

TRUECRYPT

FREE OPEN-SOURCE ON-THE-FLY ENCRYPTION

USER'S GUIDE

www.truecrypt.org

バージョン情報

TrueCrypt User's Guide, version 6.1a. 2008年12月1日発行

ライセンスと特許情報

TrueCrypt をインストールする、動作させる、複製、再配布、もしくは改変することにより、あなたはバイナリおよびソースコードの配布パッケージに含まれている **Licence.txt** に書かれているライセンスに記載されたすべての条項、責任と義務を受け入れたことになります。

著作権情報

全体としてのこのソフトウェア:

Copyright © 2008 TrueCrypt Foundation. All rights reserved.

このソフトウェアの一部:

Copyright © 2003-2008 TrueCrypt Foundation. All rights reserved.

Copyright © 1998-2000 Paul Le Roux. All rights reserved.

Copyright © 1998-2008 Brian Gladman, Worcester, UK. All rights reserved.

Copyright © 2002-2004 Mark Adler. All rights reserved.

詳細情報については、ソースコードに添付された法定の通知を見てください。

商標情報

TrueCrypt と TrueCrypt のロゴは TrueCrypt Foundation の商標です。

注意 : 名称や製品を金銭化することが目的ではありませんが、TrueCrypt の評判を守り同名あるいは似た名称の製品の存在が引き起こすサポートやその他の問題発生を防止するためです。TrueCrypt は商標ではありませんが、TrueCrypt は今後もオープンソースのフリーソフトウェアでありつづけるでしょう。

その他の商標は、すべてそれぞれ個々の所有者のものです。

制限

TrueCrypt Foundation は、このドキュメントがあなたの要求に合っているとか、情報に誤りがないとかを保証しません。

目次

はじめに.....	6
初心者のためのチュートリアル.....	8
TrueCrypt コンテナの作り方と使い方.....	8
TrueCrypt パーティション/デバイスの作り方と使い方.....	30
みせかけの拒否.....	32
隠しボリューム.....	33
隠しボリュームを破損から守る.....	35
隠しボリュームの安全に関する予防策.....	40
隠し OS.....	44
隠し OS 作成手順.....	46
みせかけの拒否とデータ漏洩防御.....	47
単一ドライブに二つの TrueCrypt パーティションがあることの説明のしかた.....	47
隠し OS の安全に関する予防策.....	50
システム暗号化.....	51
システム暗号化ができる OS.....	51
TrueCrypt レスキューディスク.....	52
隠し OS.....	54
TRUECRYPT ボリューム.....	55
新規 TRUECRYPT ボリュームの作成.....	55
ハッシュアルゴリズム.....	55
暗号化アルゴリズム.....	56
クイックフォーマット.....	57
ダイナミック.....	57
クラスタのサイズ.....	57
CD や DVD にある TrueCrypt ボリューム.....	58
ハードウェア/ソフトウェア・レイドと Windows ダイナミックボリューム.....	58
ボリューム作成に関する追加情報.....	58
メインプログラムウィンドウ.....	60
ファイルの選択.....	60
デバイスの選択.....	60
マウント.....	60
デバイスの自動マウント.....	60
アンマウント.....	61
すべてアンマウント.....	61
記憶したパスワードの消去.....	61

履歴を保存しない.....	61
終了.....	61
ボリュームツール.....	63
プログラムメニュー.....	64
ボリューム -> デバイスのボリュームをすべて自動でマウント.....	64
ボリューム -> 現在マウントされているボリュームをお気に入りに保存.....	64
ボリューム -> お気に入りボリュームをマウント.....	64
ボリューム -> ヘッダーキー導出アルゴリズムの設定.....	64
ボリューム -> ボリュームのパスワードを変更する.....	65
システム-> パスワードの変更.....	65
システム -> 起動前認証をせずにマウントする.....	66
ツール -> ボリューム履歴を消去.....	66
ツール -> トラベラーディスクセットアップ.....	66
ツール -> キーファイル生成.....	66
ツール -> ボリュームヘッダーのバックアップ.....	66
ツール -> ボリュームヘッダーのリストア.....	66
設定 -> 各種設定.....	68
TRUECRYPT ボリュームのマウント.....	70
パスワードをドライバのメモリーに記憶する.....	70
マウントオプション.....	70
ホットキー.....	72
キーファイル.....	72
キーファイルダイアログウィンドウ.....	74
セキュリティトークンとスマートカード.....	74
キーファイル検索パス.....	75
空のパスワードとキーファイル.....	76
簡易選択.....	76
キーファイル -> ボリュームへのキーファイルの追加/削除.....	76
キーファイル -> ボリュームから全てのキーファイルを除去.....	76
キーファイル -> ランダムキーファイルの生成.....	77
キーファイル -> デフォルトキーファイル/フォルダの設定.....	77
セキュリティトークンとスマートカード.....	78
トラベラーモード.....	79
ツール -> トラベラーディスクのセットアップ.....	79
TRUECRYPT を管理者権限なしで使う.....	81
TRUECRYPT の常駐.....	81
言語パック.....	82

インストール	82
暗号化アルゴリズム.....	83
AES.....	83
Serpent.....	84
Twofish.....	84
AES-Twofish.....	84
AES-Twofish-Serpent.....	84
Serpent-AES.....	85
Serpent-Twofish-AES.....	85
Twofish-Serpent.....	85
ハッシュアルゴリズム.....	86
RIPEMD-160.....	86
SHA-512.....	86
Whirlpool.....	86
動作対象 OS.....	87
コマンドラインの使い方.....	88
文法.....	91
使用例.....	91
ネットワーク間の共有.....	92
安全のための予防策.....	93
ページングファイル.....	93
ハイバネーションファイル.....	94
メモリダンプファイル.....	94
マルチユーザー環境.....	95
RAMにある暗号化されていないデータ.....	95
パスワードとキーファイルの変更.....	96
データの漏洩.....	96
Windows レジストリ.....	97
ウェアレベリング.....	97
セクターの再配置.....	98
デフラグ.....	98
ジャーナリングファイルシステム.....	98
安全なバックアップのとり方.....	100
非システムボリューム.....	100
システムパーティション.....	101
一般的注意事項.....	102
問題が起こったら.....	103

非互換性.....	107
既知の問題と制限.....	108
既知の問題.....	108
制限.....	108
よくある質問(FAQ)と答え.....	110
暗号化を解除するには.....	122
TRUECRYPT のアンインストール.....	123
TRUECRYPT システムファイルとアプリケーションデータ.....	123
技術解説.....	125
表記法.....	125
暗号化の仕組み.....	126
動作モード.....	127
ヘッダーキーの導出、ソルト、および反復回数.....	129
乱数発生機構.....	130
キーファイル.....	132
TRUECRYPT ボリュームフォーマット仕様.....	135
準拠規格.....	138
ソースコード	138
今後の開発予定.....	139
ライセンス.....	139
連絡先.....	139
バージョン履歴.....	140
謝辞.....	142
参考文献	143

まえがき

この文書のほとんどの章はほぼすべてのバージョンのTrueCryptに対応していますが、いくつかの節では基本的にWindows版TrueCryptユーザーを対象としていることに注意してください。そのため、それらの節ではいくつかの箇所にMac OS X版やLinux版には適切ではない情報があるかもしれません。

はじめに

TrueCryptは自動即時暗号化するボリューム(データ保存装置)の、作成と維持についてのソフトウェアです。自動即時暗号化(on-the-fly-encryption)というのは、データが読み出したり保存の直前にユーザーの介在なしに自動的に暗号化されるということです。暗号化されたボリュームのデータは、正しいパスワード/キーファイルまたは暗号化キーがなければ、読むことはできません。ファイルシステム全体(ファイル名、ディレクトリ名、空き領域、メタデータ他)が暗号化されます。

ファイルは通常のディスクと同じにマウントされたTrueCryptボリュームから、またはそのボリュームへコピー(たとえば、単純なドラッグ・アンド・ドロップ操作でも可能)することができます。ファイルは暗号化されたTrueCryptボリュームから読み込まれたりコピーされたりするつど(メモリー中で)即時に自動的に復号されます。同様に、ファイルはTrueCryptボリュームに書き込む直前に即時に自動的にRAMで暗号化されます。ただし、このことは暗号化されるまたは復号されるファイル全体がRAM中に存在しなければならないということではありません。TrueCryptには特別なメモリー(RAM)の必要はありません。これがどのように実行されるかは、以下を参照してください。

.avi ビデオファイルがTrueCryptボリュームに保存されている(つまり、ビデオファイルはまるごと暗号化されている)とします。ユーザーは正しいパスワードまたはキーファイルによってTrueCryptボリュームをマウント(オープン)します。ユーザーがビデオファイルのアイコンをダブルクリックすると、OSはそのファイルタイプに関連づけられたアプリケーション(通常はメディアプレーヤー)を起動します。メディアプレーヤーは再生するためにビデオファイルの最初の一部分をTrueCrypt暗号化ボリュームからRAM(メモリー)へと読み込み始めます。この一部分が読み込まれるときにTrueCryptは自動的に(RAMに)それを復号します。復号されたビデオの一部分はメディアプレーヤーで再生されます。この一部分が再生されているときに、メディアプレーヤーはTrueCrypt暗号化ボリュームからビデオファイルの次の一部分をRAM(メモリー)へと読み込み、この過程がくりかえされます。この過程を自動即時(オン・ザ・フライ)暗号化/復号と呼び、ビデオファイルだけでなくすべてのファイルタイプについて機能します。

TrueCryptは絶対に復号されたデータをディスクには置きません。一時的にRAM(メモリー)に置くだけです。ボリュームがマウントされていても、そのボリュームに保存されているデータは暗号化されたままです。Windowsを再起動したりPCの電源を切ったりすると、ボリュームはアンマウントされそこに保存されたファイルは暗号化された状態で、アクセス不能となります。正しいシャットダウン手順なしで電源供給が突然遮断されたとしても、そのボリュームに保存されたファイルは暗号化された状態で、アクセス不能となります。ふたたびアクセス可能にするには、正

しいパスワードやキーファイルを使ってボリュームをマウントする必要があります。

初心者のためのチュートリアル

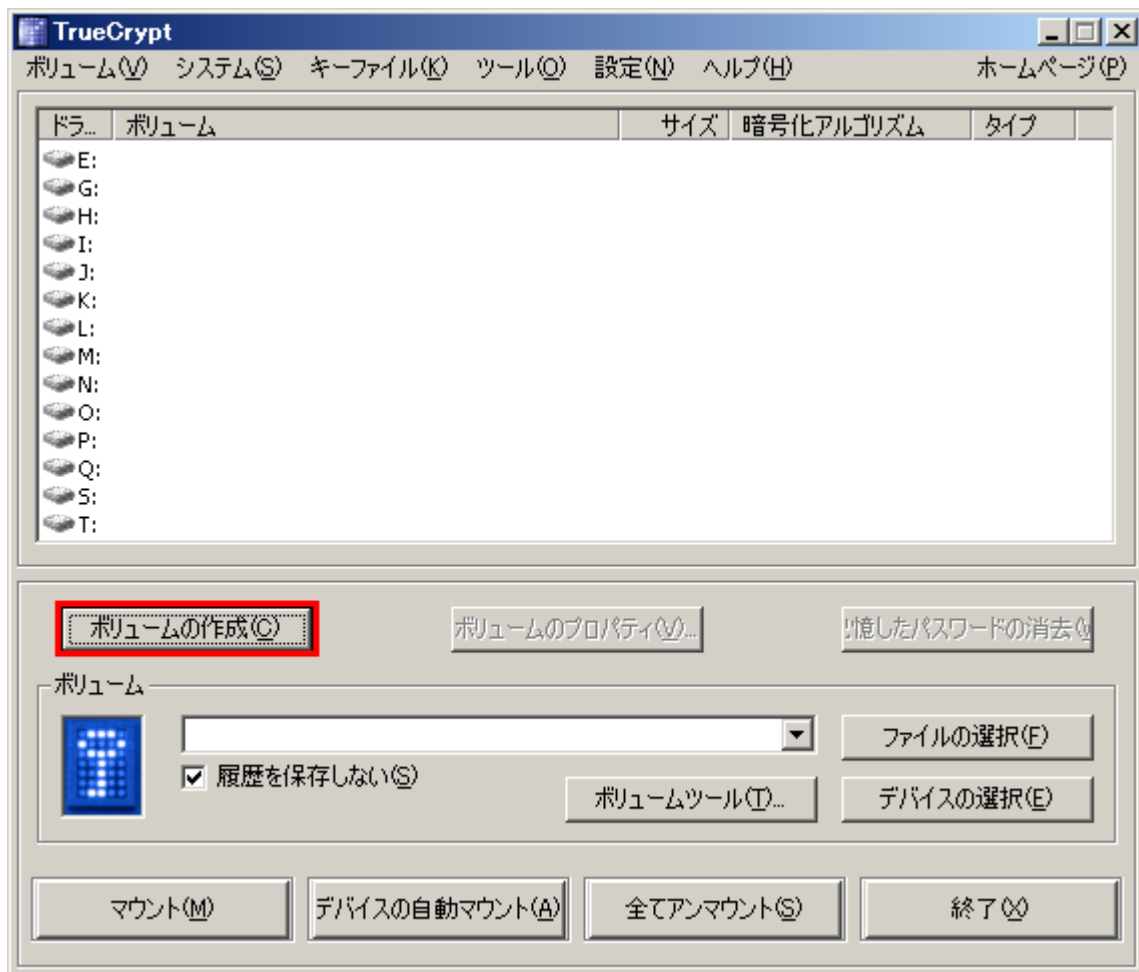
TrueCrypt コンテナの作り方と使い方

この章では TrueCrypt ボリュームの作り方、マウントのしかたと使い方を順を追って説明します。なお、他の章にも重要な情報が記載されているので、それらもぜひお読みください。

ステップ 1:

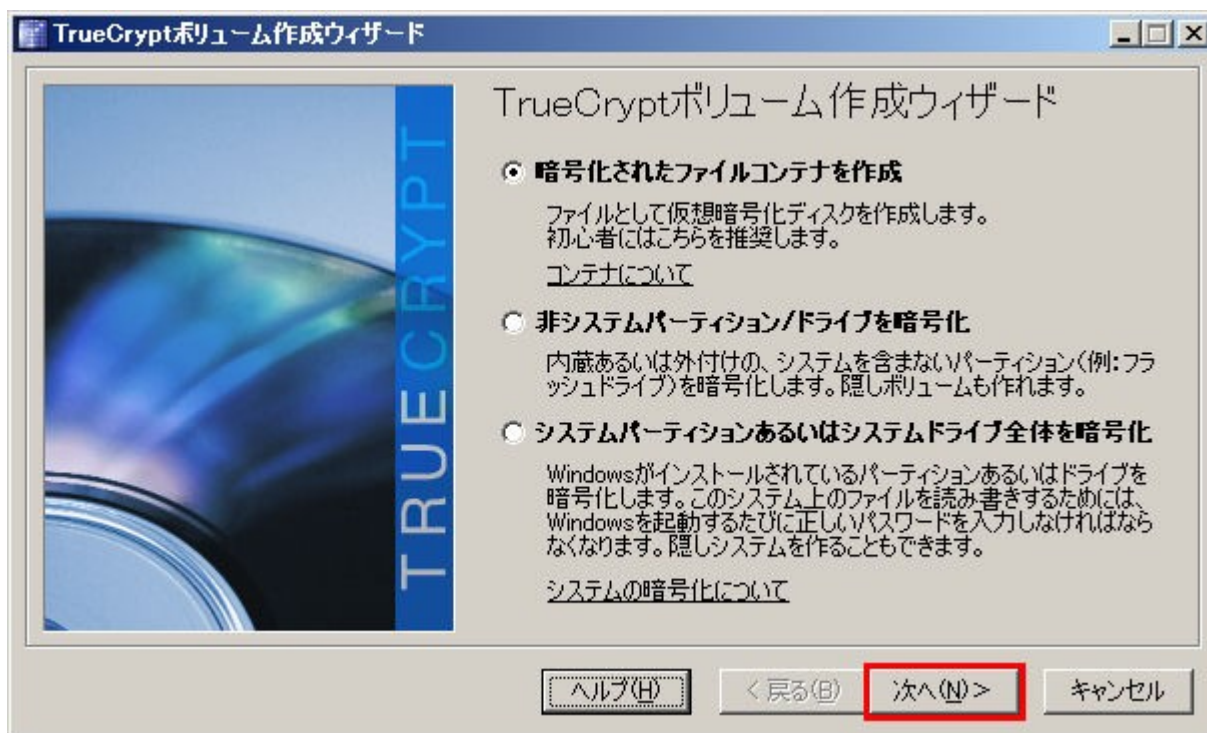
まず TrueCrypt をダウンロードし、インストールしてください。それから TrueCrypt.exe をダブルクリックするか Windows スタートメニューの TrueCrypt ショートカットをクリックして起動してください。

ステップ 2:



TrueCrypt のメインウィンドウが表示されます。「ボリュームの作成」をクリックしてください。
(赤で囲われている部分)

ステップ 3:



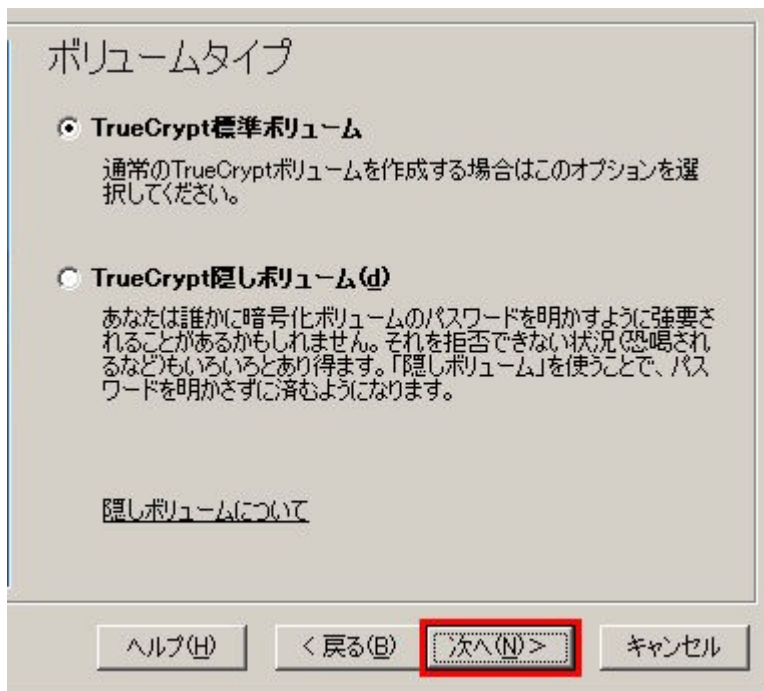
「TrueCrypt ボリューム作成ウィザード」ウィンドウが表示されます。

このステップでは、どこに TrueCrypt ボリュームを作成するかを決める必要があります。TrueCrypt ボリュームはファイル(この形態をコンテナと呼びます)として作成したり、パーティションやドライブにしたりすることができます。このチュートリアルでは最初のオプションを選択し、ファイルに TrueCrypt ボリュームをつくることとします。

オプションはデフォルトのままでいいので、あなたは「次へ」をクリックするだけです。

注意: 以降のステップではウィザードウィンドウの右側だけを掲載します。

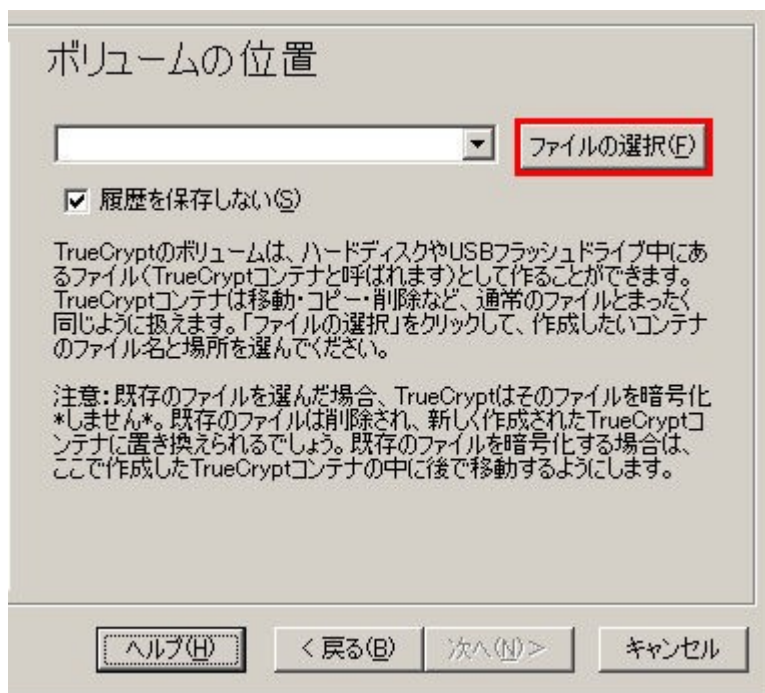
ステップ 4:



このステップでは、TrueCrypt 標準ボリュームを作成するか TrueCrypt 隠しボリュームを作るかを選択する必要があります。このチュートリアルでは上のオプションを選び、TrueCrypt 標準ボリュームを作ることとします。

そのオプションがデフォルトで選択されているので、そのまま「次へ」をクリックするだけです。

ステップ 5:

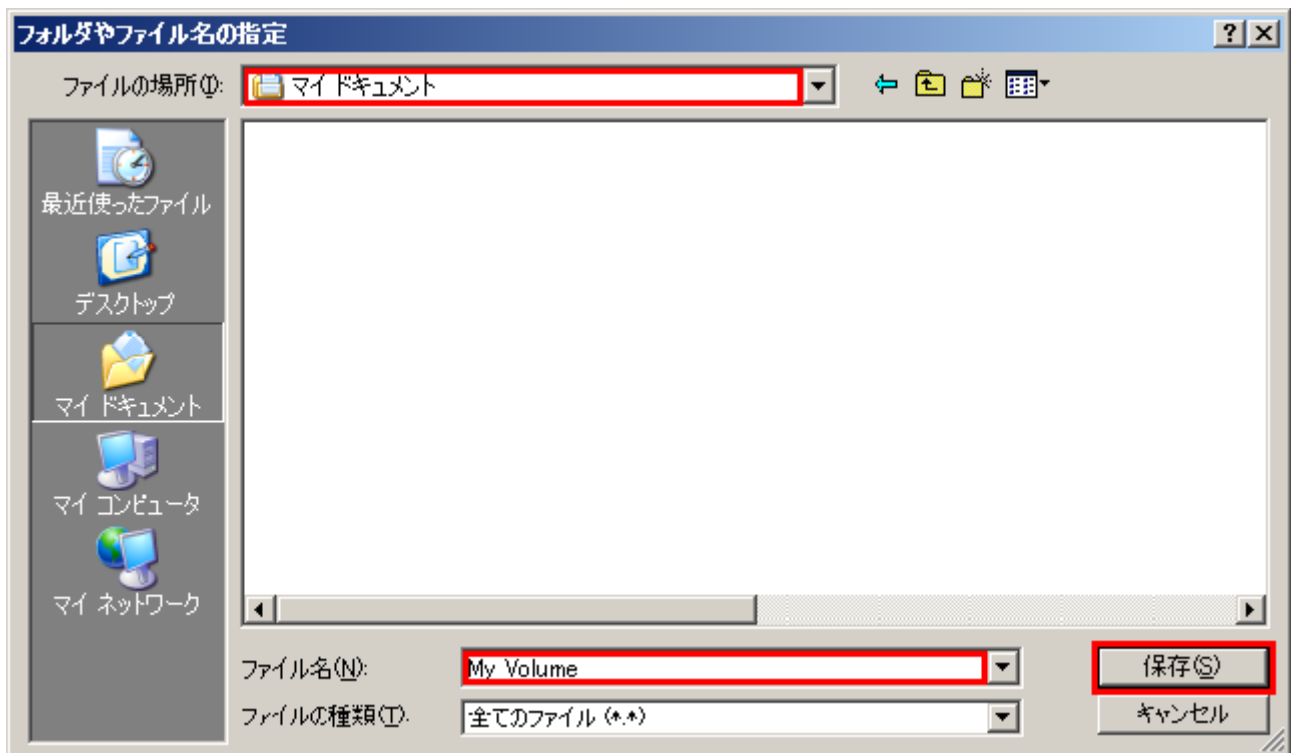


このステップでは、TrueCrypt ボリューム(ファイルコンテナ)をどこに作るのかを決めます。TrueCrypt コンテナは通常ファイルとまったく同じであることに留意してください。したがって、普通のファイルと同様に移動、コピー、削除ができます。また、次のステップで説明するようにファイル名を必要とします。

「ファイルの選択」をクリックしてください。

Windows の標準的なファイル選択ダイアログが表示されます。(TrueCrypt ボリューム作成ウィザードは背景に開いたままです)

ステップ 6:



このチュートリアルでは TrueCrypt ボリュームを上でのスクリーンショットのとおり *D:\My Documents¥* に置くこととし、ボリューム(コンテナ)のファイル名を(上のスクリーンショットのとおり) *My Volume* とします。もちろん、他のファイル名、他の場所(たとえば USB メモリ)、にすることができます。

この時点ではまだ *My Volume* は存在しません。—TrueCrypt がこれから作成します。

重要 : TrueCrypt は既存のファイルを暗号化するのではないことに注意してください。 既存のファイルを選択すると、それは新しく生成されるボリュームで上書きされます。(つまり、元ファイルは暗号化されるのではなく、失われることになります) これから作成する TrueCrypt ボリュームに既存ファイルをコピーすることで、暗号化が可能になります。¹

ファイル選択でコンテナを置きたいパスを選んでください。

コンテナの希望のファイル名を入力して、

ダイアログの「保存」をクリックしてください。

ファイル選択ウィンドウは消えます。

¹TrueCrypt ボリュームに既存の非暗号化ファイルをコピーしたあと、元の非暗号化ファイルを完全削除するべきです。完全削除のためのツールは(多くはフリーで)存在します。

以降のステップでは「TrueCrypt ボリューム作成ウィザード」へ戻ります。

ステップ 7:

ボリュームの位置

D:\My Documents\My Volume ファイルの選択(F)

☒ 履歴を保存しない(S)

TrueCryptのボリュームは、ハードディスクやUSBフラッシュドライブ中にあるファイル(TrueCryptコンテナと呼ばれます)として作成することができます。TrueCryptコンテナは移動・コピー・削除など、通常のファイルとまったく同じように扱えます。「ファイルの選択」をクリックして、作成したいコンテナのファイル名と場所を選んでください。

注意: 既存のファイルを選んだ場合、TrueCryptはそのファイルを暗号化*しません*。既存のファイルは削除され、新しく作成されたTrueCryptコンテナに置き換えられるでしょう。既存のファイルを暗号化する場合、ここで作成したTrueCryptコンテナの中に後で移動するようにします。

ヘルプ(H) < 戻る(B) 次へ(N) > キャンセル

ボリューム作成ウィザードで「次へ」をクリックします。

STEP 8:

暗号化オプション

暗号化アルゴリズム

AES テスト(T)

FIPS(連邦情報処理基準)で規格化された暗号化方式(Rijndael 1998年)であり、アメリカ政府の各省庁において、最高機密レベルの情報保護に使われています。256ビットの鍵長、128ビットブロックで、ラウンド数は14です(AES-256)。動作モードはXTSです。

[AESについての詳細](#) ベンチマーク(B)

ハッシュアルゴリズム

RIPEMD-160 [ハッシュアルゴリズムについて](#)

ヘルプ(H) < 戻る(B) 次へ(N) > キャンセル

ここで暗号化アルゴリズムとハッシュアルゴリズムを選択します。どれを選べばいいかわからな

ければ、既定値のままで「**次へ**」をクリックしてください。(詳細は暗号化アルゴリズムとハッシュアルゴリズムの章を参照)

STEP 9:

ボリュームのサイズ

☐ KB ☒ MB ☐ GB

ドライブ D:¥ の空き容量は 82421.45 MB

作成するコンテナのサイズを指定してください。

もしダイナミック(スパースファイル)コンテナを作成するのであれば、このパラメータは上限サイズの指定になります。

下限サイズはFATボリュームの場合で275KB、NTFSボリュームの場合で2829KB となります。

ここでは例として TrueCrypt コンテナのサイズ(容量)を 1MB にします。もちろん、これとは異なるサイズにすることができます。希望するサイズを入力欄(赤でマーク)に記入し「次へ」をクリックします。

ステップ 10:

ボリュームのパスワード

パスワード:

確認入力(Q):

☐ キーファイルを使用(S)

☐ パスワード表示(D)

質の良いパスワードにすることが非常に重要です。辞書に載っているような単語一つだけにしたり、あるいはそれを三つ四つ組み合わせた程度のものは避けるべきです。また何らかの名前や誕生日なども含ませるべきではありません。それは簡単に推測されてしまいます。良いパスワードとは、大文字や小文字、数字や記号(@ ^ = \$ * + など)をランダムに組み合わせたものです。またパスワードの長さは20文字以上を推奨します(長い方がより良いです)。設定可能な最大長は64文字です。

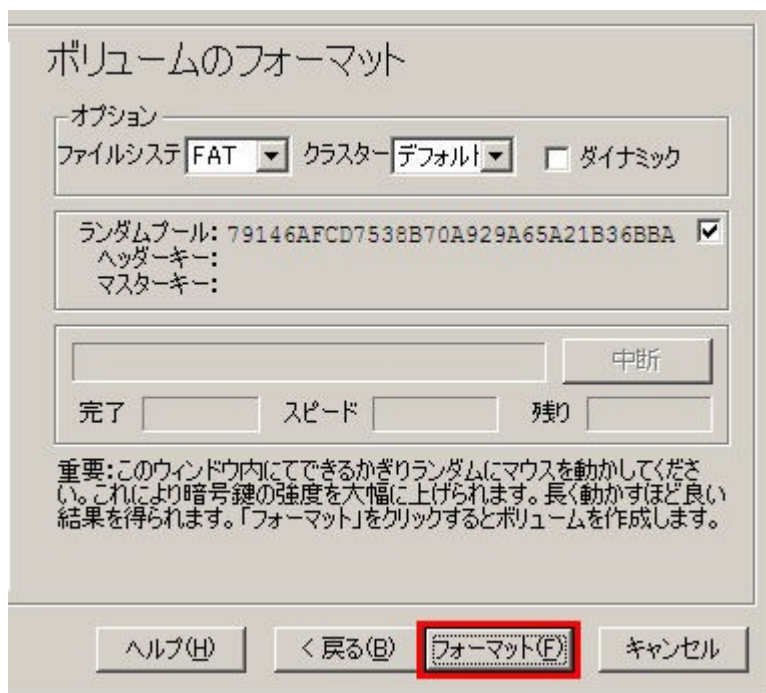
ここは重要なステップです。ここでボリュームの「良い」パスワードを決めなくてははいけません。

どのようなパスワードが「良い」のかウィザードウィンドウの説明を注意深く読んでください。

良いパスワードを決めたら、最初の入力欄に記入し、その直下の入力欄に同じものをもう一度記入して、「次へ」をクリックしてください。

注意：「次へ」ボタンは両方の欄に同じパスワードを記入しないと、クリックできるようになりません。

ステップ 11:



ウィザードウィンドウの中ですくなくとも **30 秒間**、マウスをランダムに動かしてください。動かすのが長ければ長いほど、いいのです。これは暗号化キーの強度を非常に高めることになり、安全性を向上させることにもなります。

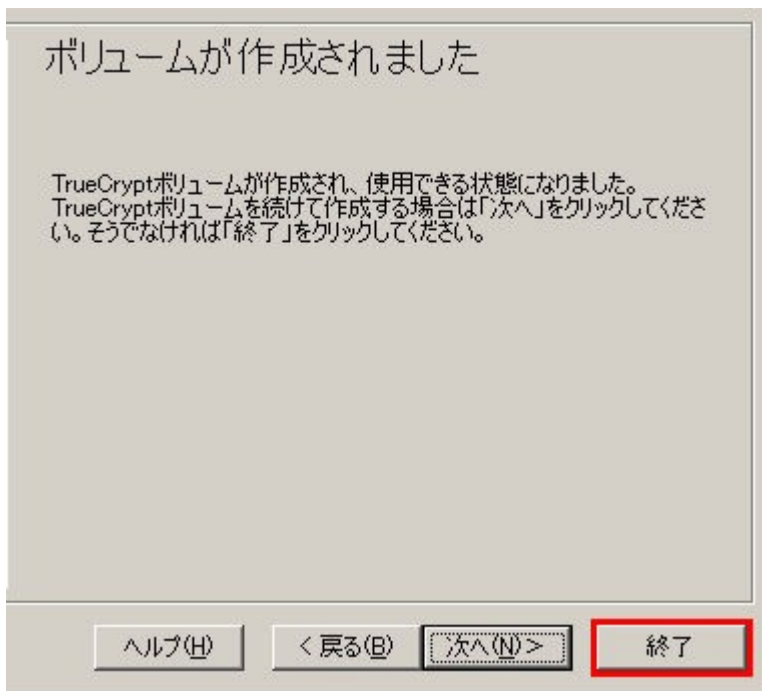
「**フォーマット**」をクリックしてください。

ボリューム作成が始まります。TrueCrypt は(Step 6 で指定したように)My Documents フォルダーに **My Volume** という名前のボリュームを作ります。このファイルは TrueCrypt コンテナであり、暗号化された TrueCrypt ボリュームを含みます。ボリュームの大きさによってはボリューム生成に時間がかかるかもしれません。完了すると、次のダイアログが表示されます。



「**OK**」をクリックしてダイアログを閉じてください。

ステップ 12:



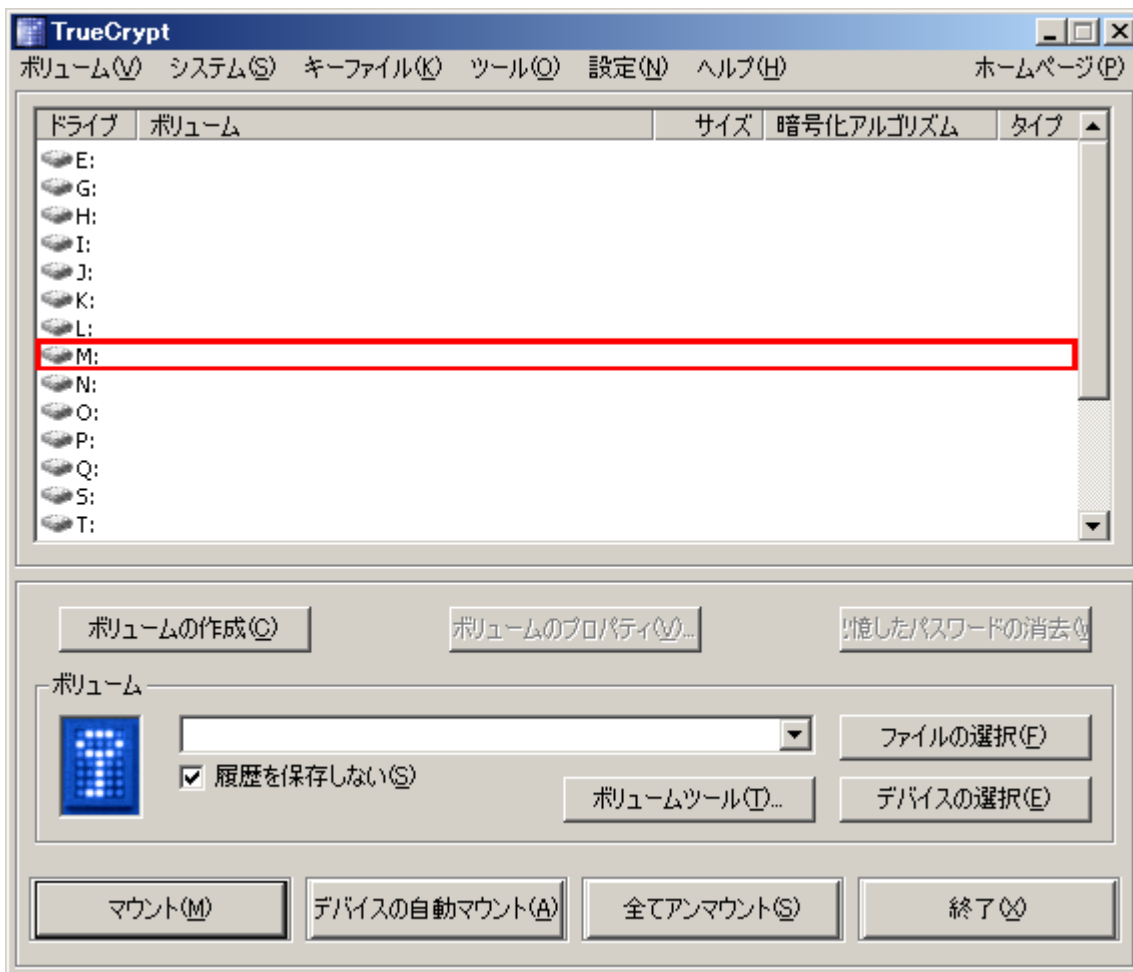
これで TrueCrypt ボリューム(ファイルコンテナ)の作成ができました。

TrueCrypt ボリューム作成ウィザードの「終了」をクリックしてください。

ウィザードウィンドウが消えます。

残りのステップでは、作ったばかりのボリュームをマウントします。TrueCrypt ウィンドウに戻りますが、これは表示されたままのはずです。もし、そうでなければステップ 21 戻って TrueCrypt を起動し、ステップ 13 から続けてください。

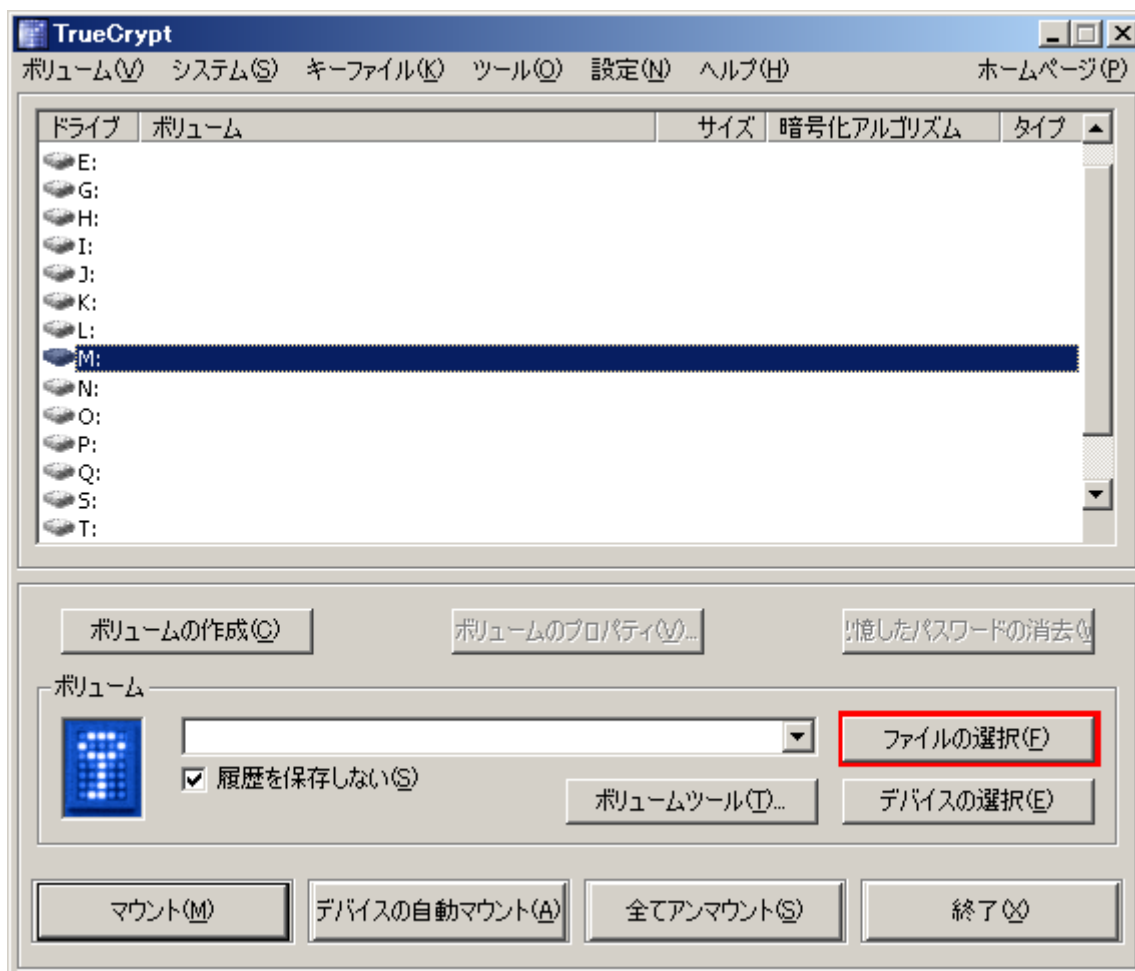
ステップ 13:



リストから(赤で囲ってある)ドライブレターを選んでください。これが **TrueCrypt** コンテナがマウントされるドライブレターになります。

注意: このチュートリアルではドライブ **M** を選びます。しかし、もちろんどの空きドライブレターでも選ぶことができます。

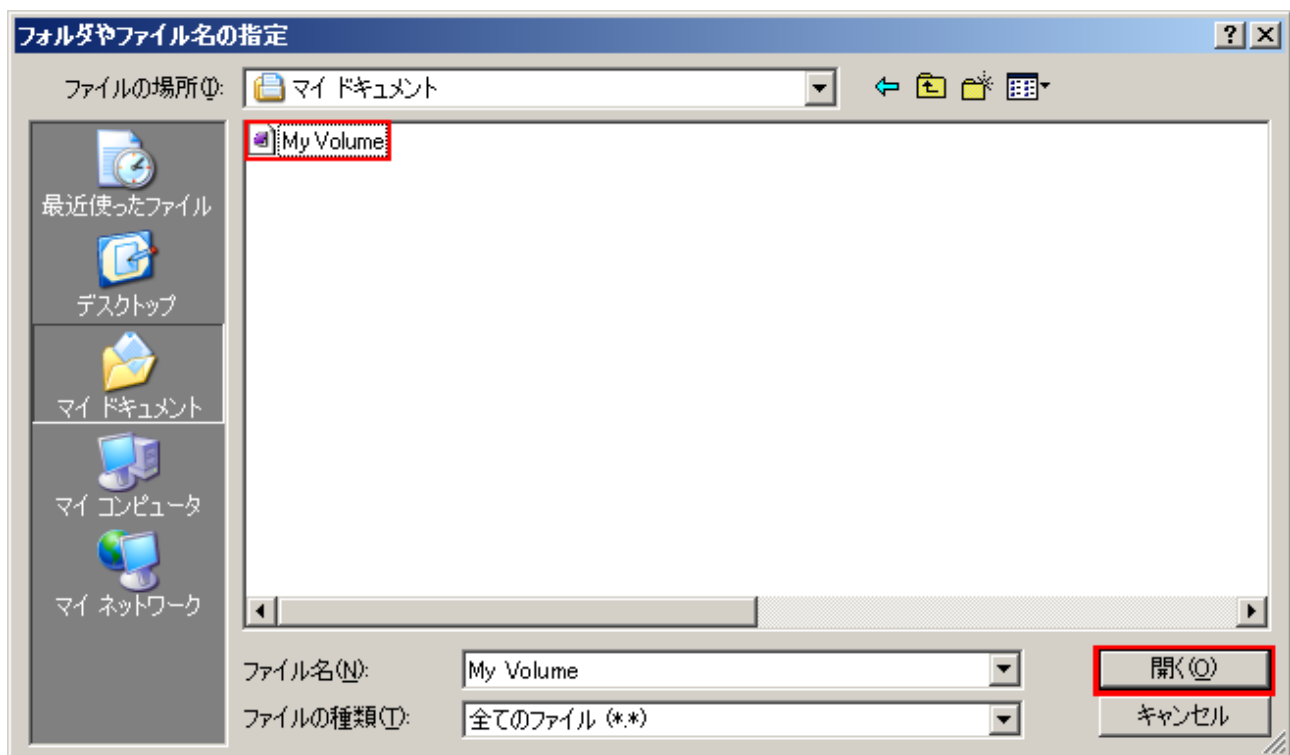
ステップ 14:



「ファイルの選択」をクリックしてください。

標準ファイル選択ウィンドウが表示されます。

ステップ 15:



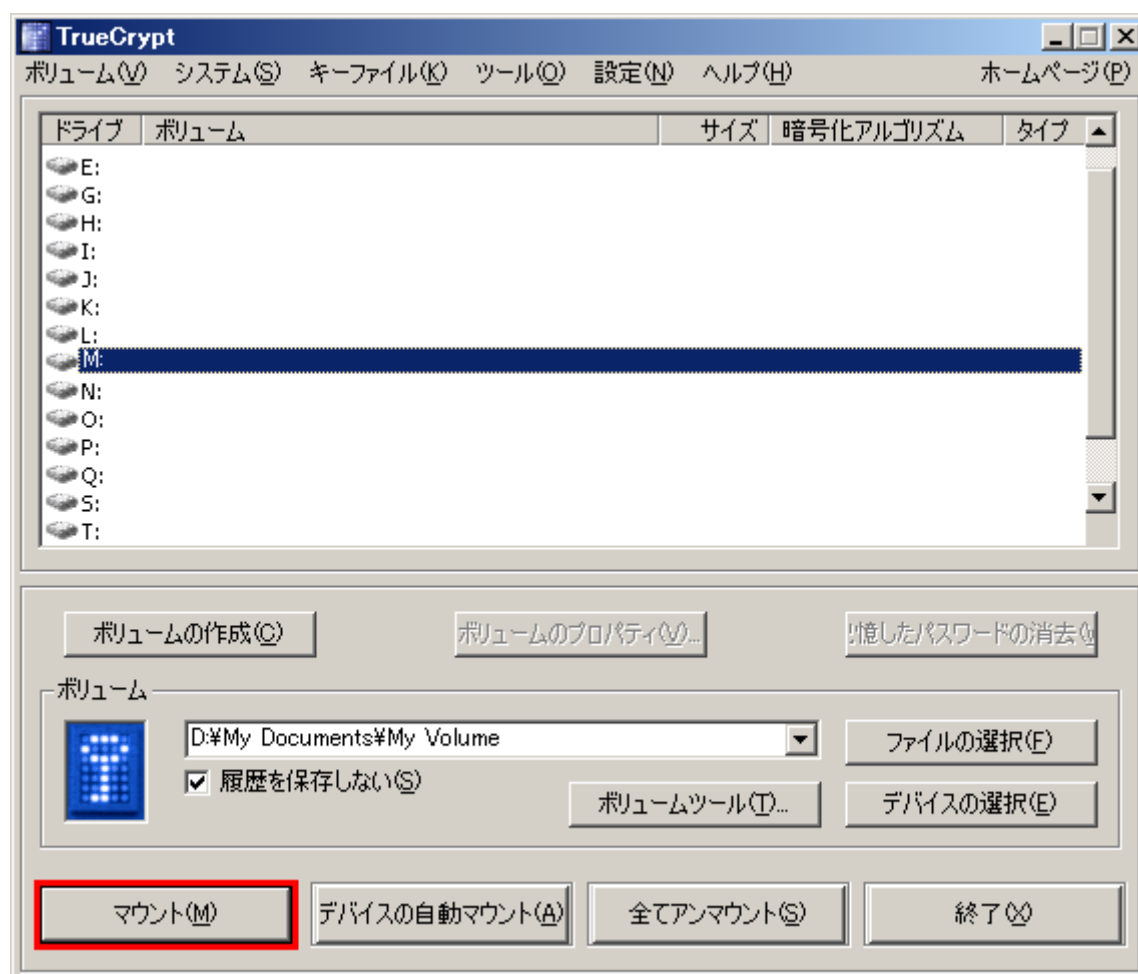
ファイル選択でコンテナファイル(ステップ 6-11 で作成したもの)を探し、それを選択してください。

ファイル選択ウィンドウの「開く」をクリックしてください。

ファイル選択ウィンドウが消えます。

以降のステップでは、TrueCrypt のメインウィンドウに戻ります。

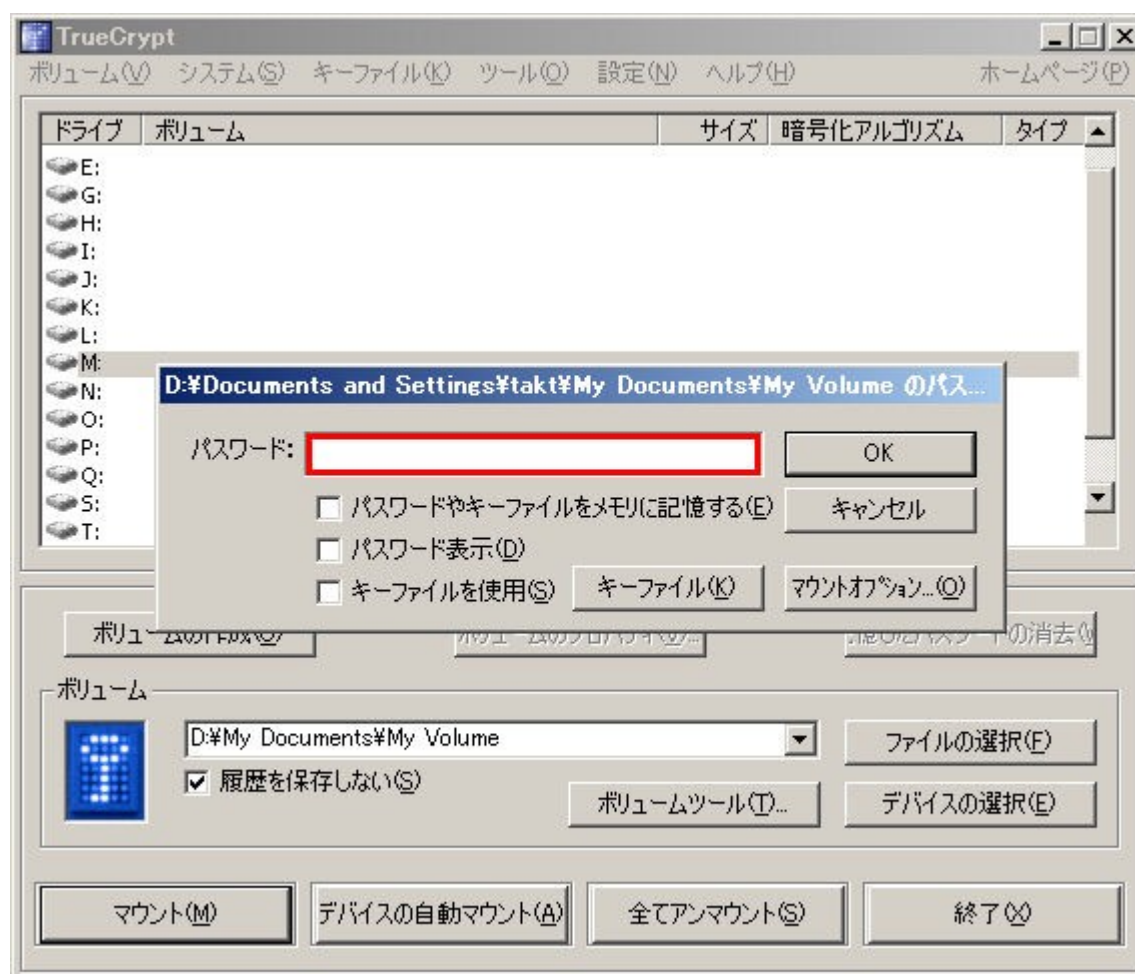
ステップ 16:



TrueCrypt メインウィンドウで、「マウント」をクリックしてください。

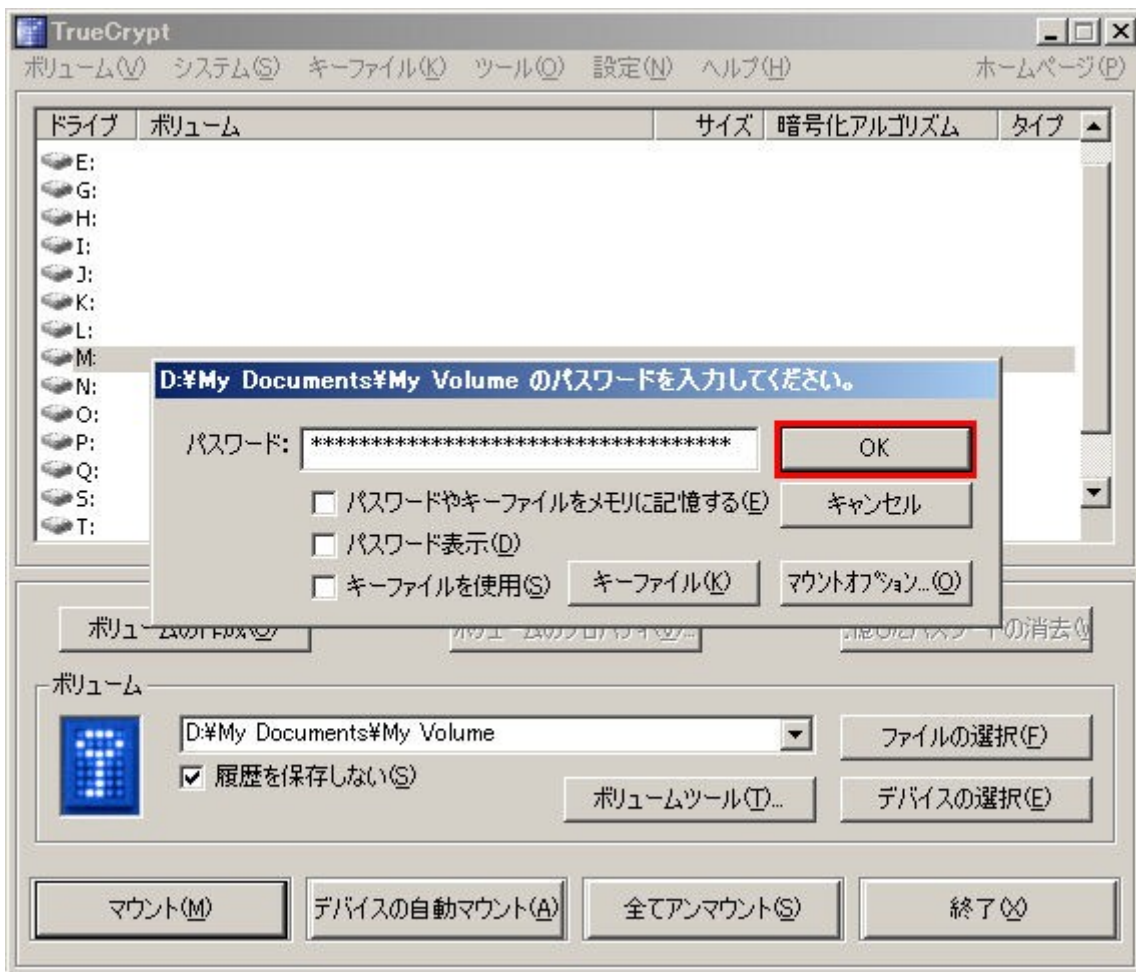
パスワード入力を求めるダイアログが表示されます。

ステップ 17:



ステップ 10 で設定したパスワードをパスワード入力欄(赤で囲んである)に記入してください。

ステップ 18:

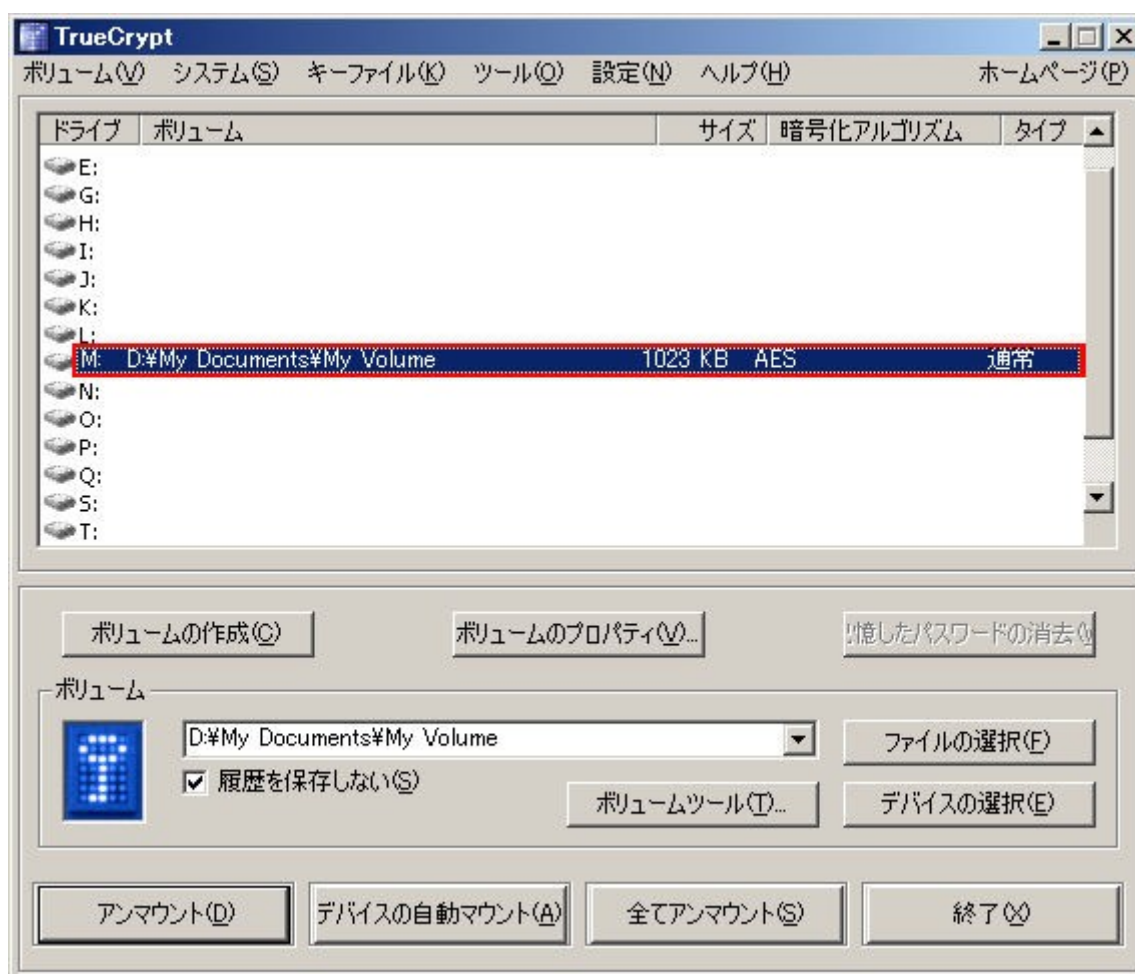


パスワード入力ウィンドウの「OK」をクリックしてください。

TrueCrypt はボリュームをマウントしようとしています。もしパスワードが一致しなければ(たとえばパスワード入力を間違えたとか)、その旨が報告され、前のステップに戻って、パスワードを再入力し OK をクリックすることになります。パスワードが一致すれば、ボリュームはマウントされます。

(次のページに続く)

最終ステップ:



これでコンテナを仮想ディスク **M:**としてマウントできました。

仮想ディスクは全体(ファイル名、アロケーションテーブル、空き領域など)が暗号化されており、実際のディスクと同じに扱えます。ファイルをそこに保存(またはコピー、移動)すれば、書込時に即時に暗号化されます。

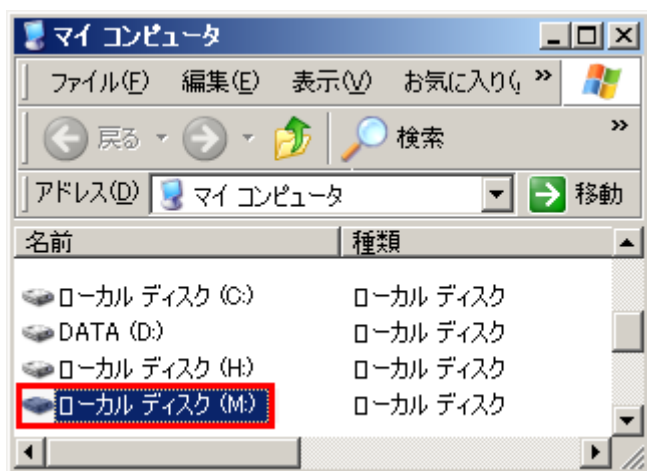
たとえばメディアプレーヤーで **TrueCrypt** ボリュームにあるファイルを開くと、ファイルは読み出し時に即時に **RAM(メモリ)**に復号されます。

重要: **TrueCrypt** ボリュームにファイルを保存したりコピーしたするときには、パスワード入力を求められません。パスワードはボリュームをマウントするときに必要なだけです。

上のスクリーンショットでいえば、赤で囲まれた項目をダブルクリックすることで、マウントされたボリュームを開くこともできます。

(次のページに続く)

また、通常のボリュームを参照するのと同じ方法でマウントされたボリュームを参照することもできます。たとえば、コンピュータ(またはマイ コンピュータ)を開いて該当のドライブ文字(この場合は M:)をダブルクリックするということです。



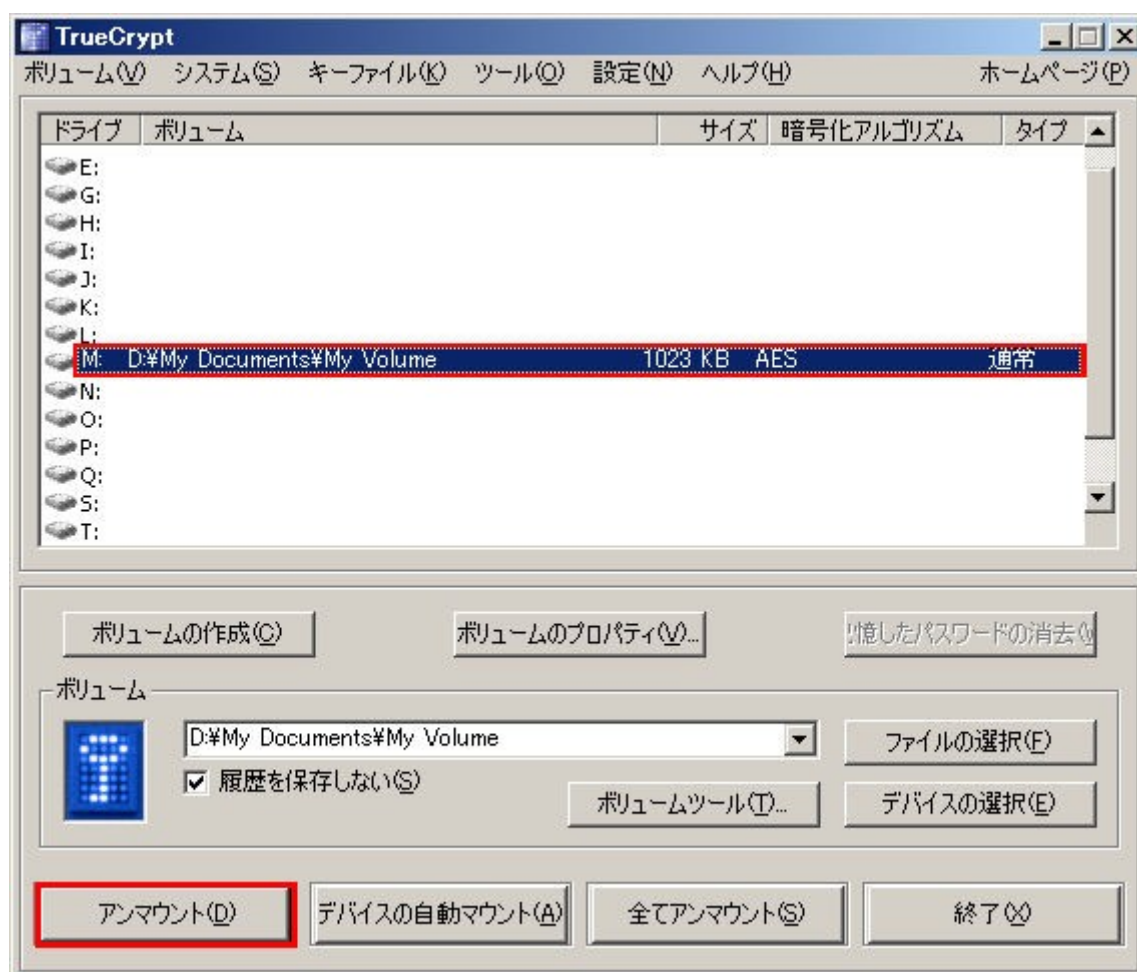
ファイルを TrueCrypt ボリュームから、あるいは TrueCrypt ボリュームへコピーするのはほかの通常のディスクに対するのと同じに実行できます。(たとえば、単純にドラッグ・アンド・ドロップもできます) 暗号化された TrueCrypt ボリュームから読み出したりコピーしたりされるファイルは、自動的に即時に(メモリ/RAM に)復号されます。

同様に、暗号化された TrueCrypt ボリュームに書き込まれるファイルは、自動的に(ディスクに書き込まれる直前に)RAM に暗号化されます。

TrueCrypt は絶対に復号されたデータをディスクに書き込みません。一時的に RAM(メモリ)に置くだけです。ボリュームがマウントされていても、そのボリュームにあるデータは暗号化されたままです。Windows を再起動したり電源を切ったりしたときにはボリュームはアンマウントされそこに保存されたファイルは(暗号化されているので)アクセスできなくなります。電源供給が(正しい手順ではなく)突然停止してもボリュームのファイルはアクセスできなくなります。もう一度アクセスするには、そのボリュームをマウントする必要があります。この手順はステップ 13-18 です。

(次のページに続く)

ボリュームを閉じてそこに保存されたファイルにアクセスできないようにするには、OS を再起動するかボリュームをアンマウントしてください。それは以下の手順で実行します。



主 TrueCrypt ウィンドウのマウントされたボリュームのリスト(上のスクリーンショットで赤く囲まれた部分)を選択し、**アンマウント**(同様に赤で囲まれています)をクリックしてください。そこに保存されたファイルに再度アクセス可能にするには、ステップ 13-18 を再度実行してください。

TrueCrypt パーティション/デバイスの作り方と使い方

ファイルコンテナのかわりに、物理的パーティションやドライブを暗号化する(TrueCrypt デバイス型ボリューム)ことができます。これを実行するには、このチュートリアル of ステップ 1-18 を実行してください。ただし、ステップ 3 で 2 番目か 3 番目のオプションを選び、ウィザードの残りの指示にしたがってください。非システムパーティション/デバイスにデバイス型 TrueCrypt ボリュームを作成する場合には、主 TrueCrypt ウィンドウで「デバイスの自動マウント」をクリックすることでマウントすることができます。システムパーティション/ドライブの暗号化についての情報は、システム暗号化に記載しています。

重要: このマニュアルの他の章にはチュートリアルを簡単にするため省略した重要な情報が含まれています。それらの章もぜひ読んでください。

みせかけの拒否

敵対者があなたにパスワードを明かすことを強制するような場合、TrueCrypt は 2 レベルのみせかけの拒否(もっともらしい説明で相手をごまかす)の手段をあなたに提供します。

1. 隠しボリューム(詳細は後記の隠しボリュームの節を参照)
2. TrueCrypt ボリュームであるかどうかを特定するのは不可能です。復号されるまでは TrueCrypt ボリュームはランダムなデータにしか見えません。(TrueCrypt ボリュームであるという「署名」のようなものではありません) ですから、あるファイル、パーティション、デバイスが TrueCrypt ボリュームであるとか暗号化されているということを証明することはできません。しかし、起動ドライブを暗号化した場合には、ドライブの最初のトラックには暗号化されていない TrueCrypt ブートローダーがあり、そのことは簡単にわかってしまいます。(詳細はシステム暗号化の章を参照してください) そのような場合には、隠し OS(隠し OS の節を参照)を作ること、みせかけの拒否をうまくやることができます。

TrueCrypt コンテナ(ファイル型ボリューム)は、どんな拡張子(たとえば .raw, .iso, .img, .dat, .rnd, .tc)をつけてもかまいません。または拡張子がなくてもまったくかまいません。TrueCrypt は拡張子を見ません。もし「みせかけの拒否」をする必要があれば、TrueCrypt ボリュームに .tc という拡張子をつけてはいけません。(この拡張子は'公式に'TrueCryptに関連づけられているからです)

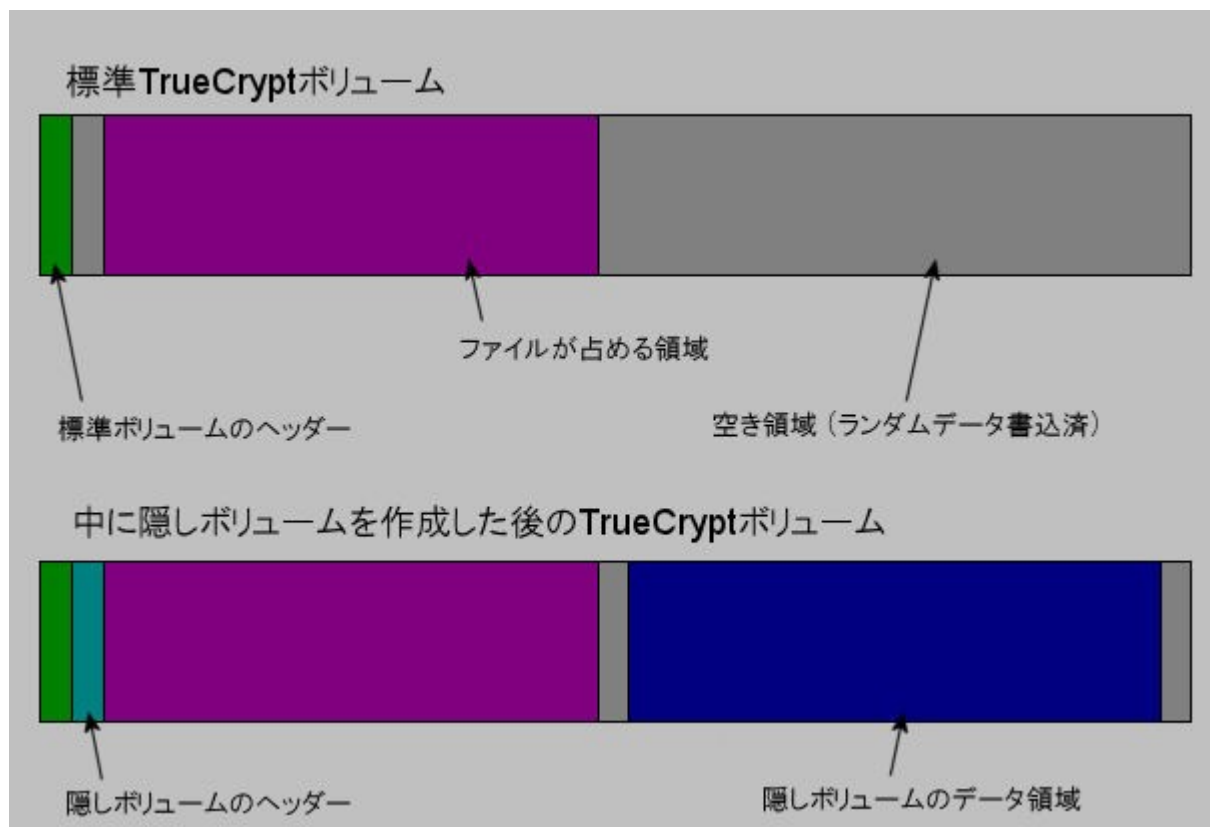
ハードディスクのパーティションを TrueCrypt ボリュームとしてフォーマットする場合でも、パーティションテーブル(パーティションタイプを含む)は変更されません。(TrueCrypt の署名や ID のようなものはパーティションテーブルには書き込まれません)

TrueCrypt がファイル型ボリュームにアクセス(アンマウント、マウント試行、パスワードの作成と変更、中に隠しボリュームを作成、など)したりキーファイルにアクセスしたりするどのような場合でも、コンテナやキーファイルのタイムスタンプ(コンテナやキーファイルの最終アクセス¹、変更日時)は変更されません。ただし、設定でこの機能を無効にしていなければ、です。

¹Windows でコンテナやキーファイルのタイムスタンプを見るために「プロパティ」を参照(コンテナやキーファイルを右クリックして「プロパティ」を選択)すると、コンテナやキーファイルのアクセス日時を変更することになります。また、Windows のファイル選択でサムネール表示にする(縮小表示モードでコンテナやキーファイルを選択する場合)には、Windows がアクセス日時を変更することがあります。

隠しボリューム

誰かが暗号化ボリュームのパスワードを明かすよう強要するかもしれません。それを拒否できない状況、たとえば脅迫などもあり得ます。そこで、いわゆる「隠しボリューム」を使うことで、ボリュームのパスワードを明かさずに策略で解決する方法があります。



隠しボリューム作成前後の標準TrueCryptボリュームの状態

他の TrueCrypt ボリュームの空き領域に TrueCrypt ボリュームを作るというのが、ポイントです。外殻ボリュームがマウントされた状態でも、それが隠しボリュームを含むかどうかを判断することはできません¹。なぜなら、どの TrueCrypt ボリュームの空き領域も作成時²にランダム値で埋められているからです。そして、マウントされていない隠しボリュームのどの部分もランダムデータと区別できません。また、TrueCrypt は外殻ボリュームのファイルシステム(空き領域情報など)を変更することはありません。

隠しボリュームのパスワードは、外殻ボリュームのパスワードとは異なったものでなくてはなりません。隠しボリュームを作成する前に、外殻ボリュームには本当には隠そうとは思っていない

¹TrueCrypt ボリューム作成ウィザードの指示にすべて従い、隠しボリュームの安全に関する予防策にある注意をまもった場合です。

²クイックフォーマットとダイナミックのオプションは使用不可になっています。空き領域をランダムデータで満たす方法については、技術解説の章、TrueCrypt ボリュームフォーマット仕様を参照してください。

何か秘密情報らしいファイルをいくつかコピーしておいてください。これらのファイルは、あなたにパスワードを明かすことを強要する人に見せるためのものです。隠しボリュームのパスワードは守り、外殻ボリュームのものだけを明かせばいいのです。本当に秘密にしたいファイルは隠しボリュームに入れてください。

隠しボリュームは通常の **TrueCrypt** ボリュームと同じ手順でマウントできます。「ファイルの選択」または「デバイスの選択」をクリックし外殻ボリュームを選択してください。(重要: それらがすでにマウントされていないことを確認してください) 「マウント」をクリックし、隠しボリュームのパスワードを入力してください。隠しボリュームがマウントされるか、外殻ボリュームがマウントされるかは、入力されたパスワードで決定されます。(つまり、外殻ボリュームのパスワードを入力すれば外殻ボリュームが、隠しボリュームのパスワードを入力すれば隠しボリュームがマウントされます)

TrueCrypt は最初に、入力されたパスワードを使って標準ボリュームヘッダーを復号しようとし、それに失敗すると隠しボリュームのヘッダーが存在する可能性がある領域 (**65536-131071** バイト。隠しボリュームがない場合には、この領域はすべてランダムデータが書き込まれています) を **RAM** に読み込み入力されたパスワードで復号しようとしています。

隠しボリュームのヘッダーはそれとわかるようにはなっていないことに留意してください。それはまったくランダムなデータとしか見えません。ヘッダーがうまく復号できたら(**TrueCrypt** がどうやってうまく復号できたかを判断するかについては、暗号化の仕組みの節を参照)、復号されたヘッダー(**RAM** に保持)から隠しファイルのサイズについての情報が得られ、隠しボリュームがマウントされます。(そのサイズはオフセットを決定することにもなります)

隠しボリュームはどのようなタイプの **TrueCrypt** ボリュームにでも作成することができます。ファイル型にでもパーティション/デバイス型(管理者権限が必要)にでも、です。**TrueCrypt** の隠しボリュームを作成するには、メインウィンドウで「ボリュームの作成」をクリックし「**TrueCrypt** 隠しボリュームを作成する」を選択してください。ウィザードは **TrueCrypt** 隠しボリュームを作成するためのヘルプと必要な情報を表示します。

隠しボリューム作成時に、隠しボリュームが外殻ボリュームのデータを上書きしてしまわないように隠しボリュームの容量を決めるのは、経験のないユーザーには難しい、あるいはほとんど不可能です。ですから、ボリューム作成ウィザードは隠しボリュームが生成される前に外殻ボリュームのクラスタ配置を調べて、隠しボリュームを作成可能な最大容量を決めます。¹

隠しボリュームを作成するのに何か問題があれば、問題が起こったらの章で解決策を探してください。

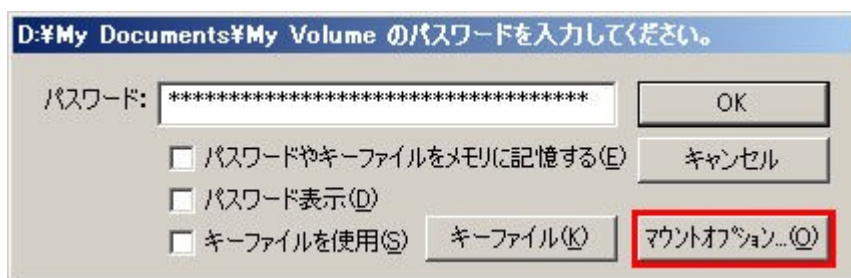
隠しボリュームに **OS** を置き、それからブートすることもできます。(詳細はみせかけの拒否の隠し **OS** を参照)

¹この機能は **Windows** 版のみに実装されています。ウィザードは外殻ボリュームの終端に一致する連続した空き領域のサイズを得るように、クラスタ配置を調査します。それが得られれば、この領域が隠しボリュームとなり、隠しボリュームの可能な最大容量となります。

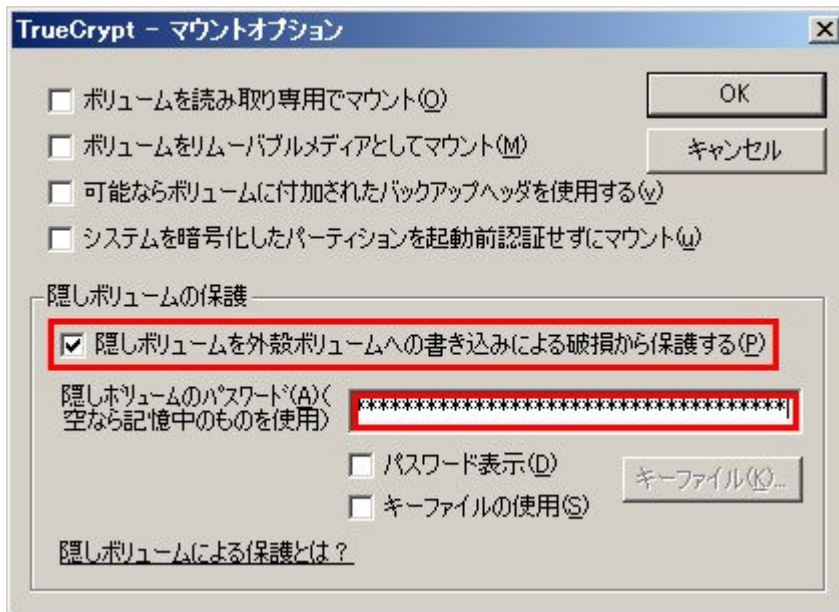
隠しボリュームを破損から守る

隠しボリュームを含む TrueCrypt ボリュームをマウントすると、何の危険もなしに外殻ボリュームのデータを読むことができます。しかし、あなた(あるいはシステム)が外殻ボリュームにデータを保存しようとする、隠しボリュームの一部が上書きされ破損する危険があります。これを防ぐため、ここで記載する方法で保護してください。

外殻ボリュームをマウントするときに、パスワードを入力し、「OK」をクリックする前に「マウントオプション」をクリックしてください。



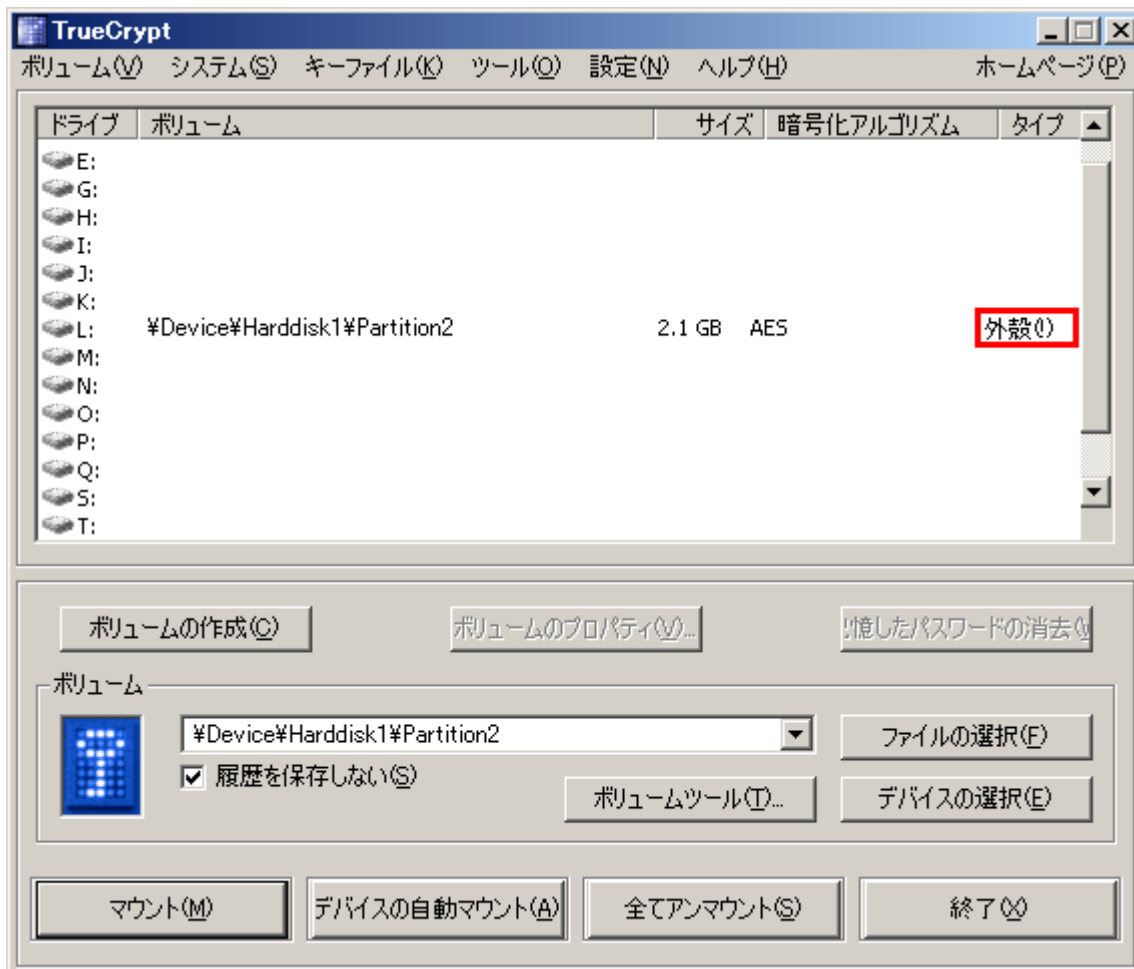
「マウントオプション」ダイアログで「隠しボリュームを外殻ボリュームへの書き込みによる破損から保護する」を有効にしてください。つぎに「隠しボリュームパスワード」の入力欄に隠しボリュームのパスワードを記入してください。そして「OK」をクリックし、メインパスワード入力ダイアログの「OK」をクリックしてください。



両方のパスワードが正しいものでなくてはなりません。そうでなければ、外殻ボリュームはマウントされません。隠しボリューム保護が有効な場合、TrueCryptは隠しボリュームをマウントするのではなく(RAMにある)ヘッダーを復号し、隠しボリュームのサイズを(復号されたヘッダーから)得るだけです。そして、外殻ボリュームがマウントされ、(外殻ボリュームがアンマウントされるまで)隠しボリューム領域へのどんなデータ保存も拒否されます。**TrueCryptは外殻ボリュームのファイルシステム(クラスタ割り当て情報、空き領域情報など)をいっさい変更しません。**ボリュームがアンマウントされると、ただちに保護は機能しなくなります。そのボリュームが再マウントされても、そのボリュームが隠しボリューム保護に使われているかどうかの判別はできません。隠しボリューム保護機能はユーザーが隠しボリューム用の正しいパスワード(またはキーファイル)を入力/提供した場合のみ、有効となります。

隠しボリューム領域への書き込み動作が(隠しボリューム保護のため)拒否/防止されるとただちにホストボリューム(外殻ボリュームと隠しボリュームの両方)はアンマウントされるまで書き込み不可に設定(TrueCryptドライバがそのボリュームへの書き込みに対して「不正なパラメータ」エラーを返す)されます。これが「みせかけの拒否」を守ります。(そうでなければ、ある種のファイルシステムの矛盾がそのボリュームが隠しボリューム保護を使っていることを示してしまうかもしれません) 隠しボリューム破損が防止されると、警告が表示されます。(TrueCryptが常駐している場合のみ表示 -TrueCryptの常駐を参照)

さらに、メインウィンドウで表示されるマウントされている外殻ボリュームのタイプは「外殻(!)」に変わります。

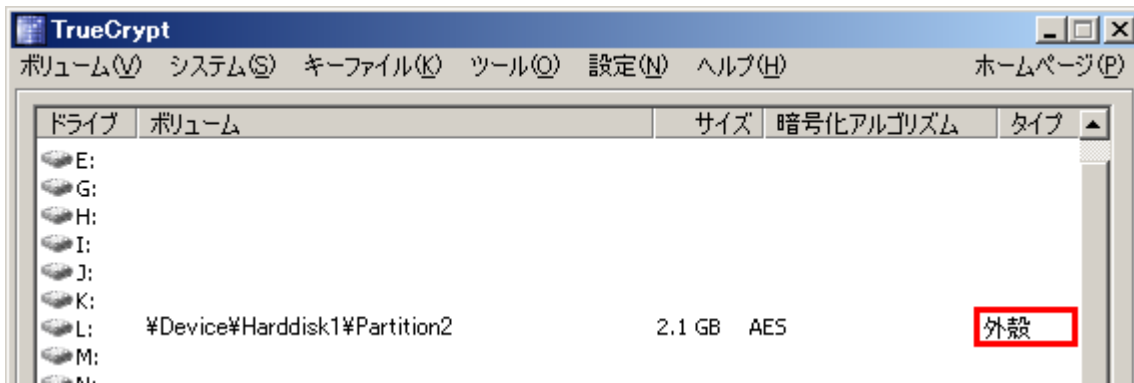


さらに、「ボリュームプロパティ」の「隠しボリューム保護」フィールドでは「はい(破損は防止されました!)」と表示されます。

隠しボリュームの破損が防止されても、そのことについての情報はボリュームには書き込まれません。外殻ボリュームをアンマウントして、ふたたびマウントしてもボリュームプロパティには「破損は防止されました」というメッセージは表示されません。

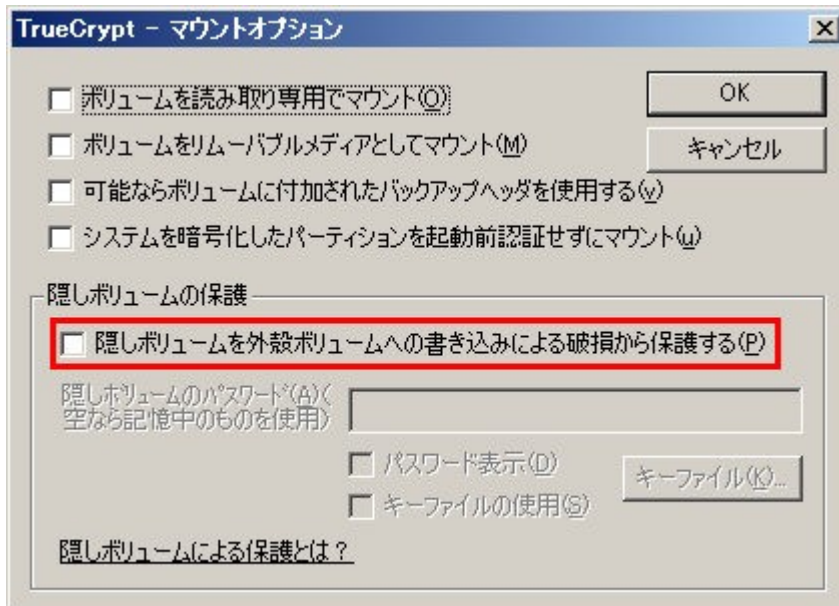
隠しボリュームが破損から保護されているかどうかを調べるには、いくつかの方法があります。

1. 外殻ボリュームがマウントされたあと、確認メッセージボックスに隠しボリュームは保護されているという表示がでます。(これが表示されなければ、隠しボリュームは保護されていません)
2. 「ボリュームプロパティ」ダイアログで、「隠しボリューム保護」は「はい」になります。
3. マウントされた外殻ボリュームは「外殻」と表示されます。



重要: 敵対者が外殻ボリュームをマウンとするよう求めてきた場合には、当然のことながら隠しボリューム保護を有効にして外殻ボリュームをマウントしてはいけません。隠しボリューム保護を有効にして外殻ボリュームをマウントしていると、敵対者は(ボリュームがアンマウントされるまでは)外殻ボリュームに隠しボリュームが存在することを発見することができてしまうことに注意してください。

警告: 「マウントオプション」ダイアログウィンドウの「隠しボリュームを外殻ボリュームへの書き込みによる破損から保護する」というオプションは、マウント試行が完了すると、マウントが成功したか否かによらず自動的に不可になります。(すでに保護されているすべての隠しボリュームは、もちろん保護されたままです) したがって、(隠しボリュームを保護したいなら)外殻ボリュームをマウントしようとするときには毎回オプションをチェックする必要があります。



キャッシュされたパスワードを使って、隠しボリュームを保護しながら外殻ボリュームをマウントしたいなら、次のステップで実行してください。: コントロール(Ctrl)キーを押しながらマウントをクリック(または、ボリュームメニューの「オプション付でマウント」をクリック。「マウントオプション」ダイアログが開きます。「隠しボリュームを外殻ボリュームへの書き込みによる破損から保護する」を有効にしてください。そして、パスワードを空欄のままにし、「OK」をクリック

ックしてください。

外殻ボリュームをマウントする必要があるが、どのようなデータもそこに保存しないということがわかっている場合には、隠しボリュームを破損から保護する最も簡単な方法は読み出し専用で外殻ボリュームをマウントすることです。(マウントオプション参照)

隠しボリュームの安全に関する予防策

隠しボリュームを使うなら、以下の安全予防策にしたがってください。

- もし敵対者が、アンマウントされた **TrueCrypt** ボリュームの特定の場所を何回もアクセスすると、ボリュームのどのセクターに変更があったかをつきとめることができます。あなたがファイルをつくったり、コピーしたり、ファイルの更新、削除、リネーム、移動などで隠しボリュームの内容に変更を加えると、隠しボリュームにあるセクターの内容（暗号化出力されたデータ）は変更されることになります。外殻ボリュームのパスワードを教えたにもかかわらず、なぜこれらのセクターの内容に変更が生じているのかについて追求されるかもしれません。あなたの回答如何によっては、相手はボリュームに隠されたボリュームがあると疑うかもしれません。

上記の問題は以下のような場合でも起きる可能性があります。

- ファイル型 **TrueCrypt** コンテナをデフラグして、ホストボリューム(デフラグされたファイルシステム)の空き領域にコンテナや断片のコピーが残っている場合。これを防ぐには以下のどれかを実行してください。
 - ファイル型のかわりに、パーティション/デバイス型 **TrueCrypt** ボリュームを使う
 - ホストボリューム(デフラグされたファイルシステム)の空き領域に完全消去をかける
 - **TrueCrypt** ボリュームを格納するファイルシステムではデフラグをしない
- ファイル型 **TrueCrypt** コンテナが(NTFS のような)ジャーナリングファイルシステムに格納されている場合。**TrueCrypt** コンテナあるいはその断片のコピーがホストボリュームに残る可能性があります。これを防ぐには以下のどれかを実行してください。
 - ファイル型のかわりに、パーティション/デバイス型 **TrueCrypt** ボリュームを使う
 - **FAT32** のようなジャーナリング機能を持たないファイルシステムにコンテナを格納する
- ファイル型 **TrueCrypt** ボリュームがウェアレベリング機構を持つデバイス(たとえば、いくつかの **USB** フラッシュメモリ)に格納されている場合。**TrueCrypt** ボリュームの断片のコピーがそのデバイスに残る可能性があります。ウェアレベリングについての詳細は安全のための予防策のウェアレベリングを参照してください。
- 隠しボリュームを作ろうとするパーティション/デバイスを暗号化するときには、クイックフォーマットはしてはいけません。
- **Windows** では、隠しボリュームをつくらうとするボリュームのどのファイルも削除していないことを確認してください。(クラスタ配置調査ツールでは、削除されたファイルを検出でき

ません)

- **Linux** や **Mac OS X** ではファイル型 **TrueCrypt** ボリュームの中に隠しボリュームを作る場合には、**スパース(sparse)**ファイルシステムのボリュームであってははいけません。(Windows 版では **TrueCrypt** はスパースファイルシステムを区別し、その中に隠しボリュームを作ることはできないようになっています)
- 隠しボリュームがマウントされると、**OS** や他社のアプリケーションは非隠しボリューム（通常は暗号化されていないシステムボリューム）に、隠しボリュームに保存されている情報（ファイル名、最近使ったファイルの保存場所、ファイル索引ツールが作成するデータベース など）や非暗号化形式のデータそのもの（テンポラリファイルなど）、または隠しボリュームのファイルシステムに関する暗号化されていない情報（これはファイルシステムを特定し外殻ボリュームにファイルシステムが存在すると結論付けるかもしれない）などを書き込むかもしれません。このため、以下のガイドラインと事前の注意にしてください。

- **Windows** : 隠し **OS** を作成し（作成方法については隠し **OS** を参照）、隠し **OS** が稼働中のときだけ隠しボリュームをマウントする。

注意：隠し **OS** が稼働中の場合には、**TrueCrypt** はすべての非暗号化ファイルシステムと **TrueCrypt** の非隠しボリュームを読み取り専用（つまり、それらのファイルシステムや **TrueCrypt** ボリュームにはいっさいのファイルは書き込まれないということ）にします。データは **TrueCrypt** の隠しボリュームにのみ書き込みができます。

- **Linux** : 使っている **Linux OS** の「live CD」版（CD/DVD にまるごと **Linux** システムが格納されてそれからブートできるようになっている）を作るかダウンロードし、システムボリュームに書かれるすべてのデータが **RAM** ディスクに書き込まれるようにしてください。このような「live CD」システムが稼働中であるときのみに、隠しボリュームをマウントするようにしてください。このセッションの間には **TrueCrypt** 隠しボリュームにあるファイルシステムのみが読み書き可としてマウントが可能（外殻または非暗号化ボリューム/ファイルシステムは読み取り専用でマウントするか、まったくマウントしない、アクセス不可にしておくこと）です。このような「live CD」版が入手できないとか、アプリケーションや使っている通常の（「live CD」ではない）**OS** が上記のような機密データを非隠しボリューム（またはファイルシステム）に書き込まないようにできないなら、**Linux** で **TrueCrypt** 隠しボリュームを作ったりマウントするべきではありません。
- **Mac OS X** : アプリケーションや **OS** が上記のような機密データを非隠しボリューム（またはファイルシステム）に書き込まないようにできないなら、**Mac OS X** で **TrueCrypt** 隠しボリュームを作ったりマウントするべきではありません。
- 隠しボリューム内の **OS**（隠し **OS** を参照）を使うなら、前述の注意点に加えて、下記の予備的安全策をとってください。
 - 自分のコンピュータを使うときにはできるだけ多く**OS**を使うべきです。たとえば、機密データを使わない場合すべてについてです。そうでないと隠し **OS** についてのみせかけの拒否は敵対者には通用しにくくなるかもしれません。（**OS** へのパスワードを

明かしたら、そのシステムがあまり使われていないことが判明し、それは隠された OS がある可能性を示していると考えられるかもしれません) ㊦ OS のパーティションには隠しボリュームが破損する危険なしにいつでも書込みができることに留意してください。(なぜなら、㊦ OS は外殻ボリュームにインストールされるわけではないからです)

- OS がアクティベーションを必要としているなら、複製（複製は隠し OS 作成のプロセスの一部です-隠し OS を参照）を作る前に実行し、隠し OS（つまり複製）で絶対に再アクティベーションをしてはいけません。これは、隠し OS は隠しボリュームのシステムパーティションの内容をコピーすることで作成され、元の OS がアクティベートされていなければ隠し OS もアクティベートされていないことになるからです。もし隠し OS をアクティベートまたは再アクティベートすると、アクティベーション日時やその他のデータがマイクロソフトのサーバーと隠し OS に記録され、㊦ OS には記録されないことになります。したがって、㊦ OS へのパスワードを明かし、敵対者がサーバーに保存されたデータにアクセスしたりサーバーへの要求を傍受したりすると、㊦ OS のアクティベート日時が異なることをつきとめ、隠された OS が存在するかもしれないという手がかりを与えることになるかもしれません。

同様の理由で、アクティベーションを必要とするアプリケーションは隠し OS を作成する前にインストールし、アクティベーションを実行しておかなければなりません。

- 隠し OS をシャットダウンし㊦ OS を起動する必要がある場合には、コンピュータの再起動をしてはいけません。代わりに、シャットダウンか休止にして、数分間は電源オフの状態にしたあと、電源を入れて㊦ OS を起動してください。これは機密データを含むメモリーをクリアするのに必要なことです。詳細は安全のための予防策の RAM にある暗号化されていないデータを参照してください。
- コンピュータのネットワーク（インターネットを含む）接続は、㊦ OS が起動中のときにだけにしてください。隠し OS 稼働中のネットワーク（インターネットを含む）接続はするべきではありません。（ネットワーク接続を回避するもっとも確実な方法のひとつは、ネットワーク接続ケーブルを外すことです）リモートサーバーへのアップロードやダウンロードはサーバーにアクセス時刻他のデータを残します。さまざまなデータは OS にも記録を残します。（たとえば Windows 自動アップデートのデータ、アプリケーションの稼働記録、エラー記録他）したがって、㊦ OS へのパスワードを明かし、敵対者がサーバーに保存されたデータにアクセスしたりサーバーへの要求を傍受したりすると、ネットワーク接続が㊦ OS で実行されたのではないということが判明し、隠された OS が存在するかもしれないという手がかりを与えることになるかもしれません。

隠し OS でネットワーク間でのファイルシステムの共有（ファイルシステムがローカルリモートかを意識しない）をすると、同様な問題がおきます。ですから、隠し OS 稼働中にはネットワーク間（双方向）でのファイルシステム共有はしてはいけません。

- BIOS、EFI、または何らかの機構が Windows の記録に残るような電源断あるいは他のイベントを記録するのであれば、そのような機能を使用不可にするか、セッションごとに記録を確実に消去するべきです。

上記事前注意事項に加えて、下記の安全への事前注意にしてください。

- 安全のための予防策
- 安全なバックアップのとり方

隠し OS

TrueCrypt でシステムパーティションあるいはシステムドライブを暗号化している場合、コンピュータを起動あるいは再起動したあとに TrueCrypt ブートローダー画面でパスワード入力が必要になります。このようなときに、誰かに OS を復号するとか起動前認証のパスワードを明かすよう強要されることがあるかもしれません。こういった要求を拒否できない場合（たとえば 暴力による場合）も多く想定できます。TrueCrypt は隠し OS を作成することを可能にし、これは（ガイドラインにしたがっていれば-下記参照）存在することすらわかりません。これによって、隠し OS を復号したり隠し OS のパスワードを明かしたりしなくて済みます。

この節を読む前に、隠しボリュームの節を読み、TrueCrypt 隠しボリュームとは何かということを理解しておいてください。

隠し OS とは TrueCrypt 隠しボリュームにインストールされたシステム（たとえば Windows Vista や Windows XP）のことです。隠しボリュームは（ガイドラインにしたがっていれば-下記参照）存在することすらわかりませんし、そのために隠し OS が存在するかどうかも判別できません。

しかし、TrueCrypt で暗号化されたシステムを起動するには、TrueCrypt ブートローダーの暗号化されていないコピーがシステムドライブか TrueCrypt レスキューディスクに格納されている必要があります。ということは、TrueCrypt ブートローダーが存在するということが、そのコンピュータに TrueCrypt で暗号化されたシステムがあることを示していることにもなります。したがって、TrueCrypt ブートローダーが存在することについてのもっともらしい説明ができるように、TrueCrypt ウィザードは隠し OS を作成する過程で第二の暗号化 OS(㊦ OS と呼ぶ)を作る手助けをします。㊦ OS はいかなる機密ファイルを含んでいてもいけません。その存在は秘密ではありません(隠しボリュームにインストールされるのではない)。㊦ OS のパスワードは起動前認証のパスワードを明かすよう強要する相手に公開しても安全なのです。¹

自分のコンピュータを使うときにできるだけ㊦ OS を使うべきです。たとえば、機密データを使わない場合すべてについてです。そうでないと隠し OS についてのみせかけの拒否は敵対者には通用しにくくなるかもしれません。（㊦ OS へのパスワードを明かしたら、そのシステムがあまり使われていないことが判明し、それは隠された OS がある可能性を示していると考えられるかもしれません）

二つの起動前認証パスワードが必要になります。一つは隠し OS に、もう一つは㊦ OS に使われます。隠し OS を起動したいなら TrueCrypt ブートローダー画面(コンピュータの電源を入れるか再起動時に表示)で隠し OS 用パスワードを入力すればいいだけです。同様に㊦ OS を起動したい(たとえば OS 起動を強要された場合)には、TrueCrypt ブートローダー画面で㊦ OS 用のパスワードを入力するだけです。

注意：起動前認証でパスワード入力があると TrueCrypt は最初に(そのパスワードを使って)システムドライブの最初の論理トラック(通常なら隠し OS ではない暗号化システムパーティション/ドラ

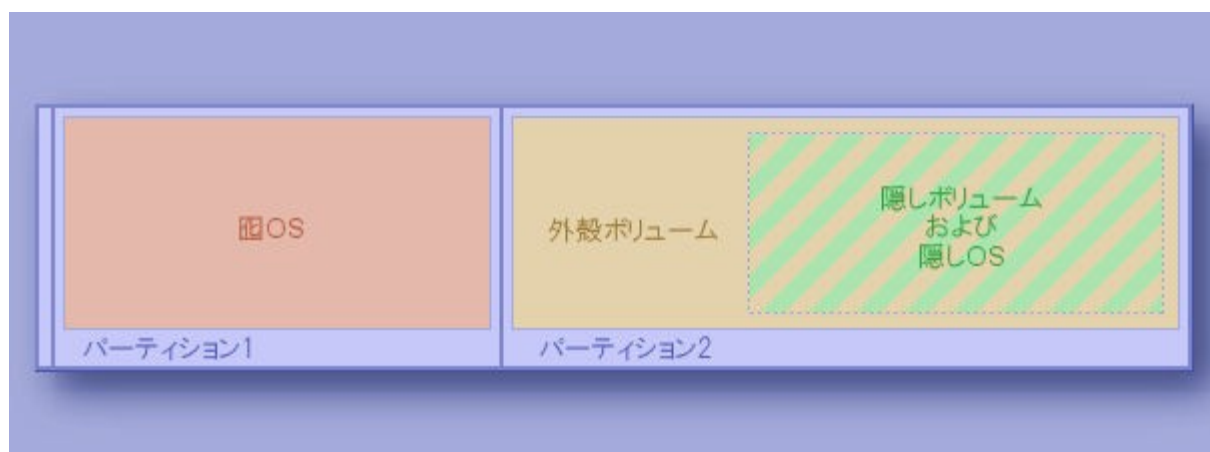
¹OS を単一のパーティションに含まれる 2 個の TrueCrypt ボリュームにインストールするのは実際的ではなく、サポートもされていません。なぜなら、外部の OS はしばしば隠し OS 領域にデータを書き込もうとするからです。(このような書き込み動作が隠しボリューム保護機能で防がれると、システムクラッシュ、たとえばブルースクリーン・エラーを引き起こすでしょう)

イブのマスターキーの暗号化されたデータを格納)の最後の 512 バイトを復号しようとします。それに失敗しブートパーティションの後ろにパーティションがあれば、TrueCrypt ブートローダーは(実際にはそのドライブに隠しボリュームがなかったとしても)自動的に同じパスワードを使ってブートパーティションのすぐ後のパーティションの隠しボリュームの暗号化されたヘッダーが格納されているかもしれない領域を復号しようとします。TrueCrypt は事前に隠しボリュームがあるかどうかを知ることはできないというこに留意してください。これは隠しボリュームのヘッダーを特定することはできず、そうであったとしても単なるランダムデータにしか見えないためです。ヘッダーの復号が成功すれば(成功したかどうかを TrueCrypt がどのように判断するかについては暗号化の仕組みを参照)、隠しボリュームのサイズを(RAM に保存されている)復号されたヘッダーから得て、隠しボリュームがマウント(サイズがオフセットを決定します)されます。技術的詳細については技術解説の暗号化の仕組みを参照してください。

稼動中には隠し OS は元になっている OS(図 OS)と同じパーティションにインストールされているように見えます。しかし実際には(隠しボリューム中の)図 OS の後ろにインストールされています。読み書きのすべてはシステムパーティションから隠しボリュームへと透過的にリダイレクトされます。OS もアプリケーションもシステムパーティションへの読み書きが実際には(隠しボリューム中の)後ろにあるパーティションに対するものだということを認識しません。どのようなデータも通常のように(図 OS とは異なる暗号化キーを使って)読み書きは即時に暗号化されたり復号されたりします。

パスワードはもう一つあることに注意してください。外殻ボリュームのパスワードです。これは起動前認証のパスワードではなく、通常の TrueCrypt ボリュームのパスワードです。これは、(隠し OS がある)隠しボリュームを設定してある暗号化パーティションのパスワードであり、パスワードを明かすよう強要する相手に開示しても安全です。このことに確信を持てないとか、外殻ボリュームとは何であるかがわからないなら、隠しボリュームの節を読んでください。

要約すると、合わせて 3 個のパスワードがあるということになります。2 個は図 OS と外殻ボリューム用であり、攻撃者に明かしてもかまいません。最後のパスワード、つまり隠し OS のパスワードを秘密にすればいいのです。



隠し OS があるシステムドライブのレイアウト例

隠し OS 作成手順

隠し OS 作成を開始するには「システム -> 隠し OS 作成」を選択し、ウィザードの指示にしたがってください。

最初に、ウィザードはシステムドライブに隠し OS に適したパーティションがあるかどうかを確認します。隠し OS を作る前に、システムドライブにパーティションを作っておく必要があることに注意してください。それはシステムパーティションの直後に置かなくてはなりませんし、システムパーティション(現在稼働中の OS がインストールされているパーティション)より少なくとも 5% 大きい必要があります。しかし、外殻ボリューム(システムパーティションと混同しないように)が NTFS でフォーマットされていれば、隠し OS のパーティションの大きさは少なくとも 110%(2.1 倍)の大きさが必要になります。というのは、NTFS ファイルシステムは常に内部データを正確にボリュームの中央に置くため、システムパーティションの複製を置く隠しボリュームはそのパーティションの後半部分を使うことになるからです。

次のステップでは、ウィザードはシステムパーティションの直後のパーティションに二つの TrueCrypt ボリューム(外殻と隠し)を作ります。隠しボリュームは隠し OS を格納することになります。隠しボリュームの大きさは常にシステムパーティションと同じです。その理由は、隠しボリュームはシステムパーティションの内容の複製(下記参照)を格納しなくてはならないからです。複製は元のものとは異なる暗号化キーで暗号化されることに留意してください。いくつかの秘密にしているように見せるファイルを外殻ボリュームにコピーする前に、ウィザードは隠しボリュームに十分な空き領域が残るように、ファイルが占めることができる最大領域サイズをユーザーに通知します。

注意: 秘密にしているように見せるファイルを外殻ボリュームにコピーした後に、外殻ボリュームの最後に一致する連続した空き領域サイズを決定するために、クラスター配置が調査されます。この領域は隠しボリュームを格納することになり、それが可能なサイズの上限になります。隠しボリュームの最大可能サイズが決定され、システムパーティションより大きいかどうか(システムパーティションの全内容が隠しボリュームにコピーされる必要があるから - 下記参照)が確認されます。このようにして、外殻ボリュームにあるデータがどれも隠しボリュームに書かれるデータ(つまりシステムの複製)で上書きされないことを確実にします。隠しボリュームのサイズは常にシステムパーティションのサイズと同じになります。

次に TrueCrypt はシステムパーティションの内容を隠しボリュームにコピーすることで、隠し OS を作成します。コピーされるデータは 4 OS とは異なるキーで即時に暗号化されます。コピー作業はブート前(Windows 開始前)に実行され、完了まで長時間がかかります。システムパーティションの大きさやコンピュータの性能によりますが、数時間から数日かかることもあります。作業を中断してコンピュータをシャットダウンし、OS を開始して作業を再開することもできます。しかし、中断するとシステムコピーの全過程を最初からやりなおすことになります。(なぜならシステムパーティションの内容は複製中に変更があってはいけないからです)隠し OS はウィザードを開始した OS の複製なのです。

Windows はユーザーが知ること同意もなくシステムパーティションにいろいろな記録ファイル(ログファイル)や臨時ファイルを作ります。同様に RAM の内容を休止(ハイバネーション)ファイルやページングファイルに書き出します。このことは、敵対者が元の OS(隠し OS の複製元)があるパーティションのファイルを調べると、TrueCrypt ウィザードを隠し OS 作成モードで使ったこ

と(コンピュータに隠し OS があることを示す)に気づくかもしれません。このようなことを防ぐために、TrueCrypt は元の OS があるパーティションの全内容を安全に消去します。その後みせかけの拒否をするために TrueCrypt はユーザーにそのパーティションに新しいシステムをインストールし、TrueCrypt で暗号化するよう通知します。このようにして ㊦ OS が作成され、隠し OS 作成の全過程が完了します。

みせかけの拒否とデータ漏洩防御

安全上の理由から、隠し OS が稼働中の場合には TrueCrypt はすべての非暗号化ファイルシステムと非隠しボリュームを読み取り専用(つまり、そのようなファイルシステムや TrueCrypt ボリュームには何のファイルも書き込まれない)として扱います。¹データは TrueCrypt 隠しボリュームにのみ(隠しボリュームが非暗号化ファイルシステムあるいは他の読み出し専用ファイルシステムにあるコンテナに置かれていない限りは)書き込みが可能です。

このような対策が組み込まれているのには三つの理由があります。

- このようにすることで、TrueCrypt 隠しボリュームをマウントする安全な環境を作ります。隠しボリュームは隠し OS 稼働中にのみマウントされるようにすることを公式に推奨します。詳細は隠しボリュームの安全に関する予防策を参照してください。
- いくつかの場合に、OS の特定の状態(たとえばファイルシステムジャーナルやタイムスタンプ、アプリケーションログ、エラーログの分析や比較によって)の元で特定の時刻に特定のファイルシステムがマウントされない(あるいはファイルシステムの特定のファイルが保存されないとか、内部からアクセスできない)ように決定することができます。これはコンピュータに隠し OS がインストールされていることを示してしまうかもしれません。この対策はこの問題を防止します。
- ㊦ OS や隠し OS の元でマウントされたファイルシステムを、システムが休止した場合にも完全さを守ります。

㊦ OS から隠しシステムに安全にファイルを転送する必要があるなら、下記の手順にしたがってください。

1. ㊦システムを開始する。
2. ファイルを非暗号化ボリュームか TrueCrypt 外殻/通常ボリュームに保存する。
3. 隠し OS を開始する。
4. TrueCrypt ボリュームに保存したなら、マウントする。(自動的に読み取り専用でマウントされる)
5. ファイルを隠しシステムパーティションあるいは他の隠しボリュームにコピーする。

単一ドライブに二つの TrueCrypt パーティションがあることの説明のしかた

敵対者が、ディスク全体を一つの暗号化キーで暗号化せずに、単一ドライブに二つの TrueCrypt

¹これは CD/DVD のようなメディアや、非標準的なデバイスやメディアには適用されません。

パーティション(システムパーティションと非システムパーティション)を作った理由を聞いてくるかもしれません。そうした理由としてはいろいろと考えられます。しかし、何も思いつかない(隠し OS を作ったこと以外)なら例として下記の説明のうちの一つを答えればいいでしょう。

- システムドライブに二つ以上のパーティションがあり、二つ(システムパーティションとその直後のもの)を暗号化し、それ以外のパーティションを非暗号化のままにしたい(たとえば、機密ではないデータの非暗号化パーティションへの読み書きの性能を高めるため)なら、唯一の方法は両方のパーティションを別々に暗号化することです。(TrueCrypt は単一の暗号化キーではシステムドライブ全体、つまりシステムドライブ上のすべてのパーティションを暗号化することはできますが、二つだけを選んで暗号化することはできないことに注意してください。単一キーでは一つのパーティションだけか、すべてのパーティションを暗号化するかのどちらかです)結果として、システムドライブには隣接した二つ(第一にシステムパーティション、次に非システムパーティション)の TrueCrypt パーティションがあることになり、それぞれが異なったキーで暗号化されます。(隠し OS を作った場合でも同様で、これが説明になります)

システムドライブに複数のパーティションがなければならない、いい理由を思いつかなければ：

一般的に非システムファイル(文書)はシステムファイルと別にしておくことが推奨されています。このためにはシステムドライブに二つのパーティション、一つは OS 用、もう一つは文書(非システムファイル)用、を作るのがもっとも簡単で確実な方法です。

この方法が推奨されている理由は

- パーティションの一つのファイルシステムが破損すると、そのパーティションのファイルは破損したり失われたりするかもしれません。しかし、他のパーティションのファイルは影響を受けません。
 - 文書を失うことなしに、システムの再インストールが容易になります。(OS の再インストールはシステムパーティションの再フォーマットをとらない、そのパーティションにあるすべてのファイルは失われます)システムが破損した場合には、しばしば再インストールしか方法がないことがあります。
- カスケード(多段処理)暗号化アルゴリズム(たとえば、AES-Twofish-Serpent)は非カスケードのもの(たとえば AES)より 4 倍遅くなることがあります。しかし、カスケード暗号化アルゴリズムは非カスケードのものより安全性が高くなります。(たとえば暗号化理論の進歩によって、三つの個別の暗号化アルゴリズムが破られる可能性は、一つだけのものが破られる可能性より、はるかに低くなります)したがって、**OS** は非カスケードで、外殻ボリュームをカスケード暗号化アルゴリズムで暗号化したとすると、システムパーティションには最高の性能(付随して安全性も)が、機密ではあるものの(非常に頻繁に使い、最高の性能がほしい OS ではなく)アクセスが比較的少ないデータを保存する非システムパーティション(つまり外殻ボリューム)には最高の安全性(性能は落ちますが)が欲しかったと答えることができます。システムパーティションには、非システムパーティション(つまり外殻ボリューム)に保存するものより重要ではない(しかし頻繁にアクセスする)データを置きます。
 - 外殻ボリュームをカスケード暗号化アルゴリズム(たとえば、AES-Twofish-Serpent)で暗号化し、**OS** を非カスケードのもの(たとえば AES)で暗号化しているならば、これはシステム暗号化のときにカスケード暗号化アルゴリズムを選択しようとする警告が出る(下記

の問題リスト参照)のを避けるためだと答えることもできます。しかし、それでも非常に機密性が高いデータを守るため、(非カスケードより安全な)カスケード暗号化アルゴリズムを使いたかったので、第二パーティションを作って、上記の問題が出ない(システムパーティションではないから)ので、カスケード暗号化アルゴリズムで暗号化した、というわけです。システムパーティションには、非システムパーティション(つまり外殻ボリューム)に保存するものより重要ではない(しかし頻繁にアクセスする)データを置きます。

注意：システムパーティションをカスケード暗号化アルゴリズムで暗号化しようとする、TrueCrypt は下記の問題が起こりうるという警告を出し、非カスケード暗号化アルゴリズムを選ぶことを推奨します。

- カスケード暗号化アルゴリズムでは TrueCrypt ブートローダーのサイズが通常より大きくなります。そのため最初のトラックに TrueCrypt ブートローダーのバックアップを格納する余地がなくなります。それが破損した場合(ある種のプログラムの不適切に設計された不正コピー対策ツールのよう、しばしば発生します)には、ユーザーは TrueCrypt ブートローダーを修復したりブートしたりするために TrueCrypt レスキューディスクを使わなくてはなりません。
 - メモリー容量を多く必要とするために、いくつかのコンピュータではシステムパーティション/ドライブの暗号化ができないことがあります。
 - いくつかのコンピュータではハイバネーションからの復帰に時間がかかります。
- TrueCrypt 非システムボリュームのパスワードにくらべて、起動前認証のパスワードはコンピュータの電源を入れたときや再起動時には毎回入力する必要があります。したがって、起動前認証のパスワードが長い(安全にはそのほうがよい)と頻繁に入力するのは面倒です。このため、システムパーティション(☑ OS)に短い(弱い)パスワードを使うほうが簡単だし、もっとも機密にしたい(しかし、頻繁にはアクセスしない)データを非常に長いパスワードをつけた TrueCrypt 非システムパーティション(つまり、外殻ボリューム)に保存するほうが便利だと答えることができます。
システムパーティションのパスワードは短く弱いため、機密データをシステムパーティションに保存してはいけません。しかし、機密にしたほうがいい、あるいは適度に機密であるデータ(たとえば、ブラウザが記憶する訪問したオンラインフォーラムのパスワードやブラウジング履歴、使ったアプリケーション、その他)はコンピュータの日々の使用によってシステムパーティションに保存されるので、システムパーティションが暗号化されているほうが望ましいといえます。
 - (外でノート PC を使っていたりして)攻撃者が TrueCrypt ボリュームがマウントされた状態のコンピュータを入手してしまった場合、通常はボリュームの内容すべてを(即時復号なので)読まれてしまいます。ですから、ボリュームがマウントされている時間を最小にするのが賢明なことです。しかし、機密データがシステムパーティションあるいは全体的に暗号化されたシステムドライブに置かれていると、このようにするのは明らかに不可能です。(なぜなら、コンピュータを使う時間を最小にしなくてはならなくなってしまうからです)ですから、機密重要データを保管するために(システムパーティションとは別のキーで暗号化した)別のパーティションを作り、必要なときだけマウンとし(ボリュームがマウントされている時間を極小にするために)可能なかぎりすぐにアンマウントするようにしていると答えることができます。システムパーティションには、非システムパーティション(つまり外殻ボリューム)に保存するものより重要ではない(しかし頻繁にアクセスする)データを置

きます。

隠し OS の安全に関する予防策

隠し OS は TrueCrypt 隠しボリュームに置かれることになるので、隠し OS を使う場合には通常の TrueCrypt 隠しボリュームの安全のための予防策にしたがうべきです。これらの予防策は隠し OS に関連する追加の予防策と同様に隠しボリュームの安全に関する予防策に記載されています。

警告：隠しボリュームを保護(方法については隠しボリュームを破損から守るを参照)しないなら、外殻ボリューム(**隠し OS** は外殻ボリュームにインストールされているのではないことに注意)に書込みをしてはいけません。そうでないと、隠しボリューム(および、その中の隠し OS)を破損してしまうでしょう。

ウィザードのすべての指示にしたがい、隠しボリュームの安全に関する予防策で述べられている予防策にもしたがっていけば、外殻ボリュームがマウントされていたり **隠し OS** が非暗号化されたり開始したりしていても、隠しボリュームや隠し OS が存在することを立証することは不可能です。

システム暗号化

TrueCrypt はシステムパーティションまたはシステムドライブ全体(Windows がインストールされ起動するパーティションやドライブ)を自動即時暗号化することができます。

システム暗号化は、**Windows** とアプリケーションが作成しシステムパーティションに置かれるすべての臨時ファイル(一般的には使用者が知ることも同意もなく作られる)やハイバネーションファイル、スワップファイルなども常に(とつぜんの電源断でも)完全に暗号化するため、安全性とプライバシー保護を最高レベルにします。また、**Windows** は大量の秘密にするべきであろうデータ、たとえば開いたファイルや使ったアプリケーションの名前や保存場所など、を記録します。このようなすべてのログファイルやレジストリ項目も同様に常に暗号化されます。

システム暗号化は起動前認証をとません。これは、暗号化システムを起動したり暗号化システムドライブに保存されたファイルの読み書きをしようとする場合には、**Windows** がブート(開始)する前に毎回正しいパスワード入力が必要になるということです。起動前認証は、ブートドライブ(起動ドライブ)および TrueCrypt レスキューディスク(下記参照)の最初のトラックにある TrueCrypt ブートローダーが扱います。

TrueCrypt は既存の非暗号化システムパーティション/ドライブを OS が動作中にそのままの状態でも暗号化できることに留意してください。(システムが暗号化されている間、そのコンピュータを制限なしに通常のように使うことができます) おなじように、TrueCrypt で暗号化されたシステムパーティション/ドライブは OS が動作中にそのままの状態でも復号されます。暗号化または復号のプロセスはいつでも中断できますし、パーティション/ドライブの一部を非暗号化状態のままにしたり、再起動、終了することもでき、プロセスは中断したところから再開されます。

システム暗号化の動作モードは XTS(動作モードを参照)です。 システム暗号化についての技術的詳細は技術解説の暗号化の仕組みの節を読んでください。

システムパーティションまたはシステムドライブ全体を暗号化するには「システム -> システムパーティション/ドライブの暗号化」を選択し、ウィザードの指示に従ってください。システムパーティション/ドライブを復号するには、「システム -> システムパーティション/ドライブの暗号化解除」を選択してください。

システム暗号化ができる OS

TrueCrypt は今のところ、下記の OS を暗号化することができます。

- Windows Vista
- Windows Vista x64 (64-bit) Edition
- Windows XP
- Windows XP x64 (64-bit) Edition
- Windows Server 2008
- Windows Server 2008 x64 (64-bit)

- Windows Server 2003
- Windows Server 2003 x64 (64-bit)

TrueCrypt レスキューディスク

システムパーティション/ドライブの暗号化の準備過程で、TrueCrypt は以下の目的のため TrueCrypt レスキューディスク (CD/DVD) の作成を要求します。

- コンピュータを起動しても TrueCrypt ブートローダー画面が表示されない(あるいは、Windows が起動しない)ときには、**TrueCrypt ブートローダーが破損しているかもしれません**。TrueCrypt レスキューディスクはそれを復旧し、暗号化されたシステムやデータに再度アクセスできる(ただし、正しいパスワード入力が必要)ようにします。レスキューディスク画面で、「**Repair Options > Restore TrueCrypt Boot Loader (修復オプション -> TrueCrypt ブートローダーの復旧)**」を選択してください。動作選択を確認するために Y を押し、レスキューディスクを CD/DVD ドライブから取り外し、コンピュータを再起動してください。
- 正しいパスワードを入力しても TrueCrypt がパスワードが間違っていると回答してくる場合は、**マスターキーまたは他の重要なデータが破損している可能性があります**。TrueCrypt レスキューディスクはそれを復旧し、暗号化されたシステムやデータに再度アクセスできる(ただし、正しいパスワード入力が必要)ようにします。レスキューディスク画面で、「**Repair Options > Restore key data (修復オプション -> キーデータの復旧)**」を選択してください。それからパスワードを入力し、動作選択を確認するために Y を押し、レスキューディスクを CD/DVD ドライブから取り外し、コンピュータを再起動してください。

注意：この機能は隠し OS(隠し OS の節を参照)が存在する隠しボリュームのヘッダーを復旧することには使えません。このようなボリュームのヘッダーを復旧するには、「デバイスの選択」をクリックし、ブートパーティションの直後のパーティションを選択し OK とし、「ツール -> ボリュームヘッダーのリストア」を選択し、あとは指示にしたがってください。う

警告：TrueCrypt レスキューディスクでキーデータを復旧するということは、パスワードも TrueCrypt レスキューディスクを作成した時点で有効だったものにもどるということです。ですから、パスワードを変更するつど、TrueCrypt レスキューディスクを破壊廃棄して、新しい TrueCrypt レスキューディスクを作成すべきです。(「システム -> レスキューディスク作成」を選択) そうでないと、攻撃者がキーロガーなどで古いパスワードを知っていて、古い TrueCrypt レスキューディスクを入手すると、それらを使ってキーデータを古いパスワードで暗号化されたマスターキーに戻すことができ、システムパーティション/ドライブを復号することができてしまいます。

- **TrueCrypt ブートローダーが破損したりマルウェアに感染したりした場合**には、それから起動せずに TrueCrypt レスキューディスクから直接起動することができます。レスキューディスクを CD/DVD ドライブに挿入し、レスキューディスク画面でパスワードを入力して

ください。

- **Windows が破損し起動できない場合は、TrueCrypt レスキューディスクが Windows 起動前にパーティション/ドライブを完全に非暗号化状態に戻す(復号する)ことができます。**レスキューディスク画面で、「**Repair Options > Permanently decrypt system partition/drive (修復オプション -> システムパーティション/ドライブの暗号化を解除)**」を選択してください。それから正しいパスワードを入力し、復号が完了するまで待ってください。その後、MS Windows インストール CD から起動して、Windows を修復してください。この機能は隠し OS(隠し OS の節を参照)が存在する隠しボリュームのヘッダーを復旧することには使えません。

注意: ほかの手段として、Windows が破損(起動しない)して、それを修復(あるいはそのファイルにアクセスする)必要があるなら、以下の手順でシステムパーティション/ドライブを復号せずにすますこともできます。:.コンピュータに複数の OD がインストールされているなら、起動前認証を必要としない OS を起動してください。もし複数の OS がインストールされていないなら、WinPE または BartPE CD/DVD からブートするか、システムドライブを他のコンピュータのセカンダリまたは外付けドライブとして接続し、そのコンピュータの OS をブートしてください。システムが起動したら、TrueCrypt を起動し、「デバイスの選択」をクリックし問題のシステムパーティションを選択します。次に「システム -> 起動前認証をせずにマウントする」を選択し、起動前認証用のパスワードを入力し OK をクリックしてください。それでパーティションは通常の TrueCrypt ボリュームとしてマウントされます。(データは通常どおり、アクセスするつど RAM で即時に復号/暗号化されます)

- TrueCrypt レスキューディスクはドライブの最初のトラックの元の(TrueCrypt ブートローダーが書き込まれる前の)内容のバックアップを持っています。このため、必要ならそれを復旧することもできます。最初のトラックには通常はシステムローダーかブートマネージャーがあります。レスキューディスク画面で、「**Repair Options > Restore original system loader (修復オプション -> 元のシステムローダーの復旧)**」を選択してください。

もし、TrueCrypt レスキューディスクを紛失し、敵対者がそれを入手したとしても、正しいパスワードなしではシステムパーティションやドライブを復号することはできません。

TrueCrypt レスキューディスクから起動するには、それを CD/DVD ドライブに挿入しコンピュータを再起動してください。TrueCrypt レスキューディスク画面が表示されない(または画面上の'Keyboard Controls'に'Repair Option'がない)場合には、BIOS が CD/DVD よりハードディスクからの起動を優先する設定になっている可能性があります。その場合には、コンピュータを再起動し F2 または Delete キーを(BIOS 開始画面がでるとすぐに)押してください。もし、BIOS 設定画面が表示されなければ、再度コンピュータを起動してコンピュータ起動直後から F2 か Delete を押し続けてください。BIOS 設定画面が表示されたら、BIOS を CD/DVD からの起動を優先するように設定してください。(具体的には BIOS かマザーボードの説明書を読むか、メーカーのサポートに問い合わせてください) その後コンピュータを再起動してください。こんどは TrueCrypt レスキューディスク画面が表示されるはずですが。注意 : TrueCrypt レスキューディスク画面では F8 を押すことで'Repair Option'を選択することができます。

レスキューディスクが破損した場合は、「システム -> レスキューディスクの作成」を選択すれば

新しいものを作成できます。TrueCrypt レスキューディスクが破損しているかどうかを調べるには、それを CD/DVD ドライブに挿入し、「システム -> レスキューディスクのベリファイ」を選択してください。

隠し OS

誰かに OS を復号するように強要されるかもしれません。

こういった要求を拒否できない場合（たとえば暴力による場合）も多く想定できます。TrueCrypt は隠し OS を作成することを可能にし、これは（ガイドラインにしたがっていれば-下記参照）存在することすらわかりません。これによって、隠し OS を復号したり隠し OS のパスワードを明かしたりしなくて済みます。詳細はみせかけの拒否の隠し OS を参照してください。

TrueCrypt ボリューム

二つのタイプの TrueCrypt ボリュームがあります:

- ファイル型 (コンテナ)
- パーティション/デバイス型

注意: 上記の仮想ボリューム作成に加えて、TrueCrypt は Windows がインストールされている物理的なパーティション/ドライブを暗号化することもできます。(詳細は、システム暗号化を参照)

TrueCrypt ファイル型ボリュームは、どんな記憶装置にでも存在することができる通常のファイルです。これは内部に、暗号化され完全に独立した仮想ディスク・デバイスを含みます。

TrueCrypt パーティションは TrueCrypt で暗号化されたハードディスクのパーティションです。ハードディスク、USB ハードディスク、フロッピーディスク、USB メモリスティック、および他の形式の記憶装置の全体をを暗号化することもできます。

新規 TrueCrypt ボリュームの作成

新しく TrueCrypt のファイル形式ボリュームを作ったりパーティションを暗号化(管理者権限が必要)するには、メインウィンドウの「ボリュームの作成」をクリックしてください。TrueCrypt ボリューム作成ウィザードが現れます。ウィザードは現れたらすぐに、新規ボリュームのためのマスターキー、第二キー(XTS モード)、ソルトを生成するためのデータを収集はじめます。収集されたデータは可能な限りランダムであるべきで、マウスの動き、マウスボタンのクリック、キーストロークなどを含み、システムから集められます。(詳細は、乱数発生機構を参照) ウィザードは、新規 TrueCrypt ボリュームを確実に作るために必要な情報とヘルプを提供します。しかしながら、いくつかの項目ではさらに詳細な説明が必要です。

ハッシュアルゴリズム

TrueCrypt がどのハッシュ・アルゴリズムを使うかを選択することができます。選択されたハッシュ・アルゴリズムは、マスターキー、第二キー(XTS モード)、ソルトを生成する乱数発生機構(疑似乱数混合関数)で使われます。(詳細は乱数発生機構を参照) また、これはボリュームの新規ヘッダーキー、第二ヘッダーキーを導出することにも使われます。(詳細はヘッダーキーの導出、ソルト、および反復回数を参照)

実装されているハッシュアルゴリズムについては、ハッシュアルゴリズムを参照してください。

ハッシュ関数の出力は決して直接には暗号化キーとして使われないことを覚えておいてください。詳細は技術解説を参照してください。

暗号化アルゴリズム

新規ボリュームを暗号化する暗号化アルゴリズムを選択することができます。暗号化アルゴリズムはボリューム作成後には変更できないことに注意してください。詳細は暗号化アルゴリズムを参照してください。

クイックフォーマット

ここにチェックが入っていない場合、新規ボリュームの各セクターはフォーマットされます。このことは、新規ボリュームはランダムなデータで完全に満たされるということを意味します。クイックフォーマットははるかに速く実行されますが、安全性は劣ります。なぜなら、ボリューム全体がファイルで満たされるまでは、(空き領域がランダムデータで前もって満たされなかった場合には)どれだけのデータがそのボリュームに存在するかがわかってしまうかもしれないからです。クイックフォーマットをしてもよいかどうか判断がつかない場合には、このオプションにチェックをいれないことを勧めます。パーティション/デバイスを暗号化する場合のみ、クイックフォーマットが可能になることに注意してください。

重要: 隠しボリュームを後で作成するつもりパーティション/デバイスを暗号化する場合は、このオプションにチェックをいれないでください。

ダイナミック

ダイナミックな(動的な)TrueCrypt コンテナは、データの増加にともなって物理的容量(実際のディスク上のサイズ)が増加する NTFS スパースファイルに割り当てられます。TrueCrypt ボリューム上でファイルを削除してもコンテナの物理的容量(実際にディスク上でコンテナが占めるサイズ)は減少しないことに留意してください。コンテナの物理的容量はボリューム生成過程でユーザーがきめた最大値まで増加するだけです。きめられた最大値に達すると、コンテナの物理的容量はそこで一定することになります。

スパースファイルは NTFS ファイルシステムにのみ作成することができます。FAT ファイルシステムにコンテナを作るときには「ダイナミック」オプションは選択不可になります。

Windows や TrueCrypt から返されるダイナミックな(スパースファイルの)TrueCrypt ボリュームのサイズは常にボリューム作成時に指定した最大容量になります。コンテナの現在の物理的容量(ディスク上の実際のサイズ)を知るには、Windows のエクスプローラウィンドウでコンテナファイルを右クリックして、プロパティを選び「ディスク上のサイズ」を見てください。(TrueCrypt のウィンドウ上では、このようになりません)

警告: ダイナミックな(スパースファイルの)TrueCrypt ボリュームでの速度は通常のボリュームより大きく悪化します。また、ダイナミックな(スパースファイルの)TrueCrypt ボリュームはどのセクターが未使用かを知ることができるので、セキュリティも劣ります。さらに、ホストファイルシステムに十分な空き領域がない場合にダイナミックなボリュームに書き込みをすると、暗号化したファイルシステムが破損する可能性があります。

クラスタのサイズ

クラスタはファイル配置の単位です。例えば、1 バイトのファイルのために FAT ファイルシステムで少なくとも 1 個のクラスタを割り当てられます。ファイルがクラスタ境界を越えて大きくなると、別のクラスタが割り当てられます。理論的に、クラスタサイズが大きくなるほど、(性能はありますが)ディスクにより多く無駄な部分が増えます。クラスタサイズにどのような値をセットすればいいかわからなければ、初期値のままにしておいてください。

CD や DVD にある TrueCrypt ボリューム

TrueCrypt ボリュームを CD や DVD に置きたい場合には、まずファイル形式のボリュームをハードディスクに作成してください。それから、CD/DVD 書き込みソフト(Windows XP/Vista ならば、OS 標準の CD 書き込みツールでも可)でそれを CD/DVD に書き込んでください。

Windows2000 で読み出し専用メディア(CD/DVD 他)にある TrueCrypt ボリュームをマウントする場合には、TrueCrypt ボリュームを FAT でフォーマットしなくてはならないことを覚えておいてください。なぜなら Windows2000 では読み取り専用メディアの NTFS ファイルシステムはマウントできないからです。(Windows XP/Vista なら可能です)

ハードウェア/ソフトウェア・レイドと Windows ダイナミックボリューム

TrueCrypt はハードウェア/ソフトウェア・レイドと同様に Windows のダイナミックボリュームをサポートします。

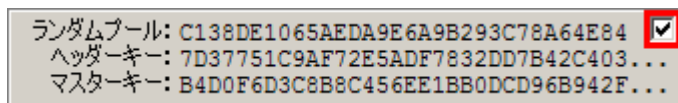
Windows Vista 以降：ダイナミックボリュームは「デバイスの選択」ダイアログに
¥Device¥HarddiskVolumeN として表示されます。

Windows XP/2000/2003 : Windows ダイナミックボリュームを TrueCrypt ボリュームとしてフォーマットする場合には、Windows ダイナミックボリュームを(Windows ディスク管理ツールで)作成した後に TrueCrypt ボリューム作成ウィザードの「デバイスの選択」ダイアログにボリュームを表示させるためにシステムを再起動する必要があることに留意してください。また、「デバイスの選択」ダイアログでは Windows ダイナミックボリュームは単一のデバイス(項目)として表示されないことにも注意してください。また、「デバイス選択」ウィンドウでは、Windows ダイナミックボリュームは単一のデバイス(項目)としては表示されません。そのかわり、Windows ダイナミックボリュームを構成するすべてのボリュームが表示されるので、ダイナミックディスク全体をフォーマットするために、そのうちのどれか一つを選択してください。

ボリューム作成に関する追加情報

ボリューム作成ウィザードの最終段階で「フォーマット」ボタンをクリックしたあと、システムが追加のランダムデータを得るのに少し間があきます。その後、新規ボリュームのためのマスターキー、ヘッダーキー、第二キー(XTS モード)、ソルトなどが生成され、マスターキーとヘッダーキーの内容が表示されます。

セキュリティを強化するために、該当のフィールドの右上のチェックボックスにチェックを入れないことで、ランダムプール、マスターキー、ヘッダーキーの内容を表示しないようにできます。



プール/キーの最初の 128 ビットだけが表示されます(全体の内容ではありません)

TrueCrypt では FAT(FAT12、FAT16、FAT32 のいずれかかはクラスタの数で自動的に決定される) か NTFS のボリュームを作成することができます。(しかし、NTFS ボリュームを作成するには、管理者権限が必要です) マウントされた TrueCrypt ボリュームは、いつでも FAT(FAT12、FAT16、FAT32)や NTFS にフォーマットしなおすことができます。これらは通常のディスク・デバイスと同じに扱うことができるので、マウントされた TrueCrypt ボリュームのドライブレターを(たとえば、「コンピュータ」または「マイ コンピュータ」の中で)右クリックしてフォーマットを選択してください。

TrueCrypt ボリュームに関する詳細については、隠しボリュームも参照してください。

メインプログラムウィンドウ

ファイルの選択

ファイル形式の TrueCrypt ボリュームを選びます。選択したあとで、いろいろな操作(たとえば「マウント」をクリックすることでマウント)ができます。ボリュームのアイコンを TrueCrypt.exe のアイコンまたはメインプログラムウィンドウにドラッグ&ドロップして、TrueCrypt を起動させることもできます。

デバイスの選択

TrueCrypt パーティションか記憶デバイス(たとえばフロッピーディスクや USB メモリスティック)を選びます。選択したあとで、いろいろな操作(たとえば「マウント」をクリックすることでマウント)ができます。

補足: TrueCrypt パーティション/デバイスをマウントするもっと簡単な方法があります。デバイスの自動マウントを参照してください。

マウント

「マウント」をクリックすると、TrueCrypt はキャッシュにパスワードがあればそれを使ってマウントしようとします。キャッシュになれば、ユーザーにパスワード入力を要求します。正しいパスワードを入力すれば、マウントされることになります。正しいパスワードを入力するか(あるいは正しいキーファイルを指定すれば)、ボリュームはマウントされます。

重要: TrueCrypt アプリケーションを終了しても TrueCrypt ドライバーが機能しており、どの TrueCrypt ボリュームもアンマウントされません。

デバイスの自動マウント

この機能を使うと(「デバイスの選択」を使って)手動で目的のパーティション/デバイスを選択しなくても TrueCrypt パーティション/デバイスをマウントすることができます。TrueCrypt はあなたのシステムの有効なパーティション/デバイスのヘッダーを調べて、それぞれを TrueCrypt ボリュームとしてマウントしようとします。TrueCrypt パーティション/デバイスであるかどうかは特定できず、使われている暗号の種類も特定できないことに注意してください。ですから、プログラムは目的の TrueCrypt パーティションを直接には見つけることはできません。そのかわり、TrueCrypt は暗号化されていてもいなくても、すべての暗号化アルゴリズムと(存在するなら)キャッシュにあるパスワードを使って、パーティション/デバイスを一つずつ試します。このため遅いマシンでは、このプロセスに長時間かかることは了承してください。

入力したパスワードが不正であれば、キャッシュのパスワードを(存在すれば)使ってマウントを試行します。デバイスの自動マウントでは、空のパスワードを入力し「キーファイルの使用」にチェックが入っていなければ、パーティション/デバイスのマウント試行にはキャッシュされたパスワードのみが使われます。マウントオプションを設定する必要がなければ、「デバイスの自動マ

ウント」でシフトキーを押しながらクリックすることで、パスワード入力要求をとばしてしまうこともできます。(この場合、存在すればキャッシュされたパスワードのみが使われます)

ドライブレターはメインウィンドウのドライブリストで選択された最初のものに割り当てられます。

アンマウント

TrueCrypt ボリュームをアンマウントすると、そのボリュームは読み書き不可になります。

すべてアンマウント

TrueCrypt ボリュームをアンマウントすると、そのボリュームは読み書き不可になります。この機能は、現在マウントされているすべての TrueCrypt ボリュームをアンマウントします。

記憶したパスワードの消去

ドライバのメモリーに記憶(キャッシュ)されたすべてのパスワード(処理されたキーファイルの内容を含む)を消去します。キャッシュにパスワードが存在しなければ、このボタンは押せないようになっています。(詳細はパスワードをドライバのメモリーに記憶するを参照)

履歴を保存しない

これが無効になっていると、マウントしたボリュームの直近 20 件のファイル名やパスは履歴ファイルに保存されます。(履歴はメインウィンドウのボリュームのコンボボックスをクリックすると表示されます) このオプションが有効になると、TrueCrypt はコンテナやキーファイルが Windows のファイル選択でどこから選択されていようとも Windows のファイル選択機能が TrueCrypt について作成したレジストリエントリをクリアし、現在のディレクトリをユーザーのホームディレクトリとして設定します。(トラベラーモードの場合は、TrueCrypt が起動されたディレクトリに設定します) ですから、Windows のファイル選択機能は最後にマウントされたコンテナ(または最後に選択されたキーファイル)のパスを記憶しません。さらに、このオプションが有効になっていれば、TrueCrypt をどこに隠したとしても TrueCrypt の主ウィンドウのボリュームパス入力欄はクリアされます。

補足: 「ツール → ボリューム履歴の消去」を選んで、ボリューム履歴を消去することができます。

終了

TrueCrypt アプリケーションを終了します。ドライバーは継続して動作し、TrueCrypt ボリュームはアンマウントされません。トラベラーモードのときには、ドライバは必要がなくなれば(つまり、主アプリケーションとボリューム作成ウィザードが閉じられ、マウントされた TrueCrypt ボリュームがない状態になったとき)、メモリーから除去されます。しかし、TrueCrypt がトラベラーモ

ードで動いているときに、TrueCrypt ボリュームが強制的にアンマウントされると「終了」しても TrueCrypt ドライバーは除去されません。(システムを停止するかリスタートする場合のみ、除去されます) これは Windows のバグによって引き起こされるいろいろな問題(たとえば、アンマウントされたボリュームを使っているアプリケーションがあると TrueCrypt を再起動できない)を防止します。

ボリュームツール

ボリュームパスワードの変更

ボリューム -> ボリュームのパスワードを変更するを参照

ヘッダーキー導出アルゴリズムの設定

ボリューム -> ヘッダーキー導出アルゴリズムの設定を参照

ボリュームヘッダーのバックアップ

ツール -> ボリュームヘッダーのバックアップを参照

ボリュームヘッダーのリストア

ツール -> ボリュームヘッダーのリストアを参照

プログラムメニュー

注意: 自明のメニュー項目は、このドキュメントでは説明しません。

ボリューム -> デバイスのボリュームをすべて自動でマウント

デバイスの自動マウントの項を参照。

ボリューム -> 現在マウントされているボリュームをお気に入りに保存

この機能はひんばんに一つあるいは複数の TrueCrypt ボリュームを同時に開いて仕事をし、それらがつねに特定のドライブレターにマウントされている必要がある場合に役に立ちます。

すべての現在マウントされているボリューム(およびマウントされているドライブレター)がアプリケーションのデータを保存するフォルダー(たとえば *C:\Documents and Settings\YourUserName\Application Data\TrueCrypt*)に **Favorite Volumes.xml** という名前のファイルに保存されます。トラベラーモードでは、ファイルは **TrueCrypt.exe** を起動したフォルダー(**TrueCrypt.exe** が存在するフォルダー)に保存されます。

この機能を使うと、お気に入りに以前に保存したすべてのアンマウントされたボリュームはお気に入りリストから削除されます。

「お気に入りに」として保存されたボリュームをマウントするには、**ボリューム -> お気に入りにボリュームをマウント**を選択してください。

お気に入りにボリュームリストを削除するには、TrueCrypt ボリュームをすべてアンマウントし、「**ボリューム -> 現在マウントされているボリュームをお気に入りにして登録**」を選択してください。

ボリューム -> お気に入りにボリュームをマウント

この機能は、以前に「お気に入りに」として保存したボリュームをマウントします。上記の**ボリューム -> 現在マウントされているボリュームをお気に入りに保存**を参照してください。

ボリューム -> ヘッダーキー導出アルゴリズムの設定

この機能は、異なる PRF 関数で導出されたヘッダーキーでボリュームヘッダーの再暗号化を可能にします。(たとえば、HMAC-RIPEMD のかわりに HMAC-Whirlpool を使うということが可能です) ボリュームヘッダーはボリュームを暗号化するマスターキーを含んでいることに留意してください。このため、この機能を使ってもボリュームに保存されたデータはいっさい失われることはありません。詳細は「技術解説」の章、ヘッダーキーの導出、ソルト、および反復回数を参照してください。

注意: TrueCrypt がボリュームヘッダーを再暗号化する場合、敵対者が微視的残留磁気[17]から上書きされたヘッダーを復元できないようにするため、最初に元のボリュームヘッダーをランダムデータで 200 回の上書きをします。(安全のための予防策も参照)

ボリューム -> ボリュームのパスワードを変更する

現在選ばれている TrueCrypt ボリュームのパスワードを変更することができます。(通常ボリュームか隠しボリュームかを問いません) ヘッダーキーと第二ヘッダーキー(XTS モード)のみが変更され、マスターキーは変更されません。この機能は、新しいパスワードから導出されるヘッダー暗号化キーを使ってボリュームヘッダーを再暗号化します。ボリュームヘッダーはボリュームを暗号化するマスターキーを格納していることに留意してください。ですから、この機能を使ってもボリュームに保存されたデータが失われることはありません。(パスワード変更は、ほんの数秒で完了します)

TrueCrypt ボリュームのパスワードを変更するには、「ファイルの選択」か「デバイスの選択」をクリックし、ボリュームを選択し、「ボリュームツール」メニューで「ボリュームパスワードの変更」を選んでください。

注意: 起動前認証用パスワードの変更のしかたについては、システム-> パスワードの変更を参照してください。

安全のための予防策も参照してください。

導出アルゴリズム:

この入力欄では、新しいボリュームヘッダーキー(詳細はヘッダーキーの導出、ソルト、および反復回数を参照)の導出と新しいソルト(詳細は乱数発生機構を参照)を生成したり、新しいソルトを生成(乱数発生機構を参照)するアルゴリズムを選択することができます。

注意: TrueCrypt がボリュームヘッダーを再暗号化する場合、敵対者が微視的残留磁気[17]から上書きされたヘッダーを復元できないようにするため、最初に元のボリュームヘッダーをランダムデータで 200 回の上書きをします。(安全のための予防策も参照)

システム-> パスワードの変更

起動前認証用パスワードを変更します。(システム暗号化を参照)

警告: TrueCrypt レスキューディスクでキーデータを復旧するということは、パスワードも TrueCrypt レスキューディスクを作成した時点で有効だったものにもどるということです。ですから、パスワードを変更するつど、TrueCrypt レスキューディスクを破壊廃棄して、新しい TrueCrypt レスキューディスクを作成すべきです。(「システム -> レスキューディスク作成」を選択) そうでないと、攻撃者が古い TrueCrypt レスキューディスクを発見し、それでキーデータを復旧すると、古いパスワードを使ってシステムパーティション/ドライブを復号できるかもしれません。安全のための予防策も参照してください。

システム -> 起動前認証をせずにマウントする

システム暗号化のキーの効力の範囲にあるパーティションを起動前認証をせずにマウントする必要がある場合には、ここをチェックしてください。たとえば、稼働中でないほかの OS の暗号化システムドライブにあるパーティションをマウントする必要があるような場合です。これは TrueCrypt で暗号化された OS を(他の OS 上で)修復したり、バックアップするときに役立ちます。

注意 1: 複数のパーティションを同時にマウントする必要がある場合は、「デバイスの自動マウント」を選択し、「マウントオプション」をクリックし、「システムを暗号化したパーティションを起動前認証せずにマウント」を有効にしてください。

この機能は全体的に暗号化されたシステムドライブにある拡張(論理)パーティションでは使えないことに注意してください。

ツール -> ボリューム履歴を消去

直近 20 件の正常にマウントされたボリュームのファイル名(ファイル型の場合)とパスのリストを消去します。

ツール -> トラベラーディスクセットアップ

トラベラーモードの章を参照してください。

ツール -> キーファイル生成

キーファイル -> ランダムキーファイルの生成を参照してください。

ツール -> ボリュームヘッダーのバックアップ

ツール -> ボリュームヘッダーのリストア

TrueCrypt ボリュームのヘッダーが破損すると、ほとんどの場合はマウント不可能になります。このため TrueCrypt 6.0 以降で作成されたボリュームはボリュームの最後の部分にバックアップを付加しています。さらに安全にするために、外部にボリュームヘッダーのバックアップを作成することができます。このためには、「デバイスの選択」または「ファイルの選択」をクリックし、「ツール -> ボリュームヘッダーのバックアップ」を選択し、指示にしたがってください。

注意：(付加された、または外部の)バックアップヘッダーはオリジナルのヘッダーキーのコピーではなく、異なるソルトを使って導出された異なるヘッダーキーで暗号化されています。(ヘッダーキーの導出、ソルト、および反復回数を参照) ボリュームパスワードやキーファイルが変更されたり、ヘッダーが付加された(または外部の)ヘッダーバックアップから復旧されたりすると、ボリュームヘッダーと(ボリュームに付加された)バックアップヘッダーは新しく生成されたソルト(バックアップヘッダーのソルトとボリュームヘッダーのソルトは異なります)で導出されたヘッダーキー

一で再暗号化されます。それぞれのソルトは **TrueCrypt** 乱数発生機構で生成されます。(乱数発生機構を参照)

両方の(付加されたものと外部の)ヘッダーバックアップはボリュームヘッダーの破損を修復するのに使えます。このためには「デバイスの選択」または「ファイルの選択」をクリックし、「ツール -> ボリュームヘッダーのリストア」を選択し、指示にしたがってください。

警告：ボリュームヘッダーを復旧すると、ボリュームパスワードもバックアップが作成された時点のものに戻ります。さらに、バックアップが作成された時点でキーファイルが必要だったとすると、ボリュームヘッダー復旧後にマウントするには前と同じキーファイルが必要になります。詳細は技術解説の暗号化の仕組みを参照してください。

ボリュームヘッダー作成後にボリュームパスワードやキーファイルを変更したら、新しいバックアップを作成する必要があります。そうでなければ、ボリュームヘッダーは変更されないままであり、バックアップは最新のもののままということになります。

注意：ソルト(連続したランダム値)は別として、外部のヘッダーバックアップは非暗号化情報をいっさい含まず、正しいパスワードやキーファイルなしに復号することはできません。詳細は技術解説を参照してください。

外部にヘッダーバックアップを作成すると、標準ボリュームヘッダーと隠しボリュームのヘッダーが格納されているかもしれない領域の両方がバックアップされます。そのボリュームに隠しボリュームがないとしても(隠しボリュームのみせかけの拒否を確実にするために)、そのようになります。ボリュームに隠しボリュームがなければ、バックアップファイルの隠しボリュームのヘッダーがあるはずの領域は(みせかけの拒否のために)ランダムな値になります。

ボリュームヘッダーをリストアするときには、隠しボリュームのヘッダーか標準ボリュームのヘッダーかを選択することになります。一度に一つのヘッダーのみをリストアすることができます。両方のヘッダーをリストアする場合は、この機能を二回実行する必要があります。(「ツール」 -> 「ボリュームヘッダーのリストア」) ユーザーはボリュームヘッダーのバックアップが作成された時点で有効だったパスワードやキーファイルが必要になります。復旧しようとするボリュームの種類によってパスワードやキーファイルは自動的に決定されます。つまり、標準か隠しかということです。(TrueCrypt は試行してみることで種類を決定することに留意してください)

注意：ボリュームマウント時に正しいパスワード入力やキーファイルの用意に 2 回連続して失敗すると、ユーザーがボリュームをマウントしようとするたびに(キャンセルがクリックされるまで)、TrueCrypt は自動的に(正規のヘッダーに加えて)付加されたバックアップヘッダーを使ってマウントしようとします。TrueCrypt が正規のパスワードの復号に失敗しても、付加されたバックアップヘッダーの復号に同時に成功すれば、ボリュームはマウントされ、ユーザーにはボリュームヘッダーが破損しているという警告が(修復方法の案内とともに)出されます。

補足: この仕組みは企業などで、ユーザーがパスワードを忘れた(あるいは、キーファイルを失った)場合の対策として使うこともできます。ボリュームを作ったあと、管理者権限を持たないユーザーにそのボリュームの使用を認める前に、(ツール -> ボリュームヘッダーのバックアップを選択して)そのヘッダーのバックアップをとります。パスワード/キーファイルから導出された暗号化されたヘッダーキーで暗号化されているボリュームヘッダーは、ボリュームを暗号化したマスターキーを持っています。そこで、ユーザーにパスワードを選んでもらいその人のためにパスワード

ドを設定します。(ボリューム -> ボリュームのパスワード変更) そうすれば、ユーザーにそのボリュームの使用許可を与えるとともに、いつでも管理者の許可や助力なしで任意のパスワードに変更させることができます。ユーザーが自分が決めたパスワードを忘れた場合でも、ボリュームヘッダーのリストアを実行(ツール -> ボリュームヘッダーのリストア)をすることで、ボリュームのパスワードをオリジナルの管理者パスワード/キーファイルに戻すことができます。

設定 -> 各種設定

設定ダイアログを起動して、下記のいろいろな項目を変更できます。

終了時に記憶していたパスワードを消去

有効にされていれば、ドライバのメモリーに記憶されているパスワード(処理されたキーファイルを含む)を、TrueCrypt 終了時に消去します。

パスワードをドライバのメモリーに記憶する

チェックされていると、直近の正常にマウントされた TrueCrypt ボリュームのパスワードやキーファイルの内容を最大 4 件まで記憶します。これはボリュームをマウントするときに、繰り返し同じパスワードを入力したりキーファイルを選択したりしなくてもよくします。TrueCrypt は絶対にいかなるパスワードもディスクには保存しません。(しかし、安全のための予防策も参照してください) パスワードの記憶は設定(設定 -> 各種設定)とパスワード入力ウィンドウで有効にも無効にもできます。

マウント成功時にそのボリュームのウィンドウを開く

このオプションがチェックされていると、TrueCrypt ボリュームが正常にマウントされたあと、エクスプローラのウィンドウが自動的に開きそのボリュームのルートディレクトリ(たとえば T:\) を表示します。

ボリュームがアンマウントされたときウィンドウを閉じる

TrueCrypt ボリュームをアンマウントしたいときに、そのボリュームにある何かのファイルかフォルダーが使用中でロックされているためにアンマウントできないということがあります。エクスプローラウィンドウが TrueCrypt ボリュームにあるディレクトリを表示しているときも同様です。このオプションがチェックされていると、そのようなウィンドウはアンマウント前にすべて自動的にクローズされ、ユーザーが手動でクローズする必要がありません。

TrueCrypt の常駐 - 常駐する

「TrueCrypt の常駐」を参照してください。

TrueCrypt の常駐 - マウントされたボリュームがなくなれば常駐終了

このオプションがチェックされていると、TrueCrypt はマウントされたボリュームがなくなったら、自動的に何もメッセージは出さずに常駐終了します。詳細は TrueCrypt の常駐を

参照してください。このオプションは TrueCrypt がトラベラーモードで稼働しているときには、不可にはできないことに注意してください。

右に示す時間内に読み書きがなければ自動的にアンマウント

TrueCrypt ボリュームに n 分間書き込みも読み出しもなければ、そのボリュームは自動的にアンマウントされます。

ボリュームに開かれたファイルやフォルダーがあっても強制的にアンマウント

このオプションは、自動アンマウントのみに適用されます。(通常のアンマウントには適用されません) これは、ボリュームのファイルやフォルダー(ディレクトリ)が開いている場合でもメッセージを出さずに強制的に自動アンマウントをします。(システムやアプリケーションで使われているファイルやディレクトリがあった場合です)

TrueCrypt ボリュームのマウント

まだ実行したことがなければ、「メインプログラムウィンドウ」の章のマウントとデバイスの自動マウントを読んでください。

パスワードをドライバのメモリーに記憶する

このオプションは特定のマウント試行にのみ適用されるように、パスワード入力ダイアログで設定することができます。また、「設定」で既定値として設定することもできます。詳細は設定 → 各種設定の節、「パスワードをドライバのメモリーに記憶する」を参照してください。

マウントオプション

マウントオプションはボリュームのマウントのされかたに影響します。マウントオプションダイアログはパスワード入力ダイアログのマウントオプションボタンをクリックすることで開きます。正しいパスワードが記憶されていると、マウントをクリックするだけでボリュームは自動的にマウントされます。記憶されたパスワードを使ってマウントされているボリュームのマウントオプションを変更したい場合には、コントロール(**Ctrl**)を押しながらマウントをクリックするか、ボリュームメニューのオプションを指定してボリュームをマウントを選択してください。

マウントオプションの既定値は、メインプログラム設定(設定 → 各種設定)で設定しなおすことができます。

ボリュームを読み取り専用でマウント

チェックが入っていると、マウントされたボリュームにはいっさい書き込みができません。なお、Windows 2000 では NTFS ボリュームを読み取り専用ではマウントできません。

ボリュームをリムーバブルメディアとしてマウント

Windows が勝手に **Recycler** や **System Volume Information** といったフォルダー(これらはごみ箱やシステム復元機能のために使われます)を作ることを防止したいなら、このオプションにチェックを入れてください。

可能ならボリュームに付加されたバックアップヘッダーを使う

TrueCrypt 6.0 以降で作成されたすべてのボリュームには(ボリュームの最後に置かれる)付加されたバックアップヘッダーがあります。このオプションをチェックすると、TrueCrypt は付加されたバックアップヘッダーを使ってマウントしようとします。ボリュームヘッダーが破損した場合には、このオプションを使う必要はありません。そのかわりに、「ツール → ボリュームヘッダーのリストア」を選択して、ヘッダーを修復することができます。

システムを暗号化したパーティションを起動前認証せずにマウント

システム暗号化のキーの効力の範囲にあるパーティションを起動前認証をせずにマウントする必

要がある場合には、ここをチェックしてください。たとえば、稼働中でないほかの OS の暗号化システムドライブにあるパーティションをマウントする必要があるような場合です。これは TrueCrypt で暗号化された OS を(他の OS 上で)修復したり、バックアップするときに役立ちます。注意: このオプションは「デバイスの自動マウント」や「全てのデバイス型ボリュームをマウント」でも有効化できます。

隠しボリュームの保護

隠しボリュームを破損から守るを参照してください。

ホットキー

システム全般にわたる TrueCrypt ホットキーを設定するには、「設定 -> ホットキー」をクリックしてください。ホットキーは TrueCrypt が起動中か TrueCrypt が常駐している場合にのみ動作することに留意してください。

キーファイル

キーファイルはパスワードと結合される内容を持つファイルです。(どのようにキーファイルとパスワードを結合させるかについての詳細は技術解説の章、キーファイルの項を参照) 正しいキーファイルが与えられるまで、キーファイルを使うボリュームはマウントされません。

かならずしもキーファイルを使う必要はありません。しかし、キーファイルを使うのはいくつかの有利な点があります。:

- キーロガーへの対策になる(敵対者がキーロガーでパスワードをキャプチャしても、キーファイルなしではボリュームをマウントできません)。
- 総当たり攻撃からの保護を強化します。(特にパスワードが脆弱な場合)
- 複数のユーザーでの共有アクセスを可能にします(すべてのキーファイル所有者は、ボリュームがマウントされる前にキーファイルを提示しなければなりません)

どんな種類のファイル(たとえば .txt, .exe, mp3, .avi) でも TrueCrypt キーファイルとして使うことができます。(しかし、.mp3, .jpg, .zip のような圧縮形式のファイルをおすすめします) TrueCrypt はキーファイル自体に改変を加えることはしないことに注意してください。ですから、たとえば巨大な mp3 コレクションの中から 5 個のファイルを TrueCrypt キーファイルとして使うことができるわけです。(そしてファイルを調べても、それらがキーファイルとして使われているということはわかりません)

複数のキーファイルを選択することができます。順番はどうでもかまいません。また、TrueCrypt にランダムな内容のファイルを生成させ、それをキーファイルとして使うこともできます。そうするためには、「キーファイル -> ランダムキーファイルを生成」を選んでください。

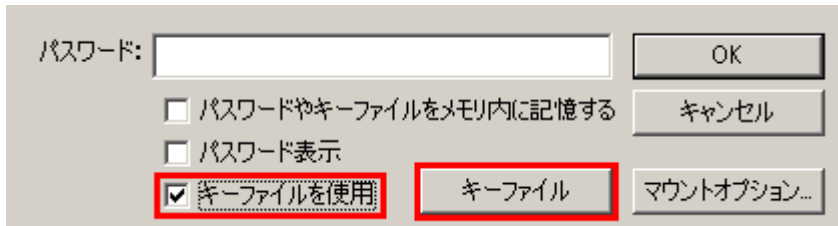
重要: 総当たり攻撃に対抗するため、ひとつのボリュームに対するキーファイルの大きさは少なくとも 30 バイトが必要です。ボリュームが複数のキーファイルを使うなら、そのうちのひとつは 30 バイト以上が必要です。30 バイトという制限は、キーファイルの平均情報量を増大させます。ファイルの先頭 1024 キロバイトの平均情報量が少ないと、(ファイルサイズに関わりなく) キーファイルとしては使われません。平均情報量という意味がよくわからなければ、TrueCrypt にランダムな内容のファイルを生成させ(キーファイル->ランダムキーファイルの生成を選択)、それをキーファイルとして使うことをおすすめします。

警告: キーファイルを紛失したり、キーファイルの先頭 **1024** キロバイトが **1** ビットでも破損したりすると、キーファイルを使ったボリュームをマウンとするのは不可能になります！

警告: パスワードの記憶が有効になっていると、パスワード記憶にはボリュームを正常にマウントしたキーファイルの処理された内容も含まれます。このため、その後にキーファイルがなくなっても再マウントが可能になります。これを防ぐには「記憶したパスワードの消去」をクリックするかパスワードの記憶を無効にしてください。(詳細は「設定 -> 各種設定」の「パスワードをドライバのメモリーに記憶する」を参照してください)

キーファイルダイアログウィンドウ

ボリュームを作成したりマウントしたり、パスワードを変更したりするときに、キーファイルを使いたい(適用したい)ならば、下図のパスワード入力フィールドの「キーファイルを使用」オプションと「キーファイル」ボタンを探してください。



これらの要素はいろいろなダイアログに出現し、常に同じ機能を意味します。「キーファイルを使う」オプションをチェックし、「キーファイル」をクリックしてください。キーファイルダイアログウィンドウが表示され、使うキーファイルを指定(「ファイルの追加」か「トークンファイルの追加」をクリック)するか、キーファイル検索パス(「フォルダの追加」をクリック)を指定できます。

セキュリティトークンとスマートカード

TrueCrypt は PKCS #11 規格に準じるセキュリティトークンあるいはスマートカードに保存されているキーファイルを直接扱うことができ、ユーザーがトークンあるいはカードにファイル(データオブジェクト)を保存することも可能にします。このようなファイルを **TrueCrypt** キーファイルとして使う場合は、キーファイルダイアログの中の「トークンファイルの追加」をクリックしてください。

セキュリティトークンやスマートカードに保存されたキーファイルにアクセスするには通常は PIN コードで保護されており、それはハードウェア PIN パッドか **TrueCrypt GUI**(グラフィック・ユーザー・インターフェース)経由で入力することができます。また、指紋認証のような他の方法で保護されていることもあります。

TrueCrypt がセキュリティトークンやスマートカードにアクセスできるようにするには、最初にトークンやカード用の **PKCS #11** ソフトウェアライブラリをインストールする必要があります。このようなライブラリはデバイスに同梱されているか、製造者またはサードパーティのウェブサイトからダウンロードできるでしょう。

セキュリティトークンやスマートカードが **TrueCrypt** キーファイルとして使えるファイル(データオブジェクト)を持っていないければ、(デバイスがサポートしていれば)**TrueCrypt** でトークンやカードに何らかのファイルを保存することができます。これには次の手順にしたがってください。

1. キーファイルダイアログで「トークンファイルの追加」をクリック。
2. トークンやカードが PIN やパスワードあるいは指紋認証のような他の方法で保護されているならば、自分で認証(たとえば PIN パッドで PIN を入力)してください。

3. 「セキュリティトークンキーファイル」ダイアログが表示されます。「キーファイルをトークンにインポート」をクリックし、トークンやカードに保存したいファイルを選んでください。

TrueCryptで生成されたランダムな内容の512ビットのキーファイルを保存することもできます。
(「キーファイル->ランダムキーファイルの生成」を参照)

キーファイル検索パス

ファイルのかわりにキーファイルダイアログウィンドウで(「フォルダの追加」をクリックして)フォルダーを追加することで、キーファイル検索パスを指定できます。そのフォルダーで見つかるファイルすべてが¹キーファイルとして使われます。

重要: キーファイルフォルダーの中のフォルダー(と、その中のファイル)は無視されます。

キーファイル検索パスは、たとえば、持ち歩くUSBメモリースティックにキーファイルを保存するときなど、特に有用です。USBメモリースティックのドライブレターをキーファイルの既定の設定に追加することもできます。このためには「キーファイル」->「デフォルトキーファイル/フォルダの設定」を選んでください。そして、「フォルダの追加」をクリックしUSBメモリースティックに割りあてるドライブレターを決め、「OK」をクリックしてください。これでボリュームをマウントするたびに(パスワードダイアログの「キーファイルを使う」がチェックされていれば)TrueCryptはフォルダーを調べてそこにあるファイルすべてをキーファイルとして使います。

警告: 既定のキーファイルリストに(ファイルではなく)フォルダーを追加すると、パス(フォルダー)だけが記憶されファイル名は記憶されません！ということは、そのフォルダーに新規にファイルを作成したり追加したりすると、そのフォルダーに依存しているキーファイルを使うボリュームはすべてマウント不可になります。(新しく追加されたファイルをフォルダーから除去すれば復旧します)

¹ボリュームをマウントする、パスワードを変更する、その他ボリュームヘッダーを再暗号化するときに見つかったすべて

空のパスワードとキーファイル

キーファイルを使うときに、パスワードは空かもしれません。そうすると、キーファイルのみがボリュームをマウントする唯一のアイテムになります。(これは推薦されません) 既定のキーファイルが設定されボリュームをマウントするときに使える状態なら、パスワード入力画面の前に TrueCrypt はまず空のパスワードと既定のキーファイルを使ってマウントしようとしています。もしこの方法でマウントするボリュームにマウントオプション(読取専用でマウントとか隠しボリュームを保護するとか)を設定する必要があるなら、コントロール(Ctrl)キーを押しながら「マウント」をクリック(または「ボリューム」メニューの「ボリュームをオプションを指定しながらマウント」を選択)してください。「マウントオプション」ダイアログが開きます。

簡易選択

キーファイルとキーファイル検索パスは下記の方法で簡単に選択できます。

- パスワード入力ダイアログでキーファイルボタンを右クリックし、メニュー項目の一つを選ぶ。
- 該当するファイル/フォルダーをキーファイルダイアログかパスワード入力ダイアログにドラッグする。

キーファイル → ボリュームへのキーファイルの追加/削除

この機能はいくつかのキーファイル(パスワードなし、またはあり)またはキーファイルがなしで生成されたヘッダー暗号化キーでボリュームヘッダーを再暗号化します。パスワードのみでマウント可能なボリュームを、(パスワードに加えて)キーファイルが必要なボリュームに変換します。ボリュームヘッダーはそのボリュームを暗号化しているマスター暗号化キーを含むことに注意してください。そのボリュームに保存されたデータはこの機能を使ってもまったく失われたりはしません。

また、この機能はボリュームのキーファイルを変更/設定することにも使われます。(いくつか、あるいは全部のキーファイルを除外し新しいものを適用する)

補足: この機能は内部的にはパスワード変更機能と同じです。

注意: TrueCrypt がボリュームヘッダーを再暗号化する場合、敵対者が微視的残留磁気[17]から上書きされたヘッダーを復元できないようにするため、最初に元のボリュームヘッダーをランダムデータで 200 回の上書きをします。(「安全のための予防策」も参照)

キーファイル → ボリュームから全てのキーファイルを除去

この機能は、キーファイルではなくパスワードから導出されたヘッダー暗号化キーでボリュームヘッダーを再暗号化します。(キーファイルをまったく使わずに、パスワードのみでマウントされ

るようになります) ボリュームヘッダーはそのボリュームを暗号化しているマスター暗号化キーを含むことに注意してください。そのボリュームに保存されたデータはこの機能を使ってもまったく失われたりはしません。

補足: この機能は内部的にはパスワード変更機能と同じです。

注意: TrueCrypt がボリュームヘッダーを再暗号化する場合、敵対者が微視的残留磁気[17]から上書きされたヘッダーを復元できないようにするため、最初に元のボリュームヘッダーをランダムデータで 200 回の上書きをします。(安全のための予防策も参照)

キーファイル → ランダムキーファイルの生成

この機能を使って、キーファイルとして使えるランダムな内容のファイル(推奨)を生成できます。この機能は TrueCrypt の乱数発生機構を使います。結果として生成されるファイルのサイズは常に 64 バイト(512 ビット)であり、これは TrueCrypt のパスワードの最大長でもあります。

キーファイル → デフォルトキーファイル/フォルダの設定

既定のキーファイルまたはいっしょにキーファイル検索パスを設定するには、この機能を使ってください。これは、たとえば、持ち歩く USB メモリースティックにキーファイルを保存するときなど、特に有用です。ドライブレターをキーファイルの既定の設定に追加することもできます。このためには「キーファイル → 既定キーファイルパス」を選んでください。そして、「パスの追加」をクリックし USB メモリースティックに割りあてるドライブレターを決め、「OK」をクリックしてください。これでボリュームをマウントするたびに(パスワードダイアログの「キーファイルを使う」がチェックされていれば)TrueCrypt はパスを調べてそこにあるファイルすべてをキーファイルとして使います。

警告: 既定のキーファイルリストに(ファイルではなく)フォルダーを追加すると、パスだけが記憶されファイル名は記憶されません！ということは、そのフォルダーに新規にファイルを作成したり追加したりすると、そのフォルダーに依存しているキーファイルを使うボリュームはすべてマウント不可になります。(新しく追加されたファイルをフォルダーから除去すれば復旧します)

重要: デフォルトキーファイルやデフォルトキーファイルフォルダを設定すると、ファイル名やパスは暗号化されずに **Default Keyfiles.xml** に保存されることに注意してください。詳細は TrueCrypt システムファイルとアプリケーションデータを参照してください。

セキュリティトークンとスマートカード

TrueCrypt は PKCS #11 プロトコル[23]でアクセスできるセキュリティ(または暗号機能)トークンとスマートカード(スマートカードリーダー)をサポートします。詳細はキーファイルのセキュリティトークンとスマートカードを参照してください。

トラベラーモード

TrueCrypt はいわゆるトラベラー(旅行者)モードで動作させることができます。これは、TrueCrypt を稼働する OS に対してインストールしなくていいということです。しかし、次の 2 項目は覚えておいてください。

- 1) TrueCrypt をトラベラーモードで動かすには管理者権限が必要
- 2) トラベラーモードで起動したとしても、レジストリファイルを検査すれば、Windows で TrueCrypt を使った(そてけ、TrueCrypt ボリュームをマウントした)ということがわかってしまうかもしれません。

この問題に対処する必要があるなら、BartPE を使うことをおすすめします。またよくある質問(FAQ)と答えの「Windows で痕跡を残さずに TrueCrypt を使うことはできますか?」を参照してください。

TrueCrypt トラベラーモードを使うには、二つの方法があります。

- 1) バイナリ配布パッケージを展開し、(インストールせずに)直接 TrueCrypt.exe を走らせる。
- 2) 「トラベラーディスク作成」を利用して、特別なトラベラーディスクを作りそこから TrueCrypt を起動する。

2 番目のほうがいくつか有利な点があり、この章の以下の節でそれらについて説明します。

注意: トラベラーモードのときには、ドライバは必要がなくなれば(つまり、主アプリケーションとボリューム作成ウィザードが閉じられ、マウントされた TrueCrypt ボリュームがない状態になったとき)、メモリーから除去されます。しかし、TrueCrypt がトラベラーモードで動いているときに、TrueCrypt ボリュームが強制的にアンマウントされると「終了」しても TrueCrypt ドライバーは除去されません。(システムを停止するかリスタートする場合のみ、除去されます) これは Windows のバグによって引き起こされるいろいろな問題(たとえば、アンマウントされたボリュームを使っているアプリケーションがあると TrueCrypt を再起動できない)を防止します。

ツール -> トラベラーディスクのセットアップ

特別なトラベラーディスクを作りそこから TrueCrypt を起動するために、この機能を利用できます。TrueCrypt トラベラーディスクは TrueCrypt ボリュームではなく暗号化されてもいないことに注意してください。トラベラーディスクは TrueCrypt 実行ファイルとオプションとして

‘autorun.inf’を含みます。(「自動実行設定」を参照) 「ツール」->「トラベラーディスクのセットアップ」を選択すると、「トラベラーディスクセットアップ」ダイアログが表示されます。そこで設定できるいくつかの設定項目については、これから説明します。

TrueCrypt ボリューム作成ウィザードを含める

トラベラーディスクから起動した TrueCrypt を使って新しい TrueCrypt ボリュームを作りたいなら、ここにチェックを入れてください。このオプションをチェックしなければ、トラベラーディスク

の容量の節約になります。

自動実行ファイル(**autorun.inf**)の設定

この項目で、トラベラーディスクが挿入されると自動的に **TrueCrypt** を起動したり、自動的に特定の **TrueCrypt** ボリュームをマウントするように設定できます。これは、トラベラーディスクに **autorun.inf** という特別なスクリプトファイルを作ることによって可能になります。このファイルはトラベラーディスクが挿入されるつど **OS** によって自動実行されます。ただし、これは **CD/DVD** のようなリムーバブルメディアのみで、それらが読取可能な場合のみに動作します。(USB メモリステイックでこの機能を使うには、**Windows XP SP2** か **Windows Vista** が必要です)

また、この機能を有効にするためには、**autorun.inf** ファイルは暗号化されていないディスクのルートディレクトリに置かれなくてはならないことに注意してください。(たとえば、G:¥, X:¥, Y:¥ などです)

TrueCrypt を管理者権限なしで使う

Windows では管理者権限がないユーザーでも TrueCrypt を使うことができます。しかし、管理者がシステムに TrueCrypt をインストールしたあとに限ります。その理由は、TrueCrypt 即時自動暗号化/復号のデバイスドライバを必要とし、管理者権限がないと Windows にデバイスドライバをインストールできないからです。

システム管理者が TrueCrypt をインストールしたあとは、管理者権限がないユーザーでも TrueCrypt を起動しどんな種類の TrueCrypt ボリュームでもマウント/アンマウントすることができ、データをそこに保存/読み出しができ、ファイル型 TrueCrypt ボリュームの作成もできます。しかし、管理者権限がないユーザーはパーティションを暗号化/フォーマットしたり NTFS ボリュームをつくることはできませんし、TrueCrypt のインストール/アンインストールもできません。また、デバイス型ボリュームのパスワード/キーファイル変更や TrueCrypt をトラベラーモードで動かすこともできません。

TrueCrypt の常駐

メイン TrueCrypt ウィンドウが閉じていても、TrueCrypt は常駐し以下の機能を実行します。

- 1) ホットキー
- 2) 自動アンマウント(ログオフ時、不用意なデバイスの取り外し時、タイムアウト時など)
- 3) 通知メッセージ (隠しボリュームの破損が防止されたとき)
- 4) タスクトレイアイコン

警告: TrueCrypt が常駐していず TrueCrypt も動いていなければ、上記の機能は無効になります。

TrueCrypt の常駐は実際には TrueCrypt.exe そのものであり、TrueCrypt メインウィンドウを閉じてバックグラウンドで動きつづけているということです。それが起動中であるかどうかは、タスクトレイで判別できます。TrueCrypt アイコンがあれば、TrueCrypt は常駐しているということです。アイコンをクリックして、TrueCrypt メインウィンドウを開くことができます。アイコンを右クリックすれば、いろいろな TrueCrypt 関連機能のポップアップメニューが開きます。

常駐はタスクトレイの TrueCrypt アイコンを右クリックして、「終了」を選択することで停止できます。TrueCrypt の常駐を完全に永続的に止めたいなら、「設定 -> 各種設定」を選び、「各種設定」ダイアログで「TrueCrypt の常駐」の「常駐する」のチェックを外してください。

言語パック

言語パックは TrueCrypt ユーザーインターフェースのテキストの第三者の翻訳を含みます。いくつかの言語パックは TrueCrypt ユーザーズガイドの翻訳も含みます。言語パックは、現在のところ TrueCrypt の Windows 版のみでサポートされていることに留意してください。

インストール

言語パックは以下の手順でインストールしてください。

1. 言語パックをダウンロードする: <http://www.truecrypt.org/localizations.php>
2. TrueCrypt を(稼働中であれば)終了する。
3. 言語パックを TrueCrypt をインストールしたフォルダー(TrueCrypt.exe が存在するフォルダー、たとえば C:\Program Files\TrueCrypt とか C:\Program Files (X86)\TrueCrypt など)に展開する。
4. TrueCrypt を起動する。
5. 言語パックは自動的に検出され、既定の言語パックとして設定されます。(「設定 -> 言語」をクリックしていつでも言語を選択できます)

英語にもどすには、「設定 -> 言語」を選んで、**English**を選び、「OK」をクリックしてください。

暗号化アルゴリズム

TrueCrypt ボリュームは以下のアルゴリズムで暗号化することができます。

アルゴリズム	設計者	キーサイズ (Bits)	ブロックサイズ (Bits)	動作モード
AES	J. Daemen, V. Rijmen	256	128	XTS
Serpent	R. Anderson, E. Biham, L. Knudsen	256	128	XTS
Twofish	B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson	256	128	XTS
AES-Twofish		256; 256	128	XTS
AES-Twofish-Serpent		256; 256; 256	128	XTS
Serpent-AES		256; 256	128	XTS
Serpent-Twofish-AES		256; 256; 256	128	XTS
Twofish-Serpent		256; 256	128	XTS

XTS モードについての詳細は動作モードを参照してください。

AES

Advanced Encryption Standard は FIPS（連邦情報処理規格）で承認された暗号アルゴリズム (Rijndael, designed by Joan Daemen and Vincent Rijmen, published in 1998) であり、アメリカ政府各部署、各機関で重要(機密扱いでない)情報を暗号化して保護するために[3]使われています。TrueCrypt は AES を XTS モード(動作モードを参照)で 14 ラウンド、256-bit キー(AES-256, published in 2001)として使っています。

2003 年 6 月に、NSA (US National Security Agency)が AES を分析、評価し、U.S. CNSS (Committee on National Security Systems)は[2]の中で AES-256(および AES-192)の強度は最高機密にいたるまでの機密扱いの情報を保護するのに充分であると発表しました。これは、Advanced Encryption Standard (AES)を使うか組み込むことで国家安全システムと国家安全情報に関連する Information Assurance の要求を満たすと考えるアメリカ政府各部署、各機関で採用可能ということです。[2]

Serpent

Ross Anderson, Eli Biham, および Lars Knudsen によって設計され、1998 年に発表されました。256-bit キー、128-bit ブロックで XTS モード(動作モードを参照)です。Serpent は AES の最終候補の一つです。これは Rijndael [4] より高度な安全性があるように見えるにもかかわらず、AES の推薦には選ばれませんでした。具体的には、Rijndael でも安全確保に充分であるのに対し、Serpent は高度な安全確保ができるように見えます。また、Rijndael はその数学的構造が将来攻撃対象となるかもしれないという、いくつかの批判を受けています。[4]

[5]において、Twofish チームは各 AES 最終候補の安全係数の表を示しています。安全係数は、完全に暗号化するラウンド数をすでに破られた最大のラウンド数で割ったもので定義されます。だから、破られた暗号は最低の係数 1 ということになります。Serpent は AES 最終候補の中で、(すべてのサポートされたキーサイズで)もっとも高い安全係数 3.56 を持ちます。Rijndael-256 の安全係数は 1.56 であり、Rijndael-256 は安全係数 1.56 です。

これらの事実にもかかわらず、Rijndael は安全性、速度、効率、実装のしやすさ[4]、柔軟性などのバランスのよさで、AES の中で適切な選択であると考えられています。最後の AES 会議で、Rijndael は 86 票、Serpent は 59 票、Twofish は 31 票、RC6 は 23 票、MARS は 13 票でした。[18, 19]¹

Twofish

Bruce Schneier, David Wagner, John Kelsey, Niels Ferguson, Doug Whiting, Chris Hall によって設計され、1998 年に発表されました。256-bit キー、128-bit ブロックで XTS モード(動作モードを参照)で動きます。Twofish は AES の最終候補の一つです。この暗号は、キーから独立した S-ボックスを使います。Twofish は、 2^{128} (2 の 128 乗)の異なった暗号システムの集まりに見え、256-bit キーから導出される 128bits がその集まりの中からの暗号システムの選択をコントロールします。[4] [13]の中で、Twofish チームは、キーから独立した S ボックスが未知の攻撃に対する安全性を高めると主張しています。[4]

AES-Twofish

2 つの暗号方式が XTS モード(動作モードを参照)でカスケード(多段処理)[15, 16] されます。それぞれの 128-bit ブロックは、まず XTS モードの Twofish (256-bit キー)で暗号化され、つぎに XTS モードの AES (256-bit キー)で暗号化されます。カスケードの暗号のそれぞれは、それ自身のキーを使います。それぞれのキーは相互に独立しています。(補足: ヘッダーキーは一つのパスワードから導出されるものの、きちんと独立しています。「ヘッダーキーの導出、ソルト、および反復回数」を参照) カスケードのそれぞれの暗号方式については、上記の個別解説を参照してください。

AES-Twofish-Serpent

3 つの暗号方式[15,16]が XTS モード(動作モードを参照)でカスケード(多段処理)されます。128-bit ブロックは、まず XTS モードの Serpent (256-bit キー、128-bit ブロック)で暗号化され、次に XTS

¹ これは肯定的な票です。肯定的な票から否定的な票を引くと、次の結果となります。Rijndael: 76 票, Serpent: 52 票, Twofish: 10 票, RC6: -14 票, MARS: -70 票 [19]

モードの Twofish (256-bit キー)、最後に XTS モードの AES (256-bit キー, 128-bit ブロック)で暗号化されます。カスケードの暗号のそれぞれは、それ自身のキーを使います。それぞれのキーは相互に独立しています。(補足: ヘッダーキーは一つのパスワードから導出されるものの、きちんと独立しています。ヘッダーキーの導出、ソルト、および反復回数を参照) カスケードのそれぞれの暗号方式については、上記の個別解説を参照してください。

Serpent-AES

2つの暗号方式[15,16]が XTS モード(動作モードを参照)でカスケード(多段処理)されます。それぞれの 128-bit ブロックは、まず XTS モードの AES (256-bit key)で暗号化され、つぎに XTS モードの Serpent (256-bit key)で暗号化されます。カスケードの暗号のそれぞれは、それ自身のキーを使います。それぞれのキーは相互に独立しています。(補足: ヘッダーキーは一つのパスワードから導出されるものの、きちんと独立しています。ヘッダーキーの導出、ソルト、および反復回数を参照) カスケードのそれぞれの暗号方式については、上記の個別解説を参照してください。

Serpent-Twofish-AES

3つの暗号[15,16]が XTS モード(動作モードを参照)でカスケード(多段処理)されます。128-bit ブロックは、まず XTS モードの AES (256-bit key)で暗号化され、次に XTS モードの Twofish (256-bit キー)、最後に XTS モードの Serpent (256-bit key)で暗号化されます。カスケードの暗号のそれぞれは、それ自身のキーを使います。それぞれのキーは相互に独立しています。(補足: ヘッダーキーは一つのパスワードから導出されるものの、きちんと独立しています。ヘッダーキーの導出、ソルト、および反復回数を参照) カスケードのそれぞれの暗号については、上記の個別解説を参照してください。

Twofish-Serpent

2つの暗号方式[15,16]が XTS モード(動作モードを参照)でカスケード(多段処理)されます。それぞれの 128-bit ブロックは、まず XTS モードの Serpent (256-bit key)で暗号化され、つぎに XTS モードの Twofish (256-bit key)で暗号化されます。カスケードの暗号のそれぞれは、それ自身のキーを使います。それぞれのキーは相互に独立しています。(補足: ヘッダーキーは一つのパスワードから導出されるものの、きちんと独立しています。ヘッダーキーの導出、ソルト、および反復回数を参照) カスケードのそれぞれの暗号方式については、上記の個別解説を参照してください。

ハッシュアルゴリズム

ボリューム作成ウィザードやパスワード変更ダイアログウィンドウ、キーファイル生成ダイアログウィンドウなどで、ハッシュアルゴリズムを選択できます。ユーザーが選択したハッシュアルゴリズムは TrueCrypt 乱数発生機構で疑似乱数混合関数で使われ、ヘッダーキー導出関数(PKCS #5 v2.0 で規定されているとおり HMAC ハッシュアルゴリズムに依存します) で疑似乱数関数として使われます。新しいボリュームを作成するとき、乱数発生機構はマスター暗号化キー、第二キー(XTS モード)、ソルトを生成します。詳細は乱数発生機構とヘッダーキーの導出、ソルト、および反復回数の項を参照)

RIPEMD-160

RIPEMD-160 は 1996 年に発表され、Hans Dobbertin, Antoon Bosselaers, と Bart Preneel によってオープンな学術的コミュニティで設計されました。RIPEMD-160 の出力サイズは 160bits です。RIPEMD-160 は、EU の RIPE(*RACE Integrity Primitives Evaluation*)プロジェクト(1988-1992)で開発された RIPEMD ハッシュアルゴリズムの強化版です。RIPEMD-160 は国際標準化機構(ISO)と IEC in the ISO/IEC 10118-3:2004 の国際規格[21]に適合しています。

SHA-512

SHA-512はNSAが設計し2002年に(最初の概要は2001年に)FIPS PUB 180-2[14]でNISTによって発表されました。このアルゴリズムの出力サイズは512bitsです。

Whirlpool

Whirlpool ハッシュアルゴリズムは Vincent Rijmen (AES 暗号化アルゴリズムの共作者)と Paulo S. L. M. Barreto による設計です。このアルゴリズムの出力サイズは 512bits です。 Whirlpool-0 と呼ばれるようになった Whirlpool の最初のバージョンは 2000 年 11 月に発表されました。Whirlpool-T と呼ばれるようになった第二版は NESSIE (*New European Schemes for Signatures, Integrity and Encryption*)の暗号資産(AES 競技に似た、ヨーロッパ連合によって組織されたプロジェクト)に選択されました。TrueCrypt は、International Organization for Standardization (ISO) や ISO/IEC 10118-3:2004 international standard [21] の IEC に採択された Whirlpool の第三版(最終版)を採用しています。これは国際標準化機構(ISO)と IEC in the ISO/IEC 10118-3:2004 の国際規格 [21]に適合しています。

動作対象 OS

TrueCrypt は次の OS で稼働します。

- Windows Vista
- Windows Vista x64 (64-bit) Edition
- Windows XP
- Windows XP x64 (64-bit) Edition
- Windows Server 2008
- Windows Server 2008 x64 (64-bit)
- Windows Server 2003
- Windows Server 2003 x64 (64-bit)
- Windows 2000 SP4

- Mac OS X 10.5 Leopard
- Mac OS X 10.4 Tiger

- Linux (kernel 2.4, 2.6 or compatible)

注意: 次の OS はサポートされていません: Windows 2003 IA-64, Windows 2008 IA-64, Windows XP IA-64, Windows 95/98/ME/NT.

システム暗号化ができる OS も参照してください。

コマンドラインの使い方

この節は Windows 版 TrueCrypt を対象とします。Linux と Mac OS X でのコマンドラインの使い方については `truecrypt -h` としてください。

<code>/help or /?</code>	コマンドラインヘルプを表示します。
<code>/volume or /v</code>	マウントする TrueCrypt ボリュームのファイルとパスの名前(アンマウント時には使わないこと)。ハードディスクのパーティションをマウントする場合の例は <code>/v ¥Device¥Harddisk1¥Partition3</code> (パーティションのパスを決めるには、TrueCrypt を起動して「デバイスの選択」をクリックしてください)。デバイスのパスは大文字小文字を区別します。
<code>/letter or /l</code>	ボリュームをマウントするドライブレター。/1 が省略され /a が指定されている場合には最初の空きドライブレターを使います。
<code>/explore or /e</code>	ボリュームがマウントされると、そのボリュームのウィンドウを開きます。
<code>/beep or /b</code>	ボリュームが正常にマウントまたはアンマウントされるとビーブを鳴らします。
<code>/auto or /a</code>	パラメータが指定されていなければ、ボリュームを自動マウントします。 <code>devices</code> がパラメータとして指定(<code>/a devices</code>)されていれば、すべての使用可能なデバイス/パーティション型 TrueCrypt ボリュームを自動マウントします。パラメータとして <code>favorites</code> が指定されていれば、お気に入りボリュームを自動マウントします。 <code>/quit</code> と <code>/volume</code> が指定されると <code>/auto</code> も暗黙のうちに指定されたことになることに注意してください。
<code>/dismount or /d</code>	ドライブレターで指定されたボリュームをアンマウントします。(例: <code>/d x</code>) ボリュームが指定されていないと、現在マウントされているすべての TrueCrypt ボリュームをアンマウントします。
<code>/force or /f</code>	強制的に(そのボリュームのファイルがシステムかアプリケーションに使われていても)アンマウントを実行し、マウントを共有モード(排他制御なし)にします。

<code>/keyfile</code> or <code>/k</code>	<p>キーファイルかキーファイル検索パスを指定します。複数のキーファイルの指定は <code>/k c:¥keyfile1.dat /k d:¥KeyfileFolder /k c:¥keyfile2</code> のようにします。</p> <p>セキュリティトークンやスマートカードに保存されたキーファイルを指定するには、次の文を使ってください。</p> <p><code>token://slot/SLOT_NUMBER/file/FILE_NAME</code></p>
<code>/tokenlib</code>	<p>セキュリティトークンやスマートカード用に特定の PKCS#11 ライブラリを指定します。</p>
<code>/cache</code> or <code>/c</code>	<p><code>y</code> またはパラメータなしの場合は、パスワード記憶を有効にします。<code>n</code> の場合 (<code>/c n</code>) はパスワード記憶を無効にします。パスワード記憶を無効にしても記憶したものを消去するわけではありません。(消去するには <code>/w</code> をお使いください)</p>
<code>/history</code> or <code>/h</code>	<p><code>y</code> またはパラメータなし : マウントしたボリュームの履歴を保存; <code>n</code>: マウントしたボリュームの履歴を保存しない。(例 <code>/h n</code>)</p>
<code>/wipecache</code> or <code>/w</code>	<p>ドライバに記憶したパスワードをすべて消去</p>
<code>/password</code> or <code>/p</code>	<p>ボリュームのパスワード。パスワードに空白を含む場合には引用符で囲むこと (例 <code>/p "My Password"</code>). 空パスワードを表すには <code>/p ""</code> としてください。</p> <p>警告: この方法でボリュームパスワードを入力することは、暗号化されていないコマンドプロンプトの履歴が暗号化されていないディスクに保存される場合に、安全に問題があるかもしれません。代わりに <code>/q</code> を使うことを検討してください。</p>
<code>/quit</code> or <code>/q</code>	<p>要求された動作を実行し、終了します。(TrueCrypt メインウィンドウは表示されません) <code>preferences</code> が指示されていれば (<code>/q preferences</code>) プログラム設定が読込/保存されます。</p> <p><code>/q background</code> は TrueCrypt 常駐 (トレイアイコン) を開始します。</p> <p><code>/q</code> はコンテナがローカルユーザー名前空間でしかアクセスできない場合 (ネットワークボリューム) には効果がなく、TrueCrypt はボリュームがアンマウントされた後のみ終了します。</p>
<code>/silent</code> or <code>/s</code>	<p><code>/q</code> が指定されていれば、ユーザーへのメッセージ (プロンプト、エラーメッセージ、警告 など) を表示しません。</p>

/mountoption or /m

ro または **readonly**: 読取専用でマウント

rm または **removable**: リムーバブルメディアとしてマウント

ts または **timestamp**: ボリューム/キーファイルのタイムスタンプを変更

sm または **system**: 起動前認証をせずにシステム暗号化のキーが有効なパーティションをマウントします。(たとえば、起動中ではないほうの OS の暗号化システムドライブにあるパーティション)

注意: /p の引数としてパスワードを記述する場合には、かならず標準 US キーボードレイアウトで入力してください。(対照的に、GUI では自動的にこれを確実にします)

bk または **headerbak**: 付加されたバックアップヘッダーを使ってボリュームをマウントします。**TrueCrypt 6.0** 以降で作成されたすべてのボリュームはバックアップヘッダーが付加されています。(ボリュームの最後に位置します)

recover: ボリュームヘッダーに保存されているチェックサムを確認しないでください。このオプションはボリュームヘッダーが破損し **headerbak** オプションでもボリュームをマウントできない場合のみに使うべきです。

例: /m ro 複数のマウントオプションを指定する場合は、/m rm /m ts を使う

TrueCrypt Format.exe (TrueCrypt ボリューム作成ウィザード):

/noisocheck or /n

TrueCrypt レスキューディスクが正しく作成されたことを確認しない。これは企業の管理部門などで、CD や DVD で保管したものをメンテナンスするよりも ISO イメージで保管するほうが簡単な場合などに有用です。警告：以前に作った TrueCrypt レスキューディスクを再利用するために、このオプションを使うのは厳禁です。システムパーティション/ドライブを暗号化するつど、同じパスワードを使ったとしても TrueCrypt レスキューディスクを新しくつくらなくてはならないことに注意してください。古い TrueCrypt レスキューディスクを使うと異なるマスターキーを生成してしまうので、再利用してはいけません。

文法

```
TrueCrypt.exe [/a [devices|favorites]] [/b] [/c [y|n]] [/d [drive letter]] [/e] [/f]
[/h [y|n]] [/k keyfile or search path] [/l drive letter] [/m {bk|rm|recovery|ro|sm|ts}] [/p
password] [/q [background|preferences]] [/s] [/tokenlib path] [/v volume] [/w]
```

```
"TrueCrypt Format.exe" [/n]
```

オプションを記述する順番は重要ではありません。

使用例

d:¥myvolume という名前のボリュームを最初の空きドライブレターに割り当ててマウント、パスワードプロンプトを表示(メインプログラムウィンドウは表示しない)

```
truecrypt /q /v d:¥myvolume
```

ドライブ **X** としてマウントされているボリュームをアンマウントする。

```
truecrypt /q /dx
```

myvolume.tc という名前のボリュームを **MyPassword** というパスワードで、ドライブ **X** にマウント

TrueCrypt はウィンドウを開き、ビープを鳴らし、自動でマウントします。

```
truecrypt /v myvolume.tc /lx /a /p MyPassword /e /b
```

ネットワーク間の共有

ある特定の TrueCrypt ボリュームを複数の OS から同時にアクセスする必要があるなら、二つの方法があります。

- TrueCrypt ボリュームを特定のコンピューター(たとえば、サーバー)にのみマウントし、マウントされた TrueCrypt ボリュームの内容(TrueCrypt ボリュームのファイルシステム)をネットワーク間で共有します。個々のコンピューターやシステムのユーザーは個別にはボリュームをマウントしません。(すでにサーバーでマウントされています)

長所: すべてのユーザーが TrueCrypt ボリュームの読み書きができます。共有されるボリュームはファイル型でもパーティション/デバイス型でもかまいません。

短所: ネットワークを通じて送られるデータは暗号化されません。ただし、SSL, TLS, VPN , およびその他の技術で経路を暗号化することはできます。

- 特定のコンピューター(たとえば、サーバー)にマウントされていないファイルコンテナを置きます。この暗号化されたファイルをネットワーク間で共有します。個々のコンピューターやシステムのユーザーは各自で共有されたファイルをマウントします。これで、ボリュームは複数の OS で同時にマウントされたことになります。

長所: ネットワークを通じて送られるデータは暗号化されます。(しかし、通信経路での解析を困難にし、データの正確さを保つために、SSL, TLS, VPN , およびその他の技術で経路を暗号化することをすすめます)

短所: 共有できるボリュームはファイル型だけ(パーティション/デバイス型は不可)です。ボリュームは個々のシステムでは読み取り専用でマウントしなければなりません。(読み取り専用でのマウント方法についてはマウントオプションの節を参照) この条件は暗号化されていないボリュームでも同様であることに注意してください。その理由の一つは、たとえば、ある OS のファイルシステムから読み出されたデータが一方では他の OS でファイルシステムの変更があったとすると、データの一貫性がなくなる(これはデータ破損につながる)ということです。

安全のための予防策

この章では TrueCrypt ボリュームに保存された機密データの安全性に影響するいくつかの項目について述べます。すべての危険性について網羅することはできないことを、ご了承ください。残念ながら非常に多くの種類の危険があり、すべてを解説しようとするあまりに膨大になってしまうためです。

ページングファイル

注意: ここで述べることは、システムパーティションあるいはシステムドライブが暗号化(詳細は「システム暗号化」参照)され、ページングファイルがシステム暗号化のキーが有効な範囲のパーティション(通常はそうになっています)、たとえば **Windows** がインストールされているパーティション、にあるならば、関係はありません。

スワップファイルとも呼ばれます。Windows はこの(通常ハードドライブに置かれる)ファイルを、メモリに入りきらないプログラムやデータファイルを保持するために使います。ということは、メモリ上だけにあると信じている機密データが実際には知らないうちに Windows によって暗号化もされずにディスクに書かれているということです。

TrueCrypt はパスワード、暗号化キー、および他の機密データがあるメモリー領域を、それらのデータがページングファイルへもれないように、つねにロックしようとします。しかし、Windows ではいろいろな(文書化したものも、されていないものもある)理由で、ロックが拒否されることがあります。さらに、TrueCrypt は、RAM 上に開かれた機密ファイルが暗号化されない状態でスワップに保存されることを防ぐことはできません。(TrueCrypt ボリュームのファイルをテキストエディターとかなにかで開くと、そのファイルの内容は暗号化されていない状態で RAM に置かれます)

解決策 1: システムパーティション/ドライブを暗号化し(詳細はシステム暗号化を参照)、そして確実にページングファイルがシステム暗号化のキーが有効な範囲のパーティション(通常はそうになっています)、たとえば Windows がインストールされているパーティション、にあるようにしてください。

注意 : 隠し OS を作ることも考慮してください。(詳細は隠し OS を参照)

解決策 2: 少なくとも TrueCrypt ボリュームをマウントして機密データを扱っている間は毎回、ページングファイル機能を無効にする。スタートメニューの中かデスクトップにある「コンピュータ」または「マイコンピュータ」アイコンを右クリックし、プロパティ->(Windows Vista では: ->高度なシステム設定->)詳細設定->パフォーマンス->設定->詳細設定->仮想メモリ->変更->ページングファイルなし->設定->OK の順にクリックし、最後にコンピュータを再起動してください。知る限りでは、Windows 2000 ではページングファイル機能を完全には停止できないことに注意してください。したがって、TrueCrypt ユーザーは Windows 2000 から新しい Windows にアップグレードすることを推奨します。

ハイバネーションファイル

注意: ここで述べることは、システムパーティションあるいはシステムドライブが暗号化され¹(詳細は「システム暗号化」参照)、ハイバネーションファイルがシステム暗号化のキーが有効な範囲のパーティション(通常はそうになっています)、たとえば **Windows** がインストールされているパーティション、にあるならば、関係はありません。コンピューターが休止状態になるときは、データはハイバネーションファイルに書き込まれる前に即時に暗号化されます。

コンピューターがハイバネーションモード(省電力モード)に入るとき、システムメモリの内容はハードディスクのハイバネーションファイルに書き出されます。**TrueCrypt** は自動的にすべてのボリュームをアンマウントし、**RAM** にあるそれらのマスターキーやパスワードがあればそれらを消去します。しかし、システム暗号化(システム暗号化参照)をしていなければ、**TrueCrypt** は記憶したパスワード、**RAM** 上に開かれた **TrueCrypt** ボリューム上の機密ファイルが暗号化されない状態でハイバネーション・ファイルに保存されることを防ぐことはできません。たとえば、テキストエディターではファイルの内容は暗号化されない状態で **RAM** に(おそらくは電源を切るまで)保持されます。

解決策 1: システムパーティション/ドライブを暗号化し(詳細はシステム暗号化を参照)、そして確実にハイバネーションファイルがシステム暗号化のキーが有効な範囲のパーティション(通常はそうになっています)、たとえば **Windows** がインストールされているパーティション、にあるようにしてください。コンピューターが休止状態になるときは、データはハイバネーションファイルに書き込まれる前に即時に暗号化されます。

注意: 隠し **OS** を作ることも考慮してください。(詳細は隠し **OS** を参照)

解決策 2: システム暗号化を使わないなら、少なくとも **TrueCrypt** ボリュームをマウントして機密データを扱っている間は毎回、ハイバネーション機能を無効にするか抑止する。

メモリダンプファイル

注意: ここで述べることは、システムパーティションあるいはシステムドライブが暗号化(詳細は「システム暗号化」参照)され、メモリダンプファイルがシステムドライブ(通常はそうになっています)、に置かれるようにシステムが設定されているならば、関係はありません。

Windows を含むほとんどの **OS** でデバッグ情報の取得やエラー発生時(システムクラッシュ、ブルースクリーン、バグチェック)のシステムメモリの内容の取得(メモリーダンプ)が可能です。このメモリーダンプファイルには機密データを含んでいるかもしれません。**TrueCrypt** は記憶したパスワード、暗号化キーや **RAM** に展開された機密ファイルの内容が暗号化されていない状態でメモリ

¹お断り: マイクロソフトがハイバネーションを扱う **API** を公開していないため、マイクロソフト以外のディスク暗号化開発者はハイバネーションファイルの暗号化ができるように、**Windows** の非公開コンポーネントに手を加えることを余儀なくされています。このため、現在のところ(マイクロソフトの **BitLocker** 以外の)どのディスク暗号化ソフトウェアでも、確実にハイバネーションファイルを暗号化できるという保証はありません。マイクロソフトは(**Windows** 自動更新によって)いつでも任意に非公開で **API** 経由では使えない **Windows** のコンポーネントを修正することができます。そのような変更や、非正規または特製の記憶装置デバイスドライバの使用は、マイクロソフト以外のディスク暗号化ソフトウェアがハイバネーションファイルの暗号化をうまくできないようにしてしまうかもしれません。注意: われわれは、この問題とこのことでマイクロソフトのディスク暗号化ソフトウェア(**BitLocker**)が不利になるわけではないということについてマイクロソフトへ(却下されたら、ヨーロッパ委員会へ)苦情を申し立てるつもりです。

ードンプファイルに書き出されることを防ぐことはできません。TrueCrypt ボリュームのファイルをテキストエディターとかなにかで開くと、そのファイルの内容は暗号化されていない状態で RAM に置かれます。(そして、電源を切るまでそのまま暗号化されない状態で RAM に残るかもしれません) また、TrueCrypt ボリュームがマウントされていると、そのマスターキーは暗号化されていない状態で RAM に保持されます。ですから、少なくとも機密データを扱ったり TrueCrypt をマウントするセッションの間だけでもコンピュータのメモリーダンプファイル生成機能が無効にすることを強くおすすめします。WindowsXP/Vista の場合には、デスクトップかスタートメニューのマイコンピュータ・アイコンの上で右クリックし、プロパティ->Windows Vista では->高度なシステム設定->)詳細設定->起動と回復->設定->デバッグ情報の書き込みの項目->(なし)を選択>OK としてください。

注意: システムパーティション/ドライブが暗号化され、メモリーダンプファイルがシステムドライブ(通常はそうになっています)に置かれるようにシステムが設定されているならば、TrueCrypt ドライバーは自動的に Windows がどんなデータもメモリーダンプファイルに書かないようにします。(どのようにシステムパーティション/ドライブを暗号化するかはシステム暗号化の章を参照)

マルチユーザー環境

マウントされた TrueCrypt ボリュームの内容はすべてのログオンしたユーザーには見え、アクセス可能になるということを忘れないでください。(NTFS ではファイルの許可情報の設定で、このようなことを防ぐことは可能です) また、Windows XP/Vista(簡易ユーザー切替)のユーザー切替やログオフは正常にマウントされた TrueCrypt ボリュームをアンマウントしないことに注意してください。(システムを再起動する場合には、すべてのマウントされた TrueCrypt ボリュームはアンマウントされます)

Windows 2000 ではファイル型 TrueCrypt ボリュームがマウントされる時には、コンテナファイルのパーミッション(許可情報)は無視されます。Windows のすべてのバージョンで、管理者権限を持たないユーザーでも正しいパスワードまたはキーファイルがあれば、パーティション/デバイス型の TrueCrypt ボリュームをマウントできます。しかし、管理者権限がないユーザーは自分がマウントしたボリュームしかアンマウントできません。

RAM にある暗号化されていないデータ

TrueCrypt はディスクを暗号化するソフトウェアであることに留意してください。つまり、ディスクを暗号化するのであって、RAM(メモリ)を暗号化するのではないということです。

ほとんどのプログラムは TrueCrypt ボリュームから読み込んだファイルの暗号化されていないデータのあるメモリー領域(バッファ)に置き、クリアしないことに気をつけてください。これは、そのようなプログラムを終了しても、そのプログラムが使った暗号化されていないデータは電源を切るまで(ある研究者によれば、電源を切ったあとのしばらくの間までも¹⁾)メモリーに残っているかもしれないということを意味します。また、テキストエディターなどで TrueCrypt ボリュームのファイルを開いて、そのボリュームを強制アンマウントしたとしても、ファイルはテキストエ

¹開くところでは、通常の動作温度(26-44 °C) では 1.5~3.5 秒、メモリーモジュールが(コンピューター稼動中に)非常に低温(たとえば -50 °C)で冷却された場合には数時間だということです。新しいタイプのメモリーモジュールでは減衰時間が旧タイプよりずっと短い(1.5~2.5 秒)ということです。

ディーターが確保した暗号化されないメモリー(RAM)領域に残ります。このことは自動アンマウントについても同じです。

本来、暗号化されていないマスターキーも RAM 中に保持されることになっています。非システム TrueCrypt ボリュームがアンマウントされるときに、TrueCrypt は(RAM に保持された)マスターキーを消去します。コンピューターが正常に再起動または終了、休止(ハイバネート)すれば、すべての非システム TrueCrypt ボリュームは自動的にアンマウントされ、RAM 中に保持されたすべてのマスターキー(システムパーティション/ドライブのためのマスターキーを除く-詳細は下記)は TrueCrypt ドライバーによって消去されます。しかし、コンピューターが電源の瞬断、リセット(正常な手順での再起動ではなく)、あるいはシステムクラッシュなどの場合には、**TrueCrypt も当然にプロセスを停止し、キーや機密データを消去することもできません**。さらに、マイクロソフトはハイバネーションに関する API を公開していないので、コンピューターが休止(ハイバネート)するときに、システム暗号化用のマスターキーを確実に消去することもできません。

要約すると、TrueCrypt は RAM に機密データ(パスワード、マスターキー、復号されたデータ)が含まれないということを確約できないということです。したがって、TrueCrypt ボリュームをマウントしたり暗号化 OS を使ったりした後はシステムをシャットダウンするか休止するかして、再度電源を入れる前に数分間電源オフの状態にしておくべきです。これは RAM をクリアするのに必要なことです。(ハイバネーションファイルも参照してください)

パスワードとキーファイルの変更

ボリュームヘッダー(パスワードやキーファイルから導出されるヘッダーキーで暗号化されている)はボリュームを暗号化しているマスターキーを含んでいることに留意してください。もし、敵対者がパスワードやキーファイルを変更する前のボリュームのコピーを取得可能なら、そのコピーあるいは断片(旧ヘッダー)とともにパスワードやキーファイルの変更前にボリュームをマウントするのに必要だったパスワードを推測(たとえばキーロガーで取得するなど)したりキーファイルを推測したりして、TrueCrypt ボリュームをマウントすることができるようかもしれません。

パスワードやキーファイルを変更するときに敵対者がパスワードやキーファイルを知っているかどうか、ボリュームのコピーを持っているかどうかに不安があるなら、新しい(異なるマスターキーを持つ)TrueCrypt ボリュームを作成し旧ボリュームから新ボリュームヘッダーファイルを移動させることをおすすめします。

また、注意すべきは敵対者がパスワードを知っていたりキーファイルを持っていてボリュームへアクセスできるとすると、敵対者はマスターキーを再取得して保管しておくことができるかもしれないということです。そうだとすると、敵対者はパスワードやキーファイルを変更してもボリュームを復号できることになります。(パスワードやキーファイルを変更しても、マスターキーは変更されないからです)このような場合には、新しい TrueCrypt ボリュームを作成し旧ボリュームから新ボリュームヘッダーファイルを移動させてください。

データの漏洩

注意：下記の問題はシステムパーティションあるいはシステムドライブが暗号化されている場合(詳細は「システム暗号化」の症を参照)や、TrueCrypt ボリュームがマウントされている間あるいは

は暗号化 OS が稼動中に書き込み可能な非暗号化ファイルシステム(あるいはボリューム)がないなら、影響はありません。

TrueCrypt ボリュームがマウントされている場合に、OS や他社アプリケーションは TrueCrypt ボリュームにあるデータ(たとえば、最近使ったファイルのファイル名や場所、ファイルインデックスツールが作成したデータベース)についての非暗号化情報や、非暗号化形式でのデータそれ自身(臨時中間ファイル他)や、TrueCrypt ボリュームのファイルシステムについての非暗号化情報などを、非暗号化ボリューム(通常は非暗号化システムボリューム)へ書込みます。Windows は自動的に大量の機密であるかもしれないデータ(開いたファイル、使ったアプリケーションなどの名前や場所他)を記録することに注意してください。

解決策 : システムパーティション/ドライブを暗号化し(詳細はシステム暗号化を参照)、そして機密データを扱う場合には、かならず暗号化ファイルシステムだけをマウントするようにしてください。(TrueCrypt ボリュームがマウントされているとか暗号化 OS が稼動中の場合には、非暗号化ファイルシステム/ボリュームをマウントするべきではありません)

注意 : 隠し OS を作ることも考慮してください。(詳細は隠し OS を参照)

Windows レジストリ

TrueCrypt の「みせかけの拒否」は、あるファイルかパーティションが TrueCrypt ボリュームであるとか、隠しボリュームがあるとかを証明できないということにかかっている(みせかけの拒否を参照)ということを重視してください。Windows は TrueCrypt が安全確実に消すことができないさまざまなデータをレジストリに保持しています。レジストリファイルを調べれば、攻撃者は TrueCrypt がそのシステムで稼働したこと、TrueCrypt ボリュームがマウントされた(ボリュームの型¹やファイル名、大きさ、保存場所はわからない)こと、そして TrueCrypt ボリュームがどのドライブ文字を使ったか(ボリュームの型やファイル名、大きさ、保存場所はわからない)がわかってしまうかもしれません。

注意: システムパーティション/ドライブを暗号化することで、レジストリファイルも暗号化することができます。(その方法についてはシステム暗号化を参照)隠し OS を作ることも考慮してください。(詳細は隠し OS を参照)

ウェアレベリング

いくつかの記憶装置(たとえば、いくつかの USB フラッシュドライブ)やいくつかのファイルシステムでは装置や媒体の寿命を延ばすため、ウェアレベリングという機能を持ちます。この機能は、アプリケーションが同じ論理セクターに繰り返しデータを書き込む場合に、メディア全体に分散して書き込む(論理セクターが違う物理セクターに再配置される)というものです。ですから、あるセクターの複数の版が攻撃者に入手可能になるかもしれません。これはセキュリティに問題を生じます。たとえば、ボリュームパスワードやキーファイルを変更した場合に通常ではヘッダーを再暗号化したもので上書きします。しかし、ボリュームがウェアレベリング機能を持つデバイスにあると、TrueCrypt は古いヘッダーがほんとうに上書きされるとは保証できなくなります。もし敵対者が本来なら上書きされてしまうはずの古いヘッダーをそのデバイス上で見つけたとすると、古い(ヘッダーが再暗号化される前にマウントするのに必要だった)パスワードやキーファイルを使

¹ボリュームの型というのは、隠しボリュームか通常ボリュームかということです。

ってボリュームをマウントすることができてしまいます。安全上の理由から、TrueCrypt ボリュームをウェアレベリング機能を持つデバイス(またはファイルシステム)に置かないことをおすすめします。この助言にしたがわず、ウェアレベリング機能を使ったシステムドライブでシステム暗号化(システム暗号化を参照)するならば、機密データを完全に暗号化される前のシステムパーティション/ドライブに置かないでください。(TrueCrypt はそのようなドライブにすでに存在するデータをそのまま暗号化できないかもしれないからです。ただし、システムパーティション/ドライブが完全に暗号化された後で追加されるデータは確実にその場で暗号化されます)デバイスにウェアレベリング機能があるかどうかは、そのデバイスの説明書を参照するかメーカーに問い合わせてください。

セクターの再配置

いくつかの記憶装置では不良セクターを内部で再配置します。デバイスが書込みできないセクターを検出すると、そのセクターに不良マークをつけ、ドライブの予約領域にそのセクターを割り当てます。不良セクターに対するすべての読み書きは、予約領域のセクターに対するものに振り返られます。これは、不良セクターにあるデータはそのまま残り、他のデータで上書きされることがないので、消去されることもないということを意味します。このことは安全性についてのいろいろな不安要素となります。たとえば、その場所にあるデータが暗号化されるべきだったとしても、不良セクターに非暗号化状態で残ってしまうかもしれません。同様に、(隠し OS 作成過程などで)消去されるべきデータが不良セクターに残ってしまうかもしれません。可能性がある安全性の不安要素はウェアレベリングにリストがあります。しかし、このリストは単なる例として記載しているだけで、完全なものではないことに注意してください。また、TrueCrypt はセクターの再配置に起因するいかなる問題点も防ぐことができないことにも注意してください。ハードディスクの再配置されたセクター数を知るには、いわゆる **S.M.A.R.T.**を読み出すサードパーティのツールを使うことができます。

デフラグ

ファイル型 TrueCrypt コンテナを格納したファイルシステムをデフラグする場合、TrueCrypt コンテナ(あるいは、その断片)のコピーがホストボリューム(断片化していたファイルシステム)の空き領域に残る可能性があります。このことはいろいろなセキュリティの問題を生じます。たとえば、ボリュームのパスワードやキーファイルをあとから変更しても、敵対者が TrueCrypt ボリュームの古い(ヘッダーが再暗号化される前にマウントするのに必要だった)ヘッダーやその断片を見つけたら、古いパスワードでボリュームをマウントできるかもしれません。これを防ぐには、以下のどれかを実行してください。

- ファイル型のかわりに、パーティション/デバイス型 TrueCrypt ボリュームを使う。
- デフラグのあとで、ホストボリューム(断片化していたファイルシステム)の空き領域に完全消去をかける。
- TrueCrypt ボリュームを格納しているホストファイルシステムではデフラグをしない

ジャーナリングファイルシステム

ファイル型 TrueCrypt コンテナをジャーナリングファイルシステム(NTFS のような)に格納する場合、TrueCrypt コンテナ(あるいは、その断片)のコピーがホストボリュームの空き領域に残る可能性があります。このことはいろいろなセキュリティの問題を生じます。たとえば、ボリュームの

パスワードやキーファイルをあとから変更しても、敵対者が **TrueCrypt** ボリュームの古い(ヘッダーが再暗号化される前にマウントするのに必要だった)ヘッダーやその断片を見つけたら、古いパスワードでボリュームをマウントできるかもしれません。いくつかのジャーナリングファイルシステムは、ファイルのアクセス日時や他の機密であるべき情報を内部的に記録します。ジャーナリングファイルシステムに関する安全性の問題を防ぐには、以下のどれかを実行してください。

- ファイル型のかわりに、パーティション/デバイス型 **TrueCrypt** ボリュームを使う。
- コンテナをジャーナリング機能がないファイルシステム(たとえば **FAT32**)に格納する。

みせかけの拒否の隠しボリュームの安全に関する予防策も参照してください。

安全なバックアップのとり方

ハードウェアやソフトウェアのエラーや欠陥のために、TrueCrypt ボリュームに保存したデータが破損することもあります。したがって、定期的にすべての重要なファイルのバックアップをとることを強くすすめます。(これは TrueCrypt ボリュームに保存された暗号化データだけではなく、それ以外のどんな重要なデータについても同様です)

非システムボリューム

TrueCrypt 非システムボリュームを安全にバックアップするには、下記手順にしたがってください。

1. TrueCrypt ボリューム作成ウィザードを使って(クイックフォーマットやダイナミックオプションは使わずに)新規の TrueCrypt ボリュームを作成してください。それがバックアップボリュームになるので、そのサイズはバックアップ元のボリュームと同じか大きくなるようにしてください。

主となるボリュームが TrueCrypt 隠しボリューム(隠しボリュームを参照)であれば、バックアップボリュームも同様に TrueCrypt 隠しボリュームでなくてはなりません。隠しバックアップボリュームを作る前に、クイックフォーマットオプションを使わずに新しい外殻ボリュームを作っておく必要があります。さらに、バックアップボリュームがファイル型であれば、隠しバックアップボリュームにはコンテナのほんのわずかな部分しか使わず、外殻ボリュームの大部分はファイルで占められるべきです。(そうでないと、隠しボリュームに関するみせかけの拒否には不利な影響があるかもしれません)

2. 新しく作成したバックアップボリュームをマウントしてください。
3. 主となるボリュームをマウントしてください。
4. マウントされたバックアップ主となるボリュームのすべてのファイルを直接にバックアップボリュームへコピーしてください。

重要: 敵対者が繰り返しアクセスできる場所(たとえば、銀行の貸し金庫に保管したデバイス)にバックアップボリュームを保存するなら、バックアップ作成時には上記のすべての手順(ステップ1を含む)を繰り返す必要があります。(下記参照)

上記の手順に従えば、敵対者が下記のことを判別することを防止することができます。

- ボリュームのどのセクターが変更されているか(常にステップ1を実行するため)ということ。たとえば、銀行の貸し金庫(あるいは他の敵対者が繰り返しアクセスできる場所)に保管するデバイスにバックアップボリュームを保存し、そこに隠しボリュームがある場合には、これは特に重要なことです。(詳細はみせかけの拒否の章の隠しボリュームの安全に関する予防策の節を参照)
- ボリュームのうちの一つが他のもののバックアップであること。

システムパーティション

注意: ファイルのバックアップに加えて、TrueCrypt レスキューディスクのバックアップをとる (「システム -> レスキューディスク作成」を選択)ことを強くすすめます。詳細は TrueCrypt レスキューディスクを参照してください。

暗号化したシステムパーティションを安全にバックアップするには、以下の手順によることをすすめます。

1. コンピューターに複数の OS がインストールされているなら、起動前認証を必要としない OS を起動する。

そのコンピューターに複数の OS がインストールされていないなら、BartPE CD/DVD からブートすることができます。(Windows そのものを CD/DVD に保存して、そこからブートするということです。詳細はよくある質問(FAQ)と答えで BartPE を探してください)

上記のどれもが不可能なら、システムドライブを他のコンピュータのセカンダリドライブに接続して、そのコンピューターの OS をブートしてください。

注意 : 安全上の理由から、バックアップしたい OS が TrueCrypt 隠しボリューム(隠し OS の節を参照)にある場合は、この段階でブートしたい OS は他の隠し OS であるか” live-CD”(上記参照)OS でなくてははいけません。詳細はみせかけの拒否の隠しボリュームの安全に関する予防策を参照してください。

2. TrueCrypt ボリューム作成ウィザードで新しい TrueCrypt 非システムボリュームを作成する。(クイックフォーマットやダイナミックオプションを有効にしないこと)それがバックアップボリュームになるので、そのディスク容量はバックアップしたいシステムボリュームと同じかそれ以上であること。

バックアップしたい OS が TrueCrypt 隠しボリュームにある(隠し OS を参照)のなら、バックアップボリュームは同様に TrueCrypt 隠しボリュームでなくてははいけません。隠しバックアップボリュームを作る前に、クイックフォーマットオプションを使わずに新しい外殻ボリュームを作っておく必要があります。さらに、バックアップボリュームがファイル型であれば、隠しバックアップボリュームはコンテナのほんのわずかな部分しか使わず、外殻ボリュームの大部分はファイルで占められるべきです。(そうでないと、隠しボリュームに関するみせかけの拒否には不利な影響があるかもしれません)

3. 新しく作成したバックアップ用ボリュームをマウントする。
4. バックアップしたいシステムボリュームを以下の手順でマウントする。
 - a. 「デバイスの選択」をクリックし、バックアップしたいシステムパーティションを選択する。(隠し OS の場合は、OS がインストールされたい隠しボリュームを含むパーティションを選択)
 - b. OK をクリック。
 - c. 「システム -> 起動前認証をせずにマウント」を選択。
 - d. 起動前認証パスワードを入力し、OK をクリック。

5. バックアップボリュームをマウントし、(前の手順で通常の TrueCrypt ボリュームとしてマウントされた)システムボリュームからすべてのファイルをバックアップボリュームへ直接にコピーする。

重要： 敵対者がボリュームを繰り返しアクセスできるような場所(たとえば銀行の貸し金庫)にバックアップを保管するならば、バックアップするつど上記の手順(手順 2 を含む)にしたがうべきです。(下記参照)

上記の手順にしたがうならば、敵対者が以下のことをを見つけることを防ぐことができます。

- ボリュームのどのセクターが変更されたか。(手順 2 のおかげです) たとえば敵対者がボリュームを繰り返しアクセスできるような場所(たとえば銀行の貸し金庫)にバックアップを保管し、それに隠しボリュームが含まれるなら、これは特に重要なことです。(詳細はみせかけの拒否の隠しボリュームの安全に関する予防策を参照)
- どれがどのボリュームのバックアップであるか。

一般的注意事項

注意: 敵対者がボリュームを繰り返しアクセスできるような場所にバックアップを保管するならば、ボリュームを暗号化するときに複数の暗号方式をカスケード(たとえば、AES-Twofish-Serpent)することを考えてください。もしボリュームを暗号化するときに一つの暗号化アルゴリズムしか使っていないと、あとでそのアルゴリズムが破られたときには、攻撃者は彼が持っているボリュームのコピーを復号できてしまうかもしれません。1 件の暗号化アルゴリズムが破られる可能性よりも 3 件の暗号化アルゴリズムすべてが破られる可能性は非常に低いものです。

問題が起こったら

ここでは TrueCrypt を使っていて遭遇するかもしれない一般的な問題への解決策を提示します。
ここにはない問題であれば、次のところに記載があるかもしれません。

非互換性

既知の問題と制限

よくある質問(FAQ)と答え

問題::

ボリュームへの読み書きが非常に遅い。ベンチマークの結果によれば、私が使っている暗号化方式はハードディスクの速度より早いはずなのですが。

想定される原因:

なにかのアプリケーションがじゃまをしている可能性があります。T

対策案:

最初に、TrueCrypt コンテナのファイル名に実行ファイルであると予約されている拡張子(たとえば、.exe, .sys, .dll)がつけられていないことを確認してください。もし、そういった拡張子がついていると、Windows やアンチウイルスソフトがコンテナを妨害したり、ボリュームのパフォーマンスを低下させることがあります。

次に、障害になっていそうなアプリケーションを停止するかアンインストールしてください。アンチウイルスソフトウェアや自動デフラグツールなどがそれにあたります。アンチウイルスソフトウェアなら、設定でリアルタイムスキャンを停止することで解決する場合があります。それでも効果がなければ、一時的にウイルス防御ソフトウェアを停止してみてください。それもまた効果がないなら、それを完全にアンインストールしてコンピューターを再起動してみてください。

問題::

正常にボリュームがマウントされたのに、Windows から「このデバイスは有効なファイルシステムではありません」というようなメッセージが出る。

想定される原因:

TrueCrypt ボリュームのファイルシステムが破損している、あるいはボリュームがフォーマットされていない。

対策案:

TrueCrypt ボリュームのファイルシステムを修復するために OS が用意しているファイルシステム

修復ツールを使うことができます。Windows では **chkdsk** です。TrueCrypt はこのツールを TrueCrypt ボリュームで使う簡単な方法を用意しています。(chkdsk はファイルシステムを破損する可能性があるため) 最初に TrueCrypt ボリュームのバックアップコピーをとってから、そのボリュームをマウントしてください。TrueCrypt メインウィンドウの(ドライブリストで)マウントされたボリュームを右クリックしてください。そして、表示されるメニューから「ファイルシステムの修復」を選択してください。

問題:

隠しボリュームを作ろうとしたら、作成可能な最大サイズが予想外に小さい。(外殻ボリュームにはこれよりずっと大きい空き容量があるのですが)

想定される原因:

ファイルの断片化(フラグメンテーション)

または

クラスタサイズが小さすぎるところに、外殻ボリュームのルートディレクトリに置いたフォルダーやファイルが多すぎることが考えられます。

対策案:

注意: 下記の解決策は **FAT** ボリュームに作成した隠しボリュームにのみ適用されます。

外殻ボリュームにデフラグをかける。(マウントしてコンピュータまたはマイコンピュータのそのドライブレターを右クリック、プロパティをクリック、ツール・タブを選択、「最適化する」をクリック) ボリュームのデフラグが終わったら、もう一度隠しボリューム作成を試してください。

これで効果がなければ、外殻ボリュームのすべてのファイルとフォルダーを **Shift+Delete** を押すことで削除してください。フォーマットで消してはいけません。(事前に「ごみ箱」と「システムの復元」を無効にすることを忘れないでください) そして、完全に空になった外殻ボリュームに隠しボリュームを作成してみてください。(テスト目的だけです) それでも隠しボリュームの可能な最大サイズが変わらなければ、問題は拡張ルートディレクトリにありそうです。もし(ウィザードの最終ステップで)クラスタサイズを既定値のままにしなかったなら、こんどはクラスタサイズを既定値のままにして外殻ボリュームをフォーマットしなおしてください。

さらにこれでもだめなら、外殻ボリュームを再フォーマットして前回より少ないファイルやフォルダーをルートに置いてください。それでだめなら、再フォーマットしてルートのファイルやフォルダーを減らすことを繰り返してください。やっつけられないとか、効果なしなら、より大きいクラスタサイズで外殻ボリュームを再フォーマットしてください。それでも解決しなければ、解決するまで外殻ボリュームをクラスタサイズを大きくしながら再フォーマットを繰り返してください。他の方法として、**NTFS** ボリュームに隠しボリュームを作るということも試してください。

問題:

パーティション/デバイスを暗号化しようとする、**TrueCrypt** ボリューム作成ウィザードから使用中だというメッセージが出て、実行できません。

対策案:

そのパーティション/デバイスを何らかの形で使うプログラム(たとえば、アンチウィルスなど)を停止、アンインストールなどしてください。それでもだめなら、デスクトップのコンピュータ(またはマイコンピュータ)アイコンを右クリックして**管理 -> 記憶域 -> ディスクの管理**を選んでください。そこで暗号化したいパーティションをクリックし、**ドライブレターの変更**をクリックし、ドライブ文字とパスの変更をクリック、**削除**をクリックして **OK** としてください。最後にシステムを再起動してください。

問題:

隠しボリュームを作成しようとする、ウィザードが外殻ボリュームをロックできないと言ってきます。

想定される原因:

外殻ボリュームのファイルを何かのアプリケーションが開いています。

対策案:

外殻ボリュームのファイルを使うアプリケーションをすべて閉じてください。それでもだめなら、アンチウィルスを停止するかアンインストールし、再起動して試してください。

問題:

以下のどれかが発生:

1. **TrueCrypt** ボリュームをマウントできない。
2. **NTFS TrueCrypt** ボリュームを作成できない。

さらに、エラーメッセージが出る: 「他のプロセスで使用中のため、プロセスはファイルにアクセスできません」

想定される原因:

他のアプリケーションが干渉している可能性があります。これは TrueCrypt のバグではありません。OS が他のアプリケーションが排他アクセスのためデバイスをロックしていると TrueCrypt へ通知しています。(だから TrueCrypt はデバイスにアクセスできないわけです)

対策案:

干渉するアプリケーションを停止またはアンインストールすることで、通常は解決します。アンチウイルスやディスク管理ツールなどがこの例です。

問題:

ネットワークの先で共有になっているファイル型コンテナにアクセスしようとすると、「メモリー不足」または「サーバーストレージへアクセスできない」のエラーになります。

想定される原因:

Windows レジストリの *IRP* スタックサイズの値が小さすぎる。

対策案:

Windows レジストリで *IRP* スタックサイズキーを探し、その値を大きくし、システムを再起動する。このキーがレジストリに存在しなければ、次のように作成してください。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

そして、その値を **16** 以上に設定し、システムを再起動してください。詳細については下記を参照 <http://support.microsoft.com/kb/285089/> および <http://support.microsoft.com/kb/177078/>

非互換性

Adobe Photoshop® のアクティベーションおよびその他の FLEXnet Publisher® / SafeCast を使う製品

注意: 以下で述べることは、**TrueCrypt 5.1** 以降で非カスケード暗号アルゴリズム(つまり **AES, Serpent, Twofish**)を使っている場合¹には関係がありません。また、起動前認証(システム暗号化を参照)を使っていない場合にも関係がありません。

Acesso FLEXnet Publisher(旧 Macromedia SafeCast)アクティベーションソフトウェア(サードパーティ製のソフトウェア、たとえば Adobe Photoshop、のアクティベーションに使われている)は、データをドライブの最初のトラックに書込みます。TrueCrypt でシステムパーティション/ドライブが暗号化されているときに、これがあると TrueCrypt ブートローダーの一部が破損し、Windows を起動できなくなります。このような場合には、システムへのアクセスを回復するために、TrueCrypt レスキューディスクを使ってください。以下に二通りの手順をご案内します。

1. アクティベートされたサードパーティのソフトウェアをそのまま保持しておき、毎回 TrueCrypt レスキューディスクからシステムをブートする。これは単にレスキューディスクを CD/DVD ドライブに挿入し、レスキューディスク画面でパスワードを入れるだけです。
2. 毎回 TrueCrypt レスキューディスクを入れるのがいやなら、TrueCrypt ブートローダーを復旧することもできます。このためには、レスキューディスク画面で「**Repair Options > Restore TrueCrypt Boot Loader** (修復オプション -> TrueCrypt ブートローダーの復旧)」を選択してください。しかし、こうするとサードパーティソフトウェアのアクティベーションを無効にしてしまうでしょう。

TrueCrypt レスキューディスクの使い方については、TrueCrypt レスキューディスクを参照してください。

完全に解決できそうな案：TrueCrypt 5.1 以降にアップグレードし、システムパーティション/ドライブを復号し、非カスケード暗号化アルゴリズム(つまり、AES, Serpent, Twofish)で再暗号化する。

これは TrueCrypt のバグではない(SafeCast の不適切な設計によって起こる問題である)ことを知っておいてください。

¹その理由は、TrueCrypt ブートローダーは暗号カスケードを使わない場合のほうがより小さく、そのため、TrueCrypt ブートローダーのバックアップを保管するための十分な領域をドライブの最初のシリンダーに確保できるということです。また、TrueCrypt ブートローダーが破損すればいつでも自動的にそのバックアップコピーが代替として機能します。

既知の問題と制限

既知の問題

既知の問題についての最新情報をオンライン版で読むことを強く推奨します。 :
<http://www.truecrypt.org/docs/?s=issues-and-limitations>

- (この文書を作成した時点では、確認された問題点はありません)
-

制限

- **Windows XP/2003** では **TrueCrypt** は拡張(論理)パーティションを持つシステムドライブ全体の暗号化はサポートしていません。基本パーティションのみを含むシステムドライブ全体の暗号化は可能です。部分的あるいは全体的に暗号化するシステムドライブに拡張(論理)パーティションを作成してはいけません。(第一パーティションのみが作成できます)
注意: 拡張パーティションを含むドライブ全体を暗号化したいなら、システムパーティションを暗号化し、追加としてドライブの非システムパーティションにパーティション型 **TrueCrypt** ドライブを作成することができます。かわりに、**Windows** を **Vista** 以降のものにアップグレードすることも考慮してください。
- **TrueCrypt** は現在のところ、ダイナミックディスクに変換されたシステムドライブの暗号化はサポートしていません。
- **TrueCrypt** ボリュームパスワードはプリンタブルな **ASCII** キャラクターでなくてはなりません。パスワードに **ASCII** キャラクター以外を使うことはサポートしていませんし、問題を起こすこともあります。(ボリュームをマウントできないなど)
- **Windows2000** の制限のため、**TrueCrypt** は **Windows2000** での **Windows** マウントマネージャをサポートしていません。したがって、**Windows2000** のいくつかの標準ツール(たとえばディスク・デフラグ)は **TrueCrypt** ボリュームに対しては機能しません。さらに、**Windows2000** のマウントマネージャを使うこともできません。たとえばマウントポイントに **TrueCrypt** ボリュームを割り当てる(**TrueCrypt** ボリュームをフォルダーとして割り当てる)ということなどです。
- **Windows** ボリュームシャドーコピーサービスは現在のところシステム暗号化の範囲内のパーティション(たとえば **TrueCrypt** で暗号化されたシステムパーティションまたは **TrueCrypt** で暗号化されたシステムドライブ上の非システムパーティション)のみをサポートしています。ボリュームの他の型ではボリュームシャドーコピーサービスはサポートされていません。これは、必要な A P I についての資料がマイクロソフトから非公開という条件でしか入手できないから

です。

- 暗号化パーティションのサイズ変更はできません。
- システムパーティション/ドライブが暗号化されていると、システムは(Windows XP から Windows Vista とするように)アップグレードしたり、Windows インストール CD/DVD で OS ブート前の環境での修復はできません。このような場合には、最初にシステムパーティション/ドライブを復号する必要があります。注意 システムパーティション/ドライブが暗号化されていても、システムのアップデート(セキュリティパッチやサービスパックなど)は可能です。
- ノート PC の電池が少ないと、Windows はコンピュータが省電力モードに入るときに、動作中のアプリケーションに適切なメッセージを送らないかもしれません。したがって、このような場合には TrueCrypt は自動アンマウントに失敗します。
- TrueCrypt で暗号化されたフロッピーディスク: フロッピーディスクが排出され他のディスクが挿入されると、ゴミが書かれたり読まれたりしてデータが破損するかもしれません。これはフロッピーディスクをまるごとボリュームとして扱う場合で、フロッピーディスク上のファイル形式コンテナの場合ではありません)

よくある質問(FAQ)と答え

TrueCrypt FAQ の最新版は <http://www.truecrypt.org/faq.php> で入手できます。(英語版)

Q: 「クイックスタートガイド」のような初心者用の説明はありますか？

A: はい。第1章の「初心者のためのチュートリアル」が TrueCrypt ボリュームの作成、マウント、使用についてスクリーンショットや段階を追った解説を記載しています。

Q: TrueCrypt は Windows がインストールされたパーティション/ドライブを暗号化できますか？

A: はい。(システム暗号化の章を参照)

Q: TrueCrypt ボリュームに保存されたビデオ(.avi, .mpg, etc.) を直接再生できますか？

A: はい、TrueCrypt の暗号化ボリュームは通常のディスクと同じです。正しいパスワードやキーファイルで TrueCrypt ボリュームをマウント(オープン)してください。ビデオファイルをダブルクリックすれば、OS がそのファイルタイプに関連づけられているアプリケーション(通常は再生ソフト)を起動します。再生ソフトはビデオファイルの最初のある部分を TrueCrypt の暗号化ボリュームから RAM に読み込みます。その部分が読み込まれているあいだ、TrueCrypt は RAM にデータを復号します。そして、復号された RAM 中のデータが再生ソフトによって再生されるということになります。それが再生されているあいだに、再生ソフトは次の一定部分を TrueCrypt の暗号化ボリュームから RAM に読み込み、このプロセスがくりかえされることになります。同じことが録画でもおこなわれます。ビデオファイルの一部でも TrueCrypt ボリュームに書き込まれる前に、TrueCrypt は RAM 中でそれを暗号化しディスクに書き込みます。このプロセスは即時自動暗号化/復号(on-the-fly encryption/decryption)と呼ばれ、ビデオファイルだけではなくすべてのファイルタイプに適用されます。

Q: TrueCrypt はずっとこのままオープンソースでフリーなのですか？

A: はい、そうです。商業版は計画していませんし、そうもならないでしょう。私たちはオープンソースでフリーなセキュリティソフトウェアに信頼をおいています。

Q: TrueCrypt プロジェクトに寄付できますか？

A: はい。詳細については <http://www.truecrypt.org/donations/> を参照してください。

Q: パスワードを忘れてしまいました。TrueCrypt ボリュームからファイルを復旧することはできますか？

A: TrueCrypt はデータの暗号化に使った正しいパスワードやキーなしで暗号化したデータの一部あるいは全体を復旧する機構は持っていません。唯一の方法はパスワードやキーを破ることで、ソフト/ハードの性能、パスワードあるいはキーファイルの質と長さによって数千年から数百万年かかるでしょう。

Q: ファイル名やフォルダー名も暗号化されるのですか？

A: はい、そうです。TrueCrypt ボリュームの中のファイルシステム全体(ファイル名、フォルダー名、ファイルの内容なども含む)が暗号化されます。これはファイルコンテナ(仮想 TrueCrypt ディスク)と TrueCrypt 暗号化パーティション/デバイスの両方について適用されます。

Q: USB フラッシュドライブでどのようにして TrueCrypt を使うことができますか？

A: 二つの方法があります

- 1) USB フラッシュドライブ全体を暗号化する。しかし、この方法では TrueCrypt を USB フラッシュドライブから起動することはできません。
注意: Windows では USB フラッシュドライブの複数パーティションをサポートしていません。
- 2) USB フラッシュドライブに TrueCrypt ファイルコンテナを作る。(作り方については初心者のためのチュートリアルを参照) USB フラッシュドライブに十分な空き領域があれば(そうなるように TrueCrypt コンテナの大きさを決めれば)、TrueCrypt を USB フラッシュドライブの中に(コンテナの中ではなく、コンテナと併存して)格納し、TrueCrypt を USB フラッシュドライブから起動することができるでしょう。(詳細はトラベラーモード参照)

Q: TrueCrypt 隠しボリュームにインストールした Windows から起動できますか？

A: TrueCrypt 6.0 から可能です。詳細は隠し OS を参照してください。

Q: 私の TrueCrypt ボリューム(コンテナ)をどのコンピュータにでもマウントできますか？

A: TrueCrypt ボリュームは(物理的なパーティション/ドライブを TrueCrypt で暗号化した場合に比べると)OS から独立しています。TrueCrypt を起動できるコンピューターならどれにでもマウントできます。(「管理者権限がなくても Windows で TrueCrypt を使えますか?」も参照)

Q: マウントされた TrueCrypt ボリュームがあるホットプラグデバイス(USB フラッシュディスクや USB ハードディスク)を取り外したり電源を切ったりできますか？

A: デバイスを取り外したり電源を切ったりする前に、TrueCrypt で TrueCrypt ボリュームをアンマウントし、可能なら「取り出し」(「コンピュータ」か「マイコンピュータ」の該当デバイスを右クリック)操作をするか、「ハードウェアの安全な取り外し」(タスクバーから操作可能)をしてください。そうしないと、データが失われるかもしれません。

Q: 隠し OS とは何ですか?

A: 隠し OS の節を参照してください。

Q: OS を再インストールやアップグレードしても元からある TrueCrypt パーティション/コンテナをマウントできますか?

A: はい、TrueCrypt ボリュームは OS から独立しています。ただし、OS のインストーラが TrueCrypt ボリュームがあるパーティションをフォーマットしないようにしてください。

注意：システムパーティション/ドライブを暗号化していて **Windows** を再インストールやアップグレードしたい場合は、最初にそれを復号する必要があります。(「システム - システムパーティション/ドライブの暗号化を解除」を選択)

Q: TrueCrypt の旧バージョンから最新バージョンには問題なくアップグレードできますか?

A: はい、一般的には可能です。しかし、アップグレード前に使用中のバージョンのあとに公開されたすべてのバージョンのリリースノートを読んでください。使用中のバージョンから新しいバージョンへのアップグレードについての既知の問題や非互換性があれば、リリースノートに記載があるはずです。

Q: システムパーティション/ドライブを暗号化していても TrueCrypt をアップグレードできますか? それとも最初に復号しておかなくてはならないでしょうか?

A: はい、一般的には、システムパーティション/ドライブを復号しなくても最新版にアップグレードできます。(単に TrueCrypt インストーラを起動すれば、自動的にシステムにある TrueCrypt をアップグレードします) しかし、アップグレードする前に、使用中のバージョン以降のバージョンに関するリリースノートを読んでください。もし、使用中のバージョンから新しいものへのアップグレードに問題があるとか非互換性があるというような場合には、リリースノートに記載があるはずです。注意：システムパーティション/ドライブが暗号化されている場合は、TrueCrypt をダウングレードしてはいけません。

Q: 起動前認証を使っています。私がコンピュータを起動するのを見張っている人(敵対者)に TrueCrypt を使っていることを知られないようにすることはできますか?

A: はい(TrueCrypt 6.1 ならば)。暗号化システムを起動し、TrueCrypt を開始、設定のシステム暗号化で「起動前認証画面で一切の文字を表示しない(以下のカスタムメッセージを除く)」オプションを有効にして、OK をクリックしてください。そうすれば、コンピュータを起動したときに TrueCrypt ブートローダーは(パスワードを間違えたときでさえも)何も表示しません。パスワード入力可能な状態でも、コンピュータはフリーズしたように見えます。しかし、敵対者がハードディスクを調査すれば TrueCrypt ブートローダーがあることに気がついてしまうだろうということには、重要な点として留意しておいてください。

Q: 起動前認証を使っています。TrueCrypt ブートローダーが偽のエラーメッセージしか表示しないようにできますか?

A: はい(TrueCrypt 6.1 ならば)。暗号化システムを起動し、TrueCrypt を開始、設定のシステム暗号化で「起動前認証画面で一切の文字を表示しない(以下のカスタムメッセージを除く)」オプションを有効にして、対応するフィールドに偽のエラーメッセージ(たとえば Windows ブートローダーが Windows パーティションを見つけるところができないときに表示する「Missing operation system」というようなもの)を入力してください。しかし、敵対者がハードディスクを調査すれば TrueCrypt ブートローダーがあることに気がついてしまうだろうということには、重要な点として留意しておいてください。

Q: 隠しボリュームはどうやってマウントするのですか?

A: 隠しボリュームは通常の TrueCrypt ボリュームと同じ方法でマウントできます。「ファイルの選択」または「デバイスの選択」をクリックして、外殻ボリュームを選択(すでにマウント済でないことを確認)してください。つぎに「マウント」をクリックし、隠しボリューム用のパスワードを入力してください。マウントしようとしているのが隠しボリュームか外殻ボリュームかは入力されたパスワードで決定されます。(つまり、外殻ボリューム用パスワードを入力すれば外殻ボリュームが、隠しボリューム用パスワードを入力すれば隠しボリュームがマウントされます)

注意: TrueCrypt は入力されたパスワードで標準ボリュームヘッダーを復号しようとします。それに失敗すれば、通常なら隠しボリュームのヘッダーがあるはずの領域(つまり 65536-131071 バイトで、そのボリュームに隠しボリュームがなければ、すべてランダムデータとなる)を RAM に読み込み、入力されたパスワードでそれを復号しようとします。隠しボリュームのヘッダーは単なるランダムデータにしか見えないので、それと特定することはできないことに留意してください。ヘッダーの復号に成功(どのように成功したかを判断するかについては暗号化の仕組みを参照)すると、まだ RAM にあるヘッダーから隠しボリュームの大きさを得て、隠しボリュームをマウントします。(大きさはオフセットで決定されます)

詳細については隠しボリュームに記述しています。

Q: 隠し OS を破損する恐れなしに、囲 OS にデータを保存できますか?

A: はい。隠し OS を破損することなく、いつでも囲 OS にデータを書き込むことができます。(囲 OS は隠し OS と同じパーティションにインストールされないからです)隠し OS を参照してください。

Q: 管理者権限がなくても Windows で TrueCrypt を使うことはできますか?

A: TrueCrypt を管理者権限なしで使うを参照してください。

Q: TrueCrypt はパスワードをディスクに保存しますか?

A: いいえ。

Q: パスワードのハッシュはどこかに保存されますか？

A: いいえ。

Q: TrueCrypt ボリュームにアプリケーションをインストールし、動かすことができますか？

A: はい。

Q: TrueCrypt はどのようにして正しいパスワードが入力されたかを判断しているのですか？

技術解説の暗号化の仕組みを参照してください。

Q: TrueCrypt はハードウェア/ソフトウェア レイドと Windows のダイナミックボリュームをサポートしていますか？

A: はい。ただし、Windows XP/2000/2003 ではダイナミックボリュームに関する次の記述 (Windows Vista およびそれ以降は除く) を読んでください。

Windows のダイナミックボリュームを TrueCrypt ボリュームとしてフォーマットする場合には、(Windows のディスク管理ツールを使って)ダイナミックボリュームを作成したあと、システムを再起動して、TrueCrypt ボリューム作成ウィザードの「デバイス選択」に目的のボリュームが表示され、選択できるようにすることを忘れないようにしてください。また、「デバイス選択」ウィンドウで、ダイナミックボリュームは単一のデバイス(項目)としては表示されないことにも注意してください。そのかわり、ダイナミックボリュームを構成するすべてのボリュームが表示されるので、ダイナミックディスク全体をフォーマットするために、そのうちのどれか一つを選択してください。

Q: CD や DVD に保管された TrueCrypt コンテナをマウントできますか？

A: はい。しかし、Windows2000 で読み出し専用メディア(CD/DVD 他)にある TrueCrypt ボリュームをマウントする場合には、TrueCrypt ボリュームを FAT でフォーマットしなくてはならないことを覚えておいてください。(Windows2000 では読み取り専用メディアの NTFS ファイルシステムはマウントできません)

Q: TrueCrypt をインストールせずに実行できますか？

A: はい、トラベラーモードの章を参照してください。

Q: トラベラーモードで TrueCrypt を実行しようとする、なぜ Windows Vista は毎回許可を求めてくるのですか？

A: TrueCrypt をトラベラーモードで動かすときには、TrueCrypt は TrueCrypt デバイスドライバを読み込んで起動する必要があります。TrueCrypt は透過的な即時暗号化/復号機能を提供するためにデバイスドライバを必要としますが、管理者権限がないユーザーは Windows でデバイスドライバを起動することができません。だから、Windows Vista は管理者権限で TrueCrypt を起動してもいいかどうかを問い合わせてくるというわけです。

TrueCrypt をトラベラーモードで動かすのではなく、システムにインストールすれば、毎回許可を求められることはありません。

Q: TrueCrypt が扱える最大ボリュームサイズはどのくらいですか？

A: 可能な TrueCrypt ボリュームの最大サイズは 8589934592 GB です。しかし、安全上の理由から、最大ボリュームサイズは 1PB(1,048,576 GB)となっています。これは、暗号化アルゴリズムのブロックサイズに依存する単一のキーで暗号化するデータの合計で安全なのは、この大きさまでだと考えられるからです。さらに、他の制限となる要因を考慮する必要があります。たとえば、ファイルシステムの制限、ハードウェア接続や OS による制約などです。

Q: Windows の終了や再起動の前に、TrueCrypt ボリュームをアンマウントする必要がありますか？

A: いいえ。TrueCrypt はシステムの終了や再起動時には、すべてのマウントされた TrueCrypt ボリュームを自動的にアンマウントします。

Q: パーティションとファイルコンテナと、どちらの TrueCrypt ボリュームがいいのでしょうか？

A: ファイルコンテナは通常のファイルであり、通常のファイルと同じに扱うことができます。(たとえば、ファイルコンテナは通常のファイルと同じ方法で移動、リネーム、削除ができます) パーティション/デバイスは性能に関しては優れています。コンテナがひどく断片化していると、コンテナへの読み書きがあきらかに遅くなることに注意してください。これを解決するにはコンテナがアンマウントされている状態のときに、デフラグを実行してください。

Q: TrueCrypt ボリュームをバックアップするいい方法がありますか？

安全なバックアップのとり方を参照してください。

Q: TrueCrypt パーティションをフォーマットするとどうなるのでしょうか？

この FAQ の「暗号化ボリュームのファイルシステムを変更できますか？」を参照してください。

Q: 暗号化ボリュームのファイルシステムを変更できますか？

A: マウントされていれば、可能です。TrueCrypt ボリュームは FAT12, FAT16, FAT32, NTFS, またはほかのどんなファイルシステムでもフォーマットすることができます。TrueCrypt ボリューム

ムは普通のボリュームと同じように扱うことができるので、コンピュータまたはマイコンピュータなどでデバイスのアイコンを右クリックし、フォーマットを選んでください。ボリュームの内容は失われますが、ボリュームは暗号化された状態のままになります。もし、パーティション形式の TrueCrypt ボリュームがマウントされていないときにそのパーティションをフォーマットすると、ボリュームは破壊され、パーティションは暗号化された状態ではなくなり、空となります。

Q: Windows 起動時に自動的に TrueCrypt を起動してパスワード要求を表示し、ボリュームをマウントするように設定できますか？

はい、以下の手順で可能です。

1. ボリュームをマウントし、「ボリューム -> 現在マウントされているボリュームをお気に入り」に保存」を選択
2. 「設定 -> 各種設定」の Windows の項目、「ログオン時に自動的に実行する内容」で「お気に入りボリュームをマウント」オプションを有効にしてください。
3. 「各種設定」ウィンドウで OK をクリックしてください。

Q: 隠しボリュームのパスワードを変更できますか？

A: はい。パスワード変更ダイアログは標準ボリュームにも隠しボリュームにも機能します。ボリュームパスワード変更ダイアログの「現在のパスワード」に隠しボリュームのパスワードを入力してください。

注: TrueCrypt は最初に標準ボリュームヘッダーを復号しようとします。これに失敗するとその中に隠しボリュームがあると想定し、隠しボリュームのヘッダーがあると想定される位置のデータを復号しようとします。これが成功するとパスワード変更は隠しボリュームに対して適用されることになります。(どちらの試みも「現在のパスワード」に入力されたパスワードを使います)

Q: HMAC-RIPEMD-160 を使うとき、キーサイズは 160 ビットに制限されているのですか？

A: いいえ。TrueCrypt は(HMAC アルゴリズムだけではなく)ハッシュ関数の出力を直接暗号化キーとして使うことはありません。詳細は「ヘッダーキーの導出、ソルト、および反復回数」を参照してください。

Q: ボリュームに保存されたデータを失わずに、ヘッダーキー導出アルゴリズムを変更できますか？(たとえば、HMAC-RIPEMD-160 から HMAC-SHA-512 へ)

A: はい。「ボリューム」->「ヘッダーキー導出アルゴリズムの設定」を選択してください。

Q: 2GB 以上の TrueCrypt コンテナをどうやって DVD に焼くのですか？

A: あなたが使っている DVD 作成ソフトで DVD のフォーマットを選択できるはずです。そこで、UDF フォーマットを選んでください。(ISO フォーマットは 2GB を越えるファイルをサポートしていません)

Q: TrueCrypt はどのようなライセンス形態で配布されているのですか？

A: ライセンスは TrueCrypt のバイナリまたはソースコードのパッケージに含まれる License.txt に記載されており、[d http://www.truecrypt.org/license](http://www.truecrypt.org/license) で入手することもできます。

Q: Windows のファイルセクタがマウントした最後のコンテナや最後に選択したキーファイルを記憶しています。防止できますか？

A: はい。まだであれば、TrueCrypt4.2a 以降にアップグレードしてください。TrueCrypt を起動してメインウィンドウの「履歴を保存しない」を有効にしてください。「履歴を保存しない」を有効にしたくなければ、コンテナアイコンを TrueCrypt.exe のアイコンにドラッグ(TrueCrypt は自動的に起動します)するか、TrueCrypt プログラムウィンドウにドラッグすれば、ファイルセクタを使うことを避けることができます。同様に、キーファイルもキーファイルウィンドウかパスワード入力ウィンドウへドラッグすることができます。

Q: 現在保存しているデータを失わずに、パーティション/ドライブを暗号化できますか？

A: はい。以下の条件があります。システムドライブ全体(複数のパーティションがあるかもしれない)、またはシステムパーティション(Windows がインストールされているパーティション)を暗号化する場合に、Windows XP 以降の Windows(たとえば Windows Vista)で TrueCrypt 5.0 以降を使う場合には可能です。非システムパーティションをそのまま暗号化することなら、NTFS フォーマットで、TrueCrypt 6.1 以降を Windows Vista 以降(たとえば Windows 2008)で使う場合には可能です。

Q: マウントされた TrueCrypt ボリュームの内容に対して、chkdsk や Defrag といったツールを使うことはできますか？

A: はい。TrueCrypt ボリュームは本物の物理的なディスクと同じに扱うことができますから、どんなファイルシステムのチェックや修復、デフラグのツールでもマウントされた TrueCrypt ボリュームに対して使うことができます。

Q: 暗号化されていない Windows で痕跡を残さずに TrueCrypt を使うことはできますか？

A: はい。これは BarPE のもとで TrueCrypt をトラベラーモードで起動することで実現できます。BartPE とは Bart's Preinstalled Environment (バートのプリインストール環境)を意味します。これは、基本的に用意された WindowsOS そのものを CD/DVD に格納し(レジストリ、臨時ファイル、他は RAM に保持されます - ハードドライブはまったく使いませんし、ハードドライブが存在する必要ありません)、そこから Windows を起動するというものです。フリーウェアである Bart's PE Builder は Windows XP インストール CD を BartPE に変換することができます。TrueCrypt 3.1 以降を使っているなら、BartPE の TrueCrypt プラグインは必要ありません。BartPE を起動し、最新の TrueCrypt を RAM ディスク(BartPE が作成)にダウンロードし、パッケージを RAM ディス

クに展開、TrueCrypt.exe を RAM ディスクから起動するだけです。

注意：隠し OS を作成することも考慮してください。(詳細は隠し OS の節を参照)

Q: TrueCrypt ボリュームの中に格納されている TrueCrypt ボリュームをマウントすることはできますか？

A: はい、TrueCrypt ボリュームは無制限に入れ子にできます。

Q: TrueCrypt と他の自動即時暗号化ツールを同じシステムで併用できますか？

A: TrueCrypt と他の自動即時暗号化ツールを併用することで問題が起きるとも起きないとも聞いていません。

Q: TrueCrypt パーティションのサイズを変更できますか？

A: 残念ですが、こういったことはできません。PartitionMagic のようなプログラムで TrueCrypt パーティションのサイズを変更すると、多くの場合はデータを壊すことになるでしょう。

Q: TrueCrypt は Windows Vista x64 (64-bit) Edition で動きますか？

A: はい(バージョン 4.0 の場合)。 注意: すべての TrueCrypt の .sys と .exe ファイルは認証機関 GlobalSign によって発行された TrueCrypt Foundation のデジタル認証によってデジタル署名されています。

Q: TrueCrypt は mac OS X で動きますか？

A: はい、動きます。

Q: TrueCrypt は Linux で動きますか？

A: はい。

Q: Windows と Linux と Mac OS X で同じ TrueCrypt ボリュームをマウントできますか？

A: はい。TrueCrypt ボリュームは完全にクロスプラットフォーム(OS を問わない)です。

Q: TrueCrypt ボリュームの一部が破損するとどうなりますか？

A: 暗号化データではあるひとつのバイトが破損すると、通常はそれが発生した暗号化ブロック全体が破損したことになります。TrueCrypt では暗号化ブロックのサイズは 16 バイト(128 ビット)で

す。TrueCrypt で使われる動作モードはあるブロック内でのデータ破損が他のブロックに影響を及ぼさないことを保証します。(詳細は動作モードを参照)

「TrueCrypt ボリュームの暗号化したファイルシステムが破損した場合、どうすればいいですか?」という質問も参照してください。

Q: TrueCrypt ボリュームの暗号化したファイルシステムが破損した場合、どうすればいいですか?

A: TrueCrypt ボリュームのファイルシステムは他の暗号化されていないファイルシステムと同様に破損の可能性があります。こうなったとき、ファイルシステム OS が提供する修復ツールを利用することができます。Windows では **chkdsk** です。TrueCrypt はこのツールを TrueCrypt ボリュームで使う簡単な方法を用意しています。(chkdsk はファイルシステムを破損する可能性があるため) 最初に TrueCrypt ボリュームのバックアップコピーをとってから、そのボリュームをマウントしてください。TrueCrypt メインウィンドウの(ドライブルISTで)マウントされたボリュームを右クリックしてください。そして、表示されるメニューから「ファイルシステムの修復」を選択してください。

Q: 企業内で TrueCrypt を使っています。ユーザーがボリュームのパスワードを忘れたとき(またはキーファイルを失ったとき)や起動前認証のパスワードを忘れたときに管理者がリセットする方法はありますか?

A: はい。TrueCrypt には「裏口」は用意されていません。しかし、TrueCrypt ボリュームのパスワード/キーファイルや起動前認証のパスワードをリセットする方法はあります。ボリュームを作ったあと管理者権限を持たないユーザーにそのボリュームの使用を認める前に、(ツール -> ボリュームヘッダーのバックアップを選択して)そのヘッダーのバックアップをファイルにとります。パスワード/キーファイルから導出されたヘッダーキーで暗号化されているボリュームヘッダーは、ボリュームを暗号化したマスターキーを持っています。そこで、ユーザーにパスワードを選んでもらいその人のためにパスワードを設定します。(「ボリューム」->「ボリュームのパスワード変更」) そうすれば、ユーザーにそのボリュームの使用許可を与えると同時に、いつでも管理者の許可や助力なしで任意のパスワードに変更させることができます。ユーザーが自分が決めたパスワードを忘れた場合でも、バックアップファイルからボリュームヘッダーを復旧(ツール -> ボリュームヘッダーのリスト)することで、ボリュームのパスワード/キーファイルをオリジナルの管理者パスワード/キーファイルに戻すことができます。

同様に、起動前認証でもパスワードをリセットすることができます。マスターキーデータのバックアップを作成(TrueCrypt レスキューディスクに保存され、管理者パスワードで暗号化される)するには、「システム -> レスキューディスク作成」を選択してください。ユーザーの起動前認証パスワードを変更するのは「システム -> パスワードの変更」を選択してください。管理者パスワードに戻すには、TrueCrypt レスキューディスクから起動し、「'Repair Options' > 'Restore key data'」を選択し、管理者パスワードを入力してください。注意：TrueCrypt レスキューディスクの ISO イメージを CD/DVD に書き込まなくてもかまいません。全ワークステーション用に中央で(CD/DVD そのものではなく)ISO イメージを保管しておくことができます。詳細はコマンドラインの使い方(オプション /noisocheck)を参照してください。

Q: ある単一の **TrueCrypt** ボリュームを複数の **OS** から同時にアクセスできますか(ボリュームがネットワークで共有されている場合など)?

A: ネットワーク間の共有を参照してください。

Q: ネットワーク経由で **TrueCrypt** ボリュームにアクセスできますか?

A: ネットワーク間の共有を参照してください。

Q: 非システムパーティションを暗号化しましたが、そのドライブ文字が「マイコインピューター」に表示されたままです。それをダブルクリックすると、**Windows** はそのドライブをフォーマットするかと聞いてきます。ドライブ文字をつけないとか隠すとかできませんか?

A: できます。ドライブ文字をつけないようにするには、下記の手順にしたがってください。

1. デスクトップまたはスタートメニューの「コンピュータ」または「マイコンピュータ」アイコンを右クリックして「管理」を選択してください。「コンピュータの管理」ウィンドウが開きます。
2. 左のリストから、「ディスクの管理」(「記憶域」の下にある)を選択してください。
3. 暗号化されたパーティションを右クリックし、「ドライブ文字とパスの変更」を選択してください。
4. 「削除」をクリックしてください。
5. **Windows** が確認を求めてきたら、「はい」をクリックしてください。

Q: 必要がなくなったとき、どうやって暗号化を解除できますか? どうすればボリュームを完全に復号できますか?

A: 暗号化を解除するにはを参照してください。

Q: ボリュームをリムーバブルメディアとしてマウントすると、何が変わるのですか?

A: たとえば **Windows** が自動的に **TrueCrypt** ボリュームに *Recycled* や *System Volume Information* といったフォルダー(これらはごみ箱やシステムの復元機能のために作られます)を作ることを防止したいなら、このオプションにチェックを入れてください。しかし、これには不利な点もあります。たとえば、このオプションを有効にすると、コンピュータまたはマイコンピュータのリストでは空き領域を表示しません。(これは **TrueCrypt** のバグではなく、**Windows** の制限です)

Q: 既存のコンテナを複製することで、新しいコンテナを作っても安全ですか?

A: 新しい **TrueCrypt** コンテナを作る場合は、つねにボリューム作成ウィザードを使ってください。もし、コンテナをコピーして両方を使うと、両方に異なったデータが入ることになり暗号解析の手がかりになるかもしれません。なぜなら、両方のボリュームが同じキーセットを持つためです。安全なバックアップのとり方も参照してください。

Q: TrueCrypt ボリュームの空き領域を完全削除するべきでしょうか？

補足: 完全削除とは、安全に消去すること、復元不可能なように機密データを上書きすること

A: 敵対者がボリュームを復号できると思う(たとえば、パスワードを明かすことを強制されるとか)なら、「はい」です。そうでなければ必要ありません。というのは、ボリューム全体が暗号化されているからです。

Q: TrueCrypt はどのようにして、データを暗号化したアルゴリズムを判別するのですか？

A: 技術解説の暗号化の仕組みを参照してください。

暗号化を解除するには

TrueCrypt はシステムパーティションまたはシステムドライブについてのみ、そのままの状態での復号(「システム -> システムパーティション/ドライブの暗号化解除」を選択)ができます。もし、暗号化が必要なくなって、暗号化を除去したいなら、下記の手順にしたがってください。

1. TrueCrypt ボリュームをマウントする。
2. TrueCrypt ボリューム内のすべてのファイルを TrueCrypt 外へ移動する。
3. TrueCrypt ボリュームをアンマウントする。
4. **TrueCrypt ボリュームがファイル型の場合**には、他の一般のファイルと同様の操作でそのファイル(コンテナ)を削除する。

ボリュームがパーティション型(USB フラッシュドライブも含む)の場合には上記 1-3 に続いて、下記の手順による。

- a. デスクトップかスタートメニューの「コンピュータ」か「マイコンピュータ」を右クリックし「管理」を選択する。「コンピュータの管理」ウィンドウが表示される。
- b. 「コンピュータの管理」ウィンドウの左のリストの「記憶域」の下「ディスク管理」を選択する。
- c. 復号したいパーティションを右クリックして「ドライブ文字とパスの変更」を選択。
- d. 「ドライブ文字とパスの変更」ウィンドウでドライブ文字が表示されなければ「追加」、それ以外は「キャンセル」をクリックする。
「追加」をクリックした場合は「ドライブ文字またはパスの追加」が表示されるので、割り当てたいドライブ文字を選んで **OK** をクリックする。
- e. 「コンピュータの管理」ウィンドウで復号したいパーティションを再度クリックする。そして、「フォーマット」を選択すると「フォーマット」ウィンドウが表示される。
- f. 「フォーマット」ウィンドウで **OK** をクリックする。フォーマットが完了すれば、そのパーティションは読み書きのために **TrueCrypt** でマウントする必要はない。

ボリュームがデバイス型(つまり、デバイスが区画にわけられていなくて、デバイスがまるごと暗号化されている)の場合には上記 1-3 に続いて、下記の手順による。

- a. デスクトップかスタートメニューの「コンピュータ」か「マイコンピュータ」を右クリックし「管理」を選択する。「コンピュータの管理」ウィンドウが表示される。
- b. 「コンピュータの管理」ウィンドウの左のリストの「記憶域」の下「ディスク管理」を選択する。
- c. 暗号化デバイスを示す領域を右クリックし、「新規パーティション」または「新規シンプルボリューム」を選択する。
- d. 警告: 作業を続ける前に、目的のデバイスを選んでいかどうかを確認してください。そうでないと、そこに保存されたすべてのファイルが失われることになります。
「新規パーティションウィザード」か「新規シンプルボリュームウィザード」が表示されるので、新規パーティションを作成するためにウィザードの指示にしたがう

こと。パーティションが作成されれば、そのパーティションは読み書きのために TrueCrypt でマウントする必要はない。

TrueCrypt のアンインストール

TrueCrypt をアンインストールするには、Windows Xp では「スタート->コントロールパネル->プログラムの追加と削除」->TrueCrypt->変更と削除」と進んでください。Windows Vista では「スタート->コントロールパネル->プログラム: プログラムの削除->TrueCrypt-> 変更と削除」と進んでください。

TrueCrypt をアンインストールしても TrueCrypt ボリュームは削除されません。TrueCrypt をインストールするかトラベラーモードで起動すれば、その TrueCrypt ボリュームをまたマウントできます。

TrueCrypt システムファイルとアプリケーションデータ

注意: %windir% は windows をインストールした主要パス(通常は C:\WINDOWS)のことです。

TrueCrypt ドライバ

%windir%\SYSTEM32\DRIVERS\truecrypt.sys (32-bit Windows)

または

%windir%\SysWOW64\drivers\truecrypt.sys (64-bit Windows)

注意: TrueCrypt がトラベラーモードで動くなら、このファイルは存在しません。

TrueCrypt 設定 / アプリケーションデータ:

次のファイルがアプリケーションデータが通常保存される場所に保存されます。(たとえば C:\Documents and Settings\UserName\Application Data\TrueCrypt\, UserName はあなたの Windows のユーザー名) トラベラーモードでは、これらのファイルは TrueCrypt.exe を起動するフォルダー(TrueCrypt.exe が存在するフォルダー)に保存されます。**警告: TrueCrypt はこれらのファイルを暗号化しません(TrueCrypt でシステムパーティション/ドライブを暗号化した場合を除く)。**

Configuration.xml

Original System Loader (ドライブの最初のトラックの TrueCrypt ブートローダー書込み前の元データのバックアップ)

補足: システムパーティション/ドライブが暗号化されていないならば、このファイルは存在しません。

System Encryption.xml (システムパーティション/ドライブを暗号化する過程での臨時設定ファイル)

Default Keyfiles.xml

注意 TrueCrypt の該当する機能を使っていなければ、このファイルは存在しないかもしれません。

Favorite Volumes.xml

注意 TrueCrypt の該当する機能を使っていなければ、このファイルは存在しないかもしれません。

History.xml (TrueCrypt ボリュームとして直近のマウント試行があったか TrueCrypt ホストとして使われたファイルやデバイスや直近 20 件のリスト; この機能は無効にすることができます。履歴を保存しないの項を参照)

注意 TrueCrypt の該当する機能を使っていなければ、このファイルは存在しないかもしれません。

技術解説

表記法

C	暗号テキストブロック
$D_k()$	暗号化/復号キー K を使う復号アルゴリズム
$E_k()$	暗号化/復号キー K を使う暗号化アルゴリズム
$H()$	ハッシュ関数
i	n -bit ブロックのブロックインデックス; n は状況による
K	暗号キー
P	プレーンテキストブロック
\wedge	排他的論理和 (XOR)
\oplus	加算して 2^n で割った余り。 n が左のオペランドと結果のビットサイズ。 (左のオペランドが 1-bit 値で、右のオペランドが 2-bit 値の場合: $1 \oplus 0 = 1$; $1 \oplus 1 = 0$; $1 \oplus 2 = 1$; $1 \oplus 3 = 0$; $0 \oplus 0 = 0$; $0 \oplus 1 = 1$; $0 \oplus 2 = 0$; $0 \oplus 3 = 1$)
\otimes	2 つの 2 項を越える多項式 GF(2) 剰余の乗算モジュール $x^{128}+x^7+x^2+x+1$ (GF はガロア域のこと)
\parallel	連結

暗号化の仕組み

TrueCrypt ボリュームをマウントするとき(パスワード/キーファイルが記憶されていないと仮定して)、または起動前認証中に、次のステップが実行されます。

1. ボリュームの最初の 512 バイト(標準ボリュームのヘッダー)が RAM に読み込まれます。その最初の 64 ビットがソルトです。(「TrueCrypt ボリュームフォーマット仕様」を参照) システム暗号化(システム暗号化参照)については、最初の論理ドライブトラックの最後の 512 バイトが RAM に読み込まれます。(TrueCrypt ブートローダーはシステムドライブの最初のトラックおよび TrueCrypt レスキューディスクにあります)
2. ボリュームの 65536-66047 バイトが RAM に読み込まれます。(TrueCrypt ボリュームフォーマット仕様を参照)システム暗号化の場合は、起動パーティションの直後のパーティションの 65536-66047 バイトが読み込まれます。そのボリューム(または起動パーティションの直後のパーティション)に隠しボリュームがあれば、この時点でそのヘッダーを読み込んだことになります。そうでなければ、単に無意味なランダムデータを読み込んだだけということになります。(隠しボリュームがあるかないかは、このデータを復号できるかどうかで決まります。詳細は隠しボリュームの項を参照)
3. TrueCrypt は(1)で読み込んだ標準ボリュームヘッダーを復号しようとします。復号の過程で使われたり生成されたりしたデータは RAM に保持されます。(TrueCrypt はこれらをけっしてディスクに保存しません) 次のパラメータは未知¹で、試行錯誤で決定していきます。(以下の可能な組み合わせをすべて試します)
 - a. ヘッダーキー導出に使われる PRF(PKCS #5 v2.0 に規定。ヘッダーキーの導出、ソルト、および反復回数を参照) これは以下のどれかになります:
HMAC-SHA-512, HMAC-RIPEMD-160, HMAC-Whirlpool.
ユーザーが入力したパスワード(一つ以上のキーファイルも適用されるかもしれない - キーファイルの節を参照)と(1)で読み込まれたソルトはヘッダーキー導出関数へ渡され、一連の値(ヘッダーキーの導出、ソルト、および反復回数を参照)が作られます。そしてそれから、ヘッダー暗号化キーが生成され、第二ヘッダーキー(XTS モード)が形づくられます。(これらのキーはボリュームヘッダーの暗号化につかわれます)
 - b. 暗号化アルゴリズム: AES-256, Serpent, Twofish, AES-Serpent, AES-Twofish-Serpent など
 - c. 動作モード: XTS, LRW(旧式で使われない), CBC(旧式で使われない),
 - d. キーサイズ
4. 復号データの最初の 4 バイトが” TRUE”という ASCII 文字列であり、復号されたデータ(ボ

¹ これらのパラメータは、攻撃の困難さを強化するために秘密にされているのではなく、TrueCrypt ボリュームであるかどうかを事前に知ることができないためです。(単なるランダムデータと区別がつかない) ボリュームヘッダーにこれらのパラメータを格納しておくと、こうはなりません。

リユームヘッダー)の最後の 256 バイトの CRC-32 チェックサムが復号データの 8 番目のバイトの値と一致したなら、復号が成功したと判断します。(この値は暗号化されているので、敵対者にはわかりません。TrueCrypt ボリュームフォーマット仕様を参照) この条件が満たされなければ、プロセスは(3)に戻って続きます。

しかし、今回は(1)で読んだデータの代わりに(2)で読んだデータ(隠しボリュームのボリュームヘッダーの可能性)を使います。それでも条件に合わなければ、マウント動作は終了します。(間違ったパスワード、ボリュームの破損、または TrueCrypt ボリュームではないということになる)

5. これで正しいパスワード、適切な暗号化アルゴリズム、モード、キーサイズ、正しいヘッダーキー導出アルゴリズムがわかった(あるいは非常に高い可能性でわかったと仮定できる)ことになります。また、(2)で読んだデータを復号できたなら、隠しボリュームをマウントしようとしているということがわかり、そのサイズは(2)で読み込んで(3)で復号された結果から得ることができます。
6. 暗号化ルーチンは復号されたボリュームヘッダー(TrueCrypt ボリュームフォーマット仕様を参照) から得られたマスターキー¹と第二キーで再初期化(XTS モード - 動作モード参照)されます。このキーはボリュームヘッダー領域(または、システム暗号化のためのキーデータ領域)をのぞく、ボリュームのどのセクターでも復号するのに使うことができます。これでボリュームはマウントされました。

動作モード、ヘッダーキーの導出、ソルト、および反復回数も参照してください。

動作モード

TrueCrypt がパーティション、ドライブ、仮想ボリュームを暗号化するのに使う動作モードは XTS です。

XTS モードは 2003 年にフィリップ・ログウエイが設計した XEX モード[12]ではありますが、細かい修正(XEX

は単一のキーを 2 つの異なる目的に使いますが、XTS はそれぞれ別のキーを使います) 2007 年 12 月に XTS モードはブロック型記憶装置の暗号化保護についての IEEE 1619 規格で承認されました。

XTS モードの説明

$$C_i = E_{K1}(P_i \oplus (E_{K2}(n) \otimes \alpha^i)) \oplus (E_{K2}(n) \otimes \alpha^i)$$

ここでは:

⊗ 2 つの 2 項を越える多項式 $\Gamma\Phi(2)$ 剰余の乗算を示す $x^{128}+x^7+x^2+x+1$

K1 は暗号化キー(各暗号 AES, Serpent, Twofish についてそれぞれ 256 ビット)

K2 は第二キー(各暗号 AES, Serpent, Twofish についてそれぞれ 256 ビット)

¹ マスターキーはボリューム作成のときに生成され、あとで変更することはできません。ボリュームのパスワード変更は、新しいパスワードから導出される新しいヘッダーキーでボリュームヘッダーを再暗号化することで実施されます。

i はデータユニット内の暗号ブロックのインデックス。最初の暗号ブロックは $i=0$ となる。

n は K1 から見たデータユニットのインデックス。最初のデータユニットは $n=0$ となる。

α はガロア域の原始関数要素であり、多項式 x (つまり 2) に一致する。

それぞれのデータユニットのサイズは通常 512 バイト(セクターサイズは無視して)である。

XTS モードについての詳細は[12]を参照。

ヘッダーキーの導出、ソルト、および反復回数

ヘッダーキーはマスターキー他のデータを持つ TrueCrypt ボリュームヘッダーの暗号化領域を暗号化、復号するのに使われます。(暗号化の仕組みと TrueCrypt ボリュームフォーマット仕様を参照) TrueCrypt ヘッダーキーと第二キー(XTS モード)を生成する技法は PBKDF2 であり、PKCS #5 v2.0 に規定されています。[7]を参照。(PKCS #5 v2.0 文書は RSA 研究所のご厚意で <http://www.truecrypt.org/docs/pkcs5v2-0.pdf> で入手可能)

512-bit ソルト(ボリューム作成プロセスで組み込みの乱数発生機構で生成されるランダム数)が使われます。ということは、それぞれのパスワードについて 2^{512} (2 の 512 乗)のキーがあるということです。これは、オフライン辞書攻撃に対する脆弱性を大きく減少させます。(ソルトが使われると、事前にすべてのキーをコンピュータで組み合わせてパスワード辞書を作るということは、非常に難しくなります) [7] ソルトは TrueCrypt ボリューム作成過程で乱数発生機構によって生成される乱数値から成ります。ヘッダーキー導出関数は、HMAC-SHA-512 , HMAC-RIPEMD-160, または HMAC-Whirlpool([8, 9, 20, 22]を参照) に基づいており、ユーザーはどれかを選択できます。導出されるキーの長さは、基礎となるハッシュ関数の出力サイズに制限されません。たとえば、HMAC-RIPEMD-160 を使ったとしても、AES-256 のヘッダーキーはつねに 256 ビット長(XTS モードでは、256 ビット第二ヘッダーキーが追加され、結果として AES-256 では 256 ビットキーが二つ使われる)です。 詳細は[7]を参照してください。 ヘッダーキーを導出するにはキー導出関数を 1000 回 (HMAC-RIPEMD -160 を基礎としている場合は 2000 回)繰り返さなくてははいけません。これは徹底したパスワード探索(総当たり攻撃)に要する時間を増大させます。 [7]

カスケードの個々の暗号が使うヘッダーキーは同じパスワード(キーファイルも適用されるかもしれない)から導出されますが、相互に独立しています。たとえば、AES-Twofish-Serpent では、ヘッダーキー導出関数はパスワードから 768-bit キーを(XTS モードでは追加として 768 ビットの第二ヘッダーキーも)導出するように指示を受けます。生成された 768 ビットキーは三つの 256-bit キーに分割され(XTS モードでは第二キーも三つの 256 ビットキーに分割され、カスケード全体としては 6 個の 256 ビットキーを使う)、最初のものが Serpent で、二番目のものが Twofish、三番目のものが AES で(XTS モードでは最初の第二キーが Serpent、次の第二キーが Twofish、最後の第二キーが AES で)使われます。キーが導出される元になったパスワードを求める方法は(弱いパスワードへの総当たり攻撃を除いて)ないので、敵対者がキーの一つを知ったとしても、それから他のキーを導出することはできません。

乱数発生機構

TrueCrypt 乱数発生機構(RNG)は RAM(メモリ)に、マスター暗号化キー、第二キー(XTS モード)、ソルトおよびキーファイルを生成することに使われます。プールは 640 バイト長で、以下から発生するデータで満たされます。

- マウスの動き
- キーストローク¹
- Mac OS X, Linux: 内蔵 RNG(/dev/random と /dev/urandom の両方)から生成される値
- Windows のみ: MS Windows 暗号 API (500-ms 間隔で定期的に収集される)
- Windows のみ: ネットワークインターフェース統計(NETAPI32)
- Windows のみ: さまざまな Win32 ハンドル、時間変数、カウンタ(500-ms ごとに収集)

上記のソースのどれかから得られた値はプールに書き込まれ、個々のバイトに分割されます。(たとえば、32-bit 値は 4 バイトに分割されます) これらのバイトは個々に modulo 2^8 addition 演算をしてキーファイルプールの(プールの古い値の上書きではなく)プールカーソルの位置に書き込まれます。バイトが書き込まれたら、プールカーソルは 1 バイト進み、終端までくるとプールの先頭に位置づけられます。プールに 16 バイト書き込むごとに、プール混合関数がプール全体に適用されます。(下記参照)

プール混合関数

この関数の目的は拡散です。拡散することで、個々の「生の」入力ビットの影響をできるだけ広げます。これは統計的関連を隠すことにもなります。プールに 16 バイトを書き込むごとに、プール混合関数がプール全体に適用されます。

プール混合関数の説明は以下のとおり:

2. R を乱数プールとする。
3. H をユーザーが選択したハッシュ関数(SHA-512, RIPEMD-160 または Whirlpool)とする。
4. l はハッシュ関数 H の出力のバイト長。(つまり、 H が RIPEMD-160 なら、 $l = 20$; H が SHA-512 なら $l = 64$)
5. z = ランダムプール R のバイト長 (640 バイト)
6. $q = z / l - 1$ (H が Whirlpool なら $q = 4$)
7. R を l -バイトブロック $B_0 \dots B_q$ に分割
条件 $0 \leq i \leq q$ (各ブロック B ごとに) であるあいだ、以下のステップを実行:
 - a. $M = H(B_0 \parallel B_1 \parallel \dots \parallel B_q)$ [ランダムプールはハッシュ M を作るハッシュ関数 H で処理される]
 - b. $B_i = B_i \wedge M$
8. $R = B_0 \parallel B_1 \parallel \dots \parallel B_q$

¹Linux ではマウスが使えない場合にのみ、キーストロークが読み取られます。

たとえば、 $q = 1$ ならば、ランダムプールは次のように混合される:

$$(B_0 \parallel B_1) = R$$

$$B_0 = B_0 \wedge H(B_0 \parallel B_1)$$

$$B_1 = B_1 \wedge H(B_0 \parallel B_1)$$

$$R = B_0 \parallel B_1$$

乱数発生機構の設計と実装は下記の論文に基づく:

- *Software Generation of Practically Strong Random Numbers* by Peter Gutmann [10]
- *Cryptographic Random Numbers* by Carl Ellison [11]

キーファイル

TrueCrypt キーファイルは、その内容がパスワードと結びつけられるファイルです。キーファイルの内容について、特別の制限はありません。ユーザーは TrueCrypt RNG によってランダムな内容のファイルを作成する組み込みのキーファイル生成機能を使って、キーファイルを作成することもできます。(TrueCrypt RNG についての詳細は乱数発生機構を参照)

キーファイルの最大サイズに制限はありませんが、先頭の 1,048,576 bytes (1 MB)だけが処理対象となります。(巨大なファイルを作成するのに伴う性能上の問題から、残りの部分は無視されます) ユーザーは複数のキーファイルを使うことができます。(キーファイル数に制限はありません)

キーファイルは複数の PIN コード(PIN パッドや TrueCrypt GUI で入力可能)で保護された PKCS-11 規格[23]のセキュリティトークンやスマートカードに保管することもできます。

キーファイルは以下の方法で処理され、パスワードに適用されます。

1. P をユーザーが入力したパスワード(空かもしれません)とする。
2. KP をキーファイルプールとする。
3. kpl をキーファイルプール KP のバイト長(64 つまり 512 ビット)とする。
4. pl をパスワード P のバイト長(現バージョンでは $0 \leq pl \leq 64$)とする。
5. $kpl > pl$ ならば $(kpl - pl)$ の長さのバイト(値はゼロ)をパスワード P に追加する。
6. キーファイルプール KP を kpl バイトのゼロで満たす。
7. それぞれのキーファイルについて、以下のステップを実行:
 - a. キーファイルプールのカーソル位置をプールの先頭にセットする。
 - b. ハッシュ関数 H を初期化する。
 - c. キーファイルの全バイトを 1 個ずつロード、それぞれについて以下のステップを実行する。
 - i. 中間ハッシュ(状態) M を得るために、ハッシュを初期化せずにハッシュ関数 H でロードされたバイトのハッシュを作る。ハッシュの終了処理はしない(次回のために状態を保持する)。
 - ii. 状態 M を個々のバイトに分割する。例として、ハッシュの出力が 4 バイトなら $(T_0 \parallel T_1 \parallel T_2 \parallel T_3) = M$
 - iii. (7.c.ii で得られた)これらのバイトを個々に modulo 2^8 addition 演算をしてキーファイルプールの(プールの古い値の上書きではなく)プールカーソルの位置に書き込む。バイトが書き込まれたらプールカーソルは 1 バイト進む。カーソルがプールの終端までくると、位置はプールの先頭に設定される。
8. キーファイルプールの内容を以下の方法でパスワード P に適用する。
 - a. パスワード P を個々のバイト $B_0 \dots B_{pl}$ に分割する。
 - b. キーファイルプール KP を個々のバイト $G_0 \dots G_{kpl}$ に分割する。
 - c. For $0 \leq i \leq kpl$ の条件で順に実行 $B_i = B_i \oplus G_i$
 - d. $P = B_0 \parallel B_1 \parallel \dots \parallel B_{pl-1} \parallel B_{pl}$
9. パスワード P は(キーファイルプールの内容が適用されたあと)ヘッダーキー導出関数 PBKDF2 (PKCS #5 v2)へ渡され、それがユーザーが選択した安全なハッシュアルゴリズム (RIPEMD-160 か Whirlpool)の暗号を使って(ソルトや他のデータとともに)処理します。詳細

はヘッダーキーの導出、ソルト、および反復回数を参照してください。

関数 H の役割はたんに拡散が目的です[26]。CRC-32 はハッシュ関数 H で使われます。CRC-32 の出力はつづけて安全なハッシュアルゴリズムの暗号で処理されます。キーファイルプールの内容は(CRC-32 でハッシュされたのに加え)、パスワードに適用されます。それがヘッダーキー導出関数 PBKDF2 (PKCS #5 v2)へ渡され、それがユーザーが選択した安全なハッシュアルゴリズム(たとえば、RIPEMD-160 か Whirlpool)の暗号を使って(ソルトや他のデータとともに)処理します。結果として得られる値がヘッダーキーと第二ヘッダーキー(XTS モード)として使われます。

TrueCrypt ボリュームフォーマット仕様

Offset (bytes)	Size (bytes)	Encryption Status ¹	Description
0	64	Unencrypted ³	ソルト
64	4	Encrypted	アスキー文字列 “TRUE”
68	2	Encrypted	ボリュームヘッダーフォーマットバージョン
70	2	Encrypted	ボリュームを開くプログラムの最小バージョン
72	4	Encrypted	(復号された) 256-511 バイトの CRC-32 チェックサム
76	16	Encrypted	予約(0 をセット)
92	8	Encrypted	隠しボリュームのサイズ(通常ボリュームなら 0 をセット)
100	8	Encrypted	ボリュームのサイズ
108	8	Encrypted	マスターキーの開始位置オフセット
116	8	Encrypted	マスターキー内の暗号化領域サイズ
124	4	Encrypted	フラグビット (bit 0 set: システム暗号化; bits 1-31 は予約)
128	124	Encrypted	予約(0 をセット)
252	4	Encrypted	(復号された)64-251 バイトの CRC-32 チェックサム
256	Var.	Encrypted	連結された第一、第二マスターキー ⁴
512	65024	Encrypted	予約 (システム暗号化ではこの項目は除外 6)
65536	65536	Encrypted / Unencrypted ³	隠しボリュームヘッダー領域(このボリュームに隠しボ リュームがなければ、この領域はランダムデータ ⁵)。 シ ステム暗号化ではこの項目は除外 ⁶ 。 0-65535 バイトを参 照
131072	Var.	Encrypted	(マスターキーのスコープによる)データ領域。システム 暗号化では(システムパーティションのオフセットによっ て)オフセットは異なる。
S-131072 ²	65536	Encrypted / Unencrypted ³	バックアップヘッダー(異なるソルトから導出された異な るヘッダーキーによって暗号化)。システム暗号化ではこ の項目は除外 ⁶ 。 0-65535 バイトを参照
S-65536	65536	Encrypted / Unencrypted ³	隠しボリュームのバックアップヘッダー(異なるソルトか ら導出された異なるヘッダーキーによって暗号化)。 こ のボリュームに隠しボリュームがなければ、この領域は

¹ボリュームの暗号化領域はヘッダーキー(および XTS モードでは第二ヘッダーキー)で暗号化されます。詳細は暗号化の仕組みとヘッダーキーの導出、ソルト、および反復回数を参照してください。

² S はボリュームのサイズ(バイト)を意味します。

³ ソルトは秘密にする必要がないため[7]暗号化されていません。(ソルトは一連のランダムな値です)

⁴ ボリュームがカスケード方式で暗号化された場合には複数のマスターキー(XTS モードでは第二マスターキーも)が連結されてここに保管されます。

⁵ ボリューム作成時にランダム値で空き領域を埋める方法についてはこの節に記載しています。

⁶ ここでは「システム暗号化」という意味は、隠し OS を含む隠しボリュームを含んでいません。

			ランダムデータ 5 システム暗号化ではこの項目は除外 6 。
--	--	--	-----------------------------------

ファイル型ボリュームのフォーマットはパーティション/デバイス型ボリュームと同じです。(しかし、システムパーティション/ドライブのボリュームヘッダーやキータはドライブの最初の論理トラックの最後の 512 バイトに保管されます) TrueCrypt ボリュームには署名や ID 文字列のようなものはありません。復号されるまでは、すべてがランダムなデータにしか見えません。したがって、TrueCrypt コンテナやパーティションであるかどうかを判断することはできません。

それぞれの TrueCrypt ボリュームの空き領域はボリュームが作られるときにランダム値で埋められます。ランダム値は以下のように生成されます: TrueCrypt ボリュームのフォーマットが始まる直前に臨時の暗号化キーと臨時の第二キー(XTS モード)が組み込みの乱数発生機構(乱数発生機構参照)で生成されます。ユーザーが選んだ暗号化アルゴリズムは臨時キーで初期化されます。つづいて暗号化アルゴリズムは、組み込みの乱数発生機構で生成されたプレーンテキストを暗号化します。暗号化アルゴリズムは XTS モードで動きます。(動作モード参照) それが作り出した暗号テキストブロックがボリュームの空き領域を埋める(上書きする)のに使われます。キーは RAM 中に保管され、フォーマットが終了すると安全に廃棄されます。ボリューム作成中にはバイト #0(ソルト)および #256(マスターキー)に置かれるフィールドには乱数発生機構(乱数発生機構参照)で生成されたランダム値があります。

TrueCrypt ボリュームの空き領域に隠しボリュームがある場合には、隠しボリュームのヘッダーはホストボリュームの #65536 にあります。(ホスト/外殻ボリュームのヘッダーはホストボリュームのバイト #0 先頭にあります - 隠しボリューム参照) TrueCrypt ボリュームに隠しボリュームがない場合には、ボリュームの 65536-131071 バイト(つまり隠しボリュームのヘッダーが格納されるはずの領域)はランダムデータ(ボリューム作成時に空き領域をランダムデータで埋める方法についての上記の記載を参照)隠しボリュームのヘッダーのレイアウトは標準ボリュームのものと同一(0-65535 バイト)です。

TrueCrypt がサポートする最大ボリュームサイズは 8,589,934,592 GB (2^{63} bytes)です。しかし、安全上の理由(128 ビットブロックサイズと動作モードの観点から)、許容される最大サイズは 1 PB (1,048,576 GB)です。

付加されたバックアップヘッダー

TrueCrypt 6.0 以降で作成された TrueCrypt ボリュームはボリュームの最後に位置する(上記参照)付加された組み込みのバックアップヘッダーを持ちます。ヘッダーバックアップはボリュームヘッダーのコピーではなく、異なったソルトから導出された異なったヘッダーキーで暗号化されます。(ヘッダーキーの導出、ソルト、および反復回数を参照)

ヘッダーバックアップについての詳細は、メインプログラムウィンドウのツール -> ボリュームヘッダーのリストアを参照してください。

準拠規格

TrueCrypt は以下の規格、仕様、勧告に準拠しています：

- PKCS #5 v2.0 [7]
- PKCS #11 v2.20 [23]
- FIPS 197 [3]
- FIPS 198 [22]
- FIPS 180-2 [14]
- ISO/IEC 10118-3:2004 [21]

実装された暗号化アルゴリズムの正確さは、テストベクターを使う(ツール->テストベクターを選択)か TrueCrypt のソースコードを調べることで検証できます。

ソースコード

TrueCrypt はオープンソースのフリーソフトウェアです。TrueCrypt の完全なソースコード(C、C++ およびアセンブラで書かれています)はみなさんのレビューのため次のところで自由に入手できます:

<http://www.truecrypt.org/>

今後の開発予定

将来の計画に含まれている機能については以下を参照してください:

<http://www.truecrypt.org/future.php>

ライセンス

TrueCrypt の公開についてのライセンスは TrueCrypt バイナリあるいはソースコードの配布パッケージに含まれる `Licence.txt` に記載されています。また、次のところでも入手できます:

<http://www.truecrypt.org/legal/license>

連絡先

われわれへの連絡方法については、次のところを参照してください:

<http://www.truecrypt.org/contact>

バージョン履歴

6.1a

2008 年 12 月 1 日

改善、バグ修正および安全性強化:

- 細かい改善、バグ修正および安全性強化 (Windows, Mac OS, and Linux)

注意: TrueCrypt 旧バージョンを使っているならば、最新バージョンにアップグレードすることを強く推奨します。

6.1

2008 年 10 月 31 日

新機能:

- 既存データを失わずに非システムパーティションを暗号化できる。(Windows Vista/2008)

注意: 非システムパーティションをそのまま暗号化する場合は、「ボリュームの作成->非システムパーティションの暗号化->標準ボリューム->デバイスの選択->そのままでのパーティション暗号化」をクリックし、ウィザードの指示にしたがってください。Windows XP/2000/2003 ではファイルシステムの縮小がサポートされていないために、この機能はサポートされていないことに注意してください。(ボリュームヘッダーとバックアップヘッダーの場所を作るために、ファイルシステムを縮小する必要があります)

- セキュリティトークンとスマートカードのサポート(詳細はキーファイルのセキュリティトークンとスマートカードを参照)
- TrueCrypt ブートローダーがメッセージを表示しないようにできる(「設定->システム暗号化」を選択し、起動前認証で何も表示しない」を有効にしてください)
- TrueCrypt ブートローダーに任意のメッセージを表示させることができる。(「設定->システム暗号化」を選択し、該当する入力欄にメッセージを入力してください)メッセージなしにすることもできる。そうでなければ、TrueCrypt ブートローダーの標準メッセージになる。
- 起動前認証のパスワードをドライバのメモリーに記憶しておくことができ、これを TrueCrypt 非システムボリュームのマウント時に利用できる。(「設定->システム暗号化」を選択し、「起動前認証のパスワードを記憶する」を有効にしてください)
- Linux および Mac OS 用: TrueCrypt で暗号化された Windows のシステムパーティションおよび Windows の TrueCrypt で全体を暗号化されたドライブにあるパーティションをマウントする機能。

機能改善:

- 特定の BIOS のバグによる、TrueCrypt ブートローダーが正しく機能することを妨害するメモリー破損時の対策。(Windows Vista/XP/2008/2003)

- 隠し OS 作成過程で、隠し OS 作成後に TrueCrypt は元の OS があったパーティションの全内容を安全に消去する。ユーザーはパーティションに新しいシステムをインストールし、TrueCrypt で暗号化するよう要求はされない。(隠システムはこのようにして作成される)

注意: TrueCrypt の前バージョンでは隠システムに関する安全性の問題には気づいていなかったが、未発見の問題点があっても防止できるように、この機能を導入した。そうしなければ将来的には、元のファイルシステム(隠し OS の複製元)があるパーティションに保存される Windows が作成するログファイルを調査することによって、TrueCrypt ウィザードが隠システム作成モードで使用されたこと(つまり、このコンピュータに隠し OS があることを示す)に気づかれてしまう脆弱性が発見されるかもしれなかった。さらに、この変更によって、隠し OS 作成時にページングファイル機能やハイバネーションを無効にしておく必要がなくなった。

- その他の細かい改善 (Windows, Mac OS X, and Linux)

バグ修正:

- その他の小さいバグ修正と安全性の改善 (Windows, Mac OS X, and Linux)

旧バージョンでの変更履歴は <http://www.truecrypt.org/docs/?s=version-history> を参照してください。

謝辞

私たちは以下のみなさんに感謝します:

Paul Le Roux は彼の E4M ソースコードを入手できるようにしてくれました; TrueCrypt のいくつかの部分は E4M から派生したものです。

Dr. Brian Gladman, 彼はすばらしい AES, Twofish, SHA-512 そして多様な有限体 $GF(2^{128})$ ルーチンを書いてくれました。

Peter Gutmann, 彼の乱数についての論文と、TrueCrypt の乱数発生機構の一部のソースである cryptlib を作ってくれたことに。

Wei Dai は Serpent ルーチンを書いてくれました。 *Dag Arne Osvik* には「*Serpent* の高速化」論文について。

Markus Friedl は RIPEMD-160 ルーチン (OpenBSD より) を書いてくれました。

mark Adler と共作者はインフレートルーチンを書いて九列した。

暗号化とハッシュ・アルゴリズムの設計者のみなさん:

Horst Feistel, Don Coppersmith, Walt Tuchmann, Lars Knudsen, Ross Anderson, Eli Biham, Bruce Schneier, David Wagner, John Kelsey, Niels Ferguson, Doug Whiting, Chris Hall, Joan Daemen, Vincent Rijmen, Carlisle Adams, Stafford Tavares, Phillip Rogaway, Hans Dobbertin, Antoon Bosselaers, Bart Preneel, Paulo S. L. M. Barreto.

このプロジェクトを可能にしてくれたみなさん、精神的に支援してくれたみなさん、バグレポートや改善提案を送ってくれたみなさん

ありがとうございました。

参考文献

- [1] U.S. Committee on National Security Systems (CNSS), *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*, CNSS Policy No. 15, Fact Sheet No. 1, June 2003, available at http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf and also at <http://csrc.nist.gov/cryptval/CNSS15FS.pdf>.
- [2] C. E. Shannon, *Communication Theory of Secrecy Systems*, Bell System Technical Journal, v. 28, n. 4, 1949
- [3] NIST, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001, available at <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.
- [4] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti, E. Roback, NIST, *Report on the Development of the Advanced Encryption Standard (AES)*, October 2, 2000, available at <http://csrc.nist.gov/CryptoToolkit/aes/round2/r2report.pdf>.
- [5] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, *The Twofish Team's Final Comments on AES Selection*, May 15, 2000, available at <http://csrc.nist.gov/CryptoToolkit/aes/round2/comments/20000515-bschneier.pdf>.
- [6] M. Bellare, *New Proofs for NMAC and HMAC: Security without Collision-Resistance*, Cryptology ePrint Archive: Report 2006/043, February 6, 2006, available at <http://eprint.iacr.org/2006/043>
- [7] RSA Laboratories, *PKCS #5 v2.0: Password-Based Cryptography Standard*, RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS), March 25, 1999, available at <ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2-0.pdf> and also courtesy of RSA Laboratories at: <http://www.truecrypt.org/docs/pkcs5v2-0.pdf>
- [8] H. Krawczyk, M. Bellare, R. Canetti, *HMAC: Keyed-Hashing for Message Authentication*, Request for Comments 2104, February 1997, available at <http://www.ietf.org/rfc/rfc2104.txt>.
- [9] P. Cheng, IBM, R. Glenn, NIST, *Test Cases for HMAC-MD5 and HMAC-SHA-1*, Request for Comments 2202, February 1997, available at <http://www.ietf.org/rfc/rfc2202.txt>.
- [10] Peter Gutmann, *Software Generation of Practically Strong Random Numbers*, presented at the 1998 Usenix Security Symposium, available at <http://www.cs.auckland.ac.nz/~pgut001/pubs/usenix98.pdf>.
- [11] Carl Ellison, *Cryptographic Random Numbers*, originally an appendix to the P1363 standard, available at <http://world.std.com/~cme/P1363/ranno.html>.

- [12] M. Liskov, R. Rivest, D. Wagner, *Tweakable Block Ciphers*, Advances in Cryptology – CRYPTO '02, vol. 2442 of Lecture Notes in Computer Science, pp. 31-46. Springer-Verlag, 2002; also available at:
<http://theory.lcs.mit.edu/~rivest/LiskovRivestWagner-TweakableBlockCiphers.pdf>
- [13] J. Kelsey, *Twofish Technical Report #7: Key Separation in Twofish*, AES Round 2 public comment, April 7, 2000
- [14] NIST, *Secure Hash Standard*, August 1, 2002, available at
<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.
- [15] U. Maurer, J. Massey, *Cascade Ciphers: The Importance of Being First*, Journal of Cryptology, v. 6, n. 1, 1993
- [16] Bruce Schneier, *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996.
- [17] Peter Gutmann, *Secure Deletion of Data from Magnetic and Solid-State Memory*, first published in the Sixth USENIX Security Symposium Proceedings, San Jose, California, July 22-25, 1996, available at http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
- [18] Serpent home page: <http://www.cl.cam.ac.uk/~rja14/serpent.html>.
- [19] M. E. Smid, *AES Issues*, AES Round 2 Comments, May 22, 2000, available at
<http://csrc.nist.gov/CryptoToolkit/aes/round2/comments/20000523-msmid-2.pdf>.
- [20] A. Menezes, P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996
- [21] International Organization for Standardization (ISO), *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*, ISO/IEC 10118-3:2004, February 24, 2004
- [22] NIST, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198, March 6, 2002, available at
<http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf>.
- [23] RSA Laboratories, *PKCS #11 v2.20: Cryptographic Token Interface Standard*, RSA Security, Inc. Public-Key Cryptography Standards (PKCS), June 28, 2004, available at
<http://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf>

この文書は TrueCrypt ディストリビューションの一部です。この文書を使う、印刷する、複製する、配布することが認められています。また、この文書を TrueCrypt Translator Agreement または TrueCrypt ライセンスにしたがって、修正、翻訳、再配布することができます。

Translated by: Takuto Niki