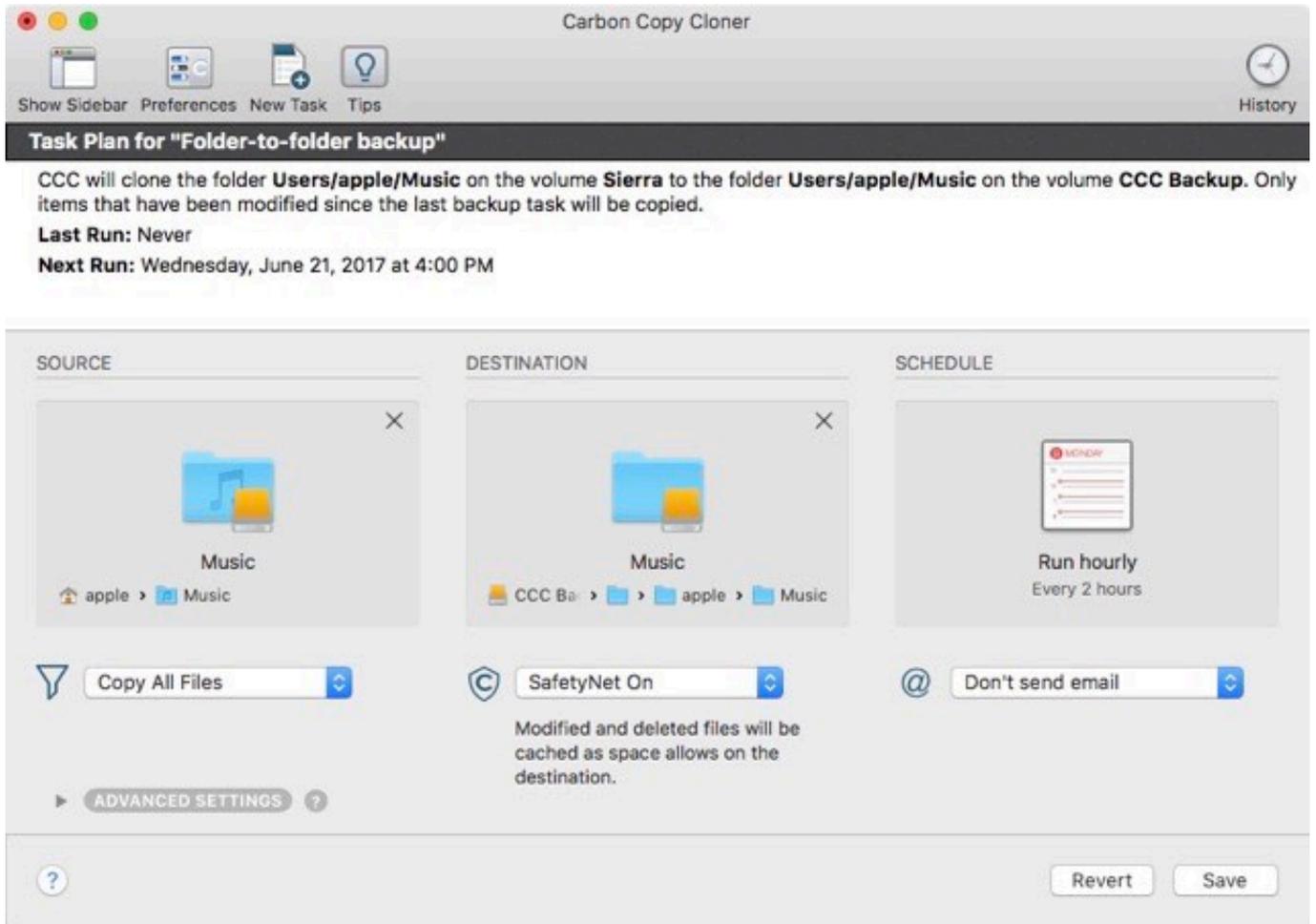
Click in the Schedule box and design a backup schedule that meets your needs. Click Done when you have

finished.



Save and clone

Once you have your source, destination and schedule complete, click on Save in the bottom right-hand corner. This will save the task and you can find it in the tasks area on the left sidebar. If you don't see the sidebar, click on Show Sidebar in the CCC window header. You may click the Clone button to run the backup manually, or let it run on a schedule.





Backing up and restoring Finder's Trash

Backing up Trash content

CCC will not back up the contents of Finder's Trash by default, but CCC 5 offers an [option to back up the Finder's Trash](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task#trash) <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task#trash>> in the Task Filter window. Choose Copy Some Files from the popup menu underneath the Source selector to reveal CCC's Task Filter window.

The Trash is not a simple folder, it's a complex mechanism that aggregates Trash folders from multiple volumes and user home folders on the startup disk; it behaves quite unlike other folders. When you back up the contents of the Trash, those items are copied to the Trash folder on the destination, and may reside in "the Trash" as viewed in the Finder. If you subsequently empty the Trash, that will delete the Trash on the backup disk if it is mounted when you empty the Trash. If you choose the option to back up the Finder Trash, we recommend that you unmount and detach your backup disk before emptying the Trash if you wish to retain the Trash on the backup disk.

Restoring Trash content

If you eject your backup disk and detach it from your Mac, and then you empty the Trash, you can simply reattach the backup disk to your Mac and the Trash will again appear to be filled. You can simply drag items out of the Trash to recover those items.

The Trash is a little bit more complicated than that

For external data-only volumes, the Trash behaves in the fairly straightforward manner previously described. For your startup disk, though, it's not quite that simple. There is more than one Trash folder on the startup disk, e.g. there is a Trash folder in each user's home folder. When you move an item (that you are the owner of) on your startup disk to the Trash, that item is placed in your home folder's Trash, not in the volume's trash folder. It still appears in "the Trash", but its location is important with regard to the backup. Suppose you do the following:

1. Move an item from your Desktop to the Trash
2. Run a backup
3. Detach your backup disk
4. Empty the Trash
5. Reattach your backup disk

Result: That item is not in the Trash! The file is actually in a Trash folder on the backup disk, but the Finder doesn't show you items in the home folder trash folders on external volumes. In this scenario, you can [boot from your backup volume to recover the item](http://bombich.com/kb/ccc5/how-restore-from-your-backup) <<http://bombich.com/kb/ccc5/how-restore-from-your-backup>>, because once booted from the backup volume, that item will appear in the Trash.

You can also recover an item from a user home folder Trash folder on the backup volume using the procedure described here: [Restoring an item from a hidden folder](http://bombich.com/kb/ccc5/restoring-item-from-hidden-folder) <<http://bombich.com/kb/ccc5/restoring-item-from-hidden-folder>>. The hidden Trash folder is located at /Users/{yourname}/.Trash.

Refining the scope of a backup task

Watch a video of this tutorial on YouTube <<https://youtu.be/mctdmbKLgNY>>

We often see backup tasks configured with the whole startup disk selected as the source, and then everything excluded from the backup except for a single folder. This kind of configuration is suboptimal for several reasons:

- The entire folder hierarchy up to the non-excluded folder is preserved, so it takes longer to navigate to your files on the destination.
- With the startup disk selected, CCC may perform unnecessary subtasks related to making a bootable backup on the destination.
- The task involves more overhead (e.g. evaluating lots of exclusion rules), so it will take longer.
- The scope of the task is very broad; CCC's effects are applicable to the whole destination rather than to a single folder.
- If the destination is a folder on the startup disk or on a non-Apple formatted volume, then the task will likely produce errors related to preserving special file flags of folders on the startup disk.

A better configuration is to create a folder-to-folder backup. With a specific folder selected as the source and a specific folder selected as the destination, you greatly reduce the scope of the task, thus reducing the amount of work that the task has to do and also reducing any risks to other content on the destination.

Converting a whole-disk, single folder task to a folder-to-folder backup

For the sake of an example, let's suppose you selected Macintosh HD as the source for a backup task, then chose "Copy some files" and excluded everything except for Users > yourname > Documents > Work In Progress. Let's also suppose that you selected a volume named CCC Backup as the destination for this task. If you navigate to the CCC Backup volume in the Finder, you will find a folder hierarchy of Users > yourname > Documents > Work In Progress. To convert this backup configuration to a folder-to-folder backup, you would do the following:

1. Navigate to the CCC Backup volume in the Finder
2. Navigate to Users > yourname > Documents > Work In Progress
3. Move the Work In Progress folder to the root level of the CCC Backup volume
4. Move the (now containing empty folders) Users folder to the Trash
5. Open CCC and select the relevant backup task
6. Drag the Work In Progress folder from the CCC Backup volume onto CCC's Destination selector
7. Drag the Work In Progress folder from your home folder on the Macintosh HD volume onto CCC's Source selector
8. Save the task

Related Documentation

- [Folder-to-Folder Backups <http://bombich.com/kb/ccc5/folder-folder-backups>](http://bombich.com/kb/ccc5/folder-folder-backups)



トラブルシューティング

macOS Big Sur Known Issues

Some Big Sur startup volumes don't appear in the Startup Disk Preference Pane

In the past, the Startup Disk Preference Pane would list all available startup volumes, including volumes cloned by CCC (whether CCC used ASR or its own file copier). Some Big Sur cloned volumes do not appear in the Startup Disk Preference Pane, despite being perfectly bootable.

We have reported this issue to Apple (FB8889774) and we are currently awaiting a response.

Workaround: To boot from the cloned volume, restart your Mac while holding down the Option key, then select the cloned volume in the Startup Manager. When your Mac has completed booting, you can optionally choose to set the startup disk to the current startup volume (i.e. if you want the Mac to always boot from the cloned volume).

CCC will not update the System volume on a Big Sur bootable backup

Starting in macOS Big Sur, the system now resides on a cryptographically sealed "[Signed System Volume](#)" <https://developer.apple.com/news/?id=3xpv8r2m>. That volume can only be copied using Apple's proprietary APFS replication utility ("ASR"). Right now, ASR will only copy whole volume groups (System and Data), we can't choose to clone just the System volume. As a result, every time an OS update is applied to the source, we would have to erase the whole destination volume ([including any existing snapshots on that volume](#) <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>) just to update the system on the destination.

To avoid deleting your snapshots and the rest of your backup, CCC will not update the System volume on the destination when System updates are applied to the source.

We made a feature request to Apple in September 2019 (FB7328230) to allow ASR to clone just the System volume. Apple's APFS team acknowledged the request in June 2020 and clarified the requirements, and now we're waiting on the implementation.

Our recommendation: We recommend erasing the destination only for the purpose of establishing the initial bootable backup. CCC can then use its own file copier to maintain the backup of your user data, applications, and system settings. If you would like to update the OS on the backup volume, you can boot your Mac from the backup and apply any updates via the Software Update preference pane in the System Preferences application. This is not something that we anticipate you would need to do frequently, nor even proactively. You could apply updates before attempting to restore from the backup, for example, if that need ever arises.

Apple Software Restore doesn't yet support the storage in Apple Silicon Macs

In the current shipping version of macOS Big Sur (11.2.3), Apple's ASR utility cannot replicate the startup disk in an M1-based Mac. Attempting to do so results in an error:

'Apple System Restore Tool': Source volume format not yet supported in this version of macOS

Apple is aware of the problem and is working towards resolving it for a future update to macOS. CCC 5.1.23+ will automatically perform Data Volume backups on M1 Macs and avoid any attempts to copy a System volume on those Macs — that's a complete backup of your data, applications, and system settings. If you would like to make your Apple Silicon Mac backup bootable, you can [install Big Sur onto the CCC Data Volume backup](#) <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#installmacos> . Please keep in mind, however, that [your CCC backup does not have to be bootable for you to be able to restore data from it](#) <http://bombich.com/kb/ccc5/creating-and-restoring-data-only-backups#migrate>.

When Apple posts an update to macOS that resolves the ASR problem, we'll post an update to CCC that adds back support for copying the System volume on these Macs.

Finder will not show, nor allow you to set custom icons on other Catalina and Big Sur startup disks

Finder will show and allow you to customize the volume icon for your current startup disk, but not for other Catalina- or Big Sur-bearing startup disks that your Mac is not currently booted from. This problem is not specific to CCC backups, but we see this frequently because CCC creates bootable backups. This problem is the result of a design flaw in the implementation of custom icons in an APFS volume group. Up to macOS Catalina, the custom volume icon is stored in a file at the root of the startup disk named ".Volumelcon.icns". To keep the System volume read-only, yet allow the apparent modification of this icon file, Apple chose to create a symbolic link at the root of the startup disk that points to System/Volumes/Data/.Volumelcon.icns. For the current startup disk, this path resolves correctly because the Data member of the volume group is mounted at /System/Volumes/Data. That's not the case for external volumes, those Data volumes are mounted at /Volumes/CCC Backup - Data (for example). As a result, the symbolic link to .Volumelcon.icns is unresolvable for any volume that is not the current startup disk.

We have reported this issue to Apple (FB7697349) and we are currently awaiting a response.

Other Catalina and Big Sur startup disks can't be renamed in the Finder

Finder will let you rename the current startup disk, but you won't be able to rename any other startup disks that have an installation of Catalina or Big Sur because the System volume is mounted read-only.

Solution: Unmount and remount the volume in Disk Utility, then right-click on the volume in Disk Utility's sidebar and choose the option to rename the volume.

We have reported this issue to Apple (FB8912480) and we are currently awaiting a response.

The System volume is not encrypted when FileVault is enabled on a Big Sur startup disk

This is not a bug, this appears to be a deliberate change on macOS Big Sur. When you enable FileVault on a Big Sur startup disk, the System volume member of the APFS volume group is not encrypted. Considering that this volume is identical on all Macs, encrypting its contents is not going to prevent someone from knowing what's on it, so the encryption does appear to be unnecessary. There is one undesirable effect of this change, however, regarding an encrypted, bootable backup disk. When you attach the device to your Mac, the System volume is mounted automatically, regardless of whether you unlock the associated Data volume. If you specifically choose to not unlock the Data volume, there are three results that range from confusing to annoying to alarming:

- The volume appears to be mounted in the Finder, despite not wanting to mount it
- None of the data on the volume is accessible because the Data volume isn't mounted, so you might be led to believe that your data has been lost
- There is no apparent way in the Finder to get the Data volume unlocked and mounted

You can unlock and mount the Data volume in Disk Utility to access the data. If you provided the volume's password to CCC, then you can simply run your CCC backup task and CCC will automatically unlock and mount the Data volume.

We have reported this issue to Apple (FB8918177) and we are currently awaiting a response.

Apple's SMB filesystem client causes system stalls on M1 Macs, leads to kernel panics

We have received several reports from M1 Mac users of kernel panics that occur while copying files to an SMB-mounted NAS volume. The kernel panic reports have confirmed that the SMB filesystem client (implemented via

the smbfs.kext kernel extension) was stalled, which led to a ["watchdog" panic](#). These panic reports are automatically submitted to Apple, so we can presume that Apple is aware of the problem and working on a solution.

Workaround: Users have reported that using AFP rather than SMB consistently works around the panic (in cases where using AFP is an option):

1. Eject the NAS volume if it's currently mounted
2. Choose "Connect to Server" from the Finder's Go menu
3. Type in "afp://{server address}" to connect to the NAS volume via AFP
4. Open CCC and select the applicable backup task
5. Drag the currently-mounted NAS volume (or folder or disk image on that volume) onto CCC's source or destination selector (whichever is applicable for your particular task)

macOS Catalina Known Issues

Apple introduced a bug in 10.15.5 that prevents the creation of firmlinks

The `chflags` system call no longer works correctly on 10.15.5 with regard to setting the special "firmlink" flag that establishes links between the System and Data volume group members. If you're establishing a new backup of macOS 10.15.5 or later, CCC 5.1.17 (and earlier) will be unable to create a correctly-functioning APFS volume group. Many folders on the destination volume will appear empty, and the volume will not be bootable.

Solution: Update to macOS 10.15.6 and CCC 5.1.20. See [this blog post for more details](http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered) <<http://bombich.com/blog/2020/05/27/bug-in-macos-10.15.5-impacts-bootable-backups-weve-got-you-covered>>.

We have reported this issue to Apple (FB7706647) and we are currently awaiting a response. Update: Apple resolved this issue in macOS 10.15.6. Apple made this "bug" a permanent change, however, in macOS Big Sur.

Some SMB volumes can't support macOS sparse disk images

We have received several reports that macOS is unable to create disk images on SMB volumes hosted by various NAS devices. If you attempt to create the disk image in Disk Utility (for example), Disk Utility reports an "RPC Error". After months of investigation, we have concluded that macOS Catalina has more stringent requirements for sparse disk images than previous OSes.

Solution: Several users have reported that [adjusting the SMB configuration on the NAS to support Time Machine](https://kirb.me/2018/03/24/using-samba-as-a-time-machine-network-server.html) <<https://kirb.me/2018/03/24/using-samba-as-a-time-machine-network-server.html>> can resolve the problem. Time Machine also uses sparse disk images on NAS volumes, so its requirements for the NAS file sharing service would be the same as those required for generic sparse disk image support.

Workaround A: Several users are reporting that connecting to the network volume via AFP rather than SMB resolved the problem:

1. Eject the NAS volume if it's currently mounted
2. Choose "Connect to Server" from the Finder's Go menu
3. Type in "afp://{server address}" to connect to the NAS volume via AFP
4. Choose "New disk image..." from CCC's Destination selector and specify a new disk image on the AFP-mounted NAS volume

Workaround B: If connecting to your NAS volume via AFP is not an option, then you can back up user data (e.g. your home folder) directly to the NAS volume (i.e. don't use a disk image). We also recommend disabling support for extended attributes (via the Advanced Settings).

We recommend using NAS devices for secondary backups. For primary backups, we recommend that you procure a USB or Thunderbolt hard drive and create a bootable backup on that locally-attached disk. Local, bootable backups are much simpler and more reliable, and a lot easier to restore from should your Mac's startup disk fail. The logistics of restoring the operating system from a disk image on a network volume are pretty complicated if you don't have a functional startup disk. Providing that functional startup disk is the primary appeal of the CCC backup solution.

2012-vintage Macs can't boot macOS Catalina from an encrypted USB device

We have received several reports that the 2012 Mac mini and the 2012 MacBook Pro can initially boot from a non-encrypted external USB device, but then will fail to boot from that device when FileVault is enabled on the external device. This issue is not specific to CCC, we have confirmation that this occurs when installing Catalina directly

onto an external device as well. This problem does not appear to be specific to any particular enclosure, rather it appears to be specific to the 2012 models of Mac mini and MacBook Pro.

We have reported this issue to Apple (FB7433465) and we are currently awaiting a response.

macOS Catalina will not boot from a FireWire device

Apple has dropped support for booting from FireWire devices. The macOS Catalina Installer will explicitly disallow installation onto a FireWire-attached device, and if you attempt to boot macOS Catalina from a FireWire-attached device, the startup process will fail with the universal "no entry" symbol.

Solution: If your external device also has a USB interface, attach the device to your Mac using a USB cable instead.

Workaround: If your external device does not have a USB interface, you can continue to make backups to that device, but they will not be bootable while that device is attached via Firewire. If you need to restore data from this backup, you can either place the external hard drive into a different hard drive enclosure, or you can migrate the data to a fresh installation of macOS Catalina via the Migration Assistant application. If you prefer to maintain bootable backups, you should purchase an enclosure that will be bootable with macOS Catalina. We offer [specific hard drive recommendations here](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations) <<http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>>.

Emerging issue: Higher incident rate of macOS Catalina failure to boot from Western Digital My Passport enclosures

We have received several reports now of Western Digital My Passport hard drive enclosures failing to function as a startup disk with macOS Catalina. In all cases the end user was able to [confirm that the macOS Installer was also unable to make the device bootable](http://bombich.com/kb/ccc5/help-my-clone-wont-boot#installmacos) <<http://bombich.com/kb/ccc5/help-my-clone-wont-boot#installmacos>> . The results are inconsistent — in some cases the system proceeds approximately 75% into the startup process, then shuts down. In other cases the system transparently boots to the internal disk, and in other cases (probably most) the enclosure boots fine. Due to the number of cases of confirmed failed bootability, however, we discourage users from purchasing new WD My Passport HDD enclosures if your intent is to create a bootable macOS Catalina backup. Please note that the WD My Passport SSD is NOT included among these reports. WD My Passport enclosures with a rotational HDD should be avoided.

[Specific hard drive recommendations](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations) <<http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>>

Mount issues render USB thumb drives unsuitable for bootable backups

[We have discouraged the use of thumb drives in the past](http://bombich.com/kb/ccc5/choosing-backup-drive#notrecommended) <<http://bombich.com/kb/ccc5/choosing-backup-drive#notrecommended>> due to performance and reliability issues related to making these devices bootable. In the past the macOS loginwindow service has prevented CCC from mounting the APFS helper partitions on these devices. Now that the Catalina System and Data volumes are also special APFS volumes, we're seeing the same sort of interference from the loginwindow service, although now it leads to failures in backing up the Data volume. We are no longer offering support for these devices as bootable backups. You're welcome to create a non-bootable backup of your Catalina Data volume instead:

1. Open CCC and click the Show Sidebar button in CCC's toolbar if it is not already visible
2. Select your backup task in the sidebar
3. Drag the Macintosh HD - Data volume from CCC's sidebar into the Source selector
4. Save the task

Startup Disk Preference Pane doesn't show OS versions for external volumes

The System Preferences application lacks full disk access by default, so it cannot read the System Version file on

external volumes for the purpose of presenting the system version string underneath the volume icons. Ironically, System Preferences has the privilege to change the startup disk, but it can't make a read-only access to the system version file on external volumes.

Solution: Open System Preferences > Security & Privacy > Privacy, click the padlock icon and authenticate when prompted, then add the System Preferences application to the Full Disk Access category.

We have reported this issue to Apple (FB6723060) and we are currently awaiting a response.

Spotlight's "mds" helper aggressively prevents volume unmount requests

During our Catalina testing we repeatedly had trouble unmounting volumes in Disk Utility, particularly when erasing a backup volume. Upon closer inspection we found that an mds process is nearly always the process that is preventing the unmount. We've seen this [occasionally in the past <http://bombich.com/kb/ccc5/why-cant-i-eject-destination-volume-after-backup-task-has-completed>](http://bombich.com/kb/ccc5/why-cant-i-eject-destination-volume-after-backup-task-has-completed), and for a long time CCC's option to unmount the destination volume at the end of a backup task has worked around the occasional Spotlight dissent with a followup forced-unmount. In Catalina, however, the problem seems to be far worse, affecting nearly every casual unmount attempt (except in the Finder, oddly).

Workaround for general unmount annoyances: You can disable Spotlight on your CCC backup volume to avoid its interference (and for better performance in general). To disable Spotlight, open the Spotlight preference pane in the System Preferences application, click on the Privacy tab, then drag the backup volume into the Privacy table. This only affects the destination volume, and it's reversible, you can remove it from that list should you decide that you want to re-enable indexing.

Workaround when attempting to erase a volume: If you're trying to erase a volume in Disk Utility and Disk Utility is reporting that it cannot unmount the volume to erase it — brace yourself for this one — unmount the volume before erasing it. That's right, Disk Utility can't walk and chew gum at the same time. If you unmount the volume before erasing it, though, the unmount request typically succeeds and you are then able to erase the volume.

We have reported this issue to Apple (FB6905679) and we are currently awaiting a response.

Apple's volume group manipulation tool doesn't work with encrypted volumes

To create a bootable backup of a macOS Catalina volume, CCC must create a volume group at the destination. If your existing destination is a FileVault-protected volume (e.g. container a backup of Mojave), that destination can't be converted into a volume group — Apple's diskutil utility will fail, e.g.:

```
apple@Apollo ~% diskutil ap addVolume disk8 APFS "CCC Backup" -passphrase apple -groupWith disk8s1 -role S
```

```
Will export new encrypted APFS Volume "CCC Backup" from APFS Container Reference disk8
```

```
Started APFS operation on disk8
```

```
Preparing to add APFS Volume to APFS Container disk8
```

```
Error: -69475: You cannot request initial encryption while creating a new APFS Volume to be added to an APFS Volume Group
```

Considering the error message, this appears to be intentional behavior. However, we have submitted an enhancement request Apple (FB7418398) and we are currently awaiting a response.

Workaround: You can [temporarily decrypt your destination volume or erase it as APFS <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversionencrypted>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversionencrypted) , then re-enable FileVault after establishing the initial backup of macOS Catalina.

Related documentation

- [Will my encrypted backup volume be automatically converted to an APFS volume group? <http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversionencrypted>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversionencrypted)
- [Working with FileVault Encryption <http://bombich.com/kb/ccc5/working-filevault-encryption>](http://bombich.com/kb/ccc5/working-filevault-encryption)
- [Frequently Asked Questions about encrypting the backup volume <http://bombich.com/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>](http://bombich.com/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume)
- [What if I don't want my personal data to ever be on the destination in unencrypted form? <http://bombich.com/kb/ccc5/working-filevault-encryption#highestsecurity>](http://bombich.com/kb/ccc5/working-filevault-encryption#highestsecurity)

Disk Utility fails to create a volume group on T2 Macs when the startup disk is encrypted

Similar to the issue described above, we have discovered an edge case in which Disk Utility fails to create an APFS volume group on the internal SSD of a T2 Mac when the current startup disk is encrypted. The typical scenario in which we see this is when the Mac is booted from an encrypted backup volume, and the user is attempting to restore the backup to the freshly-erased internal SSD. Unlike the issue described above, this failure occurs when the destination is not encrypted — it appears to be specific to the current startup disk being encrypted, which seemingly should not play a role at all in the creation of a volume group on an unrelated device.

We have reported this issue to Apple (FB7477894) and we are currently awaiting a response.

Workaround A: Decrypt the backup volume

We don't want to even suggest this solution given the hassle that most users have had to endure to get their backups re-encrypted after the Catalina upgrade, but this will effectively work around the bug in Disk Utility:

1. Boot your Mac from the backup volume
2. Disable FileVault in the Security & Privacy Preference Pane
3. Wait for decryption to complete
4. Reboot — this step is important
5. Perform the restore and reset the startup disk
6. Re-enable FileVault on the backup volume, then reboot from the restored internal disk

Workaround B: Boot your Mac from another macOS Catalina volume that is not encrypted

The problem is not specific to the backup volume that you would like to restore from, rather Disk Utility only fails when the current startup disk is encrypted. If you can boot your Mac from another non-encrypted startup disk, you can restore your encrypted backup volume to the internal disk of your T2 Mac.

When you eject the destination in the Finder, Finder prompts to unmount other volumes that you can't see

When you make a bootable backup of a macOS Catalina system volume, the destination will consist of two volumes arranged in a volume group. Finder shows only one of these volumes, but both volumes are mounted as a pair. When you ask the Finder to eject your destination volume, Finder will indicate that other volumes on that device are mounted, and will ask if you want to unmount all volumes:

"CCC Backup" is a volume on a disk that has 2 volumes. Do you want to eject "CCC Backup" only, or both volumes?

Finder doesn't tell you the identity of the other volume, which makes the decision a bit difficult to make. Rest assured, though, that the other volume is the hidden Data volume associated with your backup. You should unmount both volumes to avoid any Finder admonitions when you physically detach the backup disk from your Mac.

Solution: Click the Eject All button when prompted to unmount both the System and Data volumes.

We have reported this issue to Apple (FB7422542) and we are currently awaiting a response.

Finder will not show, nor allow you to set custom icons on other Catalina startup disks

Finder will show and allow you to customize the volume icon for your current startup disk, but not for other Catalina-bearing startup disks that your Mac is not currently booted from. This problem is not specific to CCC backups, but we see this frequently because CCC is designed to create bootable backups. This problem is the result of a design flaw in the implementation of custom icons in an APFS volume group. Up to macOS Catalina, the custom volume icon is stored in a file at the root of the startup disk named ".Volumelcon.icns". To keep the System volume read-only, yet allow the apparent modification of this icon file, Apple chose to create a symbolic link at the root of the startup disk that points System/Volumes/Data/.Volumelcon.icns. For the current startup disk, this path resolves correctly because the Data member of the volume group is mounted at /System/Volumes/Data. That's not the case for external volumes, those Data volumes are mounted at /Volumes/CCC Backup - Data (for example). As a result, the symbolic link to .Volumelcon.icns is unresolvable for any volume that is not the current startup disk.

We have reported this issue to Apple (FB7697349) and we are currently awaiting a response.

Resolved Issues

On login, macOS fails to unlock and mount the Data volume of an encrypted APFS volume group

If you have an installation of macOS Catalina on a separate volume (e.g. a backup disk) and FileVault is enabled on that volume, the prompt to unlock the volume only unlocks the System volume. If the Data volume is not unlocked and mounted, the volume does not work correctly and the bulk of your data will appear to be missing.

Workaround: You must manually mount the Data volume in CCC (or Disk Utility) to get access to your data on the backup: Right-click the Data volume in CCC's sidebar and choose Mount.

We have reported this issue to Apple (FB6786776) and we are currently awaiting a response.

Update: This issue appears to be resolved in Catalina Beta 7.

The APFS filesystem causes a kernel panic when remounting the System volume in an encrypted APFS volume group

If you unmount and then remount the System volume (or sometimes when you then unmount the System volume again) in an encrypted APFS volume group, the system will kernel panic. CCC will only need to mount or unmount the System volume of the backup disk during a backup task if changes have been made to the source System volume (e.g. after applying a software update). If a kernel panic occurs, simply re-run the backup task after the system reboots to complete the backup.

Partial mitigation: Disabling Spotlight on the destination appears to reduce the incidents of kernel panics. To disable Spotlight, open the Spotlight preference pane in the System Preferences application, click on the Privacy tab, then drag the backup volume into the Privacy table. This only affects the destination volume, and it's reversible, you can remove it from that list should you decide that you want to re-enable indexing.

Update: This issue appears to be resolved in Catalina Beta 9.

System Preferences cannot enable FileVault on external volumes

This is an emerging issue as of Catalina Beta 6. When attempting to enable FileVault on an external volume (whether it is a backup or an installation placed there by the Installer), the FileVault preference pane claims:

FileVault Failed [sic]

This operation is restricted by your settings in System Preferences > Security & Privacy > Privacy > Files and Folders.

The meaning of this dialog is ambiguous, and you can't actually make configuration changes in the "Files and Folders" category. In fact, the problem is not that you have misconfigured something in "Files and Folders", rather some component of the Security Preference Pane, or a service that it relies upon to enable FileVault lacks access to external volumes (i.e. "Full Disk Access"). The identity of that service is not made clear by this dialog.

We have reported this issue to Apple (FB7083306) and we are currently awaiting a response.

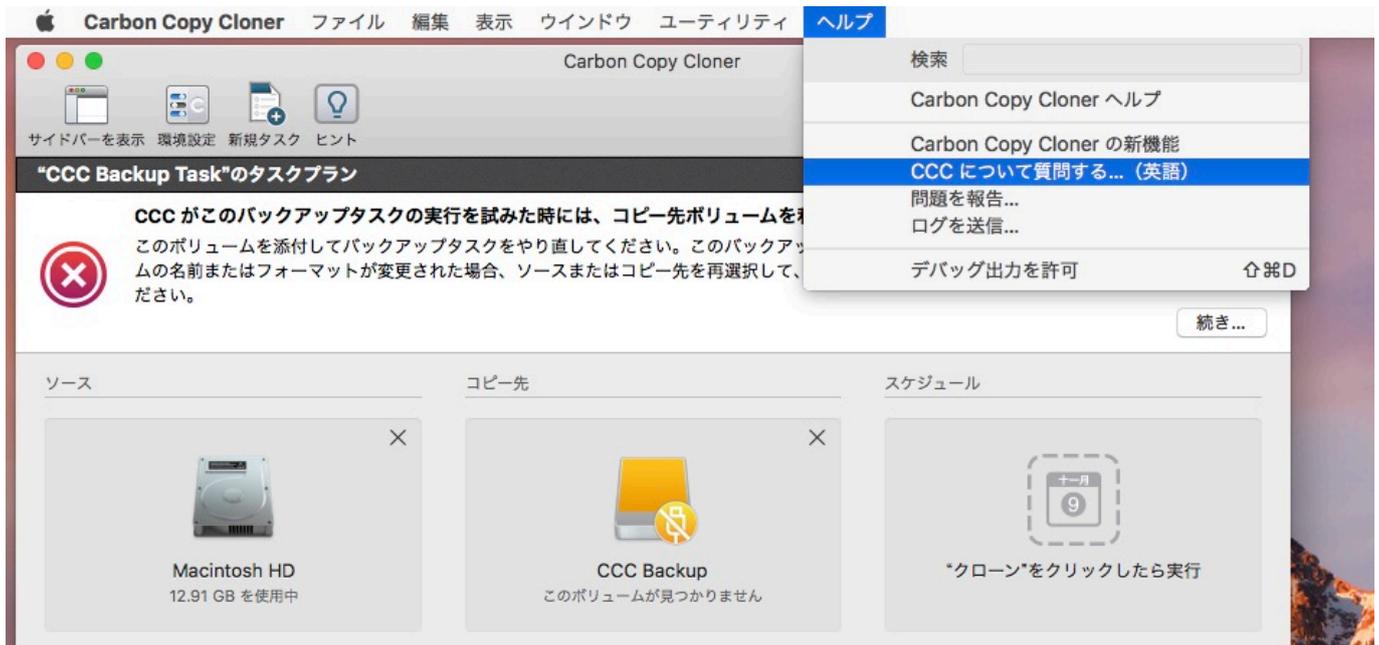
Update: This issue appears to be resolved in Catalina Beta 7.

ヘルプが必要な時はどうすればいいですか。

ヘルプが必要な時は、Carbon Copy Clonerアプリケーション内からヘルプの請求をしていただくのが最善の方法です。営業日の1日以内にご対応できるよう努力しています。但し、対応は英語のみとなっていますのでご注意ください。

ヘルプを開く

CCCに関するご質問、または問題解決にヘルプが必要な場合、いつでもお問い合わせください。Carbon Copy ClonerのヘルプメニューからCCCについて質問する... (英語) を選択してください。



質問や問題の内容を記入する

お名前、メールアドレス、件名を記入して、ご質問や問題の内容を具体的に記述してください。ヘルプリクエストにログが添付されていると、より迅速に対応できます。通常サポートリクエストを受け取ってから営業日1日以内にこちらからご連絡します。それより早いこともあります。

Carbon Copy Cloner ヘルプ

ドキュメント CCC のサポートを請求 ログを送信

ご質問または関連する内容を以下に詳しくご入力下さい。リクエストは Bombich Software のヘルプデスクに送信され、メールまたはヘルプデスクで直接返信いたします。ファイルの添付が必要な場合は、最初のリクエストを送信した後にヘルプデスクで添付することができます。お名前やメールアドレス、サポートリクエストの内容は第三者に開示されません。

お名前

メールアドレス

リクエストの件名

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec finibus egestas sagittis. Etiam id nisl turpis. Donec eu consequat justo. Vestibulum eget egestas elit, et ornare augue. Duis dapibus consectetur tortor eu fringilla. Proin tellus leo, elementum ac odio ac, ultrices mattis sem. In ut sapien porta neque hendrerit lobortis ac commodo massa. In iaculis rutrum aliquet. Nulla facilisi. Integer et nisi aliquam, fringilla erat in, rhoncus libero. Nulla ac aliquam enim, laoreet aliquam odio. Ut lobortis diam id ornare venenatis. Aliquam ut erat et libero efficitur viverra.]

このリクエストに CCC 診断ログを添付

送信されるログファイルの内容が公開されることはなく、ディスカッションとは別に扱われます。ディスカッションが投稿される前に、CCC は送信するファイルを選択することができる専用のパネルを表示します。

ログとリクエストを送信...

ヘルプ！クローンが起動しません！

起動の可能性に関する問題を喜んで [ヘルプします](http://bombich.com/ja/software/gethelp) <<http://bombich.com/ja/software/gethelp>>

。ヘルプを請求される前に以下のトラブルシューティングの手順をお試しください。手順通りに進めない場合、または解決法のオプションが無くなった場合、どこまで進んだか、またはMacがどの起動プロセスまで進むことができたかをお知らせください。

工場出荷時に搭載されているOSよりも古いIOSから起動できるMacはありません

Appleはこれまで、工場出荷時に搭載されているOSよりも古いIOSから新しいiMacを起動することをサポートしたことはありません。新しいiMacにコンテンツを移行する場合は、[その目的のために“移行アシスタント”を使用し](#) <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-volume-backups#migrate>> —
古いiMacのバックアップを新しいiMacに復元しようとすることはやめてください。

関連ドキュメント

- 1台のコンピュータをバックアップし、そのクローンを使用して別のコンピュータを復元できますか？ <<http://bombich.com/ja/ja/kb/ccc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer>>
- Apple Kbase #HT2186：コンピュータに搭載されているOSよりも古いバージョンのMac OSをインストールしないでください <<https://support.apple.com/kb/HT2186>>
- Apple Kbase #HT204350：新しいiMacにコンテンツを移動する方法 <<https://support.apple.com/en-us/HT204350>>

macOS 11、“Big Sur”の起動の可能性に関するトラブルシューティング

macOS Big Sur以降、システムは新しく“署名付きのシステムボリューム”

<<https://developer.apple.com/news/?id=3xpv8r2m>>

にあります。このボリュームは暗号で封印されていて、その封印はAppleのみが適用できます。つまり、システムボリュームの通常のコピーはAppleの封印がないと、起動可能ではありません。CCC

5.1.23、またはそれ以降を使って、Big

Surの起動ディスクのバックアップを作成する際、CCCは自動的にAppleのAPFS複製ユーティリティ (ASR) を使って、ソースのブロックごとの正確なコピーを作成します。それが起動可能なボリュームを生成しない場合、および以下の [ファームウェアの発見の可能性に関するトラブルシューティング](#)

のステップを使い果たしてしまった場合、macOSをバックアップにインストールすることを推奨します。それが起動可能なデバイスを生じない場合、そのデバイスはお使いのMacで起動可能なデバイスとして機能するには向いていません。

関連ドキュメント

- macOSのシステムボリュームをApple Software Restoreを使ってクローンするには <<http://bombich.com/ja/ja/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>>
- macOSをCCCのバックアップにインストールするには <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#installmacos>>

Macのファームウェアが、時々バックアップデバイスを検出できないことがあります

Optionキーを押したままMacを起動すると、[Macの起動マネージャ](#) <<https://support.apple.com/en-gb/HT202796#startupmanager>>

が利用可能な起動デバイスの一覧を表示します。Macのファームウェアチップに保管されたデバイスのドライバーのみを使用すると、ファームウェアはすべてのSATA、PCI、USB、およびThunderboltのバスをハードウェアデバ

イスのためにスキャンしてから、それらのハードドライブボリュームヘッダを読み取り、macOSシステムがそれぞれのボリュームで利用できるかを判断します。通常、CCCの起動可能なバックアップボリュームはこの一覧に表示されますが、時々Macのファームウェアがバックアップをホストするハードウェアを見つけにくいことがあります。

CCCのタスクプランからバックアップボリュームの設定に関する問題の報告がないにも拘らず、そこから起動できない場合、以下の[ファームウェアの発見の可能性に関するトラブルシューティング](#)を試してください。

Macの中には、2TBより大きなUSBデバイスから起動できないものもあります

いくつかのMac、特に2014年より前に製産されたものの中には、起動時にディスクで2TBを超えるボリュームのコンテンツを“見つける”ことができないことがあります。古いMacをお持ちで、2TBよりも大きいUSBデバイスから起動できない場合、ディスクの初めに2TBのパーティションを作成して、そのパーティションにバックアップしてみてください。ディスクユーティリティでディスクをパーティションする際、パイチャートの一番上がディスクの初めであることに注意してください。言い換えると、最初のパーティションは“12時”に始まります。

考えられる回避策：

外部デバイスにFirewireインターフェースがあり、お使いのMacがCatalinaよりも古いIOSを実行している場合、Firewire経由でデバイスをMacに接続すると、どんなサイズのボリュームからも起動できます。MacにFirewireポートがなく、Thunderboltポートがある場合、AppleのThunderboltをFirewireアダプタに使用できます。

2012年のピンテージMacは、暗号化されたUSBデバイスからmacOS Catalinaを起動できない

2012年のMac mini、および2012年のMacBook Proは、非暗号化された外部USBデバイスから最初起動できるが、外部デバイスでFileVaultが有効になると、そのデバイスから起動できなくなるという報告を数件受けています。この問題はCCCに特化したものではありません。この問題はCatalinaを外部デバイスに直接インストールする際にも起きることが確認されています。この問題は特定のエンクロージャ限定ではなく、むしろ、2012年モデルのMac miniおよびMacBook Proに特有と思われる。暗号化されたバックアップが必要な場合、コピー先をAPFS、またはHFS+暗号化として消去してから、[データのみのバックアップをそのボリュームに作成する](http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable) <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable>> ことをお勧めします。

この問題は、弊社から2019年11月にAppleに報告済みで (FB7433465)、現在回答を待っているところです。

AppleがRAIDデバイスからMacを起動するサポートを終了

macOS Mojave以降、AppleはmacOSをRAIDデバイスにインストールすることをサポートしていません <<https://support.apple.com/en-us/HT201316>>

。MojaveをRAIDアレイにクローンできることがわかっていますが、これはサポートされていない方法であるだけでなく、macOS Catalinaにおいては実行可能なオプションとは思えません。

T2 Macで“外部起動”を有効にする (これはM1 Macでは必要ありません)

CCCの起動可能なバックアップからApple T2 コントローラチップ <<https://support.apple.com/en-us/HT208862>> を搭載したMac (例：2018 MacBook Pro、またはiMac Pro)

を起動しようとする場合、外部ハードドライブからの起動を許可するよう、お使いのMacの **外部起動** に関するポリシーを必ず変更してください。Appleのこちらのサポートページ <<https://support.apple.com/en-us/HT208198>> でもその手順が説明されていますが、ここでも紹介します：

1. コマンド()キー + “R” キーを押しながらMacを再起動します。
2. メニューバーのユーティリティメニューから **起動セキュリティユーティリティ** を選択します (詳細はこのスクリーンショットをご覧ください <<http://bombich.com/ja/images/help-clone-wont-boot/startupsecurityutility.jpg>>)。
3. macOS のパスワードを入力

- ボタンをクリックし、管理者アカウントを選択して、そのパスワードを入力してください。
4. **外部起動** (または “許可する起動メディア”) の設定を**外部メディアからの起動を許可** に変更してください。
 5. 再起動してください。

しかし、バックアップから起動することを目的に**安全な起動** 設定を変更することはやめてください。 “完全なセキュリティ” はデフォルト設定です。その設定は、それ自体のバックアップからT2を起動することに対応しています。但し、別のMacのバックアップからこれらのMacの1つを起動する場合は、例外です <<http://bombich.com/ja/ja/kbcc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer#secureboot>> 。ご注意ください。

非QWERTYキーボードを使用する場合の注意：最初、リカバリモードに起動する際、言語を選択するよう促されます。この際、必ずお使いのキーボードに一致する言語を選択してください。そうでないと、起動セキュリティユーティリティがパスワードを承認しないことがあります。

この設定を変えないで、今後実際に自分のバックアップから起動する必要がある場合にのみ変更することは可能ですか？

一般的には、できません。起動セキュリティユーティリティで設定を変更するには、お使いのMacの内部ディスクで機能しているユーザアカウントが必要です。もしお使いのMacの起動ディスクに問題が起きた場合、起動セキュリティの設定を変更することは不可能です。CCCの起動可能なバックアップの主要な目的は、Macの起動ディスクに問題が起きた、または機能しなくなった場合の救援ディスクとして機能することなので、Macを外部デバイスから起動できるように設定しておくことを推奨します。

追加の起動セキュリティのために、ファームウェアパスワードを適用できます。ファームウェアパスワードが適用されると、お使いのMacは起動時にStartup Managerを読み込むためのパスワードが必要になります。

Apple Kbase HT204455:Macにファームウェアパスワードを設定するには <<https://support.apple.com/en-us/HT204455>>

T2ベースのMacが暗号化されたHFS+ボリュームから起動できない

弊社のテストでは、AppleのT2コントローラチップを搭載したMacは暗号化された、Mac OS拡張フォーマットされた、外部ボリュームからは起動できないことが確認されています。外部ボリュームから起動することは、一般的に問題ありませんが、もし外部ディスクがAppleのレガシーHFS+、Mac OS拡張フォーマットでフォーマットされている場合、そのボリュームでFileVaultを有効にすると、それが起動不能になり、起動時に次のようなエラーメッセージが表示されます：

この起動ディスクを使用するにはソフトウェアアップデートが必要です。今すぐアップデートするか、別の起動ディスクを選択してください。

ネタバレ注意：“アップデート” オプションは動作しません。これはT2 Macのファームウェアのバグか、あるいは、Appleが公表するつもりのない制限かもしれません。いずれにしろ、T2ベースのMacの外部で起動可能なバックアップを暗号化したい場合、そのバックアップボリュームをAPFSとしてフォーマットすることを推奨します。

起動マネージャーに追加のドライバーを読み込ませる

サードパーティの外部デバイスには**オプションROMファームウェア** <<https://en.wikipedia.org/wiki/OptionROM>> を使用するものがあります。 “最新のソフトウェア” <<https://support.apple.com/en-us/HT202796#optionROM>> を搭載したMacは自動的にオプションROMファームウェア読み込みません。そのため、そのファームウェアを読み込むまでMacはオ

プションROMファームウェアを搭載して

いるデバイスを認識しません。 **起動マネージャーウインドウ**で “Option-Shift-Command-ピリオド” を押すと、現在接続中の

ハードウェアエン

クロージャからオプションROMファ

ームウェアを読み込むことができます。

以下はオプションROMファームウェアを使用しているデバイスの一例です：

- LaCie 5Big Thunderbolt <<http://www.lacie.com/professional/big/5big-thunderbolt-2/>>

一般的に互換性のない設定とファイルシステムの例外を排除する

外部ハードドライブエンクロージャまたはアダプタを使用している場合、お使いのエンクロージャが過去に問題が見られたエンクロージャとして[このページの下に](#)表示されているか確認してください。またさらに、ディスクユーティリティの“ 応急処置 ” ユーティリティを使用すると、コピー先ボリュームに存在する可能性のあるファイルシステムの問題を検証して修復することができます。

Macの起動マネージャーで発見の可能性の問題に関するトラブルシューティング

1. Macの電源を切ります
2. キーボードとマウス以外のすべての周辺機器をMacから接続解除します
3. バックアップディスクをMacのUSB、またはThunderboltのポートに直接接続します (ハブ、アダプタ、モニター、デジチェーン、他社製USBカードのいずれも必要ありません)
4. Optionキーを押しながらMacを再起動します
[注意:有線接続のキーボードにはこのステップが必要なことがあります]
5. 約30秒待ち、バックアップボリュームが表示されるか確認してください。
この段階でバックアップボリュームが表示され、起動プロセスがAppleのロゴよりも先に進んだ場合、[以下の次のステップにスキップしてください。](#)
6. 起動マネージャーウィンドウで “ Option-Shift-Command-ピリオド ” を押すと、存在していて、外部ハードドライブエンクロージャを必要とするオプションROMファームウェアを読み込むことができます。
7. バックアップボリュームのUSB、またはThunderboltケーブルをMacから一旦取り外してから再接続し、もう30秒待ちます。バックアップボリュームが表示されたら、それを選択して起動プロセスを進めてください。
8. まだバックアップボリュームがオプションの1つとして表示されない場合は、Macを完全にシステム終了してください。その後、Optionキーを押しながら起動し、ボリュームが表示されるまでもう30秒待ちます。
9. ボリュームが表示されるまで、別のインタフェースを使用して上記の手順を繰り返してください (例えば、Thunderboltを試したらUSB、すでにUSBを試したらThunderboltというように)。
10. ハードドライブエンクロージャがバス電源の場合、Macを起動前にDC電源に接続してみてください。バス電源のエンクロージャは、しばしばスピニングに時間がかかることがあるか、また単純に早い時期の起動プロセスでは利用できません。

追加のUSBデバイスに関するトラブルシューティング

以下の追加のステップを実行することで、Macに起動プロセスの早い段階でお使いのUSBデバイスを “ 発見 ” させることができます。

1. Optionキーを押しながらMacを再起動します。
2. Macに複数のUSBポートがある場合、コピー先ディスクをそれぞれのポートに接続してみてください (必ずハブ、キーボード、ディスプレイモニターではなく、Macのポートに直接接続してください)。
3. USB 3.0エンクロージャを使用している場合、USB 2.0ケーブルを使用してください (はい、**間違いなく**動作します!)。USB 3.0デバイスはUSB 2.0に後方互換性がありますが、必ずしもMacのファームウェアに組み込まれた古いUSBデバイスドライバーとうまく動作するわけではありません。USB 2.0のケーブルを使用することで、MacのファームウェアUSBドライバーを使用する際にのみ明らかになる互換性の問題をしばしば回避してエンクロージャから異なる動作を引き出します。以下はUSB 2.0とUSB 3.0

のケーブルの写真です：

USB 2 Micro B



USB 3 Micro B



MacのパラメータRAMをリセット

最後にMacのパラメータRAM (PRAM) を再設定してみてください。PRAMはMacの起動に関連する設定を維持しているため、その設定が無効なために、Macが外部エンクロージャを検出するのを干渉している可能性があります。PRAMをリセットするには：

1. 起動時に Command+Option+P+R を押したままにします
2. 2度目の起動チャイムが鳴るまで、これらのキーを押したままにします。
3. 2度目の起動チャイムが鳴ったらOptionキー以外のキーをすべて離してください。

互換性のないエンクロージャを完全に排除する

それでもまだボリュームが表示されない場合は、ファームウェアがエンクロージャを検知できない可能性があります (macOSが一旦起動され、さらに多くのデバイスドライバーにアクセスして、エンクロージャを問題なく見つけているにも拘らず)。起

動の可能性をテストする黄金のリトマス試験がある

とすれば、[macOSを直接ボリュームにインストールすることです](http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#installmacos) <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#installmacos>>

。それでもデ

ィスクが起動可能にならな

い場合、それは絶対に起動可能にならないということ

です。 [このようなエンクロージャはこちらまでご報告ください](http://bombich.com/ja/software/gethelp) <<http://bombich.com/ja/software/gethelp>>

。問題のあるエンクロージャのリストを作成します。

バックアップボリュームはMacの起動を開始しますが、速度が遅いか、またはFinderに全くたどり着きません

バックアップボリュームが起動プロセスのどの辺りまで進んでいるかを視覚的に知るヒントがいくつかあります：

1. Apple ロゴ： “ 起動用 ” のファイルが見つかり、実行されました。
2. 進行インジケータが回転中： OSの “ カーネル ” が実行され、起動プロセスをコントロールできます。カーネルは、カーネル拡張機能のキャッシュを読み込み、起動ディスクをマウントしてから、“ 起動 ” を実行することでその他すべてのシステムのプロセスを開始します。
3. プログレスバー： WindowServerの読み込みが完了しました。システムは、通常のアプリケーションまたは loginwindowの読み込み開始の準備が整っています。
4. loginwindowまたはデスクトップ： システムが読み込みを終了し、ユーザが操作できる準備が整っています。

バックアップボリュームが Option

キーの起動ディスク選択画面に表示されたが、そこから起動しようとするAppleロゴを表示しない場合、Macは

このボリュームに“起動用”ファイルを見つけれないということです。これはハードドライブエンクロージャの干渉によるか、バックアップボリュームのファイルシステムが壊れているか、ボリュームが不正に“プレス”されているかによるものです（ボリュームをプレスすると、起動ファイルに関する特定の情報がボリュームのヘッダに保管され、Macはその情報を使用して起動プロセスを開始します）。

1. バックアップディスクを消去 <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>> してから、起動ディスクをコピー先にクローンし直してください。
2. もう一度バックアップボリュームから起動してみてください。

バックアップからMacを起動する場合に期待されるパフォーマンス

バックアップから起動する場合、Macのパフォーマンスは、ほぼ完全にハードウェアのパフォーマンス次第です。より具体的に言えば、そのハードウェアのファイルシステムのパフォーマンスによって異なります。お使いのバックアップディスクがSSDの場合、内蔵のSSDからMacを起動するときに得られるパフォーマンスに比べて、非常に優れたパフォーマンスを期待できます。お使いのバックアップディスクが回転式HDDの場合、そのパフォーマンスは、“一応十分”から“非常に劣る”まで、さまざまです。パフォーマンスは、バックアップボリュームのフォーマット、オペレーティングシステムのバージョン、およびバックアップディスク固有のパフォーマンス特性によって異なります。特に、AppleのAPFSファイルシステムは回転式HDDデバイスで比較的劣るパフォーマンスになります <<http://bombich.com/ja/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>>。しかも、5400RPMディスクおよび [シングル磁気記録方式](http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive#smr) <<http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive#smr>> を使用するディスクでは、そのパフォーマンスはかなり悪化します。これらの遅いHDDのパフォーマンスでは、バックアップからMacを起動する目的に使用可能できない可能性があります。

関連ドキュメント

- バックアップドライブを選択するには:推奨デバイス <<http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive#recommendations>>
- 移行アシスタントを使ってCCCのバックアップからデータを移行するには <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#migrate>>

起動ディスクを選択後、ユニバーサルな“アクセス不可”のシンボルが表示された場合

これは、macOSが起動ディスクを読み込めない、または起動ディスクをマウントできないことを示しています：



この原因として頻繁に見られるのは、Macを互換性のない（例：古すぎる）オペレーティングシステムから起動しようとするということです。

また、起動を試みているエンクロージャとデバイスのドライバーが競合していることが原因で、または、Macとエンクロージャ間のファームウェアの互換性が原因でも、この問題が起きることがあります。USB 3.0エンクロージャから2013年より前のMacを起動しようすると、この問題が起きることがあります。また、重大なカーネル拡張のコード署名が無効な場合、Yosemiteでこの現象が頻繁に表示されます。例えば、[TRIM Enabler](#)

<https://www.cindori.org/trim-enabler-and-yosemite/>

などを使用してmacOSストレージドライバを変更する場合に起こる可能性があります。

- macOS Catalinaの時点では、AppleはFireWire接続されたデバイス経由でMacを起動することをサポートしていません。お使いのデバイスがFireWire経由で接続され、USBポートもある場合は、デバイスをUSB経由でMacに接続してみてください。
- セーフ起動モードに起動してみてください（バックアップボリュームを起動ディスクとして選択後、Shiftキーを押したままMacを開始してください）。
- Macをリカバリモード <<https://support.apple.com/en-us/HT204904>>で起動したまま、クローンしたボリュームにmacOSを直接インストールしてください。インストールも失敗した場合には、エンクロージャとお使いのMacの間に互換性の問題があるので、起動ディスクとしては相応しくありません。
- サードパーティユーティリティ（例、TRIM Enabler）を使用してmacOSソフトウェアを変更した場合、その変更を取り消してから、バックアップタスクを実行し直してください。

バックアップボリュームから起動中、

Macが進行インジケータ（Appleロゴの下）よりも先に進まない、またはAppleロゴ+プログレスバーで機能停止する場合、おそらく起動プロセスの初期の段階で呼び出されたシステムファイルのいくつかに問題があるか、またはmacOSが起動プロセスのそのステージで外部エンクロージャのための正しいドライバを読み込むことができないと考えられます。この場合も、エンクロージャとの互換性の問題を排除するために、**リカバリモード**

<<https://support.apple.com/en-us/HT204904>>

で起動したまま、macOSをクローンしたボリュームに直接インストールしてみてください。

“ Unapproved Caller SecurityAgent may only be invoked by Apple Software ” のメッセージが起動時に表示されます

このメッセージは一般的に起動しようとしているボリュームに空き容量がない、またはほとんどない時に表示されます。CCC SafetyNetフォルダから項目を（またはフォルダ全体を）削除することができます。次に、そのボリュームから起動を試みる前にゴミ箱を空にするか、またはそのボリュームからスナップショットを削除して、空き容量を確保してください。macOSは、起動時にキャッシュの作成と仮想メモリのファイルを収容するために最低2GB、できれば5-10GBの空き容量が必要です。

関連ドキュメント:

- CCC SafetyNet フォルダの自動管理 <<http://bombich.com/ja/ja/kb/coc5/automated-maintenance-coc-safetynet-folder>>
- スナップショットと領域の問題：スナップショットを削除するには <<http://bombich.com/ja/ja/kb/coc5/leveraging-snapshots-on-apfs-volumes#space>>

“ 起動ディスクを選択されたディスクに変更することはできません。プレスツールが現在のブートディスクを設定できませんでした。 ”

時々、環境設定の“ 起動ディスク ” パネルから役立つ内容がないままこのエラーが報告されることがあります。それよりも頻繁に、環境設定の“ 起動ディスク ” パネルで起動ディスクを変更できないことは、実際ボリュームが起動可能でないことを示すものではなく、環境設定の“ 起動ディスク ” パネルが起動ディスクの選択肢をその特定のボリュームに変更できないことを意味しています。起動ディスクの選択を妨げるいくつかの条件が見つかりました：

APFSが古いIOSでサポートされていない、起動できないフォーマットである

古いバックアップ（例：macOS Sierra）から起動する場合、APFSフォーマットされたボリュームがFinderにマウントされたとしても、起動ディスクとして選択するには問題がある可能性があります。APFSはSierraのベータファイルシステムでした。APFSボリュームを起動可能にするために必要なコンポーネントが未だ完成していなかったからです。

同様に、APFSフォーマットされたFusionボリュームのサポートはmacOS Mojaveまで追加されませんでした。High Sierraのバックアップボリュームから起動する場合、APFSフォーマットされた、Mojaveを含むFusionボリュームは読み出し専用でマウントされていること、そして、そのボリュームを起動ディスクとして設定できないことに気が付くでしょう。

どちらの場合も、解決策は別の起動ディスクを選択するために起動マネージャー (Optionキーを押したままMacを起動する) を使用することです。一旦新しいOSからMacを起動すると、起動ディスクの選択肢をリセットできるようになります。

システム整合性保護が現在の起動ディスクのプリブートヘルパーパーティションへの変更を禁止する

APFSボリュームを現在の起動ディスクのAPFSコンテナに追加する場合、macOSのプレス機能はコンテナのプリブートボリュームをアップデートして、第2のパーティションのためのサポートファイルを含めることはできません。1つのAPFSコンテナに複数の、起動可能なボリュームがあることはサポートされている構成ですが、第2のボリュームを起動可能にすることができるのは、クローンしている間に他の起動ディスクから起動する場合のみです。同様に、最初のボリュームから起動中、起動ディスクに第2のボリュームを選んで変更することはできません。解決策は上記と同じです。つまり、起動マネージャー (Optionキーを押したままMacを起動してください) を使用して、一時的に起動ディスクの選択を変更してから、起動ディスクを明示的に新しい起動ボリュームに設定することです。

Catalinaを使用している場合:システム整合性保護は、現在の起動ディスクと同じAPFSコンテナにある、他のすべてのボリュームでシステムファイルの保持を妨げます。このように、現在の起動ディスクのAPFSコンテナ内にあるコピー先とタスクを構成する際、CCCはシステムファイルを除外します。

または、起動ディスクに別のパーティションを作成することもできます (同じAPFSの親コンテナに2つ目のボリュームを追加する代わりに)。そして、その別のパーティションにバックアップを作成できます。

1. ディスクユーティリティを開きます
2. 表示メニューから “すべてのデバイスを表示” を選択します
3. Macintosh HDボリュームのための一番上の親デバイスをクリックします
4. ツールバーの “パーティション” ボタンをクリックしてください
5. ディスクユーティリティがこの操作を勧めない場合は、 “ボリュームを追加” を先に選択して、 “パーティション” ボタンをクリックしてください
6. “+” ボタンをクリックして、APFSフォーマットされた第2のパーティションを起動ディスクに追加してください

プレスユーティリティがFirewire接続されたデバイスをプレスできない

macOS Mojaveユーザの一部の報告によると、Firewire接続されたボリュームを起動ディスクとして選択しようとすると、同様の “プレスできません” というエラー結果になるそうです。USBが代替オプションである場合、同じデバイスをUSB経由でMacに接続して、そのデバイスを起動ディスクとして選択すると問題なく動作します。

問題が承知されている構成

- USBメモリスティックは本来遅いデバイスですので、起動可能なバックアップの作成にこれらを使用することは推奨しません。
- SanDiskのフラッシュドライブ (Cruzer、Ultra)、およびSDカードをmacOS High Sierraで使用すると、起動性にムラがあるという報告を数多く受けています。これらのデバイスは遅いという報告も頻繁に寄せられるので、これらを起動可能なバックアップに使用することはどちらにしても推奨できません。Catalinaおよびそれ以降:

Catalinaより前のOSでこれらのデバイスに起動性の問題を引き起こす同じ問題が、新たに、システムボリュームとデー

タボリュームの基本的なバ

ックアップすらも妨げるエラーを発生しています。

[Catalinaデータボリュームの起動可能ではないバックアップ](http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable) <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable>>

を作成する場合にのみ、これらのデバイスを使用することをお勧めします。

- Western Digitalエンクロージャは、起動ディスクとして使用される場合、その実績には信頼性がありません。互換性のないものには次のものが含まれます：
 - WD My Passport Studio 2TBは、T2 MacBook Proを起動できないという報告を受けています (この報告は、macOS Mojaveをこのデバイスにインストールする試みが不成功に終わったことで確認されています)。
 - Western Digital My Passport ハードドライブエンクロージャは、起動ディスクとしてmacOS Catalinaと機能しないという報告を数多く受けています (macOSをこのデバイスにインストールできないこと、または、インストーラ経由でmacOSをインストール後、このデバイスから起動できないことが確認されています)。
 - Western Digital EasyStore は、起動ディスクとしてmacOS Catalinaと機能しないことが報告されています (上記と同様に確認されています)。
 - 例外：WD MyPassport SSDは、Western Digitalデバイスの中ですばらしい結果を生むと確認できた唯一の例外です。
- Hands Off! と可能性として Little Snitchは、クローンしたボリュームが起動するのを妨げます <<http://bombich.com/ja/kb/discussions/no-boot-from-firewire800-disc>>
- 一部のMacではUSB 3.0 エンクロージャからの起動に問題のある場合があります
- 報告によると <<https://discussions.apple.com/thread/4243814>>、公開されているドキュメントに反して、NewerTech Voyager Dock <<http://www.newertech.com/products/voyagerq.php>> エンクロージャはFirewire経由で起動できません。
- Nexstar 6G <http://www.vantecusa.com/productsdetail.php?pid=25&pname=NexStar+6G&pcid=2&pc_name=3.5%22+Enclosure&ptid=1&ptname=Hard+Drive+Enclosures> のUSB 3.0 ハードドライブエンクロージャはデバイスを発見できないと言う問題のために起動できない、と言う報告があります。VantecのNexstar TXは起動可能です (同じ内蔵ハードドライブを使用)。しかし、Nexstar 6Gは起動できる
という別の報告も受け取っていますので、このエンクロージャに関してはそれぞれのMac固有のファームウェアの問題が潜んでいる可能性があります。
- 複数ベイのハードドライブエンクロージャが不安定な起動結果を引き起こすという報告を数件受け取っています。すべてのケースで、ハードドライブがエンクロージャの最初のベイに設置されている限り、Macは起動可能なバックアップから起動できると報告されています。他のベイに設置すると、起動可能なボリュームはMacのファームウェアによって見つけられませんが、複数のベイのあるエンクロージャでディスクから起動するときには問題がある場合は、エンクロージャ内のドライブの位置を変えてみてください。以下はこれまで報告のあった影響を受けるエンクロージャのリストです：
 - Mediasonic HF2-SU3S2
 - CineRAID Home CR-H212 USB 3.0 バス電源デュアルドライブ RAID/JBOD
ポータブルエンクロージャ <<http://www.cineraid.com/products/homeh212.htm>>
 - StarTech S3520WU33ER USB 3.0 バス電源デュアルドライブ RAID/JBOD
ポータブルエンクロージャ <<https://www.startech.com/HDD/Enclosures/S252BU33R>>
 - MyDigitalSSD BOOST <<http://mydigitalssd.com/mobile-ssd.php#boost-usb-3.1>>
 - OWC Mercury Elite Pro Dual <<https://eshop.macsales.com/shop/Thunderbolt/External-Drive/OWC/Elite-Dual-RAID>>
- Orico 3588US3 USB3のエンクロージャはデバイスを発見できないと言う問題のために起動できない、と言う報告があります。
- Webroot SecureAnywhereのバックアップタスク中に“脅威を削除する”リクエストに同意すると、起動できないバックアップを作成するという報告があります。
- “ASMedia 1051E”チップセットを使用するUSB 3.0デバイス (例：[このOWC Mercury On-The-Go](http://www.owc.com) <<https://eshop.macsales.com/item/Other%20World%20Computing/MOTGS3U3/>> エンクロージャ) から2013年以前のMacを起動する際に問題が起きることも報告されています。ファームウェアの互換性の問題は、2015年のファームウェアアップデートでこれらのMacに紹介されています。これらのMacはその古いチ

ブセットを搭載するUSB 3デバイスから起動できません。

- 数人のユーザから、ASMediaのASM1352Rエンクロージャに発見可能性の問題があると報告を受けています。
- 1人のユーザから、MyDigitalSSD Boostエンクロージャは起動できないとの報告がありました。
- AmazonBasics 10 Port USB 3.0 Hubに接続されたデバイスは、Optionキーを使った起動マネージャで利用できないという報告があります。CCCの起動可能なバックアップから起動する必要がある場合、USBデバイスをMacのUSBポートに直接接続してください。
- Sonnetのカスタマーサポートによると、Sonnet Allegro Pro USB 3 PCIカードは起動ディスクとして機能しないことが確認されています。
- Inateck USB 3.0 2.5"ハードドライブエンクロージャのモデル番号"FEU3NS-1"には起動の問題があるという報告が何人かのユーザから報告されています。
- Sabrent Rocket Pro 2TB NVMe USB 3.1 External Aluminum SSD は 起動可能ではないという報告を受けています。
- Other World Computingの6-bay ThunderBay 63は macOS Catalinaでは起動可能ではないという報告を受けています。macOSは起動処理を75%まで進めた後、動かなくなります。まったく同じディスクが異なるエンクロージャに使用されると問題なく起動します。
- LaCie d2は起動可能ではないという報告が最低2件届いています。
- VisionTek 1 GB Thunderbolt3 SSD は、macOS Big Surで起動できないという報告を受けています (テストケースは、2019 MacBook Proに関して。Big Surインストーラが完了後、デバイスが起動に失敗するのを確認)。上記のケースにおいて、同デバイスはCatalinaでは起動可能でした。

Samsung T5 Portable SSDに特有の互換性の問題

macOS Catalinaユーザ向けに:これらのエンクロージャはmacOS Catalinaでは良い結果が出ていることが確認されています。弊社の内部テストでは100%成功をおさめ、弊社の結果を裏付ける報告も数件届いています。以下のコメントはmacOS MojaveおよびHigh Sierraに特定のもです。

Samsung T5 Portable SSDはT2ベースのMacBook Pro 2018で起動可能なデバイスとして全く機能しないという報告を数人のユーザから受けています。このデバイスにmacOS Mojaveをインストールしても起動可能なボリュームを生むことができませんでした。これはこれまで成功を納めてきたよく使われているエンクロージャなので、今のところこれらの報告は2018 MacBook Proに限定されると考えられます。

また、Samsung T5 Portable SSD (およびTranscend StoreJet SSD)

は、そのデバイスから、またはMacの内部ハードドライブから起動を試みるとき、起動時に (T2 MacだけでなくどのMacでも)

例外的に長い遅延をもたらすことも知られています

。これは、SSDがAPFSとしてフォーマットされていて、SSDにmacOSがインストールされている場合に (クローンまたはインストーラ経由で)、Macのファームウェアとこの特定のSSDの間に互換性の問題が起きるためと考えられます。この遅延を避けるために、そしてお使いのMacがmacOS Mojave、または *それ以前のOS* を実行している場合に限り、互換性の問題が解決するまで、これらのSSDをHFS+としてフォーマットすることを推奨します:

1. ディスクユーティリティを開きます
2. 表示メニューから**すべてのデバイスを表示**を選択します
3. ディスクユーティリティのサイドバーからSamsung T5 SSDの一番上のレベルの“親”デバイスを選択します
4. ツールバーの“消去”ボタンをクリックしてください
5. フォーマットを Mac OS Extended (ジャーナリング)に、スキームを GUIDパーティションマップに設定してください。
そして、新しいボリュームに名前を付けてください
6. “消去”ボタンをクリックします
7. CCCを開いて、新しいボリュームをコピー先として選択し直してから、バックアップタスクを実行してください

注意: T2 Macを使用している場合、[T2 Macは暗号化されたHFS+フォーマットのデバイスから起動できない](#)ことを忘れないでください。バックアップディスクが暗号化されている必要がある場合、Samsung TシリーズのデバイスはT2ベースのMacのバックアップデバイスとしては相応しくありません。

その他の注意:HFS+は、**製品（システム）**の起動ディスクのフォーマットには適していません。Mojave **バックアップ** ディスクをHFS+としてフォーマットすることは問題ありませんが、Samsung T5をシステムの起動デバイスとして使用している場合、それをHFS+にフォーマットしている限り、システムアップデートをそのボリュームに適用することはできません。

2019年 iMacが誤ってUSB-Cデバイスから起動します

弊社は、2019 iMacとUSB-C (Thunderboltと同じポート) 経由で接続された外部ディスクに特定の、新たに浮上してくる問題を追跡しています。この問題は、iMacが内蔵ディスクから起動することが優先されているにも拘らず、内蔵ハードドライブではなく、外部デバイスから起動する、ということです。これは、このiMacに特有のファームウェアの問題だと考えています。ファームウェアが起動ディスクとしてどのデバイスを使用するかを判断して、ユーザの優先する設定

(内部起動ディスク)

を無視していると思われる。あるユーザが実行したシンプルで非常に信頼のおけるテストによると、macOS Catalinaをきれいに消去した、外部ドライブにインストールすると、そのデバイスがUSB-C経由で接続されている限り、選択中の設定に関係なく、Macはそのデバイスからのみ起動しました。この動作はCCCまたは特定のエンクロージャに固有のものではなく、ファームウェアのバグと考えられます。

回避策：お使いの外部ハードドライブエンクロージャに**USB-C to USB Type A ケーブル**

<https://static.bhphoto.com/images/images2000x2000/15103156031335192.jpg>

が付いている場合、それを使って、ディスクをiMacのUSB type Aポートに接続することでこの問題を回避できます。または、単純に、再起動の前にMacからディスクを取り外すこともできます。

関連ドキュメント

- 1台のコンピュータをバックアップし、そのクローンを使用して別のコンピュータを復元できますか？
<<http://bombich.com/ja/ja/kb/ccc5/can-i-back-up-one-computer-and-use-clone-restore-another-computer>>
- CCCがどのようにコピー先ボリュームの"bootability"（起動の可能性）を決定するかについての詳しい検証
<<http://bombich.com/ja/ja/kb/ccc5/closer-look-how-ccc-determines-bootability-destination-volume>>
- Apple Kbase：Macが起動する時に表示される画面について <<https://support.apple.com/en-us/HT204156>>

CCCを最新に保つには

環境設定を開く



Carbon Copy Cloner メニューから**環境設定**を開きます。

ソフトウェアアップデートを選択



今すぐアップデートを確認をクリックすると、すぐにアップデートを確認できます。

CCCは 1 週間に 1 度アップデートを確認するようデフォルト設定されています。この設定は日や月ごとに変更することができます。アップデートの自動確認をオフにするには、**アップデートを確認する割合：毎**の横にあるチェックボックスのチェックマークを外してください。

デフォルトで、CCCはベータ版のリリースは通知しません。但し、ソフトウェアを改良したことで特定の問題が解決したかどうかを確認するために、ベータ版アップデートが提供されることがあります。一般的に、ベータ版アップデートはソフトウェアデベロッパがユーザの発見した問題を再現できない場合にのみ発表されます。そのため、ベータ版アップデートはBombich Softwareの指示に従ってのみ適用されることをお勧めします。

サードパーティのアップデートメカニズムを使用しない

MacUpdate DesktopまたはCNETインストーラなど、サードパーティのアップデートサービスを使用した際にアップデートに問題があったと言う報告を数多く受けます。中には、サードパーティのアップデートサービスがアップデートと共に**他の宣伝用のソフトウェア**をインストールした、または、アップデートを完全にめちゃくちゃにしたためCCCが使えなくなった、と言う報告もあります。どうかこれらのサービスをCCCのアップデートに適用しないでください。必ずCCCの内蔵ソフトウェアアップデートメカニズムをご使用ください。

CCCをアンインストールするには

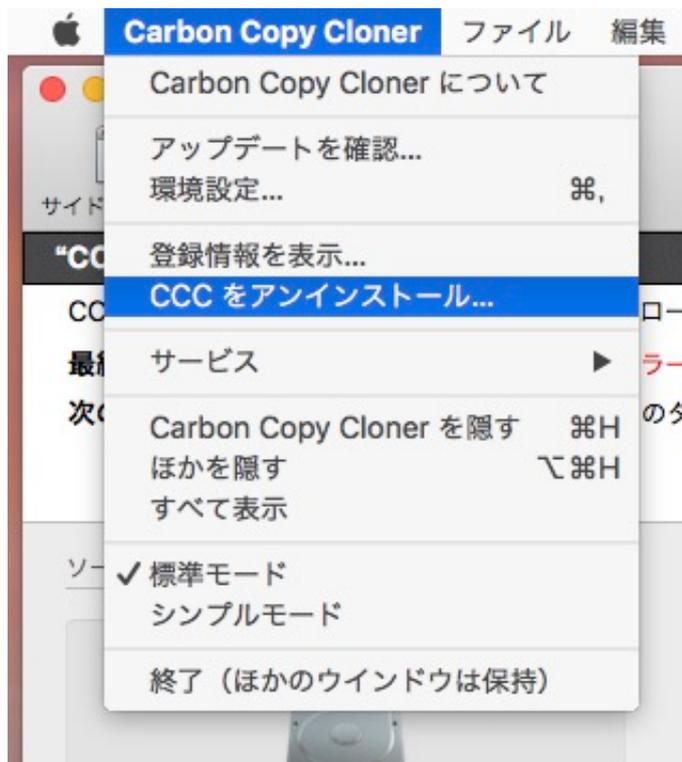
Carbon Copy Cloner内からアンインストールするには

Carbon Copy Clonerをアンインストールするには、Optionキーを押したまま、Carbon Copy ClonerメニューからCCC

をアンインストール...

を選択してください。CCCをアンインストールすると、CCCの権限ヘルプツールとすべての保存済みのタスクは即座に削除されます。Carbon Copy

ClonerアプリケーションファイルとCCC環境設定はその後ゴミ箱に移動します。



CCCをアンインストールする前にスナップショットを削除

CCCをお使いのMacから完全に削除したい場合、CCCが作成したスナップショットを先に削除する必要があります。CCCのサイドバーにあるそれぞれのボリュームを選択して、そのボリュームにスナップショットが存在するかどうかを確認してください。スナップショットのリストにスナップショットがあれば、それらをすべて選択してから“Delete”キーを押して削除してください。

スナップショットと領域の問題：スナップショットを削除するには <<http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes#space>>

Carbon Copy Clonerに関連するファイルを手動で削除するには

アンインストール機能を活用する前にCarbon Copy Clonerアプリケーションを削除してしまった場合、CCCに関連する以下のファイルとフォルダを手動で削除することができます：

- /Library/Application Support/com.bombich.ccc
- /Library/LaunchDaemons/com.bombich.ccchelper.plist

- /Library/PrivilegedHelperTools/com.bombich.ccchelper
- /Users/yourname/Library/Application Support/com.bombich.ccc
- /Users/yourname/Library/Application Support/CCC Stats Service
- /Users/yourname/Library/Caches/com.bombich.ccc
- /Users/yourname/Library/Caches/com.bombich.ccc.stats
- /Users/yourname/Library/Caches/com.bombich.ccc.useragent
- /Users/yourname/Library/Cookies/com.bombich.ccc.binarycookies
- /Users/yourname/Library/Preferences/com.bombich.ccc.plist

ホームディレクトリのライブラリフォルダを入手するには、Optionキーを押したまま、Finderの **移動** メニューから **ライブラリ** を選択してください。項目をゴミ箱に移動し終わったら、コンピュータを再開し、ゴミ箱を空にしてください。

CCCユーザエージェントと com.bombich.ccchelper 権限ヘルパーツールを手動で無効にするには

Carbon Copy Clonerをインストールして使用する時、CCCタスクをサポートするために背景ユーティリティがインストールされます。タスクの実行と調整のためのヘルパーアプリケーションは、タスクに関連するすべてのアクティビティに必要です。スケジュールされたタスクがない場合、また、CCCのアイコンをメニューバーで表示しないように設定した場合には、ヘルパーツールは自動的に終了します。ヘルパーツールはCCCを開始時、およびCCCユーザエージェントを実行中、自動的に起動します。

CCCユーザエージェントは、ヘルパーツールから通知センターへの通知、ユーザへの確認メッセージとリマインダー、およびエラー状況のサブセットを送信する役目を担っています。CCCアイコンをメニューバーで表示しないように設定した場合、スケジュールされたタスクがない場合、実行中のタスクがない場合、CCCが実行中でない場合には、ユーザエージェントは自動的に終了します。

これらのアプリケーションを無効にする特定の理由がある場合、例えば、CCCをたまにしか使用しないと言うような場合、CCCの使用を完了した時に以下のことを実行できます：

1. CCCのアイコンがメニューバーに表示されないように設定する (Carbon Copy Cloner メニュー > 環境設定 > 通知)
2. Command+Optionキー ()を押しながら、Carbon Copy Cloner メニューをクリックします
3. **すべてのタスクを無効にして終了**を選択してください (キーボードショートカット：Command+Option+Q)

CCCの権限ヘルパーツールが無効に設定されている限り、スケジュールされたタスクは実行されませんのでご注意ください。

関連ドキュメント

- CCCの権限ヘルパーツールとは何ですか？ <<http://bombich.com/ja/ja/kb/ccc5/what-cccs-privileged-helper-tool>>

Antivirus software may interfere with a backup

Some antivirus applications may prevent Carbon Copy Cloner from reading certain files, mounting or unmounting disk image files, or, in general, degrade the performance of your backup. In some cases, antivirus applications can even affect the modification date of files that CCC has copied, which will cause CCC to recopy those files every time as if they have substantively changed. In another case, we have seen such software create massive cache files on the startup disk during a backup, so much so that the startup disk became full. We recommend that you temporarily disable security software installed on your Mac (e.g. for the duration of your backup task) if problems such as these arise.

If CCC reports that antivirus software may be interfering with your backup task, here are some troubleshooting steps that you can take to resolve the problem:

1. Determine whether the files in question are being quarantined by your antivirus software. Perform a system scan with your antivirus software and address any issues that are reported. Please refer to the Help documentation associated with your antivirus product for more information.
2. If the problem persists, try running your backup task with the antivirus software temporarily disabled.

If the antivirus software's behavior cannot be resolved, you may be able to workaround the problem with an advanced setting. Select your task in CCC's main application window, then:

1. Click the Advanced Settings button.
2. Check the Don't update newer files on the destination option in the Troubleshooting box
3. Save and run your task.

If these steps do not address the issue, or if you do not have antivirus software installed, please [open a support request <http://bombich.com/software/gethelp>](http://bombich.com/software/gethelp) and we'll do our best to help you resolve the problem.

"Real time" protection scanning and Digital Loss Prevention applications have significant performance ramifications

We regularly receive reports that the backup task is running too slow, only to find that some "real time" protection application is directly causing the problem by taking too long to either scan content that CCC is writing, or by taking too long to permit the filesystem requests that CCC makes to the source or destination. While these applications do provide a valuable service to protect your Mac from malware, they're doing a disservice if they're interfering with backups.

The following applications are frequently implicated in these scenarios:

- Symantec DLP (com.symantec.dlp.fsd)
- Avira (avguard-scanner)
- Sophos File Protection (OnAccessKext)

Problem reports related to antivirus software

- [Sync problems and ACL issues <http://bombich.com/kb/discussions/sync-problems-and-acl-issues>](http://bombich.com/kb/discussions/sync-problems-and-acl-issues)
- [Subsequent backups are slow <http://bombich.com/kb/discussions/subsequent-backups-both-full-and-incremental-slow.>](http://bombich.com/kb/discussions/subsequent-backups-both-full-and-incremental-slow.>)
- [Source Disk becomes full when cloning <http://bombich.com/kb/discussions/source-disk-becomes-full-when-cloning>](http://bombich.com/kb/discussions/source-disk-becomes-full-when-cloning)
- [System hangs during scheduled backup task <http://bombich.com/kb/discussions/having-finished-backup-task-launches-if-connecting-specific-firewire-disk-waking-up>](http://bombich.com/kb/discussions/having-finished-backup-task-launches-if-connecting-specific-firewire-disk-waking-up) (Sophos)

- [Problem with CCC and F-Secure 2011 virus scanner](http://bombich.com/kb/discussions/problem-ccc-and-f-secure-2011-virus-scanner) <<http://bombich.com/kb/discussions/problem-ccc-and-f-secure-2011-virus-scanner>>
- [McAfee changes modification date of files on the destination](http://bombich.com/kb/discussions/unchanged-files-being-archived) <<http://bombich.com/kb/discussions/unchanged-files-being-archived>>
- [Backup task is slower than it should be](http://bombich.com/kb/discussions/change-in-time-backup) <<http://bombich.com/kb/discussions/change-in-time-backup>> (VirusBarrier)
- [Slow performance during backup](http://bombich.com/kb/discussions/slow-incremental-clone) <<http://bombich.com/kb/discussions/slow-incremental-clone>> (F-Secure)
- [Symantec Internet Security may cause kernel panics during a backup task](http://bombich.com/kb/discussions/ccc-causes-my-os-x-lion-10.7.4-panic) <<http://bombich.com/kb/discussions/ccc-causes-my-os-x-lion-10.7.4-panic>>
- BitDefender may generate excessive read activity on the destination volume during a backup task, and may cause the destination device to spontaneously eject. Add the destination volume to BitDefender's exclusion list to avoid the problem.
- We have received a report that agreeing to Webroot SecureAnywhere's request to "remove threats" during a backup task can produce a non-bootable backup.
- Little Flocker (now Xfence) can interfere with some of the subtasks required (e.g. creating a kernel extension cache, blessing the destination) to make a cloned system volume bootable.
- We have received and confirmed a report in which Sophos CryptoGuard can have a debilitating effect on system performance while running a backup task.
- We have received several reports that McAfee's FileCore and Symantec's Data Loss Prevention software can cause the backup task to hang or to take a very, very long time. The applicable daemon processes may also consume an exceptional amount of CPU during a backup task leading to debilitating system performance for the duration of the task.
- We have received a report that ESET Endpoint Security can cause the backup task to hang or to take a very, very long time.
- We have received a report that Bit9 Carbon Black can cause the backup task to hang or to take a very, very long time.
- We have received a report that TrendMicro's "filehook" service can cause the backup task to hang or to take a very, very long time.
- We have received a report that Cylance's "CyProtectDrvOSX" kernel extension can cause the backup task to hang or to take a very, very long time.
- We have multiple reports in which [CoSys Endpoint Protector](https://www.endpointprotector.com/) <<https://www.endpointprotector.com/>> prevents CCC from backing up a pair of video-related system files (e.g. /Library/CoreMediaIO/Plug-Ins/DAL/AppleCamera.plugin).
- We have received reports that Avira antivirus may terminate CCC's file copier resulting in an incomplete backup. Avira "Real time protection" will also cause the backup task to take a very long time and consume an exceptional amount of CPU resources.

Antivirus Software concerns regarding the BaseSystem.dmg file

There is a file named "BaseSystem.dmg" on the Recovery volume associated with your Mac's startup disk. That disk image file contains the lightweight recovery operating system that is used when your Mac is booted in Recovery mode. At the beginning of every backup task that backs up a startup volume, CCC mounts the recovery volume and creates an archive of the data on that volume. Copying the "BaseSystem.dmg" file is part of that procedure. CCC stores an archive of the recovery volume at /Library/Application Support/com.bombich.ccc/Recovery on the startup disk so that the archive can be included in the backup of that volume.

We have received some reports of users seeing a dialog window (presented by antivirus software) reporting that "the BaseSystem.dmg disk image is being opened", perhaps with a suggestion that the disk image contains a virus or malware. This dialog appears and disappears very quickly, and some users are understandably concerned about the presence and erratic behavior of that dialog. Lacking any creditable information from the AV software, users naturally turn to the Internet, and unfortunately are greeted with terrible advice and misinformation. The BaseSystem.dmg file is not a virus. You should not attempt to delete parts of the operating system.

Users that have attempted to delete that file are prompted for admin credentials, and the deletion attempt still fails.

Contrary to what AV software purveyors may claim, the prompt for admin credentials is not coming from a virus, it's coming from macOS because you're trying to delete system files. The attempt to delete system files subsequently fails thanks to macOS's System Integrity Protection. This is not an attempt to get your admin credentials, it's normal macOS system processes working to protect the operating system. The BaseSystem.dmg file is not a virus. You should not attempt to delete parts of the operating system.

If you're seeing a dialog related to the BaseSystem.dmg file and it occurs at the beginning of a CCC backup task, this is a false positive from your antivirus software. Please contact your antivirus application vendor and ask them to fix that. Making a backup of the BaseSystem.dmg file is not something that should be brought to your attention.

Related Documentation

- [CCC automatically manages the special "helper" volumes on APFS-formatted destinations](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition#apfs) <<http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition#apfs>>
- [Apple Kbase HT201314: About macOS Recovery](https://support.apple.com/en-us/HT201314) <<https://support.apple.com/en-us/HT201314>>

CCCはどのような条件を使って、ファイルを再コピーする必要があるかどうかを判断しますか？

CCCはソースとコピー先で異なる項目のみをコピーするよう設定されています。つまり、バックアップタスクを完了後、次の日にもう1度実行した場合、CCCは最後のバックアップタスク後に作成または変更された項目のみをコピーします。CCCはそのサイズと変更日を使用してファイルが異なるかどうかを判断します。もしファイルのサイズまたは変更日がソースとコピー先でまったく異なる場合、CCCはそのファイルをコピー先にコピーします。

CCCが**すべての**ファイルを再コピーしていると結論付ける前に、CCCのタスク履歴ウインドウからもっとも最近完了したタスクを開き、**ソースのデータセットの合計サイズとコピー済みデータ**の値を比較してください。例えば、2から5GBほどのファイルが、たとえ、ソースボリュームになんの変更も加えていないように思える時でさえ、毎日のバックアップでアップデートされることは珍しくありません。macOSはさまざまなキャッシュとログファイルを休みなくアップデートしています。そしてこれらが1日の終わりには実に蓄積されているのです。コピーされたデータ量が総データセットのほんの一部だとするなら、コピーされたデータ量はおそらく正常です。

組織的変更は大容量のデータが再コピーされることにつながります

ソースボリュームに大規模な組織的変更を加えた場合、例えば、多くのデータを含むフォルダを移動した、またはその名前を変更した場合、それらの項目へのパスが変更されたので、多くの項目がコピー先に再度コピーされるという結果になります。バックアップタスクを実行する前に同じ組織的変更をコピー先に適用することで、この再コピーの動作を回避することができます。

アンチウイルスアプリケーションがファイルの変更日を実際に変更することがある

CCCがファイルをコピー先にコピーした後、一番最後にするのはファイルの変更日をソースファイルの変更日に設定することです。このファイルシステムのアクティビティは、アンチウイルスソフトにファイルをスキャンするよう指示します。これは一般的には問題ありません（たとえバックアップタスクのパフォーマンスが低下しても）。ファイルを読むだけではそのファイルの変更日を変更するには当たりません。それで、うまく設計されたアンチウイルスアプリケーションはCCCがコピーしたファイルをスキャンすることで害を及ぼすことはありません。けれども、アンチウイルスアプリケーションがファイルに“手をつける”、つまりファイルに変更を加える時、変更日は現在の日付に変更されます。

コピー先のファイルの変更日がバックアップタスクの日時に設定されようとする場合、CCCがコピーした後に、アンチウイルスソフト、または他の背景サービスがファイルに変更を加えている可能性が高いと考えられます。アンチウイルスソフト（または他のソフトウェア）による変更日の改ざんを解決できない場合は、CCCがコピー先の新しいファイルをアップデートしないように設定できます。この設定を適用するには、CCCのメインアプリケーションウインドウからバックアップタスクを選択してから：

1. 高度な設定をクリックします。
2. トラブルシューティングボックスの中の**コピー先の新しいファイルをアップデートしない**のボックスをチェックします。
3. タスクを保存して実行してください。

関連ドキュメント

- アンチウイルスソフトがバックアップを干渉する <<http://bombich.com/ja/ja/kb/ccc5/antivirus-software-may-interfere-backup>>
- 高度な設定 <<http://bombich.com/ja/ja/kb/ccc5/advanced-settings>>

一部のファイルシステムで時間帯の変化が変更日に影響する

HFS+、APFS、NTFS、およびその他の最近のファイルシステムは協定世界時 (UTC、注：GMTに匹敵) を基にファイルの変更日を保存しています。一方、FATファイルシステムは、ファイルの変更日をコンピュータのローカル時間帯設定を基に保存しています。一般的にこの差は問題ではありませんが、FATボリュームとNTFSまたはMacフォーマットのボリュームの間で

(または、Macフォーマットのファイルシステムとタイムスタンプにローカル時間を使用するNASデバイスの中で) ファイルをコピーする場合、問題が生じます。時間帯と夏時間が変化する間に、FAT32ボリュームのファイルの変更日は変化してしまいます。その結果、CCCはこれらのファイルの日付が古いとしてそれぞれのファイルを再度コピーします。残念ながら、CCCはこのFATファイルシステムの欠点を正しく設定し直すことはできません。そのため、ファイルをFATボリュームに (または、から) コピーする必要がある場合、呼応するソースまたはコピー先のボリュームもFATフォーマットされていることをお勧めします。

Microsoft MSDN ライブラリ : File Times <[https://msdn.microsoft.com/en-us/library/ms724290\(VS.85\).aspx](https://msdn.microsoft.com/en-us/library/ms724290(VS.85).aspx)>

前述のファイルシステムのバックアップを使って夏時間への移行を処理するには

この問題に遭遇した場合、上記で提案された高度な設定、**コピー先の新しいファイルをアップデートしない** を使用することで、夏時間への変更のうちの1つの問題が解決しますが、もう1つの問題は解決しません。もう1つのアプローチは、タイムスタンプの差においてもっと寛大な解決策を使用するようCCCを設定することです。CCCのグローバル “ NASTimestampLeniency ” の属性を設定することで達成できます。これは、CCCのコマンドラインユーティリティ (“ ターミナル ” アプリケーションなどで) を使って設定できる高度なグローバル設定オプションです :

```
"/Applications/Carbon Copy Cloner.app/Contents/MacOS/ccc" -g NASTimestampLeniency int 3601
```

この設定を使うと、コピー先の同じファイルの変更日内でファイルの変更日が1時間 (と1秒) 以内であればCCCはファイルを再コピーしません。ファイルサイズの差が優先権を持つことに注意してください。また、これがグローバル設定である一方、この設定は非HFSおよび非APFSのソースまたはコピー先があるタスクにのみ適用されます (設定の名前に関わらず、NASファイルシステムに制限されません)。起動可能なバックアップタスクがある場合、この設定は適用されません。

メールの “ 接続動作状況のログを記録 ” を設定すると非常に大きなファイルが作成されます

メールの “ 接続診断 ” ウィンドウで “ 接続動作状況のログを記録 ” を有効にして、その設定を無効にするのを忘れると、メールは膨大なログファイルを作成して、やがて起動ディスクがいっぱいになります。CCCがバックアップの度に異常に大量のデータをコピーしていて、バックアップが連続して実行されていることもあることに気付いたら、以下の手順を実行して、この大量のデータがメールのアクティビティログに関連していないかを検証してください:

1. メールを開きます
2. “ ウィンドウ ” メニューから “ 接続診断 ” を選択します
3. “ 接続動作状況のログを記録 ” の横にあるボックスのチェックマークを外します
4. Finderで、Optionキーを押したまま、Finderの “ 移動 ” メニューから “ ライブラリ ” を選択します
5. ライブラリ > コンテナ > com.apple.mail > データ > ライブラリ > ログ > メール、と進みます
6. 大容量のログファイルを削除してください

"CCC found multiple volumes with the same Universally Unique Identifier"

Occasionally a circumstance arises in which CCC presents the following error message before creating or running a backup task:

CCC found multiple volumes with the same Universally Unique Identifier that was associated with the volume you designated as the source/destination for this task.

CCC cannot proceed with confidence in having correctly identified the volume you originally chose when you configured this backup task. Unmount one of the conflicting volumes and try the task again, or please choose "Ask a question" from CCC's Help menu to get help resolving the issue.

Most modern operating systems apply a universally unique identifier to a new volume when you format that volume (e.g. in Disk Utility). Volumes should never have the same identifier, these identifiers are called "universally unique" because they're supposed to be unique, universally! [Wikipedia <https://en.wikipedia.org/wiki/Universally_unique_identifier#Random_UUID_probability_of_duplicates>](https://en.wikipedia.org/wiki/Universally_unique_identifier#Random_UUID_probability_of_duplicates) notes that, for 122 bit UUIDs, there is a 50/50 chance of having a single duplicate UUID if 600 million UUIDs were allocated to every person on Earth. The chances of two volumes having the same UUID should, then, be slim enough that the UUID can be reliably used to positively identify the source and destination volumes.

Given these odds, it is statistically more likely that CCC's discovery of a duplicate UUID is due to a hardware or software problem rather than to two volumes randomly having the same UUID. Therefore, CCC makes the conservative decision to not back up to either volume if another volume with the same UUID is detected.

Unfortunately, it has come to our attention that many Iomega and Western Digital drives that are pre-formatted for macOS are stamped with the same UUID at the factory. As a result, this situation can arise if you own and attach two "factory fresh" Iomega hard drives to your computer.

Solution

Reformatting one of the affected volumes will resolve the problem, however there is a non-destructive solution:

1. Hold down Control+Option and click on one of the volumes that was identified as having a non-unique identifier in CCC's sidebar
2. Choose the "Reset UUID" contextual menu item
3. Try configuring your backup task again

Note: This procedure may cause bootability problems for a volume that is intended to boot non-Apple computers (aka "Hackintoshes"). Those issues are beyond the scope of our support.

Identity problems specific to Western Digital hard drive enclosures

We have been tracking an issue that can lead to CCC producing the alert described above in cases where a duplicate device is not physically present. Occasionally Western Digital volumes will drop offline (especially during a sleep/wake cycle, and sometimes in the middle of a backup task), but the macOS diskarbitration service errantly retains the virtual device object. When the volume remounts, it is assigned a new device identifier and virtual device object. At that point, any application that asks the macOS diskarbitration service for a list of disks and volumes will get duplicate values for the WD device. Most applications wouldn't care about the duplicate devices, but CCC tracks both mounted and non-mounted devices so that CCC can mount the source and destination at the beginning of the task, if necessary.

CCC works around the underlying macOS issue in every case where it's practical. The one case where it is impossible to reliably work around the issue is in cases where the affected volume is not mounted, but is physically attached to your Mac and currently has duplicate virtual objects on record in the diskarbitration service (both not mounted). If you encounter this scenario, please report this problem to us via the Report a Problem menu item in CCC's Help menu so we can add your OS and device details to our open problem report with Apple (rdar://28972958).

If you ever see two mounted instances of your Western Digital device in the Finder, you should immediately unmount the device, detach it from your Mac, and then restart your computer. In most of the cases we've seen, the duplicate instances of the device are unmounted and therefore harmless. In a couple cases, however, macOS mounted two instances of the volume and the volume wound up corrupted.

Potential workaround

Western Digital's Support Knowledgebase <<https://support.wdc.com/knowledgebase/answer.aspx?ID=18502>> states that the Put hard disks to sleep when possible setting should be disabled when using their external USB hard drives. If you're using a Western Digital external USB device, open the Energy Saver Preference Pane in the System Preferences application and uncheck the box next to the Put hard disks to sleep when possible setting.

Finder or App Store finds other versions of applications on the backup volume

Occasionally we receive reports of odd system behavior, such as:

- When opening a document, the application on the backup volume is opened rather than the version from your startup disk
- When trying to update an application in App Store, the update appears to fail — the older version is always present
- The destination volume cannot be (gracefully) unmounted because various applications or files are in use
- When choosing Open With... from a Finder contextual menu, duplicates of your applications appear in the list

These problems consistently go away if the destination volume is ejected.

These problems are ultimately caused by problems with the LaunchServices database, which is an issue outside of the scope of the backup process. There are a few things that you can do to address the problem:

Disable Spotlight on the destination volume

Disabling Spotlight indexing on the destination volume should prevent new additions being made to the LaunchServices database that reference the destination. Open the Spotlight preference pane, click on the Privacy tab, then drag your destination volume into the privacy tab. Check whether applications still open by default from the destination volume, because this step may be enough to address the issue.

Configure CCC to eject the destination volume at the end of the backup task

With an advanced setting, you can [configure CCC to unmount the destination](http://bombich.com/kb/coc5/performing-actions-before-and-after-backup-task#destpostactions) when CCC has finished copying files to it. By keeping the destination volume unmounted, Finder and App Store will be unable to find applications on that volume. You'll save wear and tear on that hard drive by keeping it spun down as well.

Reset the LaunchServices database

If applications still open from the destination volume, you can use this [Reset LaunchServices Register](http://bombich.com/software/files/tools/Reset_LaunchServices_Register.app.zip) application to reset the LaunchServices database, then restart your Mac.

Launchpad ignores settings created while booted from another volume

If you have assembled a custom arrangement of your application icons in the Launchpad application, you will discover that that arrangement is lost when booted from your backup volume. When you see this happen, you would naturally think, "Why didn't CCC copy the Launchpad settings?" In fact, though, CCC is faithfully copying the Launchpad settings. Here we'll show you how you can verify that, and also why the settings don't work while booted from your backup volume.

Verifying the fidelity of the backup copy of your Launchpad settings

The LaunchPad preferences database is stored in your home folder at this location:

```
/Users/yourname/Library/Application Support/Dock/{long number}.db
```

You can calculate a checksum of this file on the source and destination volumes (immediately after running a backup task) to verify that it matches, e.g. in the Terminal application:

```
[bombich:~]$ md5 /Library/Application/Support/Dock/*.db  
MD5 (/Users/bombich/Library/Application Support/Dock/861852F1-B632-455A-8632-78BC7137A959.db) =  
1988498deef00393db335a7015995413
```

```
[bombich:~]$ md5 /Volumes/Home/Backup/Users/bombich/Library/Application/Support/Dock/*.db  
MD5 (/Volumes/Backup/Users/bombich/Library/Application  
Support/Dock/861852F1-B632-455A-8632-78BC7137A959.db) = 1988498deef00393db335a7015995413
```

Why don't the settings work while booted from another volume?

If you boot from the backup volume, you may notice an additional database file in that folder (it will be removed every time your backup runs, though). That's the new settings file that Launchpad creates because it's ignoring the settings file from your original volume.

If you examine the contents of that database file †, you'd see references to each application that resides in Launchpad. It's these references to your applications that are not "portable". Rather than referencing the application based on its relative path to your startup disk, the references are complex, proprietary "bookmark" data. These bookmark data have references to several defining attributes of the application files, such as path, name, volume unique identifier, and inode number. This allows you to move these applications around on your startup disk without breaking things inside of Launchpad. Unfortunately, though, the bookmark data is completely meaningless when you're booted from a physically different volume, because those attributes within the bookmark are volume specific. It is not possible to alter the contents of this database such that the references will point to the cloned volume.

† Paste this in Terminal to get a "dump" of the database:

```
sqlite3 /Library/Application/Support/Dock/*.db
```

"The task was aborted because a subtask did not complete in a reasonable amount of time"

Occasionally a backup task can stall if the source or destination stops responding. To avoid waiting indefinitely for a filesystem to start responding again, Carbon Copy Cloner has a "watchdog" mechanism that it uses to determine if its file copying utility has encountered such a stall. By default, CCC imposes a ten minute timeout on this utility. If ten minutes pass without hearing from the file copying utility, CCC will collect some diagnostics information, then stop the backup task. Our support team can analyze this diagnostic information to determine what led to the stall.

Common factors that lead to stalls

Hardware problems are the most common cause of a stall. There are a few other factors that can lead to a stall, though, depending on how the backup task is configured:

- Filesystem corruption or media problems on the source or destination can prevent that filesystem from providing a file or folder's filesystem entry
- A firmware problem in an external hard drive enclosure can cause that device to stop responding
- File sharing service errors can lead a network volume to become unresponsive
- Access to a network volume via a wireless connection may become slow enough that the volume stops responding
- Excessive bandwidth competition from other software can cause a volume to appear unresponsive, though it may just be responding very slowly

Troubleshooting suggestions

The first thing you should do if a task ends with this result is to reboot your Mac and run the task again. In many cases, an unresponsive filesystem is a transient problem, and the simple act of restarting will get the volume remounted in a better state. If the problem recurs, please choose Report a problem from CCC's Help menu and our support team can offer more specific troubleshooting suggestions. Below is a list of some of the troubleshooting suggestions we may offer depending on how your task is configured.

- Use Disk Utility's First Aid tool to check for any filesystem problems on the source volume. If any are discovered and the source is your startup disk, reboot while holding down Command+R (Intel Macs) or the Power button (Apple Silicon Macs) to boot in [Recovery Mode <https://support.apple.com/en-us/HT201314>](https://support.apple.com/en-us/HT201314), then use Disk Utility to repair the problems. Please note: A report of "No problems found" from Disk Utility does not mean that there are no problems with that volume. There are no hardware diagnostic utilities on the market that will inform you of a problem with a cable, port, or enclosure, or report a bug in the firmware of a hard drive or SSD.
- Exclude a file or folder from the backup task. Select Selected files... from the Clone popup menu (underneath the Source selector), then uncheck the box next to the item that the source filesystem is unable to read.
- Remove a corrupted item from the destination volume.
- Erase the destination volume (we make this recommendation sparingly, and only when the stall can be definitively identified as a filesystem problem on the destination).
- Disable Spotlight on the destination volume to reduce bandwidth competition. To disable Spotlight, open the Spotlight preference pane, click on the Privacy tab, then drag the backup volume into the Privacy table. This only affects the destination volume, and it's reversible, you can remove it from that list should you decide that you want to re-enable indexing.
- If the stalling volume is a network volume, connect your Mac and the host of the network volume to the network via a wired connection (i.e. rather than via a wireless connection, if applicable).

-
- If the stalling volume is a network volume, eject that volume in the Finder, then [remount the volume using a different file sharing protocol <http://bombich.com/kb/ccc5/backing-up-to-from-network-volumes-and-other-non-hfs-volumes#nasEINVAL>](http://bombich.com/kb/ccc5/backing-up-to-from-network-volumes-and-other-non-hfs-volumes#nasEINVAL) .
 - If you have DriveGenius installed, that software may be performing a verification on the destination that "freezes" the volume for the duration of the verification. DriveGenius support suggests that you create a file in the root of the destination volume with the name ".com.prosofteng.DrivePulse.ignore" (no quotes) to stop Drive Pulse from acting on that volume.

Troubleshooting slow performance when copying files to or from a network volume

Network performance is usually the bottleneck of a backup task that copies files to or from a network volume, but there are several other factors that can affect performance as well. Here are some suggestions for improving the performance of your NAS-based backups.

Use ethernet instead of WiFi

Backing up data over a wireless connection will be considerably slower than backing up over an ethernet connection. 802.11n networks support approximately 300 Mb/s of rated (theoretical) bandwidth under the best conditions, but they usually operate at much lower speeds (130 Mbps and below, which is comparable to 16 MB/s). Bandwidth drops considerably as you get further from the base station (a wooden door between your Mac and the router will cut the signal in half), and the file sharing protocol overhead will reduce your achievable bandwidth yet more. So practically speaking, you're lucky to get 8 MB/s over a wireless connection while sitting right next to the base station. If you're running Yosemite or later, that performance could be cut in half due to Apple Wireless Direct Link (AWDL), which causes the Airport card's interface bandwidth to be shared between your ordinary WiFi network and an ad hoc network hosted by your Mac.

We performed a simple bandwidth test to a fourth generation Airport Extreme Base Station (802.11n) to demonstrate the performance decline. We copied a 100MB file to an external hard drive attached to the base station via USB in three scenarios: 1. An ethernet connection to the base station, 2. Sitting a few feet from the base station, and 3. Sitting across the house from the base station (35 feet, no line of sight to the base station). The results were 6.5s (15.5 MB/s), 18.7s (5.3 MB/s), and 256s (0.39 MB/s) for the three scenarios, respectively. So, before you try to back up over a wireless network, consider running a simple test in the Finder to see just how fast your connection is. If it takes more than a minute to copy a 100MB file, your connection is too slow to be practical for backup purposes.

Eject the network volume in the Finder

Our first recommendation is to eject your network shares in the Finder, then run your task again. We have run several tests and positively identified an issue in which the Finder will make repeated and ceaseless access attempts to the items of a folder on your network share if you simply open the network volume in the Finder. This persists even after closing the window. If you eject the network volume(s), then run your CCC backup tasks, CCC will mount the network volume privately such that it is not browseable in the Finder.

Disable support for extended attributes

If a performance issue persists despite trying the steps above, you can try dropping the extended attributes from the source. While it is our preference to preserve extended attributes, Apple considers extended attributes to be "disposable" because some filesystems cannot support them.

1. Open CCC and select your backup task.
2. Click the Advanced Settings button.
3. Check the box next to Don't preserve extended attributes in the Troubleshooting Options box.
4. Save and run the task.

Try using AFP instead of SMB to connect to the NAS

Apple deprecated AFP many years ago, but it still remains faster and more reliable than SMB in many cases. To try

AFP instead of SMB:

1. Eject the NAS volume if it's currently mounted
2. Choose "Connect to Server" from the Finder's Go menu
3. Type in "afp://{server address}" to connect to the NAS volume via AFP
4. Open CCC and select the applicable backup task
5. Drag the currently-mounted NAS volume (or folder or disk image on that volume) onto CCC's source or destination selector (whichever is applicable for your particular task)

Avoid running tasks simultaneously if they read from or write to the same NAS device

Especially with locally-attached source volumes, CCC won't have any trouble saturating your network connection with a single backup task. If you run more than one task at the same time, especially to the same NAS device, the network connection or the NAS device may not be able to handle the load. Leverage CCC's [task chaining functionality](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#chaintasks) <<http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#chaintasks>> , or [place your tasks into a task group](http://bombich.com/kb/ccc5/task-organization) <<http://bombich.com/kb/ccc5/task-organization>> so that they will be run sequentially instead.

Consider backing up to a disk image on the NAS device rather than directly to it

Network file sharing is a surprisingly CPU-intensive task. While network appliances are well suited to the task of serving media to multiple workstations, the overhead of individual filesystem transactions makes them less suited to the task of backing up millions of files. Media files, in comparison, are generally large and the required data rate for streaming media is relatively low. Consider a 1-hour, 1GB HD movie file. Streaming 1GB over the course of an hour requires only 0.27MB/s. That's an easy task, even over a weak wireless network. But if you want to back up 100GB of data in an hour, and that 100GB is made up of a million smaller files, then a network appliance may not be up to that task.

The actual bandwidth that you achieve in your backup task will be based on the number of files you're copying, the file size distribution, and the number and size of extended attributes in the source data set. Copying large files (e.g. media files) to a network volume will achieve the maximum potential bandwidth, while copying lots of small files will take quite a bit longer due to network filesystem overhead. If the data that you're backing up consists primarily of large files, e.g. music, photos, video — backing up directly to a network appliance will be fine. If you're backing up system files or applications, or many files that are smaller than a few MB, we recommend that you [back up to a disk image on your network appliance](http://bombich.com/kb/ccc5/i-want-back-up-my-whole-mac-time-capsule-nas-or-other-network-volume) <<http://bombich.com/kb/ccc5/i-want-back-up-my-whole-mac-time-capsule-nas-or-other-network-volume>> to improve performance and to maintain important filesystem metadata.

Where can I find CCC's log file?

It is our aim to have the Task History window provide the user with enough information to find and troubleshoot any problems they're having with their backup tasks. For debugging and support purposes, however, CCC logs its activity in the following files:

- Task Activity: /Library/Application Support/com.bombich.ccc/phtdebug.log
- Task Editing: /Library/Application Support/com.bombich.ccc/ccdebug.log
- CCC User Agent: /Library/Application Support/com.bombich.ccc/uaddebug.log
- Remote Mac Authentication Agent: /Library/Application Support/com.bombich.ccc/sshauthdebug.log

Tip: Hold down Command+Option and choose Open Debug Logs from the Carbon Copy Cloner menu to open these four files in the Console application.

If there's something specific that you're retrieving from the log that is not presented in the Task History window, [please let us know <http://bombich.com/software/gethelp>](http://bombich.com/software/gethelp) . We'd prefer to consider exposing that information in the Task History window so you don't have to dig through the log. Also, note that basic details of task history are exposed in CCC's command-line utility, so that may be an easier way to get the information.

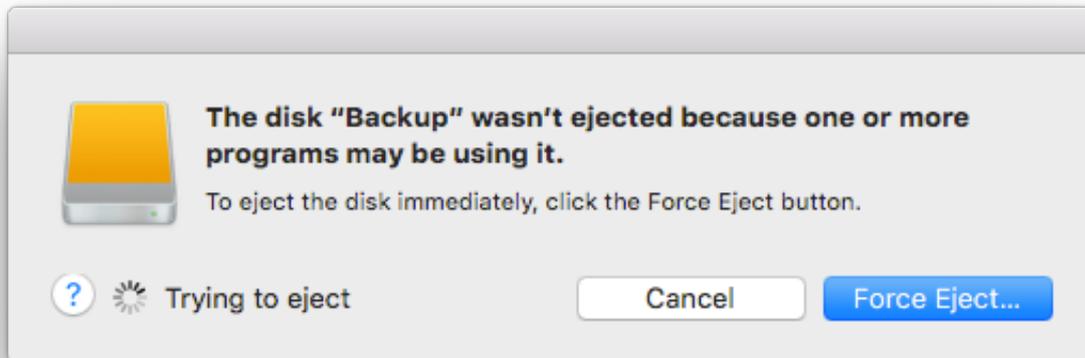
Where can I find a list of every file that CCC has copied?

CCC does not retain that information for each backup task. If you're concerned that CCC is copying too many or too few files, please [contact us for assistance <http://bombich.com/software/gethelp>](http://bombich.com/software/gethelp) .

Related documentation

- [Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks <http://bombich.com/kb/ccc5/using-ccc-command-line-tool-start-stop-and-monitor-ccc-backup-tasks>](http://bombich.com/kb/ccc5/using-ccc-command-line-tool-start-stop-and-monitor-ccc-backup-tasks)
- [Why is CCC recopying every file during each backup? <http://bombich.com/kb/ccc5/why-ccc-recopying-every-file-during-each-backup>](http://bombich.com/kb/ccc5/why-ccc-recopying-every-file-during-each-backup)
- [How do I get help? <http://bombich.com/kb/ccc5/how-do-i-get-help>](http://bombich.com/kb/ccc5/how-do-i-get-help)

Why can't I eject the destination volume after the backup task has completed?



Occasionally this annoying message comes up when you're trying to eject your destination volume. If CCC is currently using that volume as a source or destination to a running backup task, then CCC will effectively prevent the volume from being unmounted gracefully. If your backup task isn't running, though, CCC isn't preventing the volume from being unmounted. But what application is?

If this occurs within a minute or so after the backup task completes, it's probably caused by macOS's "kextcache" utility — that utility rebuilds a cache file on the destination that is required for startup. That process usually finishes after a minute or two, and usually the destination can be ejected when that completes. If this frequently affects your backup volume, you can ask CCC to unmount the destination after the backup task completes. CCC will wait for kextcache to finish, resulting in a more reliable (and automated!) ejection of the destination at the end of the backup task:

1. Open CCC and select your backup task.
2. Click the Advanced Settings button.
3. In the After Copying Files box, choose the option to [unmount the destination volume](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#destpostactions) after the backup task completes.
4. Save and run your backup task.

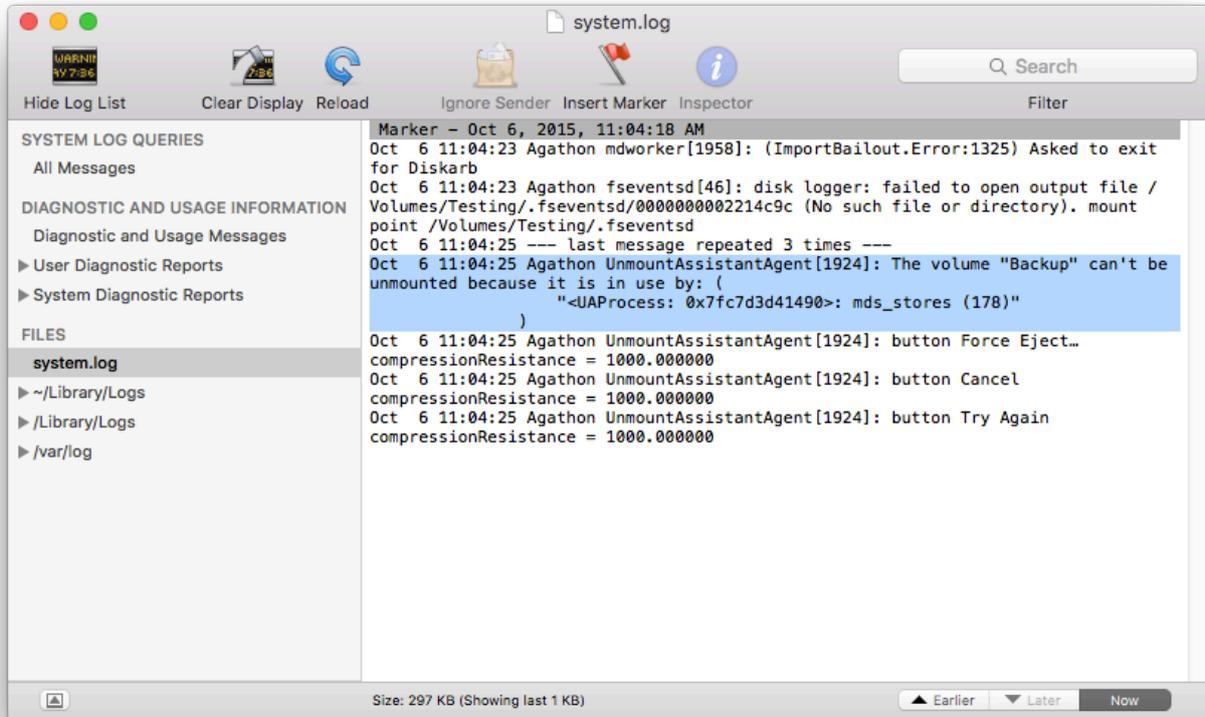
If the disk cannot be unmounted several minutes after the backup task has completed, or if CCC is also unable to eject the destination, use the Console application to track down the culprit.

Sierra and later OSes:

1. Open the Console application (in /Applications/Utilities)
2. Type or paste UnmountAssistantAgent into the Search field in the toolbar

El Capitan and earlier OSes

1. Open the Console application (in /Applications/Utilities)
2. Click on system.log in the sidebar
3. Go to the Edit Menu > Find > Find... (or press Command+F) to search for messages from the UnmountAssistantAgent application. Avoid using the Search field in the toolbar for this search, because that will hide important context.



In the example above, we can see that an application named `mdsstores` is preventing the Backup volume from being ejected. `mdsstores` and `mdworker` are Spotlight helper applications, so the issue here is that Spotlight is preventing the destination from being ejected. We have received numerous reports showing the same culprit since El Capitan was introduced. To resolve the conflict caused by Spotlight, you can disable Spotlight on the destination volume:

1. Open the Spotlight preference pane
2. Click on the Privacy tab
3. Drag the backup volume into the Privacy table

Disabling Spotlight in this manner only affects the destination volume, and it's reversible — you can remove your destination volume from that list should you decide that you want to re-enable indexing.

Other applications that frequently prevent volumes from unmounting

We've received (and confirmed) reports of the following applications causing trouble with volume unmounts. If you have one of these applications, you should see if you can add your CCC backup volume to a "whitelist" within that software to avoid the interference it causes. The name of the offending process (which is what you would see in the Console application) is noted in parentheses.

- BitDefender (BDLDaemon)

- Time Machine (backupd)
- Spotlight (mds or mdsstores)
- Disk Drill (cfbackd)
- Retrospect (RetrospectInstantScan)
- CleanMyDrive
- Intego Virus Barrier (virusbarriers)
- AppCleaner (AppCleaner SmartDelete)
- AVG AntiVirus (avgoad)
- ClamXAV

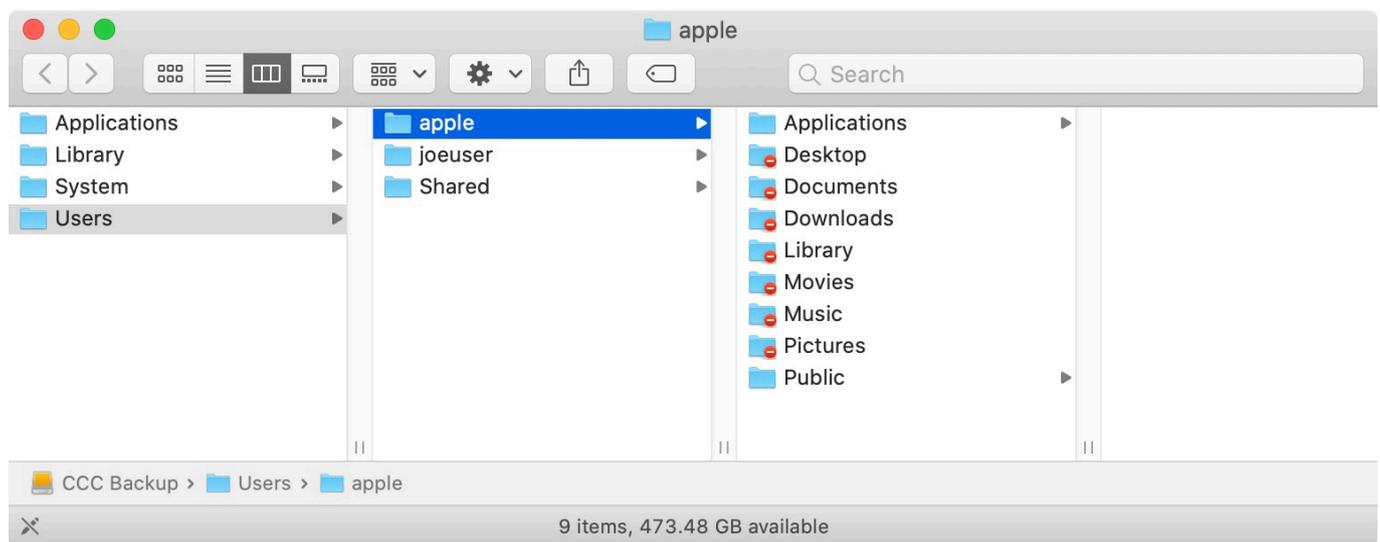
Remove any duplicate keychain entries in the Keychain Access application

Sometimes references to the keychain files on your backup volume can show up in the Keychain Access application. As a result, any application that leverages Keychain Services (e.g. Safari) will maintain an open file handle on the keychains on your backup disk, thus preventing that disk from unmounting. To resolve this, open the Keychain Access application (in /Applications/Utilities) and look for any duplicate keychain references in the sidebar. If you see duplicates, hover your mouse over those item until a tooltip appears revealing the path to the keychain file. If the keychain file is located on your backup disk, click on the keychain, then press the Delete key. When prompted, remove the references to the keychain file, not the file.

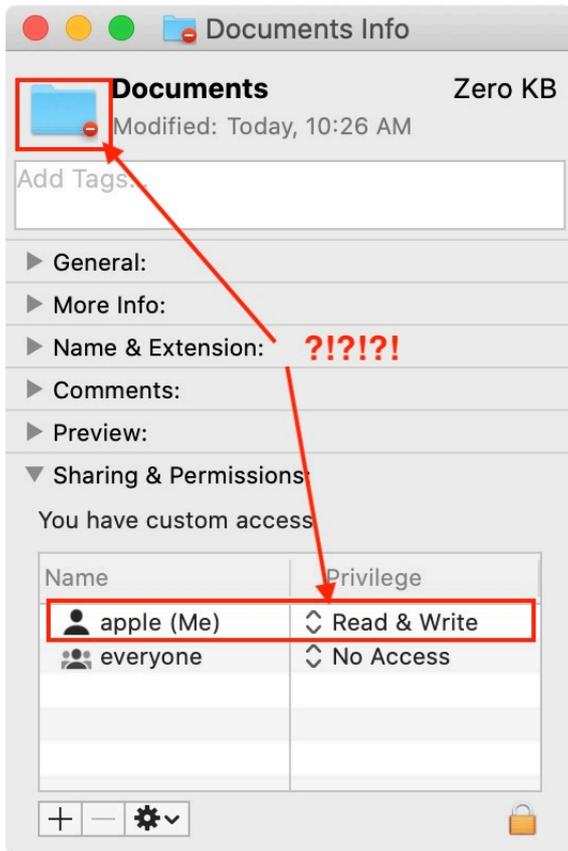
Why does Finder prevent me from viewing the home folder on my backup when it's attached to another Mac?

Update November 2020: Apple has resolved this Finder bug in macOS Big Sur.

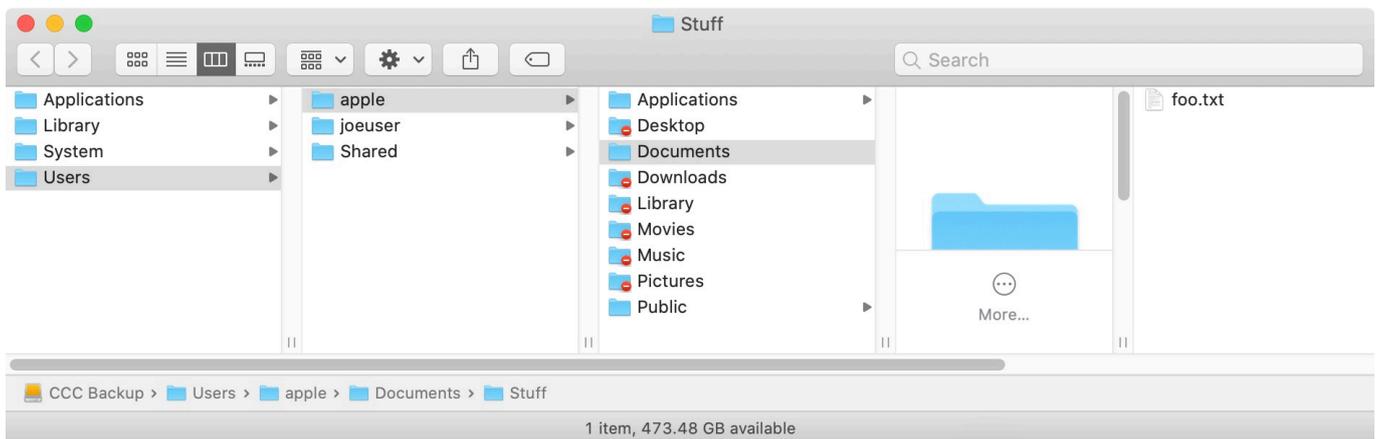
We are currently tracking a Finder bug in which the Finder incorrectly determines your access to some folders. The issue occurs when an "access control list" is applied to a folder and when ownership is disabled on the backup volume. Ownership is disabled by default when you attach your backup volume to a different Mac, and the folders in your home directory each have an access control list, so we often see this problem when trying to access the contents of the home folder on a backup disk when that backup disk is attached to some other Mac. Here's what you might see in the Finder:



Naturally, you might think, "OK, I'll just correct the permissions". But, if you select one of those folders and choose "Get Info" from the Finder's File menu, you'll discover that you already have Read & Write privileges for that folder!



The information in the Get Info panel is contradictory — on one hand, you have no access to the folder (indicated by the universal "no access" badge applied to the folder icon). According to the Sharing & Permissions section, though, you have full read and write access. If you try to access the contents of that folder via the Terminal, you can view and open the folders just fine. In fact, you can even reveal items nested within these folders in the Finder, with a really odd artifact!



There is nothing inherently wrong with these folders on the backup volume — CCC has retained file ownership and permissions such that the backup can be properly restored back to the original Mac. In fact, you shouldn't see this Finder bug if you boot the other Mac from the backup. If you're doing a one-time transfer of files to the other Mac, booting from the backup is one option to avoid this Finder bug.

How can I set up my backup task to regularly share files between two Macs?

If you're trying to set up a backup task that allows you to regularly transfer files between two Macs, then a better

solution is to set up a folder-to-folder backup:

1. Drag the folder whose contents you'd like to share between Macs to CCC's Source selector
2. Create a new folder on the destination volume and drag that new folder onto CCC's Destination selector
3. Click the Advanced Settings button
4. Check the box next to Don't preserve permissions
5. Save and run the task

Your account on the second Mac should then have no trouble accessing the contents of that new folder on the backup disk.

Can I keep my backup bootable, yet also occasionally access my files on another Mac?

If your goal is to create a bootable backup that you occasionally use to transfer files between Macs, and if enabling ownership on the volume does not resolve the access issue, then we have developed a workaround that will avoid this Finder bug. Drag the affected folders (or your entire home folder) from the backup volume onto our [Finder bug permissions workaround script <http://bombich.com/software/files/tools/finderpermsbug.zip>](http://bombich.com/software/files/tools/finderpermsbug.zip) †. This script will remove the access control entries and set your current user account as the owner. Keep in mind that this change will be reversed when you attach the disk to the original Mac and re-run the backup task, so keep the script handy if you're using this disk between Macs frequently.

†Catalina users: Gatekeeper throws a wrench into this workaround. [Download this script instead <http://bombich.com/software/files/tools/finderpermsbug.sct>](http://bombich.com/software/files/tools/finderpermsbug.sct) and run the script from within the Script Editor application.

Some third-party storage drivers may cause hardware misbehavior

We occasionally receive reports of strange behavior from USB devices, e.g. slow performance, disks dropping offline in the middle of the backup task. In some of those cases we've discovered that third-party storage drivers are causing the problem. In particular, the SAT-SMART drivers and some ancient BlackBerry USB drivers can lead to problems. If you're troubleshooting a USB device behavior or performance problem, we recommend that you consider uninstalling these drivers.

Removing BlackBerry drivers

Assuming you're not actively using any USB BlackBerry devices with your Mac, we recommend uninstalling that old software. BlackBerry doesn't offer an uninstallation guide, but [this helpful forum post makes a recommendation <https://superuser.com/questions/647762/how-can-i-remove-blackberry-tools-entirely-from-os-x>](https://superuser.com/questions/647762/how-can-i-remove-blackberry-tools-entirely-from-os-x). Simplifying those instructions a bit:

Choose "Computer" from the Finder's Go menu, then navigate to these locations to find extension and agent components (you may not have all of these locations on your version of macOS):

Macintosh HD > Library > LaunchAgents
Macintosh HD > Library > LaunchDaemons
Macintosh HD > Library > Extensions
Macintosh HD > System > Library > Extensions
Macintosh HD > Library > StagedExtensions > Library > Extensions

If you find the BlackBerry components in those folders, just drag them to the Trash, authenticating when prompted. When you're done, reboot. Here's a complete list of components that the website recommended that you remove (you may not find all of these components, but hopefully you can at least find and remove the extensions):

/Library/Application Support/BlackBerry
/Library/Application Support/BlackBerryDesktop
/Library/Frameworks/RimBlackBerryUSB.framework
/Library/LaunchAgents/com.rim.BBLaunchAgent.plist
/Library/LaunchDaemons/com.rim.BBDaemon.plist

/System/Library/Extensions/BlackBerryUSBDriverInt.kext
/System/Library/Extensions/RIMBBUSB.kext
/System/Library/Extensions/RIMBBVSP.kext

Removing SAT-SMART drivers

The [SAT-SMART drivers <https://github.com/kasbert/OS-X-SAT-SMART-Driver>](https://github.com/kasbert/OS-X-SAT-SMART-Driver) aim to offer SMART support for USB devices. These drivers have not been actively maintained since late 2016, so their compatibility with newer macOS releases is dubious. Their uninstallation instructions may also be out of date for newer macOS releases, so we offer the following suggestion.

Choose "Computer" from the Finder's Go menu, then navigate to these locations to find extension components (you may not have all of these locations on your version of macOS):

Macintosh HD > Library > Extensions
Macintosh HD > System > Library > Extensions

Macintosh HD > Library > StagedExtensions > Library > Extensions

If you find the SAT-SMART components in those folders, just drag them to the Trash, authenticating when prompted. When you're done, reboot. Here's a list of components that may be installed by the SAT-SMART installer (you may not find all of these components, remove as many as you find):

Library/Extensions/SATSMARTDriver.kext
Library/Extensions/SATSMARTLib.plugin
Library/Extensions/SATSMARTDriver.kext
Library/Extensions/SATSMARTLib.plugin

APFSの複製に関するトラブルシューティング

AppleのAPFSレプリケータは通常処理速度が速く、なんの問題ありませんが、状況によってはうまく（または、まったく）処理できないことがあります。CCCはこれらの残念な結果をできるだけ回避するように動作しますが、もしAppleのAPFSレプリケータが失敗した場合に備えて、以下のことを推奨します。

CCCから “ APFSの複製処理を完了できませんでした ” と報告がありました

最初のバックアップの試みが失敗した場合、以下の手順を試してください。これらの手順を試した後も問題が継続する場合は、[次のセクションからその他のアドバイスをご覧ください](#)。

1. Macを再起動します
2. 一般的なハードウェアの問題を排除 <<http://bombich.com/ja/ja/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems#steps>>して、コピー先デバイスがMacのUSBまたはThunderboltのポートに直接接続されているか確認してください（ハブは避けてください）。競合する可能性のあるハードウェアドライバはすべて取り外す <<http://bombich.com/ja/ja/kb/ccc5/some-third-party-storage-drivers-may-cause-hardware-misbehavior>> ことも考えてください。
3. ディスクユーティリティを開きます
4. 表示メニューから **すべてのデバイスを表示** を選択します
5. コピー先ボリュームをマウント解除します。ステップ7で失敗を避けるために、この重複するステップが必要なことが良くあります。
6. ディスクユーティリティのサイドバーからコピー先ボリュームの **親デバイス** を選択します †
7. ツールバーの “ 消去 ” ボタンをクリックしてください
8. "ASRDataVolumexxx" という名前のボリュームが表示されたら、そのボリュームを選択して、ツールバーの “ 消去 ” ボタンをクリックして削除してください。
9. CCCに戻り、コピー先の選択をリセットしてから、タスクをもう一度実行してください

† コピー先ディスクに喪失したくない他のボリュームまたはパーティションがある場合は、ディスク全体を消去しないように注意してください。その代わりに、このステップではコピー先ボリュームを選択してください。 “ ボリュームを消去 ” のパネルに “ ボリュームグループを消去 ” が提示されたら、それをクリックしてください。

APFSの複製処理が繰り返し失敗する場合

AppleのAPFSレプリケータは、macOSのインストールに問題がある場合、ソースのファイルシステムに損傷がある場合、ストレージドライバに競合がある場合、ハードウェアに問題がある場合、またはメディアの読み出しの問題がある場合、失敗します。要するに、現実の状況ではあまり実用的ではありません。CCCのファイルコピー機能は実戦でテストされ、その長い年月の経験を生かし、あらゆる種類の困難な状況を優雅に処理します。AppleのAPFSレプリケータが仕事を完了できない場合、CCCのファイルコピー機能を使ってMacのDataボリュームのバックアップを作成することをお勧めします。

1. データのみのバックアップを作成して保持する

データのみのバックアップはお使いのすべてのデータ、設定、およびアプリケーションの完全なバックアップです。このバックアップは、お使いのすべてのアプリケーション、データ、および設定をCatalinaのフレッシュなインストールに移行するのに最適です（万が一その必要が起きた場合）。ただバックアップを作成するだけでは、データ保護の目的には十分ですが、起動可能なバックアップを作成することにはなりませんし、ソースのどんな問題にも対処できません。データのみ

のバックアップを設定する方法についての詳細は、[データのみのバックアップを作成するには](#) <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#create>> を参照してください。

2. macOSをデータのためのバックアップにインストールして起動可能なバックアップを作成する

macOSをデータのためのバックアップにインストールすると、システムの完全で、起動可能なバックアップを作成できます。起動ディスクの損傷が最終的にそのボリュームの不具合につながる場合、バックアップからMacを起動して、バックアップから作業を継続できます。また、内部ディスクに完全な復元を実行することも可能です（例えば、消去したり、置き換えてしまった後）。macOSをデータのためのバックアップにインストールする手順に関する詳細は、[macOSをデータのためのバックアップにインストールするには <http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#installmacos>](http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#installmacos) を参照してください。

3. ソースを消去してバックアップから復元する

ディスクユーティリティは一般的にAPFSフォーマットされたボリュームのファイルシステムのダメージを修正できません。たいていの場合、APFSファイルシステムの損傷を解決する唯一の方法は、影響を受けたボリュームを消去して、それをバックアップから復元することです。特に、ソースボリュームのファイルシステムの損傷がシステムの誤作動を引き起こしている場合、バックアップボリュームからMacを起動し、内部ディスクを消去して、バックアップを復元できます。バックアップの復元方法の詳細は [バックアップから復元するには <http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup>](http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup) を参照してください。

関連ドキュメント

- データのためのバックアップを作成および復元するには [<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups>](http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups)
- バックアップから復元するには [<http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup>](http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup)

バックアップタスクを停止したら、コピー先ディスクが完全に応答しなくなりました

AppleのAPFSレプリケータは複製タスクのキャンセルをうまく処理できません。このコピー先ボリュームは基本的に壊れていますが、ASRはそのボリュームを消去して、タスク前の状況に戻すということはありません。さらに、コピー先デバイスが完全に応答しないだけでなく、ディスクユーティリティでさえデバイスとボリュームを読み込めません。これは最初の状況よりもさらに恐ろしいですが、ラッキーなことに簡単な解決策があります。

解決策:

物理的にコピー先デバイスをMacから一旦接続解除して、再度接続し直してください。コピー先が内部デバイスで、簡単に接続解除できない場合は、コンピューターを再起動するだけで大丈夫です。次に、CCCの“ユーティリティ”メニューから**ディスクユーティリティ**を選択し、コピー先を再フォーマットしてください。

この残念な結果は2019年9月にAppleに報告しています (FB7324207) が、まだ返答を待っている段階です。

CCCから、使用中のソースまたはコピー先が読み込み/書き出しエラーを報告していると、報告がありました

AppleのAPFSレプリケータはソースボリュームを非常に低いレベルでクローンします。それは、個々のファイルをコピーする代わりに、ファイルシステムのデータ構造を直接コピーします。このユーティリティが個々のレベルでファイルを検証していないため、メディアエラーやファイルシステムの破損をうまく処理できません (FB7338920)。ASRがメディアエラーやファイルシステムの破損に遭遇すると、クローンタスクは失敗し、コピー先ボリュームは破損状態になります。メディアエラーの存在は、ASRがクローンを完了できる可能性を非常に低くします。従って、ソースまたはコピー先から読み込み/書き出しエラーが報告された場合、CCCはASRユーティリティを使用しません。

解決策:

データのためのバックアップを作成してから、読み込み/書き出しエラーにつながるハードウェアの問題に対処し、その後バックアップからデータを復元することをお勧めします。

関連ドキュメント

- データのみのバックアップを作成および復元するには <<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups>>
- ハードウェア関連の問題を識別してトラブルシューティング <<http://bombich.com/ja/ja/kb/ccc5/identifying-and-troubleshooting-hardware-related-problems>>
- ディスクエラーの統計情報 <<http://bombich.com/ja/ja/kb/ccc5/disk-center#errors>>

Coping with errors caused by APFS filesystem corruption

We regularly see cases of APFS filesystem corruption that lead to errors during a backup task. This corruption is typically presented in an error like one of these:

```
readlinkstat("/Photos/Foo/2020Dumpsterfire.jpg") failed: Illegal byte sequence (92)
rename("/Photos/Foo/.2020Dumpsterfireoutofcontrol.jpg.asdfgh" ->
"/Photos/Foo/2020Dumpsterfireoutofcontrol.jpg") failed: No such file or directory (2)
```

When CCC encounters these errors, the affected items are listed in CCC's Task History window, often with this overly-optimistic advice:

Use Disk Utility to repair any filesystem problems, then try the backup task again. Note that you will need to boot from your backup volume or the Apple Recovery HD volume if repairs are required on your startup disk's filesystem. If this error persists and Disk Utility is unable to detect or repair the problems, you may have to reformat the affected volume to address the problems.

In both of these cases, the file or the parent folder is corrupted, and the APFS filesystem will not allow any modifications to those items. Sometimes you can simply delete the affected items, but sometimes this is not possible because the Finder does not reveal these corrupted items to you (because they are corrupted). Typically Disk Utility does not even detect this filesystem corruption, and it will never repair the corruption if doing so would require the removal of files or folders. Sadly, lacking any other utilities to repair the damage, your only remaining option for resolving the corruption is to erase the affected volume.

The folder swap method

If you are unable to see a corrupted item in the Finder (and therefore unable to delete it to resolve the corruption), there is one alternative that you may be able to consider. Often when errors are encountered while trying to make changes to a file (especially its name or location), the corruption is affecting the parent folder, not the file itself. In those cases you can replace the folder to remove the corruption. Supposing CCC is reporting errors on a file at "My Media Volume" > Photos > Foo > 2020Dumpsterfire.jpg, you could do the following to replace the folder while retaining the bulk of its content:

1. If the item you're looking for resides in a hidden folder (e.g. "/Users/yourname/Library"), you can press Command+Shift+Period to toggle the Finder's display of hidden items
2. Navigate in the Finder to "My Media Volume" > Photos
3. Create a new folder here named "Foo new"
4. Select all of the items in "Foo" (e.g. Command+A) and drag them into "Foo new"
5. Move "Foo" to the Trash †
6. Rename "Foo new" --> "Foo"

† This does not solve the corruption problem, rather it only cordons the corruption off to a separate (and disposable) folder. In most of these cases, you'll find that Finder cannot empty the Trash, claiming that the files are "in use". That's just the Finder's way of expressing that it can't cope with the corrupted content, and has no advice that would actually be helpful. If you are unable to empty the Trash, and you would rather not erase the affected volume to remove the corruption, then you can create a new folder on the affected volume, e.g. "Corrupted Items" and move the items from the Trash into that new folder. You can then [exclude that folder from your backup task](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task) <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>> to avoid the errors that its content would cause.

ハードウェアに関連する問題を識別してトラブルシューティングするには

時々ハードウェアコンポーネントはゆっくりと機能が低下し、様々な一貫性のない問題をもたらします。ある時には、データをディスクにコピーし、普段通りに使用できます。次の瞬間、ランダムと見られるエラー、機能停止、クラッシュ、バックアップタスクの途中でコピー先ボリュームが“消える”、Finderがロックする、など手に負えない動作が起こります。

ハードウェアがこのように失敗すると、OSやCCCがダイアログを表示して、“ の取り替え時です！”ということとはほぼ不可能です。代わりに、もう少し深読みして、コンポーネントを探し当て、別のコンポーネントに置き換えてみるなど、欠陥のあるコンポーネントを特定する必要があります。

ハードウェアの問題が起きる多くの場合、CCCはmacOSカーネルからなんらかのハードウェアの問題を明白に示す有意義なエラーを受け取り、バックアップタスクの最後にこれを報告します。しかし、macOSまたはCCCがフリーズしたファイルシステムを感知するケースもあります。その場合CCCから以下のいずれかのメッセージが表示されます：

“（ソースまたはコピー先の）ボリュームのマウントポイントが変更されたため、バックアップタスクは中止されました。”

このメッセージが表示された場合、macOSのカーネルは、影響を受けたファイルシステムが応答しないで終了したことを認識しています。これは明らかにバックアップタスクが突然終了したことを意味しますが、次に述べる別のmacOSの動作よりまだましです。

“（ソースまたはコピー先の）ファイルシステムが応答しないため、バックアップタスクは中止されました。”

CCCがこのメッセージを表示するのは、ソースまたはコピー先ボリュームが読み取りまたは書き出し動作を少なくとも10分間受け入れなかった時です。慎重な追跡テストの結果、単純な読み出しまたは書き出しリクエストが失敗することが検証されました。これらのケースでは、macOSカーネルは誤作動中のファイルシステムに措置を講じることができず、影響を受けたボリュームから読み取りを、あるいは影響を受けたボリュームに書き出しを試みるすべてのアプリケーションに機能停止が見られることが予想されます。機能停止を解除するには、影響を受けたディスクをMacから強制的に接続解除する必要があります。あるいは、ディスクが内部ディスクの場合、電源ボタンを押したままにして再起動する必要があります。

トラブルシューティングの手順

CCCからハードウェアの問題がある可能性があるという提示を受けた場合、以下の手順に従って問題を特定することをお勧めします。それぞれの手順の間にバックアップタスクを繰り返してください。問題が解決したらそこで停止してください：

1. 影響を受けたボリュームが外部ハードドライブに常駐している場合、そのディスクをMacから一度接続解除し、再度接続してください。ベつな方法では、先に進む前にMacを再起動してください。一般的にこの方法は、ファイルシステムが機能停止した場合の突発的な問題のみを解決しますので、ご注意ください。ディスクが再接続されると、問題なく機能しているように見えますが、問題が再発しないということではありません。
2. ソースボリュームとコピー先ボリュームでディスクユーティリティの**応急処置**のツールを実行してください。ファイルシステムの問題はよくあることで、簡単に特定することができます。ファイルシステムの問題が起動ディスクにあることがわかった場合、CCCのバックアップボリューム

- から起動するか、または **リカバリモード** <<https://support.apple.com/en-us/HT201314>> に起動して、ディスクユーティリティを実行すると、問題を修復できます。
3. Macに接続されている他のハードウェアデバイスがある場合 (例: USB ウェブカメラ、プリンター、iPhone、つまりモニター、キーボード、マウス、およびソース/コピー先ディスク以外すべて)、それらを接続解除してください。ソースまたはコピー先ボリュームがUSBハブ、キーボード、モニターに接続されている場合、Macの内蔵ポートに接続し直してください。
 4. 外部ハードドライブエンクロージャをMacに接続するために使用しているケーブルを取り替えてください (該当する場合)。
 5. 外部ハードドライブエンクロージャを別のインタフェース経由でMacに接続してください (該当する場合)。
 6. 同じハードドライブを別の外部ハードドライブエンクロージャで使用してください (**推奨製品はこちらから** <<http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive#recommendations>>)。
 7. ディスクユーティリティでハードドライブをフォーマットし直してください。影響を受けたディスクがSSDではない場合、消去タブの**セキュリティオプション** をクリックして、スライダーを右にドラッグして、ゼロのシングルパスを書くオプションを指定してください。各セクターにゼロを書くことは、まだ発見されていない問題のある追加セクターを効果的に探知し、“スベアアウト”します。
 8. 以上のどの方法も問題を解決しない場合、ハードドライブが破損しているか欠陥があると考えられます。この場合、ハードドライブを取り替えてください。

“ どうしてCCCはコピー先を取り出すのですか？ ” また
“ どうしてCCCはコンピュータ全体を機能停止させるのですか？ ”

これはよく耳にすることですが、概して、“その非難は的外れですよ”と答えています。大抵の場合、CCCはファイルに影響を受けたボリュームにコピーしている唯一のアプリケーションであるか、少なくともアクセスの大部分を実行しているアプリケーションであるかのどちらかです。そのため、問題がCCCに特定しているかのように見えるだけです。典型的なバックアップタスクは何十万ものファイルシステムのリクエストを作成するので、CCCがハードウェアの問題をディスクで明らかにするのは驚くことではありません。CCCは単にディスクからディスクへファイルをコピーしているだけで、これはシステム全体を機能停止させるような類いのタスクではありません。複数のアプリケーションがボリュームへのアクセス中に機能停止してしまう時、過失は完全にmacOSカーネルにあり、それが破損しているか欠陥があるハードウェアを誤作動させているのです。この判定に確信を持っていない場合は、CCCのヘルプウィンドウから報告を送信してください。CCCが機能停止したファイルシステムを探知すると、診断情報を収集して機能停止がどこで起きているかを判定します。私たちは喜んで診断を検証し、ハードウェアの問題のある、なしを評価します。

“ しかし、ディスクユーティリティはディスクに何の問題もないと言っていますが...”

ディスクユーティリティは、ファイルシステムの構造的な問題を探知する能力はありますが、ファイルシステムに、読み取り、書き出しのリクエストに応答するのを停止させるようなハードウェアの欠陥を必ずしも探知できるわけではありません。さらに、たとえディスクがSMART対応で“検証済み”であるとしても、SMARTステータスが報告する属

性は偏っ

ていて、ハードウ

エアが故障寸前の状態であることを

まだ示すことができないかもしれません。

ディスクユーティリティは悪いセクターを見つけるためにスキャンしている訳ではありません。ファイルシステムの健康状態のみをチェックします。

悪いセクターはディスクユーティリティから報告されません

。“検証済み”であっても、ディスクにハードウェアの問題がまったくないということを示すことにはなりません。

“ しかし、Disk WarriorやTech Tool、[その他のサードパーティユーティリティ]は、ハードウェアに問題はないと言っています。ハードウェアは大丈夫だと思いますよ！”

今の市場には、ケーブル、ポート、またはエンクロージャの問題を指摘したり、ハードドライブやSSDのファームウェアに存在する不具合を報告するハードウェア診断ユーティリティはありません。Macプラットフォームで現在利用可能なツールが指摘できるのは、ソフトウェアベースのファイルシステムの問題、メディアの欠陥、およびエンクロージャ内のハードドライブデバイス限定のSMART診断の結果です。これらのツールはその範疇で問題を識別するには素晴らしいですが、ケーブル、ポート、またはエンクロージャの問題、あるいはハードドライブのファームウェアの不具合を感知する能力がこれらのツールには欠けています。その大きな穴は、オールドファッションのトラブルシューティングで埋めるしかないでしょう。つまり、構成要素を隔離し、変数を1つずつ除外していき、テストを繰り返すことです。

機能停止につながるその他の要因

バックアップタスクが機能停止する時、ハードウェアが犯人であることがよくあります。しかし、ソフトウェアがバックアップタスクを干渉し、システム全体をも機能停止させることがあります。カスタムソフトウェアに同梱される外部ハードドライブエンクロージャを使用している場合、次のバックアップタスクを実行する前にそのソフトウェアを無効にするか、またはアンインストールしてみてください。エンクロージャにファームウェアアップデートが利用できるのであれば、それも適用してください。そして、エンクロージャとの問題がソフトウェアアップデートを通して最近解決されたかを確認してください。

関連記事

- [Seagate 診断ユーティリティをアンインストールするとフリーズが緩和される](http://bombich.com/ja/kb/discussions/cant-restore-image)
<<http://bombich.com/ja/kb/discussions/cant-restore-image>>
- ProSoftのDrive Pulseソフトウェアがバックアップタスクの失速を引き起こすという報告を数件受けています。CCCのコピー先ボリュームのスキャンを無効にすることは、この問題の効果的な解決方法と考えられますが、この方法が効果的ではないという報告も1件あります。その場合、Drive Pulseをインストール解除することで解決します。

さらに、ハードドライブエンクロージャの中には、スリープ/スリープ解除のイベントに反応が悪いものもあります。遭遇している問題が、システムがスリープしたりスリープ解除されたりした後にだけ起きる傾向があるなら、エンクロージャ特定のスリープの問題を除外するために、別のハードドライブエンクロージャがインタフェースを試してみるべきです。

“メディアエラー”のトラブルシューティング

読み込みエラーは典型的なメディアの損傷による結果です。ハードドライブの一部のセクターが破損していて、macOSはそれらからデータを読み取ることはできません。読み込みエラーはソースでもコピー先でも起きる可能性があります。古いディスクも新品のディスクも影響を受ける可能性があります。

読み込みエラーが起きたら、悪いセクターを使用しているファイルは削除される必要があります。

悪いセクターは、その上にあるファイルが削除される時だけスペアアウト、つまり完全に使用不可能としてマーク、されます。

CCCがメディアエラーによる読み込み不能なファイルを何十、何百と報告した場合、影響されるハードドライブが壊れていると考えられるので、取り替えることをお勧めします。しかし、その数が小さい場合は、必ずしもハードドライブが壊れているという兆候ではありません。以下にメディアエラーの解決法を説明します。

1. 影響を受けた項目をタスク履歴ウインドウでクリックしてから、Finder に表示をクリックします。
2. 影響を受けたファイルやフォルダをゴミ箱に移動し、
3. ゴミ箱を空にしてください。
4. ソースボリュームから項目を削除しなければならない場合は、それらの項目をバックアップボリュームに配置し、もう一度ソースにコピーし直します（必要であれば）。+
5. 数個を超えるファイルまたはフォルダに問題があるとCCCから報告を受けた場合、影響を受けたディスクをディスクユーティリティでフォーマットし直すことを強くお勧めします。影響を受けたディスクがSSDではない場合、消去タブのセキュリティオプション

をクリックして、スライダーを右にドラッグして、ゼロのシングルパスを書くオプションを指定してください。各セクターにゼロを書くことは、まだ発見されていない問題のある追加セクターを効果的に探知し、“スベアアウト”します。影響を受けたディスクが起動ディスクの場合、CCCの起動可能なバックアップボリュームから起動し、この手順を実行してください (CCCにバックアップを許可した後)。

† Finderに隠れている項目を探している場合、

“Com

mandキー+

Shiftキー+ピリオド”を

押すと、Finderの非表示の項目の表示を切り

替えられます。または、[CCCドキュメントのこのセクションからCCCを使って隠れている項目を復元する方法](#)

<http://bombich.com/ja/ja/kb/coc5/restoring-item-from-hidden-folder>をご参照ください。

影響を受けたファイルを削除したら、問題なくバックアップタスクを再実行できるはずで

注意：影響を受けたファイルのバックアップがない場合、このドキュメントのトップにスクロールし、ハードウェアに関するトラブルシューティングの方

法を先にすべてお試してください。上記のように、読み込みエラーは典型的にメディア破損の結果です。まれに、ハードウェア関連の問題 (例、ポート、ケーブル、エンクロージャなど) が存在する場合に、メディアエラーが不規則に報告されることがあります。ファイルに残る唯一のコピーを削除することが解決策であると提案された場合、そのファイルを削除する前に、問題の原因と考えられるその他すべての可能性を除外していくことが懸命です。

物理的なドライブの機能不全によって引き起こされた読み込み / 書き出しエラー

ソースまたはコピー先のハードドライブが重大な物理的機能不全を起こしている場合 (上記の“入力 / 出力”の読み込みエラーを超えたエラー)、そのディスクから他のハードドライブにデータをバックアップできるチャンスは非常に低いでしょう。もう時間がありません。コンポーネントが今にも故障して、ドライブが完全にマウント不可能になってもおかしくありません。読み込み操作は、瀕死のボリュームにはストレスが多すぎます。特にフルボリュームのバックアップは、最も重要なファイルを直ちにバックアップすることをお勧めします。最も重要なデータをバックアップできたら、次はボリューム全体をバックアップしてみてください。できるだけたくさんのデータを修復したら、影響を受けたハードドライブを取り替えることをお勧めします。

もし今にも死にそうなドライブのボリュームがマウントしなかったら？

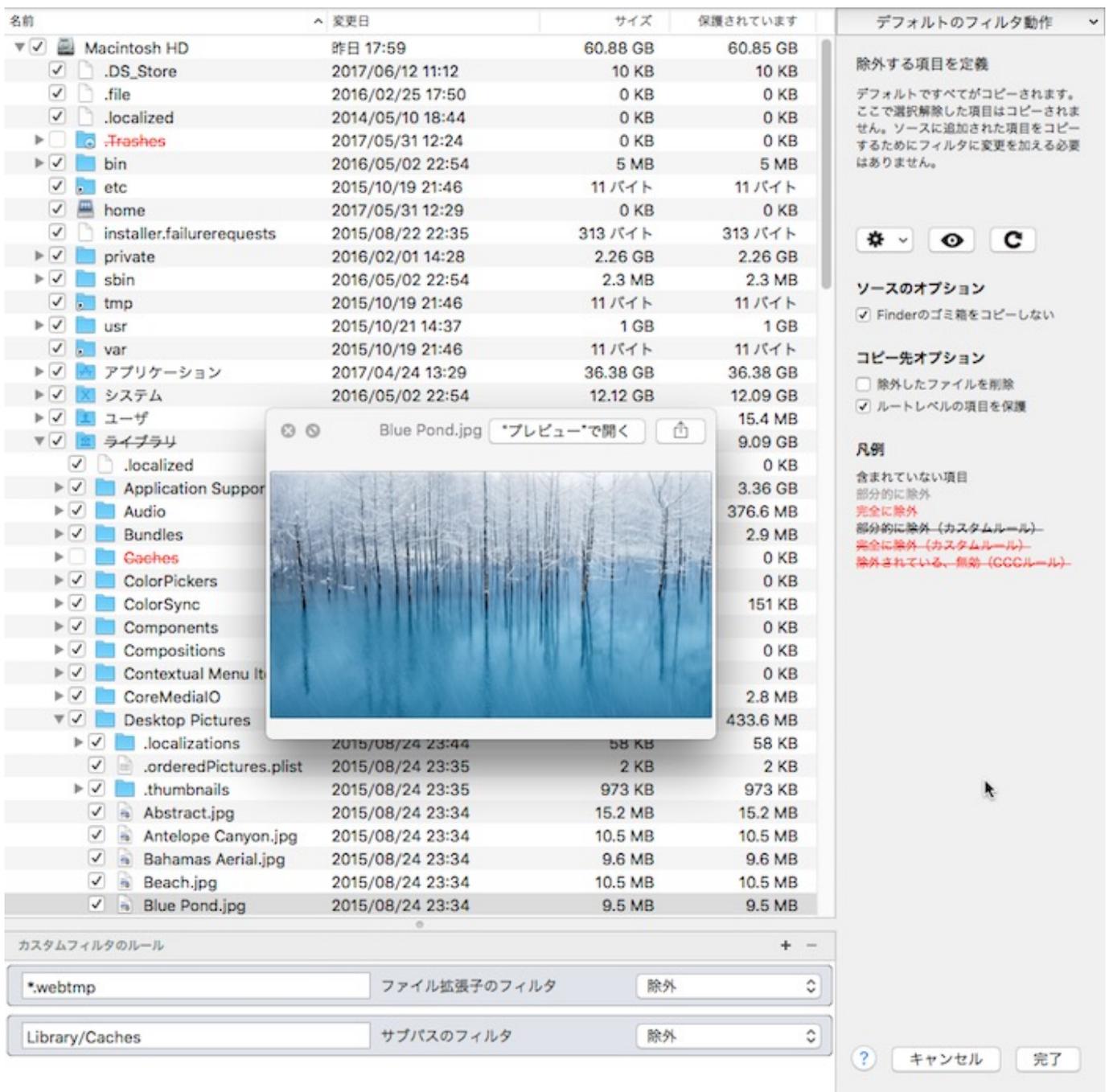
マウントしなかったらというより、もう万事休すですよ。ドライブの温度を下げ (どこか涼しい、しかし寒くない乾燥した場所で)、その後サービスワークステーションに接続してパワーアップさせることで、短時間だけハードドライブを回復させることができるかもしれませんが (そこから起動を試みるのは無理です。時間が足りません)。

高度な使用例

バックアップタスクからファイルとフォルダを除外するには

CCCはソースとして指定されたフォルダやボリュームからすべてをコピーするようデフォルト設定されています。ソースからすべての項目をコピーしたくない場合は、どの項目をコピーするかを制限するタスクフィルタを定義できます。ソースセレクトタの下にあるポップアップメニューから

いくつかのファイルをコピーを選択し、“タスクフィルタ”のボタンをクリックして、“タスクフィルタ”パネルを開いてください。



The screenshot shows the Carbon Copy Cloner interface. On the left, a file browser displays the contents of a Macintosh HD, including folders like bin, etc, home, private, sbin, tmp, usr, var, and Desktop Pictures. A preview window for 'Blue Pond.jpg' is open. On the right, the 'タスクフィルタ' (Task Filter) panel is visible, showing options to exclude items and a list of file types to be excluded.

名前	変更日	サイズ	保護されています
Macintosh HD	昨日 17:59	60.88 GB	60.85 GB
.DS_Store	2017/06/12 11:12	10 KB	10 KB
.file	2016/02/25 17:50	0 KB	0 KB
.localized	2014/05/10 18:44	0 KB	0 KB
.Trash	2017/05/31 12:24	0 KB	0 KB
bin	2016/05/02 22:54	5 MB	5 MB
etc	2015/10/19 21:46	11 バイト	11 バイト
home	2017/05/31 12:29	0 KB	0 KB
installer.failurerequests	2015/08/22 22:35	313 バイト	313 バイト
private	2016/02/01 14:28	2.26 GB	2.26 GB
sbin	2016/05/02 22:54	2.3 MB	2.3 MB
tmp	2015/10/19 21:46	11 バイト	11 バイト
usr	2015/10/21 14:37	1 GB	1 GB
var	2015/10/19 21:46	11 バイト	11 バイト
アプリケーション	2017/04/24 13:29	36.38 GB	36.38 GB
システム	2016/05/02 22:54	12.12 GB	12.09 GB
ユーザ			15.4 MB
ライブラリ			9.09 GB
.localized			0 KB
Application Support			3.36 GB
Audio			376.6 MB
Bundles			2.9 MB
Caches			0 KB
ColorPickers			0 KB
ColorSync			151 KB
Components			0 KB
Compositions			0 KB
Contextual Menu It			0 KB
CoreMediaIO			2.8 MB
Desktop Pictures			433.6 MB
.localizations	2015/08/24 23:44	58 KB	58 KB
.orderedPictures.plist	2015/08/24 23:35	2 KB	2 KB
.thumbnails	2015/08/24 23:35	973 KB	973 KB
Abstract.jpg	2015/08/24 23:34	15.2 MB	15.2 MB
Antelope Canyon.jpg	2015/08/24 23:34	10.5 MB	10.5 MB
Bahamas Aerial.jpg	2015/08/24 23:34	9.6 MB	9.6 MB
Beach.jpg	2015/08/24 23:34	10.5 MB	10.5 MB
Blue Pond.jpg	2015/08/24 23:34	9.5 MB	9.5 MB

タスクフィルタのルール

- *.webtmp (ファイル拡張子のフィルタ) 除外
- Library/Caches (サブパスのフィルタ) 除外

タスクフィルタ動作

除外する項目を定義

デフォルトですべてがコピーされます。ここで選択解除した項目はコピーされません。ソースに追加された項目をコピーするためにフィルタに変更を加える必要はありません。

ソースのオプション

- Finderのゴミ箱をコピーしない

コピー先オプション

- 除外したファイルを削除
- ルートレベルの項目を保護

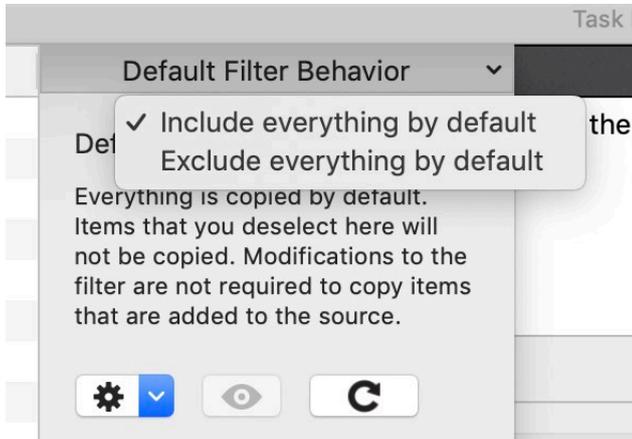
凡例

- 含まれていない項目
- 部分的に除外
- 完全に除外 (カスタムルール)
- 部分的に除外 (カスタムルール)
- 完全に除外 (カスタムルール)
- 除外されている (無効 (CCCルール))

ボタン: ? キャンセル 完了

デフォルトのフィルタ動作

CCCのタスクフィルタはタスクフィルタを定義するために2つのパラダイムを提供します。タスクフィルタは、デフォルトですべてを含めるか、デフォルトですべてを除外するかのどちらかです。どちらの動作を選択するかは、ソースに追加された新しい項目をCCCにどう対処させたいかによります。タスクフィルタウインドウの右上のボタンをクリックすることで、デフォルトのフィルタ動作を変更できます：



デフォルトですべてを含める：除外するものを定義する

CCCのデフォルト動作は、デフォルトですべてを含めることです。このモードでは、ファイルリストの項目の横にあるチェックボックスをチェックしないことでバックアップタスクから除外するものを定義します。このモードは、ほんの数項目を除外したいが、一般的にすべてをバックアップしたいユーザには最も簡単な方法です。新しい項目がバックアップタスクに含まれるように指示するために、いちいちタスクフィルタをやり直す必要がありません。ファイルまたはフォルダをソースに追加し(例：将来タスクフィルタを定義した後に)、その項目がバックアップタスクから除外したフォルダにない場合、その項目は自動的にバックアップタスクに含まれます。

デフォルトですべてを除外：含まれるものを定義する

このモードでは、デフォルトですべてが除外されます。ファイルリストの項目の横にあるチェックボックスをチェックすることでバックアップタスクに**含まれる**ものを定義します。将来項目をソースに追加し、その項目がタスクフィルタによって明確に含まれると指定されているフォルダにない場合、その項目は**バックアップされません**。このモードは、サブフォルダが頻繁に変更されるボリュームのほんの数項目をバックアップしたい場合に限り便利です。

ディスクの使用状況と保護されているサイズを計算するには

どのフォルダでも右クリックすると、**サイズを更新**

を選択でき、CCCにそのフォルダのコンテンツを列挙させ、そのコンテンツに対するタスクフィルタを評価させることができます。CCCはフォルダの合計サイズとフォルダの保護されているサイズ

(例えば、バックアップタスクに含まれているデータ量)を報告します。**ディスクの使用状況を更新** (C) をクリックして、ソース全体のコンテンツを列挙することもできます。この操作には、特にネットワークボリュームの場合、しばらく時間がかかることがありますので、個々のフォルダのディスクの使用状況を更新することをお勧めします

。CC

Cがフォル

ダを列挙している最中

に、そのフォルダを右クリックすると列挙を

停止できます。または、**ディスクの使用状況を更新**をもう1度クリックすると、計算を停止します。

ソースとコピー先のオプション

Finderのゴミ箱はデフォルトで除外されます

デフォルトで、CCCはFinderのゴミ箱のコンテンツをコピーしません。なぜなら、つまり...ゴミだからです。CCCにゴミ箱をバックアップさせたい場合は、[“タスクフィルタ”ウインドウを開き](#)

Finderのゴミ箱をコピーしない

のボックスをチェックしないままにしておくと、その除外が取り除かれます。Finderのゴミ箱のメカニズムの特性、およびそれがゴミ箱のコンテンツのバックアップおよび復元にどのように関連しているかについての詳細は、[CCCドキュメントのこのセクション](http://bombich.com/ja/ja/kb/ccc5/backing-up-and-restoring-finders-trash) <<http://bombich.com/ja/ja/kb/ccc5/backing-up-and-restoring-finders-trash>> をご覧ください。

除外したファイルがコピー先から削除されていない

CCCのバックアップタスクから項目を除外する場合

、これは **その項目をコピーしない**

”ことをCCCに指示します。しかし、

これはCCCがコピー先からその項目を**削除する**

ということではありません。つまり、前のバックアップタスクで既にコピーされている場合、削除されません。実際、項目をバックアップタスクから除外することは、コピー先のその項目を暗黙的に保護することになります。バックアップタスクから現在除外されていて、コピー先に残したくない項目がコピー先にある場合、ゴミ箱にドラッグするだけでコピー先

から削除できます。CCCにそのクリーンアップ

をさせたい場合は、**除外したファイルを削除**をチェックしてください。

タスクが**何も削除しない**のSafetyNet設定になっている場合、このオプションは無視されます。この設定は、CCC SafetyNet

フォルダに配置されたCCCの明示的な保護も上書きします。そのため、このオプションがCCCの“SafetyNetオン”の設定と組み合わせられて使用された時、項目は即座に削除されずに、SafetyNetフォルダに移動します。

デフォルトですべてを除外

のフィルタ動作を使う際に、このオプションが与える影響の範囲を十分に考慮してください。

ルートレベルの項目を保護の設定は [高度な設定の記事](#) <<http://bombich.com/ja/ja/kb/ccc5/advanced-settings#protect>>でもっと詳しく説明されます。

カスタムフィルタ

一致したいファイルがファイルシステムにバラバラに散らばっている場合、それらを1つ1つ手動で見つけて、決まったルールを作成する(例: ファイルリストで項目をチェックする/チェックを外す)のは手間がかかることです。これを処理するために、CCCは式を使ってフィルタルールを定義するカスタムフィルタのオプションを提供します。歯車メニューから**カスタムフィルタを表示**を選択して、カスタムフィルタの表を表示します。

カスタムフィルタのルールを追加す

るには、カスタムルール表の見出しにある+

ボタンをクリックしてください。または、フィルタまたはフォルダをファイルリストからカスタムフィルタ表にドラッグして、その項目をテンプレートとして追加してください。カスタムフィルタの順番を変更するには、項目をカスタムフィルタ表にドラッグ&ドロップするだけです。カスタムフィルタのルールは通常のフィルタルールの前にタスクフィルタによって評価されます。

アンカーパスフィルタ

アンカーパスフィルタは、ソースのルートに関連する絶対的なパスを使ってルールを定義します。例えば、/Library/Cachesは“/”で始まるので、アンカーパスフィルタです。このフィルタは/Library/Cachesに一致しますが、/Users

/someuser/Library/Cachesには一致しません。また、式にワイルドカードを含めることもできます。例えば、/Users/*/Library/CachesはそれぞれのユーザのホームフォルダでLibrary/Cachesと一致します。

サブパスフィルタ

サブパスフィルタは部分的なパス、または“/”で始まらないファイル名を使ってルールを定義します。上記の例を続けると、Library/Cachesは/Library/Caches および /Users/someuser/Library/Cachesと一致することになります。ワイルドカードは式で受け入れられます。特定のファイルタイプと一致するには、*.movのような式を使用するとすべての.movファイルに一致します。

ワイルドカード文字

ワイルドカード文字を式に追加してより広範囲のファイルとフォルダを一致させることができます。*はどれでも1つのファイル名またはフォルダ名にある1つ以上の文字を一致させます。例えば、*.movはすべてのムービーファイルに一致します。

/**/ は1つ以上のパスコンポーネントを一致します。例えば、/Users/**/* .jpg はすべてのユーザホームフォルダにあるすべてのJPEGの写真と一致しますが、/Library/Desktop Picturesなど、それ以外の場所にあるJPEG写真とは一致しません。また、特定のフォルダとそのサブフォルダ内のすべての項目をコピーするための“含める”のルールを定義する際、**のワイルドカードも使用できます。例えば、/Users/yourname/Documents はフォルダのみを含めますが、その内容は含めません。/Users/yourname/Documents/** にすると書類フォルダ、そのすべての内容、およびそのフォルダ内のすべてのサブフォルダの内容を含めます。

ワイルドカード**の後に追加のコンポーネントを指定すると、そのワイルドカードはそのワイルドカードの後に来るパスコンポーネントに対して一致するものにのみ適用されます。例えば、/Data/**/Marine/Invertebratesという除外ルールは/Data/2018/Marine/Invertebratesを除外しますが、/Data/2018/Marine/Benthic/Marine/Invertebratesは除外しません。後者のケースでは、**/Marine は 2018/Marineと一致しますが、次のパスコンポーネントは一致しません (そしてこの場合故意に ** のワイルドカードが 2018/Marine/Benthic と一致できないようにしているのです)。

? はどれか1つの文字と一致させるように使用できます。例えば、*.mp? は .mp3ファイル と .mp4 ファイルの両方と一致します。?のワイルドカードは、タスクフィルタを評価するために要する時間を多大に増加させるので、控えめに使用してください。

かっこ文字、"[および "]"

かっこ文字を含むカスタムルールを指定する場合、それらの文字は“エスケープ”される必要があります (例: [foo/])。エスケープしたかっこ文字を使用する場合、カスタムフィルタルールの結果は、フォルダリストに表示されません。これについては、CCCの今後のバージョンで解決される予定です。

エキスパート設定

カスタムフィルタルールは通常、項目を含める、または除外するために適用されます。しかし、“除外”は、実際には2つの動作から成り立っています。1つは、ソースにある一致する項目がコピーされない

(コピーするものから項目を隠す

)。もう1つは、コピー先に

ある一致する項目が保護される(コピーするものから項

目を保護する)。同様に、“含める”はソースにある一致する項目がコピーされる (コピーするものに項目表示する

)ことと、コピー先にある一致する項目が削除される可能性がある

(項目をリスクする

)ことを示しています。時には、ソースにある一致する項目のみ、またはコピー先にある一致する項目のみに影響

を与えるルールを定義することが便利な場合があります。例えば、“アーカイブ”という名前のフォルダがコピー先

にあって、ソースに存在しない場合、その項目はソースリストに表示されないため、通常の方法では除外できません

(よって保護されます)。/Archives 保護 のルールを追加すると、明示的にコピー先のその項目を保護できます。

“ デフォルトですべてを除外 ” のフィルタ操作とカスタムルールについて特に注意する点

通常 “ デフォルトですべてを除外 ” のフィルタ操作は、タスクフィルタで明示的に含まれていない、ソースのフォルダをすべて無視します。この “ 無視 ” の動作は、それらの項目にも明示的な保護を加えます。つまり、もしそれらの項目がコピー先に存在する場合、CCCはそれらを放っておきます。しかし、タスクにカスタムフィルタを追加すると、CCCは指定されたカスタムルールに一致する項目を検索するために、ソースの完全なスキャンを実行しなければなりません。そうすることで、CCCはソースの全フォルダのリストを収集することになります。スキャンの最後には、これらのフォルダの多くは空になる可能性があります。コピー先にこのような空フォルダが作成されるのを回避するために、CCCは “ 見直す必要のある項目リスト ” からすべての空フォルダを削除します。しかし、それには副作用があり、暗黙的に除外されているフォルダに与えられているすべての保護を削除することになります。ですから、 “ デフォルトですべてを除外 ” するフィルタを設定し、そのフィルタにカスタムルールを追加する場合、CCCがカスタムルールに一致する項目がないコピー先のフォルダを削除する、ということを念頭に置いてください。この動作を回避したい場合は、SafetyNet設定から “ 何も削除しない ” を選択してください。

“ デフォルトですべてを除外 ” のフィルタ操作とカスタムルールを使ってフォルダとそのコンテンツを含めるには

カスタムルールを使ってフォルダ、またはバンドルファイルとそのコンテンツを含めるには、直感的ではない式が必要です。なぜなら、フィルタルールは複数のパスコンポーネントと一致する必要があるからです。フォルダとそのすべてのコンテンツを含めるには、** をフィルタ式の最後に追加してください。例えば、ホームディレクトリからフォトライブラリを含めるには、以下の式が含めるルールとして適用されます：

```
/Users/johnny/Pictures/Photos Library.photolibrary**
```

フィルタを書き出す、読み込むには

歯車メニューからタスクフィルタ全体を読み込んだり、書き出したりできます。フィルタを読み込む場合、現在のフィルタは読み込まれたフィルタで置き換えられます。CCCは、通常のルールが現在選択中のソースに適用できない場合、自動的にフィルタからそれらをパージします。例えば、フィルタで/Applicationsが除外されたが、/Applicationsが現在のソースに存在しない場合、そのルールは、万が一/Applicationsフォルダがソースに追加された場合に起きる予期しない結果を避けるために、フィルタから削除されます。このパージはカスタムフィルタのルールには適用されません。

また、カスタムフィルタのルールの1つ、またはグループを書き出すこともできます。ルールを選択してから、項目をデスクトップにドラッグしてください。この方法で書き出されたファイルからカスタムルールを読み込むには、ファイルをカスタムフィルタのルール表にドラッグするだけです。

自動的に除外されている項目

Carbon Copy Clonerは、バックアップタスクからいくつかの項目を除外するようデフォルト設定されています。除外についての説明と除外項目の全リストは、[ドキュメントのこのセクション](#)

<http://bombich.com/ja/ja/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task>

でご覧になれます。自動的に除外されている項目を表示したい場合は、Optionキーを押したまま “ タスクフィルタ ” ボタンをクリックして、 “ タスクフィルタ ” ウィンドウを開いてください。

CCCのSafetyNetフォルダ、“CCC SafetyNet”はグローバルフィルタから除外されています。ドキュメントの[Carbon Copy Cloner SafetyNetについてのよくある質問](#) <http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet#restorearchives> にそのフォルダからの項目を復元する方法が解説されています。

さらに、CCCは起動ディスク、または非HFS+/APFSフォーマットのボリュームをコピー先として選択した場合、システムフォルダを除外して保護します。macOS Catalina、およびそれ以降で、同じAPFSコンテナにあるコピー先ボリュームを現在の起動ディスクとして選択した場合、CCCはシステムファイルも除外します。特定の項目、例えば、/Library/Application Supportの内容を復元したい場合、ソースとコピー先セレクトの[フォルダを選択](#) <http://bombich.com/ja/ja/kb/ccc5/folder-folder-backups> のオプションを経由してソースとコピー先にある特定の

フォルダを選択することで、この保護を避けることができます。大いなる権限には大いなる責任が付き物です。システムファイルの上書きを避けるために十分な注意を払ってください。

関連ドキュメント

- macOSシステムファイルを起動可能なバックアップから復元するには <<http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup>>
- フォルダからフォルダへのバックアップ <<http://bombich.com/ja/ja/kb/ccc5/folder-folder-backups>>
- 非表示のフォルダから項目を復元するには <<http://bombich.com/ja/ja/kb/ccc5/restoring-item-from-hidden-folder>>
- ファイルやフォルダの中には自動的にバックアップタスクから除外されているものもあります <<http://bombich.com/ja/ja/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task>>
- Finderのゴミ箱をバックアップおよび復元するには <<http://bombich.com/ja/ja/kb/ccc5/backing-up-and-restoring-finders-trash>>

高度な設定

CCCの高度な設定は特定の状況下でとても役立ちます。しかし、日常的な使用に必ずしも必要なものではありません。この設定の中には、リスクを伴うものも含まれていますので、ご使用には充分注意してください。特定の使用条件において以下の説明が不十分な場合は、CCC ヘルプメニューのCCC [について質問する... \(英語\)](#)からお問い合わせください。

高度な設定にアクセスするには、CCCのソースセクタの下にある**高度な設定**をクリックしてください。

Carbon Copy Cloner
履歴

サイドバーを表示 環境設定 新規タスク ヒント

"CCC Backup Task"のタスクプラン

CCC は **Sierra** を **CCC Backup** にクローンします。最後のバックアップ以来変更された項目のみがコピーされます。

ハードウェアの互換性に関する問題をふせぐには、**コピー先ボリュームは起動可能である必要があります**。

最終実行日：2017年6月21日水曜日 15:18

次の実行日時：*クローン*をクリックすると、このタスクを実行します。

ソース



Sierra
35.09 GB を使用中

コピー先



CCC Backup
221.58 GB 空き

スケジュール



*クローン*をクリックしたら実行

すべてのファイルをコピー

SafetyNet 入

変更及び削除されたファイルはコピー先の空き容量が許す限りキャッシュされま

メールを送信しない

詳細設定

ファイルをコピーする前

シェルスクリプトを実行：

SafetyNetを削除： 空き領域が次より少ないとき GB 自動調整

ファイルをコピー中

コピー先のボリューム識別番号を厳密に使用

コピー先でルートレベルの項目を保護

壊れているファイルを見つけて置き換える：

トラブルシューティングのオプション

最初に削除パスを実行

コピー先の新しいファイルをアップデートしない

アクセス権を保持しない

拡張属性を保持しない

ファイルをコピー後

シェルスクリプトを実行：

コピー先ボリューム：

別のタスクを実行：

電源管理：

クローン

ボリューム識別番号を厳密に使用

デフォルトで、CCCはソースとコピー先のボリュームを明確に識別するために、それらの名前とUniversally

Unique Identifier (UUID <<https://en.wikipedia.org/wiki/Uuid>>

)を使用します。これら両方の識別子を検証することで、例えば、通常のコピー先と同名ではあるが、実際のコピー先ではないボリュームにバックアップするようリスクが軽減されます。

このように有益である反面、この動作は間違った結果をもたらすこともあります。例えば、2つの外部ハードドライブをペアにして、その間を循環している場合、これらが同じ名前であるにも拘らず、CCCは両方にバックアップしないことになります。(例:

オフサイトバックアップ

)。その代わりに、CCCはそれらのボリュームの1つのUUIDが本来選択されたコピー先のUUIDと一致しないと表示します。

“循環するペアのバックアップボリューム”の問題を解消するには、このオプションのチェックマークを外し、CCCがコピー先ボリュームを認識するためにボリューム名のみを使用することです。このオプションを選択解除する時、コピー先の名前を変更しないこと、別の非バックアップボリュームをコピー先と同名のMacに接続しないことを特に注意してください。

このオプションは、コピー先ボリュームがUUIDを持たない時、自動的に無効になります。例えば、ネットワークボリュームとサードパーティファイルシステムには、ボリュームUUIDがないものがあります。また、このオプションは、最初に選択されたコピー先デバイスが接続されていない場合も無効になります。

注意：この設定は**コピー先**

ボリュームにの

み適用できます。CCCはソースボリュームを明確に識別するために名前とUUIDを**必ず**使用します。

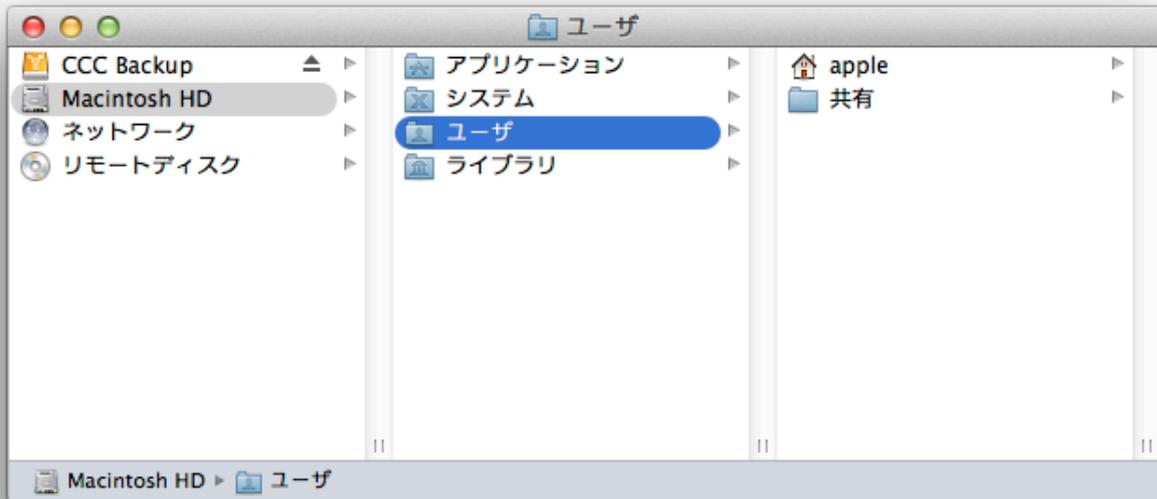
注意：循環しているコピー先ボリュームが暗号化されている場合、CCCはバックアップタスクのコピー先として選択された**オリジナルの**

暗号化されたボリュームのみをロック解除してマウントできます。CCCがコピー先ボリュームをロック解除するためには、そのボリュームの一意の識別子を必要とします。そして、CCCは特定のタスクの1つのコピー先ボリュームについての情報のみを保持します。暗号化されたバックアップディスクのペアを循環させたい場合は、その目的のために別々の2つのタスク、つまり暗号化されたコピー先それぞれのためのタスクを使用することを推奨します。

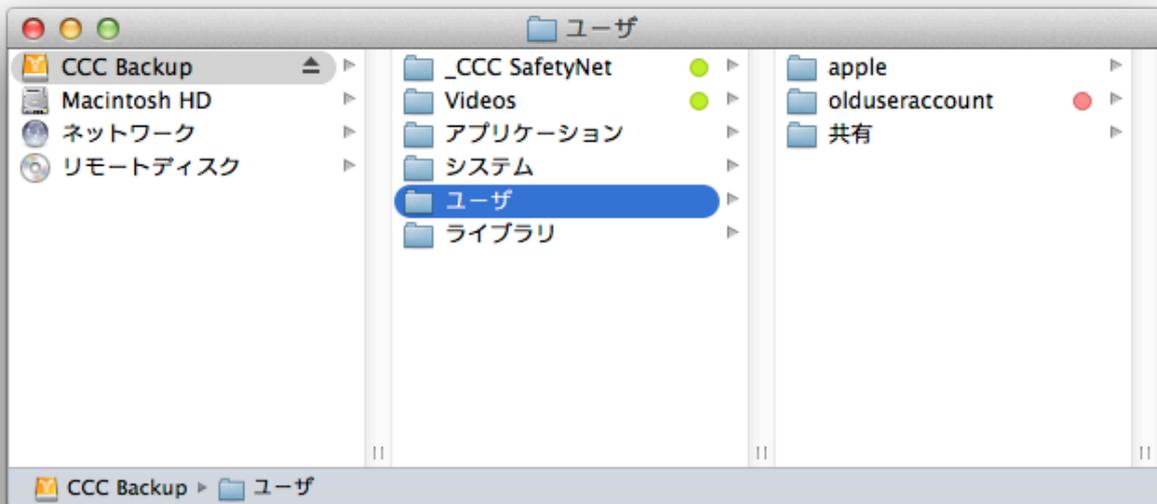
ルートレベルの項目を保護

ルートレベルにしかないファイルやフォルダがコピー先ボリュームにあり、それらを干渉されたくないが、それでもバックアップを“クリーン”に保っておきたい場合は**ルートレベルの項目を保護**

のオプションを使用してください。このオプションは、CCCのSafetyNetオプションが有効な時、デフォルトで有効になります。この機能を理解するために、これらの項目がソースボリュームにあると仮定しましょう：



そして、次の項目がコピー先ボリュームにあると仮定します：



ルートレベルの項目を保護のオプションを使用すると、ビデオ

フォルダはコピー先のルートレベルにしか存在しないため、CCC SafetyNet フォルダに移動しません。しかし、ユーザフォルダはコピー先のルートのみには存在するわけではないので(ソースにも存在します)、その内容はソースに一致するようにアップデートされます。その結果、olduseraccount フォルダは、CCC SafetyNet フォルダに移動します (SafetyNet を無効にしている場合は削除されます)。

コピー先の“ルート”とは、**選択中の**コピー先に対して最初の、または一番上のフォルダを指します。CCC

バックアップ

という名前のボリュームをコピー先として選択した場合、ルートレベルはそのボリュームのルートを指し、そのボリュームをFinderで開いたときにはそれが表示されます(上のスクリーンショットの真ん中のパネルを参照)。フォルダをタスクのコピー先として選択する場合、“コピー先のルートにある項目”とは、コピー先として選択した特定のフォルダにある項目を指しています。ボリューム全体のルートのことではありません。フォルダをコピー先として選択すると、そのフォルダの外にあるものはすべて、完全にバックアップタスクの領域外になり、その特定のバックアップタスクから除外されます。

壊れているファイルを見つけて置き換える、“バックアップヘルスチェック”

CCCは通常ファイルサイズと変更日を使用して、ファイルがコピーされるべきかどうかを決定します。このオプションを使用すると、CCCはソースのすべてのファイルと呼応するコピー先のすべてのファイルのMD5チェックサムを計算します。チェ

ックサムが異なる場合、CCCはファイルをコピー

し直します。このオプションを使用すると、バックアップにかかる時間が長くなります

(CCCがソースとコピー先の各ファイルを再読み込

みするため)が、ソースとコピー先のバックアップのセットの中の壊れているファイルを明らかにできます。

ハードドライブの寿命のどこかで、ほとんどすべてのハードドライブにメディアの損傷が起きます。これらのエラーはデータに無作為な影響を与え、メディアの損傷した箇所からデータの読み込みを試みるまで、探知されないまま放置されることが多々あります。もし、ファイルが前の(成功している)バックアップ以来変更されていなければ、CCCはそのファイルの内容を1バイトごとに取り出すことは通常しません。その結果、壊れたファイルがソースまたはコピー先ボリュームで気付かれないままになっている可能性があります。そのファイルが重要で、その内容を将来実際に復元する必要がある場合、これは明らかに問題となります。

チェックサムを頻繁に計算するオプションは不必要で、生産性の重荷になることがあります。そのため、CCCはチェックサムが発生する頻度を制限するために週または月ごとのオプションを提供します。

注意: CCCが、有効なファイルを、ソースからの読み取れない壊れたファイルに置き換えることは決してありません。CCCがソースボリュームのファイルを読み取れない場合、そのファイルの既存のすべてのバックアップはバックアップボリュームにそのまま残り、CCCはエラーを報告して、ソースファイルを影響を受けていないバックアップバージョンに置き換えるように忠告します。**壊れているファイルを見つけて置き換える**の設定は、コピー先の壊れているファイルのみを、ソースファイルが完全に読み取り可能な場合にのみ、自動的に置き換えます。

“壊れている”または“読み取れない”ファイルとは何ですか？

ソースのファイルに関しては、CCCの**壊れているファイルを見つけて置き換える**オプションは、物理的にディスクから読み取れないファイルのことを明確に指しています。ファイルを作成したアプリケーションで開くことができないように、誤ってまたは故意に変更されたファイルはこの範囲ではありません。

バックアップを検証するために、“壊れているファイルを見つけて置き換える”のオプションを使用する

CCCのチェックサムオプションは、ファイルがコピーされる前にコピー先ボリュームのファイルの整合性を検証します。その直前に書き出されたファイルの検証ではありません。一般的に、ディスクに書き込まれた直後のファイルのチェックサムの値は、疑わしい傾向があります。ほとんどのディスクには書き込みキャッシュがあり、ファイルデータは実際のメディアに書き込まれる前にキャッシュに入ります。ファイルを書き込み、その直後にもう一度読み取りを行うと、xの量のデータ(x=キャッシュサイズ)が揮発性キャッシュから来ます。いかなる量であろうとファイルデータが書き込みキャッシュから来た場合、チェックサムは永続的なメディアのデータ状況を反映せず、チェックサムを行うという当初の意味が全くなりません。

コピー先ファイルの整合性をフ

ァイルをコピー後すぐに検証したい場合、CCCの

“壊れているファイルを見つけて置き換える”

オプションを使って、その次のバックアップを使用するのが最善の方法と考えられます。このプロセスを自動化するには、まずこのオプションを使用

して第2のタスクを作成し、高度な設定の“タスク実行後”

の中のポップアップメニュー、“別のバックアップタスクを実行”から第2のタスクを選択してください。

トラブルシューティングのオプション

最初に削除パスを実行

CCCのSafetyNetオプションが無効の時には、CCCは一意的項目に遭遇すると、一般的にコピー先からそれらの項目を削除します。CCCはソースのフォルダ間をアルファベット順に繰り返し実行するので、削除される予定のファイルすべてがコピー先から削除される前に、コピー先にコピーされてしまうファイルがあります。コピー先ボリュームに空き容量がほとんどない場合、CCCはそのボリュームにバックアップを完了することができない可能性があります。このオプションは、ファイルをコピーする前にCCCが削除パスをコピー先全体に実行するように設定します。このオプションを使用すると、バックアップタスクに時間が長くなります。

このオプションはSafetyNetオプションがオフに設定されている時のみ、有効になります。

コピー先の新しいファイルをアップデートしない

ソース上のファイルは一般的に権威あるマスターと考えられ、CCCはソースとコピー先で変更日がまったく異なる場合、新しくても古くても、ファイルを再コピーします。時々、コピー先のファイルの変更日がバックアップタスク実行後に変更されるという状況があります（アンチウイルスアプリケーションによってなど）。その変更はCCCにこれらのファイルを毎回コピーさせることにつながります。このオプションを使うと、変更日の変更の根本原因が説明できない時、これらの状況を避けて動作できます。

アクセス権を保持しない

この設定は、ファイルのアクセス権および所有権の変更を許可しないネットワークボリュームにより生成されたエラーを回避します。またCCCがコピー先の所有権を有効にするのを妨げます。アプリケーションまたはmacOSのシステムファイルをバックアップ中にこのオプションを使用すると、それらの項目がコピー先で正確に動作するのを妨げます。

拡張属性を保持しない

この設定は、FinderInfo、リソースフォーク、およびその他のアプリケーション専用の属性など、読み取りと書き出しの拡張属性のサポートを無効にします。拡張属性はファイルに関するデータを保管します。ファイルを保存する際に取り替えのきかないユーザーデータを拡張属性に保管しないよう、デベロッパーはAppleから明示的に推奨されています。それは、拡張属性がすべてのファイルシステムでサポートされている訳ではないので、ファイルをコピーする際に(Finderなどによって)警告なくドロップされてしまう可能性があるからです。

このオプションが役立つのは、ソースまたはコピー先のファイルシステムが拡張属性の読み取りまたは書き出しのパフォーマンスに並外れて劣る場合、またはmacOSのネイティブの拡張属性のサポートがあまりに制限されているために、これらのメタデータをコピーしようとする際に多くのエラーが報告されるような場合です。

関連ドキュメント

- CCCからコピー先がいっぱいという報告がありました。この問題を回避するにはどうすればいいですか？ <<http://bombich.com/ja/ja/kb/ccc5/ccc-reported-destination-full.-what-can-i-do-avoid>>
- ネットワークボリュームに / からファイルをコピーする際にパフォーマンス速度が低下する問題のトラブルシューティング <<http://bombich.com/ja/ja/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume>>
- バックアップタスクの前後に別の操作を実行するには <<http://bombich.com/ja/ja/kb/ccc5/performing-actions>>



[before-and-after-backup-task>](#)

Performance Suggestions

There are several factors that affect the performance of your backup tasks. Here we describe the most common conditions that affect backup performance, and offer some suggestions for mitigating the effects of those conditions.

Reduce the number of files considered for backup

CCC analyzes all of the files that are included in your backup set for consideration to be copied. If you have a particularly high number of files on your source volume, you may want to put some thought into how your files are organized. For example, if you have a large number of files that never change (perhaps some old, completed projects), you can collect these into a folder named "Archives", back it up once, then exclude it from future backups. CCC will not delete excluded items from your destination (unless you ask it to using Advanced Settings), so as long as you keep the original on your source volume, you will always have two copies of your archived content. Because these items are excluded from your daily backups, CCC will not spend time or RAM enumerating through those files for changes.

Related Documentation

- [Excluding files and folders from a backup task <http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task)
- [Folder-to-Folder Backups <http://bombich.com/kb/ccc5/folder-folder-backups>](http://bombich.com/kb/ccc5/folder-folder-backups)

Hard drive performance and interface bandwidth

Your backups will be no faster than your slowest disk. Performance will be worse for smaller rotational hard drives (e.g. physically smaller, like those in 2.5" hard drive enclosures), for older hard drives, and for hard drives that are nearly full and thus more likely to be fragmented. Especially as Apple's new APFS filesystem becomes harder to avoid, [we recommend using SSDs for any volume that has an installation of macOS <http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations), including your backups.

You will also get longer copy times when you have lots of small files vs. a volume filled with just a few very large files. Finally, you will see better performance with faster/more efficient interfaces — USB 3.1 is faster than USB 3.0, USB 3.0 is faster than USB 2.0, etc.

Additionally, if your source volume is nearly full and is a rotational disk, we recommend that you replace it with a larger hard drive to avoid the performance implications of filesystem fragmentation.

Filesystem performance and hardware type

It's important to choose the right filesystem for the hardware that you have and the data that you're backing up. If you have an older, rotational HDD, it's generally better to [format that device using the "Mac OS Extended, Journaled" \(HFS+\) format <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) if you're backing up macOS High Sierra (or older), or if you're making a data-only backup. APFS is the new, modern standard, but [its performance on rotational devices is inferior to HFS+ <http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>](http://bombich.com/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives). If you're making a backup of macOS Catalina, APFS is required. If you find the performance of your backups to be too slow, [we recommend using an SSD for your backups <http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations>](http://bombich.com/kb/ccc5/choosing-backup-drive#recommendations).

Spotlight Indexing

Anything that causes CCC to compete for bandwidth to your source or destination volume will increase the amount of time that it takes to back up your data. Spotlight indexing is one such process that CCC typically must compete with for disk bandwidth. As you copy new data to your destination volume, for example, Spotlight wants to read those "new" files so it can index their contents. Having a Spotlight index of your backup volume may be unnecessary as you probably want to search for files only on your source volume. To disable Spotlight indexing on a volume that is dedicated to backup, drag the icon of the destination volume into the "Privacy" tab of Spotlight Preference Pane in the System Preferences application. If you do want the backup volume indexed, drag its icon out of the "Privacy" tab after the cloning and indexing will start immediately.

Find and replace corrupted files

CCC offers an advanced option to "Find and replace corrupted files" <<http://bombich.com/kb/ccc5/advanced-settings#checksum>>. When using this option, CCC will re-read every file on the source and every file on the destination, calculating a checksum of each file. CCC then compares these checksums to see if a file should be recopied. While this is an excellent method for finding unreadable files on the source or destination, it will dramatically increase the amount of time that your backup task takes, and it will also increase CPU and hard drive bandwidth consumption on your Mac. We recommend limiting the use of this option to weekly or monthly, and scheduling such tasks to run when you are not typically using your Mac.

Target Disk Mode is slow

In fact it's unbelievably slow. If you attach an SSD-bearing Mac in Target Disk Mode to another Mac via a USB-C cable (so both at 10Gb/s connections), you might expect to get incredible speed (e.g. >500MB/s). You will be sorely disappointed by speeds of less than 20MB/s; slower than USB 2.0. For better performance, we recommend that you avoid Target Disk Mode. Boot the target Mac from the volume you're trying to restore instead. Not only will you get better performance, but you also have the assurance that the Mac can boot from the OS that you're restoring to it.

Other applications and conditions that can lead to performance problems

Over the years we have received numerous queries about poorer performance than what is expected. Careful analysis of the system log and Activity Monitor will usually reveal the culprit. Here are some things that we usually look for:

- Other backup software copying simultaneously to the same volume, a different volume on the same disk, or across the same interface as CCC's destination.
- Utilities that watch filesystem activity and do things when file changes are detected. [Antivirus software](http://bombich.com/kb/ccc5/antivirus-software-may-interfere-backup) <<http://bombich.com/kb/ccc5/antivirus-software-may-interfere-backup>> is a common culprit, but we have also seen problems caused by other watcher applications, such as memiod and Western Digital's SmartWare.
- Slow interfaces — USB hubs (including the ports on a USB keyboard or display) and even some USB cables can reduce the bandwidth to your disk dramatically. If you're using USB, be sure that your device is plugged directly into one of the USB ports on your Mac.
- Daisy chaining Firewire devices is usually OK, though some enclosures can stall the entire Firewire bus when given too much bandwidth. If you see this behavior, try switching the order of devices in the chain, or attach your backup disk directly to a Firewire port on your Mac.
- Using a wireless network connection to connect to a network volume. If you're seeing poor performance with a wireless connection, compare the performance when using a wired (ethernet) connection.
- Symantec's Digital Loss Prevention (DLP) can cause performance problems when backing up a specific Microsoft font cache (e.g. `/Users/yourname/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/FontPreviewCache`). The problem appears to be specific to DLP's ability to cope with the dorky emojis that Microsoft uses in the file names in this folder (i.e. replacing the word "family" with the ? family emoji). [Exclude that FontPreviewCache folder from your backup task](#)

<<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>> to avoid the performance problem.

Use the Console application to view the contents of the system log. If you're still having trouble identifying a performance problem, [we're here to help <http://bombich.com/software/gethelp>](http://bombich.com/software/gethelp) .

Related Documentation

- Slow performance of network appliances can be mitigated by backing up to a disk image <<http://bombich.com/kb/ccc5/slow-performance-network-appliances-can-be-mitigated-backing-up-disk-image>>
- Troubleshooting slow performance when copying files to or from a network volume <<http://bombich.com/kb/ccc5/troubleshooting-slow-performance-when-copying-files-or-from-network-volume>>

FileVault暗号化で作業するには

CCCはFileVault保護されたボリューム (HFS+ および APFS) との使用に十分適しています。ディスクセンターで暗号化を有効にすることについてCCCからいくつかのアドバイスがあります。

macOSのインストールを含む (または今後含むであろう) ボリュームで暗号化を有効にするには

起動可能な、暗号化されたバックアップを作成することが最終目的であれば、以下の手順を使用してください：

1. CCCのドキュメントに従って **コピー先ボリュームを正しくフォーマットします**
<<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>>
。ボリュームを暗号化としてフォーマット **しない** てください。お使いのMacがT2 Macの場合はAPFSを選択してください <<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#t2encryptedhfs>> (例：iMac Pro、2018 MacBook Pro; [全リストはこちらからご覧ください](#) <<https://support.apple.com/en-us/HT208862>>)。
2. CCCを使って非暗号化されたコピー先ボリュームに **起動ディスクをバックアップ**
<<http://bombich.com/ja/ja/kb/ccc5/how-set-up-your-first-backup>> してください。
3. Mojaveよりも古いIOSを実行している場合、CCCのサイドバーでコピー先を選択してから、Recovery HDボタンをクリックして、**Recovery HD** <<http://bombich.com/ja/ja/kb/ccc5/cloning-apples-recovery-hd-partition>> ボリュームを作成してください。
注意：このステップを実行するには管理者アカウントにログインする必要があります。コピー先がAPFSフォーマットされたボリュームの場合は、このステップは必要ありません。
4. システム環境設定アプリケーションの**起動ディスク**パネルから、**バックアップボリューム**を起動ディスクとして選択してから、**再起動**してください。
5. システム環境設定の**セキュリティとプライバシー** パネルからFileVaultの暗号化を有効にしてください。
6. システム環境設定アプリケーションの**起動ディスク**パネルから、**製品 (システム) 起動ボリューム**を起動ディスクとして選択してから、**再起動**してください。
7. 暗号化されたバックアップボリュームに**CCCを通常のバックアップのために設定**
<<http://bombich.com/ja/ja/kb/ccc5/how-set-up-scheduled-backup>> してください。

製品 (システム) 起動ディスクから再起動する前に、変換プロセスが完了するのを待つ必要はありません

さらに、**バックアップディスク**
を使用する前に、**変換プロセスが完了するのを待つ必要はありません**

。単純に、FileVault暗号化を有効にして、すぐに主要な起動ディスクから再起動すると、変換処理がバックグラウンドで実行されます。暗号化はバックアップディスクが接続されている限り続きます。macOSは変換の進行状況を表示する便利な方法を提供しませんが、ターミナルアプリケーションで `diskutil apfs list` (または、該当するボリュームがHFS+フォーマットの場合は `diskutil cs list`) と入力すると、変換の進行状況を確認できます。メインの起動ボリュームから起動中、管理者アカウントにログインするまでが変換が再開されないことがあるという報告が数人のユーザから寄せられていますので、変換が途中で止まっているようでしたら、ログインしてみてください。

暗号化の変換中はお使いのMacをAC電源に接続したままにしてください

暗号化の変換中にAC電源を抜くと暗号化の変換が永続的に一時停止したままになる、という報告が少数のmacOS Catalinaユーザから寄せられています。弊社のテストラボではこの問題の再現に成功していません。通常、AC電源を抜くと暗号化の変換は一時停止しますが、AC

電源が復元された時には操作が再開されます。しかし、弊社に寄せられた報告の数から見て、macOS Catalinaに特有の何かしらの潜在的な問題があることを示しています。この問題を避けるために、暗号化の変換中はAC電源を接続したままにしておくことをお勧めします。暗号化の変換が一時停止していることを確認した場合は、一晩システムをAC電源に接続したままにしてみてください。

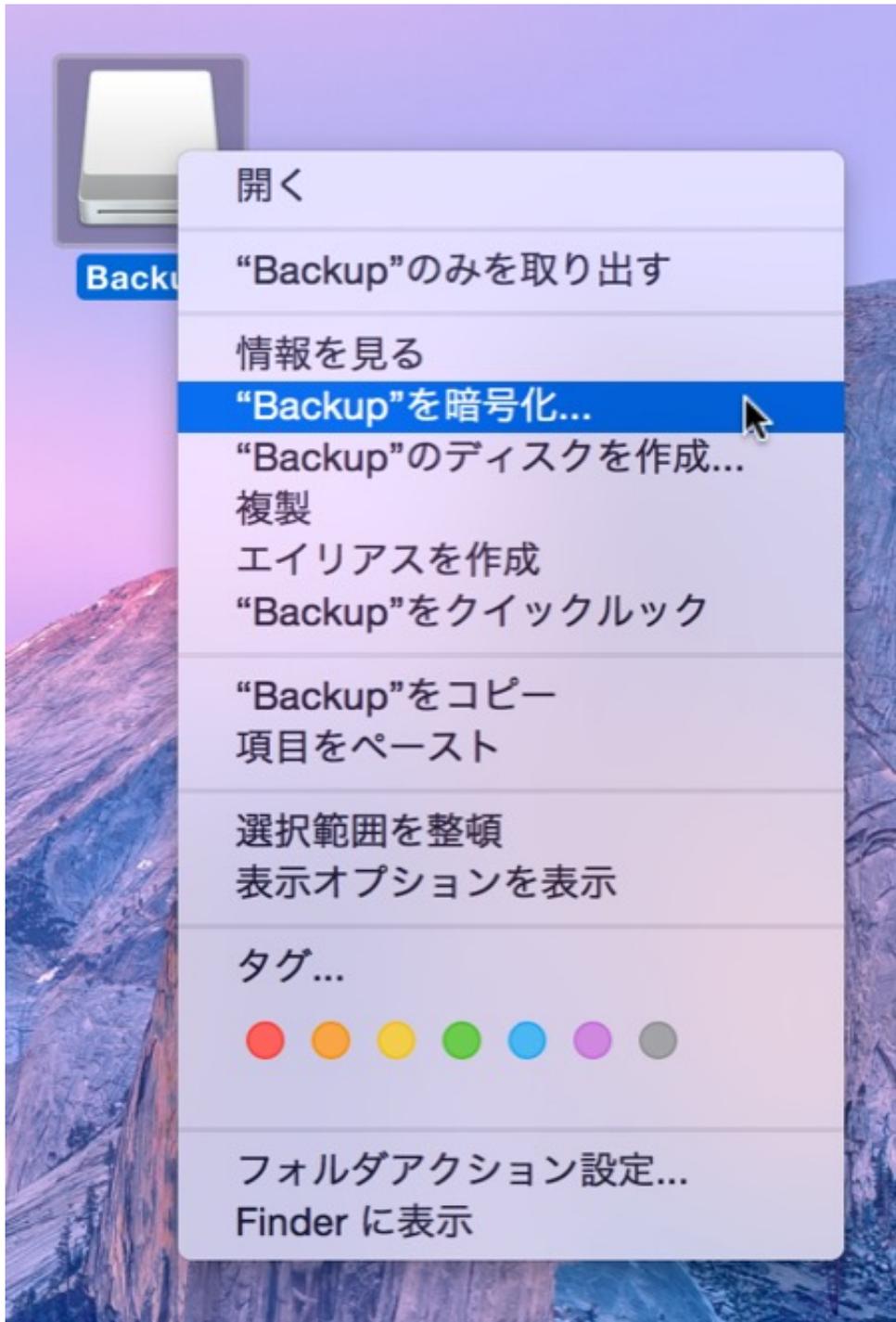
個人データを暗号化されていないフォームでコピー先に絶対に残したくない場合はどうすればいいですか？

FileVaultをコピー先で有効にするということは、ボリュームが暗号化されずに開始され、それから数時間のうちにデータは適切に暗号化されるということを意味します。暗号化の変換プロセスが問題なく完了すると、ほぼ事実上、非暗号化されたデータの痕跡はそのディスクに残りません。しかし、警告があります。お使いのバックアップボリュームがSSDで、かつ、暗号化を有効にする前にそのSSDからファイルを削除した場合、そのSSDは、まだ暗号化されていない、基になるブロックを自動的にローテーションから移動する可能性があり(ウェアレベリングの目的で)、それによりそれらのデータが専門家によって修復可能になる可能性があります。同様に、変換プロセスが何らかの理由で完了できなかった場合、そのディスクのデータを復元することも不可能ではありません。これらのシナリオのいずれかでも容認できない場合、初期のバックアップタスクから**すべての機密データを除外する** <<http://bombich.com/ja/ja/kb/ccc5/excluding-files-and-folders-from-backup-task>> ことを推奨します。ホームフォルダ全体を除外することはしないでください。ホームディレクトリから最低1つのフォルダを必ず含めて、バックアップでそのアカウントにログインできる必要があります。

バックアップボリュームから起動して、FileVaultを有効にした後、プロダクション起動ディスクから再起動して、バックアップタスクから除外項目を削除し、それからもう一度バックアップタスクを実行して残りのデータをコピーしてください。暗号化の変換途中にあるボリュームにコピーされたすべてのデータがすぐに暗号化されます。

macOSのインストールを含まないボリュームで暗号化を有効にするには

バックアップボリュームがmacOSの起動可能なバックアップでない場合は、Finderからそのボリュームを右クリックして、ボリュームを暗号化するオプションを選択してください。お使いのMacがmacOS High Sierra、またはそれ以降を実行している場合、この方法で暗号化を有効にするとmacOSはHFS+フォーマットされたボリュームをAPFSに変換します <<http://bombich.com/ja/blog/2017/09/29/think-twice-before-encrypting-your-hfs-volumes-on-high-sierra>> ので注意してください。



関連ドキュメント

- バックアップボリュームの暗号化についてのよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>>
- ディスクセンター <<http://bombich.com/ja/ja/kb/ccc5/disk-center>>
- [Apple Kbase] FileVaultに関する詳しい情報 <<https://support.apple.com/kb/HT4790>>
- T2ベースのMacが暗号化されたHFS+ボリュームから起動できない <<http://bombich.com/ja/ja/kb/ccc5/help-my-clone-wont-boot#t2encryptedhfs>>

Some files and folders are automatically excluded from a backup task

Carbon Copy Cloner maintains a list of certain files and folders that are automatically excluded from a backup task. The contents of this list were determined based on Apple recommendations and years of experience. The following is a list of the items that are excluded along with an explanation of why they are excluded.

Legend:

Items prefixed with a "/" indicate that they will only be ignored if located at the root of the volume.

Items postfixed with a "/*" indicate that only the contents of those folders are ignored, the folders themselves will be copied.

Items postfixed with a "*" indicate that the filename will be matched up to the asterisk.

Filesystem implementation details

- .HFS+ Private Directory Data*
- /.journal
- /.journalinfo**l**ock
- .afpDeleted*
- *
- ._
- .AppleDouble
- .AppleDB
- /lost+found
- Network Trash Folder
- .TemporaryItems

These items only show up if you're running an older OS than what was used to format the source volume, and on some third-party implementations of AFP and SMB network filesystems. These items should never, ever be manipulated by third-party programs.

Volume-specific preferences

- .metadataneverindex
- .metadataneverindexunlessrootfs
- /.com.apple.timemachine.donotpresent
- .VolumeIcon.icns
- /System/Library/CoreServices/.disklabel*
- /TheVolumeSettingsFolder
- [/private/var/db/dslocal/nodes/Default/secureaccesstoken.plist](#)

These items record volume-specific preferences, e.g. for Spotlight, Time Machine, and a custom icon for the volume. [Feedback on the exclusion of these items is welcome <http://bombich.com/software/gethelp>](http://bombich.com/software/gethelp) . Because they are volume-specific preferences, the exclusion of these items from a day-to-day backup seems most appropriate.

Apple-proprietary data stores

- .DocumentRevisions-V100*
- .Spotlight-V100
- /.fseventsd

- `/.hotfiles.btree`
- `/private/var/db/systemstats`
- [/private/var/folders/*/*/C](#)
- [/private/var/folders/*/*/T](#)

These items are Apple-proprietary data stores that get regenerated when absent. Attempting to copy these data stores without unmounting the source and destination is not only futile, it will likely corrupt them (and their respective apps will reject them and recreate them).

The DocumentRevisions data store is used by the Versions feature in macOS. The Versions database stored in this folder contains references to the inode of each file that is under version control. File inodes are volume-specific, so this dataset will have no relevance on a cloned volume.

Volume-specific cache files

- `/private/var/db/dyld/dyld*`
- `/System/Library/Caches/com.apple.bootstamps/*`
- `/System/Library/Caches/com.apple.corestorage/*`

Copying these caches to a new volume will render that volume unbootable. The caches must be regenerated on the new volume as the on-disk location of system files and applications will have changed. macOS automatically regenerates the contents of these folders when CCC is finished updating the backup volume.

NetBoot local data store

- `/.com.apple.NetBootX`

In the unlikely event that your Macintosh is booted from a Network device, macOS will store local modifications to the filesystem in this folder. These local modifications are not stored in a restorable format, therefore should not be backed up. In general, you should not attempt to back up a NetBooted Mac.

Dynamically-generated devices

- `/Volumes/*`
- `/dev/*`
- `/automount`
- `/Network`
- `/.vol/*`
- `/net`

These items represent special types of folders on macOS. These should not be backed up, they are dynamically created every time you start the machine.

Quota real-time data files

- `/.quota.user`
- `/.quota.group`

When these files are copied to a destination volume using an atomic file copying procedure, the macOS kernel will prevent the destination from being gracefully unmounted. The contents of these files is never accurate for the destination volume, so given the kernel's unruly behavior with copies of these files, CCC excludes them. According to the `quotacheck` man page, these files should be regenerated every time a quota-enabled volume is mounted (e.g. on startup). We have not found that to be consistently true. If you're using quotas, run `sudo quotacheck /` after

restarting from your backup volume or a restored replacement disk to regenerate these files.

Large datastores that are (or should be) erased on startup

- /private/var/vm/*
- /private/tmp/*
- /cores
- /macOS Install Data

macOS stores virtual memory files and your hibernation image (i.e. the contents of RAM are written to disk prior to sleeping) and temporary items in these folders. Depending on how you use macOS and your hardware configuration, this could be more than 50GB of data, and all of it changes from one hour to the next. Having this data for a full-disk restore does you absolutely no good — it makes the backup and restore processes take longer and the files get deleted the next time you boot macOS.

Trash

- .Trash
- .Trashes

Moving an item to the trash is typically considered to be an indication that you are no longer interested in retaining that item. If you don't want CCC to exclude the contents of the Trash, you can modify each task's filter:

1. Choose Copy Some Files from the popup menu underneath the Source selector
2. Click the Inspector button adjacent to that same popup menu to reveal the Task Filter window
3. Uncheck the box next to Don't copy the Finder's Trash
4. Click the Done button

Time Machine backups

These folders store Time Machine backups. Time Machine uses proprietary filesystem devices that Apple explicitly discourages third-party developers from using. Additionally, Apple does not support using a cloned Time Machine volume and recommends instead that you start a new Time Machine backup on the new disk.

- /Backups.backupdb
- /.MobileBackups
- /.MobileBackups.trash
- /private/var/db/com.apple.backupd.backupVerification

Corrupted iCloud Local Storage

iCloud leverages folders in your home directory for local, offline storage. When corruption occurs within these local data stores, macOS moves/renames the corrupted items into the folders indicated below. macOS doesn't report these corrupted items to you, nor does it attempt to remove them. CCC can't copy the corrupted items, because they're corrupted. To avoid the errors that would occur when trying to copy these corrupted items, CCC excludes the following items from every backup task:

- Library/Mobile Documents.*
- .webtmp

Special files

Files included in this section are application-specific files that have demonstrated unique behavior. The kacta and

kactd files, for example, are created by antivirus software and placed into a special type of sandbox that makes them unreadable by any application other than the antivirus software.

The "com.apple.loginwindow" item can be found in each user home folder. Excluding this item prevents the applications that were open during the backup task from opening when you boot from the backup volume. This seems appropriate considering that Apple intends the feature to be used to open the applications that were in use when you log out, restart or shutdown, not at an arbitrary point during the backup task.

- /private/tmp/kacta.txt
- /private/tmp/kactd.txt
- /private/var/audit/*.crashrecovery
- /private/var/audit/current
- /Library/Caches/CrashPlan
- /PGPWDE01
- /PGPWDE02
- /.bzvol
- /.cleverfiles
- /Library/Application Support/Comodo/AntiVirus/Quarantine
- /private/var/spool/qmaster
- \$Recycle.Bin
- Library/Preferences/ByHost/com.apple.loginwindow*
- .dropbox.cache <<https://www.dropbox.com/help/desktop-web/cache-folder>>
- /private/var/db/atpstatdb*
- @thumb
- /com.prosofteng.DrivePulse.ignore
- com.apple.photolibraryd/tmpoutboundsharing

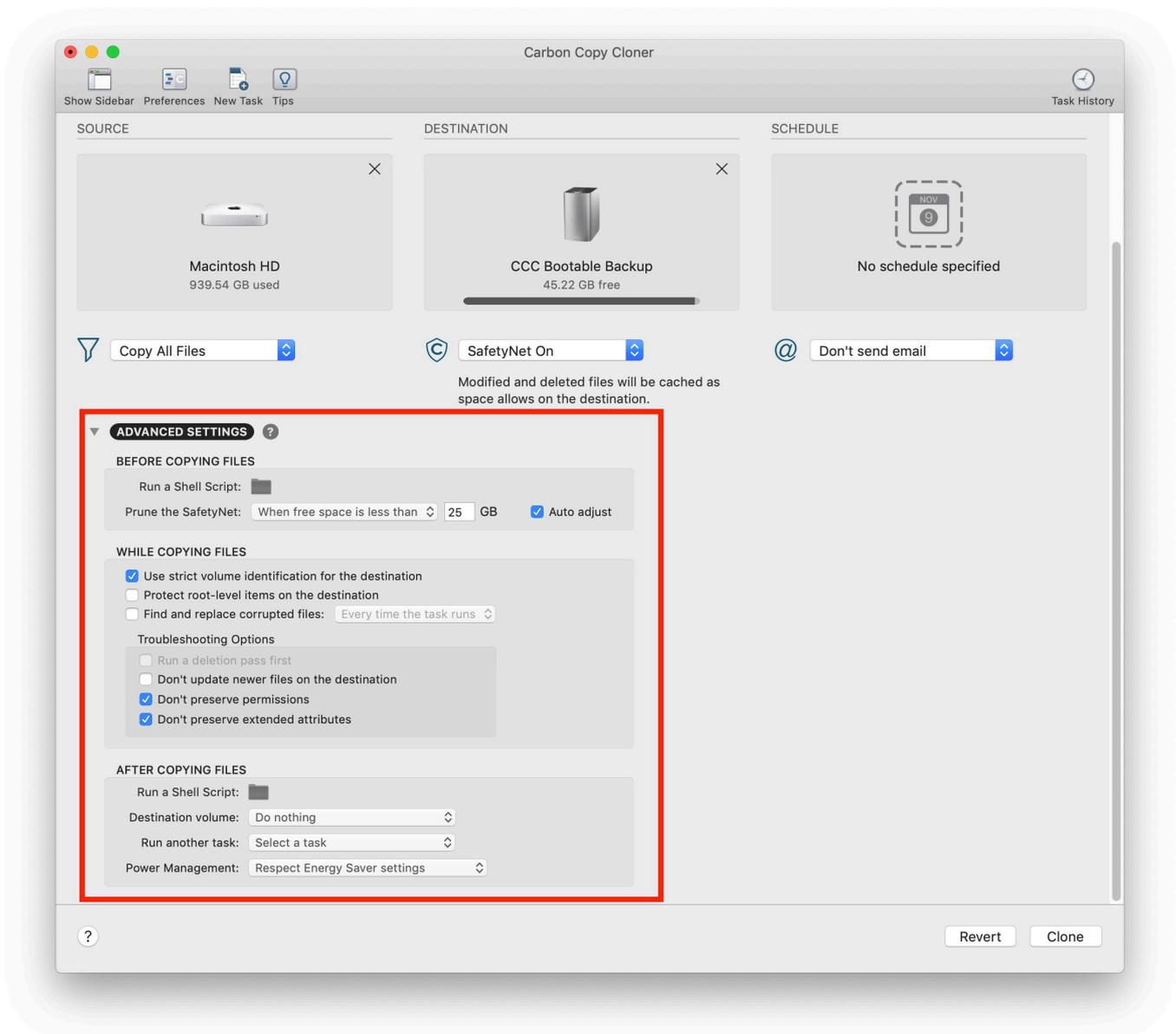
CCC SafetyNet folders

When CCC's SafetyNet feature is enabled, CCC creates a CCC SafetyNet folder at the root of the selected destination volume or folder. When CCC encounters an item on the destination that does not exist on the source, or an item that will be replaced with an updated item from the source, that item gets placed into the SafetyNet folder rather than being deleted immediately. The SafetyNet folder is literally a safety net for files on your destination. If you accidentally delete a file from the source and you don't realize it until after your backup task runs, you'll find the item in the SafetyNet folder. Likewise, if you accidentally specify the wrong volume as a destination to a CCC backup task, the mistake does not catastrophically delete every file from the selected destination; you simply recover the items from the CCC SafetyNet folder.

The protection that the SafetyNet folder imparts is specific to the volume upon which the SafetyNet folder resides. As such, CCC never includes the contents of the CCC SafetyNet folder in a backup task. So, for example, if your hard drive fails and you restore your backup to a replacement disk, the CCC SafetyNet folder is automatically excluded from that restore task. If you have several tasks backing up to separate folders on a backup volume, for example, the CCC SafetyNet folders that are created in those subfolders would not be included in a secondary backup task that copies your backup disk to a third disk.

Performing actions Before and After the backup task

Often when you have a backup task that runs on a scheduled basis, there are associated tasks that you would like to perform before or after files are actually copied. CCC offers the option to run shell scripts before and after a backup task, unmount or set the destination as the startup disk, run another CCC backup task, and power management options such as restart and shutdown. If you would like to perform any of these pre or post clone tasks, click the Advanced Settings button below CCC's Source selector.



Mounting the source or destination volume before a backup task begins

Without any additional configuration, CCC will attempt to mount your source and destination volumes before a backup task begins. This applies to many different volume types — ordinary volumes on locally-attached hard

drives, disk images, network volumes, encrypted volumes – even encrypted volumes on remote Macs. If your source or destination volume is on a disk that is physically attached to your Mac (e.g. via Thunderbolt or USB), but it is not mounted, CCC can "see" that device and will attempt to mount it. If your source or destination is a network volume, CCC will obtain the credentials that you use to mount that device when you create the backup task, and will use those credentials to mount the volume before the task begins.

This also applies for nested volumes. For example, suppose you are backing up to a disk image on a network volume. CCC will first attempt to mount the network volume, then it will attempt to mount the disk image. Likewise, suppose you have a task configured to back up the contents of a folder on an encrypted volume. If you have saved the encrypted volume's passphrase in CCC's keychain, CCC will unlock and mount the encrypted volume before the backup task begins.

CCC's attempts to mount the source and destination volumes occur automatically before any other tasks, including pre clone shell scripts (described below), therefore it is not necessary to implement a shell script to pre-mount the source or destination.

Little Snitch may prevent the automated mounting of network volumes

If you're using Little Snitch to monitor and filter your inbound and outbound network traffic, you may find that CCC has trouble automatically mounting a network volume. If you run into this problem, configure Little Snitch to allow network access to the NetAuthSysAgent system service. NetAuthSysAgent is the macOS system service that fulfills application requests to mount network volumes.

SafetyNet Pruning

SafetyNet pruning is covered in more detail [in this section of CCC's documentation](http://bombich.com/kb/ccc5/automated-maintenance-ccc-safeynet-folder) <<http://bombich.com/kb/ccc5/automated-maintenance-ccc-safeynet-folder>>.

Destination volume options

If you would like CCC to unmount your destination volume at the end of the backup task, choose Unmount the destination volume from the Destination volume management menu. If your destination is a folder, the text will be Unmount the underlying volume. If the destination is a disk image, CCC always unmounts the disk image volume, so this setting refers to the underlying physical volume upon which the disk image resides.

CCC will not forcefully unmount the destination volume. If an application has open files on the destination volume, CCC's attempt to unmount the volume will fail. CCC does not report this as an error, though it will make a note of it in the Task History window.

Yosemite users have an option to set the destination volume as the startup disk. Starting in El Capitan, however, Apple's System Integrity Protection prevents third-party applications from changing the startup disk setting. We do not recommend disabling System Integrity Protection to make this feature work, rather we recommend that you use the Startup Disk Preference Pane to change the startup disk selection.

Power management options

By default, at the end of a backup task, CCC will not perform any power management tasks. Instead, the system will perform as defined by the settings in the Energy Saver preference pane. For example, if you have the system configured to idle sleep after 20 minutes, the system will go to sleep if there hasn't been any user activity in the last 20 minutes. CCC activity is not considered user activity, so often the system will go to sleep immediately after CCC finishes a backup task.

If you choose one of the options from the Power management menu, CCC will reboot or shut down your Mac when the backup task finishes. The reboot and shutdown options are not forceful. If you have a document open with

unsaved modifications, for example, the application would prompt you to save the document. If a save dialog is not attended to, the shutdown or reboot request will time out.

Turn off the computer if it was previously off

If your backup task is scheduled to run on a regular basis, this option will be enabled in the Power Management popup menu. This option is applicable if you would like to have CCC shut down your Mac at the end of the task, but only in cases where the Mac was booted at the task's scheduled run time. If your backup task runs when the system has been on for a while or has been sleeping, CCC will not shut down the Mac when using this option.

Power Management options are ignored in some cases

Power management options will not be applied to backup tasks that are cancelled (e.g. you click the Stop button). Additionally, power management tasks will not be applied if other CCC backup tasks are running or queued to run immediately after the current task finishes running. If your task is running as part of a Task Group, power management options will be deferred to when all tasks within the group have completed.

Power Management options are applied regardless of task success

Power management options will be applied whether the backup task completes successfully or not. If you prefer for a backup task to perform the power management action only when the backup task exits without error, see the [pmonsuccess.sh](#) postflight script below.

Run another backup task (task chaining)

If you have more than one CCC backup task configured, the other tasks will be listed in this popup menu. To create a task chain (e.g. to run tasks sequentially), simply choose one of these tasks to have that task run automatically after the current task finishes. Tasks run in this manner will start after the current task has finished completely. Chained tasks will run regardless of the exit status of a preceding task in the chain, e.g. if the first task reports errors or fails to run at all, the second task will still run. Only the first task in a chain needs to be scheduled to start the chain.

Note: Postflight tasks will not be started if the current task was started via a [task group](#) <http://bombich.com/kb/coc5/task-organization>. When you run a task group, we're specifically aiming to run exactly the tasks within that task group, and within the order specified. If you run the task manually, however, or if the task is run separately from the group on its own schedule, then the task's postflight task will be run.

Running shell scripts before and after the backup task

If there is functionality that you need that does not exist within CCC, pre and post clone shell scripts may be the solution for you. Pre clone shell scripts run after CCC has performed "sanity" checks (e.g. are the source and destination volumes present, is connectivity to a remote Macintosh established) but before copying files. If you need your preflight script to run before CCC does the source/destination sanity checks, specify the preflight script as a global preflight script in the Advanced section of CCC's Preferences window. Note that global preflight scripts run prior to every task, they are not task-specific. Also, please bear in mind that [CCC automatically attempts to mount the source and destination at the beginning of the task](#), you should not be implementing a shell script to achieve that functionality. If you're having trouble with CCC pre-mounting the source and destination, [please ask us for help](#) <http://bombich.com/software/gethelp> rather than attempt to address the issue with a preflight shell script.

Post-clone shell scripts run after CCC has finished copying files and performing its own internal cleanup, but before unmounting any volumes.

CCC passes several parameters to pre and post clone shell scripts. For example, the following shell script:

```
#!/bin/sh
```

```
echo "Running $0"  
echo `date`  
echo "Source: $1"  
echo "Destination: $2"  
echo "Third argument: $3" # Exit status for post-clone scripts, underlying volume path for a disk image for pre-clone scripts  
echo "Fourth argument: $4" # Destination disk image path, if applicable
```

Would produce the following output (you can redirect this output to a file of your own specification) if implemented as a post clone script:

```
Running /Library/Application Support/com.bombich.ccc/Scripts/postaction.sh  
Wed Oct 8 21:55:28 EDT 2014  
Source: /  
Destination: /Volumes/Offsite Backup  
Third argument: 0  
Fourth argument:
```

First parameter

The path to the source volume or folder. If the source volume is APFS-formatted, then this path will usually be the path to a temporary, read-only snapshot of the source (or the path to the source folder on the temporary, read-only snapshot). On macOS Catalina and later, if the source volume is a System volume, CCC will send the path to a snapshot of the Data sibling of the source as the first parameter.

Second parameter

The path to the destination volume or folder. If the destination is a disk image, this is the path to the mounted disk image. On macOS Catalina and later, if the destination volume is a System volume, CCC will send the path to the Data sibling of the destination as the second parameter, e.g. "/Volumes/Clone - Data".

Third parameter

- Pre clone script: The underlying mountpoint for the volume that holds the destination disk image, if applicable.
- Post clone script: The exit status of the file copying phase of the backup task.

Fourth parameter

The path to the destination disk image, if applicable.

If your pre clone script exits with a non-zero exit status, it will cause CCC to abort the backup task. This can be used to your advantage if you want to apply preconditions to your backup operation. If you want to be certain that errors in your pre clone shell script never cause the backup task to be aborted, add "exit 0" to the end of your script. If you would like that script to silently cancel the backup task, add "exit 89" to the end of the script. If the script is a global preflight script (specified in the Advanced section of CCC's Preferences window), you can add "exit 104" to the end of the script to cancel the backup task and to avoid recording a Task History event.

The post clone script will run whether the backup task exits successfully or not. If your script should behave differently depending on the result of the task, you can test whether the third parameter is zero (an exit status of "0" means the task ended successfully). For example:

```
#!/bin/sh

source="$1"
dest="$2"
exitStatus=$3

if [ "$exitStatus" = "0" ]; then
    # task succeeded
else
    # task failed or reported errors
    # Note: Do not assume that $source and $dest are populated
    # These will be empty if source or destination validation fails
fi
```

If your postflight script exits with a non-zero exit status, CCC will not report this as a failure of the backup task. The failure will be noted in the Task History window, however.

AppleScripts are not supported

You cannot specify an AppleScript as a pre or post clone script, CCC currently only supports running shell scripts.

Shell scripts require a shell interpreter line

CCC does not assume a default shell environment when running your pre or postflight script. Not doing so gives users a great deal of flexibility; they can choose to write their scripts in any shell or programming language (e.g. bash, python, perl, ruby, C). For CCC to execute a shell script as an application, though, the system needs to know what shell should be used to interpret the script, and that value needs to be defined in your shell script. This is done simply by placing a shell interpreter line at the top of the file, e.g. `#!/bin/sh`.

Shell scripts run as the root user

CCC's pre and post clone shell scripts are executed as the System Administrator (aka "root"). As such, any references to your own shell environment will be invalid. When referencing tools that lie outside of the default `$PATH`, be sure to either specify the full path to the item (e.g. `/usr/local/bin/foo`), or export your own `$PATH` at the top of your script. Likewise, if you make relative references to files (e.g. `/Desktop/foo.log`), those files will be created in the root user account, e.g. `/var/root/Desktop/foo.log`. Use absolute paths for more reliable results.

Security implications of pre and post clone shell scripts

To prevent unauthorized modifications to your shell scripts, we recommend that you restrict the ownership and permissions of these scripts and to the folder in which they are contained. The parent folder and scripts should be writable only by the root user. For example, running the following in the Terminal application would secure any shell scripts located in the default location for pre and post clone scripts:

```
sudo chown -R root:wheel /Library/Application/Support/com.bombich.ccc/Scripts
sudo chmod -R 755 /Library/Application/Support/com.bombich.ccc/Scripts
```

To further enhance the security of your pre and postflight scripts, CCC will require that scripts stored in the default location are owned by the root user and writable only by the root user, and that the Scripts folder itself is also

owned and writable only by the root user. If a script that resides within the default Scripts folder does not meet these requirements, CCC will refuse to execute that script and the associated task will report an error.

After copying scripts into CCC's Scripts folder or making changes to those scripts, you can choose "Secure CCC's Scripts folder" from CCC's Utilities menu to correct any ownership or permissions concerns. Please note that these additional security requirements are only applied to scripts stored within the /Library/Application Support/com.bombich.ccc/Scripts folder. If you prefer to manage the security of your shell scripts on your own, you may store them in another location.

Example pre and post clone shell scripts

To use any of these example scripts, download the script and place it somewhere on your startup disk. By default, CCC looks in /Library/Application Support/com.bombich.ccc/Scripts.

[parallelspause.sh](http://bombich.com/software/files/tools/parallelspause.sh.zip) <<http://bombich.com/software/files/tools/parallelspause.sh.zip>>

This is a pre clone script that you can use to pause all currently-running Parallels VM containers. This script will also retain state information that can be read by the corresponding `parallelsstart.sh` post clone script to resume these VMs after the backup task has completed. Note: This script relies on command-line tools offered only in Parallels Desktop for Mac Pro or Business Edition.

[parallelsstart.sh](http://bombich.com/software/files/tools/parallelsstart.sh.zip) <<http://bombich.com/software/files/tools/parallelsstart.sh.zip>>

This post clone script will resume any Parallels VM containers that were suspended by the `parallelspause.sh` pre clone script. Note: This script relies on command-line tools offered only in Parallels Desktop for Mac Pro or Business Edition.

[playsound.sh](http://bombich.com/software/files/tools/playsound.sh.zip) <<http://bombich.com/software/files/tools/playsound.sh.zip>>

If you want to play a unique sound, use this script. You can plug in the path to any audio file of your liking or try one of the examples included.

[ejectsourceanddestination.sh](http://bombich.com/software/files/tools/ejectsourceanddestination.sh.zip) <<http://bombich.com/software/files/tools/ejectsourceanddestination.sh.zip>>

CCC's option to [automatically unmount the destination volume](#) is a volume-level task, not a device task. It's also limited to the destination. If you want to eject the destination device, or if you want to unmount or eject the source, use this post clone script instead. Note that ejecting a device will unmount all volumes on the device. Also note that this example script adds a 60-second delay to accommodate macOS's desire to automatically regenerate various cache files. This delay can be adjusted if necessary by editing the script.

[pmonsuccess.sh](http://bombich.com/software/files/tools/pmonsuccess.sh.zip) <<http://bombich.com/software/files/tools/pmonsuccess.sh.zip>>

This post clone script will perform the requested power management option (e.g. shutdown, restart, sleep) at the end of the backup task if the backup task completes without errors. Use this in lieu of one of the [Power Management postflight options](#) if you prefer the power management action does not occur when a task ends with errors (e.g. if the destination volume is missing).

[quitapplication.sh](http://bombich.com/software/files/tools/quitandopenapplication.sh) and [openapplication.sh](http://bombich.com/software/files/tools/openapplication.sh)

<<http://bombich.com/software/files/tools/quitandopenapplication.zip>>

This pair of scripts can be used to quit and open an application before and after the backup task. Open these scripts in a text editor to define the application that should be quit or opened.

[posttoslack.sh](http://bombich.com/software/files/tools/posttoslack.sh.zip) <<http://bombich.com/software/files/tools/posttoslack.sh.zip>>

This postflight script will post the status of your backup task to a [Slack](https://slack.com) <<https://slack.com>> channel.

[iftttmaker.sh](http://bombich.com/software/files/tools/iftttmaker.sh.zip) <<http://bombich.com/software/files/tools/iftttmaker.sh.zip>>

This postflight script will post an [IFTTT Maker Event](https://ifttt.com/makerwebhooks) <<https://ifttt.com/makerwebhooks>> of the status of your backup task.

Restoring non-system files

Watch a video of this tutorial on YouTube <<https://www.youtube.com/watch?v=nZJgLKyW0>>

Because CCC backups are non-proprietary copies of your original volume, you can navigate the contents of your CCC backup volume in the Finder and find your files exactly where you would find them on the original source volume. If you need to restore a single file, you can copy it directly from your backup volume in the Finder. CCC is not required to gain access to your data. If you have a larger restore need, though, CCC is ready to help make the restore process as easy as it was to back up in the first place.

Restoring non-system files

The restore process is virtually identical to the backup process. The notable differences are that you will probably be restoring a smaller subset of files than what you backed up, and that you may want to indicate that files newer on the original volume shouldn't be overwritten by potentially older versions on your backup.

1. Launch CCC and create a new task
2. Select Choose a folder... from the Source selector and select a folder on your backup volume as the source
3. Select Choose a folder... from the Destination selector and choose a folder on your original source volume as the destination
4. Click the Clone button

Note: If you choose your startup disk as the destination volume directly (rather than choosing a folder on that volume), CCC will impose a protective filter on system files and folders. It wouldn't be a good idea to overwrite or delete system files on the OS that you're booted from, so this isn't something that CCC will allow. If you need to restore system items or items in the Applications folder, we recommend that you [boot from the backup volume before attempting to restore](http://bombich.com/kb/cc5/how-restore-from-your-backup) <<http://bombich.com/kb/cc5/how-restore-from-your-backup>>.

Backing up to a disk image

Disk images are not bootable backups. To create a bootable backup, you must back up to a hard drive that is attached directly to your Mac. We recommend that you only use a disk image if you are backing up to a network volume connected to via ethernet, and we recommend using locally-attached storage for your primary backups.

A disk image is a single file residing on your hard drive that contains the entire contents of another hard drive (except for the free space). When you want to access the contents of that filesystem, you double-click on the disk image to mount the disk image as if it were an external drive attached to the machine. We recommend using disk images sparingly. If you're backing up to a network volume and your Mac and the NAS device are connected to the network via ethernet, then a disk image may be a good fit. In most cases, however, disk images are not a great choice for your backup strategy.

To back up to a new disk image:

1. Choose your source volume from the Source selector
2. Choose New disk image... from the Destination selector
3. Provide a name and choose a location to save your disk image
4. If you plan to back up to this disk image again in the future, set the image format to one of the read/write formats. If you want a read-only disk image for archival purposes, set the image format to one of the read-only formats.

To back up to an existing disk image, select Choose disk image... from the Destination selector and locate your disk image.

Read/write "sparseimage" disk images

A sparseimage disk image is a type of read/write disk image that grows as you copy files to it. In general, sparse disk images only consume as much space as the files they contain consume on disk, making this an ideal format for storing backups. Use of this older disk image format is only recommended when backing up to non-AFP network volumes on an OS older than macOS Sierra. Please note that sparseimage files are monolithic and potentially very large files. If the underlying filesystem has a 2TB file size limit and the sparseimage file reaches that limit, the sparseimage file cannot be grown. In most of these cases the sparseimage file becomes corrupted when the underlying filesystem limit is reached, so we don't recommend this disk image format for large data sets.

Read/write "sparsebundle" disk images

A sparse bundle disk image is similar to a sparseimage insofar as it grows as you add data to it, but it retains its data in many smaller files inside of a bundle rather than inside a single file. We recommend this disk image format for most scenarios.

Running out of space on a sparseimage or sparsebundle disk image

CCC reported that the destination is full, but the underlying disk has plenty of free space. CCC initially sets the capacity of your disk image to the amount of free space on the underlying disk. If you have freed up some space on that disk since you created the disk image, you can manually expand the capacity of the destination disk image in Disk Utility. Choose Resize... from the Images menu in Disk Utility, select your destination disk image, then expand it as desired. We recommend that you do not expand the disk image such that it is larger than the capacity of the underlying disk.

The disk image file is larger than the amount of data it contains, why? Sparseimage and sparsebundle disk images grow as you add data to them. They do not, however, automatically shrink when files are deleted from them. As a

result, the amount of disk space that the disk image file consumes will not necessarily reflect the amount of data that they consume. To reclaim disk space that is occupied by the free space on your sparse disk image, CCC will compact the disk image before attempting to mount it if the free space on the underlying volume is less than 25GB, or is less than 15% of the total disk capacity. In most cases, you do not need to compact the disk image yourself, but this functionality is documented here so you'll understand why you might see CCC spending time "Compacting the destination disk image" at the beginning of a backup task.

If you would like to compact a disk image manually, drop the disk image file onto this application: [Compact Sparse disk images <http://bombich.com/software/files/tools/CompactSparseImage.app.zip>](http://bombich.com/software/files/tools/CompactSparseImage.app.zip) . Be sure to unmount the disk image volume if it is already mounted. Also, note that the compacting process can take a while (e.g. an hour for a 100GB disk image on a locally-attached volume). Finally, be sure that your system is running on AC power. The system utility that compacts the disk image will refuse to run while the system (e.g. a laptop) is running on battery power.

CCC applies more aggressive SafetyNet pruning to disk image volumes

When you configure a task to back up to a new disk image, CCC will configure the task's SafetyNet pruning to prune anything older than 1 day. You are welcome to [change these settings <http://bombich.com/kb/coc5/automated-maintenance-coc-safetynet-folder>](http://bombich.com/kb/coc5/automated-maintenance-coc-safetynet-folder), but we have found that more aggressive SafetyNet pruning will avoid excessive use of disk space on the underlying device, and will reduce the need to compact the disk image.

Please keep in mind that SafetyNet is not intended to offer access to older versions of your files, [it is a safety mechanism that is designed to avoid the loss of data on an errantly-selected destination volume <http://bombich.com/kb/coc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/coc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet). SafetyNet is generally not applicable to disk image backups because the disk image is typically dedicated to the backup task. However, enabling SafetyNet with even a very aggressive pruning limit does offer a modicum of protection in cases where you've accidentally removed files from the source.

If you're looking for a solution that retains older versions of your files and your source volume is APFS-formatted, consider CCC's snapshot functionality instead. [Snapshots are disabled on disk image destinations by default](http://bombich.com/kb/coc5/leveraging-snapshots-on-apfs-volumes), but you can [enable snapshot support <http://bombich.com/kb/coc5/leveraging-snapshots-on-apfs-volumes>](http://bombich.com/kb/coc5/leveraging-snapshots-on-apfs-volumes) either on the disk image volume or on the source volume.

Read-only disk images

Read-only disk images cannot be modified without invalidating the built-in checksum, therefore they are a good container for storing archived material. Compression rates vary on the content of your source, but you can typically expect to reduce the size of your disk image by about half when using compression. There is a subtle behavior that you should take note of when considering this option as a space-saving measure: CCC will first create a read/write disk image, copy the selected items to it, then convert the disk image to read-only compressed. In this case, you will actually need twice the space on your destination as the items to be copied consume on the source.

Encrypting disk images

If any of the data that you are backing up is sensitive, and if your backup device may be in an insecure location, encrypted disk images can improve the security of your backup. CCC offers [128 bit and 256 bit AES encryption <https://en.wikipedia.org/wiki/AdvancedEncryptionStandard>](https://en.wikipedia.org/wiki/AdvancedEncryptionStandard) to encrypt disk images. To create an encrypted disk image, select one of the encryption levels from the Encryption menu. After you click on the OK button, you will be prompted to specify a passphrase for the new disk image, and CCC will give you an opportunity to save the passphrase in your own keychain. CCC will also store the passphrase in a private keychain so the disk image can be mounted automatically during scheduled backup tasks.

Note: If you create a read-only, encrypted disk image, the intermediate disk image that CCC creates is NOT

encrypted. This intermediate disk image file is deleted once the final, read-only, encrypted disk image has been created, but it is not shredded. Take this into consideration when choosing your destination media. If the destination may be placed in an insecure location, use Disk Utility to securely erase free space on the underlying destination volume after you have created your encrypted disk image archive.

Running a backup task whose destination is a disk image on the startup disk

If you specify a disk image that resides on your startup disk as the destination to a scheduled task, CCC will impose some more conservative requirements on this task. To proceed with this configuration, one of the following requirements must be met:

- The amount of free space on the startup disk is at least 1GB larger than the amount of consumed space on the source volume.
- The disk image won't grow, e.g. it is a .dmg file, not a sparseimage or sparsebundle disk image.

These requirements avoid a scenario in which the startup disk runs out of free space, causing instability on macOS. If you cannot accommodate the free space requirement, we recommend that you create a .dmg disk image in Disk Utility (choose File > New... > Blank Disk image, set the image format to read/write disk image). Disk Utility will pre-allocate exactly as much space as you request, and CCC will gladly use this disk image without fear of filling up the startup disk.

Sparsebundle disk images are not supported on some filesystems

If your Mac is running an OS older than macOS Sierra, CCC will refuse to save or mount a sparse bundle disk image if the underlying filesystem that the disk image file resides upon does not support the `FFULLFSYNC` file control. Most filesystems support this file control, but the SMB file sharing protocol does not. Most people that encounter issues with creating a sparsebundle disk image on a network volume are encountering issues because the network volume is mounted via SMB.

Starting in Mavericks, Apple's preferred file sharing service is SMB. As a result, if you attempt to connect to a network volume, Finder will use SMB to establish that connection unless you explicitly specify AFP as the protocol to use. In this configuration, a sparse bundle disk image will not work, and CCC will issue an error. To avoid this error, connect to the network volume explicitly using AFP:

1. Eject the network volume if it is currently mounted
2. Choose Connect to server from the Finder's Go menu
3. Type in "afp://yourserver.local" (changing the hostname, of course), then click the Connect button and mount the network volume
4. Go back to CCC and choose Choose disk image... from the Destination selector, then select the sparsebundle disk image on your network volume

Why can't I use a sparsebundle disk image on a filesystem that does not support the `FFULLFSYNC` file control?

When your computer writes a file out to the hard drive, the data usually goes to a "write buffer" — a small portion of RAM that is installed on the circuit board of the hard drive. By accumulating smaller write operations onto this RAM chip, the hard drive can increase overall write performance by writing large blocks of cached data to the physical media all at once. While this write buffer improves performance, it also carries a risk. If the power fails or the disk's connection to the computer is suddenly broken between the time that data was written to the buffer and when the buffer is flushed to the disk, your filesystem will have an inconsistency. Filesystem journaling typically mitigates this risk, however it doesn't offer enough protection for Apple's sparsebundle disk image type.

In Mac OS 10.5, Apple implemented the `FFULLFSYNC` file control for network servers and clients. The `FFULLFSYNC` file control is a command that is sent to the hard drive after some (or all) write operations that tells

the disk to immediately flush its cache to permanent storage. To provide better protection for data on sparsebundle disk images, Apple disabled support on Mac OS 10.6 for using sparsebundle disk images that reside on filesystems that do not support the `FFULLFSYNC` file control. Apple relaxed this requirement in macOS 10.12 (Sierra).

You are likely to encounter this error condition if your sparse bundle disk image is hosted on a pre-Mac OS 10.5 Macintosh or various Network Attached Storage (NAS) devices (especially SMB). When you encounter this error, copy the sparsebundle disk image to another network volume, or ask CCC to create a new sparseimage disk image file (sparseimage disk images are not the same as sparsebundle disk images).

Snapshots and Disk Images

When creating a new disk image, CCC will format the disk image to match the source volume. For better performance on APFS-formatted disk images, CCC will disable snapshot support on the destination disk image volume if:

- The backup task was originally configured to create a new disk image
- Snapshots are currently enabled for the destination disk image
- The snapshot retention policy limit for SafetyNet snapshots is set to the default value of 7 days

When CCC disables snapshots on that destination disk image volume, it explicitly sets the SafetyNet limit in the snapshot retention policy to 0. If you subsequently re-enable snapshot support on that volume without changing the SafetyNet limit back to the default, then snapshots should remain enabled (because the three logical conditions are no longer matched).

If you would like to enable snapshot support on your disk image and keep it enabled, be sure to either leave the SafetyNet limit set to 0, or change it to anything other than 7. If you ever change the SafetyNet retention value for that disk image back to 7 (or other reset the values to defaults), CCC will again disable snapshots on the disk image when the task next runs.

A message for new Mac users coming from the Windows world

Backups on a Windows system are very different from those on a Macintosh. If you're coming from a Windows background, the term "imaging" and the concept of making a disk image backup is probably familiar to you. Restoring from disk image backups is made simpler on Windows because the startup environment is built around them. That's not the case for a Macintosh. When you create a disk image backup of your Mac's startup disk, the logistics of restoring that backup are actually fairly complicated. Due to these complications, we don't recommend using a disk image as your primary backup on a Mac. Disk images are useful for storing a backup of your user data on a network volume, but for your Mac's startup disk, we recommend that you back up directly to a disk that is attached to your Mac; not to a disk image.

Related Documentation

- [Restoring from a disk image <http://bombich.com/kb/coc5/restoring-from-disk-image>](http://bombich.com/kb/coc5/restoring-from-disk-image)

Restoring from a disk image

You can access the contents of a disk image the same way that you access other volumes and external hard drives on macOS. Double-click on the disk image file to mount its filesystem, then navigate the filesystem in the Finder to access individual files and folders. If you have the permission to access the files that you would like to restore, simply drag those items to the volume that you would like to restore them to.

Restoring individual items or an entire disk image to another hard drive using CCC

To restore files or an entire filesystem from a disk image:

1. Launch CCC
2. Select Restore from disk image... from the Source selector and locate your backup disk image. CCC will mount the disk image for you.
3. Choose a volume from the Destination selector. You may not choose the current startup disk as a destination, however you may choose to restore to a folder on the current startup disk.
4. If you do not want to restore everything, choose Some files... from the Clone menu (below the Source selector) and deselect any item that you do not wish to restore.
5. Click the Clone button.

Restoring system files to your startup disk

If you want to restore system files to your startup disk, you must start up your Macintosh from an installation of macOS on another hard drive, such as a bootable backup created by CCC. Once you have booted your Mac from another volume, follow the steps from the previous section.

Restoring system files to your startup disk when you don't have a bootable backup

If you do not have an installation of macOS on another hard drive, you can boot your Mac from your macOS Recovery volume and use Disk Utility to restore the entire disk image:

High Sierra and Mojave

Note: The destination volume format must match the format of the disk image that you're restoring from. This limitation is specific to Disk Utility – if you're [restoring from a disk image using CCC](#), CCC can restore an APFS disk image to an HFS+ volume, and you can restore an HFS+ disk image to an APFS volume. Use Disk Utility as a last resort.

1. Hold down Command+R while you restart your computer.
2. Choose Disk Utility in the Utilities application.
3. Choose Show All Devices from the View menu.
4. Click on the device you want to restore to in the sidebar (see [this article for specific formatting instructions <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x)).
5. Click the Erase button in the toolbar and proceed to erase the device using the GUID Partition Map partitioning scheme, and the format that matches your source disk image.
6. Reselect the volume that you would like to restore to. If you are restoring to an APFS volume, choose the parent APFS container.
7. Choose Open Disk Image... from the File menu and select the disk image file that you would like to restore from.
8. Choose Restore... from the Edit menu.
9. Select the mounted disk image volume that you would like to restore. If you are restoring to an APFS

volume, choose the container that is the parent of the disk image volume you are trying to restore.

10. Click the Restore button.

El Capitan and Sierra

1. Hold down Command+R while you restart your computer
2. Choose Disk Utility in the Utilities application
3. Click on the volume you want to restore to in the sidebar
4. Choose Restore... from the Edit menu
5. Click on the Image... button and locate the disk image that you would like to restore
6. Click the Restore button

Yosemite

1. Hold down Command+R while you restart your computer
2. Choose "Disk Utility" in the Utilities application
3. From the File menu, choose Open Disk Image... and locate the disk image that you would like to restore
4. In the list in the pane on the left, click on the mounted disk image's volume
5. Click on the Restore tab on the right side of the window
6. Drag the mounted disk image to the Source field. If the Source field does not accept the dragged volume, right-click on the disk image's mounted volume and choose Set as source from the contextual menu.
7. Drag the hard drive that you would like to restore to into the Destination field
8. Check the box to erase the destination (if present), then click on the Restore button.
9. Restart your Mac from your newly restored volume, then [use CCC to restore the Recovery HD volume](http://bombich.com/kb/cc5/cloning-apples-recovery-hd-volume) [<http://bombich.com/kb/cc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/cc5/cloning-apples-recovery-hd-partition) from the archive on your startup disk.

Using Migration Assistant to migrate data from a disk image

If you have a clean installation of macOS and simply want to restore your user data from a full-system backup on a disk image, you can use Migration Assistant for this task. Simply mount the disk image, then open Migration Assistant and proceed as directed, using the mounted disk image as the source. Note that Migration Assistant will only accept a disk image that has a full system backup, it will not accept a disk image that has only user data.

Migration Assistant and the CCC SafetyNet

If your backup volume has a "CCC SafetyNet" folder, you can move that folder to the Trash before using Migration Assistant to avoid copying that folder during a migration. This is particularly important if that folder has a lot of data in it and you're migrating to a disk that is smaller than the backup volume. If you would like to retain the SafetyNet folder on the backup volume, don't empty the Trash. After Migration Assistant has completed, then you can move the SafetyNet folder back to the root of the backup volume.

Migration Assistant and Yosemite, El Capitan

On Yosemite and El Capitan, Migration Assistant will ask that you close all applications, and it will then log you out before presenting migration options. This poses a problem for migrating data from a disk image because the disk image will be unmounted when you are logged out, and Migration Assistant doesn't offer any interface to choose a disk image. To work around this problem, you can use our [Mount disk image for Migration Assistant](http://bombich.com/software/files/tools/MountdiskimageforMigrationAssistant.app.zip) [<http://bombich.com/software/files/tools/MountdiskimageforMigrationAssistant.app.zip>](http://bombich.com/software/files/tools/MountdiskimageforMigrationAssistant.app.zip) application. Simply drag the disk image containing your full system backup onto the application and it will guide you through a fairly simple procedure that will make the disk image available to Migration Assistant after a short delay.

Preliminary tests indicate that this workaround is not required on Sierra and later OSes.

I have a full-volume backup in a folder or a disk image, but I don't have a bootable backup. How can I restore everything?

CCC makes bootable backups specifically to avoid this kind of situation. When you have a bootable backup, you simply boot from that, then restore everything to a replacement disk or the original disk. One step, minimal time, couldn't be easier. Occasionally people get into this sticky situation though -- I have a backup of everything in a disk image or in a folder on the backup volume, there's a clean installation of macOS on my replacement disk, now how do I get everything back to the way that it was before?

The first thing that you need to do is make a boot volume that is not the volume you want to restore to. Once you have done that, you can boot from that volume and then do a complete restore of your backup to the replacement disk. There are several options for how and where you create this other bootable volume. For example, you could install macOS onto a thumb drive, or you could use CCC to clone your clean installation of macOS to a thumb drive. You could also create a new partition on your replacement disk and clone the fresh installation of macOS to that. The steps below attempt to make very few assumptions about the resources you'll have in this scenario: a) You have a fresh installation of macOS on a hard drive and b) you have your backup in a folder or disk image on some other disk. Given those assumptions, here is how we recommend that you proceed.

Create a new partition on your replacement disk

1. Open the Disk Utility application and click on the disk icon that represents your internal hard drive. Don't click on the Macintosh HD icon, click on the one above that.
2. Click on the Partition tab.
3. Click on the + button.
4. Set the size of the new partition to 20GB and name it something like Rescue.
5. Click the Apply button.

This video <<https://www.youtube.com/watch?v=XQG6-OJiv3s>> describes the same procedure (albeit in a slightly different context).

Clone your fresh installation of macOS to the Rescue volume

1. Open Carbon Copy Cloner and create a new task.
2. Choose your current startup disk as the source.
3. Choose the Rescue volume as the destination.
4. If you aren't working from a fresh installation of macOS, choose Some files... from the Clone popup menu and take a moment to exclude third-party applications from the list of items to be copied, as well as any large items in your home folder (e.g. /Users/yourname/Music).
5. Click the Clone button.

Boot from the Rescue volume and restore your data to the replacement disk

1. Open the Startup Disk Preference Pane, set the Rescue volume as the startup disk, then click on the Restart button.
2. Once restarted from the Rescue volume, attach the backup volume to your Mac and open the Carbon Copy Cloner application.
3. If your data is backed up in a folder, choose Choose a folder... from the Source selector and select that folder as the source. Otherwise, choose Restore from a disk image... and locate your backup disk image.

4. Choose your Macintosh HD volume as the destination.
5. Verify that CCC's SafetyNet feature is enabled.
6. Click the Clone button.

Reboot from your restored volume and clean up

1. Open the Startup Disk Preference Pane, set the restored volume as the startup disk, then click on the Restart button.
2. Open the Disk Utility application and click on the disk icon that represents your internal hard drive.
3. Click on the Partition tab.
4. Click on the Rescue volume, then click on the - button to delete that volume.
5. Click the Apply button.

Finally, make a new backup to the root of a locally-attached hard drive so you'll have a bootable backup from here forward.

Using Carbon Copy Cloner to back up to/from another Macintosh on your network

Carbon Copy Cloner offers the option of securely copying your selected data to another Macintosh on your network (or anywhere on the Internet for that matter) via the Remote Macintosh... options in the Source and Destination selectors. After a brief setup procedure to establish trust between your Mac and the destination Mac, simply choose the source or destination volume/folder on the remote Mac and CCC will take care of the rest.

Note on bootability: This feature is not intended to create bootable backups of the source Macintosh. See [this section below](#) for additional details.

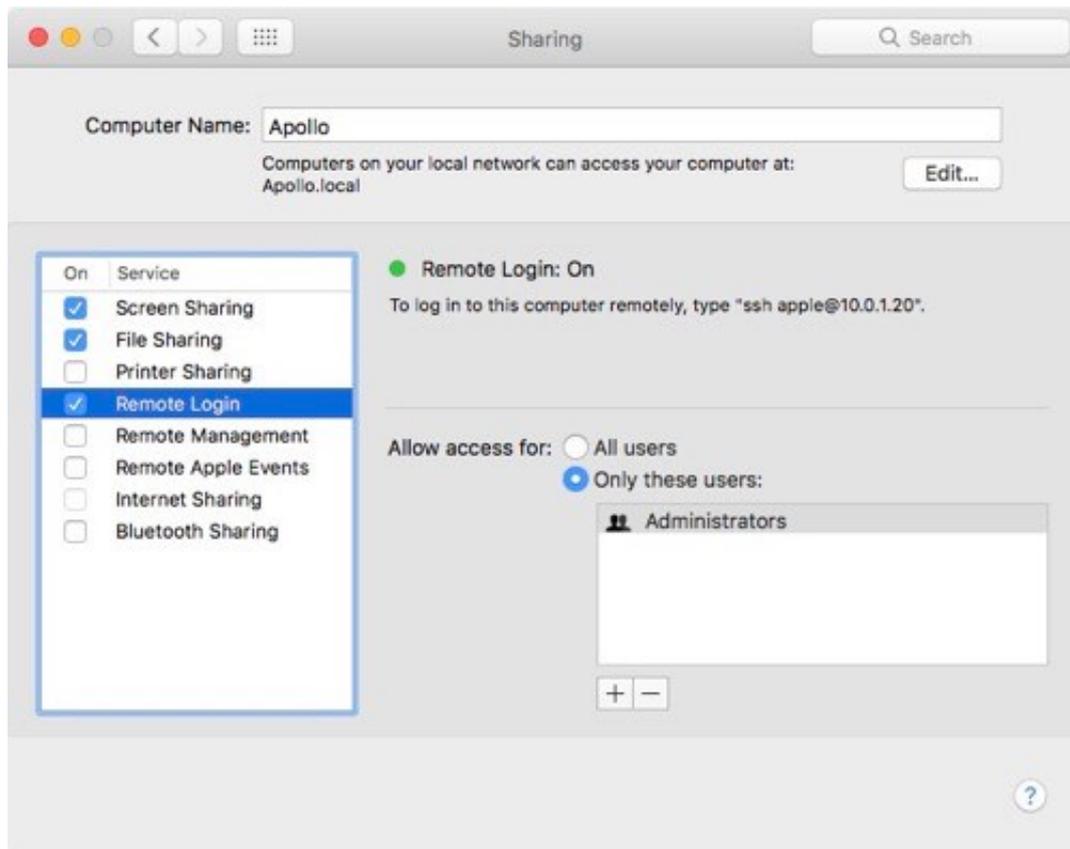
Before setting up CCC to back up to a remote Macintosh, you must:

1. Confirm that the remote Macintosh is running a supported OS (OS X 10.7 or later)
2. Enable Remote Login in the Sharing Preference Pane on the remote Macintosh
3. Verify that any firewalls between the two Macs are permitting "secure shell" traffic over port 22 (or a custom port that you specify).

Enabling Remote Login on the remote Macintosh

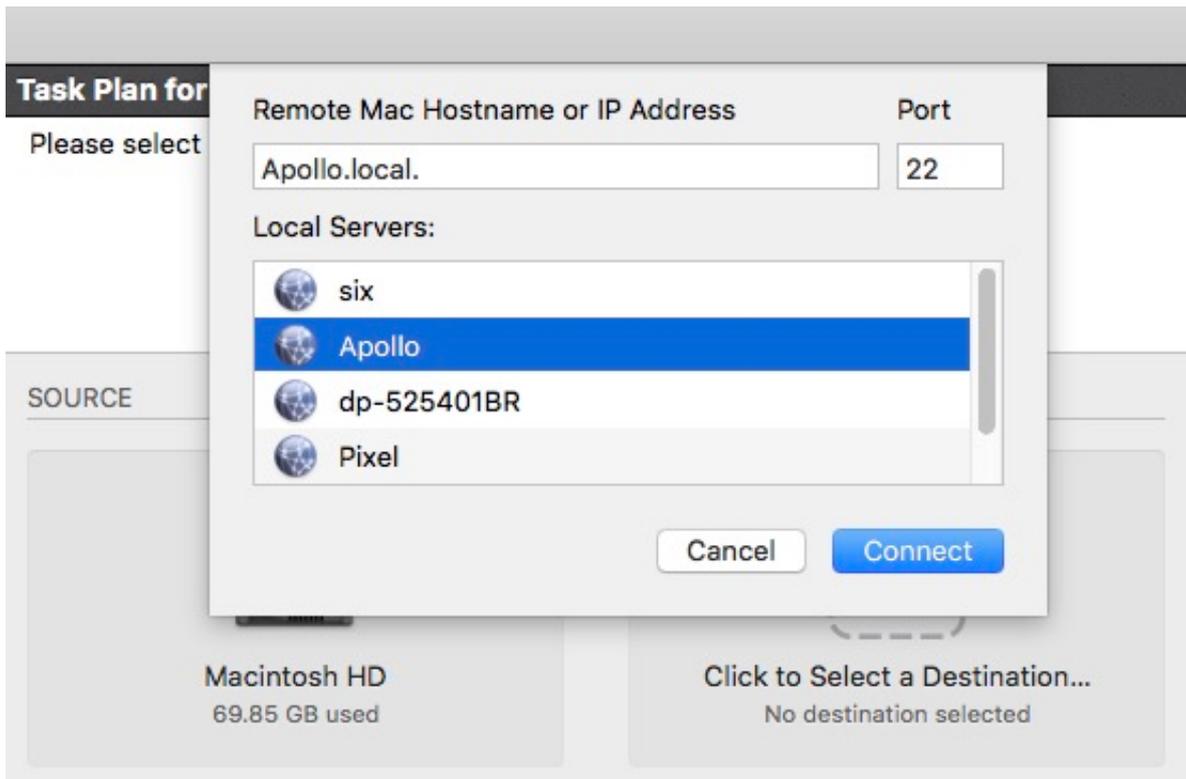
To enable Remote Login on your remote Macintosh:

1. Log in to that machine as an admin user.
2. Open the System Preferences application.
3. Open the Sharing Preference Pane.
4. Check the box next to Remote Login.
5. Be sure to allow access to All users, or explicitly add the Administrators group to the list of restricted users and groups.
6. Make a note of your remote Mac's hostname. The hostname is indicated underneath the Computer Name text field. In the screenshot below, "Apollo.local" is the hostname of the remote Macintosh.



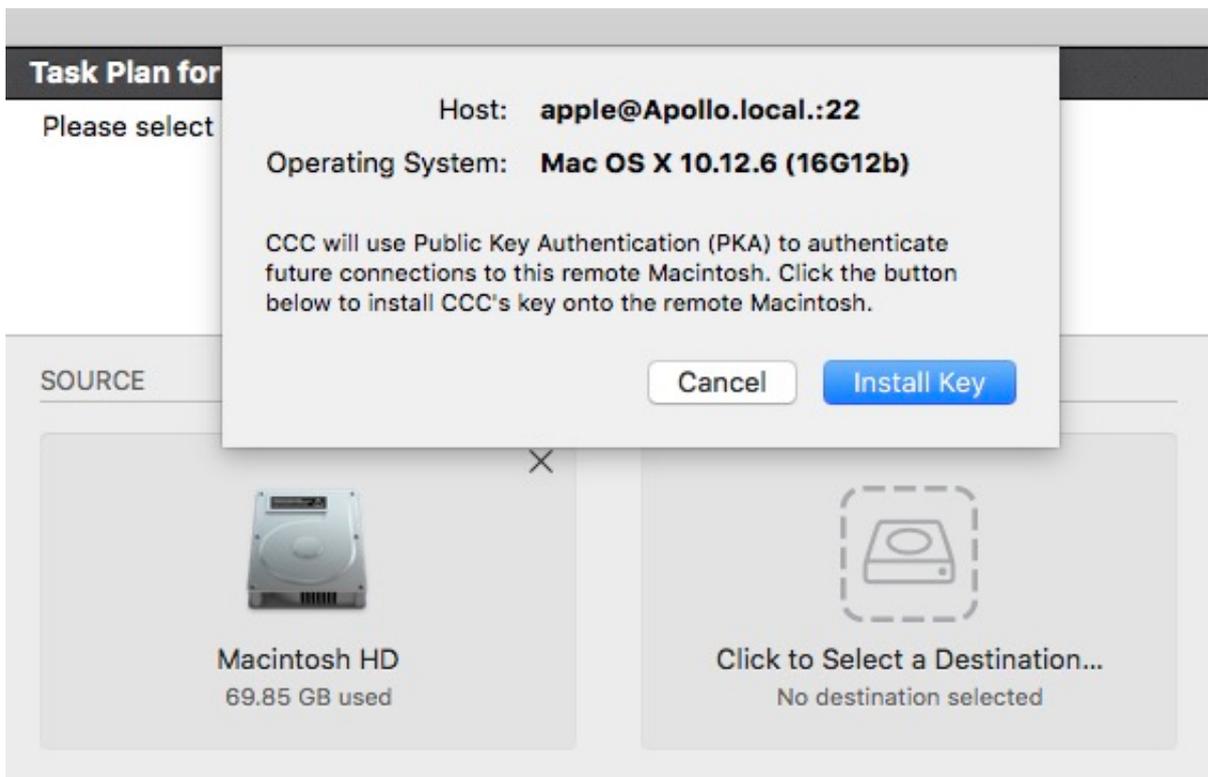
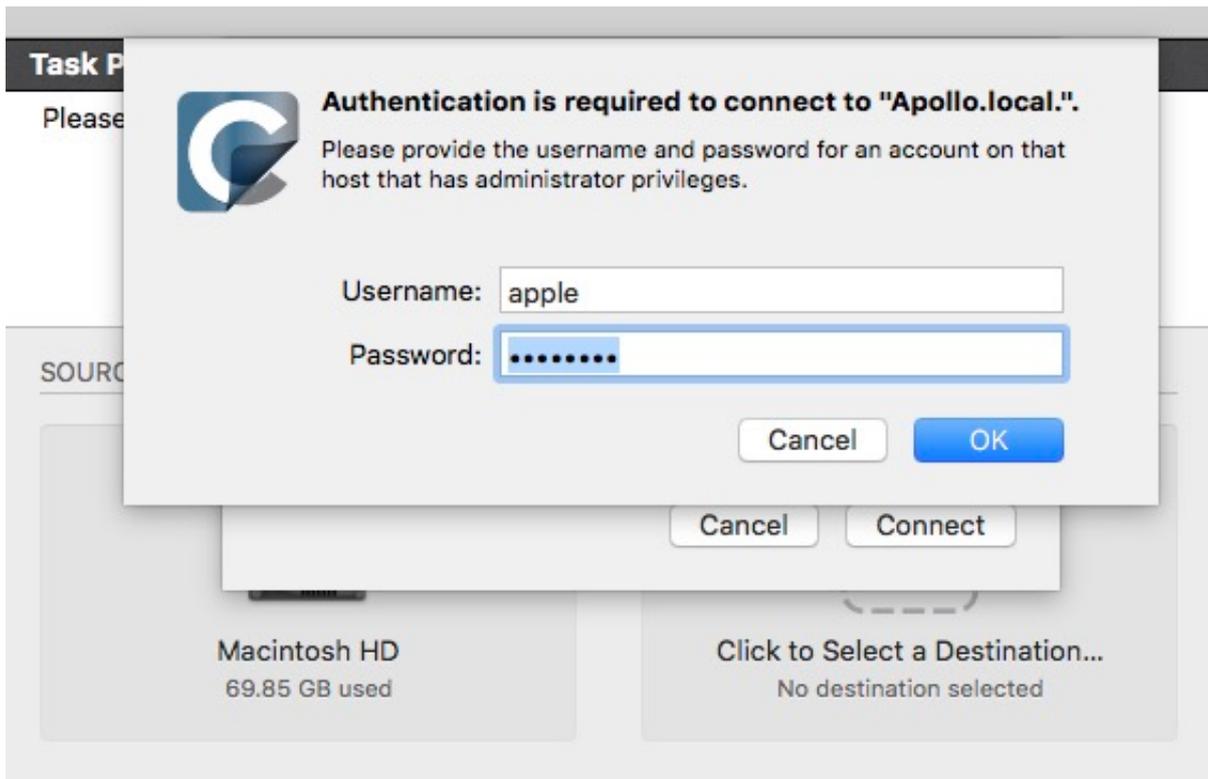
Configuring a Remote Macintosh source or destination

With the Remote Login service enabled on the remote Mac, the next step is to choose Remote Macintosh... from CCC's Source or Destination selector. CCC will present a browser that lists any hosts on your local network that advertise the Remote Login service. Find and select your remote Mac in this list, then click the Connect button. If you do not see your Mac listed here, type in the hostname of your remote Mac, then click the Connect button. If the remote Mac is not on your local network, you may need to specify the IP address of the public-facing router that your Mac resides behind. Be sure to configure the router to forward port 22 traffic to the IP address that is assigned to the remote Mac.

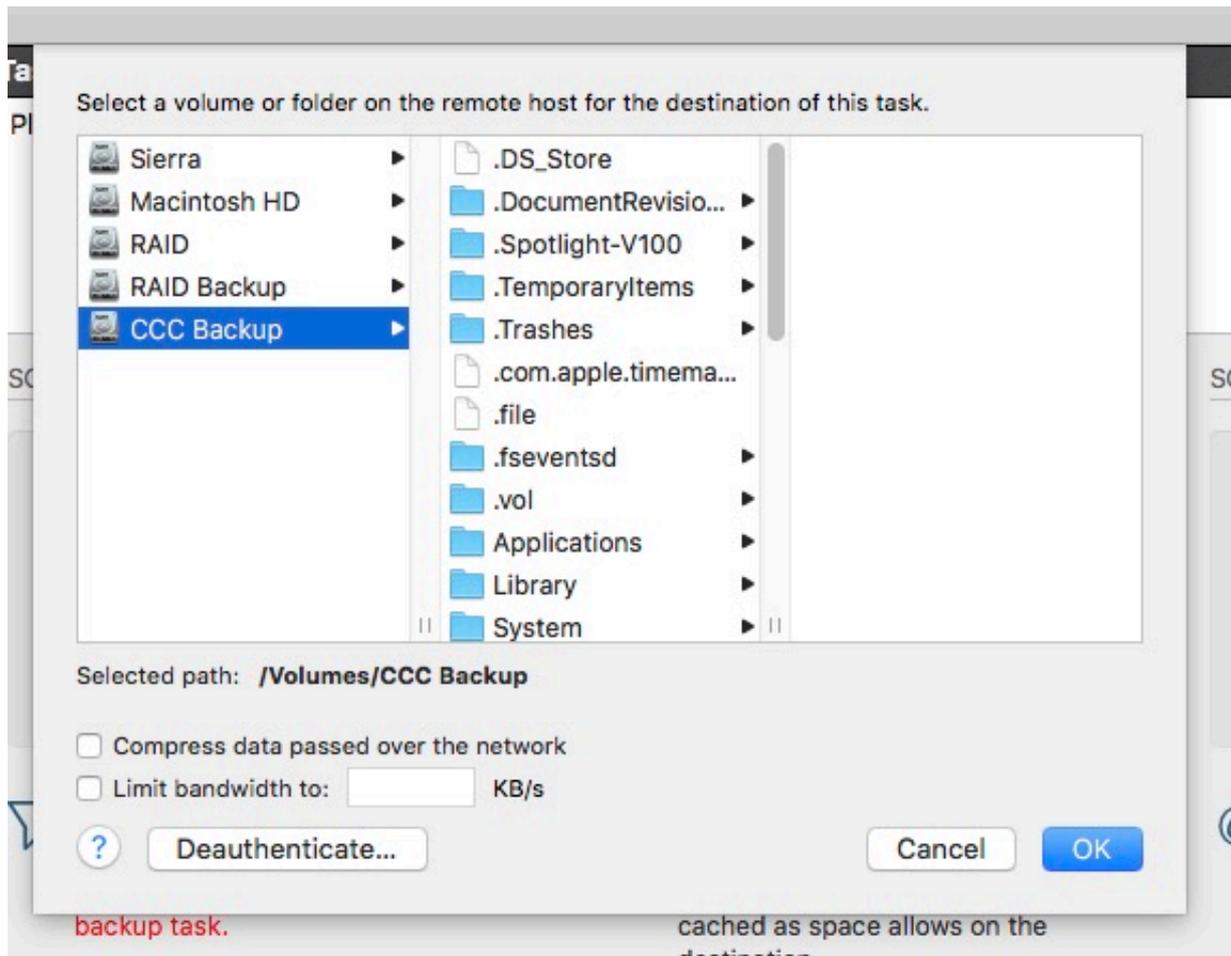


Once CCC has established a connection to the remote Mac, you will be prompted to install a Mac-specific Public Key Authentication (PKA) key pair onto the remote Mac. You must provide the username and password of an admin user on the remote Mac to permit this, and that admin user must have a non-blank password. Those requirements are only for the initial public key installation. For future authentication requests, CCC will use the PKA key pair.

Note: This step establishes a high level of trust between the local and remote Mac; this is required to correctly preserve file ownership. The local Mac will have access to all data on the remote Mac, and administrative users on the remote Mac can gain access to the data that you back up to that Mac. Both Macs should be within your administrative control.



Once you have connected to the remote Mac and installed CCC's key on that system, CCC will present a volume browser. Select the volume or folder to use as the source or destination for your task. Note: avoid selecting a volume or folder that contains an apostrophe (').



Bandwidth management options

CCC offers two options that can help you address bandwidth concerns. The option to Compress data passed over the network can greatly reduce your backup time and total bandwidth used. The time savings depend on just how slow the connection is between the two Macs. If you have a connection that is slower than 10MB/s, compression will make the transfer faster. If your bandwidth is better than that, compression may actually slow down your transfer. CCC will not compress certain file types that are already compressed, such as graphics files, movies, and compressed archives. Specifying the option to compress data passed over the network does not create a proprietary or compressed backup; files are automatically decompressed on the destination volume on the remote Macintosh.

CCC also offers a bandwidth limitation option. If your ISP requires that your transfers stay below a certain rate, you can specify that rate here. Note that CCC errs on the conservative side with this rate, so the average transfer rate may be slightly lower than the limitation that you specify.

De-authenticating a remote Macintosh

If you no longer wish to use a particular remote Macintosh, you can click the Deauthenticate... button to remove CCC's PKA key pair from the remote Mac.

Remote Macintosh prerequisites

At this time, CCC requires the use of the root account (though it does not have to be enabled) on both the source and destination Macs. To successfully back up to a remote Macintosh, you must have administrative privileges on

both machines.

CCC also requires that the remote Macintosh be running macOS 10.7 or later. Non-Macintosh systems are not supported with the Remote Macintosh feature.

Note for Yosemite, El Capitan, & Sierra users: If your source contains macOS Yosemite (or later) system files, the Remote Macintosh must be running macOS 10.9.5 or later. If the Remote Macintosh is not running 10.9.5 or later and you attempt to back up macOS Yosemite (or later) system files, the backup task will report numerous "Input/output" ("Media") errors. Filesystem changes introduced on Yosemite cannot be accommodated by older OSes. Apple added support for those filesystem changes in 10.9.5 to offer a modest amount of backwards compatibility.

Additional pointers for advanced users

Carbon Copy Cloner's public key-based authentication is designed to work with no additional configuration of the services required for backing up over a network connection. CCC uses rsync over an ssh tunnel to perform the backup. If you do make modifications to the sshd configuration, you should consider how that may affect your backup. For example, CCC requires use of the root account over ssh. If you set the "PermitRootLogin" key in the sshdconfig file to "no", you will not be able to use CCC to or from that machine. It's an important distinction to note that the root account does not have to be enabled, but sshd must permit the use of the root account. The "PubkeyAuthentication" key must also not be set to "no", because Public Key Authentication is required for CCC to authenticate to the remote Mac. CCC will attempt to proactively present these configuration scenarios to you if authentication problems are encountered.

Additionally, the initial Public Key Authentication (PKA) setup requires the use of an admin user on the remote Macintosh. That admin user account must have a non-blank password, and the Remote Login service must permit password-based authentication. These requirements apply only to the initial installation of CCC's PKA credentials. Once CCC has installed these credentials on the remote Mac, CCC will use PKA for authentication to the remote Mac.

Troubleshooting connectivity problems to a remote Macintosh

Problems connecting to a remote Macintosh generally are caused by configuration problems with the Remote Login service on the remote Macintosh. Try the following if you are having trouble making a backup to a remote Mac:

1. Verify that the Remote Login service is enabled in the Sharing preference pane on the Remote Macintosh.
2. Verify that access to the Remote Login service is allowed for All users.
3. Re-select Remote Macintosh from CCC's Source or Destination selector and verify that authentication to the remote Mac is configured.
4. Verify that your firewall and the remote Mac's firewall permits traffic on port 22. If you have an application firewall in place (e.g. Little Snitch), verify that access is granted to CCC's privileged helper tool, "com.bombich.ccchelper".
5. If your local Mac and remote Mac are not on the same network (e.g. you're connecting across a VPN or through a router and over the Internet), confirm that a connection can be established between the two Macs. How you do this will vary from one scenario to the next, but you can generally verify connectivity by typing "ssh root@192.168.1.1" into the Terminal application (replace 192.168.1.1 with the hostname or IP address of your remote Mac). If you see a request for a password, then connectivity is established. If not, your network configuration isn't permitting the traffic, or the hostname that you're connecting to is invalid or unavailable. If you are accessing a remote Mac that is behind a router, consult the router's port forwarding documentation and verify that port 22 traffic is directed to the internal IP address of the remote Mac.

VPN and port forwarding configuration is outside of the scope of support for CCC, though our support staff will make every effort to identify whether problems are occurring within that configuration or within the service configuration on your remote Mac. If you have worked through the troubleshooting steps above and are still having trouble backing up to a remote Macintosh, please choose Report a problem from CCC's Help menu and submit a

support request.

Meraki router intercepts Secure Shell traffic

Some users that have a Meraki router involved in their configuration have reported that its default configuration will interrupt Secure Shell traffic. The firewall rule that causes interference is in place to protect the network from [vulnerabilities that are irrelevant between two modern Macs <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0639>](http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0639). Nonetheless, the firewall intercepts traffic after initially allowing a connection, which is presented by CCC as a "lost connection" or a failure to authenticate to the remote Mac. The following steps correct the Meraki configuration concern:

1. Log into the Meraki as an administrative user and open the "Security report"
2. Filter the log for SSH events
3. Click the "SSHEVENTREPOVERFLOW" event from the list to open it and review the blocked event
4. To allow the blocked traffic of this type, click "Yes" to add this event to the whitelist.

Thomson Gateway router intercepts Secure Shell traffic

Similar to the problem described above for Meraki router, the Thomson Gateway router can also cause interference that appears as an authentication failure. Forwarding traffic to a non-standard secure shell port (e.g. 2222, then be sure to specify that port when connecting to the Remote Macintosh in CCC) resolves the problem.

A note about access privileges to backed up data

While logged in to your remote Macintosh, you may not have permission to view the contents of your backup in the Finder. Your access to the files will be based on the unique id that is associated with the user account that you're logged in to on the remote Macintosh and the one associated with the account(s) on the other Mac(s) that you're backing up. The first administrator account always gets a uid of "501", and subsequent accounts are assigned incrementally higher uids — 502, 503, etc. For security and privacy purposes, macOS restricts access to the contents of user home directories to the owners of those home directories, and these restrictions are preserved when your data is backed up to a remote Macintosh.

To learn what user id is associated with your account:

1. Open System Preferences and click on the User Accounts preference pane.
2. Click on the lock and authenticate.
3. Control+click on your account in the accounts table and choose "Advanced options".

You will see your User ID in the panel that appears.

This may be annoying from the perspective of trying to access those files on your remote Macintosh, but it is important for CCC to preserve the ownership and permissions information when backing up your data. If/when you want to do a restore, you could do either of the following:

a) Attach the external drive directly to the machine that you want to restore files to — the accounts on those systems will be able to access their backed up files.

b) [Do a restore directly within CCC <http://bombich.com/kb/ccc5/restoring-from-backup-on-remote-macintosh>](http://bombich.com/kb/ccc5/restoring-from-backup-on-remote-macintosh) from the original source Macintosh.

If you must have read access to some of this data (e.g. the original Mac is gone, the user account changed, etc.), you can change the ownership of the home folder and its contents in the Finder:

1. Choose Get Info from Finder's File menu.
2. In the Sharing and Permissions section at the bottom, click on the lock icon to make the permissions

editable.

3. Click on the + button.
4. In the window that appears, select your account, then click the Select button.
5. Set the access privileges to Read & Write.
6. Click on the Gear menu and choose to apply the change to enclosed items.

Making bootable backups on remote Macs

If you are attempting to create a bootable backup of your Mac, you should attach the backup disk directly to your local Mac for an initial backup task. After verifying that the backup volume is bootable, you can then attach that disk to a remote Macintosh and proceed with regular backups. You should also repeat the local backup any time you apply major operating system upgrades so that any helper partitions on the backup disk can be updated accordingly.

Catalina users: Starting with macOS Catalina, creating bootable backups on a remote Macintosh is no longer practical — CCC can only perform the myriad of partitioning tasks that are required by Catalina on a locally-attached device. You can establish a bootable backup by attaching the destination disk directly to your Mac for the initial backup, but once that disk is attached to a remote Mac, CCC will only be able to maintain a backup of the Data volume. Copying system files to a remote Macintosh is not supported on systems running Catalina or later. If you select a Catalina startup disk as the source for a backup task and a remote Macintosh destination, CCC will automatically exclude system files from the backup task. When selecting a destination on the remote Mac for this sort of backup, choose the "Data" volume that is associated with your backup destination, e.g. "CCC Backup - Data" (NOT the volume named just "Data"; that is your remote Mac's startup disk Data volume!). If you would like to avoid the system file restriction and back up your whole source Data volume, you can drag that volume (e.g. "Macintosh HD - Data") from CCC's sidebar onto the Source selector.

Likewise, CCC will not allow the selection of a Catalina+ System volume on a remote Mac as the source for a backup task. Instead, choose the "Data" volume on the remote Mac to back up the user data portion of the startup disk. This backup will not be bootable, but it can be used as a source to the Migration Assistant application.

Snapshot support on remote Macs

Snapshot support is not available for volumes attached to a remote Macintosh.

Related Documentation

- [Restoring from a backup on a remote Macintosh <http://bombich.com/kb/ccc5/restoring-from-backup-on-remote-macintosh>](http://bombich.com/kb/ccc5/restoring-from-backup-on-remote-macintosh)
- [A caveat for backing up to a remote Macintosh that has no user logged in <http://bombich.com/kb/ccc5/caveat-backing-up-remote-macintosh-has-no-user-logged-in>](http://bombich.com/kb/ccc5/caveat-backing-up-remote-macintosh-has-no-user-logged-in)

A caveat for backing up to a remote Macintosh that has no user logged in

For improved detachability, macOS will unmount any non-internal volumes that are attached to the system when you log out. So, for example, if you log out of your computer while a USB or Thunderbolt hard drive enclosure is attached, you can detach those hard drive enclosures from the system without having to manually unmount them first. This is a good thing — it would be annoying if you had to log back in to your system just to eject a drive. The downside of this, though, is that if you have a CCC backup task that runs when no user is logged in, the destination volume may be unavailable. For a local backup, CCC will attempt to manually mount the destination volume. When the destination of your backup task is a remote Macintosh, however, CCC will not be able to mount that volume prior to backing up.

If you anticipate backing up to a remote Macintosh that may be sitting at the loginwindow, you can change the behavior of macOS to not unmount detachable volumes. To change this behavior, run this command in the Terminal application on the remote Macintosh:

```
sudo defaults write /Library/Preferences/SystemConfiguration/autodiskmount AutomountDisksWithoutUserLogin -bool YES
```

Related Documentation

- [Using Carbon Copy Cloner to backup to another Macintosh on your network](http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network)
<<http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network>>

Restoring from a backup on a remote Macintosh

macOS Catalina (10.15) and later

Starting with macOS Catalina, creating bootable backups on a remote Macintosh is no longer practical — CCC can only perform the myriad of partitioning tasks that are required by Catalina on a locally-attached device. You can establish a bootable backup by attaching the destination disk directly to your Mac for the initial backup, but once that disk is attached to a remote Mac, CCC will only be able to maintain a backup of the Data volume. That volume will remain bootable, but depending on how far out of date the OS is on the backup, you may not want to restore the OS to a replacement disk. You can use Migration Assistant instead in those cases:

1. Hold down Option()-Command ()-R to boot the Mac in Internet Recovery mode
2. Install macOS onto the replacement hard drive
3. When prompted, attach the backup disk to your Mac and use Migration Assistant to migrate data from the backup volume to the replacement startup disk

Related Documentation

- [Making bootable backups on remote Macs <http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network#bootable>](http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network#bootable)

macOS Yosemite, El Capitan, Sierra, High Sierra, Mojave (10.10 through 10.14)

Restoring files from a remote Macintosh is nearly the same procedure as backing up to a remote Macintosh:

1. Open CCC
2. Click the New Task button in the Toolbar
3. Select Remote Macintosh... from the Source selector
4. Configure the hostname of the remote Macintosh and connect to the remote Mac
5. Choose the path to the volume or folder that has the backup.
6. Select a destination volume
7. Click the Clone button

Related Documentation

- [Using Carbon Copy Cloner to back up to/from another Macintosh on your network <http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network>](http://bombich.com/kb/ccc5/using-carbon-copy-cloner-back-up-another-macintosh-on-your-network)

タスクを整理する

タスクを追加するには

タスクを追加するにはいくつか異なる方法があります。デフォルト設定を使って新規タスクを作成するには、タスク表から +

アイコンをクリックする、CCCのファイルメニューから **新規タスク**

をクリックする、CCCのツールバーから **新規タスク**

をクリックする、のいずれかを使用してください。また、既存のタスクを複製することもできます。タスクリストからタスクを選択して、CCCのファイルメニューから **複製**

を選択するか、またはタスクを右クリックして “複製” のオプションを選択してください。

前にCCCからタスクを書き出した (現在使用中のMacまたは別のMacに) 場合、タスクをCCCに読み込むためにタスク設定をダブルクリックしてください。

タスクを削除するには

タスクを削除するには、タスク表の見出しから -

アイコンをクリックする、CCCのファイルメニューから **タスクを削除...**

をクリックする、またはタスクを右クリックして “タスクを削除” のオプションを選択する、のいずれかを使用してください。タスクを削除することはCCCのデータベースからタスク設定のみを削除します。タスクがコピー先ボリュームにバックアップしたデータには影響がありません。

タスクを並べ替える

デフォルト設定では、タスクはアルファベットの昇順に並んでいます。並べ替え順や条件を変更するには、タスク表の三角形のアイコンをクリックしてください。タスクを並べ替えるには、名前、最後の実行時間、次の実行時間、最後の実行状況、手動で自分の定義したい順序、のいずれかを使用できます。手動で並べ替え順を定義する場合、タスクをドラッグ&ドロップして順序を調整してください。

タスクグループ

タスク表にある “タスクグループを追加” (“+” の付いたフォルダ) をクリックして、新規タスクグループを作成してください。タスクをグループにドラッグしてグループにタスクを追加してください。タスクを複数のグループに追加したい場合は、Optionキーを押したままにしてタスクを1つのグループから次のグループにドラッグしてください。タスクグループが実行中はタスクグループを変更できません。

最も基本的として、タスクグループはタスクを整理するために使用されます。グループ内のそれぞれのタスクは、その他のタスクから独立してスケジュール設定及び設定ができます。また、タスクグループはタスクを一括して実行するのに使用することもできます。“タスクグループ” を選択して、ウインドウの下にある “クローン” をクリックすると、グループ内のタスクのすべてを実行することができます。CCCは **今後のグループおよびタスクのイベント表** で定義されている順序でタスクを順番に続けて実行します。

タスクリストの並べ替え順 vs. タスクグループの実行順

タスク表のグループ内に表示されているタスクはタスク表の並べ替え条件に基づいて並べ替えられます。タスク表を手動で並べ替えたい場合は、タスク表のグループ内のタスクを好きなように並べ替えることができます。これをグループ内のタスクの実行順と

混同しないようにしてください。タスクの実行順は

今後のグループおよびタスクのイベント表 に定義されています。

タスクグループをスケジュールするには

タスクグループは個々のタスクと同じ方法でスケジュールできます。“スケジューラー”セレクトをクリックして、スケジュールの基本を選択してから、そのグループを実行したいタイミングを定義してください。タスクはグループ内で順番に続けて実行されます。タスクの1つに独自のスケジュールが設定されている場合、そのタスクはタスクグループから独立しても実行されます。タスクグループがそのタスクを開始しようとする時、そのタスクがすでに実行中の場合は、そのタスクグループはグループ内の次のタスクに移動します。タスクの1つがその独自のスケジュールされた実行時間になった時にすでにタスクグループ経由で実行中の場合、そのタスクはそのまま実行を継続し、追加で実行されることはありません。個々のタスクの実行時間の条件は、タスクグループ経由でタスクを実行する際に考慮されます。例えば、あるタスクが週末に実行されないように設定されている場合、タスクグループが週末に実行される場合でも、そのタスクはグループ経由で実行されません。唯一の例外は、タスクグループを手動で実行するように選択している場合です。その場合、実行時間の条件は無視されます。

タスクグループが実行される時、無効にされたタスク以外はそれぞれ、そのグループ内の前のタスクの失敗/成功に関係なく実行されます。唯一の例外はタスクが停止された場合です。タスクグループ経由で開始されたタスクが停止されると、グループ内の他のタスクはそれ以上タスクグループ経由で実行されません。

タスクとグループを書き出すには

タスク表のタスクを右クリックして、“書き出す”のオプションを選択すると、タスクを個別に書き出すことができます。タスクグループ内のすべてのタスクを書き出すには、タスクグループを右クリックして“グループを書き出す”のオプションを選択するか、または、CCCのファイルメニューから**タスクグループを書き出す...**を選択してください。
。すべてのタスクを書き出したい場合は、CCCのファイルメニューから**すべてのタスクを書き出す...**を選択してください。

I want to defragment my hard drive

A welcome side-effect of cloning one volume to another is that the files on the resulting volume are largely defragmented. While fragmentation is not as significant of an issue as it used to be (e.g. in the Mac OS 9 days), people that have begun to fill the last 10-15% of their boot volume may see some performance benefit from defragmentation. If you find yourself in this situation, this is also a really good time to consider migrating to a larger hard drive altogether, or to an SSD, which is not affected by fragmentation.

Defragmentation is a natural result of backing up your data to an empty backup volume. Simply [prepare your backup volume for use with Carbon Copy Cloner <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x), then use CCC to clone your source volume to your destination volume.

"Clone, wipe, restore" — think twice before you wipe that original volume

It may be really tempting to do the following:

1. Clone your boot volume — the one with your lifetime of irreplaceable data — to another hard drive
2. Boot your Mac from that cloned volume
3. Use Disk Utility to wipe the original volume
4. Restore the cloned volume to the original volume

Very quickly you'll be booted back up from your boot volume and you'll have a backup to boot, right? In most cases, this would work out great for you, and you'd be fine. There are two really good reasons, however, to stop after the second step and take a breather:

1. As soon as you erase the original volume, you're down to one copy of your data — you have no backup. The restore task will stress both the source and destination disks with massive reads and writes. If either disk were on the verge of failure, this level of stress could push it over.
2. You really should take the time to verify your backup. I trust CCC with my data, but do I trust that I asked it to copy the right items? Did my destination disk turn out to be a lemon?

The Best Practice for defragmenting your hard drive

1. Establish a backup regimen to a primary backup volume. Test your backups regularly.
2. Quit open applications and use CCC to update your backup one last time.
3. Use CCC to clone your hard drive to some physical volume other than your primary backup.
4. Boot from the cloned volume.
5. Use Disk Utility to reformat your original volume.
6. Use CCC to restore your cloned volume back to the original volume.
7. Boot from the original volume.

Performance upon first boot from a cloned volume will always be slightly slower than normal as Spotlight reindexes your data. When the system has "settled down", you will be able to evaluate whether the defragmentation has offered any performance benefit.

Using the ccc Command Line Tool to Start, Stop, and Monitor CCC Backup Tasks

Carbon Copy Cloner includes a command line utility that allows you to start, stop, and monitor the progress of specific CCC backup tasks. The utility is located inside of the CCC application bundle. To get basic usage instructions, invoke the utility without arguments in the Terminal application, e.g.:

```
user@Mac ~ % "/Applications/Carbon Copy Cloner.app/Contents/MacOS/ccc"
ccc -v|--version
    Prints the version of the CCC command-
line utility (this is not the same as the main application version)
ccc -s"Task Name" | --start="My Backup Task" (-w|--watch)
    -w|--watch: Keep running and print task output until the task is finished. Ignored
for task groups.
ccc -x["Task Name"] | --stop[="My Backup Task"] [-r]
    Stop all tasks, or the specified task.
    By default the task is treated as if cancelled.
    Use -r to report the event (e.g. nia Notification Center and, if configured, email)
.
    Use another non-zero value if you would like task notifications to be sent.
ccc -h|--history [-c|-d]
    Print a summary of task history, i.e. the data you would see in the table at the top
of the Task History window.
    -c prints in CSV format
    -d prints dates in seconds since Midnight Jan 1, 1970 (rather than formatting the date)
ccc -p|--print-schedules [-c|-d]
    List each task and when it will next run.
    -c prints in CSV format
    -d prints dates in seconds since Midnight Jan 1, 1970 (rather than formatting the date)
ccc -w["Task Name" | --watch[="Task name"]
    Watch task progress (press Control+C to exit)
    Specify a task name to limit task output to the indicated task
ccc -i|--status
    Print a status line for each task.
ccc -g|--global globalDefaultName [bool|int|float|string] globalDefaultValue
    Set a global default value.
ccc -g|--global globalDefaultName delete
    Delete a global default value.
ccc -n|--notification notificationTitle notificationBody
    Send a notification to the Notification Center.
ccc -z["Task Name"] | --disable[="Task Name"]
ccc -e["Task Name"] | --enable[="Task Name"]
    Disable or enable all tasks [or a specific task].
ccc -u | --uuids
    Print task names and their unique identifiers.
```

Here are some examples of how to use the CCC command-line tool to start and stop a task, and get its last history event:

```
[user:~] cd "/Applications/Carbon Copy Cloner.app/Contents/MacOS"
[user:/Applications/Carbon Copy Cloner.app/Contents/MacOS] ./ccc -s"CCC Backup Task"
-w
04/24 12:52:19 : CCC Backup Task [Data copied: Zero KB, Progress: -1.000000%] Prepari
ng...
04/24 12:52:20 : CCC Backup Task [Data copied: Zero KB, Progress: -1.000000%] Testing
write responsiveness of the destination...
04/24 12:52:20 : CCC Backup Task [Data copied: 126 bytes, Progress: 0.076235%] Compar
ing and copying files
04/24 12:52:21 : CCC Backup Task [Data copied: 126 bytes, Progress: 1.146266%] Compar
ing and copying files
04/24 12:52:21 : CCC Backup Task [Data copied: 126 bytes, Progress: 1.963699%] Compar
ing and copying files
04/24 12:52:22 : CCC Backup Task [Data copied: 126 bytes, Progress: 3.048320%] Compar
ing and copying files
^C

[user:/Applications/Carbon Copy Cloner.app/Contents/MacOS] ./ccc -x"CCC Backup Task"
Stopping CCC Backup Task

[user:/Applications/Carbon Copy Cloner.app/Contents/MacOS] ./ccc -h | head -n 1
CCC Backup Task|Macintosh HD|SSD Macintosh HD Backup|4/24/20, 12:52 PM|0:19|126 bytes
|Cancelled|0
```

Backing up databases on OS X Server

Databases are proprietary file types that often cannot be backed up in the conventional manner. In CCC, you can leverage a preflight shell script to perform an "out of band" backup of various databases using database-specific tools. The CCC backup task will subsequently back up the database archive files, from which you could restore the database at a later time.

The following pre-clone shell script will dump the contents of any MySQL databases. In the event that your standard backup of the database doesn't open, you can later restore it from the dump.

```
#!/bin/sh
PATH="$PATH:/Applications/Server.app/Contents/ServerRoot/usr/bin"
PATH="$PATH:/Applications/Server.app/Contents/ServerRoot/usr/sbin"
PATH="$PATH:/Applications/Server.app/Contents/ServerRoot/usr/libexec"
export PATH

# Path to recovery directory (permissions should be 700 -- read-only root or admin)
recover="/etc/recover"
ts=date "+%F"

echo "Removing manual archives older than two weeks"
find $recover/ -mindepth 1 -mtime +14 -exec rm '{}' \;

# mysqldump the databases
dbs="somedatabase anotherdatabase mysql"
for db in $dbs; do
    echo "Dumping $db"
    mysqldump --user=root --password='s3kr!t' $db > $recover/${db}${ts}.dump
    gzip $recover/${db}${ts}.dump
done

# If you ever need to restore from a database dump, you would run:
# gunzip $recover/databasename(timestamp).dump.gz
# mysql -u root -p databasename < $recover/databasename.dump
```

Backing up an Open Directory Master

Archiving an OD master database requires encryption, and providing the encryption password interactively can be challenging in an automated backup. The expect shell environment can be helpful for this task. The following pre-clone shell script will archive a macOS Server Open Directory master to a disk image for later restoration via the server administration application.

```
#!/usr/bin/expect -f

set date [timestamp -format "%Y-%m-%d"]
set archivepath "path/to/you/backup/dir"
set archivepassword "password"
set archivename "opendirectorybackup"
set timeout 120

spawn /usr/sbin/slapconfig -backupdb $archivepath/$archivename-$date
```

```
expect "Enter archive password"  
send "$archivepassword #"  
expect eof
```

Related Documentation

- [Example pre and post clone shell scripts <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples>](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples)
- [Bender - Automated Backup of OS X Server Settings \[Third-party script\] <https://forgetcomputers.zendesk.com/hc/en-us/articles/201008710-Bender-Automated-Backup-of-OS-X-Server-Settings>](https://forgetcomputers.zendesk.com/hc/en-us/articles/201008710-Bender-Automated-Backup-of-OS-X-Server-Settings)

Backing up large files, mounted disk images, and Virtual Machine containers

Note: When backing up an APFS-formatted volume with CCC 5.1 or later, CCC will copy files from a read-only snapshot of the source volume. The subject of this article is not applicable in those cases.

Mounted disk images and running Virtual Machine container files pose an interesting problem to incremental backup utilities. By simply being mounted and accessed (e.g. via browsing the contents, booting the VM), the content of these large files are subject to modification by the applications that use those files. If you run a CCC backup task while a read/write disk image is mounted or while a VM container's OS is booted, there is a chance that the disk image file or VM container will be modified while it is being backed up, resulting in a corrupted version of the file on your backup volume.

If you have disk image files or VM containers that are regularly in use on your system, you should exclude these items from your backup routine and configure an alternate backup task for these items that runs when they are not in use. Alternatively, you could quit or suspend the applications that modify those files for the duration of the backup (see the "Example pre and post clone shell scripts" link below for examples of how to automate this).

If errors do occur while backing up large files, quit or suspend the applications that modify those files, then simply run the backup task again to correct the copy of the file on the backup volume.

Related Documentation

- [Example pre and post clone shell scripts <http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples>](http://bombich.com/kb/ccc5/performing-actions-before-and-after-backup-task#examples)
- [Creating a separate task to prevent VM container versions from bloating the SafetyNet <http://bombich.com/kb/ccc5/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet>](http://bombich.com/kb/ccc5/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet)
- [Leveraging Snapshots on APFS Volumes <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes)

CCC SafetyNet フォルダの自動管理

この記事の内容はスナップショットのサポートがAPFSフォーマットされたコピー先ボリュームで有効になっている時には関連性がありません。SafetyNetのスナップショットの保持に関する詳しい情報は [スナップショットのサポートを切り替え、スナップショット保持ポリシーを設定するには](http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes#srp) <<http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes#srp>> を参照してください。

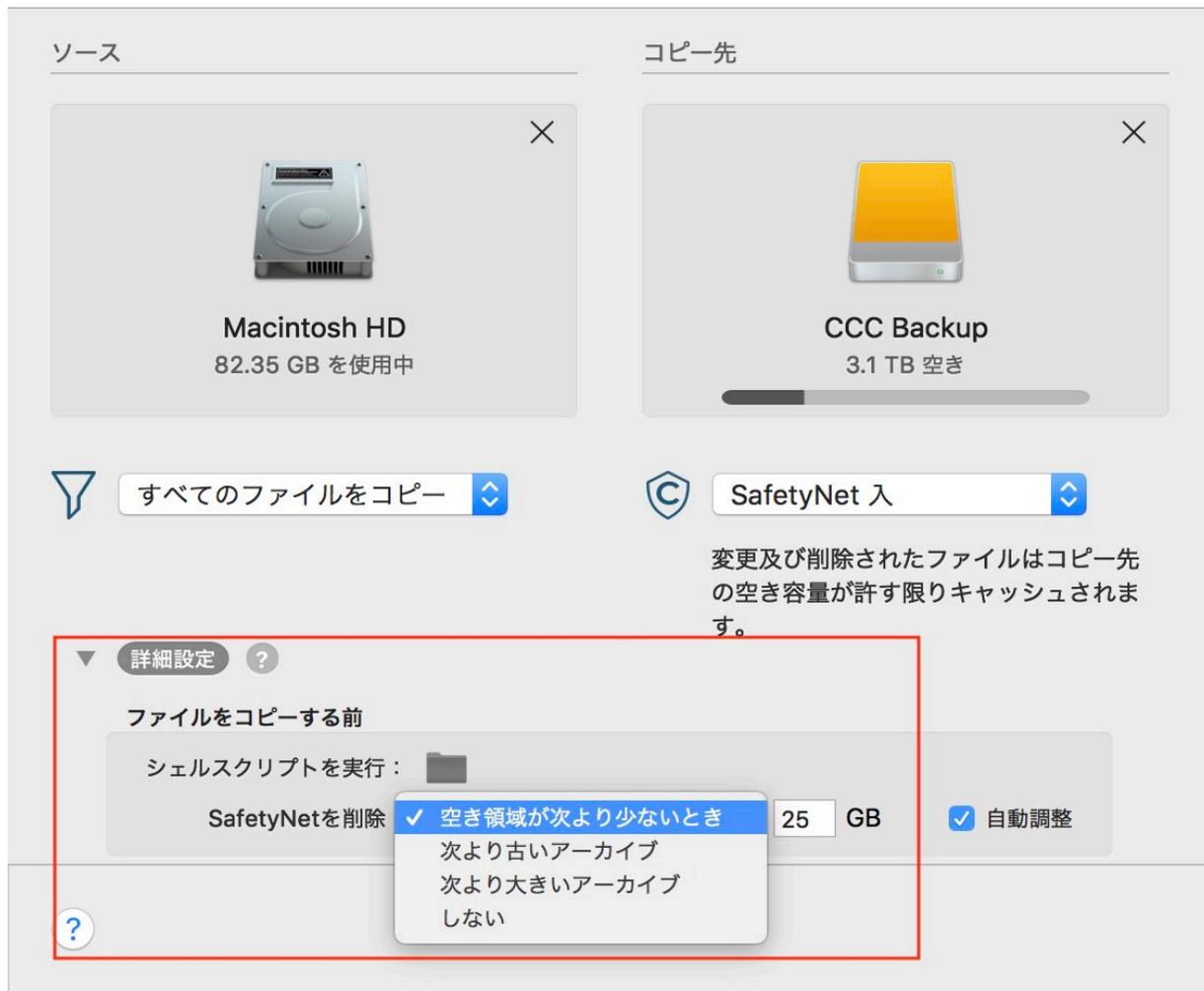
Carbon Copy Clonerは変更されたファイルの前のバージョンを、前のバックアップタスク以降に削除されたファイルと同様に、コピー先のルートにあるSafetyNetフォルダに移動します。このSafetyNetフォルダは、管理されないままにしておくと、いずれコピー先ボリュームのすべての空き容量を消費してしまうことになります。これを避けるために、CCCは空き容量が25GBを下回ると、それぞれのタスクの最初にSafetyNetフォルダのコンテンツを削除します。この制限は、25GBの制限が特定のソースとコピー先に少なすぎる場合、自動的に調整されます。これらの設定は、CCCのメインウィンドウにある**高度な設定**ボタンをクリックしてカスタマイズできます。

“CCC Backup Task”のタスクプラン

CCCはMacintosh HDをCCC Backupにコピーします。最後のバックアップタスク以降に変更されたハードウェアの互換性に問題がない限り、**コピー先ボリュームは起動可能なはず**です。

最終実行日：今日 9:20

次の実行日時：“クローン”をクリックすると、このタスクを実行します。



The screenshot shows the Carbon Copy Cloner interface with the following elements:

- ソース (Source):** Macintosh HD (82.35 GB を使用中)
- コピー先 (Destination):** CCC Backup (3.1 TB 空き)
- File Selection:** A dropdown menu set to "すべてのファイルをコピー" (Copy all files).
- Destination Filter:** A dropdown menu set to "SafetyNet 入" (Include SafetyNet).
- Advanced Settings (詳細設定):** A section with a red border containing:
 - Files to copy before: Shell script to execute: SafetyNetを削除
 - Empty space threshold: 25 GB (with a dropdown menu open showing options: "空き領域が次より少ないとき" (selected), "次より古いアーカイブ", "次より大きいアーカイブ", "しない")
 - Auto-adjust: 自動調整

SafetyNetの削除はバックアップタスクの最初に実行されるので、CCCは現在のバックアップタスクにアーカイブされた項目を削除することは決してありません。さらに、削除は必ずコピー先のルートにあるCCC SafetyNetフォルダのコンテンツに制限されます。CCCの削除はコピー先ファイルの現在のバージョンを削除することはありません。また、CCCのバックアップタスクの範囲外のファイルを削除することはありません。最後に、削除のアーカイブはマクロレベルで動作します。もし、アーカイブのいずれかのポジションが課された制限を超えると、アーカイブ全体 (例：時間のついたフォルダ) が削除されます。

“新規ディスクイメージ”のコピー先に関する注意

CCCはディスクイメージボリュームに、より積極的なSafetyNetの削除設定を適用します

<http://bombich.com/ja/ja/kb/ccc5/backing-up-disk-image#safetynet>

。デフォルトで、CCCは1日を超えたSafetyNetコンテンツはすべて削除します。

ファイルをコピーする前にアーカイブされたコンテンツを自動的に削除する

空き容量が [xx] GB以下になるとSafetyNetのアーカイブを自動的に削除

コピー先ボリュームの空き容量が指定された制限を下回ると、CCCは一番古いファイルを削除します。CCCは必要な空き容量を確保できるまで一番古いアーカイブから削除を続けます。アーカイブが累積的に必要な制限より少ない容量を消費して、コピー先ボリュームがいっぱいになった場合、CCCはすべてのアーカイブを削除しますので、注意してください。

SafetyNetの空き領域の削除制限の自動調整について

自動調整のオプションが有効になっている場合 (デフォルトで有効になっています)、バックアップタスク中コピー先に空き領域が不足してくると、CCCは自動的に空き領域の削除制限を増加します。例えば、削除制限がデフォルトの25GBに設定されていて、バックアップタスクの開始に25GBの空き領域がある場合、タスクの開始時に削除は実行されません。しかし、そのタスクが進むうちに25GB以上のデータをコピーする場合、コピー先はいっぱいになります。その場合、CCCは現在のタスクでコピーされたデータ量か、CCCがコピーしようとしている最後のファイルに必要なデータ量のどちらか大きい方で削除制限を増加します。例えば、CCCが25GBのデータをコピーした場合、削除制限は25GBに増加します。しかし、CCCが40GBのファイルをコピーしたい場合、CCCはそのファイルの25GBを無駄にコピーするのではなく、むしろ、削除制限を即座に40GBに増加して、削除をしてから、タスクを再開します。

SafetyNetにある[xx] 日より古いアーカイブを削除

CCCは“xx”日前より前に作成されたアーカイブを削除します。

SafetyNetにある[xx] GB以上のアーカイブを削除

CCCは最も新しいアーカイブから開始して、それぞれのアーカイブが消費しているディスク容量を判断します。累積的な合計が課された制限を超えると、CCCは残りの、古いアーカイブを削除します。最新のアーカイブが指定された制限よりも大きい場合、そのアーカイブはすべて削除されます。

SafetyNetのアーカイブを削除しない

CCCはコピー先のルートにある“CCC SafetyNet”のコンテンツが自動的に削除されることはありません。アーカイブされたファイルが最終的にコピー先の空き容量をすべて消費してしまう可能性があります。そのため、将来のバックアップに備えて十分な空き容量を維持するために、古いアーカイブフォルダを定期的に削除する必要があります。バックアップセットの残りに害を与えることなくSafetyNetフォルダのコンテンツを削除できます。

“ CCCはSafetyNetを削除していますが、それでもバックアップタスクの最後にはディスクがかなりいっぱいになります”

CCCがSafetyNetを削除する目的はバックアップを追加できるように空き容量を確保することです。また、CCCは非常に新しくアーカイブされた項目を削除することを避けます。なぜなら、コピー先に項目をアーカイブしてその後すぐに削除することは意味がないからです。これら両方のゴールを達成するために、CCCはバックアップタスクを実行する前にSafetyNet内のアーカイブを削除します。ファイルをコピーする直前にSafetyNetを削除することは、現在のバックアップに利用できる必要な空き容量が(例えば)あるという安心を与えてくれます。SafetyNetの削除設定を指定する際にこの詳細を必ず考慮してください。CCCのバックアップに必要な量以上にバックアップボリュームに追加の空き容量を保持しておきたい場合は、より大きな制限を指定してください(例えば、25GBではなく100GBなど)。

“ 特定の項目を長期的にアーカイブしたい時にCCC SafetyNetフォルダを使用できますか? ”

SafetyNetを長期的な保管に使用することはお勧めしません。CCCはバックアップタスクの開始時にコピー先の空き容量が25GB以下の時、SafetyNetを自動的に削除するようデフォルトで設定されています。CCCは、CCC SafetyNetフォルダの項目がCCCか他のアプリケーションか、どちらによって置かれたものかどうかを考慮しません。つまり、タイミングが正しければどんなものでも安全に削除できると考えます。バックアップボリュームにある項目を、CCCのバックアップ外で、永続的にアーカイブしたい場合、コピー先ボリュームのルートレベルにこの目的のための特定のフォルダを作成することをお勧めします。

また、別のボリュームでアーカイブデータのバックアップを保持することをお勧めします！長期的にアーカイブした項目をバックアップしない場合、バックアップディスクに問題が起きるとそれらを完全に喪失することになります。

“ CCC SafetyNetフォルダを手動でゴミ箱に移動しましたが、ゴミ箱を空にしようとしたらエラーメッセージが表示されました ”

CCCが起動ディスクをバックアップするとき、通常自分のアカウントにアクセスできないシステムファイルにアクセスするための権利を使って実行されます。当然これらのファイルの中にはソースでアップデートされるものが含まれていて、その結果コピー先でアーカイブされます。これらの項目をゴミ箱に入れ(CCC SafetyNetフォルダをゴミ箱に入れることで)、その後ゴミ箱を空にしようとする、通常Finderからこれらのファイルを削除する認証を求められます。しかし、時にはFinderの機嫌の悪い日があり、ゴミ箱を空にしようとする(または似たようなことをしようとする)と、啓発的な“-8003”エラーが表示されます。このエラーはどこにも定義または文書化されていませんが、失敗を繰り返すうちに、これは単に“ゴミ箱を空にする要求を処理できません”という意味であることがわかりました。

解決策は、

CCCのSafetyNetフォルダの削除にFinderを使用しないということです。代わりに、CCCのユーティリティメニューからSafetyNetフォルダを削除を選択して、そのインターフェースを使って、SafetyNetフォルダを手動で削除してください。

その他の参照

- [Apple Kbase HT201583 : ゴミ箱を空にしたりファイルをゴミ箱に移動したりできない場合](https://support.apple.com/en-us/HT201583)
<<https://support.apple.com/en-us/HT201583>>

関連ドキュメント

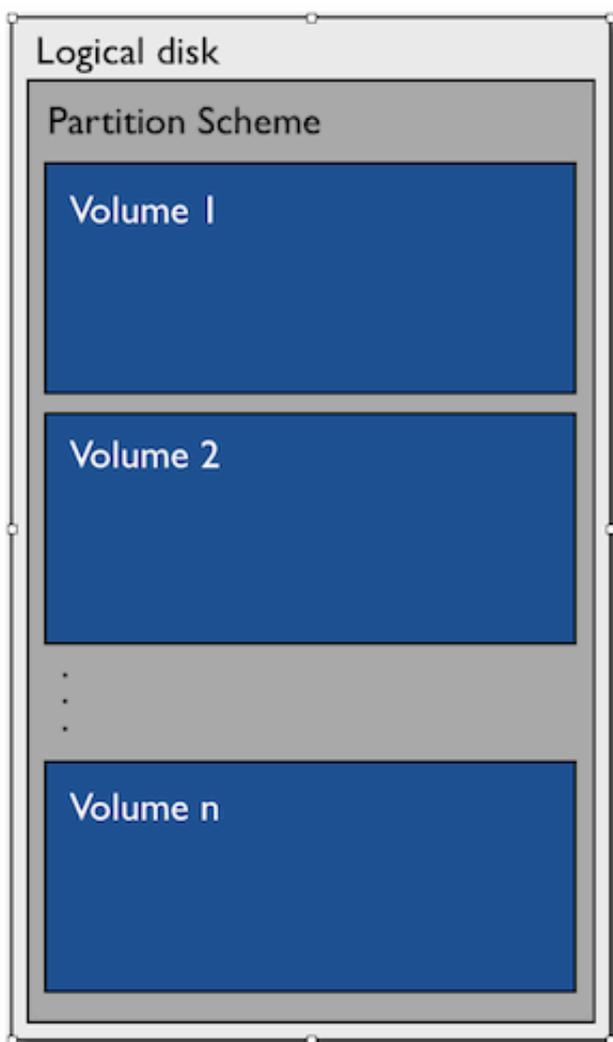
- [Carbon Copy ClonerのSafetyNetについてのよくある質問](http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet) <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet>>

"My disk is already formatted APFS or HFS+, why am I getting this warning?"

If your disk is not partitioned using the scheme recommended and supported by Apple, CCC will indicate a warning when you start the backup task such as:

"You may have difficulty booting from this destination volume, the underlying disk is not partitioned with a partitioning scheme that Apple recommends for Intel Macs.", or when CCC attempts to convert the destination to APFS after installing macOS 10.15 Catalina, CCC may be unable to convert the volume from HFS+.

How your destination volume is formatted is not actually relevant to this warning. The problem is not a matter of how your destination volume is formatted, rather it is a matter of how the disk is partitioned. The following graphic explains the relationship between a disk and a volume:



Every disk has exactly one partition scheme. A disk can be partitioned as "Apple Partition Map" (APM), "GUID Partition Table" (GPT), "Master Boot Record" (MBR), or the Fdisk partition scheme. PowerPC Macs could only boot from a disk that is partitioned with the APM partitioning scheme. Intel Macs can boot from a disk that is partitioned with either the APM or GPT partitioning scheme. Note, however, that Apple only supports booting an Intel Mac from

a disk partitioned with the GPT partitioning scheme. Because Apple no longer supports the APM partitioning scheme, CCC will warn you if your destination disk is not partitioned with the GPT partitioning scheme. As the warning indicates, you may have difficulty booting from the destination volume, but it may work just fine. We expect that Intel Macs will eventually drop support for booting from APM-partitioned disks.

Apple's New APFS format can only reside on a "GUID Partition Table" (GPT) partition scheme so if your destination is not using GPT, CCC will be unable to convert an HFS+ volume to the volume to APFS as required by macOS 10.15 Catalina and the backup will fail with a warning about the partition scheme.

Here's what you need to do about the warning

If you haven't copied any data to the destination disk, then take the time to repartition your disk using the GPT partitioning scheme (see above) so you have a sanctioned, bootable backup volume.

If you cannot repartition the disk because you already have a considerable amount of data on the disk, and are using macOS 10.14 Mojave or earlier, proceed with the backup task, but [confirm whether it can actually boot your Mac <http://bombich.com/kb/ccl5/how-verify-or-test-your-backup>](http://bombich.com/kb/ccl5/how-verify-or-test-your-backup). If it can, you're all set and you shouldn't be bothered by the warning again. If you cannot, you will have to back up the other data on your destination disk and repartition the disk using the GPT partitioning scheme to get a bootable backup.

If you are running macOS 10.15 Catalina, or newer, the volume must be repartitioned.

Backing up to/from network volumes and other non-macOS-formatted volumes

In addition to backing up to volumes formatted with the macOS standard HFS+ or APFS format (collectively referred to as "macOS-formatted" from here forward), CCC can copy user data files to network volumes (e.g. AFP and SMB via macOS and Windows File Sharing) and to other non-macOS-formatted volumes such as FAT32. Non-macOS-formatted volumes are presented in CCC's Source and Destination selectors in the same manner as macOS-formatted volumes, so there are no special steps required for backing up to or from these filesystems. However, these filesystems offer limited support for macOS-filesystem features, so special consideration must be given when backing up to these volumes. In general, you can reasonably expect to back up user data — files that belong to your user account — to and from non-macOS-formatted volumes. Specific considerations are noted below.

You can mount network volumes in the Finder, or via the Mount a network volume... option in CCC's Utilities menu. Please note that network volumes mounted by third-party software is generally not supportable.

CCC will only back up system files to or from locally-attached macOS-formatted filesystems

macOS can only be installed on a macOS-formatted volume. This requirement is also carried to a backup volume. When system files are copied to or from non-macOS filesystems, important metadata are unavoidably lost, resulting in files that cannot be restored to their original functionality. In short, you cannot restore a functional installation of macOS from a backup stored on a non-macOS volume. To prevent any misunderstandings about this result, CCC will exclude system files from a backup task if the destination is not a locally-attached, macOS-formatted volume. Likewise, CCC will not copy system files from a network volume, e.g. if you were to mount the startup disk of another Mac via File Sharing, the system files on that network volume cannot be copied in a meaningful way.

Note that the "locally-attached" caveat is an important distinction. Even if your destination volume is macOS-formatted, if it is attached to an Airport Base Station (for example), then you're accessing the volume via file sharing. If you open the Get Info panel for the volume, you will see that the volume format is "AppleShare" or "SMB", not HFS+ or APFS. It is not possible to update an OS backup on a network volume.

Related Documentation

- [Learn about alternatives to backing up macOS to non-macOS-formatted volumes <http://bombich.com/kb/cc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#diskimage>](http://bombich.com/kb/cc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive#diskimage)
- [Preparing your backup disk for a backup of macOS <http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/cc5/preparing-your-backup-disk-backup-os-x)

Ownership and permissions concerns

Network filesystems pose some interesting challenges in regards to preserving ownership and permissions. When you connect to another computer that is hosting a shared volume, you usually authenticate by providing a username and password. The account whose credentials you provide is an account on that other computer, and it is this account's privileges that determine what access you have to files and folders on the shared volume. Additionally, any files that are copied to the shared volume will be owned by that user account, regardless of the ownership of those files on the source volume. This is not a behavior specific to CCC, it is simply the nature of network filesystems.

An example will be very helpful in understanding the implications of this behavior. Suppose Sally would like to back up some Movies from her Mac's home folder to another Mac shared by Bob and Joe. On Sally's Mac, there is a user account named "sally". On Bob and Joe's Mac, File Sharing has been enabled in the Sharing Preference Pane, and there are two user accounts, "joe" and "bob". Bob has attached an external hard drive named "Backup" to his Mac that he and Joe have been using for backup, and he has created a folder named "Sally's Movies" on this volume to which Sally will copy files. Sally does the following to connect to Bob and Joe's Mac:

1. In the Finder, open a new window, then click on "Bob and Joe's Mac" in the Shared section of the sidebar.
2. Click on the Connect as... button.
3. In the authentication dialog, provide Bob's username and password, then click on the Connect button.
4. Choose the "Backup" volume from the list of shared volumes.

The Backup volume now appears on Sally's Desktop, and in CCC's Destination selector in the Network Volumes section. Next, Sally chooses Choose a folder... from CCC's Source selector and locates the folder of movies that she would like to copy to Bob and Joe's Mac. She then chooses Choose a folder... from the Destination selector and locates the "Sally's Movies" folder on the Backup network volume. She clicks the Clone button and the Movies are backed up.

Later that day, Joe is using his computer and he notices that he can see some of the movies in the "Sally's Movies" folder, but some of the subfolders have a universal "No access" badge and he cannot view those folders' contents. This occurred for two reasons:

1. Sally mounted the network volume using Bob's credentials, so the files and folders created when she copied her files to the Backup volume are now owned by Bob's user account.
2. Some of the folders on Sally's computer prevented access by "other" users.

As a result, the folders on the Backup volume are owned by Bob and some of them limit access to other users (Joe in this case). Joe asks Sally about this and she decides to try copying some of the movies to one of Joe's folders on the backup volume. When she chooses Choose a folder... from CCC's Destination menu, however, she sees the same universal "No Access" badge on Joe's folder. Sally can't copy files to this folder (nor can CCC) because the Backup volume was mounted using Bob's credentials, and Joe's backup folder on the backup volume happened to be inaccessible to Bob. Sally unmounts the backup volume and reconnects to it using Joe's credentials, and she is then able to copy files to Joe's private folder.

What can I do when there are permissions or ownership issues that prevent CCC from copying items to/from or updating items on a network volume?

First, it is important to keep in mind that no application can modify the ownership of a file or folder on a network share. Ownership changes must be applied on the computer or device that is hosting the network volume. Additionally, permissions changes can only be made to files and folders owned by the user whose credentials were used to mount the network volume. For this reason, it is generally easier to apply both ownership and permissions changes on the computer or device hosting the network volume.

If the computer hosting the network volume is a Mac, you can modify ownership and permissions in the Get Info panel for that folder (on the Mac hosting the network volume):

1. In the Finder, click on the folder whose permissions or ownership you would like to change.
2. Choose Get Info from the File menu.
3. In the Sharing & Permissions section at the bottom, click on the lock icon to make the permissions editable.
4. To change permissions, choose Read & Write from the popup menu next to the owner of the file or folder.
5. If the owner of the item is not the user account that you use to connect to this Macintosh, click on the + button
6. In the window that appears, select the user account that you use to connect to this Macintosh, then click the Select button.
7. Set the access privileges to Read & Write.

8. Click on the Gear menu and choose to apply the change to enclosed items.
9. Try your backup task again.

If the computer or device that is hosting the network volume is not a Macintosh, consult that device's documentation to learn how to change permissions and ownership of files and folders.

Alternative #1: If you have mounted the network volume with Guest privileges, unmount and remount the network volume using the credentials of an account on the machine or device hosting the network volume.

Alternative #2: You can create a new folder on the shared volume and specify that folder as the destination in CCC by choosing Choose a folder... from the Destination selector.

Alternative #3: You can have CCC [create a disk image <http://bombich.com/kb/ccc5/i-want-back-up-my-whole-mac-time-capsule-nas-or-other-network-volume>](http://bombich.com/kb/ccc5/i-want-back-up-my-whole-mac-time-capsule-nas-or-other-network-volume) on the network volume rather than copying files directly to a folder. When CCC creates a disk image on the destination, the disk image is formatted to match the source and attached locally, so CCC can preserve the permissions and ownership of the files that you are copying to it.

Limitations of non-macOS-formatted filesystems

When you choose a non-macOS-formatted volume as a destination, CCC's Cloning Coach will proactively warn you of any [compatibility issues <http://bombich.com/kb/ccc5/cloning-coach-configuration-concerns#metadatapreservation>](http://bombich.com/kb/ccc5/cloning-coach-configuration-concerns#metadatapreservation) between the source and destination volumes. You can view the Cloning Coach's warnings by clicking on the yellow caution button in the Task Plan header. If you have selected a source and destination volume, and the caution button is not present, then there are no configuration concerns.

Support for third-party filesystems

CCC offers limited support for third-party filesystems, such as those provided by [FUSE for OS X <https://osxfuse.github.io>](https://osxfuse.github.io). Due to the large number of filesystems that can be provided by FUSE, CCC provides generic support for these "userland" filesystems rather than specific support. CCC takes a best effort approach by determining the capabilities of the source and destination filesystems, warns of potential incompatibilities, then presents only unexpected error conditions that arise during a backup.

Backing up to FUSE volumes mounted without the `allowroot` flag is not currently supported (e.g. Google Drive, BitCasa). Please contact the vendor of your proprietary filesystem to ask that they offer the ability to mount the volume with the `allowroot` flag if you would like to use that volume as a source or destination to a CCC backup task.

Support for Google Drive is "best effort". We've seen odd behavior when selecting Google Drive File Stream volumes as a whole as the source or destination for a task – CCC is unable to read the root folder during a backup task. CCC explicitly disallows that configuration. Selecting a subfolder on the Google Drive volume often works, and CCC will not disallow that configuration, however we frequently receive reports of inconsistent results when backing up to Google Drive, so we cannot offer support for this configuration.

There is one other notable concern with Google Drive File Stream – Google Drive will download files when they are accessed if they do not currently reside on your Mac's hard drive. If you specify a Google Drive folder as the source to a backup task, you should anticipate that cloud-only files may be downloaded to your Mac during the backup task. That behavior lies outside of CCC's purview, it cannot be modified with a CCC task setting.

The Western Digital MyCloud Home NAS device is another special case. The "Home" model of this NAS device requires the use of WD-proprietary software to access the storage securely; direct access to the storage via SMB is only available with Guest privileges. [Users report <https://community.wd.com/t/use-my-cloud-home-with-finder-without-wds-app/216769/4>](https://community.wd.com/t/use-my-cloud-home-with-finder-without-wds-app/216769/4) that performance of the storage while using WD's software is subpar in comparison to Guest access via SMB, and other users have reported to us that macOS is unable to create or mount disk images

on the storage when mounted via Western Digital's software. When you mount WD MyCloud Home NAS storage using WD's software, the volume is vended by a 'kddfuse' filesystem. CCC won't allow these volumes as a source or destination device. To back up to a WD MyCloud Home NAS, [mount the storage via SMB in the Finder instead <https://support.wdc.com/knowledgebase/answer.aspx?ID=2686>](https://support.wdc.com/knowledgebase/answer.aspx?ID=2686). Be sure to choose the "Guest" user option when prompted to authenticate, because the MyCloud Home device doesn't support authenticated access via SMB.

Writable NTFS filesystems

We have seen several reports of problems copying large amounts of data (e.g. > 4GB) to writable NTFS filesystems. In most cases, the underlying software that vends the filesystem (e.g. Tuxera, Paragon, and others) crashes and the volume is rendered "mute". While it may be possible to complete a backup to these filesystems in chunks (e.g. 4GB at a time), we recommend using a more reliable, writable filesystem if you encounter these problems.

Related Documentation

- [Learn more about formatting volumes on macOS <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x)

Backing up a Boot Camp installation of Windows

CCC can back up the user data on a Boot Camp volume, but it cannot make an installation of Windows bootable. If your goal is to back up your user data on the Boot Camp volume, CCC will meet your needs. If you're looking to migrate your Boot Camp volume to a new hard drive, you might consider an alternative solution such as WinClone, or one of the commercial virtualization solutions that offer a migration strategy from Boot Camp.

Backing up the contents of an NTFS volume

The NTFS filesystem supports "named streams", a feature that is comparable to extended attributes on macOS-formatted volumes and many other filesystems. Unlike extended attributes, however, there is no limit to the amount of data that can be stuffed into NTFS named streams (aside from standard file size limitations). Extended attributes on macOS have a 128KB size limit. As a result, any attempts to copy a named stream larger than 128KB to a non-NTFS filesystem will fail. CCC will copy the standard file data just fine, but will not copy named streams larger than 128KB. CCC's Cloning Coach will warn of this kind of incompatibility, and any errors related to this limitation will be logged to the CCC log file, however these errors will not be raised to your attention.

This limitation applies when copying files between volumes on Windows as well, so application developers tend to use named streams only for data that can be regenerated (e.g. thumbnail icons, summary or statistical information), not for storage of irreplaceable user data.

NAS service failures can lead to unreliable backups

Access to the contents of a network volume is provided by an application that runs on another computer or Network Attached Storage (NAS) device. Every NAS device and operating system has its own vendor-specific version of the file sharing application, so we occasionally see problems with some NAS devices that don't occur on others. Problems can be minor, such as being unable to set file flags (e.g. hidden, locked) on an item, or more significant, like not being able to store or retrieve resource forks. When these problems are encountered during a backup task, CCC will copy as many files and as much data as possible, then offer a report on the items or attributes that could not be copied.

When you encounter an error caused by the file sharing service that hosts your network volume, there are a few workarounds that you can try to avoid the errors:

- Eject the network volume on your Mac, then restart the computer or NAS device that is hosting the network volume. Reconnect to the network volume and try the backup task again.
- Connect to the network volume using a different protocol. A different application is responsible for each protocol, so if the AFP service on your server has a bug, connecting to the SMB service may work more reliably (and vice versa). Choose Connect to server from the Finder's Go menu, then specify "smb://servername.local/volume" or "afp://servername.local/volume" to connect to the server using a different protocol. If you are unsure which protocol you are currently using, click on the mounted volume in the Finder, then choose Get Info from the Finder's File menu to find out.
- If the errors persist when connecting to the network volume via both AFP and SMB, and restarting the file server does not change the outcome, then we recommend that you back up to locally-attached storage instead.

Some NAS services cope poorly with files and folders with special characters

Some NAS file sharing services will automatically rename files to "DOS compatible" names, or simply issue errors when working with various file names. In particular, files or folders that start or end with a space character, or names that contain a colon character (":") are unacceptable. When the file sharing service encounters files or folders with these disallowed characters, it will automatically rename these items, e.g. " filename.txt" would become "_1CZVGB". This "mangling" of file and folder names inevitably leads to errors during a backup task. To avoid these errors, you should either rename the offending files on the source, or connect to the NAS device using AFP rather than SMB (if applicable). Choose Connect to server from the Finder's Go menu, then specify "afp://servername.local/volume" to connect to the server using a different protocol.

Possible workaround: If you can modify the configuration of the SMB file sharing service on your NAS, then you may be able to prevent the service from "mangling" these file names. The applicable setting is [documented here <https://www.samba.org/samba/samba/docs/man/manpages/smb.conf.5.html#idp60809664>](https://www.samba.org/samba/samba/docs/man/manpages/smb.conf.5.html#idp60809664).

Another common issue that people encounter when copying files to a NAS volume is errors that are the result of a name restriction. For example, [Synology NAS devices \(and many others\) disallow file names <https://community.synology.com/enu/forum/1/post/133965>](https://community.synology.com/enu/forum/1/post/133965) that start with .lock, CON, PRN, AUX, NUL, COM0 - COM9, LPT0 - LPT9, _vti_ desktop.ini, any filename starting with \$. These NAS devices often produce bogus error codes in these cases, e.g. "File name too long". Some NAS devices have specific character restrictions as well, e.g. NAS devices that follow the [Microsoft OneDrive naming conventions <https://support.microsoft.com/en-us/office/invalid-file-names-and-file-types-in-onedrive-and-sharepoint-64883a5d-228e-48f5-b3d2-eb39e07630fa>](https://support.microsoft.com/en-us/office/invalid-file-names-and-file-types-in-onedrive-and-sharepoint-64883a5d-228e-48f5-b3d2-eb39e07630fa), which exclude " * : < > ? / |", and leading and trailing spaces in file or folder names also aren't allowed.

A closer look at how CCC determines the "bootability" of a destination volume

CCC determines whether your destination volume will be bootable and indicates any configuration concerns in the "Cloning Coach" window. If you see a yellow warning icon in the Task Plan header, you can click on that icon to see these concerns. CCC will also present these concerns to you the first time that you configure a backup task to any particular destination volume.

If CCC doesn't raise any configuration concerns, and the destination volume has an OS on it when the backup task is completed, and barring any hardware problems that might interfere, your backup volume should be bootable.

Configuration concerns that affect the bootability of the destination volume

CCC looks for the following configurations to determine if a destination volume will not be bootable:

- The destination volume cannot be a disk image — you cannot boot your Macintosh from a disk image.
- The files and folders required by macOS must be present on the source volume. These include: /Library, /System, /bin, /etc, /machkernel, /private, /sbin, /tmp, /usr, and /var.
- The files and folders that are required by macOS must not be excluded from the backup (applicable only if you have chosen to back up Some files).
- The hard drive on which the destination volume resides must be partitioned using the GUID Partition Table partitioning scheme.

Related documentation:

- [What makes a volume bootable? <http://bombich.com/kb/ccc5/what-makes-volume-bootable>](http://bombich.com/kb/ccc5/what-makes-volume-bootable)
- [Don't install older versions of macOS <http://bombich.com/kb/ccc5/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dontinstallolderosversions>](http://bombich.com/kb/ccc5/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dontinstallolderosversions)

"Some file metadata cannot be preserved"

CCC will note a concern if there is a compatibility mismatch between the source and destination filesystems. For example, if you are backing up files from an HFS+ volume to a network filesystem, some of the filesystem metadata cannot be preserved. In many cases this is acceptable and you can ignore the message. The types of metadata that can't be preserved in these cases are described in more detail below.

Access Control Lists

[Access Control Lists <https://en.wikipedia.org/wiki/Access_control_list>](https://en.wikipedia.org/wiki/Access_control_list) specify a granular list of the privileges that users and groups have for a particular file or folder (e.g., read, write, get information, delete, etc.). These advanced privilege settings generally apply only to user accounts that have been created on your Macintosh — for example, to prevent other users from deleting items from your home directory. If you are backing up your own files to a locally-attached hard drive, or to a network file share on a trusted computer, the Access Control List filesystem metadata is relatively unimportant. If you are backing up to or from a network filesystem in a business or education setting, however, check with your tech support staff for additional advice on whether this metadata must be preserved.

Hard links

A [hard link <https://en.wikipedia.org/wiki/Hard_link>](https://en.wikipedia.org/wiki/Hard_link) makes a single file appear to be located in multiple places on

your hard drive. If a single file had 20 hard links scattered across the disk, each hard link file would consume no additional space on the hard drive, and editing the content of any one of those files would immediately affect the content of every other hard link to that file.

When you back up the contents of a volume that contains hard links, ideally you want to preserve the hard links. If the destination filesystem doesn't support hard links, each hard linked file will be disassociated from the original file and will become a copy on the destination. This won't result in any loss of data, but your backup set will consume more space on the destination than on the source. Hard links are leveraged quite a bit on macOS by the operating system, though they are generally less common among user data.

Ownership

File ownership indicates which user account on your Mac has control of a file. The owner of a file can limit access to that file from other users on the same computer. If the destination doesn't support ownership, then the owner of each file copied to the destination will be set to the user that mounted the destination. If the destination volume is accessed elsewhere (e.g. mounted on another Mac or even by a different user on the same Mac), then any restrictions that you have placed on those files may not be honored. If you are backing up files and folders that are not all owned by the same user (e.g. you), you should consider backing up to a local, HFS+ formatted volume or to a disk image instead.

Some filesystems have file size limitations

Some filesystems have restrictions on how large a file can be. FAT32, for example, limits files to 4GB or less. CCC will proactively warn you of this limitation if you choose to back up a volume whose filesystem supports files larger than 4GB to a filesystem that does not support files larger than 4GB. CCC will then automatically exclude files larger than 4GB from the backup task. Files that were excluded will be reported at the end of the backup task.

If you require that files larger than 4GB are backed up, you must reformat the destination volume with a format that supports larger files.

Related documentation:

- [Preparing your backup disk for a backup of macOS <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x)

The destination already has an installation of macOS. Merging a different version of macOS into this destination may cause problems with that installation of macOS

This message appears if you choose the Don't delete anything SafetyNet setting. While that setting will protect any data that you have on the destination volume that is unique to that volume, it does a disservice to the installation of macOS on your destination. This message will also appear if you use the Don't update newer files on the destination advanced troubleshooting setting.

Suppose, for example, that you have a complete backup of Mac OS 10.12.4 on your backup volume. When you apply the 10.12.5 update to your source volume, many system files are updated, some new files are added, and some files may be deleted. If you use CCC to update your backup volume, but you don't allow CCC to delete the items on the destination that the OS update had deleted from the source, then there will be a bunch of "cruft" left over on the backup volume. If you should ever need to boot your Mac from your backup volume, these cruft files could cause the OS to behave unexpectedly, and they may prevent it from booting altogether.

CCC can help you perform a clean upgrade or downgrade of macOS on the destination volume by moving items that should be deleted to the SafetyNet folder. Any files and folders that you keep only on the destination would

also be moved to the SafetyNet folder. See the [Protecting data that is already on your destination volume](http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet) <<http://bombich.com/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>> section of the documentation for more details on these settings.

Some Macs may not boot from USB devices larger than 2TB

In the past we received several reports of bootability problems related to USB devices larger than 2TB. At that time, we performed a simple litmus test: create an "x"TB partition at the beginning of the disk (varying x from 0.5 to 2.5TB) and a second partition consuming the remainder of the disk, then install macOS onto both partitions. The results of those tests suggested that some Macs couldn't "see" the partition that lied past the 2TB mark on the disk. This limitation was specific to USB devices — none of these problems occurred if you were to place the same disk into a Thunderbolt enclosure.

At the time of those initial reports and testing, the results were consistent. We concluded that there was likely a 32-bit addressing limitation imposed by the USB drivers that are embedded in the Macs' firmware ("likely" — unfortunately none of this information is documented by Apple). More recently, however, we've been unable to consistently reproduce the same results. Apple may have addressed the problem with a firmware update. It's also possible that our initial conclusion was wrong, e.g. that the problem was due to a partition alignment error; an error specific to macOS El Capitan and apparently only USB devices (you'd see "disk2s2: alignment error" messages in the system log when the affected volume is mounted).

In any case, CCC's warning was issued out of an abundance of caution. Our current recommendation is to [partition the destination device using the same procedure as defined for all other destination devices](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x>>, and do the partitioning while booted from any other OS than El Capitan. In other words, don't proactively create a 2TB partition at the beginning of the disk. Once you have completed your first backup, though, we encourage you to [verify that your Mac will boot from the backup volume](http://bombich.com/kb/ccc5/how-verify-or-test-your-backup) <<http://bombich.com/kb/ccc5/how-verify-or-test-your-backup>>. If your Mac is unable to boot from the backup volume, [please reach out to us](http://bombich.com/hc/requests/new) <<http://bombich.com/hc/requests/new>> so we can investigate your specific configuration further.

Help! My clone won't boot!

See [this section of CCC's documentation](http://bombich.com/kb/ccc5/help-my-clone-wont-boot) <<http://bombich.com/kb/ccc5/help-my-clone-wont-boot>> for troubleshooting advice if you're having trouble getting your backup volume to start your Mac.

Cloning Coach Configuration Concerns

CCC determines whether your destination volume will be bootable and indicates any configuration concerns in the "Cloning Coach" window. If you see a yellow warning icon in the Task Plan header, you can click on that icon to see these concerns. CCC will also present these concerns to you the first time that you configure a backup task to any particular destination volume.

If CCC doesn't raise any configuration concerns, and the destination volume has an OS on it when the backup task is completed, and barring any hardware problems that might interfere, your backup volume should be bootable.

Configuration concerns that affect the bootability of the destination volume

CCC looks for the following configurations to determine if a destination volume will not be bootable:

- The destination volume cannot be a disk image — you cannot boot your Macintosh from a disk image.
- The files and folders required by macOS must be present on the source volume. These include: /Library, /System, /bin, /etc, /machkernel, /private, /sbin, /tmp, /usr, and /var.
- The files and folders that are required by macOS must not be excluded from the backup (applicable only if you have chosen to back up "Selected files").
- The hard drive on which the destination volume resides must be partitioned using the GUID Partition Table partitioning scheme.
- CCC will issue a warning if the operating system that you're backing up (or restoring) is older than the OS that your model of Mac shipped with.
- CCC will issue a warning if the destination volume is larger than 2TB and the device is connected to your Mac via USB.

CCC does not maintain an exhaustive list of hardware:shipping OS pairs. CCC also cannot determine whether the destination will be bootable when the source or destination are remote Macintosh volumes.

Related documentation:

- [What makes a volume bootable? <http://bombich.com/kb/ccc4/what-makes-volume-bootable>](http://bombich.com/kb/ccc4/what-makes-volume-bootable)
- [Don't install older versions of macOS <http://bombich.com/kb/ccc4/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dontinstallolderosversions>](http://bombich.com/kb/ccc4/i-want-clone-my-entire-hard-drive-new-hard-drive-or-new-machine#dontinstallolderosversions)

Configuration concerns that affect the preservation of filesystem metadata

CCC will note a concern if there is a compatibility mismatch between the source and destination filesystems. For example, if you are backing up files from an HFS+ volume to a network filesystem, some of the filesystem metadata cannot be preserved. In many cases this is acceptable and you can ignore the message. Each of the possible concerns that CCC might raise are listed below. The "risk" associated with not preserving each type of metadata is explained plainly, so you can decide whether the destination volume will suit your needs.

The destination doesn't support Access Control Lists

[Access Control Lists <https://en.wikipedia.org/wiki/Access_control_list>](https://en.wikipedia.org/wiki/Access_control_list) specify a granular list of the privileges that users and groups have for a particular file or folder (e.g., read, write, get information, delete, etc.). These advanced privilege settings generally apply only to user accounts that have been created on your Macintosh — for example, to prevent other users from deleting items from your home directory. If you are backing up your own files to a locally-attached hard drive, or to a network file share on a trusted computer, the Access Control List filesystem metadata is relatively unimportant. If you are backing up to or from a network filesystem in a business or education

setting, however, check with your tech support staff for additional advice on whether this metadata must be preserved.

The destination doesn't support hard links

A [hard link](https://en.wikipedia.org/wiki/Hardlinks) <<https://en.wikipedia.org/wiki/Hardlinks>> makes a single file appear to be located in multiple places on your hard drive. If a single file had 20 hard links scattered across the disk, each hard link file would consume no additional space on the hard drive, and editing the content of any one of those files would immediately affect the content of every other hard link to that file.

When you back up the contents of a volume that contains hard links, ideally you want to preserve the hard links. If the destination filesystem doesn't support hard links, each hard linked file will be disassociated from the original file and will become a copy on the destination. This won't result in any loss of data, but your backup set will consume more space on the destination than on the source. Hard links are leveraged quite a bit on macOS by the operating system, though they are generally less common among user data.

The destination doesn't support ownership

File ownership indicates which user account on your Mac has control of a file. The owner of a file can limit access to that file from other users on the same computer. If the destination doesn't support ownership, then the owner of each file copied to the destination will be set to the user that mounted the destination. If the destination volume is accessed elsewhere (e.g. mounted on another Mac or even by a different user on the same Mac), then any restrictions that you have placed on those files may not be honored. If you are backing up files and folders that are not all owned by the same user (e.g. you), you should consider backing up to a local, HFS+ formatted volume or to a disk image instead.

Some filesystems have file size limitations

Some filesystems have restrictions on how large a file can be. FAT32, for example, limits files to 4GB or less. CCC will proactively warn you of this limitation if you choose to back up a volume whose filesystem supports files larger than 4GB to a filesystem that does not support files larger than 4GB. CCC will then automatically exclude files larger than 4GB from the backup task. Files that were excluded will be reported at the end of the backup task.

If you require that files larger than 4GB are backed up, you must reformat the destination volume with a format that supports larger files.

Related documentation:

- [Preparing your backup disk for a backup of macOS](http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x>>

The destination already has an installation of macOS. Merging a different version of macOS into this destination may cause problems with that installation of macOS

This message appears if you choose the "Don't delete anything" SafetyNet setting. While that setting will protect any data that you have on the destination volume that is unique to that volume, it does a disservice to the installation of macOS on your destination. This message will also appear if you use the "Don't update newer files on the destination" advanced troubleshooting setting.

Suppose, for example, that you have a complete backup of Mac OS 10.9.3 on your backup volume. When you apply the 10.9.4 update to your source volume, many system files are updated, some new files are added, and some files may be deleted. If you use CCC to update your backup volume, but you don't allow CCC to delete the

items on the destination that the OS update had deleted from the source, then there will be a bunch of "cruft" left over on the backup volume. If you should ever need to boot your Mac from your backup volume, these cruft files could cause the OS to behave unexpectedly, and they may prevent it from booting altogether.

CCC can help you perform a clean upgrade or downgrade of macOS on the destination volume by moving items that should be deleted to the SafetyNet folder. Any files and folders that you keep only on the destination would also be moved to the SafetyNet folder. See the [Protecting data that is already on your destination volume <http://bombich.com/kb/ccc4/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>](http://bombich.com/kb/ccc4/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet) section of the documentation for more details on these settings.

CCC warns that Macs cannot boot from USB devices larger than 2TB

In the past we received several reports of bootability problems related to USB devices larger than 2TB. At that time, we performed a simple litmus test: create an "x"TB partition at the beginning of the disk (varying x from 0.5 to 2.5TB) and a second partition consuming the remainder of the disk, then install macOS onto both partitions. The results of those tests suggested that some Macs couldn't "see" the partition that lied past the 2TB mark on the disk. This limitation was specific to USB devices — none of these problems occurred if you were to place the same disk into a Thunderbolt enclosure.

At the time of those initial reports and testing, the results were consistent. We concluded that there was likely a 32-bit addressing limitation imposed by the USB drivers that are embedded in the Macs' firmware ("likely" — unfortunately none of this information is documented by Apple). More recently, however, we've been unable to consistently reproduce the same results. Apple may have addressed the problem with a firmware update. It's also possible that our initial conclusion was wrong, e.g. that the problem was due to a partition alignment error; an error specific to macOS El Capitan and apparently only USB devices (you'd see "disk2s2: alignment error" messages in the system log when the affected volume is mounted).

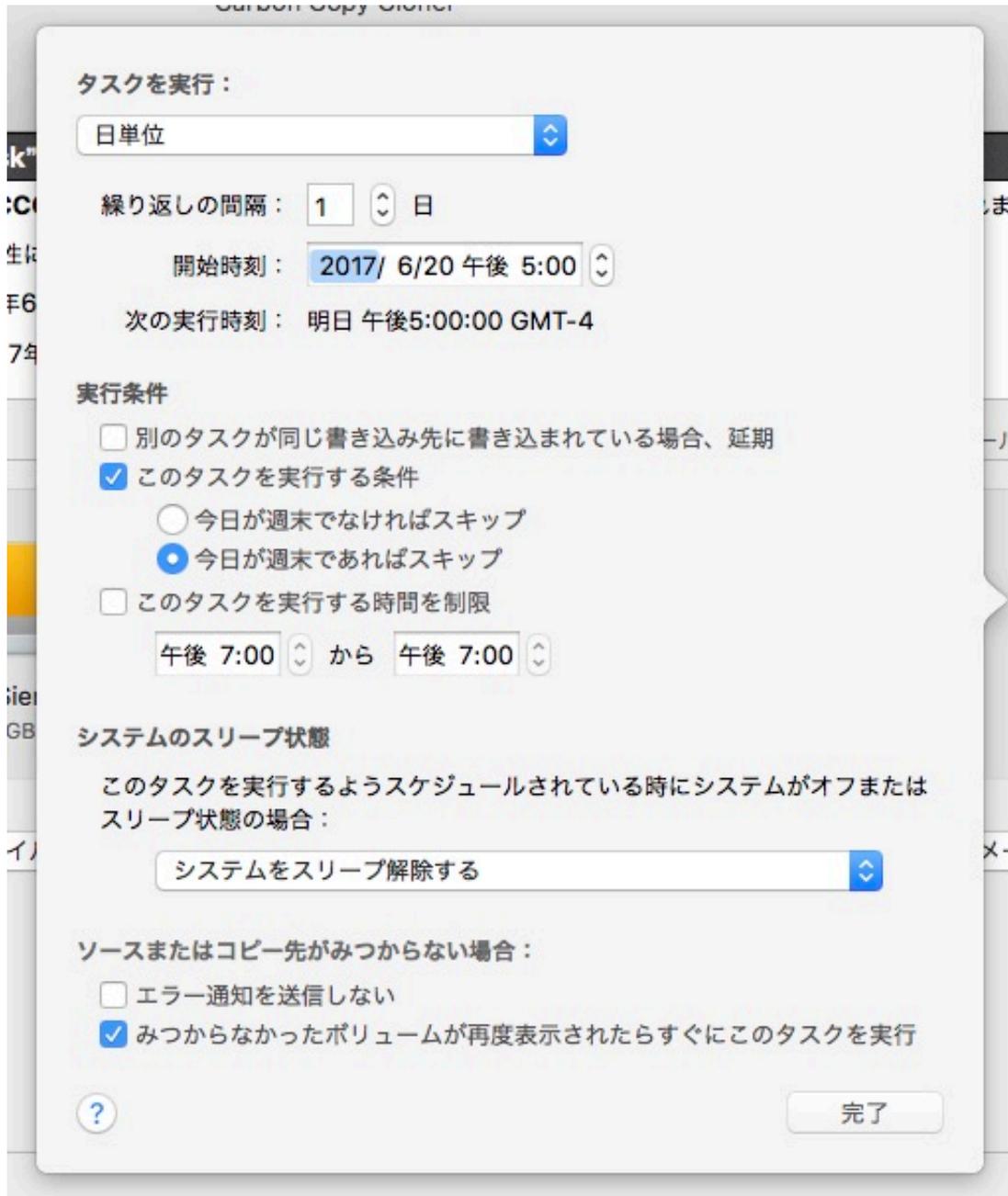
In any case, CCC's warning was issued out of an abundance of caution. Our current recommendation is to [partition the destination device using the same procedure as defined for all other destination devices <http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x>](http://bombich.com/kb/ccc4/preparing-your-backup-disk-backup-os-x), and do the partitioning while booted from any other OS than El Capitan. In other words, don't create a 2TB partition at the beginning of the disk. Once you have completed your first backup, though, we encourage you to [verify that your Mac will boot from the backup volume <http://bombich.com/kb/ccc4/how-verify-or-test-your-backup>](http://bombich.com/kb/ccc4/how-verify-or-test-your-backup). If your Mac is unable to boot from the backup volume, [please reach out to us <http://bombich.com/hc/requests/new>](http://bombich.com/hc/requests/new) so we can investigate your specific configuration further.

Help! My clone won't boot!

See [this section of CCC's documentation <http://bombich.com/kb/ccc4/help-my-clone-wont-boot>](http://bombich.com/kb/ccc4/help-my-clone-wont-boot) for troubleshooting advice if you're having trouble getting your backup volume to start your Mac.

スケジュールしたタスクの実行条件を設定するには

時間を基にしたスケジュールだけでは、タスクの実行方法を正確に指定するのに不十分なことがあります。CCCには、通常タスクの実行がスケジュールされている時、特定の条件下でタスクの実行を制限する**実行条件**を指定できる機能があります。



The screenshot shows the 'Task Execution' settings dialog in Carbon Copy Cloner. It includes sections for scheduling (frequency, start time, next run time), execution conditions (checkboxes for skipping on weekends or time restrictions), system sleep status, and source/volume availability. A 'Done' button is at the bottom right.

タスクを実行：

日単位

繰り返しの間隔： 1 日

開始時刻： 2017/ 6/20 午後 5:00

次の実行時刻： 明日 午後5:00:00 GMT-4

実行条件

- 別のタスクが同じ書き込み先に書き込まれている場合、延期
- このタスクを実行する条件
 - 今日が週末でなければスキップ
 - 今日が週末であればスキップ
- このタスクを実行する時間を制限

午後 7:00 から 午後 7:00

システムのスリープ状態

このタスクを実行しようスケジュールされている時にシステムがオフまたはスリープ状態の場合：

システムをスリープ解除する

ソースまたはコピー先が見つからない場合：

- エラー通知を送信しない
- みつからなかったボリュームが再度表示されたらすぐにこのタスクを実行

完了

別のタスクが同じ書き込み先に書き込まれている場合、延期

同一のコピー先ボリュームに書き込む予定でスケジュールされているタスクが複数ある場合、1度に1つのタスクだけがそのボリュームに書き込めるように、他のタスクを待機させるよう設定することができます。この設定を使

ってタスクを設定し、スケジュールした実行時間が経過した時、別のタスクが既に同じコピー先に書き込みを始めている場合、CCCはタスクをキューに追加し実行を延期させます。別の実行条件による妨害がない場合、最初のタスクが完了次第、CCCは延期されていたタスクを共有のコピー先ボリュームに書き込みます。

このタスクを実行する曜日を制限する

このオプションを使用すると、タスクを週末のみ、または週末以外にのみ実行するよう制限することができます。このオプションは“週ごと”および“月ごと”のスケジュール設定には適用できません。

このタスクを実行する条件

このオプションを使用すると、1日の特定の時間にタスクを実行するよう制限することができます。例えば、毎時に設定したタスクを午後実行したくない場合、開始の制限を6pmに、終了の制限を12pmに設定することができます。こう制限することで、タスクは午後6時以降のいつかに開始され、12pmまでには終了します。こうしてタスクが12pmから6pmまでの間は実行されないようにできます。タスクが既に実行中で (例えば、11:55AMに開始された場合)、終了の制限時刻になった時にまだタスクが実行中であれば、CCCはタスクを停止します。

注意：時間制限を設定する前にタスクの開始時刻を設定してください。 CCCは、タスクの現在の開始時刻を含まない時間指定を指定することはできません。

システムがスリープ状態の時の対処法

デフォルト設定では、スケジュールされたタスクの実行時に、CCCはコンピュータをスリープ解除します。この設定は、スケジュールポップオーバーの**実行条件** から変更できます。4つのオプションがあります：

システムをスリープ解除

CCCはスリープ解除イベントを設定してタスク実行の少し前にシステムのスリープを解除し、タスクをスケジュール通りに実行します。システムが切の場合、このスリープ解除イベントはシステムを入にはできません。

スリープ解除する、またはシステムの電源をオンにする

CCCは**スリープ解除する、またはシステムの電源をオンにする** イベントを設定して、タスクの実行の少し前にシステムのスリープを解除または電源をオンにして、タスクをスケジュール通りに実行します。

次回システムがスリープ解除されている時にこのタスクを実行

スケジュールされた実行時間が過ぎている場合、スリープ解除の通知と同時に、CCCはバックアップタスクを実行します。この場合、タスクはスケジュールされた正確な時刻に実行されませんが、2時間ごとに起きるmacOSのDark Wakeイベント (別名 PowerNap、または Maintenance Wake)の間、CCCはタスクを実行できます。夜間にディスプレイをオンにせずにバックアップタスクを実行させたい場合、このオプションは最適です。

このタスクをスキップ

スケジュールした実行時間にシステムがスリープしていない状態の場合にのみ、CCCはタスクを実行します。スリープ解除した時点で、スケジュールした実行時間が過ぎている場合、CCCはバックアップタスクを実行しません。

エラー通知を送信しない

タスクを実行するようにスケジュールされている時、ソースまたはコピー先のボリュームが利用できない場合、C

CCはエラーを通知するようデフォルト設定されています。このオプションを有効にすると、CCCはこのエラー通知を抑制します。さらに、エラーが起きた時にメールを送信するようにタスクを設定している場合でも、このオプションを有効にするとメール通知が抑制されます。

このオプションは、**ソースまたはコピー先が再接続される時**

のスケジュール設定には適用できません。というのは、その方法で設定されたタスクはソースとコピー先の両方が存在する場合にのみ実行を試みるからです。

みつからなかったボリュームが再表示されるとすぐにこのタスクを実行

スケジュールされた時刻にソースまたはコピー先が見つからないためにバックアップタスクが実行されなかった場合、このオプションを使用することで、みつからなかったボリュームが見つかるとうちに、CCCにバックアップタスクを実行させることができます。

関連ドキュメント

- [スケジュールしたタスクに関するよくある質問 <http://bombich.com/ja/ja/kb/coc5/frequently-asked-questions-about-scheduled-tasks>](http://bombich.com/ja/ja/kb/coc5/frequently-asked-questions-about-scheduled-tasks)

Modifying CCC's Security Configuration

Rather than requiring you to enter admin credentials every time you want to run a task or make changes to a task, CCC only requires you to authenticate once when CCC is initially installed. While this configuration is easier to use, there are situations where this configuration is not appropriate. If you leave your system unattended with an admin user logged in, someone with physical access to your system can modify or run your CCC backup tasks. If you cannot rely upon the physical security of your Mac to prevent someone from using your Mac, you can use the information below to apply a stricter security policy to CCC.

Require administrator authorization to make changes to tasks and to run or stop tasks

CCC identifies a subset of activity that causes changes to CCC tasks and preferences or that require access to privileged data (e.g. CCC's private keychain). Performing these tasks requires that the user is authorized for the "com.bombich.ccc.helper" privilege. The default rules for this privilege require that the requesting user is either an admin user, or can provide administrator credentials. Once the authorization is obtained, the user is allowed to perform the privileged tasks without additional authorization until the login session ends.

You can modify these rules in several ways. Most commonly, you may want to require the logged-in user to explicitly provide admin credentials to gain this authorization (vs. having the privileged granted simply because the user is an administrator). Additionally, you may want this authorization to expire after a specific amount of time, e.g. 5 minutes (vs. "when the user logs out"). To apply these stricter rules, paste the following into the Terminal application:

```
security authorizationdb read com.bombich.ccc.helper > /tmp/ccc.plist
defaults delete /tmp/ccc "authenticate-user"
defaults write /tmp/ccc "authenticate-admin" -bool YES
defaults write /tmp/ccc timeout -int 300
defaults write /tmp/ccc shared -bool NO
plutil -convert xml1 /tmp/ccc.plist
security authorizationdb write com.bombich.ccc.helper < /tmp/ccc.plist
security authorize -ud com.bombich.ccc.helper
```

Immediately revoking authorization to modify CCC tasks

If you have decided to apply a liberal timeout value to the "com.bombich.ccc.helper" privilege, you may occasionally want to revoke that authorization immediately. To immediately revoke that authorization, paste the following line into the Terminal application:

```
security authorize -ud com.bombich.ccc.helper
```

Resetting CCC's authorization rules back to default values

To reset CCC's authorization rules back to the default values, paste the following into the Terminal application:

```
security authorizationdb remove com.bombich.ccc.helper
security authorize -ud com.bombich.ccc.helper
```

The next time you attempt to modify or run a CCC backup task, CCC will re-apply its default rule set in macOS's Authorization database.

Creating a separate task to prevent VM container versions from bloating the SafetyNet

If you frequently use virtual machine container files (e.g. with Parallels, VMWare, VirtualBox, etc.), you may find that CCC's SafetyNet folder tends to get very large, very quickly. Every time you open your virtual machine, the monolithic virtual machine container file is modified, and CCC will require that it gets backed up during the next backup task. If the SafetyNet is on, CCC will move the older version of the VM container file into the SafetyNet folder. If you run your backup tasks on a daily basis and use your virtual memory container file every day, these large VM container files will quickly consume all of the free space on your backup volume.

You can avoid archiving the older versions of these virtual machine container files by creating a separate backup task for the parent folder of the virtual machine container files. Here's how to set things up:

1. Create a new task and name it something like Everything except Parallels
2. Choose your startup disk from CCC's Source selector
3. Choose Some files... from the Clone popup menu (underneath the Source selector)
4. In the file list in the Task Filter window, navigate to the location where your Parallels VM is saved (e.g. Users > yourname > Documents > Parallels) and uncheck the box next to the folder that contains your virtual machine container. You could exclude the container file itself, but choosing the parent folder gives you more flexibility in renaming the VM container, should you want to (e.g. Windows XP > Windows 7).
5. Choose your backup volume from the Destination selector
6. SafetyNet should be ON
7. Configure the task to run Daily and Save the changes
8. Create a new task and name it something like Parallels Backup
9. Choose Choose a folder... from the Source selector and select your Parallels folder as the source (e.g. the same folder that you excluded previously). By selecting this folder directly, you're explicitly limiting this task's scope to this folder.
10. Choose Choose a folder... from the Destination selector and select the Parallels folder on your backup volume as the destination
11. Turn SafetyNet OFF for this task
12. Schedule this task, then save the changes

Additionally, you can configure the first task to run that second task as a postflight action in Advanced Settings.

Outgoing network connections made by CCC

If you're using an application firewall such as [Little Snitch <https://www.obdev.at>](https://www.obdev.at), you will see several outgoing network connections coming from CCC. We explain below what connections you should expect to see, and also explain why some connections that look unexpected are simply misreported by Little Snitch.

Ordinary activity

CCC will make external network connections for the following activity:

- † When you launch CCC and it is a scheduled time to check for a software update (bombich.com and mc.bombich.com)
- When you submit a ticket to our help desk (mew.bombich.com and carboncopycloner.zendesk.com)
- When you view the documentation (which takes you to our website, bombich.com)
- When you visit our store (which also takes you to our website, bombich.com and our sales vendor, sites.fastspring.com)
- If you have set up email notifications for completed tasks
- If your backup task specifies a network volume or remote Macintosh as the source or destination

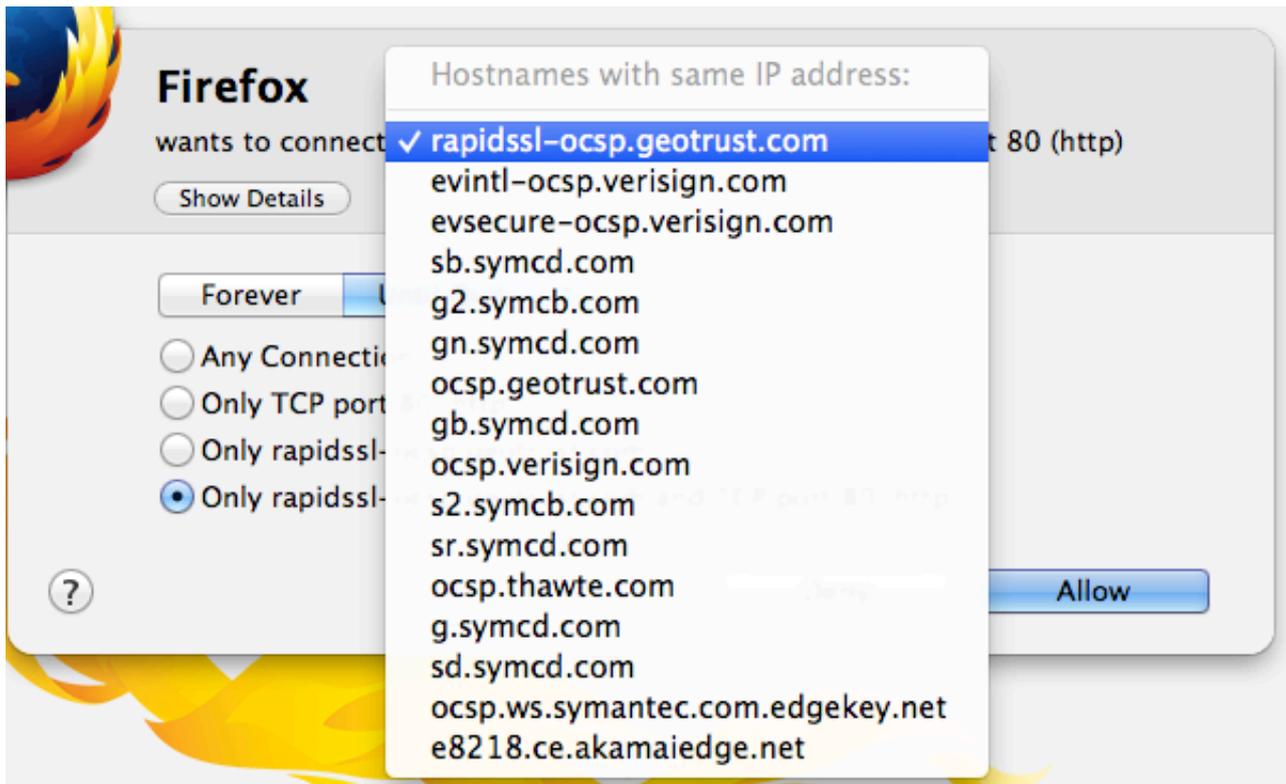
† These activities are enabled only upon your assent when you first launch CCC, and can be suppressed any time later via the Software Update section of CCC's Preferences window. No personal data, nor personally-identifiable data is ever sent to these services.

When you view the documentation via CCC, you connect to bombich.com just as you would in your web browser. Like most websites, bombich.com connects to other domains for certain purposes. We use [Content Delivery Networks \(CDNs\) <https://en.wikipedia.org/wiki/Contentdeliverynetwork>](https://en.wikipedia.org/wiki/Contentdeliverynetwork) to serve our static content, such as file downloads, images, styling, fonts, and so on. The CDNs we use are bootstrapCDN (which is hosted by maxCDN) for styling, jquery and fastly for scripts, Google for fonts, Rackspace (bombich.scdn1.secure.raxcdn.com, hosted by akamai) for files and images, and NewRelic for performance and uptime monitoring (nr-data.net, newrelic.com). CDNs not only provide powerful servers, they also have servers around the world and pick the one nearest to the user so that content can be delivered faster.

FastSpring is our e-commerce partner that handles everything to do with pricing and purchasing. If you go to our store, you are directed to their website. They use Cloudfront, Amazon's CDN service, to host some of their static content.

Why does Little Snitch indicate that CCC is connecting to google.com and other unrelated-seeming domains?

When CCC connects to any server, Little Snitch (or any monitor) sees the IP address only. It then makes a guess as to the domain name associated with that connection, which makes it much easier for the user to recognize. Because CDNs are used to serve files for hundreds of different websites and companies, everything is very interconnected, and sometimes an IP address has dozens of different domain names associated with it. You can actually see Little Snitch's other possible guesses by clicking the domain name in bold in the Little Snitch window:



It could pull any host name from the list, and we don't know what algorithm Little Snitch uses to decide which one to choose.

The result: google.ca, google.com, googleapis.com, and yting.com are all domains associated with Google's servers. We aren't actually connecting to all these domains, but when we connect to Google Web Fonts, for example, we're accessing some of the same servers.

You can view a [list of the CDNs that we use here](#)

<<http://www.cdnplanet.com/tools/cdnfinder/#site:http://bombich.com>> (and also look at any other websites you are curious about). This forum post at the ObDev website describes a similar report of the same problem (unrelated to CCC): [Little Snitch showing wrong host name for IP <https://forums.obdev.at/viewtopic.php?f=1&t=8859>](https://forums.obdev.at/viewtopic.php?f=1&t=8859).

When I boot from my backup, Little Snitch reports that its rules have been replaced by a different version. Why, and how can I avoid this?

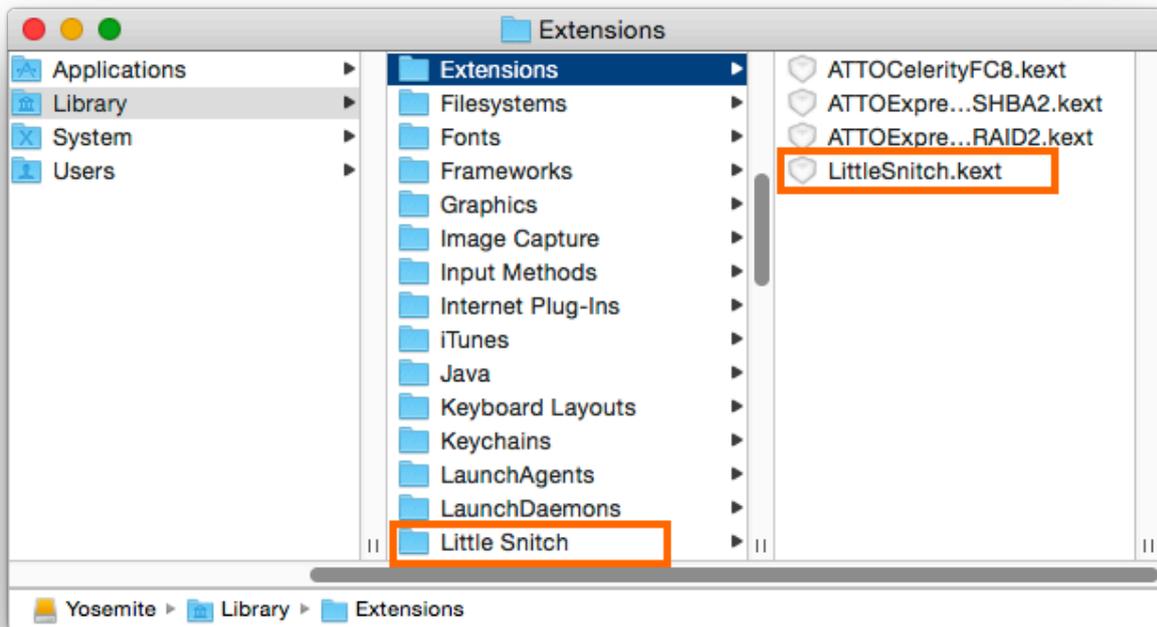
According to ObDev developers, it is crucial for Little Snitch to avoid unnoticed ruleset changes. Little Snitch therefore has numerous mechanisms to detect whether it is using the exact same ruleset file, as in, on the same volume and at the same physical address on that disk. This sort of mechanism makes it impossible for Little Snitch to use the ruleset on the booted backup volume without physical intervention from a user at the system (thus the dialog asking if it's OK to use the current version of rules or to use a default ruleset).

In cases where you have physical access to your computer while booting from the backup, the solution is straightforward — simply click the button to use the current rule set and everything behaves as normal.

In cases where you do not have physical access to the system, e.g. you have a server in a colocation facility, there is a logistical challenge. While Little Snitch is reporting that the ruleset doesn't match, it's also preventing network connectivity to and from the server. If you rely on VNC screen sharing to access the system, you will be unable to access the system to accept the current version of the Little Snitch ruleset.

According to ObDev developers, you can avoid this logistical lockout by removing the following two items from your backup volume before rebooting from it:

```
/Library/Extensions/LittleSnitch.kext  
/Library/Little Snitch
```



Once rebooted, reinstall Little Snitch to regain the application firewall and all is well.

While that method works fine for cases in which you plan to reboot from the backup volume, you're potentially in a lurch if you have an unplanned incident, e.g. the server's hard drive fails. To avoid encountering this problem altogether, you can [exclude those files from your backup task](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task) <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>>.

CCC does not delete files from the destination that are excluded from the backup task <<http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task#deleteexcluded>> , so be sure to remove those items from your destination if you have already established your backup.

Limitations of online-only placeholder files

Some cloud storage service providers offer services that allow you to sync a local folder to "the cloud", and optionally choose to store those files only online, thus freeing up space on your hard drive. Some services that currently offer this functionality include:

- Dropbox Professional's "Smart Sync" feature
- Microsoft OneDrive's "Free up space" feature
- iCloud Drive's "Optimize Mac Storage" feature
- Google's "Drive File Stream" feature

Files that are only available online will typically have a "cloud" icon or badge in the Finder, e.g. iCloud:  and

Dropbox: 

When you choose to have these services store your files only online, do so with the understanding that it's not possible to maintain a local backup of those files.

Online-only files can't be backed up

When you specify that a file stored by one of these storage services should reside only online, the local copy of your file is deleted from your Mac and replaced with a 0-byte placeholder file. If you attempt to open the placeholder file, the agent software for your storage service provider automatically downloads the data of the file to your Mac and the document opens. While this is a convenient feature that allows you to free up some space on your Mac, this feature removes files from your local storage, which means that CCC can't make a backup of these online-only files. Before using these online-only features, you should consider whether you are comfortable with not having a local backup of the files that you choose to store only in the cloud.

Placeholder files may be backed up, but may not function as placeholder files on the backup disk

As noted above, when you open a placeholder file in the Finder, the agent software downloads the original. Likewise, if you attempt to copy a placeholder file via the Finder from one volume to another, the agent software downloads the data to the source, then copies the original file (leaving the downloaded source file in place). CCC backups do not behave like Finder copies. And for good reason – if you have 1TB of online-only files on your 500GB SSD, you wouldn't want Dropbox or iCloud to download all of that data when CCC attempts to make a backup! Rather, CCC copies the placeholder files as they are, retaining all of the placeholder attributes of the source files. CCC makes a non-proprietary backup of your files; our goal is to make the destination files look exactly like the source files.

Some placeholder files won't function as placeholder files on the destination. OneDrive, for example, won't see a placeholder file that is outside of your OneDrive folder (i.e. on your startup disk) as a "true" placeholder file, and will not engage to download the file's data when you attempt to open it. CCC makes a best-effort attempt to not copy OneDrive placeholder files at all. Microsoft's OneDrive client software actively prevents applications from accessing those files — OneDrive placeholders are impossible to back up.

Dropbox's placeholder files function correctly when you back them up from an APFS volume to another APFS volume, and when you back them up from an HFS+ volume to another HFS+ volume. Because Dropbox uses a

different proprietary technique for creating the placeholder file on each volume format, though, these placeholder files won't behave correctly when transferred from one filesystem format to another.

Google Drive File Stream uses yet another proprietary device for its placeholder files. These placeholder files (which include all Google document formats) can't be opened by any application other than Google Drive, so CCC does not attempt to back them up.

OneDrive may delete online-only files from the cloud when you restore a OneDrive folder from a backup

Because Microsoft's OneDrive syncing software prevents applications from accessing the contents of OneDrive online-only placeholder files, those placeholder files cannot be present on a backup. If you restore a OneDrive folder from a backup, the OneDrive service should be smart enough to not delete files from the cloud simply because the placeholders are now absent. For comparison, Dropbox and iCloud won't delete files whose placeholders are absent, rather those services will only delete a file from the cloud when an actual file removal event occurs. In our own testing, OneDrive does not delete online-only files from the cloud when restoring from a backup. People have [reported this concern <https://answers.microsoft.com/en-us/msoffice/forum/msofficeonedrive-efb-msowin10-msoc365b/when-is-microsoft-going-to-fix-onedrive-when-a/45f8e646-7421-4249-9272-03e8f255c28f>](https://answers.microsoft.com/en-us/msoffice/forum/msofficeonedrive-efb-msowin10-msoc365b/when-is-microsoft-going-to-fix-onedrive-when-a/45f8e646-7421-4249-9272-03e8f255c28f) on Microsoft's forums [on Microsoft's forums <https://techcommunity.microsoft.com/t5/OneDrive-for-Business/Is-OneDrive-Deleting-Newer-Files-After-Backup-Restore/m-p/228811>](https://techcommunity.microsoft.com/t5/OneDrive-for-Business/Is-OneDrive-Deleting-Newer-Files-After-Backup-Restore/m-p/228811), and two CCC users have reported the same concern to us. If you restore from a backup and encounter this problem, you can restore the deleted files using [these instructions from Microsoft <https://support.office.com/en-us/article/restore-deleted-files-or-folders-in-onedrive-949ada80-0026-4db3-a953-c99083e6a84f>](https://support.office.com/en-us/article/restore-deleted-files-or-folders-in-onedrive-949ada80-0026-4db3-a953-c99083e6a84f).

If you're reading this because you encountered an error in your backup task indicating that CCC dropped a OneDrive placeholder file, take a moment to consider whether you should continue to include your OneDrive folder in your backups. On one hand, having a local backup of the OneDrive files that actually reside on your Mac is really nice to have. On the other hand, if you don't recall that placeholder files will be missing from your backup, then you may have some hassle in the future if/when you restore from that backup.

Related Documentation

- [Excluding files and folders from a backup task <http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task>](http://bombich.com/kb/ccc5/excluding-files-and-folders-from-backup-task)

What is CCC's Privileged Helper Tool?

At its core, Carbon Copy Cloner is a product that is designed to make bootable backups of your Mac's operating system. In order for CCC to be able to make copies of system files, CCC needs to have the privilege of copying files that can't be read nor written by just any user – CCC requires elevated privileges to copy macOS system files. Likewise, CCC is often tasked with copying the data associated with multiple users. macOS prevents you from accessing files that belong to other users. If you, as the administrator of the Mac, want CCC to back up everybody's files, then again, CCC requires elevated privileges.

Acquiring elevated privileges on macOS

There are a few different ways to perform a task on macOS with elevated privileges. The simplest – and least secure – method to do this would be to prompt the user to authenticate when he opens the application, and then relaunch the application as the "root" user. The application would then have all of the privileges it needs. This would grant [far too much privilege <https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/AccessControl.html#//appleref/doc/uid/TP40002589-SW6>](https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/AccessControl.html#//appleref/doc/uid/TP40002589-SW6), though, because it also gives the user (or malware that is exploiting the application) privileged access to other users' files.

A better way to securely acquire elevated privileges is to isolate the code that requires those privileges into a separate, "faceless" application. This is a common practice known as [privilege separation <https://en.wikipedia.org/wiki/Privilege_separation>](https://en.wikipedia.org/wiki/Privilege_separation). Even here, though, there is a right way and a wrong way for the isolated application to gain elevated privileges. The antiquated technique is for the parent application to ask for administrator authentication, then change the owner of the privileged application to the root user, then set a special mode on that application that allows that application to run with the privileges of the owner of the application (root). While this is a popular technique on Linux and much, much older versions of Mac OS X, there is still a significant potential vulnerability with this approach – any user can open that privileged application and potentially use it as a puppet to perform privileged tasks. [Apple specifically discourages this practice <https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/AccessControl.html#//appleref/doc/uid/TP40002589-SW18>](https://developer.apple.com/library/archive/documentation/Security/Conceptual/SecureCodingGuide/Articles/AccessControl.html#//appleref/doc/uid/TP40002589-SW18):

Note: Older software sometimes sets the setuid and setgid bits for the executable file, and sets the owner and group of the file to the privilege level it needs (often with the root user and the wheel group). Then when the user runs that tool, it runs with the elevated privileges of the tool's owner and group rather than with the privileges of the user who executed it. This technique is strongly discouraged because the user has the ability to manipulate the execution environment by creating additional file descriptors, changing environment variables, and so on, making it relatively difficult to do in a safe way.

Adhering to a higher standard of security

Starting in Mac OS X 10.6 (Snow Leopard), [Apple introduced a more secure paradigm for performing tasks with elevated privileges <https://developer.apple.com/documentation/servicemanagement/1431078-smjobbless?language=objc>](https://developer.apple.com/documentation/servicemanagement/1431078-smjobbless?language=objc). Rather than blindly granting privileged access to an application, developers can ask the system to install a "privileged helper tool". macOS then invokes the privileged helper tool on demand, and the calling application can only communicate with the helper when it has met stringent requirements:

- The calling application and the privileged helper tool must be code signed (and valid)
- The calling application must be one of the applications that is specifically approved to make requests to that specific helper
- The calling application must have a valid authorization reference

These requirements prevent unauthorized use of the helper tool and they prevent maliciously modified applications from making requests to the helper tool.

CCC has leveraged a privileged helper tool since version 3 and Mac OS X Snow Leopard – right from the start. This architecture is not only more secure and future-proof than using setuid binaries, it also affords us, for example, the ability to perform backup tasks when no users are logged in to the system.

Related Documentation

- [Modifying CCC's Security Configuration <http://bombich.com/kb/ccc5/modifying-cccs-security-configuration>](http://bombich.com/kb/ccc5/modifying-cccs-security-configuration)
- [Uninstalling CCC <http://bombich.com/kb/ccc5/uninstalling-ccc>](http://bombich.com/kb/ccc5/uninstalling-ccc)
- [Granting Full Disk Access to CCC and its helper tool <http://bombich.com/kb/ccc5/granting-full-disk-access-ccc-and-its-helper-tool>](http://bombich.com/kb/ccc5/granting-full-disk-access-ccc-and-its-helper-tool)
- [System problems can lead to a failure to install CCC's helper tool <http://bombich.com/kb/ccc5/carbon-copy-cloners-privileged-helper-tool>](http://bombich.com/kb/ccc5/carbon-copy-cloners-privileged-helper-tool)

Downgrading an APFS-formatted Fusion volume from Mojave

If you upgraded your Mac to macOS Mojave and have decided to downgrade for one reason or another, the procedure is [usually pretty straightforward](#). Fusion volumes, however, introduce a complication. Upon upgrading to Mojave, a Fusion volume will be converted from HFS+ to APFS. If you want to downgrade to High Sierra (or any earlier OS), you must reformat that Fusion volume as HFS+. Because APFS Fusion volumes are not handled gracefully by High Sierra, however, the procedure is a bit tedious. The following steps will help you downgrade your Mojave Fusion volume to High Sierra.

Warning: These instructions will permanently delete the contents of the two devices that belong to your Mac's internal Fusion device. If you're uncomfortable with any of the steps in this process, please don't hesitate to [ask us for help <http://bombich.com/software/gethelp>](http://bombich.com/software/gethelp) .

1. Boot from your CCC bootable backup that you intend to restore from (e.g. macOS High Sierra or earlier).
2. Choose "About this Mac" from the Apple menu to verify that your Mac is booted from your backup volume.
3. Open Disk Utility.
4. Choose "Show all devices" from the View menu.
5. Identify the two devices that belong to the APFS Fusion volume. Typically one will be an SSD and the other will be an HDD, and both should be in the "Internal Devices" section of Disk Utility's sidebar.
6. Erase the SSD Fusion member as "Mac OS Extended, Journaled". Name it "FusionSSD" so it's easy to identify later.
7. Erase the HDD Fusion member as "Mac OS Extended, Journaled". Name it "FusionHDD" so it's easy to identify later.
8. Quit out of Disk Utility.
9. Open Carbon Copy Cloner.
10. Click on the "FusionHDD" disk in CCC's sidebar.
11. Click the "Recovery HD..." button at the bottom of the window.
12. Click the "Create Recovery HD" button. If that button is disabled, don't worry – this step isn't essential.
13. Quit out of CCC
14. Open the Terminal application, type the following command, then press the Return key:
`diskutil list`
15. In the list of devices and volumes, find and make a note of the device identifier (in the IDENTIFIER column) associated with FusionSSD and FusionHDD. For FusionSSD, we will use the whole device identifier, e.g. disk1, whereas for the FusionHDD, we will use the volume device identifier, e.g. disk5s2.
16. Type the following command in the Terminal, substituting the device identifiers noted in the previous step, then press the Return key:
`diskutil cs create "Macintosh HD" SSDWholeDeviceIdentifier HDDvolumeidentifier`
17. The previous command will create an empty Fusion device, and print out a "Logical Volume Group" identifier. Select that identifier and copy it to the clipboard.
18. Type the following command in the Terminal, substituting the logical volume group identifier noted in the previous step, then press the Return key:
`diskutil cs createVolume LogicalVolumeGroup JHFS+ "Macintosh HD" 100%`
19. Quit out of the Terminal application.
20. Open Carbon Copy Cloner.
21. Create and run a new task, specifying your backup disk as the source and the new "Macintosh HD" Fusion volume as the destination.

22. When the restore task is complete, open the Startup Disk Preference Pane in the System Preferences application. Reset the startup disk to Macintosh HD, then reboot.

よくある質問

用語集

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

A

Apple File System (APFS) — APFSは、レガシーHFS+ファイルシステムの代替えとしてmacOS High Sierra以降Appleにより導入された新しいファイルシステムです。こちらも参照：[Carbon Copy ClonerとAPFSについて知っておくべきこと](#) <<http://bombich.com/ja/ja/kb/ccc5/everything-you-need-know-about-carbon-copy-cloner-and-apfs>>

Apple Filing Protocol (AFP) — AFPは、他のコンピュータ上およびネットワークのNASデバイスのファイルへのアクセスを許可するファイル共有のためのプロトコルです。CCCはファイルをフォルダに（または、フォルダから）コピーできます。また、SMBの共有ポイントとAFP共有ポイントにもコピーできます。OS X Yosemiteで開始されるSMBプロトコルを選ぶためAFPは非推奨です。

B

バックアップ (Backup) — [バックアップ](https://en.wikipedia.org/wiki/Backup) <<https://en.wikipedia.org/wiki/Backup>>、またはバックアップをするプロセス、はコンピュータのデータのコピーをしてアーカイブをすることを指します。データが喪失するようなイベントがあった後、オリジナルを復元するために使用されます。動詞はバックアップする。名詞はバックアップです。言い換えると、CCCを使ってデータをバックします。バックアップをすると、データのバックアップを物理的に異種なメディアに持つこととなります。

起動可能なバックアップ (Bootable backup) — バックアップと同じですが、主要な起動ボリュームに問題が起きた場合にコンピュータを起動するために使用できるオペレーティングシステムを含むボリュームのバックアップを指します。

起動セクタ (Boot selector) — [起動マネージャー](#)を参照。

C

チェックサム、または“壊れているファイルを見つけて置き換える” (Checksumming or "Find and replace corrupted items") — このオプションを使用すると、CCCはソースのすべてのファイルと、コピー先の呼応するすべてのファイルのMD5チェックサムを計算します。その後CCCはこれらのチェックサムを使用して、ファイルがコピーされるべきかどうかを決定します。このオプションを使用すると、バックアップにかかる時間が長くなりますが、ソースとコピー先のバックアップのセットの中の壊れているファイルを提示することができます。この方法は、コピー先ボリュームにコピーされているファイルがソースボリュームのファイルの内容と実際に一致しているかを検証する信頼できる手段です。

クローン (Clone) — フォルダまたはボリュームのコピー。非独占のバックアップ。完全に同一ではないものの（キャッシュの中には起動可能なバックアップに再構築される必要があるため、コピーされるべきではないものがあります。また、ゴミ箱のようなファイルは除外されます）、クローンはCCCの起動可能なバックアップに使用される一般的な用語です。

コンテナ (APFS) — APFSフォーマットされたドライブ上のコンテナは、パーティションに似ていますが、いくつかのボリュームにコンテナ内のスペースをより柔軟に共有させることができます。参照：[APFSボリュームグループを動作させるには](#) <<http://bombich.com/ja/kb/ccc5/working-apfs-volume-groups>>

クラフト (Cruft) : ゴミ — デジタルデトリタスの別名。例：必要がなくなった、またはユーザが望まないため削除できる (されるべき) ファイル。この表現は、1980年代と90年代にMIT (マサチューセッツ工科大学) のCruftラボ <<https://en.wikipedia.org/wiki/Cruft>>の廊下に大量に積み上げられていた要らなくなった技術装置に由来します。

D

コピー先 (Destination) — ソースからのファイルがコピーされる場所。コピー先として考えられるのは、Macに直接接続されたディスク、ネットワークの場所 (例：NAS、または他のコンピュータからの共有)、またはディスクイメージファイルなどです。コピー先は相対的な用語です。通常のバックアップを作成している時には、コピー先はバックアップボリュームです。しかし、復元している時には、コピー先はオリジナルのボリューム、または置き換えるためのデバイスになったりします。

差分バックアップ (Differential backup) — 差分バックアップとは、最新の完全バックアップ以降のデータの違のみを保存して、データを保持するデータバックアップの手法。CCCは差分バックアップの手法を使用しますが、独占的な方法での差分データは保存しません。むしろ、ファイルは“既に最新の日付”の項目の中のコピー先にコピーされますので、コピー先はソースのクローンになります。

ディスクイメージ (Disk image) — ディスクイメージはディスクをエミュレートするデータのコンテナです。ディスクイメージファイルを開くと、仮想ボリュームがマウントされ、まるで物理的なディスクデバイスがブラウズしているかのように、ディスクイメージに保持されているファイルをブラウズすることができます。ディスクイメージは、ネットワークボリュームによってサポートされない属性を保護するためにネットワークのコピー先へバックアップする場合のみ、推奨されます。

ディスクイメージは起動できません。ディスクイメージをバックアップするには

<<http://bombich.com/ja/ja/kb/ccc5/backing-up-disk-image>>

E

EFI パーティション — EFI パーティションはApple所有のパーティションです。このパーティションはディスクがGUIDパーティションスキームを用いてパーティションされた場合に自動的に作成されます。その内容はOS Xで内部的に管理されます。サードパーティのアプリケーションはそのボリュームの変更、またはコピーを試みるべきではありません。

拡張属性 (Extended Attribute) — ファイルに関連するその他のデータです。拡張属性には一般的にユーザによって作成されたものではないデータで、ファイルを作成したアプリケーションによって配置されたものが含まれています。例えば、写真アプリケーションがサムネイルアイコンのデータを拡張属性に配置することがあるかもしれません。CCCは可能であれば拡張属性のコピーを試みますが、拡張属性のデータは一般的に使い捨てと考えられます。というのは、それを作成し

たアプリケーションによって再度生成されるからです。高度な設定：拡張属性を保持しない

<<http://bombich.com/ja/ja/kb/ccc5/advanced-settings#ignorexattrs>>

F

ファイルシステム — ボリュームのファイルシステムは、そのボリュームのファイルとフォルダがどのように保管され、取り出されるか、また誰がそれらの項目にアクセスできるかをコントロールします。

FileVault 暗号化 — macOSに内蔵されたボリュームレベルの暗号化。ボリュームで有効にされると、そのボリュームをロック解除してマウントするのにパスワードが要求されます。所有者ベースの制限とは違って、FileVaultの保護はディスクを他のコンピュータに接続する際に継続されます。

Apple Kbase #HT204837:FileVaultを使って、Macの起動ディスクを暗号化 <<https://support.apple.com/en-us/HT204837>>

Firewire — Firewireは、外部周辺機器をコンピュータに接続するためのAppleによって開発されたインターフェースの標準です。Firewireを使ったデバイスは起動の可能性に信頼性があり、USB 3に対抗する優れたパフォーマンスを提供します。このインターフェースはその大部分を最近のMacでThunderboltによって取り代わられています

。
 Firmlink — AppleはFirmlinkを2つのファイルシステム間の“双方向ワームホール”と説明しています。Firmlinkは、ユーザに気づかれないでシステムボリュームの読み出し専用フォルダからデータボリュームの書き込み可能なフォルダにナビゲータをリダイレクトします。これらはエイリアスに似ていますが、フォルダにしか適用できない上、ユーザが作成することはできません。

H

HFS+、または“Mac OS拡張 (ジャーナリング)” — macOS

システムボリュームに使用されるデフォルトのファイルシステムフォーマット。Mac OS 8で最初に導入されたHFS+は、macOSの新機能をサポートするために何年もアップデートされてきました。AppleがmacOS High SierraでHFS+に代わるものとして導入したのが、[Apple File System](#)です。

I

増分バックアップ (Incremental backup) — 増分バックアップは、最後のバックアップ以降変更があったファイル、または新しいファイルのバックアップを提供します。最後のバックアップ以降変更が加えられたデータのみをバックアップします。最初にバックアップが作成される時には、増分バックアップはすべてのファイルをコピーします。

M

移行アシスタント (Migration Assistant) — バックアップまたは古いコンピュータからのアプリケーション、設定、および書類を新しいコンピュータまたはOSの新規インストールに移行するためのAppleのツールです。CCCの起動可能なバックアップを移行アシスタントのソースとして使用することができます。

[Apple Kbase #HT204350 : 新しいMacにコンテンツを移動する方法 <https://support.apple.com/en-us/HT204350>](#)

N

ネットワーク接続ストレージ (NAS) —

NASシステムは、1つ以上のハードドライブを含むネットワーク接続された機器 (例: ルータ、またはルータに接続する専用ストレージデバイス)。通常、SMBおよび/またはAFPネットワークプロトコルを使用して、共有ポイントをmacOS、Windows、およびLinux クライアントに利用できるようにします。

P

パーティション (Partition) — 動詞的として使われるとき、パーティションは1つ、または複数のボリュームを定義する、ハードドライブ上の分割を作成するプロセスを意味します。新しいハードドライブを購入した場合、使用しているMacintoshの使用に適切になるようにパーティションする必要が多々あります。名詞として使用される場合は、パーティションは一般的にボリュームと同じ意味合いで使用されます。パーティションテーブルはディスク上のボリュームサイズと位置を定義するディスクの隠れた構造を指します。CCCはパーティションテーブルおよびディスク上の複数のパーティションをコピーしません。その代わりに、CCCのバックアップタスクは1つのソースボリュームと1つのコピー先ボリュームで定義されます。OS

[Xのバックアップのためにバックアップディスクを準備するには <http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x>](http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x)

ブルーニング (Prune) —

コピー先ボリュームでキャッシュされた古い、アーカイブされた項目を削除します。 [CCC SafetyNet フォルダの自動管理 <http://bombich.com/ja/ja/kb/ccc5/automated-maintenance-ccc-safetynet-folder>](http://bombich.com/ja/ja/kb/ccc5/automated-maintenance-ccc-safetynet-folder)

アクセス権 (Permissions) — 項目の読み込みまたは変更に関して様々なユーザとグループが持つアクセスを定義するファイルとフォルダの仕様。

プリフライト/ポストフライトスクリプト (Preflight/Postflight script) — 高度な機能の1つで、タスクの機能を拡張するためにCCCの

バックアップタスクの最初または最後に追

加できるシェルスクリプト。バックアップタスクの前後にシェルスクリプトを実行するには

<http://bombich.com/ja/ja/kb/ccc5/performing-actions-before-and-after-backup-task#schedulersshellscripts>

R

RAID ("Redundant Array of Inexpensive Disks"、または"Redundant Array of Independent Disks"、"レイド") ソフトウェアまたはハードウェアの使用が1つ、または複数のボリュームとして表されるハードドライブを集めたもの。速度と冗長性のバランスを考慮したいいくつかのレベルのRAIDがあります。詳細は [このWikipedia記事](https://en.wikipedia.org/wiki/RAID) <https://en.wikipedia.org/wiki/RAID> を参照してください。

Recovery HD — macOSの起動ボリュームに関連する非表示のApple所有のボリューム。Recovery HDはmacOSを再インストールする方法を提供します。また、FileVault暗号化に関連する起動ボリュームで有効にする前に存在している必要があります。Recovery HDボリュームがなくても、起動ディスクの起動可能なバックアップの維持、および起動可能なバックアップからの復元に問題はありませぬ。AppleのRecovery HDパーティションをクローンするには <http://bombich.com/ja/ja/kb/ccc5/cloning-apples-recovery-hd-partition>

ルート (Root) — ルートフォルダ (別名ルートディレクトリ) は階層の最初または最上のフォルダです。Finderにあるハードドライブのアイコンをダブルタップして最初に表示されるフォルダが、ルートレベルのフォルダです。

S

SafetyNet — コピー先にあるファイルが間違えて削除されないように保護するCCCの機能。ソースに存在しないファイルがコピー先デバイスにある場合、これらのファイルはSafetyNetに保管されます。また、CCCは変更されたファイル

の古いバージョンもSa

fetyNetに保管します。SafetyNetは、コピー

先にしかないファイルの一時的な

安全な場所とすることができます。コピー先のスペースに制約を受けると、CCCはSafetyNetにある古い項目から削除を始めます。既にコピー先ボリュームにあるデータを保護するには: Carbon Copy Cloner

SafetyNet <http://bombich.com/ja/ja/kb/ccc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>

シード (Seed) — Macに直接接続されている間、コピー先ボリュームを最初に作成します。この"シードされた(種を植えられた)"ボリュームはその後、離れた場所のリモートMacintoshに接続することができます。そのため、その後続くバックアップはインターネット経由でコピーされるデータが少なくなるので、時間が短縮できます。

Server Message Block (SMB) — SMBは、他のコンピュータおよびネットワーク上のNASデバイスにあるファイルにアクセスできるファイル共有プロトコルです。CCCはファイルをフォルダに(または、フォルダから)コピーできます。また、SMBの共有ポイントとAFP共有ポイントにもコピーできます。

シェルスクリプト (Shell Script) — 面倒なタスクを自動化できるコマンドライン引数を含むテキストファイル。CCCのバックアップは、バックアップタスクの機能を拡張するためにプリフライトおよびポストフライトのシェルスクリプトを用いて設定できます。例えば、ポストフライトスクリプトを実行してソースボリュームをマウント解除することができます。バックアップタスクの前後にシェルスクリプトを実行するには <http://bombich.com/ja/ja/kb/ccc5/performing-actions-before-and-after-backup-task#schedulersshellscripts>

サイドバー (Sidebar) — CCCのツールバーにある**サイドバーを表示** ボタンをクリックするとCCCのメインウィンドウの左側に表示されるインターフェースの要素。CCCのサイドバーの上部にある表は、CCCのバックアップタスクをリスト表示します。一方、サイドバーの下にある表は現在Macにマウントされているローカルに接続されたボリュームの全リストが表示されています。サイドバーの内容はCCCの**表示** メニューからもアクセスできます。

シンプルモード (Simple Mode) — 単純化されたユーザインターフェース。シンプルモードを使用すると、ユーザ

インターフェイスの要素が軽減され、シンプルになります。サイドバー、ツールバー、スケジュールセレクト、高度な設定はすべて非表示になり、次の3つの主要なコントロールだけが表示されます：ソース、コピー先、クローンボタン。 [シンプルモード](http://bombich.com/ja/ja/kb/ccc5/simple-mode) <<http://bombich.com/ja/ja/kb/ccc5/simple-mode>>

スナップショット — スナップショットは時間の特定のポイントにおけるシステムの状態を記録したものです。写真に例えられます。スナップショットを使うことで、前の時点にシステムを復元できます。

ソース (Source) — CCCにコピーさせたいデータを保持しているフォルダまたはボリュームです。

スパン (Span) — バックアップがより多くの領域を求めてコピー先を超えること。CCCは複数のコピー先のスパンをサポートしません。

スパースファイル — スパースファイルはファイルサイズが示唆するよりも少ないスペースをディスクで消費します。スパースファイルはログファイル、データベース、および仮想マシンファイルに使用されることがあります。CCCはAPFSボリューム間でスパースファイルを保持することができますが、HFS+はスパースファイルをサポートしないので、これらのファイルはHFS+フォーマットされたバックアップディスクでより多くのスペースを消費します。

起動マネージャー (Startup Manager) — Macが起動中、起動ボリュームとして選択できるAppleのシステムツール。起動マネージャーはMacのファームウェアの一部で、Macを起動中にOptionキーを押したままにすると起動マネージャーを立ち上げることができます。

[Apple Kbase #HT204417:異なる起動ディスクを選択する方法](https://support.apple.com/en-us/HT204417) <<https://support.apple.com/en-us/HT204417>>

T

ターゲットディスクモード (Target Disk Mode) — コンピュータがログインウィンドウにもFinderにも起動しない代替の起動構成。むしろ、Firewire、USB、またはThunderboltのアイコンがMacの画面に表示されます。MacをFirewire、USB、またはThunderbolt経由で別のMacに接続すると、ターゲットディスクモード内のMacの内蔵ストレージがもう1台のMacのデスクトップに表示されます。言い換えると、ターゲットディスクモードによりMacが通常の外部ハードドライブエンクロージャのように動作します。

[Apple Kbase #HT201255:Macを起動するキーコンビネーション](https://support.apple.com/en-eg/HT201255) <<https://support.apple.com/en-eg/HT201255>>

タスク (Task) — CCCでソース、コピー先、コピーされる項目、および自動化を定義する設定の集合。

タスクの連鎖化 (Task chaining) —

タスクの最後に別のタスクを実行できるCCCの機能

。参照：[バックアップタスクの前後に別の操作を実行するには：別のバックアップタスクを実行 \(タスクの連鎖化\)](http://bombich.com/ja/ja/kb/ccc5/performing-actions-before-and-after-backup-task#chaintasks) <<http://bombich.com/ja/ja/kb/ccc5/performing-actions-before-and-after-backup-task#chaintasks>>。

Thunderbolt — Thunderboltは、Intelにより開発されたハードウェアインターフェースです。外部周辺機器をコンピュータに接続できます。Thunderboltは、比較的価格が高めであるにも拘らず、Macに外部ハードドライブを接続するための人気の高いインターフェースです。Thunderboltデバイスは優れたパフォーマンスと信頼できる起動の可能性を提供します。

U

Universally Unique Identifier (UUID) — 36文字の16進法コード (文字 A-F, 0-9) で、ボリュームを一意で識別します。例：“F5B1D7B0-66EC-4082-A34C-86FFD294FA61” ディスクユーティリティでボリュームを消去する時、新しいボリュームは新規の一意の識別子を与えられます。CCCはこの識別子をボリュームの名前と共に使用し、ファイルをコピーする前にソースとコピー先を確実に識別します。これらの識別子が一意であるということは、ボリュームを認識する際にボリューム名よりも信頼性が高いことを証明します。というのは、すべてのディスクに“Macintosh HD” という名前をつけても全く構わないからです。

ユニバーサルシリアルバス (USB) — ケーブル、コネクタ、およびコンピュータと外部デバイス (ハードドライブ、キーボード、マウスなど) 間の通信のための規格の1つ。MacとUSBデバイスは、デバイスの製造時期によって



、プロトコルのUSB 2またはUSB 3バージョンをサポートします。USB 3はUSB 2よりも大幅に高速です。2012年以前に製造されたMacはネイティブなUSB 3のサポートがありません。USB 3デバイスをそれらのMacで使用できますが、接続スピードはUSB 2のものと変わりません。

V

ボリューム (Volume) — “ディスク” と “ボリューム” はしばしば同じ意味で使用されます。しかし、複数のボリュームがあるディスクのパーティションを変更する時、曖昧さが生じます。“ディスク” という用語は、物理的なデバイス全体を指します。ボリュームを含んでいるのがディスクで、Finderに表示されるのがボリュームです (しばしばハードディスクアイコンで混乱がまたもと通りになりますが)。CCCのドキュメントのこのセクション <http://bombich.com/ja/ja/kb/ccc5/my-disk-already-formatted-hfs-why-am-i-getting-warning> から役立つ画像を参照できます。

コピー先のディスクの使用状況がソースと一致しません。CCCがコピーしていないファイルがありますか。

起動ディスクのディスク使用状況は、バックアップされる必要があるデータ量を反映しません。起動ディスクの初回バックアップの後、コピー先のディスク使用状況は、ソースのディスク使用状況よりも少ないはずですが、特別なファイルシステムデバイス(例: ファイルシステムスナップショット)といくつかのmacOSサービスデータは、別のボリュームにコピーできないか、またはするべきではありません。CCCはバックアップからの起動中問題を回避するために、そして不要なディスクの使用を避けるために、これらの項目を自動的に除外します。除外リストは以下の通りです: [ファイルやフォルダの中には自動的にバックアップタスクから除外されているものもあります](http://bombich.com/ja/ja/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task)
<<http://bombich.com/ja/ja/kb/ccc5/some-files-and-folders-are-automatically-excluded-from-backup-task>>。

CCCは仮想メモリ、ゴミ箱、およびスナップショットはコピーしません。

最大で最も顕著な除外項目は、/private/var/vm/sleepimageファイルです。sleepimageファイルはMacのRAMのライブラリの状態を含んでいますので、インストールしてあるRAMと同じ大きさです。このファイルは非常に大きく、頻繁に変わり、起動時に再作成される可能性があるため、CCCはこのファイルをすべてのバックアップタスクから除外します。

またCCCはゴミ箱の内容を除外しますので、ゴミ箱を空にしてからソースとコピー先を比較し直すと良いかもしれません。

最後に、ファイルシステムのスナップショットはソースボリュームで相当量のスペースを消費する可能性があります。CCCのサイドバーでソースボリュームを選択すると、スナップショットに関連するディスク使用量を表示できます。スナップショットは削除または変更されたファイルの参照を保持するもので、現在のデータセットを表すものではなく、また、あるボリュームから別のボリュームにコピーすることはできません。

ディスクの使用状況の計算は単純ではない

ディスクの使用状況はボリューム上のそれぞれのファイルサイズの合計という単純なものではありません。特別なファイルシステムデバイス(例: ハードリンク)は常にこの計算を複雑にしますが、最近Appleはこれをさらに複雑にする他の特別なファイルシステムデバイスを紹介しました。Appleの新しいAPFSファイルシステムのクローン機能は、ディスクの実際の許容量よりもさらに多くのデータがディスクにあるようなシナリオに導く可能性がある上、ファイルシステムのスナップショット機能は、ディスクの使用状況がそのボリューム上のファイルの合計サイズよりも多いというシナリオになる可能性があります。また、APFSは、ファイルサイズが示唆しているよりも少ないスペースをディスクで消費している“スパーズ(まばらな)”ファイルをサポートします。CCCはAPFSボリューム間でスパーズファイルを保持することができますが、HFS+はスパーズファイルをサポートしないので、これらのファイルはHFS+フォーマットされたバックアップディスクでより多くのスペースを消費します。これらのチャレンジに関するその他の詳細はCCCの以下のドキュメントをご覧ください:

- APFSには“クローン”機能があると聞きました。それはCCCがしていることと同じですか?
<<http://bombich.com/ja/ja/kb/ccc5/everything-you-need-know-about-carbon-copy-cloner-and-apfs#math>>
- Finderはファイルのディスク使用状況を正確に表していません <<https://youtu.be/Kggyul8mED0>>
- スナップショットを使用する際のディスクの使用状況を理解するには
<<https://www.youtube.com/watch?v=4wqAC4YXiaY>>

では、どうすれば自分のデータが実際にすべてコピーされているかどうかわかりますか。

APFSボリュームに関しては、ソースとコピー先で意味のある比較ができるような、正確なディスクの使用状況の値を得ることはおそらくありません。けれども、必ずソースとコピー先で同じ場所にあるファイルを見つけることはできるはずで、項目がコピー先がないということはないはずで、(もちろん、バックアップからそれを除外している場合は別です)。

[このビデオ](#)

<https://www.youtube.com/watch?v=n7JgLKyW0> は、ソースとコピー先のファイルと比較して、バックアップにファイルを見つけることができるかを検証するのに役立つでしょう。

HFS+フォーマットされたソースとコピー先ボリュームには、これらのボリュームのファイルとフォルダの基本的な列挙がされ、比較するための意味のある数値が表示されています。 [ボリュームディスクの使用状況の詳細](#) <http://bombich.com/ja/software/files/tools/VolumeDiskUsageDetails.zip> ツールはこの種の列挙を収集するのに役立ちます。このツールがソースとコピー先ボリュームのスキャンを完了すると、報告を比較し、矛盾を見つけることができます。特定のフォルダの矛盾についてより細かな詳細が必要な場合、このツールを使用して個々のフォルダを列挙することも可能です。

説明不可能な、または異常と思われるような矛盾を発見された場合、 [ご連絡ください](#)

<http://bombich.com/ja/software/gethelp> 真相解明のお手伝いをします。

I want to back up multiple Macs or source volumes to the same hard drive

Backing up multiple volumes or multiple Macs to a single hard drive can be a messy proposition. If you back up each source volume to the same destination volume without some pre-planning, data from each source volume will be merged in a heap on the backup volume. Additionally, your tasks will archive or delete each other's backed up content. Carbon Copy Cloner can solve this problem! We lay out a few different scenarios and solutions below.

"I want a bootable backup for each Mac on the same hard drive" (macOS High Sierra and later, APFS-formatted backup disk)

Each APFS volume that you add to your backup disk can hold a bootable backup of macOS High Sierra and later, or any other data that you would like to keep separate from other content on the backup disk.

It's really easy to create separate volumes in an APFS-formatted container. When you're backing up multiple volumes to the same backup disk, create a dedicated volume on that backup disk for each source volume:

1. Open Disk Utility
2. Choose "Show all devices" from the View menu
3. Select your current CCC destination volume in the sidebar
4. Choose Add APFS Volume... from the Edit menu
5. Name your new volume and click the Add button
6. Configure each of your CCC backup tasks to back up to its own dedicated volume on the destination

"I want to back up my startup disk and a data volume to the same backup disk" (macOS High Sierra and later, APFS-formatted backup disk)

Same as above — create a dedicated volume on your backup disk for each source that you're backing up:

1. Open Disk Utility
2. Choose "Show all devices" from the View menu
3. Select your current CCC destination volume in the sidebar
4. Choose Add APFS Volume... from the Edit menu
5. Name your new volume and click the Add button
6. Configure each of your CCC backup tasks to back up to its own dedicated volume on the destination

Related Documentation

- [Partitioning a new hard drive with APFS <https://youtu.be/narMTq3d58>](https://youtu.be/narMTq3d58)

"I want a bootable backup for each Mac on the same hard drive" (Sierra or older, HFS+ formatted backup disk)

Creating a bootable backup requires that you provide a dedicated backup volume for each Mac that you want to back up. If you want to maintain each bootable backup on the same hard drive, you simply create a partition for each computer that you want to back up using Disk Utility:

1. Open Disk Utility
2. Choose "Show all devices" from the View menu

3. Click on the top-most parent device of your backup disk
4. Click the "Partition" button in the toolbar
5. Click the "+" button to add a second partition to the backup disk
6. Configure each of your CCC backup tasks to back up to its own dedicated volume on the destination

Related Documentation

- [Learn more about partitioning a hard drive for use with Carbon Copy Cloner](http://bombich.com/kb/coc5/preparing-your-backup-disk-backup-os-x) <<http://bombich.com/kb/coc5/preparing-your-backup-disk-backup-os-x>>
- [Partitioning a new hard drive \[10.11 and 10.12\]](https://www.youtube.com/watch?v=3AUXkwaVVFQ) <<https://www.youtube.com/watch?v=3AUXkwaVVFQ>>
- [Partitioning a new hard drive \[10.10\]](https://www.youtube.com/watch?v=WZ1sstRdWjk) <<https://www.youtube.com/watch?v=WZ1sstRdWjk>>

"I want to back up my startup disk and a data volume to the same backup disk" (Sierra or older, HFS+ formatted backup disk)

Two CCC backup tasks will manage these backups. The first task will back up your startup disk directly to the backup volume for a bootable backup, the second task will back up your data volume to a subfolder on the backup volume. Thanks to [CCC's SafetyNet](http://bombich.com/kb/coc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet) <<http://bombich.com/kb/coc5/protecting-data-already-on-your-destination-volume-carbon-copy-cloner-safetynet>> feature, the two backup tasks will coexist peacefully.

1. Configure a CCC task to back up your startup disk to the backup volume. Choose your startup disk from the Source selector and choose the backup volume from the Destination selector.
2. Verify that the SafetyNet feature is On. [Note: If you have modified any Advanced Settings, be sure that the [Protect root-level items](http://bombich.com/kb/coc5/advanced-settings#protect) <<http://bombich.com/kb/coc5/advanced-settings#protect>> option is checked.]
3. Schedule the task, if desired, or choose "Save" from Carbon Copy Cloner's File menu. You can run this task immediately or let it run on schedule later.
4. Click the New Task button in CCC's toolbar.
5. Choose your data volume from CCC's Source selector.
6. In the Finder, create a new folder at the root level of the destination volume to store your data volume's backup. Finder may prompt you to authenticate if you ran the first task already, and that's OK.
7. Drag the new folder from the Finder onto CCC's Destination selector.
8. Schedule the task, if desired, or choose Save from Carbon Copy Cloner's File menu. Again, you can run this task immediately or let it run on schedule later.

CCC's SafetyNet will prevent the first task from erasing the content that you're backing up to a subfolder on that same destination volume.

"I want to back up multiple data volumes (no OS files) to the same backup disk"

The easiest way to back up multiple data-only volumes to the same backup disk is to create a folder on the backup disk for each volume you want to back up. Then you'll configure a task for each source volume that you want to back up, setting the destination to that disk's dedicated folder on the backup disk.

1. Click the New Task button in CCC's toolbar.
2. Choose your data volume from CCC's Source selector.
3. Choose Choose a folder... from the Destination selector
4. Select your destination volume in the sidebar
5. Click the New Folder button to create a new folder at the root level of the destination to store your data volume's backup, then select that folder as the destination.
6. Schedule the task, if desired, or choose Save from Carbon Copy Cloner's File menu. You can run this task immediately or let it run on schedule later.
7. Repeat the steps above for other source volumes, creating a new folder for each at the root level of the destination volume.

Can I run a backup while I'm using my computer? If I have open files, will they be backed up?

Generally, yes. Performance will be affected during the backup task (especially the first one) as CCC reads the entire source volume and writes to the destination volume. If your work is "disk bound" — that is your applications are reading or writing to either the source or destination, then you'll notice a performance hit. If you're just reading email or writing a document, then you probably won't notice the performance hit.

What happens if files are modified while they're being copied?

If your source volume is an APFS volume, then CCC will create a read-only snapshot of that volume and use that snapshot as a source for the backup task. With this configuration, any changes that you make to files on the source during the backup task will have no effect on the backup process. Likewise, those changes will not be part of the backup – expect the backup to contain exactly what was on the source at the moment that the backup task started.

If the source volume is not APFS-formatted, then some consideration should be given to the modification of files on the source during the backup task. Typically it's OK to work from the source volume while you're copying it, with the understanding that if CCC copied a file, then you open it, make changes, save it, then CCC completes the backup task, the modified version of your document is not backed up (this time around). Typically that's no big deal, the modifications will get backed up the next time the backup task runs. More importantly, though, if you're [working with large files](http://bombich.com/kb/coc5/backing-up-large-files-mounted-disk-images-and-virtual-machine-containers) (mounted disk image, Entourage email database, VMWare/Parallels container) during the backup operation, it is possible that those large files could be modified while CCC is backing up that file. This won't affect the source file, but there's a good chance that the backup version of that file will be corrupt. For this reason it is a good idea to stop using applications that may be modifying large files for the duration of the backup task. Again, keep in mind that this is only applicable for non-APFS source volumes.

Related Documentation

- [Backing up large files, mounted disk images, and Virtual Machine containers](http://bombich.com/kb/coc5/backing-up-large-files-mounted-disk-images-and-virtual-machine-containers)
- [Leveraging Snapshots on APFS Volumes](http://bombich.com/kb/coc5/leveraging-snapshots-on-apfs-volumes)

アプリケーションが異なる動作をしたり、クローンしたボリュームのシリアル番号を要求しません。CCCがなにか見つけられませんか。

アプリケーションの中には新しいディスクに転送されたり、別のMacで実行されると作動しないものがあります。これはCCCがデータをバックアップしているかどうかや、その方法とは全く関係がありません。それはソフトウェアの製造元が課しているシリアル番号の要求によるものです（著作権侵害対策など）。まったく問題なく動作するアプリケーションもあれば、シリアル番号の再入力を要求するアプリケーションもあります（Microsoft OfficeとAdobeアプリケーションはよくこのカテゴリに入ります）。また、アプリケーションによっては、オリジナルのインストールメディアからインストール必要のあるもの、または製造元のウェブサイト経由でオンラインアクティベーションして再インストールを要求するものもあります。

CCCは他のソフトウェア製造元が要求するアクティベーションを覆すことは法的にも技術的にも不可能です。

また、アプリケーションによっては、インストールプロセスの間、周辺機器の存在または欠落を他のハードウェアの特性と同じように判断することがあるのでご注意ください。アプリケーションをMacまたは新しいハードドライブで実行中にこの状況が異なる場合、問題に遭遇することがあります。この種の問題は過去にハイエンドなオーディオソフトウェア、特に様々なプラグインのインストールや設定で見られることがありました。

万が一アプリケーションがシリアル番号を再度要求したり、特定のインストール方法を要求する場合に備えて、アプリケーションのインストールディスクやシリアル番号のコピーを必ず保管しておかれることをお勧めします。

登録と無関係のアプリケーション固有の特徴

新規ボリュームでAppを実行中に起きるアプリケーションの登録の問題に加えて、クローンしたボリュームから起動する時に奇妙な特性に遭遇することがあります。以下にこれまで報告された考えられる予期しない動作のリストを表示します。それらは、

a)別のボリュームからまたは別のMacでアプリケーションを実行した結果と考えられるもの； b)バックアップ/クローンの過程で解決/対応しなかった、あるいはできなかったものです：

- Dropboxがアカウント設定を再設定するよう要求する
- GateKeeperは、前にソースで検証された非認証のアプリケーションを再検証する可能性があります（例：“iMovie.appを検証中”というダイアログがその項目を開く際に表示されるかもしれません）。
- “システムイベント”アプリケーションを特定するよう要求するダイアログが表示される（この表示は1度だけ表示され、ダイアログを閉じると2度と表示されません）。ログイン時に読み込むAppがたくさんある場合、Shiftキーを押しながらログインすると、これらの認証ダイアログの多くを回避できます。
- UUIDが変更されたため、Time Machineがオリジナルのソースボリュームを認識できなくなる（考えられる解決策 <<http://www.baligu.com/pondini/TM/B6.html>>）
- Google Drive を接続解除してから、アカウントに再接続してください。詳しくは [こちらから](http://bombich.com/ja/kb/discussions/google-drive-reports-google-drive-folder-missing) <<http://bombich.com/ja/kb/discussions/google-drive-reports-google-drive-folder-missing>>
- Finder 環境設定が尊重されていない（例：デスクトップにディスクを表示するかどうか、“マイファイル”項目の内容が空、など）
- Photoshopからスクラッチディスクの環境設定をリセットする必要があると要求される [考えられる解決策 <<https://forums.adobe.com/thread/370733?start=0>>]
- エイリアスがSnow Leopardまたはそれ以降に作成された場合、Finderがバックアップボリュームのファイルにエイリアスを解決できない。Finderは、これらのエイリアスを開こうとする時、それらの“アドレスを変更する”機会を与えます。
- ネットワーク設定が別のMacで尊重されない。保持したい広範囲のVPN設定がある場合、オリジナルのMacへのアクセスを喪失する前に、それらの設定をファイルに書き出すことをお勧めします。
- App Nap

を切にする

の設定は、アプリケーションの特定のインスタンスに適用されるので、この設定はアプリケーションのコピーに適用されません (例: バックアップボリュームなど)。

- **ローカル項目** キーチェーンは、パスワードと iCloud 経由で iOS 7 またはそれ以降を実行しているその他のデバイスに同期できるその他のフォームのデータのローカルなレポジトリです。Safari とメールはローカル項目のキーチェーンにパスワードを保管します。 **ローカル項目** キーチェーンは、作成されたオリジナルボリュームでのみ尊重され、どのバックアップからも (Time Machine からでも) 復元できません。しかし、iCloud キーチェーンの同期を有効にすると (自分が復元する必要のある状況にいることに気づく前に)、このキーチェーンのパスワードは iCloud に保管され、復元されたボリュームの iCloud にログインすると、その復元されたボリュームと共有されます。
- Little Snitch の設定、またはそれらのサブセットは、バックアップボリュームから起動中は認識されない可能性があります。 [Objective Development](https://forums.obdev.at/viewtopic.php?f=1&t=4874) によると <<https://forums.obdev.at/viewtopic.php?f=1&t=4874>> ルールを先に書き出し、バックアップボリュームから起動中に再読み込みすることが推奨されています。
- クローンまたは復元されたボリュームから Adobe Lightroom カタログを開くと、カタログがオリジナルのソースボリュームの名前とパスを参照するため、Lightroom から写真が見つからないと表示されることがあります。この [Adobe のサポート記事](https://helpx.adobe.com/lightroom/help/locate-missing-photos.html) <<https://helpx.adobe.com/lightroom/help/locate-missing-photos.html>>

[このビデオを YouTube チャンネルで見て <https://youtu.be/vZEdyaVbeo>](https://youtu.be/vZEdyaVbeo)

問題と解決方法をご覧ください。

- TeamViewer 製品のサポートは、バックアップを別の Macintosh に復元する場合、TeamViewer を再インストールすること推奨しています。
- ログイン時に開始するように設定した場合、バックアップから起動すると、Box Sync アプリケーションは Box Sync フォルダのコンテンツを削除し、それから、Box.com からすべてのコンテンツを再度ダウンロードします。Box Sync アプリケーションは Box Sync フォルダを認識するために、フォルダの inode 番号を使用します。その属性はバックアップ、または復元の間保持できません。
- プレビューアプリケーションにある署名は、バックアップボリュームから別の Macintosh を起動中、認識されません。署名は、署名が作成された Mac でのみ認識されます。
- バックアップから別の Mac を起動する際に Apple Pay が正しく機能しないことがあります。 [解決策 <<https://blog.yimingliu.com/2017/06/15/resolving-endless-apple-pay-add-card-loop-after-time-machine-restore/>>]

サードパーティの解決策 / 回避策の参照は情報としてのみ提供されます。これらの解決策は弊社ではテストしていませんので、保証することはできません。

1台のコンピュータをバックアップし、そのクローンを使用して別のコンピュータを復元できますか？

答えは概しておそらくできます。しかし、警告があります。

ご使用のコンピュータの出荷時に搭載されているよりも、古いバージョンのmac OSをインストールしない

Appleから新品のMacを入手した時点で、MacにはmacOSの特定のバージョンがインストールされているだけでなく、Macのそのモデル固有のビルドがなされています。OSの古いバージョン、またはビルドをインストールすると、例えば古いMacをそれにクローンすること

で、予期しない動作を引き起こすか、あるいは、全く起動しないという可能性もあります。

新しいMacが新品の場合、“移行アシスタント”を使って新しいMacにデータを移行してください。

新しい

Macが、ただの別のマシンで、新品ではない場合は、別のMacをその新しいMacにクローンしても問題なく動作するかもしれませんが。ソースMacを新しいMacにクローンする際、ソースMacがより新しいMacに元々搭載されているものよりも最低1つ後のリリースにアップデートされていること確認してください。例えば、新しい方のMacに10.12.4が搭載されているとしたら、移行する前にソースMacを10.12.5にアップデートする必要があります。もしこのようなアップデートを利用できない場合は、代わりに[移行アシスタント](#)

<https://support.apple.com/kb/HT204350>を使用してください。

T2 MacおよびAppleシリコンMacには“パーソナライズ”されたオペレーティングシステムがあります

T2 MacまたはAppleシリコンMacにmacOSがインストールされていると、macOSインストーラはお使いのMacに固有のコード署名を使って、起動リソースのいくつかに署名します。他のMacのバックアップからお使いのMacを起動しようとする時、お使いのMacはそのボリュームから起動することを拒否し、次のように表示します：

この起動ディスクを使用するにはソフトウェアアップデートが必要です。今すぐアップデートするか、別の起動ディスクを選択してください。

この“アップデート”にはシステムリソースのダウンロード、およびバックアップボリュームのOSを現在のMacにパーソナライズすることが含まれます。この操作にはインターネット接続が必要です。通常、そのアップデートは問題なく適用され、バックアップボリュームは起動可能になります。しかし、さまざまな要因によってそれが失敗することがあります。

[オペレーティングシステムのバージョンが起動しようとしているMacと互換性があることを確認](#)

<https://support.apple.com/en-us/HT201686>後、これを動作させるための2つのオプションがあります：

T2 Mac

- “Command+R”を押したまま、Macをカバリーモード <https://support.apple.com/en-us/HT201314> に起動して、[安全な起動設定を中程度のセキュリティ](#) <https://support.apple.com/en-us/HT208330>

に変更し、その後バックアップボリュームから起動してみてください。または、

- “T” キーを押しながら起動し、Macをターゲットディスクモード (TDM) <<https://support.apple.com/en-us/HT201255>> に起動して、Macとバックアップディスクをもう 1 台のMacに接続してから、バックアップをTDMのMacの内蔵ストレージに直接復元してください。CCCはmacOSにコピー先のMacをパーソナライズするように指示します。このプロシージャには、macOS Catalina、またはそれ以降、およびインターネット接続が必要です。

AppleシリコンMac

起動時にパワーボタンを押したままにして、“オプション”を選択してから、“続ける”ボタンを押してください。その後：

- ユーティリティメニューから“起動セキュリティ”を選択し、セキュリティポリシーをセキュリティを低下に変更して、バックアップボリュームから起動を試みてください。または、
- ユーティリティメニューから“ディスクを共有...”を選び、共有するボリュームを選択してから、“共有を開始”のボタンをクリックしてください。バックアップディスクを別のMacに直接接続して、共有するMacをUSBまたはThunderbolt経由でもう一台のMacに接続します。その後、バックアップを共有するMacの共有ディスクに直接復元してください。CCCはmacOSにコピー先のMacをパーソナライズするように指示します。このプロシージャには、macOS Catalina、またはそれ以降、およびインターネット接続が必要です。

Intel MacのバックアップをM1 Macに復元しようとする

ことは避けてください。データを古いiMacから新しいiMacに移行する場合には、[移行アシスタント](https://support.apple.com/kb/HT204350) <<https://support.apple.com/kb/HT204350>> を使用してください。

システム環境設定の中には“ホスト固有”とみなされるものもあります

このような環境設定は、クローンされたオペレーティングシステムとデータから別のマシンを起動する場合、無視されます。例えば、スクリーンセーバの環境設定はホスト固有です。起動可能なクローンから別のマシンを起動してスクリーンセーバが始まると、デフォルト設定に戻っているのに気がつくでしょう。データが喪失しているのではないかと恐る必要はありません。オリジナルの環境設定は、オリジナルのMacからもう 1 度起動する際に“復元”

されま

す。どの環境

設定がホスト固有かを知る

には、Optionキーを押したままFinderの“移動”メニューからライブラリを選択し、ライブラリ > 環境設定 > ByHost と進んでください。

ネットワーク設定が別のMacintoshで尊重されないことがある

アプリケーション固有の環境設定ファイルに加えて、あるMacのネットワーク構成は別のMacで受け入れられないことがあります。macOSのネットワーク設定は、/Library/Preferences/System Configuration/preferences.plist に保存され、明示的に除外しない限り、CCCはそのファイルをコピーします。時にはMacが別のMacからの設定構成ファイルを尊重することがありますが、ネットワークのハードウェア構成にmacOSがそのファイルの内容を無視する決定をするのに十分な違いがあることがよくあります。

アプリケーションの中には別のMacで開くと異なる動作をするものがあります

CCCのドキュメントのこの箇所 <<http://bombich.com/ja/ja/kb/ccc5/some-applications-behave-differently-or-ask-serial-number-on-cloned-volume.-did-ccc-miss>>

では、周知の影響を受けるアプリケーションのいくつかを紹介します。

macOSインストーラはファームウェアアップグレードを適用します

古いMacは、macOSインストーラがファームウェアアップグレードを適用するまでAPFSボリュームを起動可能なデバイスとして認識しません。High Sierraまたはそれ以降を別のMacにクローンしたい場合、新しいOSをそのMacに問題なくクローンする前にそのシステムに最低 1 度macOSインストーラを使用している必要があります。

では、実際に動作するかどうかはどうすればわかりますか？

このタイプのクローンが動作するかどうかを判断するのはとても簡単です。ソースMacのCCCバックアップからコピー先Macを起動するだけです：

1. Thunderbolt、またはUSBケーブルを使って、ソースMacのCCCバックアップをコピー先Macに接続してください。
2. コピー先Macで、システム環境設定の“起動ディスク”のパネルを開き、ソースMacのバックアップボリュームを起動ディスクとして設定してから“再起動”のボタンをクリックしてください。

コピー先MacがソースMacのmacOSのインストールから問題なく起動したら、動作するということです！CCCを開いてから、ソースMacのディスクをコピー先Macの内蔵ハードドライブにクローンしてください。コピー先MacがソースMacのmacOSのインストールから起動できなかった場合は、移行アシスタントを使用してユーザデータとアプリケーションを転送してください。

関連ドキュメント

- [Apple Kbase #HT201686](https://support.apple.com/kb/HT201686) : コンピュータに搭載されているOSよりも古いバージョンのMac OSをインストールしないでください <<https://support.apple.com/kb/HT201686>>
- [Apple Kbase #HT204319](https://support.apple.com/kb/HT204319) : Macコンピュータに含まれているmacOSバージョンとビルド <<https://support.apple.com/kb/HT204319>>
- [Apple Kbase #HT208020](https://support.apple.com/kb/HT208020) : 自分の企業 / 団体でMacのmacOSをアップグレードする <<https://support.apple.com/kb/HT208020>>

I have a clone created by another application. Will CCC recognize that data, or will it want to recopy everything?

CCC always examines the files on the destination to determine if they already match those on the source. If you have a volume that is virtually identical to your source, CCC will copy only the items that are different between the two volumes.

Scenario 1: Clone created by another cloning utility

If the software you used previously created a non-proprietary clone of your source to the destination, then CCC will copy only the items that have changed since you created the backup. CCC doesn't care what application you used to copy the files previously, only whether the files match based on name, path, and modification date.

Scenario 2: I replaced my hard drive with an SSD, and now I want to use the HDD as my backup

Whether you cloned your HDD to the SSD or used Migration Assistant to get your data there, the bulk of the data on your HDD and SSD are identical. Once again, CCC doesn't care how the data got there or what application put it there, CCC will copy only the items that are different between the two volumes.

Scenario 3: My backup is in a folder on the destination. Why is CCC recopying everything?

The common use of CCC is to create a bootable clone of your startup disk. To do this, CCC copies all of the stuff from your source volume directly to the destination volume — not into a subfolder, but directly to the destination. At the end of the task, the destination looks exactly like the source. Typically you see Applications, Library, System, and Users on the source volume, so that's exactly what you should see on the destination volume.

If your previous backup was placed in a folder, however, then you must instruct CCC to place your backup into that same folder (assuming that's what you want — macOS will not work when placed in a folder on the destination). To do this, choose Choose a folder from the Destination selector to select the folder that your backup should be placed into.

CCCはBootCamp (Windows) パーティションをバックアップできますか。

CCCはBoot Campパーティションの内容をバックアップできますが、パーティションの起動可能なクローンを作成することはできません。Boot Campパーティションにあるユーザデータをバックアップすることが目的であるなら、CCCはそのニーズを満たすことができます。もし、Boot Campパーティションを新しいハードドライブに移行することが目的である場合、別の選択肢を考える必要があります。WinClone

<https://twocanoes.com/products/mac/winclone>、またはBoot

Campから移行する方法を提供する仮

想化ソフトウェアなどはその例です。

CCCはWindowsのシステムファイルまたはアプリケーションのバックアップまたは復元を処理できるようにデザインされていません。

Windowsのシステムファイルのコピーを回避

WindowsのシステムファイルがNTFSボリュームでアクセスされた時にmacOSがクラッシュするという報告を受けました。この問題に遭遇した場合は、Windowsのシステムファイルをバックアップタスクから除外してください：

1. CCCを開き、関連するバックアップタスクを選択します
2. ソースセレクタの下のポップアップメニューから**選択したファイル...**を選びます
3. タスクフィルタパネルから **WINDOWS** と **プログラムファイル** を除外してください。
4. 完了ボタンをクリックします。
5. “保存” ボタンをクリックするか、CCCの**ファイル** メニューから**保存**を選択してください

CCCはmacOSとWindowsの両方のパーティションを同時にクローンしますか？

いいえ。CCCは1度に1つのボリュームのみをコピーします。そして、CCCはコピー先ディスクのパーティションを変更しません。新しいディスクに何かを復元する前にカスタムパーティションを適用する必要があります。

大きなディスクに移行するつもりですが、CCCはWindowsボリュームにも対応しますか？

いいえ。CCCはWindowsボリュームの起動可能なバックアップを作成しません。

CCCはParallelsまたはVMWareの仮想マシンのコンテナをコピーしますか。

もちろん！CCCにとってはこれらは普通のファイルですので、問題なくコピーします。これらのファイルはかなり大きなものですので、これらのファイルが使用される時、またはVMコンテナファイルのアップデートされたコピーを収容するだけの十分な空き容量がコピー先ボリュームにない場合、問題が起きることがあります。ご注意ください。ドキュメントの以下の3つのセクションでこの件について説明します：

コンピュータを使用しながらバックアップを実行することはできますか。開いているファイルがある場合、それらはバックアップされますか。 <<http://bombich.com/ja/ja/kb/ccc5/can-i-run-backup-while-im-using-my-computer-if-i-have-open-files-will-they-be-backed-up>>

コピー先にソースのデータを収容できるぴったりの空き容量があるのに、CCCがバックアップタスクを完了しないのはなぜですか？ <<http://bombich.com/ja/ja/kb/ccc5/ccc-reported-destination-full.-what-can-i-do-avoid#destinationistightonspace>>

プリフライトおよびポストフライトシェルスクリプトの例 (例：自動的にParallelsを中断する方法)

[<http://bombich.com/ja/ja/kb/ccc5/performing-actions-before-and-after-backup-task#examples>](http://bombich.com/ja/ja/kb/ccc5/performing-actions-before-and-after-backup-task#examples)

Can I use Carbon Copy Cloner to clone a Time Machine backup?

No, CCC will exclude the Backups.backupdb folder during a backup task because Time Machine backup folders contain Apple-proprietary filesystem devices. Apple's recommended procedure for copying a Time Machine volume is documented in [this Apple Kbase article <https://support.apple.com/en-us/HT202380>](https://support.apple.com/en-us/HT202380).

Backing up Time Machine sparsebundle disk images

When Time Machine is configured to back up a Macintosh to a network volume (such as a Time Capsule device), Time Machine stores the backup in a sparsebundle disk image. CCC can copy these sparsebundle disk image files without any special configuration; simply choose your network volume as the source of your CCC backup task. In fact, CCC quite capably copies only the bands within the sparsebundle that have changed, so you can add CCC to this type of setup for a second tier backup to an offsite network share.

Note that CCC will exclude the Backups.backupdb folder at the root level of a volume by default. If your source volume has a folder by that name, and you want CCC to copy sparsebundle disk images from this folder, you can choose Choose a folder... from CCC's Source selector and choose the Backups.backupdb folder directly to configure CCC to back up the sparsebundle disk images. Note that the only items in a Backups.backupdb folder that CCC will copy are sparsebundle disk images. Other folders, e.g. local Time Machine backups will be excluded. Further, CCC will only consider sparsebundle images for deletion in a Backups.backupdb folder on the destination. Other items in this folder on the destination will be protected from deletion.

Lastly, please note that no application can access the contents of a sparsebundle disk image file while that disk image is mounted or otherwise deemed to be in use. For example, if your Time Machine backups are currently running and backing up to a disk image, CCC will not be able to copy the disk image file, rather it will get an error that the files are in use.

CCCからコピー先がいっぱいという報告がありました。この問題を回避するにはどうすればいいですか。

デフォルトで、CCCはそれぞれのバックアップタスクの最初に、コピー先の空き容量が25GBを確保できるようにSafetyNetの削除制限を設定して開始します。CCCは必要に応じて自動的にその制限の上限を上げます。CCCのデフォルトSafetyNet設定を使用しないで、“コピー先がいっぱいです”というエラーに遭遇する場合は、“高度な設定”でより緩やかな削除制限を適用する必要があります。コピー先で必要とされる空き容量は、平均的に1日で編集されるファイルサイズによって異なります。一般的に、通常バックアップタスクの間コピーされるのと同じ容量がバックアップタスクの開始時（削除完了直後など）に利用できるようになっている必要があります。つまり、CCCが通常9GBのデータをコピーしていても、たまに14GBまで増加することがある場合には、削除の設定をその最大値に対応できるように（例えば、最低15GBの空き容量を残しておく）設定する必要があります。特に大容量のファイルを定期的に変更するような場合は、1回にコピーされるデータ量は最小でもかなり多くなります。例えば、日常的に80GBのWindowsの仮想コンテナを使用している場合、毎日のバックアップタスクの間にコピーされるデータ量は少なく見積もっても最低80GBになるので、その分を削除設定で対応しておく必要があります。

CCCのSafetyNet削除制限の設定を変更するには、CCCのメインアプリケーションウィンドウからタスクを選択し、以下の手順に従ってください：

1. **高度な設定** ボタンをクリックします。
2. **ファイルをコピーする前に** のセクションで、CCCがSafetyNetフォルダを削除する方法を指定してください。例えば、コピー先で利用できる空き容量、アーカイブの古さ、アーカイブのサイズなどを基準に指定できます。
3. 制限を指定します。
4. 空き容量のオプションを選択した場合、**自動調整** のチェックボックスをチェックしておく、CCCがその値を自動的に管理できます。
5. 変更内容をタスクに保存してください。

新しいファイルのために十分な空き容量があるのに、CCCからコピー先がいっぱいという報告があるのはどうしてですか。

良好なバックアップファイルをソースの壊れたファイルで上書きすることがないように、CCCはatomic

コピーと呼ばれる特別なファイルコピーの手順を使用します。ファイルが最後のバックアップ以来変更された場合、一時的なファイル名、例えばfilename.XXXXXXを使用してコピー先にコピーされます。ファイルのコピーが完了したら、CCCはコピー先の古いバージョンを削除（またはアーカイブ）して、アップデートしたファイルを正しいファイル名に名称変更します。ファイルのコピーが完了したら、CCCはコピー先の古いバージョンを削除（またはSafetyNetに移動）して、アップデートしたファイルを正しいファイル名に名称変更します。

CCCがこの特別なプロシージャを使用するため、

コピー先ボリュームには、最低でも、バックアップされるすべてのデータ、プラス、ソースボリュームにある最大量のファイルの一時的なコピー

を収容するだけの空き容量を確保する必要があります

。大容量のファイル、例えば、ムービー、ディスクイメージ、仮想マシンコンテナなど、を頻繁に変更する場合、バックアップタスク実行中に空き容量が不足することを避けるために、ソースボリュームで消費されるよりもずっと多い空き容量を持つバックアップボリュームを指定しておく必要があります。

ジレンマを説明する良い例

以下のシナリオを考えてみてください：

- ソースボリューム：500GB
- コピー先ボリューム：500GB
- ソース上のデータ：450GB
- ソースの最大ファイル：75GB

コピー先が空の場合、計算は簡単です。つまり、450GBのデータは問題なく500GBのディスクに収まります。

それでは、次のバックアップタスクを実行するとしましょう。ソースに何の変更も起きなかったとします。但し、問題はその75GBのファイルです。そのファイルをどのようにコピー先にコピーすれば良いでしょう。この時点でコピー先には50GBしか空き領域がありません。

オプション A：無謀

- コピー先から75GBのファイルを削除する
- 新しい75GBのファイルをソースからコピー先にコピーする

オプション B：アトミックコピー

- 新しい75GBのファイルをソースからコピー先にコピーする
- コピー先から75GBのファイルを削除する

このシナリオではオプション Bは不可能です。しかし、オプション Aはばかげています。CCCがオプション Aを使用することはありません。データでサンプルをするようなものです。それに、理論的でもありません。他の“バックアップ”ソフトを使ってこの方法でデータを喪失した人たちの話を聞いたことがあります。

CCCはアトミックファイルコピーの方法を使用します。置き換えられるファイルを削除してから置き換えるファイルをコピーする代わりに、CCCは置き換えるファイルをまずコピー先にコピーします（一時的なファイル名を使用して）。ファイルが問題なくコピーされると、CCCはそのファイルの古いバージョンを削除（またはアーカイブ）し、一時的なファイル名を正しい名前に変更します。これは、万が一メディアエラーによりソースファイルを読み取れないとCCCが気が付いた場合、特に重要です。“オプション A”のコピー操作を使うと、コピー先にファイルの良いコピーがまったく残らないで、もちろんソースに壊れたコピーが残ります。アトミックコピー法の欠点は、ファイルの古いバージョンのコピーと置き換えるバージョンを両方収容するための十分な空き領域がコピー先に必要となることです。

同様のシナリオに遭遇した場合、いくつかのオプションがあります：

- CCCが安全なバックアップを実行できるようにより大容量のコピー先ディスクを入手する。このオプションを強く推奨します。
- その75GBのファイルを削除する**プリフライトスクリプト** <<http://bombich.com/ja/ja/kb/ccc5/performing-actions-before-and-after-backup-task#schedulershellscripts>> を実行して、ソースファイルが壊れないことを期待する。**こちらからプリフライトスクリプトの例をダウンロード** <<http://bombich.com/ja/software/files/tools/removelargefile.sh.zip>> できます。

最後に、CCCの“最初に削除パスを実行”するトラブルシューティングのオプションはアトミックコピーの手順と矛盾しないので、このシナリオには適用できません。削除パスはソースに存在しなくなったファイルをコピー先から削除しますが、バックアップ中にアップデートされるであろうファイルを削除することはありません。

SafetyNet機能をオフにしているのに、どうしてコピー先がいっぱいになることがあるのですか。

CCCのSafetyNet設定を無効にしている場合、項目が削除の対象になることに出くわすと、削除が起きるというこ

とに注意してください。CCCはソースとコピー先ボリューム両方のファイルとフォルダをアルファベット順にトラバースします。そのため、CCCがソースから削除された項目を削除する前に、新しいファイルをコピー先に書き出す可能性が起きます。ソースに大規模な組織的変更が加えられた場合、(例: フォルダの名称変更または移動、削除と作成を何度も繰り返した場合)、先を見越して以下の手順でコピー先のスペースを開けておくことができます:

1. SafetyNetオプションを無効にしている、コピー先からSafetyNetフォルダを削除するオプションを選択しない場合、**ユーティリティメニューからSafetyNetフォルダを削除...**を選択してください。CCC SafetyNetフォルダをFinderから**SafetyNetフォルダを削除**のウィンドウにドラッグして、そのフォルダを削除してください。
2. “高度な設定” ボタンをクリックします。
3. **コピー先のルートレベルの項目を保護** <<http://bombich.com/ja/ja/kb/ccc5/advanced-settings#protect>>の横にあるボックスのチェックマークを外してください。
4. **トラブルシューティングのオプションボックスにある最初に削除パスを実行** <<http://bombich.com/ja/ja/kb/ccc5/advanced-settings#troubleshooting>>の横にあるボックスをチェックしてください。
5. バックアップタスクを保存して実行してください。

関連ドキュメント

- ソースとコピー先でディスクの使用状況が異なるのはどうしてですか? <<http://bombich.com/ja/ja/kb/ccc5/disk-usage-on-destination-doesnt-match-source.-did-ccc-miss-some-files>>
- SafetyNetの自動管理 <<http://bombich.com/ja/ja/kb/ccc5/automated-maintenance-ccc-safetynet-folder>>
- VM コンテナバージョンがSafetyNetを肥大化させるのを防ぐために別のタスクを作成するには <<http://bombich.com/ja/ja/kb/ccc5/creating-separate-task-prevent-vm-container-versions-from-bloating-safetynet>>
- メール “ 接続動作状況のログを記録 ” を設定すると非常に大きなファイルが作成されます <<http://bombich.com/ja/ja/kb/ccc5/why-ccc-recopying-every-file-during-each-backup#mailcdlog>>

Frequently Asked Questions about encrypting the backup volume

- [Can I back up an encrypted volume to a non-encrypted volume?](#)
- [If I back up an encrypted volume to a non-encrypted volume, will the copied files be encrypted on the destination?](#)
- [Will Carbon Copy Cloner enable encryption on my backup volume?](#)
- [Do I have to wait for encryption to complete before rebooting from my production volume?](#)
- [What password do I use to unlock my encrypted volume?](#)
- [What happens if I change my account password on the source volume? Does the encryption password on the backup volume get updated automatically?](#)
- [I enabled encryption on my 3TB USB backup disk. Why can't I boot from that volume any more?](#)
- [Can I create a bootable backup on a pre-encrypted volume? Why do you recommend cloning to a non-encrypted volume first?](#)
- [I restored my backup to another Mac that had FileVault enabled, and now I can't unlock the cloned volume.](#)
- [I can't enable FileVault, I'm told that my account cannot be used to manage encryption on this Mac](#)
- [The Startup Security Utility reports that authentication is needed, but no administrators can be found](#)
- [After cloning to an APFS volume that previously had FileVault enabled, the destination can't be unlocked on startup](#)
- [After cloning to an APFS Encrypted volume there is a 24-second stall during startup](#)
- [My YubiKey authentication device can't unlock my encrypted backup volume on startup](#)

Can I back up an encrypted volume to a non-encrypted volume?

Yes.

If I back up an encrypted volume to a non-encrypted volume, will the copied files be encrypted on the destination?

No, encryption occurs at a much lower level than copying files. When an application reads a file from the encrypted source volume, macOS decrypts the file on-the-fly, so the application only ever has access to the decrypted contents of the file. Whether your backed-up files are encrypted on the destination depends on whether encryption is enabled on the destination volume. If you want the contents of your backup volume to be encrypted, follow the [procedure documented here](http://bombich.com/kb/ccc5/working-filevault-encryption) <<http://bombich.com/kb/ccc5/working-filevault-encryption>> to enable encryption.

Will Carbon Copy Cloner enable encryption on my backup volume?

No. You can enable encryption in the Security & Privacy preference pane while booted from your bootable backup, or in the Finder by right-clicking on your backup volume (for a backup volume that does not have an installation of macOS).

Do I have to wait for encryption to complete before rebooting from my production volume?

No. Once you have enabled encryption on the backup volume, you can reboot from your production startup disk and the encryption process will continue in the background.

What password do I use to unlock my encrypted volume?

When you boot your Mac from the backup volume and enable FileVault in System Preferences, you explicitly choose which user accounts will be allowed to unlock that volume. To unlock the volume in the future, enter the

password to any of those user accounts. Do not attempt to use the Recovery Key or your Apple ID account password to unlock the volume — those passwords will not unlock the volume.

If you erased your backup volume as encrypted in Disk Utility, then you will use the password that you specified in Disk Utility to unlock the volume.

What happens if I change my account password on the source volume? Does the encryption password on the backup volume get updated automatically?

The encryption password(s) on the backup volume will not be automatically updated when you change the password for an account on the source volume. When you boot from the backup volume, you may notice that your user account icon is a generic icon, and the text indicates "[Update needed]". The update that is required is within the proprietary encryption key bundle that macOS maintains for your encrypted volume. This encryption key is not maintained on the backup volume, and it is Apple-proprietary, so it isn't something that CCC can or should modify. To update the encryption password on the destination volume:

1. Choose the backup volume as the startup disk in the Startup Disk preference pane and restart your computer. You will be required to provide the old password to unlock the volume on startup.
2. Open the Users & Groups preference pane in the System preferences application.
3. Click on the user whose password was reset on the source volume and reset that user's password again. Resetting the password while booted from the backup volume will update the encryption key for that user on the backup volume.
4. Reset the password for any other user accounts whose password was reset on the original source.

I enabled encryption on my 3TB USB backup disk. Why can't I boot from that volume any more?

Some versions of OS X have difficulty recognizing USB devices that have been encrypted with FileVault. The Western Digital My Passport Ultra 3TB disk, for example, works fine as a bootable device when not encrypted. In our tests, however, this device was no longer recognizable when FileVault encryption was enabled. This problem appears to be limited to OS X 10.11 El Capitan. The same volume was accessible using older and newer OSes, and also functioned fine as an encrypted startup device using older and newer OSes.

Can I create a bootable backup on a pre-encrypted volume? Why do you recommend cloning to a non-encrypted volume first?

Catalina users: It is not possible to create a bootable backup on a pre-encrypted backup disk, [Apple's tools just don't permit this <http://bombich.com/kb/cc5/macos-catalina-known-issues#diskutiladdvolumeencryption>](http://bombich.com/kb/cc5/macos-catalina-known-issues#diskutiladdvolumeencryption) . You can enable FileVault after establishing your initial backup, and then CCC can maintain a bootable backup on your FileVault-encrypted backup volume.

We generally [recommend that people establish a bootable backup on a non-encrypted volume <http://bombich.com/kb/cc5/working-filevault-encryption>](http://bombich.com/kb/cc5/working-filevault-encryption), and then enable FileVault while booted from the destination. Some people have discovered, however, that a pre-encrypted volume can function as a bootable device with versions of macOS prior to Catalina. So why do we recommend the former? There are a couple notable differences between pre-encrypting the disk vs. enabling FileVault after booting from the not-encrypted disk. When you enable FileVault via the Security Preference Pane:

- You get a sanity check that a recovery volume exists (this avoids spending lots of time copying files only to find out that the volume might not be bootable)
- You get the opportunity to store a recovery key with Apple
- You can unlock the disk with selected accounts
- You get a nicer UI on startup to unlock the disk (e.g. it's similar to the LoginWindow interface), vs. a less-polished looking Unlock Disk interface
- APFS-specific: You avoid a 24-second startup delay that occurs when the system can't find the "disk" user

in the system's directory service on a pre-encrypted APFS volume.

One drawback to enabling FileVault via the Security Preference Pane, however, is that [changes to account passwords on the source volume aren't immediately reflected on the backup](#) as far as unlocking the disk is concerned. The old account passwords would be required until you boot from the backup and specifically re-enable those accounts in the Security Preference Pane (at which time the disk's EncryptionKey is remastered).

As far as the backups are concerned, there's no difference between these two methods. There is still an order-of-operations concern with pre-encrypting the disk if your disk is formatted using Apple's legacy HFS+ filesystem format (the steps below are not applicable to APFS). You'd want to approach it in this manner:

1. [Erase the destination device <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x >](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x) (unencrypted!)
2. Click on the freshly-erased disk in CCC's sidebar and create a recovery volume on that disk
3. Go back to Disk Utility and erase the volume now, not the whole disk (as was emphasized in the instructions above). Now you can choose the option to encrypt the volume. By erasing just the volume here, not the whole disk, the hidden recovery partition that CCC created won't be destroyed.
4. Open CCC and configure your backup task

In general, either procedure is fine, it really is the same as far as the backup is concerned. We generally prefer the Security Preference Pane method, however, because it yields the same UI behavior you are expecting if you have enabled FileVault on your production startup volume. Many people become concerned when the Disk Utility-encrypted volume shows any behavioral difference at all with regard to unlocking the disk on startup, and that concern is best avoided by enabling FileVault in the Security Preference Pane.

I restored my backup to another Mac that had FileVault enabled, and now I can't unlock the cloned volume.

Encryption is a volume-specific endeavor, and when it's enabled via FileVault, it's also tied to the user accounts on that specific installation of macOS. If you clone another installation of macOS onto a volume that has FileVault enabled, the user accounts from the "foreign" (source) OS will not be able to unlock the FileVault-encrypted destination volume. To avoid this scenario, you should erase the destination volume as a non-encrypted volume. When erasing an APFS volume, be careful to [erase the whole APFS container, not just the encrypted volume within the container <http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#eraseapfscontainer>](http://bombich.com/kb/ccc5/preparing-your-backup-disk-backup-os-x#eraseapfscontainer) .

Please note that this concern is not applicable to restoring a backup to the original source volume. In that case, the OS on the backup volume is not foreign; the user accounts on the backup volume match the user accounts on the original source. In that scenario, FileVault will continue to function normally.

I can't enable FileVault, I'm told that my account cannot be used to manage encryption on this Mac

The Startup Security Utility reports that authentication is needed, but no administrators can be found

After cloning to an APFS volume that previously had FileVault enabled, the destination can't be unlocked on startup

After cloning to an APFS Encrypted volume there is a 24-second stall during startup

All of these conditions are caused by the same underlying problem: users on the affected volume do not have access to the volume's Secure Token. There are generally two ways to get to this result:

- The volume was erased as an encrypted volume, thus no user account was associated with the unlocking

of that volume, or

- The user accounts that are allowed to unlock the disk belonged to some previous installation of macOS on that volume

Solution: Erase the destination in Disk Utility before proceeding with the cloning task. You should erase the destination as "APFS", not "APFS (Encrypted)". For more technical users, we offer some additional background information below.

APFS volumes that contain an installation of macOS will each have a unique "secure access token". Access to this token allows users to do things like unlock the volume (e.g. if FileVault is enabled) and to change startup security settings. Because this token is volume-specific, it can't be copied to another volume; it has to be regenerated. In addition to this Secure Token, APFS volumes also have a list of users or keys that are "bound" to the volume. These "cryptographic users" are defined within the volume metadata, not within any particular file on the volume. As a result, these bound cryptographic users cannot be modified by CCC nor transferred from one volume to another. This cryptographic user list is proprietary to Apple; only Apple tools can modify the list, and only Apple tools can generate a SecureToken.

While the SecureToken-endowed users and the cryptographic users are usually in sync on a particular volume, these lists are decoupled, and it is possible to get them out of sync. If you clone a system to a pre-encrypted APFS volume, for example, the destination has only one "Disk" crypto user. None of the user accounts on the system that you copied will be (nor can be) included in the crypto users list of that volume. Likewise, if you clone an installation of macOS to a volume that already has an installation of macOS, then you will be overwriting the user accounts that are currently in the crypto user list with new, foreign user accounts. Those new user accounts are not only missing from the crypto user list, but it will be impossible to add them to the crypto user list if all of the previous crypto users were deleted. To avoid both of these scenarios, it's important to clone to a volume that has either crypto users that match those users that exist on the source, or to a destination that has no crypto users at all (e.g. a freshly erased, non-encrypted volume).

Manually regenerating a SecureToken

Apple does not offer a method for creating a SecureToken for a user on a volume that is not the current startup disk, so CCC cannot offer a postflight method that automatically creates that token. Apple does, however, offer a utility for granting access to the secure token for specific users on the current startup disk in a very limited number of circumstances. If the current startup disk has no crypto users (`diskutil ap listUsers /` returns "No cryptographic users"), or if one of the crypto users is still present on the current startup disk, then you can use the `sysadminctl` utility to generate a SecureToken for your administrator account, e.g. in the Terminal application:

```
sysadminctl interactive -secureTokenOn yourname -password -
```

I don't want to erase my destination again, is there any way to fix this?

If you can't unlock the cloned volume on startup, then you can decrypt the destination volume using the `diskutil` command-line utility. For example, running the following command in the Terminal application would decrypt a volume named "CCC Backup":

```
diskutil ap decrypt "/Volumes/CCC Backup"
```

After decrypting the backup volume, you can then boot from it and enable FileVault in the Security & Privacy Preference Pane in the System Preferences application.

If you can boot your Mac from the backup, but you're seeing a stall during startup, you can resolve that matter by decrypting the volume as indicated above, or by creating a new user account that has a Secure Access Token. Only the macOS Setup Assistant has the ability to create the first secure access token, so follow these steps while booted from the volume you're trying to repair:

1. Mojave+ only: Grant Full Disk Access to the Terminal application
2. Open the Terminal application and run the following commands, substituting your own volume name as applicable:

```
sudo rm "/var/db/.AppleSetupDone"  
sudo rm "/var/db/dslocal/nodes/Default/secureaccesstoken.plist"
```
3. Restart the system
4. Setup Assistant will ask you to create a new user. Create the new user account with default settings. A simple name like "tokenuser" will do, don't login with an Apple ID.
5. Immediately log out of the new user account, and log in using one of your own admin user accounts.
6. Open the Terminal application and run the following commands, substituting your own user names as applicable:

```
sysadminctl -secureTokenOn youraccount -password - -adminUser tokenuser -adminPassword -  
sysadminctl interactive -deleteUser tokenuser
```

Related Apple Bug Reports

- [rdar://46168739](#) — diskutil updatePreboot doesn't remove deleted crypto users

My YubiKey authentication device can't unlock my encrypted backup volume on startup

YubiKey users [discovered that the default keystroke input speed of the Yubikey is too fast](#) <https://forum.yubico.com/viewtopicb4e5.html?f=16&t=1142> for the Mac's firmware, resulting in dropped characters. You can solve this by decreasing the key input rate using the [YubiKey Manager](#) <https://www.yubico.com/products/services-software/download/yubikey-manager/>.

Frequently asked questions about scheduled tasks

- [Does CCC have to be running for a scheduled task to run?](#)
- [What happens if no one is logged in when a task is scheduled to run?](#)
- [Will CCC run when the computer is turned off?](#)
- [Will CCC run when the my laptop's lid is closed?](#)
- [How is system sleep handled?](#)
- [Why does my laptop sometimes go to sleep during a backup task?](#)
- [Why does my screen turn on shortly before a backup task starts?](#)
- [What if the backup drive is not available when a task is scheduled to run?](#)
- [Can I stop a backup task before it finishes?](#)
- [How can I disable/suspend a task?](#)
- [Can I configure a task to run immediately after the computer is turned on?](#)
- [Related documentation](#)

Does CCC have to be running for a scheduled task to run?

No. Once you have saved your tasks, you can quit CCC. Even if tasks are running, it's OK to quit CCC -- they will continue to run. A helper application, named "com.bombich.ccchelper" will be running quietly in the background, handling task operations. This helper application also loads automatically when you restart your computer, so you don't have to launch CCC again unless you want to make changes to your task configurations or scheduling.

What happens if no one is logged in when a task is scheduled to run?

The scheduled task will run whether someone is logged in to the machine or not. You can also log in or log out while tasks are running and the tasks will continue to run.

Will CCC run when the computer is turned off?

By default, any scheduled events that elapse when the computer is off will be skipped, and those tasks will run at their next scheduled run time. If you would like to schedule a task to occur when the system is typically powered off, choose the "Wake or power on the system" option from the System Sleep popup menu in the CCC Scheduler. With that configuration, CCC will schedule a "Wake or power on" event with the Power Management service and your system will turn on shortly before the task is scheduled to run.

FileVault exception

There is one notable exception to powering on the system for a scheduled task: If you have FileVault enabled on your startup disk, your computer would turn on, but it would not proceed past the FileVault authentication prompt. It is not possible for CCC to subvert this security feature, so the Wake or power on the system option will be disabled if FileVault is enabled on your startup disk. This limitation is applicable only when the system is turned off; CCC can wake a system with FileVault protection enabled and proceed to run a backup task.

Related Documentation

- [How to modify a scheduled backup <http://bombich.com/kb/ccc5/how-modify-scheduled-backup>](http://bombich.com/kb/ccc5/how-modify-scheduled-backup)

Will CCC run when the my laptop's lid is closed?

If your laptop is running on battery power, the system will not wake while the lid is closed and CCC backup tasks will not run. If your laptop is plugged in to AC power, then CCC can wake the system to start your scheduled task if the lid is closed. See the section above for the settings that indicate whether a task can wake the system.

How is system sleep handled?

By default, CCC will wake your computer when your tasks are scheduled to run. You can change this setting in the Runtime Conditions section when scheduling a task. As long as your Mac is running on AC power, CCC will prevent the system from sleeping for the duration of a backup task.

Related Documentation

- [Handling system sleep events <http://bombich.com/kb/ccc5/configuring-scheduled-task-runtime-conditions#sleep>](http://bombich.com/kb/ccc5/configuring-scheduled-task-runtime-conditions#sleep)
- [How to modify a scheduled backup <http://bombich.com/kb/ccc5/how-modify-scheduled-backup>](http://bombich.com/kb/ccc5/how-modify-scheduled-backup)

Why does my laptop sometimes go to sleep during a backup task?

If your Mac is a laptop, note that CCC will only be able to wake the system or prevent idle sleep if the system is running on AC power. CCC will attempt to thwart sleep while the system is running on battery power, but macOS may sleep the system anyway if there is no user activity while running on battery power.

Why does my screen turn on shortly before a backup task starts?

By default, CCC schedules a wake event to occur 20 seconds before a scheduled task is configured to run. Whether the system is sleeping or not, macOS turns on the display when a scheduled wake event occurs, and there is nothing that CCC can do to prevent this. If you prefer that your display does not turn on, e.g. in the middle of the night, use the Run this task when the system next wakes setting instead to have CCC tasks run during macOS Dark Wake cycles (aka PowerNap, aka Maintenance Wake).

What if the backup disk is not available when a task is scheduled to run?

If your backup disk is attached to your Mac and unmounted, CCC will attempt to mount the backup volume, then proceed with the backup task if that is successful. If the volume cannot be mounted or is not attached to your Mac, CCC will, by default, report an error, then run the task immediately when the backup disk is reattached to your Mac. You can fine-tune CCC's handling of this scenario using the options at the bottom of the Scheduler panel.

Can I stop a backup task before it finishes?

Yes, you can stop the backup task at any time. The next time you run the backup task, CCC will copy only the files that have changed or were missed since the last backup task.

How can I disable/suspend a task?

If CCC's sidebar is not revealed, reveal it by choosing Show Sidebar from CCC's View menu. To disable a task, right-click on that task in the sidebar and choose Disable from the contextual menu. Use the same procedure to re-enable the task. If you would like to disable all tasks, choose Disable all tasks... from the CCC menubar application, or hold down Command+Option and choose Disable All Tasks & Quit from the Carbon Copy Cloner menu.

Can I configure a task to run immediately after the computer is turned on?

CCC doesn't offer an option specifically to run tasks on startup. Running a task immediately after the system is

turned on often introduces a lot of extra disk activity that will compete with the disk activity that occurs normally during system startup. Also, it makes less sense to run backup tasks after the computer has been off, because no files have been modified while the system was off. We recommend configuring backup tasks to run sometime toward the end of your work day instead. You can also configure the task to [shut down your Mac when the task completes](http://bombich.com/kb/coc5/shut-down-your-mac-when-the-task-completes) <<http://bombich.com/kb/coc5/performing-actions-before-and-after-backup-task#powermgmtoptions>> .

If your work day does not end at a regular time, but begins at a fairly consistent time, then there may be one other option available to you. You can configure a backup task to run before your work day begins, and then configure that task to "Wake or power on the system". CCC will then schedule a "wake or power on" energy saver event, and then after the system powers on at that time, CCC will run your scheduled task. Note that this option is not available if you have FileVault enabled on your Mac's startup disk.

Related Documentation

- [How do I schedule a backup task?](http://bombich.com/kb/coc5/how-set-up-scheduled-backup) <<http://bombich.com/kb/coc5/how-set-up-scheduled-backup>>
- [Configuring Scheduled Task Runtime Conditions](http://bombich.com/kb/coc5/configuring-scheduled-task-runtime-conditions) <<http://bombich.com/kb/coc5/configuring-scheduled-task-runtime-conditions>>

Frequently asked questions about the Carbon Copy Cloner SafetyNet folder

Note: The topics in this article are not relevant to APFS-formatted destination volumes that have [CCC snapshot support enabled](#) <<http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes>>. For those volumes, CCC leverages snapshots to implement the SafetyNet functionality, and the snapshots aren't affected by any of the shortcomings described here.

- [How do I restore files from the CCC SafetyNet folder?](#)
- [Why can't I open some files in the CCC SafetyNet folder?](#)
- [Can I restore a previous version of the OS using one of the archives in the CCC SafetyNet folder?](#)
- [I deleted files from my startup disk to make more room, but now it's hard to find some of those files on my backup volume](#)
- [Why can't I delete some items from the SafetyNet folder? The Finder says that some items are in use.](#)
- [How can I prevent Migration Assistant from copying the CCC SafetyNet folder during a migration?](#)
- [I have SafetyNet enabled, why can't I find a "CCC SafetyNet" folder on the destination?](#)
- [I selected "Don't delete anything", why is CCC placing items in the "CCC SafetyNet" folder on the destination?](#)

How do I restore files from the CCC SafetyNet folder?

CCC's SafetyNet folder ("CCC SafetyNet") is excluded from CCC's backup tasks by default because it contains older versions of modified files, and files that were deleted from the source volume. Typically when you restore data from your backup volume, you will want to avoid restoring the items in this folder, choosing instead to restore the most recent backup of your files.

If there is something that you would like to restore from the CCC SafetyNet folder, a drag and drop restore in the Finder is usually the easiest way to do so. If you would like to restore many items, or merge them into an existing folder, choose Choose a folder... from CCC's Source selector and choose the folder from which you would like to restore. If you choose the CCC SafetyNet folder as the source, note that the full path to your archived files will be preserved, e.g. 2017-07-27 (July 27) 14-11-18/Users/fred/Documents/some file.pdf. In most cases, you will want to choose a subfolder within the archives folder as your source. Likewise, choose Choose a folder... from CCC's Destination selector and select the specific folder that you want to restore items into.

Why can't I open some files in the CCC SafetyNet folder?

When CCC evaluates the items on your destination and determines whether they should be archived or left in place, it does so on a file-by-file basis. This poses a challenge for bundle files — files that are actually a folder of files, but presented by the Finder as a single file. As a result, bundle files (e.g. applications, some types of libraries, some custom file types) may appear in an incomplete form within the CCC SafetyNet folder.

Unless all of the components within a bundle file are modified, only the items that have been updated will be present. Incomplete bundle files are generally not useful on their own, but their contents can be. For example, if you accidentally deleted a photo from your iPhoto library, you would be able to recover that lost photo from the archived iPhoto library bundle. To reveal the content of an incomplete bundle file in a CCC SafetyNet folder, right-click (or Control+click) on the item and choose Show package contents from the contextual menu.

SafetyNet is a safety mechanism, it was not designed for providing access to older versions of files. If you would like access to older versions of files on your APFS-formatted backup disk, we recommend that you [enable snapshot support on that volume](#) <<http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#srp>>.

Can I restore a previous version of the OS using one of the archives in the CCC SafetyNet folder?

No. CCC's SafetyNet folder is not intended to offer a method for rolling back software updates, OS restores should always be done from the complete backup at the root level of your destination, or [from a snapshot <http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#restore>](http://bombich.com/kb/ccc5/leveraging-snapshots-on-apfs-volumes#restore).

I deleted files from my startup disk to make more room, but now it's hard to find some of those files on my backup volume

This generally isn't a concern for ordinary "flat" file types, but it can be a concern for certain applications that store lots of files in a single, monolithic-appearing container file. Some applications offer highly customized interfaces to access a specific file type. Photos, for example, allows you to manage tens of thousands of photo files. These files are all stored in a proprietary bundle file in your home folder, but because photos are so easy to organize within Photos, many people don't consider how those files are organized on the hard drive. Usually you really don't have to either. That is, of course, until you can no longer use Photos to access your photo files, and that's exactly what happens when you delete files from your Photos library, abandoning them to the SafetyNet folder on your backup volume.

If you have a habit of periodically deleting photos, music, or movies from Photos, iTunes, Aperture, or any other application that uses a proprietary bundle file format so that you can "free up some space on your startup disk", consider how those files will be organized on the destination. Specifically, keep in mind that you use a very elaborate application to access these files on the source volume, but you will only have the Finder to access these files on the backup volume.

CCC can't reorganize your deleted files in a way that's logical to you, it can only place them at the same path in the CCC SafetyNet folder as they were on the source volume. For files buried in a bundle file on the source (as is the case for Photos, for example), this means that the files will be buried in bundle files in various time-stamped archive folders on the destination. These files will also be subject to deletion if you configure CCC to periodically prune the contents of the SafetyNet. In short, simply archiving deleted files from applications such as these isn't going to be the best way to store these items long-term if your goal is ultimately to keep them.

When you want to free up some space on your startup disk, consider this approach instead, using Photos as an example:

1. Create a new folder at the root level of your backup volume, named something like "Archived Photos 2016".
2. In Photos, delete all of the photos that you want to remove from your source volume. When you delete these items, they are placed in the Recently Deleted album.
3. Click on the Recently Deleted album in the Photos sidebar and select all of the photos in that folder.
4. Drag all of the selected photos from the Recently Deleted album to the "Archived Photos 2016" folder on the backup volume.
5. Once the photos are safely copied to and neatly organized on the backup volume (and ideally, after you have made a second backup of these precious files on some other volume), go ahead and click the Delete All button in the Recently Deleted album.

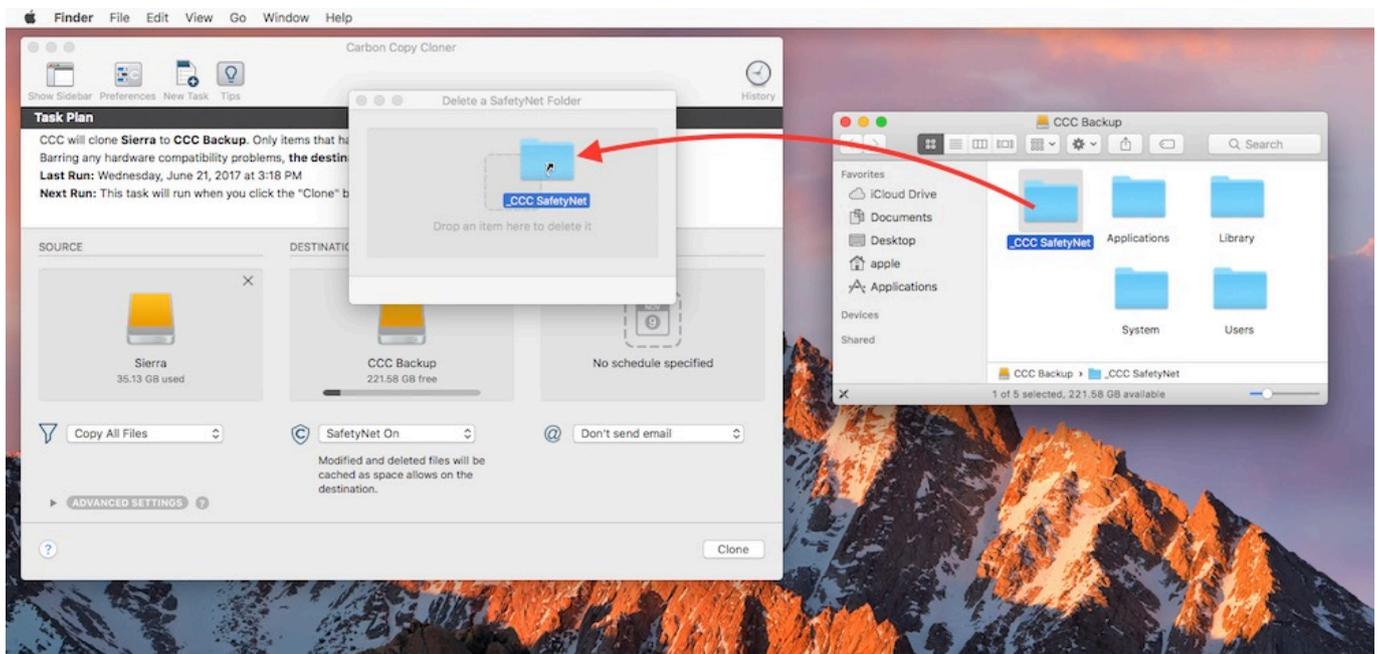
Not all applications have this kind of internal Trash folder, so be sure to see how it works for other applications before applying these exact steps. The general idea, though, is that you should deliberately archive the items that you're removing from your source volume in a way that makes sense to you rather than passively allowing CCC to archive them in a manner that makes sense to the computer.

Why can't I delete some items from the SafetyNet folder? The Finder says that some items are in use.

In OS X El Capitan, Apple introduced a new feature called System Integrity Protection (SIP). SIP works by preventing any user from deleting certain protected system items on the startup disk. If you boot your Mac from a backup volume and restore system files to your startup disk, CCC will place outdated versions of those system files into the SafetyNet folder. These modifications are allowed because CCC is making changes to that volume while it is not the current startup disk. When you restart your computer from that destination volume, however, SIP re-engages and may then prevent you from deleting the protected items that were placed into the SafetyNet folder. If you attempt to delete these items, the Finder will report that they cannot be deleted because they are in use, or because they are protected. If you try to delete these items in the Terminal application, you'll get a more distinct error message, "Operation not permitted".

CCC won't have any trouble pruning the SafetyNet folder on its own during ordinary backup tasks. If you would like to remove an item from the SafetyNet manually, however, or if you would like to remove the entire folder:

1. Choose Delete a SafetyNet folder from CCC's Utilities menu
2. Drag the folder you want to delete onto the window that is presented. Alternatively, you can click on the drop zone in the window that is presented to make your selection from a navigation panel.



If the item you're trying to remove is on your current startup disk, CCC will move the item to the root of your startup disk, then instruct you to boot your Mac from some other volume (e.g. your backup disk). Once booted from the backup volume, you can repeat the same steps with CCC to remove the SafetyNet folder.

If you're still having trouble after trying that, don't hesitate to [ask us for help](http://bombich.com/software/gethelp) <http://bombich.com/software/gethelp> .

How can I prevent Migration Assistant from copying the CCC SafetyNet folder during a migration?

If your backup volume has a "_CCC SafetyNet" folder, you can move that folder to the Trash before using Migration Assistant to avoid copying that folder during a migration. This is particularly important if that folder has a lot of data in it and you're migrating to a disk that is smaller than the backup volume. If you would like to retain the SafetyNet folder on the backup volume, don't empty the Trash. After Migration Assistant has completed, then you can move the SafetyNet folder back to the root of the backup volume.

I have SafetyNet enabled, why can't I find a "CCC SafetyNet" folder on the destination?

There are three primary reasons that the SafetyNet folder will be missing or difficult to find on the destination:

An empty SafetyNet folder will be removed at the end of the backup task

If CCC finds nothing to archive over the course of the backup task, the SafetyNet archive will be empty at the end of the backup task. If CCC finds that the SafetyNet archive is empty at the end of the task, CCC will remove it. Likewise, if the "CCC SafetyNet" folder is subsequently empty, that folder will also be removed at the end of the backup task.

The Legacy SafetyNet folder is not used when snapshots are enabled on the destination

When snapshots are enabled on an APFS-formatted destination volume, CCC will implement the SafetyNet feature using snapshots rather than placing files into a separate folder on the destination. Select your destination volume in CCC's sidebar to find these SafetyNet snapshots.

The root level of an APFS Data volume is not visible in the Finder

CCC stores the SafetyNet at the root level of the destination. When you're making a backup of macOS Catalina or later, the destination will be an [APFS Volume Group](http://bombich.com/kb/cc5/working-apfs-volume-groups) <<http://bombich.com/kb/cc5/working-apfs-volume-groups>>, and the SafetyNet will be placed at the root level of the Data member of that group. Root-level items of the Data volume are not immediately visible in the Finder. To reveal the SafetyNet folder on an APFS volume group, right-click on your CCC Backup - Data volume (for example) in CCC's sidebar and choose the Reveal in Finder option.

Related documentation

- [The legacy SafetyNet folder is not used when snapshots are enabled on the destination](http://bombich.com/kb/cc5/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination) <<http://bombich.com/kb/cc5/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>>
- [SafetyNet snapshots vs. Backup snapshots](http://bombich.com/kb/cc5/leveraging-snapshots-on-apfs-volumes#safetynetvsbackup) <<http://bombich.com/kb/cc5/leveraging-snapshots-on-apfs-volumes#safetynetvsbackup>>
- [Where did the CCC SafetyNet folder go after upgrading to Catalina?](http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet) <<http://bombich.com/kb/cc5/frequently-asked-questions-about-ccc-and-macos-catalina#safetynet>>

I selected "Don't delete anything", why is CCC placing items in the "CCC SafetyNet" folder on the destination?

When you select the Don't delete anything SafetyNet setting, CCC applies that setting very literally. If CCC encounters a file on the destination that must be replaced with a newer version from the source, CCC cannot delete the older version of that file that is on the destination. That older file is instead placed into the "CCC SafetyNet" folder on the destination.

Frequently Asked Questions about cloning Apple's "Recovery HD" partition

Reminder: Recovery HD volume cloning is not applicable to APFS-formatted destination volumes (i.e. Catalina and later)

Carbon Copy Cloner offers complete support for archiving, cloning, and recreating Apple's Recovery HD partition. See the [Cloning Apple's Recovery HD partition <http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition>](http://bombich.com/kb/ccc5/cloning-apples-recovery-hd-partition) section of CCC's Disk Center documentation for instructions to create a Recovery HD volume on your backup disk.

When do I need to create a Recovery HD volume?

CCC bootable backups offer similar functionality to the Recovery HD volume, so the Recovery HD volume is not strictly required on a backup volume. Unless you have a specific reason to not create a Recovery HD, though (e.g. because it could affect a Boot Camp partition on the same disk, you don't want to give up the 1GB, etc), we recommend that you maintain a Recovery HD volume on your backup disk. Especially if you intend to use your destination volume in production (e.g. you are migrating to a larger disk, or restoring to a replacement disk), or if you intend to enable encryption on the backup volume, then you should create a Recovery HD volume for the destination volume. If you intend to enable encryption on the destination volume, we recommend that you create the Recovery HD volume before enabling encryption. A Recovery HD volume is not required for restoring an installation of macOS from a CCC bootable backup.

What is the difference between archiving the Recovery HD and creating a new Recovery HD?

During the course of an ordinary backup of a volume that contains macOS, CCC will automatically create an archive of the Recovery HD associated with that volume. This archive is stored on the source volume, and is subsequently backed up to the backup volume along with everything else. This archive of the Recovery HD volume can be used in the future to create a new Recovery HD, and it's the first source that CCC considers when you choose to create a Recovery HD. The archive is not, however, an operational Recovery HD volume, it's just a backup file.

CCC's Disk Center offers the ability to create an operational Recovery HD volume as well. This functionality is completely separate from creating an archive of the Recovery HD. Unlike the archiving of the source Recovery HD, creating a new Recovery HD is not something that happens automatically, you have to ask CCC to do this in the Disk Center. When CCC creates a new Recovery HD, it borrows space from your destination volume to create a new, hidden volume on that disk. The resulting Recovery HD is fully operational — you can boot your Mac from it and reinstall macOS. Refer to the previous section to determine if creating a Recovery HD is required in your situation.

Why were other volumes on my disk unmounted when I created a Recovery HD?

CCC uses a command-line version of Disk Utility to resize the donor volume. Resizing that volume requires making changes to the partition table on the disk, and Disk Utility may choose to unmount other volumes on the disk while it makes those changes. CCC will specifically remount the donor volume, but whether Disk Utility remounts the other volumes is a function (or bug) of Disk Utility. You can remount these volumes manually in Disk Utility.

Can I create a Recovery HD on an Apple Fusion (aka "CoreStorage") volume?

No, not with CCC. Creating a Recovery HD requires borrowing space from a physical volume, and that is not a modification that we recommend making to an underlying member of an Apple Core Storage logical volume. The

only Apple-supported method of creating a Fusion volume is via Disk Utility or the macOS Installer, and each of those will create a Recovery HD volume before the Fusion volume is created. If you intend to create your own HFS+ formatted Fusion volume using one of the various tutorials available on the Internet, and if you want that volume to have an associated Recovery HD volume, we strongly recommend that you create a Recovery HD volume before creating the Fusion volume. You can use CCC to create the Recovery HD volume on the slowest disk that you intend to add to the Fusion logical volume group. See the following document for a demonstration.

[Creating a Fusion volume with a Recovery HD](#)

[<http://bombich.com/software/files/tools/CreatingaFusionvolumewithaRecoveryHD.pdf>](http://bombich.com/software/files/tools/CreatingaFusionvolumewithaRecoveryHD.pdf)

Why is the option to create (or remove) a Recovery HD disabled?

If you are booted from the volume that you have selected in CCC's sidebar, the option to Create or Remove the Recovery HD associated with that volume will be disabled. This is commonly encountered when you have booted from your backup volume. To make changes to the Recovery HD associated with your startup disk, first boot your Mac from some other startup volume.

This option will also be disabled if the selected volume is a Fusion or FileVault-protected volume (i.e. a "CoreStorage" volume). CCC cannot create a Recovery HD volume on a Fusion or FileVault-protected volume, therefore CCC will never allow you to remove the Recovery HD volume that is associated with a Fusion or FileVault-protected volume.

CCC says there is a Recovery volume associated with my startup disk. Why can't I see this Recovery HD volume in the Option key startup manager?

Apple uses an abstract volume type, the CoreStorage volume, for some startup disks. Because these volumes are abstract, your Mac's firmware cannot boot directly from them; a small piece of macOS needs to assemble the abstract volume first. To accommodate this limitation, Apple associates a "helper" partition with CoreStorage volumes. In many cases, the Recovery HD volume plays that role. When you hold down the Option key on startup, your Mac's firmware can't detect the abstract CoreStorage volumes, but it can detect these helper partitions. To avoid confusion, the label given to these Recovery volumes is the label of the associated volume. So if you have a startup disk named "Macintosh HD" and an associated helper partition named "Recovery HD", you will only see one volume in the startup manager — the Recovery volume, but with the Macintosh HD label. If you want to boot from the Recovery volume, click on the Macintosh HD-labeled volume while [holding down Command+R](#) [<https://support.apple.com/en-us/HT204904>](https://support.apple.com/en-us/HT204904).

I'm backing up an APFS startup disk to an HFS+ backup disk. Will CCC automatically create a Recovery HD volume on the destination?

For logistical and data safety reasons that are specific to the shortcomings of HFS+, CCC will not automatically create a Recovery HD volume on an HFS+ formatted destination volume; CCC will only automatically create recovery volumes on APFS destination volumes. But you will be able to create a Recovery HD on the destination regardless of the format of the source. During the backup task, CCC will create a format-agnostic archive of the Recovery volume that is associated with the source. At the end of your first backup task, CCC will prompt you to create the Recovery HD volume on the destination, and will then walk you through the simple procedure. You may also select your HFS+ destination in CCC's sidebar and click on the Recovery HD... button at the bottom of the window to create that volume.

Can I run backup tasks while my system is on battery power?

CCC can run backup tasks while the system is running on battery power, but will not (by default) start automated tasks when your laptop is running on battery power. Backup tasks generate a lot of disk read and write activity, and that can run your battery down. Additionally, macOS tends to aggressively put the system to sleep when it's on battery power, causing task completion to be deferred until the system is awoken. For the best performance of your backup tasks and your battery, we recommend running your backup tasks when the system is attached to an AC power supply.

Can I configure CCC to start automated tasks when the system is running on battery power?

Yes. Click the Preferences button in CCC's toolbar to access settings related to running tasks while on battery power.

Can I run my backups more frequently than Hourly?

CCC offers hourly, daily, weekly, and monthly scheduling options, which suits the needs of most users. Some usage scenarios, however, demand higher frequency backups. For example, photographers might prefer to have their SD cards offloaded to a tethered computer every 5-15 minutes during a photo shoot. When the shoot is complete, though, the backup task should not run at all. Special cases like these demand more flexible execution options, which can be achieved by leveraging CCC's built-in command-line utility. These simple steps demonstrate how to set up a high-frequency backup task that you can easily start and stop and the beginning and conclusion of a photo shoot:

1. Open CCC and click the New Task button in the toolbar to create a new backup task. Name it something like "Location Backup".
2. Click on the Source selector and choose your tethered camera's SD card as the source.
3. Drag a folder from the Finder onto CCC's Destination selector to specify that folder as the destination.
4. Save the task (do not schedule this task).
5. Download this example [Frequent Backups script](http://bombich.com/software/files/tools/frequent_backups.command.zip) [<http://bombich.com/software/files/tools/frequent_backups.command.zip>](http://bombich.com/software/files/tools/frequent_backups.command.zip) and open it in TextEdit (Applications > TextEdit.app).
6. Modify the script to specify the correct location of CCC on your Mac (the default is correct if it is located in your Applications folder), the name of your backup task, and the frequency at which you prefer it to run. Save the changes. You can store this script wherever you like.
7. When you're ready to start your shoot, simply double-click the frequent_backups.command script. The script will run the specified task at the specified frequency.
8. When your shoot is finished, quit the Terminal application to stop the script.

If you have questions about this sort of setup or need some help getting the configuration suited to your needs, please don't hesitate to [reach out to us for help](http://bombich.com/software/gethelp) [<http://bombich.com/software/gethelp>](http://bombich.com/software/gethelp) .

System problems can lead to a failure to install CCC's helper tool

Configuration files for privileged helper tools are placed in the `/Library/LaunchDaemons` folder on your startup disk. CCC never touches this folder directly, rather it uses the macOS "Service Management" service to install and load its helper tool configuration. If the permissions or ownership of this folder are incorrect, however, the Service Management daemon (`smd`) will fail to install the helper tool configuration, and this service offers no recourse, nor even a notification that something is wrong that should be corrected.

Solution

The solution to this problem is to remove the affected system folder and recreate it with the correct ownership and permissions. To avoid exposing yourself to potential security vulnerabilities, it is imperative that you remove this folder and its contents rather than simply correcting the ownership and permissions.

1. Quit CCC if it is open
2. Choose Computer from the Finder's Go menu
3. Navigate to your startup disk > Library
4. Drag the LaunchDaemons folder to the Trash, authenticating when prompted
5. Open the Terminal application (`/Applications/Utilities/Terminal.app`)
6. Paste the following into the Terminal one line at a time, pressing the Return key at the end of each line.
Type in your admin password when prompted.

```
sudo mkdir -m 755 /Library/LaunchDaemons  
sudo chown root:wheel /Library/LaunchDaemons
```

7. Open CCC and try again to save and run a backup task

Related Documentation

- [What is CCC's Privileged Helper Tool? <http://bombich.com/kb/ccc5/what-cccs-privileged-helper-tool>](http://bombich.com/kb/ccc5/what-cccs-privileged-helper-tool)

レガシーSafetyNetフォルダは、スナップショットがコピー先で有効の場合、使用されません

SafetyNetはコピー先ボリュームのデータを保護することを目的としたCCCのユニークな機能です。この機能がデザインされた最も一般的な目的は、誤ってコピー先ボリュームとして選択されたボリュームの内容を保護することです。そのボリュームの内容を即座に削除する代わりに、CCCはその内容を“CCC SafetyNet”という名前のフォルダに保管します。設定の間違いに気づいたら、SafetyNetフォルダからファイルを復元して、バックアップタスクの設定を訂正するだけです。

SafetyNetの機能は、“アーカイブされる必要のある古いデータ”と“ソースのデータセットと全く関係のないコピー先のデータ”の違いを知ることはできません。これらのファイルは同じ保護を提供されているので、多くのユーザーはSafetyNet機能をファイルの古いバージョンの復元の手段として利用しています。SafetyNetフォルダは本来この目的のためにデザインされていないので、この目的で使用される場合多くの弱点があります

<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet>

。にも拘わらず、ファイルの古いバージョンをSafetyNetフォルダで探すユーザーが増え続けています。

古い、不必要なデータでコピー先をいっぱいにならないように、CCCは空き領域が特定のしきい値より少なくなった場合SafetyNetの内容を削除します(この操作の設定を変更した場合、古さ、アーカイブのサイズを基に削除されます)。CCCがそのフォルダの内容を削除すると、それらのファイルが占有していた領域が即座に解放されます。

スナップショットとレガシーSafetyNetフォルダは相互に除外し合う

レガシーSafetyNetフォルダを含むコピー先ボリュームでスナップショットのサポートを有効にしている場合、解決しなければならないジレンマがあります。コピー先でスナップショットを作成すると、通常の削除方法はディスクスペースの解放にまるで効果が無くなります。古いスナップショットはSafetyNetフォルダのファイルすべての参照を保持するので、それらが消費している領域はその一番古いスナップショットが削除されるまで解放されることはありません。そしてその削除はコピー先がスナップショットの保持ポリシーに定義された空き領域の制限に達するまで起こりません。

このジレンマを解決するために、スナップショットがコピー先で有効な場合、CCCはSafetyNet機能を実行するためにスナップショットを活用します。レガシーの“CCC SafetyNet”フォルダがコピー先にある場合、CCCはコピー先のSafetyNetのスナップショットを作成し(こうして、SafetyNetフォルダのそれぞれのファイルの参照を保持します)、それからレガシーSafetyNetフォルダを削除します。SafetyNetフォルダのファイルは、SafetyNetのスナップショット内に保持されるので、即座に喪失することはありません。けれども、そのSafetyNetのスナップショットは新しく、コピー先ボリュームのスナップショットの保持ポリシーで指定されたSafetyNet保持の制限の対象になります。

レガシーSafetyNetフォルダよりスナップショットが有利な点

コピー先でスナップショットを活用することは、SafetyNetをファイルの古いバージョンを復元する目的で使用するという点では、フォルダベースのSafetyNetの弱点を補います。これはSafetyNet特有の利点ではなく、むしろスナップショットを使用する一般的な利点であることに注意してください。コピー先でスナップショットを使用すると決めた場合には、SafetyNetをファイルの古いバージョンを復元するメカニズムとして考えることを避ける必要があります。ファイルの古いバージョンを復元したい場合、バックアップのスナップショットを使用してください。SafetyNetはソースのデータセットと全く関係のないコピー先から何かが削除された場合にのみ使用されるはずの**安全対策**です。

過去にファイルを復元するためにSafetyNetを使用したことがある場合、スナップショットを使用してファイルの古いバージョンを復元することで得られる以下の利点を考えてみてください：

- スナップショットのバンドルファイル (例: フォトライブラリ) は完全です。フォトライブラリからいくつかのアルバムを削除した場合、レガシーSafetyNetフォルダからそれらを復元するのは困難です。スナップショットを使えば、SafetyNetの必要すらなくなります。というのは、それらのファイルはバックアップのスナップショットに保持されているからです。
- オペレーティングシステムの古いバージョンを復元できます。
- スナップショットの削除は非常にシンプルです。ゴミ箱を空にするためにアクセス権の問題やFinderの失敗に遭遇することがありません。

スナップショットベースのSafetyNetの不利な点

スナップショットはファイルの古いバージョンを復元したいユーザにとっては意義のなる利点を提供しますが、SafetyNet機能の元々の目的には少々の損失を伴います。項目がコピー先のレガシーSafetyNetフォルダに移動されても、それらはすぐにFinderに表示されるので、簡単なドラッグ&ドロップで元の場所に **即座に** 復元できます。しかし、スナップショットが有効な場合には、それらの項目はスナップショットによって保持されますが、コピー先からは削除されます。それらの項目を復元するには、SafetyNetのスナップショットをFinderに表示してから、コピー先に **コピー** し直す必要があります。そのコピーの手順は単純な移動よりもかなりの時間がかかるだけでなく、コピー先ボリュームがいっぱいの場合には特にロジスティック的に困難な可能性があります。それらの場合、ファイルを別のボリュームに復元して、SafetyNetのスナップショットを削除して領域を解放してから、ファイルをオリジナルのボリュームにコピーし直す必要がある可能性があります。

これはスナップショットのそれほど重要ではない欠点である一方、point-in-timeの復元の利点は、SafetyNetがコピー先にしかないユニークなファイルを保護するという機能を保持する限り、この不利益よりずっと重要と考えます。

自分にとってどちらのアプローチが最適かを判断するにはどうすればいいですか？

その選択は、誤って設定してしまった場合 (例えば、間違ったコピー先を選択した、またはバックアップディスクが“安全”だと思って間違えてそこに保存してしまった場合など) の安全対策としてSafetyNet機能を重視するか、それともSafetyNet機能をファイルの古いバージョンの復元手段として使用するかによって変わってきます。ファイル (または OS) の古いバージョンを復元するためにバックアップを頼りにすることが稀にしかない場合、バックアップディスクでスナップショットを有効にしても、レガシーSafetyNetのメカニズム以上に利益を得ることはあまりありません。しかし、SafetyNetをファイルの古いバージョンを探すために使用する場合は、コピー先でスナップショットを有効にすることでバンドルファイルおよびOS全体の古いバージョンを取り出すことができます、より信頼性の高い結果を得ることができます。

Why does CCC say that my Mac is booted from a backup volume?

If you boot your Mac from a backup volume, CCC will be started upon login to ask whether you'd like help restoring from that backup volume. Sometimes, though, this offer is made when you're booted from a production volume, not a backup. CCC makes this assessment based on your currently-defined backup tasks. If you used CCC to migrate from one drive to another, then the task that you used to perform that clone will still be present on your new startup disk. When you boot your Mac from the new disk, CCC will see that you have a suspended task that specifies the current startup disk as the destination, thus giving the appearance that your Mac is booted from a backup.

If you migrated to a new disk and you'd like to avoid CCC opening on startup and offering restore guidance, open CCC and delete the task that you used to clone to your current startup disk.

CCCとmacOS Catalinaについてのよくある質問

macOS Catalinaにアップグレードした場合、お使いのMacに“Macintosh HD - Data”という新しいボリュームがあるのに気がついたかもしれません。この新しいボリュームはボリュームグループの一部で、macOS Catalinaの新しいコンセプトです。[ここではボリュームグループについて詳しく説明します <http://bombich.com/ja/ja/kb/ccc5/working-apfs-volume-groups>](#)。しかし、この記事の残り部分は、macOS Catalinaのバックアップを調整するために、CCCがこの新しいボリューム構造をどのように対処するか、およびユーザが何をすれば良いのか（もし何かする必要があるとすれば）についての質問に答えることを目的としています。

[バックアップタスクを実行する前に使用中のバックアップディスクに何か変更を加える必要がありますか？](#)

かもしれません。起動ディスクの単純なバックアップを専用のバックアップディスクに作成している場合、答えは“ノー”です。CCCがそれを特に推奨しない限り、コピー先に変更を加える必要はありません。CCCは**コピー先がmacOS Catalinaの起動可能なバックアップとなるために必要とされる変更を自動的に加えます**

。しかし、お使いのコピー先ボリュームが暗号化されている場合、この後に説明されている、暗号化されたコピー先に特化した情報をご覧ください。

しかし、同じコピー先にバックアップしているタスクが複数ある場合は、今こそバックアップの“衛生状態”を再考する良いチャンスです。理想的には、バックアップするそれぞれのソースがコピー先に専用のボリュームを持っていることです。これは、ソースの1つがCatalinaの起動ディスクである場合、特に重要です。複数のソースボリュームのバックアップを収容するためのコピー先デバイスの設定方法は、CCCのドキュメントのこちらのセクションをご覧ください：

[複数のMac、またはソースボリュームを同じハードドライブにバックアップするには <http://bombich.com/ja/ja/kb/ccc5/i-want-back-up-multiple-macs-or-source-volumes-same-hard-drive>](#)
ビデオ：[macOS Catalinaにバックアップディスクを準備する <https://youtu.be/narMTq3d58>](#)

[“Macintosh HD”と“Macintosh HD - Data”にそれぞれ別のバックアップタスクを作成する必要がありますか？](#)

いいえ。起動ディスク（例：Macintosh HD）をバックアップタスクのソースとして選択している場合、CCCはそのボリュームグループにある両方のボリュームを自動的にバックアップします。

[CCCからバックアップディスクのパーティション方式が間違っていると報告がありました。どうすればいいですか？](#)

外部ハードドライブの多くはWindows中心のフォーマットとパーティション方式で出荷されます。そのパーティション方式は、AppleのAPFSファイルシステムに対応できないので、お使いのバックアップディスクを使ってCatalinaの起動ディスクの起動可能なバックアップを作成する前に、バックアップディスクが正しいパーティション方式でパーティションされているか確認してください。CCCドキュメントのこのセクションはバックアップディスクの設定方法をステップバイステップで説明します:

ハードドライブをCarbon Copy Clonerとの使用に準備するには <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x#highsierra>>

この単純なタスクを実行するためのディスクユーティリティのインターフェースは、驚くなかれ、直感的ではありません。ここでは、プロセスの概要を、特に間違いやすい箇所に焦点を当てながら、説明します:

1. ディスクユーティリティを開きます
2. ディスクユーティリティの表示メニューから**すべてのデバイスを表示**を選択します。
これは非常に重要なステップです!
3. サイドバーにあるコピー先ボリュームの**親デバイス**を選択してください。バックアップボリューム自体ではなく、親デバイスをクリックしてください。もし親デバイスをクリックしないと、パーティション方式を変更できません。
4. ツールバーの**消去**
ボタンをクリックしてください。
“パーティション” ボタンをクリックしないでください
!!
明らかな選択のように見えますが、実際には“パーティション”のインターフェースでパーティション方式を変更することはできません。
5. 方式を GUID Partition Map に、フォーマットを APFSに設定してから、**消去**
ボタンをクリックしてください。

それでも、パーティション方式の変更に問題がある場合は、[このビデオ](https://youtu.be/narMTq3d58?t=86) <<https://youtu.be/narMTq3d58?t=86>> をご覧ください。

[CCCを最初に行うとき、CCCは起動可能なバックアップディスクに何をしますか？](#)

macOS Catalinaは起動ボリュームのボリュームグループを活用するので、起動可能なバックアップの作成にはAPFSフォーマットされたコピー先ボリュームが必要です。macOS

CCCはHFS+ フォーマットされたバックアップボリュームをAPFSに自動的に変換します

。そしてコピー先にボリュームグループを作成します。この変換はHigh SierraまたはMojaveにアップグレードした際、起動ディスクで起きた変換と同じものです。但し、1つ顕著な例外があります:CCCはコピー先を変換することを通知し、変換を拒否する機会を提供します。変換は非破壊的です。つまり、コピー先ボリュームにあるすべてのデータはそのまま残り、唯一変更されるのは、ボリュームのフォーマットのみです。

[コピー先ボリュームの変換を許可したくない理由があるとすれば何ですか？](#)

一般的に変換を拒否する理由はありません。変換は非破壊的で、システムのバックアップを作成するために必要です。バックアップボリュームがCCCのバックアップタスク専用になっている場合、コピー先をAPFSに変換するのは正しい選択です。

しかし、コピー先ボリュームがCCCのバックアップタスク専用ではない場合、または、macOSシステムファイルをバックアップするつもりがない場合、変換によってあなたのコピー先の他のユーザがどんな影響を受けるかを考える必要があります。例えば、Time Machineは現在コピー先としてAPFSと互換性がないので、Time Machineのバックアップを含むコピー先ボリュームを変換すると、Time Machineのバックアップを壊すことになります。CCCは特にTime Machineのバックアップボリュームの変換を回避します。別例としては、**起動ディスクから1つのフォルダ、または、ほんの数個のフォルダのみをバックアップする場合、フォルダからフォルダのバックアップを設定** <<http://bombich.com/ja/ja/kb/ccc5/folder-folder-backups>> する必要があります。この場合、コピー先を変換する必要はありません。

また、**コピー先デバイスが、回転数の少ない2.5インチハードディスクドライブ (HDD) の場合**、例えば、回転数が5400RPM

(または、それ以下!)の場合、変換を避けるべきです。APFSはHDDデバイスではうまく動作しません

<<http://bombich.com/ja/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>>

。そればかりか、それらのシークパフォーマンスはずっと遅いため、そのパフォーマンスはこれらの非常に遅いHDDデバイスでは受け付けられません。これらの遅いディスクは、Mac OS

拡張、ジャーナリングと

してフォーマットしたままにしてください。これらのデバイスは**データのみバックアップ**に向いていますが、

起動可能なバックアップを作成するためには、SSD <<http://bombich.com/ja/ja/kb/ccc5/choosing-backup-drive#recommendations>>を取得する必要があります。

Catalinaのバックアップボリュームのルートに他のデータを残しておけますか？

いいえ。特に、Finderを使ってCatalinaのバックアップディスクのルートレベルに項目をコピーするべきではありません。Finderはそのデータをグループ内のシステムボリュームにコピーします。そして、いずれそのシステムボリュームがアップデートされると、すべての非システムファイルがそのシステムボリュームから完全に削除される可能性があります。他の項目をシステムのバックアップに関連のないバックアップディスクに保管したい場合は、その目的のために別のボリュームをそのディスクに作成してください(手順は以下の質問を参照してください)。

コピー先にすでに他のものがあります。そのコンテンツに影響を与えないようにするにはどうすればいいですか？

ビデオ:複数のソースをAPFSフォーマットされた1つのデバイスにバックアップするには
<<https://youtu.be/MXHNeCHnpnl>>

お使いのコピー先ボリュームがすでにAPFSフォーマットされているが、そのボリュームに 起動可能なバックアップを作成したくない場合、単純に、新しいボリュームを既存のAPFSコンテナに追加できます:

1. ディスクユーティリティを開きます
2. ディスクユーティリティのサイドバーにあるコピー先ディスクを選択します
3. ツールバーの “ + ” ボタンをクリックしてください

お使いのコピー先ボリュームがAPFSフォーマットされていなくて、そのボリュームをAPFSに変換できない、または変換したくない場合には、コピー先ディスクにCCCが使用するための専用パーティションを作成できます。パーティションを作成するには:

1. ディスクユーティリティを開きます
2. ディスクユーティリティのサイドバーにあるコピー先ディスクを選択します
3. ツールバーの “ パーティション ” ボタンをクリックしてください
4. “ + ” をクリックして、ディスクにパーティションを追加します
5. パーティションの名前とサイズを環境設定に指定します
6. APFSをフォーマットとして選択します
7. “ 適用 ” ボタンをクリックしてください

コピー先のルートに別のものがありましたが、見つかりません。どうすれば見つけられますか？

起動ディスクにないバックアップディスクのルートレベルに他のデータを残している場合、そのデータはまだお使いのバックアップディスクにあります。しかし、Catalinaの起動ディスクのバックアップに適用されるボリュームグループの変更のために、Finderで見つけるのがより難しくなります。もしお使いのバックアップディスクが“CC C Backup (CCCバックアップ)”という名前であれば、CCCのサイドバーで“CCC Backup - Data”ボリュームを右クリックして、“Finderで表示”を選択すると、そのコンテンツを表示できます。

ビデオ:複数のソースをAPFSフォーマットされた1つのデバイスにバックアップするには
<<https://youtu.be/MXHNeCHnpnl>>

[変換処理に要する時間はどれくらいですか？](#)

それは、お使いのコピー先ボリュームにどれくらいデータがあるか、コピー先のデバイスのパフォーマンス、およびコピー先ボリュームがどの程度断片化されているかによります。しばらく時間がかかる可能性がありますが、CCCは変換が完了するまで2時間以上待つことはありません。2時間以上かかる場合には、CCCはコピー先ボリュームを消去するよう推奨します。そうすることで、ファイルシステムの断片化によって直接引き起こされているパフォーマンスの問題を解決することができます。CCCからこの推奨が提示されても、ボリュームを消去しないで変換を完了させたい場合には、代わってディスクユーティリティのボリュームを変換してください(このオプションは“編集”メニューにあります)。

[私の暗号化されたバックアップボリュームは自動的にAPFSボリュームグループに変換されますか？](#)

残念ながら、[ディスクユーティリティは暗号化されたボリュームをAPFSボリュームグループに追加できない](#)
<<http://bombich.com/ja/ja/kb/ccc5/mac-os-catalina-known-issues#diskutiladdvolumeencryption>>
という、macOSの制限のためにそれは不可能です。Catalina以降の起動ディスクをソースとして、暗号化されたボリュームをコピー先として選択する場合、CCCはその選択を許可しないで、コピー先ボリュームを消去、または暗号解除することを提案します。

最も早く簡単な解決法:コピー先をAPFS (非暗号化) として消去する

Catalinaのバックアップを再開するには、コピー先ボリュームを消去するのがもっともシンプルで手っ取り早い方法です。その詳しい手順はこちらに表示されています:[ハードドライブをCarbon Copy Clonerとの使用に準備するには](#) <<http://bombich.com/ja/ja/kb/ccc5/preparing-your-backup-disk-backup-os-x#highsierra>>。

バックアップタスクを非暗号化されたボリュームに実行した後、そのバックアップから起動して、環境設定の“セキュリティとプライバシー”からFileVaultを再度有効にできます。

関連ドキュメント

- コピー先ボリュームを消去ではなく、一時的に暗号解除できますか? <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#conversionencrypteddecrypt>>
- HFS+フォーマットのボリューム、または、APFS暗号化されたボリュームに起動可能でないバックアップを作成できますか? <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable>>
- FileVault暗号化で作業するには <<http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption>>
- バックアップボリュームの暗号化についてのよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>>

[コピー先ボリュームを消去ではなく、一時的に暗号解除できますか?](#)

コピー先ボリュームを暗号解除するには、かなりの時間(数日かかる可能性もあります)と努力が必要ですが、以下のいずれかの方法でコピー先ボリュームを暗号解除できます。

A:バックアップボリュームから起動して、環境設定の“セキュリティ”を開き、FileVaultを無効にする

B:アプリケーション“ターミナル”でボリュームを暗号解除する。例、HFS+フォーマットされたコピー先には:
`diskutil cs decryptVolume "/Volumes/CCC Backup"`

または、APFSフォーマットされたコピー先のために、暗号化されたボリュームと関連のあるユーザIDのリストを入手してから、最初のコマンドの出力からの"Open Directoryローカルユーザ" UUIDの1つを2番目のコマンドと使用してください:

```
diskutil ap listUsers "/Volumes/CCC Backup"
```

```
diskutil ap decryptVolume "/Volumes/CCC Backup" -user B44348A3-68DF-4B7B-800D-47FE38711178
```

"B44348A3-68DF-4B7B-800D-47FE38711178"を最初のコマンドで生成されるUUIDに置き換えてください。

暗号解除が完了するのを待ってください

暗号解除処理が完了するのを待ってから、バックアップタスクに進んでください。システムの起動ディスクから起動されている間、暗号解除はバックグラウンドで続きます。macOSは変換の進行状況を確認できるような方法を提供していませんが、ターミナルアプリケーションで`diskutil apfs list` (または、該当するボリュームがHFS+フォーマットの場合は`diskutil cs list`)

と入力すると、変換の進行状況を確認できます。

CatalinaバックアップボリュームでFileVaultを再度有効にするには

バックアップタスクを非暗号化されたボリュームに実行した後、そのバックアップから起動して、環境設定の“セキュリティとプライバシー”からFileVaultを再度有効にできます。

関連ドキュメント

- HFS+フォーマットのボリューム、または、APFS暗号化されたボリュームに起動可能でないバックアップを作成できますか？ <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina#encryptednonbootable>>
- FileVault暗号化で作業するには <<http://bombich.com/ja/ja/kb/ccc5/working-filevault-encryption>>
- バックアップボリュームの暗号化についてのよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-encrypting-backup-volume>>
- Catalinaに関する周知問題:Appleのボリュームグループのは操作ツールは暗号化されたボリュームと動作しない <<http://bombich.com/ja/ja/kb/ccc5/macos-catalina-known-issues#diskutiladdvolumeencryption>>

[コピー先を暗号解除または消去して、その後再度有効にした場合、今後のバックアップでこれをやり直す必要がありますか？](#)

いいえ。これはCCCがコピー先ボリュームにmacOS Catalinaに必要な調整を加えられるようにするための1度限りのタスクです。Catalinaのバックアップを一旦確立してしまうと、FileVaultを再度有効にでき、その後のバックアップは介入を追加することなく動作します。

[HFS+フォーマットのボリューム、または、APFS暗号化されたボリュームに起動可能でないバックアップを作成できますか？](#)

macOS Catalinaの起動ディスクの起動可能なバックアップを作成することを意図的に控える場合は、起動ディスクのデータボリュームのみをバックアップするようにバックアップタスクを設定できます:

1. CCCを開いて、CCCのツールバーから“サイドバーを表示”をクリックします（まだ表示されていない場合）

2. サイドバーからバックアップタスクを選択します
3. CCCのサイドバーからソースセレクトに “ Macintosh HD - Data ” をドラッグします
4. タスクを保存

この設定をすると、CCCはコピー先ボリュームのフォーマット、または暗号化の条件を特に問いません。このコピー先は起動可能でないため、このボリュームが提供する機能性についての不明確さを避けるために、すべての既存のシステムフォルダをコピー先ボリュームから削除することをお勧めします。

お使いのバックアップディスクが “ モバイル ” 向けの2.5インチ回転式デバイスの場合 (例：回転数が5400RPMか、それ以下)、そのデバイスを “ Mac OS 拡張、ジャーナリング ” (別名：HFS+) としてフォーマットし、データのみのバックアップに使用することをお勧めします。

APFSはこれらのデバイスでは、受け付けられないパフォーマンスを提供します

<<http://bombich.com/ja/blog/2019/09/12/analysis-apfs-enumeration-performance-on-rotational-hard-drives>>

ので、起動可能なバックアップのためにこれらのデバイスを推奨できないだけでなく、サポートすることもできません。

[CCCはシステムボリュームをコピーしていましたが、2度目にはすべてをコピーし始めました。これは正常なことですか？](#)

はい。お使いのCatalinaの起動ディスクには2つの異なるボリュームがあります。1つは読み込み限定のシステムボリューム、もう1つはすべてのデータが残されている書き込み可能なデータボリュームです。システムボリュームには約10GBのコンテンツがあり、CCCはまずそれをバックアップします。CCCがシステムボリュームのコピーを終了すると、CCCはデータボリュームのコンテンツのバックアップに進みます。システムボリュームはmacOSアップデートを適用した場合のみ変更されます。しかし、このボリュームが頻繁にコピーされるのを見ることはないでしょう。CCCはソースのシステムボリュームが変更された場合のみ、コピー先のシステムボリュームをアップデートします。

[CCCがバックアップディスクに適用したボリュームグループの変更内容を取り消すことができますか？](#)

このチュートリアルビデオをYouTubeでご覧ください <<https://youtu.be/MXHNeCHnpnl>>

はい。ディスクユーティリティでボリュームグループをバラバラにすることができます。例えば、起動ディスクを

バックアップタスク専用にしていないボリュームにクローンした場合、この操作をしたいと思うかもしれません。手順は比較的シンプルです。単純にシステムボリュームを削除し、次にデータボリュームの名前を変更し、最後にボリュームをマウントし直すだけです。バックアップディスクの名前を“CCC バックアップ”としていたら、以下の手順を実行してください:

1. ディスクユーティリティを開きます
2. 表示メニューから**すべてのデバイスを表示**を選択します
3. サイドバーの**CCC バックアップ**
ボリュームを選択してください。これはグループ内のシステムボリュームです。
4. ツールバーの **—** ボタンをクリックして、そのボリュームを削除してください
5. **CCC バックアップ - データ** ボリュームを選択します
6. ツールバーの **マウント解除** ボタンをクリックしてください
7. ツールバーの **マウント** ボタンをクリックして、そのボリュームをマウントし直してください
8. そのボリュームの名前を **CCC バックアップ** に戻してください

[コピー先のCCC SafetyNetフォルダはどこにありますか？](#)

そのボリュームでスナップショットのサポートをオンにしている場合、古い(レガシー)CCC SafetyNetフォルダをコピー先で見つけることはできません <<http://bombich.com/ja/ja/kb/ccc5/legacy-safetynet-folder-not-used-when-snapshots-are-enabled-on-destination>>

。代わりに、CCCのサイドバーからコピー先のデータボリュームを選択すると、SafetyNetのスナップショットの一覧が表示されます。

コピー先ボリュームでスナップショットのサポートが有効になっていない場合は、SafetyNetフォルダをFinderで操作するのは難しくなります。それはまだコピー先のデータボリュームのルートレベルにあります。データボリュームはデフォルトでFinder内に隠れています。Finderでそれを表示するには、CCCのコピー先セクタをクリックして、**データボリュームを表示**のオプションを選択してください。

[“場所が変更された項目”にあるSafetyNetフォルダを削除できません。Finderは、それらが使用中であると報告します。](#)

CCCのバックアップから起動中にコンテンツをシステムの起動ディスクに復元したことがある場合、CCC SafetyNetフォルダがそのボリュームのルートレベルにあった可能性があります。Catalinaにアップグレードすると、ma

cOSインストーラーは起動ディスクのルートにあるすべてのコンテンツの場所を “ ユーザ > 共有 > 場所が変更された項目 > セキュリティ ” に移動します。そのフォルダには、コンテンツがそちらに移動された理由を説明するPDFもあります。手短かに言うと、コンテンツが移動されたのは、macOS Catalinaの起動ディスクのデータボリュームのルートレベルにあるコンテンツを見つけるのが非常に難しいからです。

そのSafetyNetフォルダの削除を試みる (そしておそらくそのフォルダを削除 **したい**)

場合、Finderは、項目のいくつかが使用中のためフォルダを削除できませんと — **誤まった** — 報告をすることがあります。実際そのフォルダ内で使用中のものは何もありませんが、古いシステムの項目のいくつかは “ システム整合性保護 ” で保護されている可能性があります。そのコンテンツの処分方法はCCCドキュメントの以下のセクションをご覧ください:

SafetyNetフォルダから削除できない項目があります。なぜですか? Finderから、いくつかの項目を使用中です、と報告されます。 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-carbon-copy-cloner-safetynet#sippreventsdelete>>

CCCとmacOS 11についてによくある質問

macOS Big Surの発表に伴い、AppleはMac OS X (10) を廃止し、macOS 11をその代替としました。数値の違いが示すように、これはAppleが約20年前にMac OS Xを導入して以来、macOSへの最大の変化です。新しく、システムは暗号で封印された**"署名付きのシステムボリューム"** <<https://developer.apple.com/news/?id=3xpv8r2m>>にあります。その封印はAppleだけが適用でき、システムボリュームの通常のコピーはAppleのシールがないと起動可能にはなりません。macOS 11のシステムボリュームの機能するコピーを作成するには、Appleのツールを使用してシステムをコピーするか、またはバックアップにmacOSをインストールする必要があります。

起動可能なバックアップはmacOS Big Surでどう異なりますか？

CCCはAppleのAPFS複製ユーティリティ ("ASR ") を使って、起動ディスクの初期の起動可能なクローンを確立します。このユーティリティには、これまでの古いIOSにおいてCCCで慣れ親しんだほどの柔軟性がありません。特に、このユーティリティはコピー先が消去されること、およびすべてがソースからコピー先にコピーされることを要求します。Big Surで起動ディスクの新しいバックアップを設定する際、CCCはいくつかのオプションを提供します。オプションは、お使いのコピー先デバイスのサイズと使用中のフォーマットによって異なります：

- 起動可能なクローンを作成するために、CCCがコピー先を消去することを許可する
- 新しい、専用のバックアップボリュームを既存のAPFSコピー先に追加する (十分な空きスペースがある場合)
- Dataボリュームのバックアップで続ける (これはお使いのデータ、アプリケーション、およびシステム設定の完全なバックアップです)

これらのオプションの詳細、および初めて“フルボリュームのクローン”を実行する際に気を付けることについては、[macOSのシステムボリュームをApple Software Restoreを使ってクローンするには](http://bombich.com/ja/ja/kb/ccc5/cloning-macos-system-volumes-apple-software-restore) <<http://bombich.com/ja/ja/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>>を参照してください。

CCCのバックアップからデータを復元するには、CCCのバックアップは起動可能である必要がありますか？

いいえ。起動可能であることは、起動ディスクに問題が起きた場合に作業を継続できるという利便性がありますが、CCCのバックアップからデータを復元するためには必須ではありません。CCCを使ってシステムの起動ディスクから起動中、個々のフォルダと古いバージョンのファイル (例：スナップショットからの) を復元できます。また、CCCのバックアップは移行アシスタントと互換性があるので、移行アシスタントを使って、すべてのデータをmacOSのクリーンなインストール (例：置換ディスクの) に復元できます。

CCCは初期の起動可能なバックアップを確立した後、コピー先のシステムボリュームを最新の状態に保持しますか？

いいえ。この機能を提供したいと考えていますが、そうするには、ほとんどのユーザにとって受け入れ難いと思われるトレードオフが伴います。[AppleのAPFS 複製ユーティリティ \(ASR\) の柔軟性が不足](http://bombich.com/ja/ja/kb/ccc5/mac-os-big-sur-known-issues#asrvolumegroup) <<http://bombich.com/ja/ja/kb/ccc5/mac-os-big-sur-known-issues#asrvolumegroup>>しているために、ASRを使ってシステムとDataボリュームを両方一緒にクローンすることで、コピー先のシステムボリュームのみをアップデートできます。そして、それには、コピー先を消去することが含まれます。そうすることで、コピー先のすべてのスナップショットが削除され、通常のインクリメンタルなバックアップよりもかなり時間がかかることとなります。

幸い、コピー先でシステムボリュームをアップデートすることは、それほど頻繁にする必要も、前もってする必要もありません。必要な場合と必要なタイミングで実行できます。シンプルに、バックアップボリュームからMacを起動し、システム環境設定の“ソフトウェアアップデート”からすべてのアップデートを適用できます。この操作は、バックアップから復元する必要が起きるまで延期することもできます。

私のCatalina (または、それ以前) のバックアップをBig Surにアップグレードするにはどうすればいいですか?

MacをBig Surにアップグレード後、かつまちがいなくBig Sur OSを使用すると決めた後

<http://bombich.com/ja/ja/kb/ccc5/best-practices-updating-your-macs-os#commit>

に初めて、起動ディスクのバックアップをCCCのバックアップボリュームに再開してください。CCCを開き、それぞれのバックアップタスクを確認して、新しいOSで最初のバックアップをするために何か調整が必要かどうかを確かめてください。

関連リソース

- macOSのシステムボリュームをApple Software Restoreを使ってクローンするには
<<http://bombich.com/ja/ja/kb/ccc5/cloning-macos-system-volumes-apple-software-restore>>
- 起動可能なバックアップから復元するには <<http://bombich.com/ja/ja/kb/ccc5/how-restore-from-your-backup>>
- スナップショットから復元するには <<http://bombich.com/ja/ja/kb/ccc5/leveraging-snapshots-on-apfs-volumes#restore>>
- 移行アシスタントを使ってデータのみのバックアップからデータを移行するには
<<http://bombich.com/ja/ja/kb/ccc5/creating-and-restoring-data-only-backups#migrate>>
- CCCとmacOS Catalinaについてよくある質問 <<http://bombich.com/ja/ja/kb/ccc5/frequently-asked-questions-about-ccc-and-macos-catalina>> (これらの多くはmacOS Big Surにも適用できます)
- Mac OSをアップデートするための最善策 <<http://bombich.com/ja/ja/kb/ccc5/best-practices-updating-your-macs-os>>
- macOS Big Surに関する周知の問題 <<http://bombich.com/ja/ja/kb/ccc5/macos-big-sur-known-issues>>