

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 5.1a. 2008年3月17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、あなたはバイナリと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責任と義務を同意したことになります。

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 © 1995-1997 Eric Young. All rights reserved.

Copyright © 2001 Markus Friedl. 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。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 は商標ではありますが、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.....	31
隠しボリューム.....	32
隠しボリュームを破損から守る.....	34
隠しボリューム区画づくりの前の安全策.....	37
システム暗号化.....	39
システム暗号化ができる OS.....	39
TrueCrypt レスキューディスク.....	40
TRUECRYPT ボリューム.....	43
新規 TRUECRYPT ボリュームの作成.....	43
ハッシュアルゴリズム.....	43
暗号化アルゴリズム.....	44
クイックフォーマット.....	45
ダイナミック.....	45
クラスタのサイズ.....	45
CD や DVD にある TrueCrypt ボリューム.....	46
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.....	46
ボリューム作成に関する追加情報.....	46
メインプログラムウィンドウ.....	48
ファイルの選択.....	48
デバイスの選択.....	48
マウント.....	48
デバイスの自動マウント.....	48
アンマウント.....	49
すべてアンマウント.....	49
記憶したパスワードの消去.....	49
履歴を保存しない.....	49
終了.....	49
ボリュームツール.....	51
プログラムメニュー.....	52
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.....	52
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.....	52

ボリューム -> お気に入りボリュームをマウント.....	52
ボリューム -> ヘッダーキー導出アルゴリズムの設定.....	52
ボリューム -> ボリュームのパスワードを変更する.....	53
システム-> パスワードの変更.....	53
システム -> ブート前認証なしでマウントする.....	54
ツール -> ボリューム履歴を消去.....	54
ツール -> トラベラーディスクセットアップ.....	54
ツール -> キーファイル生成.....	54
ツール -> ボリュームヘッダーのバックアップ.....	54
ツール -> ボリュームヘッダーのリストア.....	55
設定 -> 各種設定.....	55
TRUECRYPT ボリュームのマウント.....	58
パスワードをドライバのメモリーに記憶する.....	58
マウントオプション.....	58
ホットキー.....	60
キーファイル.....	60
キーファイルダイアログウィンドウ.....	62
キーファイル検索パス.....	62
空のパスワードとキーファイル.....	64
キーファイル -> ボリュームへのキーファイルの追加/削除.....	64
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.....	64
キーファイル -> ランダムキーファイルの生成.....	65
キーファイル -> デフォルトキーファイル/フォルダの設定.....	65
トラベラーモード.....	66
ツール -> トラベラーディスクのセットアップ.....	66
TRUECRYPT を管理者権限なしで使う	68
TRUECRYPT の常駐.....	68
言語パック	69
インストール	69
暗号化アルゴリズム.....	70
AES.....	70
Serpent.....	71
Twofish.....	71
AES-Twofish.....	71
AES-Twofish-Serpent.....	71
Serpent-AES.....	72
Serpent-Twofish-AES.....	72
Twofish-Serpent.....	72

ハッシュアルゴリズム.....	73
Whirlpool.....	73
SHA-512.....	73
RIPEMD-160.....	73
動作対象 OS.....	74
コマンドラインの使い方.....	75
文法.....	78
使用例.....	78
ネットワーク間の共有.....	79
ボリュームとボリュームヘッダーのバックアップ.....	80
非システムボリューム.....	80
システムパーティション.....	81
一般的注意事項.....	82
安全のための予防策.....	83
ページングファイル.....	83
ハイバネーションモード.....	84
メモリダンプファイル.....	84
Windows レジストリ.....	85
マルチユーザー環境.....	85
RAM にある暗号化されていないデータ.....	85
パスワードとキーファイルの変更.....	86
データの破損.....	86
ウェアレベリング.....	87
デフラグ.....	87
ジャーナリングファイルシステム.....	88
問題が起こったら.....	89
非互換性.....	93
既知の問題と制限.....	94
よくある質問(FAQ)と答え.....	95
暗号化を解除するには.....	106
TRUECRYPT のアンインストール.....	107
TRUECRYPT システムファイルとアプリケーションデータ.....	107
技術解説.....	109
表記法.....	109
暗号化の仕組み.....	110

動作モード	111
ヘッダーキーの導出、ソルト、および反復回数	113
乱数発生機構	114
キーファイル	116
TRUECRYPT ボリュームフォーマット仕様	118
準拠規格	120
ソースコード	120
今後の開発予定	121
ライセンス	121
連絡先	121
バージョン履歴	122
謝辞	126
参考文献	127

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、データが読み出しちゃう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 は絶対に暗号化されたデータをディスクには置きません。臨時に 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

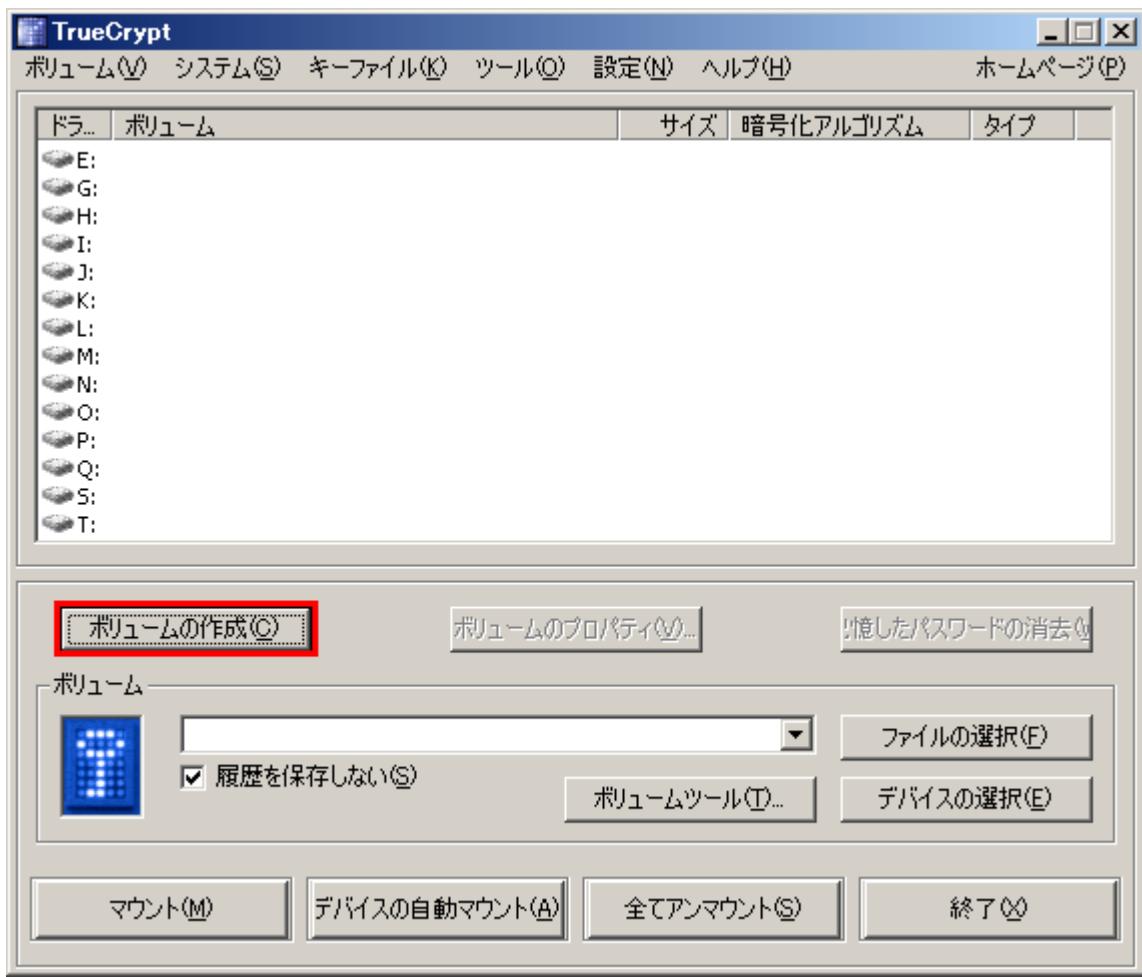
TrueCrypt コンテナの作り方と使い方

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:

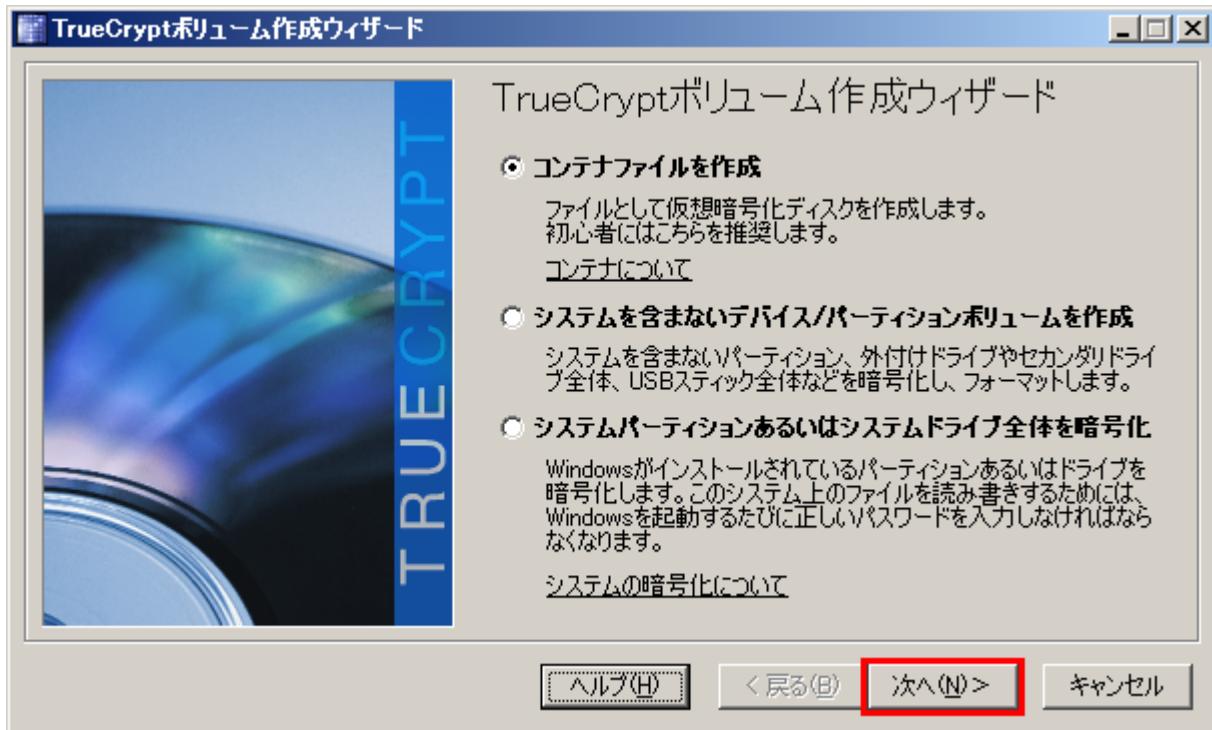
まず TrueCrypt をダウンロードし、インストールしてください。それから TrueCrypt.exe をダブルクリックするか Windows スタートメニューの TrueCrypt ショートカットをクリックして起動してください。

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:



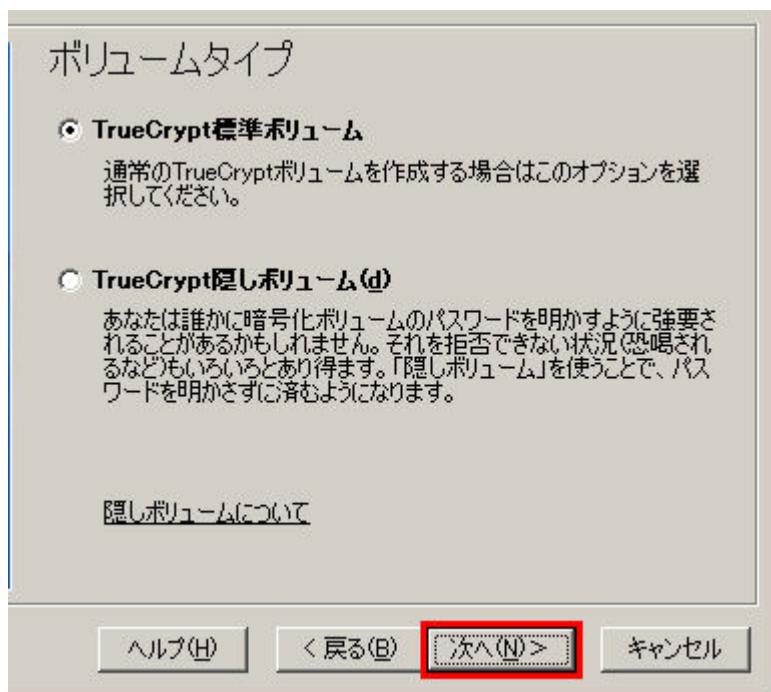
「TrueCrypt ボリューム作成ウィザード」 ウィンドウが表示されます。

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。

ウィザードウィンドウの説明を読んで、「次へ」をクリックしてください。

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。

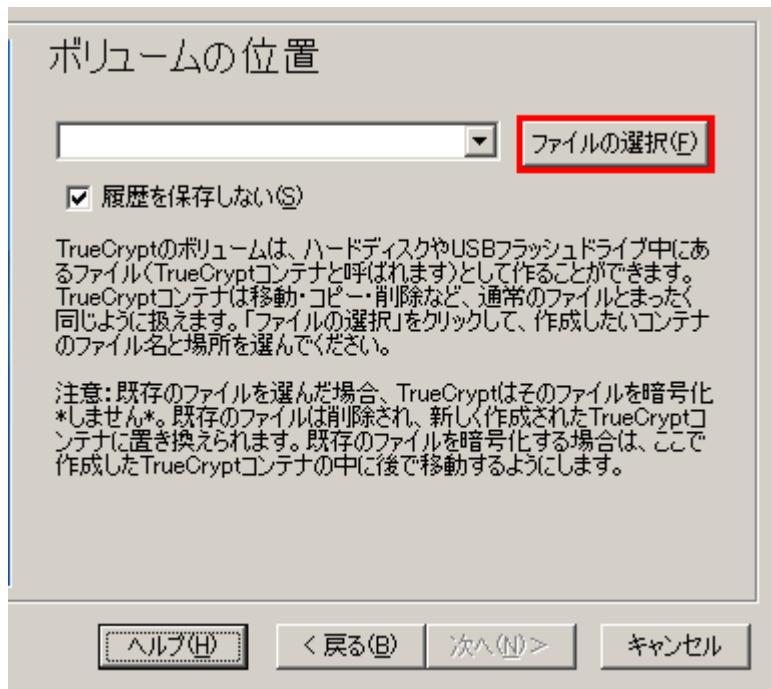
ステップ 4:



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。

そのオプションが初期状態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:



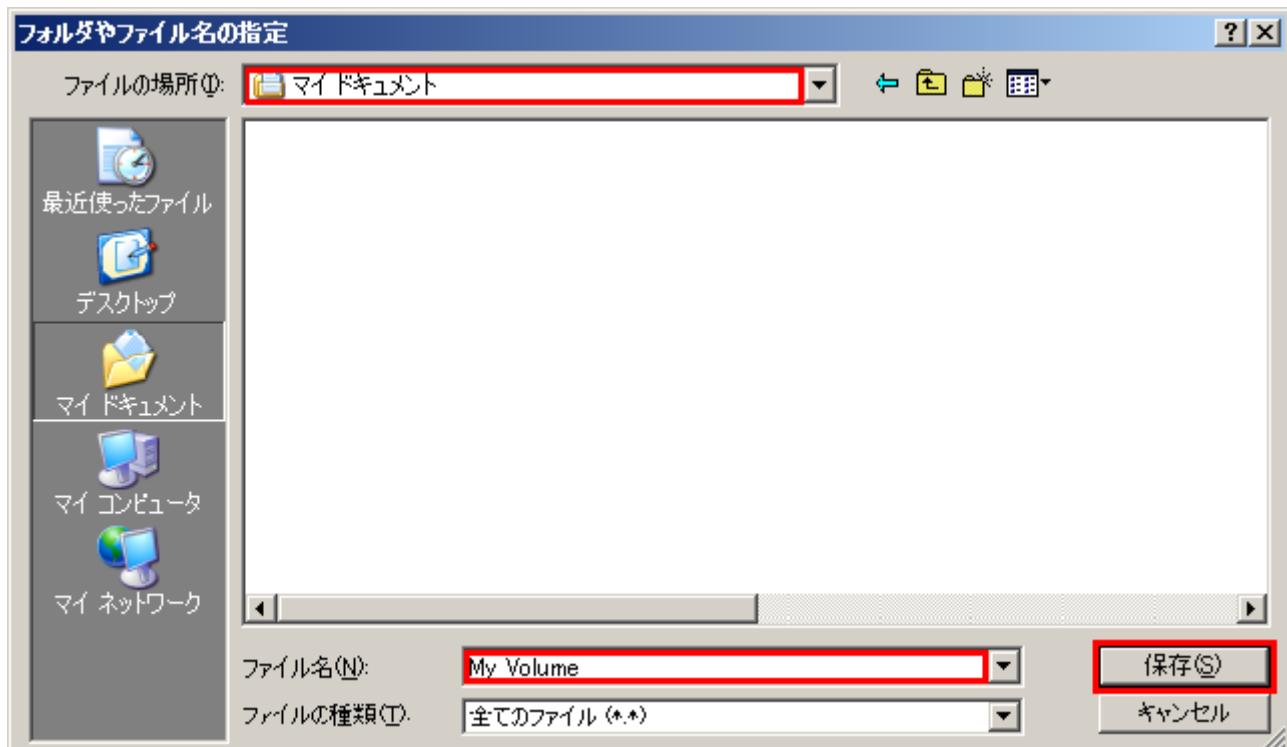
このステップでは、TrueCrypt ボリューム(ファイルコンテナ)をどこに作るのかを決めます。

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に) *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、

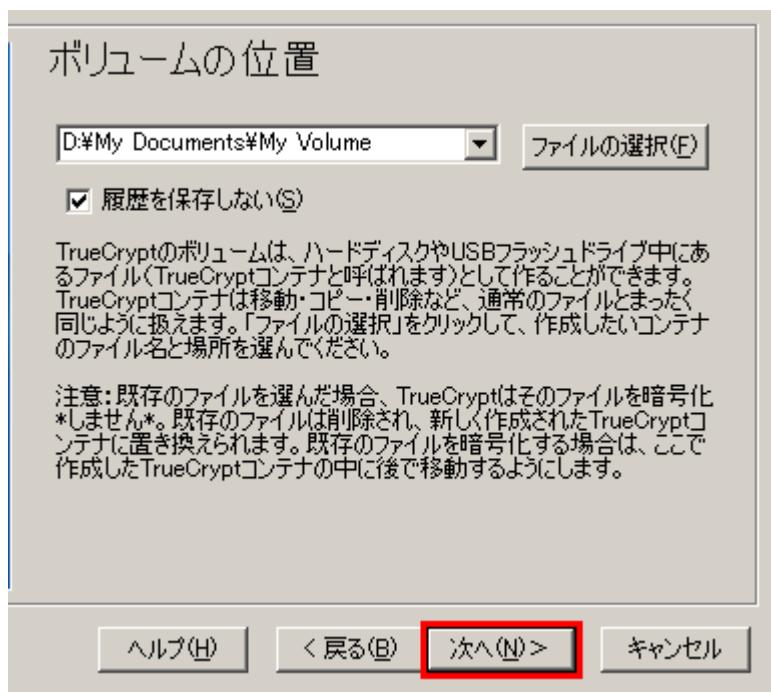
ダイアログの「保存」をクリックしてください。

ファイル選択ウィンドウは消えます。

¹**TrueCrypt** 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。

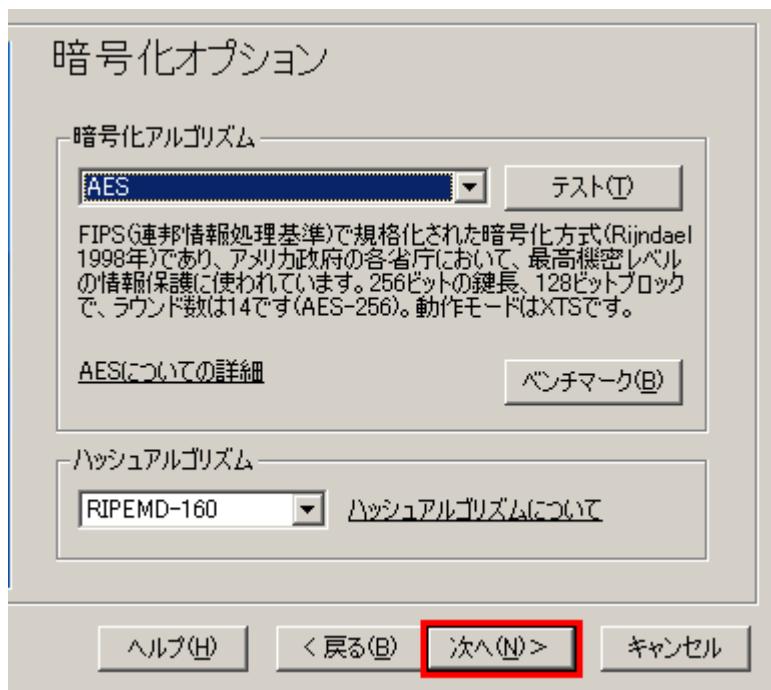
以降のステップでは「TrueCrypt ボリューム作成ウィザード」へ戻ります。

ステップ 7:



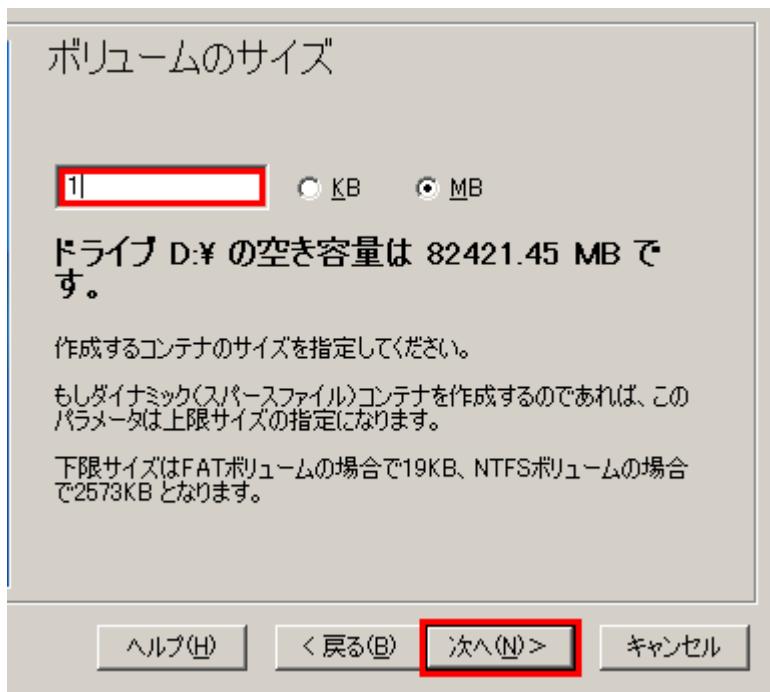
ボリューム作成ウィザードで「次へ」をクリックします。

STEP 8:



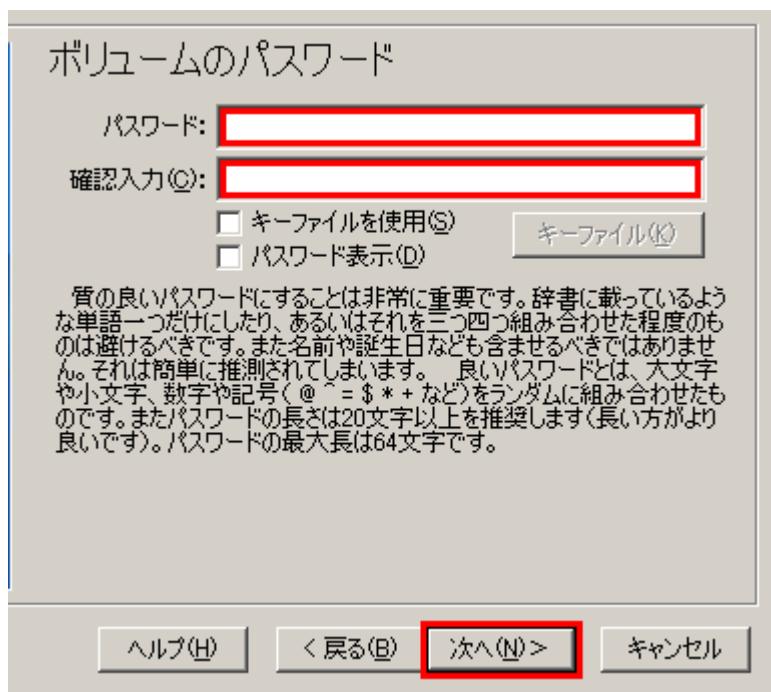
ここで暗号化アルゴリズムとハッシュアルゴリズムを選択します。どれを選べばいいかわからなければ、既定値のままで「次へ」をクリックしてください。(詳細は暗号化アルゴリズムとハッシュアルゴリズムの章を参照)

STEP 9:



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:



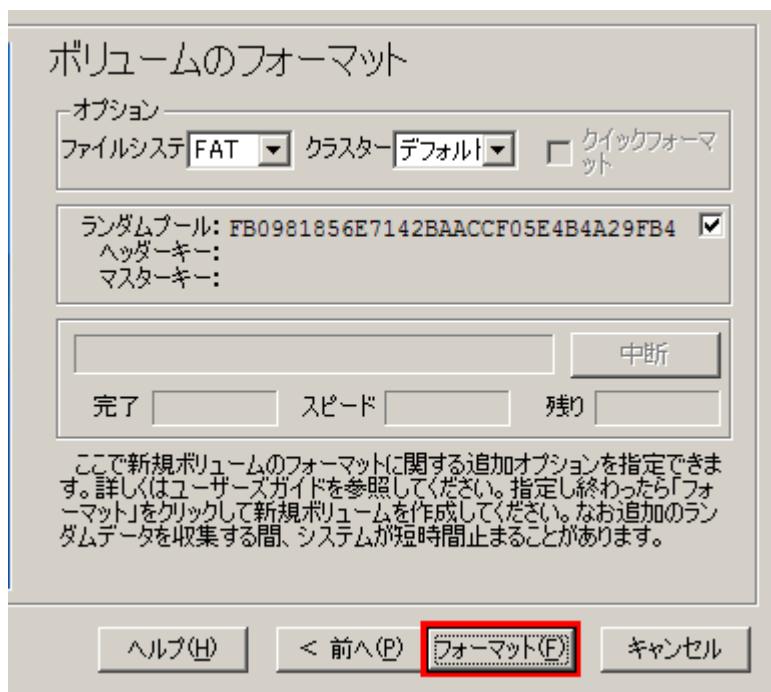
ここは重要なステップです。ここでボリュームの「良い」パスワードを決めなくてはいけません。

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す。

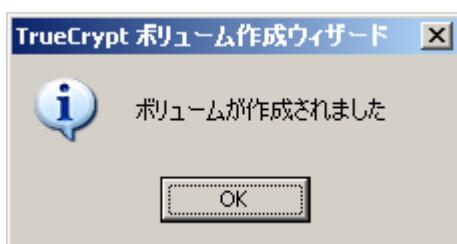
ステップ 11:



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。

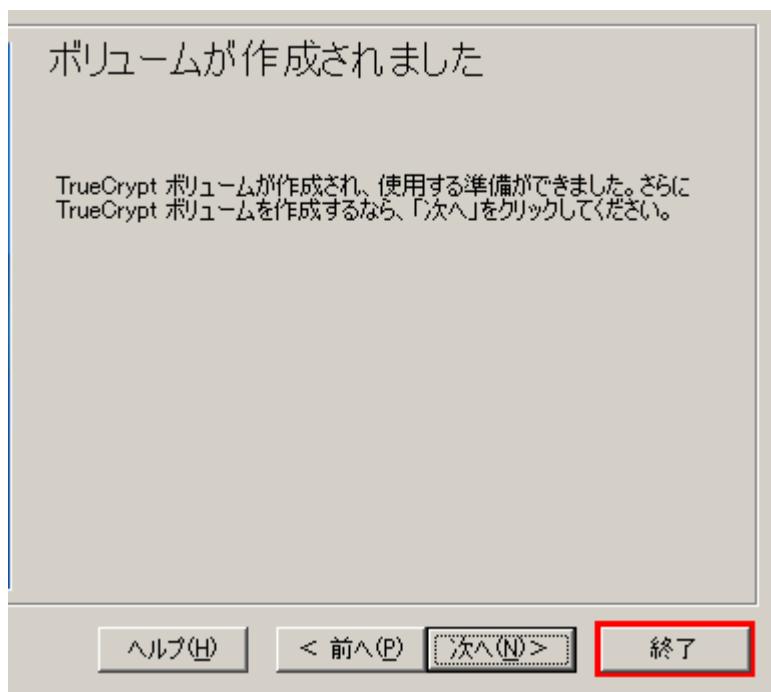
「フォーマット」をクリックしてください。

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:



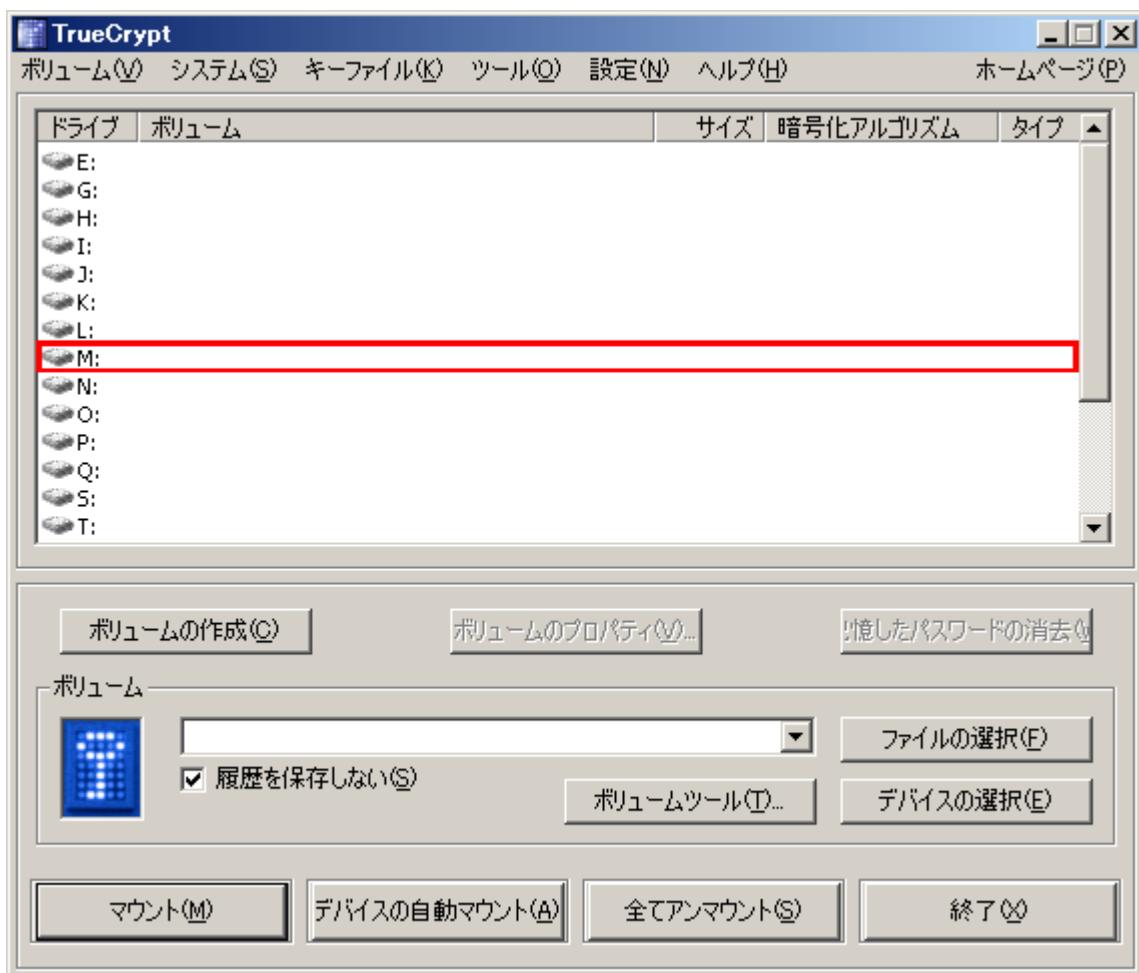
これで TrueCrypt ボリューム(ファイルコンテナ)の作成ができました。

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。

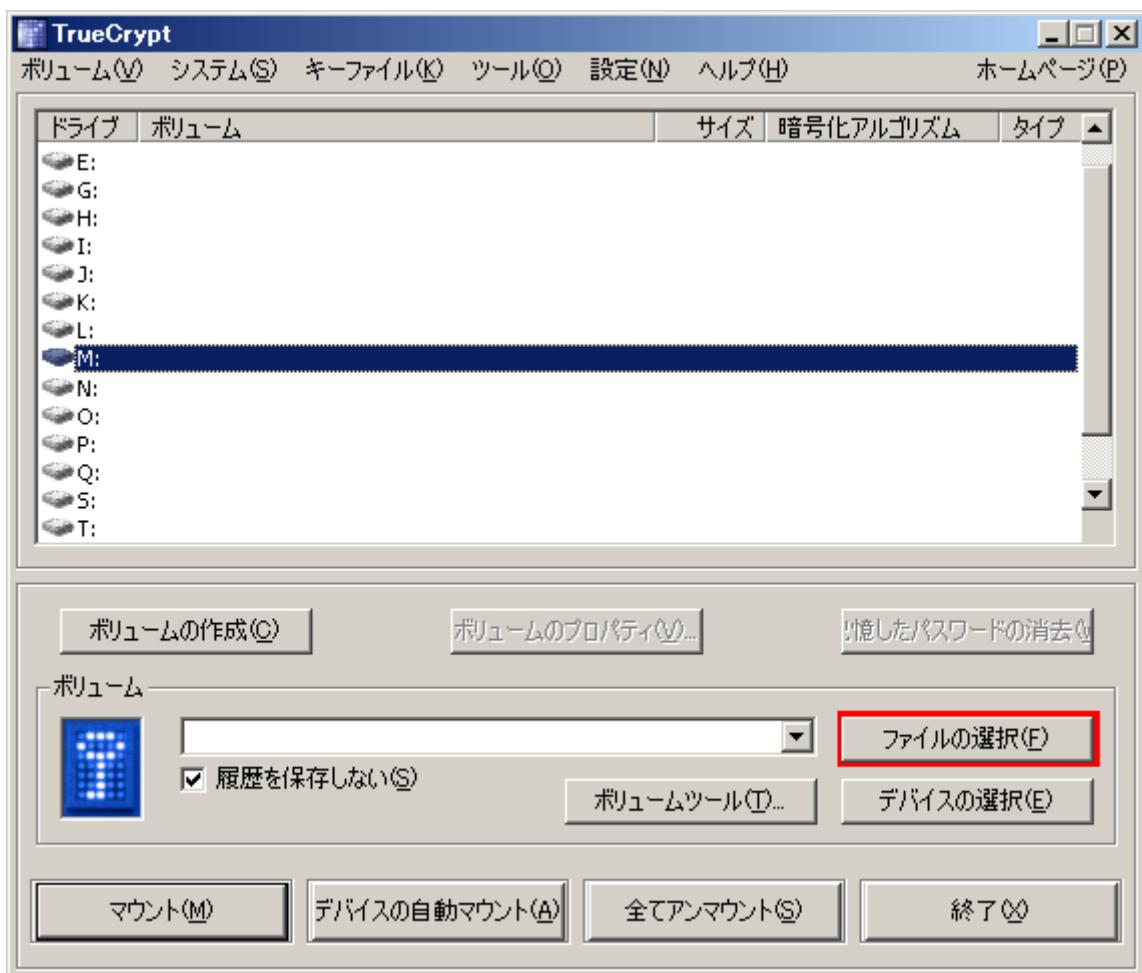
ステップ 13:



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。

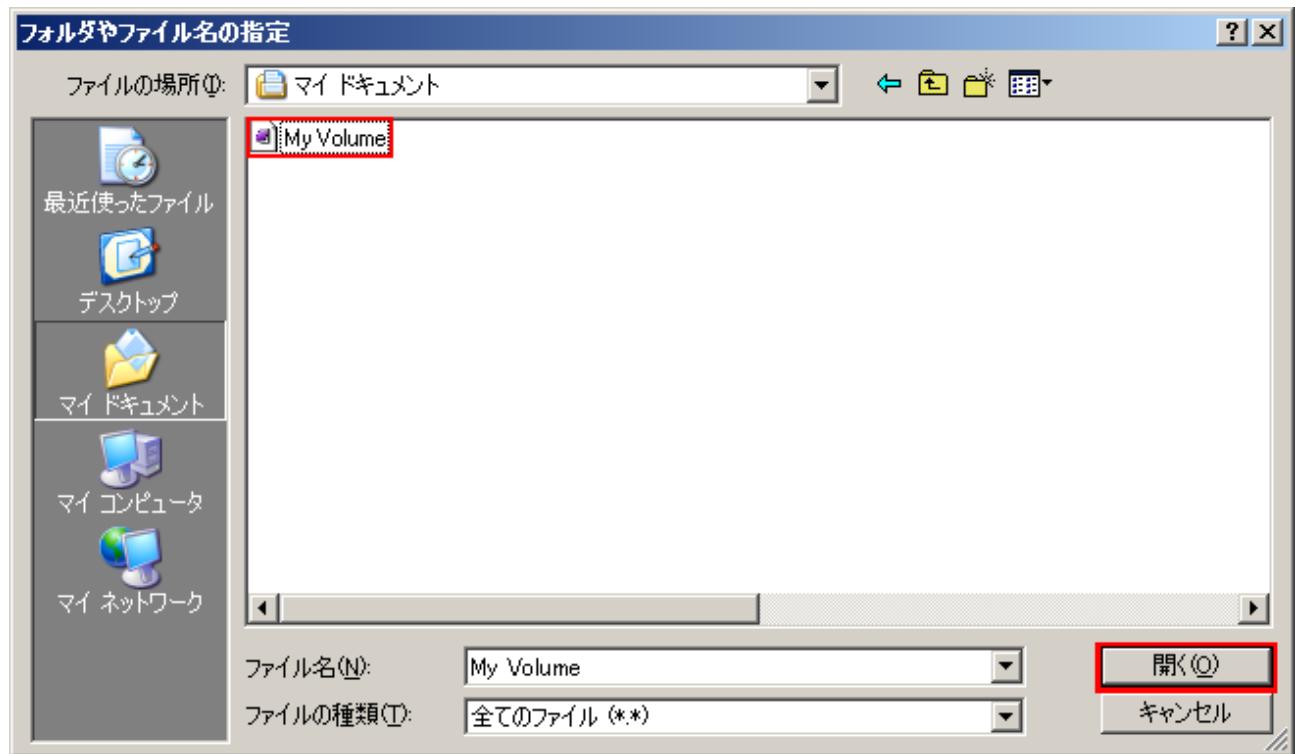
ステップ 14:



「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:



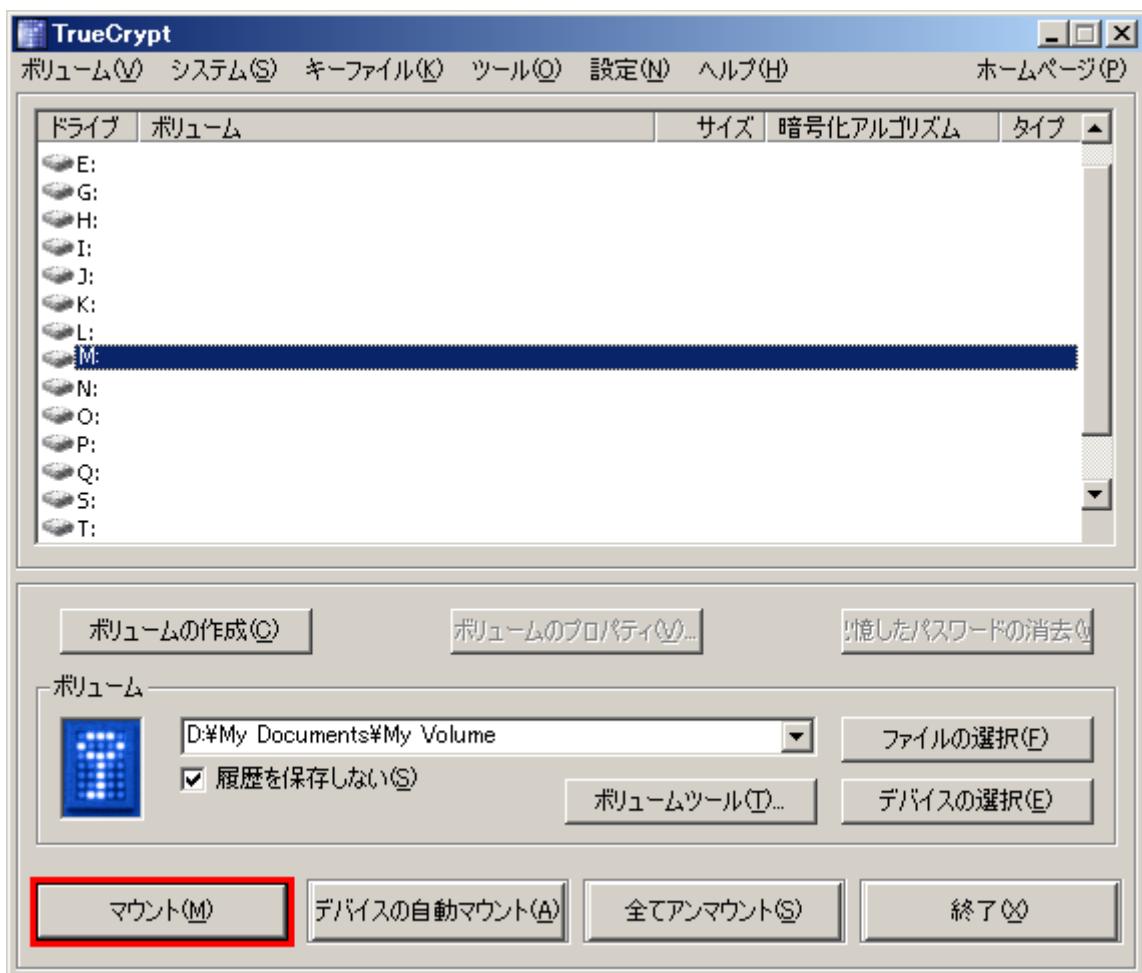
ファイル選択でコンテナファイル(ステップ 6-11 で作成したもの)を探し、それを選択してください。

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。

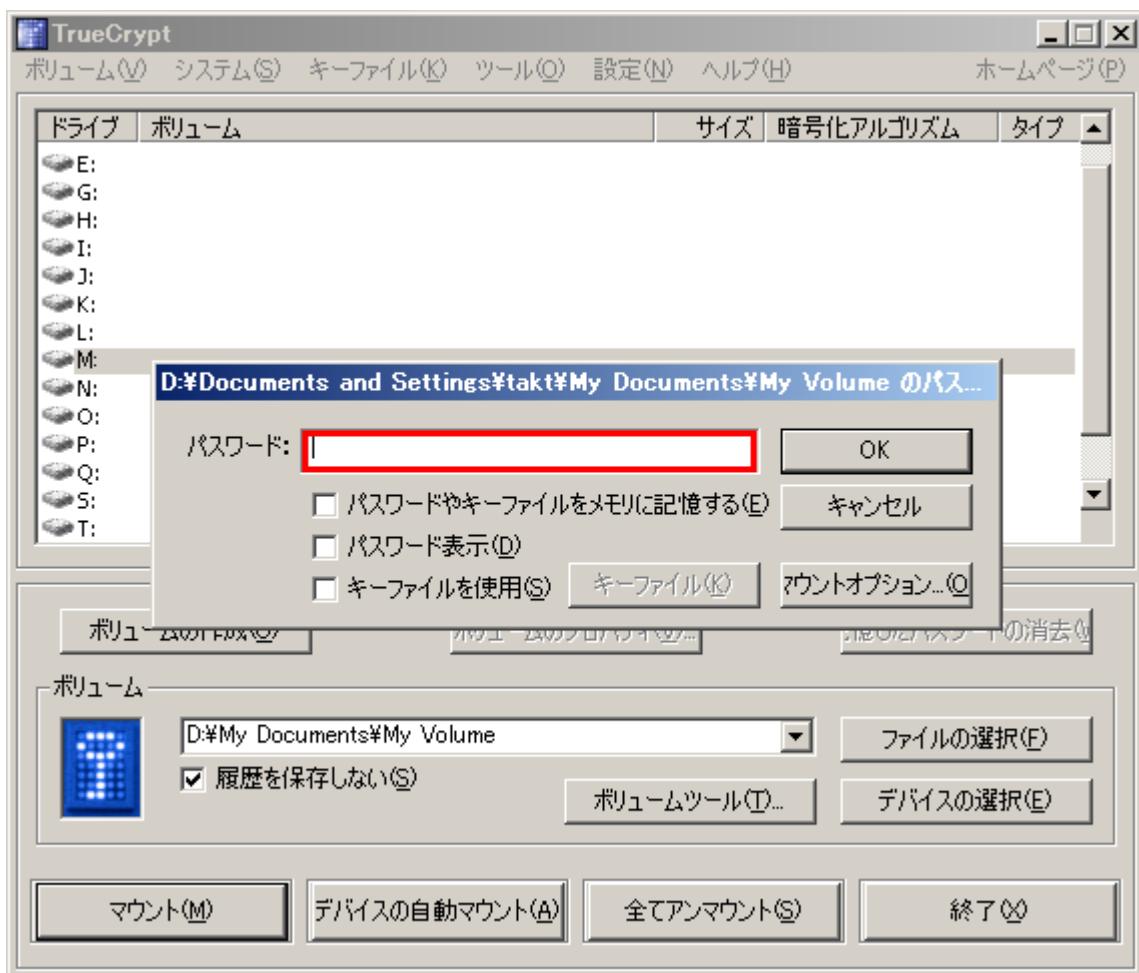
ステップ 16:



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。

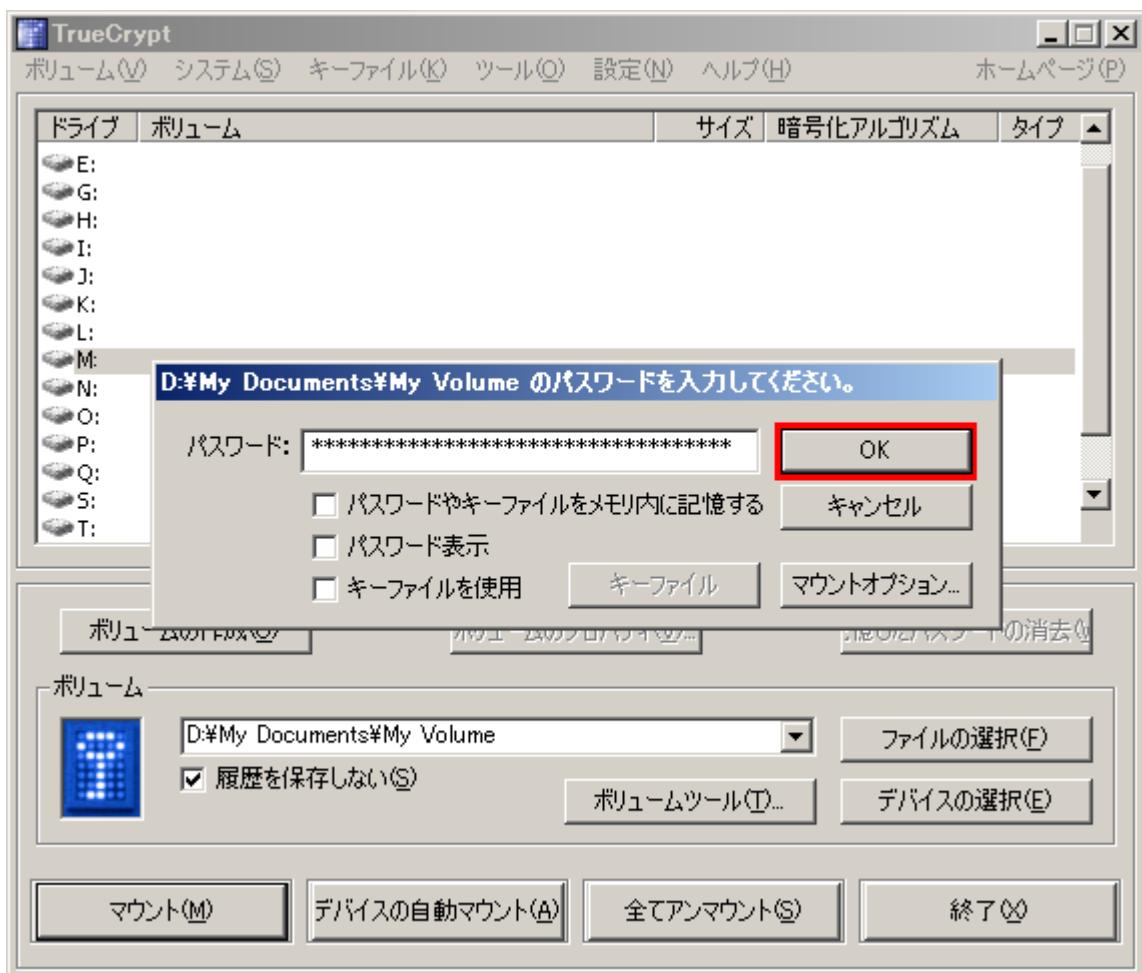
パスワード入力を求めるダイアログが表示されます。

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:

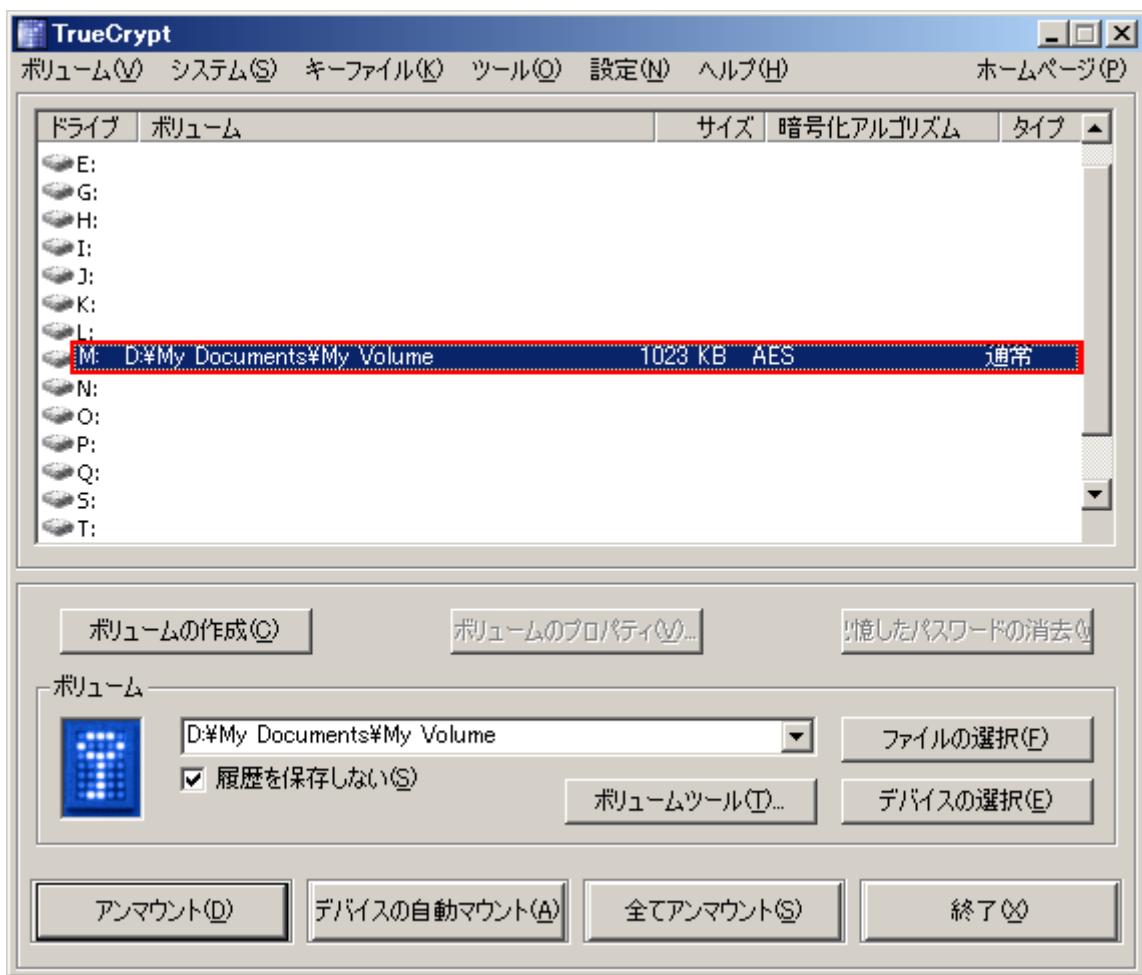


パスワード入力ウィンドウの「OK」をクリックしてください。

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。

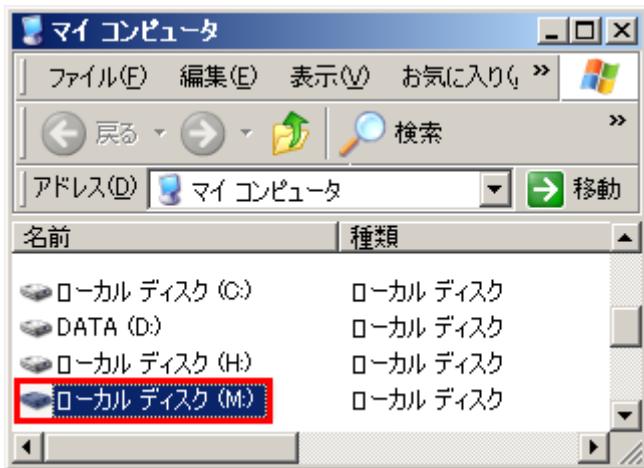
たとえばメディアプレーヤーで TrueCrypt ボリュームにあるファイルを開くと、ファイルは読み出し時に即時に RAM(メモリ)に復号されます。

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。



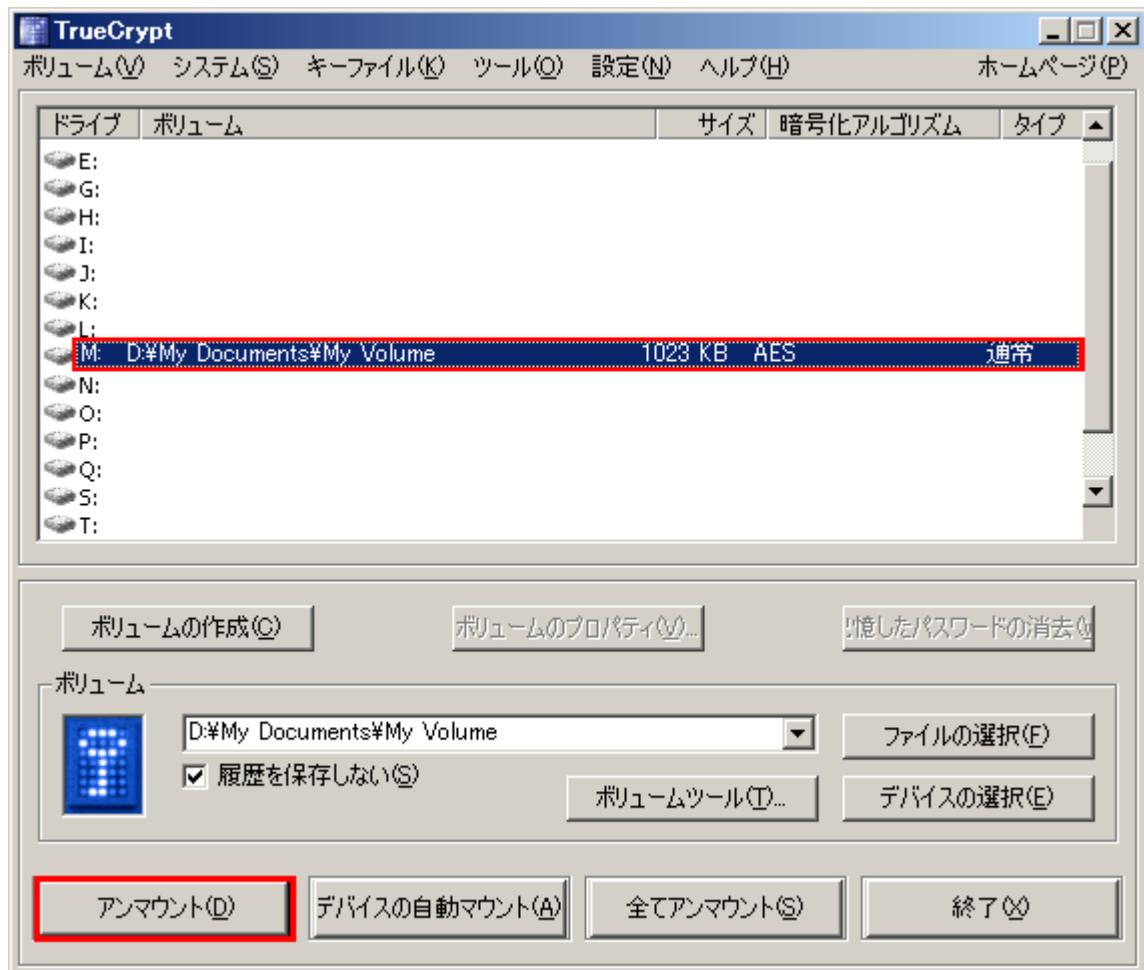
ファイルを TrueCrypt ボリュームから、あるいは TrueCrypt ボリュームへコピーするのはほかの通常のディスクに対するのと同じに実行できます。(たとえば、単純にドラッグ・アンド・ドロップもできます) 暗号化された TrueCrypt ボリュームから読み出したりコピーしたりされるファイルは、自動的に即時に(メモリ/RAM に)復号されます。

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。臨時に 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)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のステップ 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、すべての関連ステップで「ファイルの選択」ではなく「デバイスの選択」をクリックしてください。

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法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、ドライブの最初のシリンドー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つてしまします。(詳細はシステム暗号化の章を参照してください)

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 は拡張子を無視します。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)

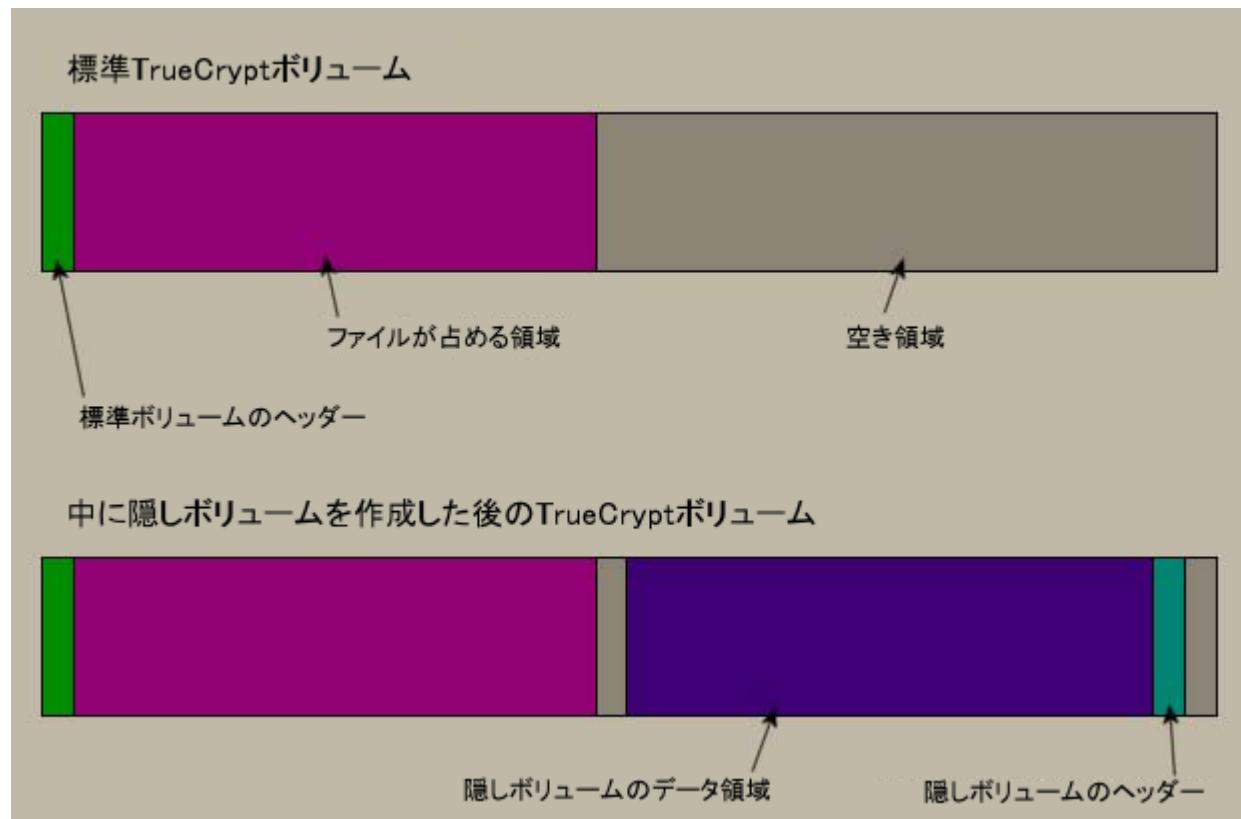
ハードディスクのパーティションを TrueCrypt ボリュームとしてフォーマットする場合でも、パーティションテーブル(パーティショントラックを含む)は変更されません。(TrueCrypt の署名や ID のようなものはパーティションテーブルには書き込まれません)

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などの場合でも、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。なぜなら、どの TrueCrypt ボリュームの空き領域も作成時¹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)を変更することもありません。

¹ 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。

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いけません。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ます。もし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セクター(ボリュームの終端からの第3セクター)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ます。隠しボリュームのヘッダーはそれとわかるようになつて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

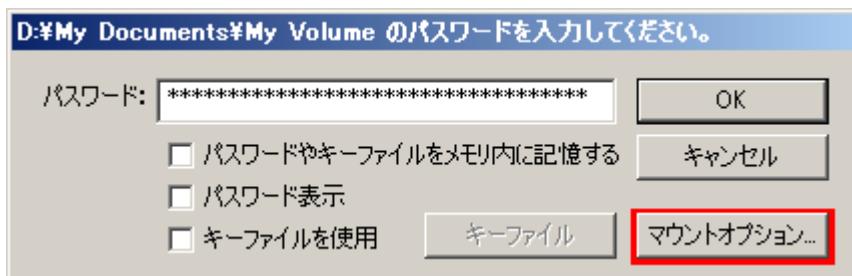
隠しボリュームを作成するのに何か問題があれば、問題が起こったらの章で解決策を探してください。

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。

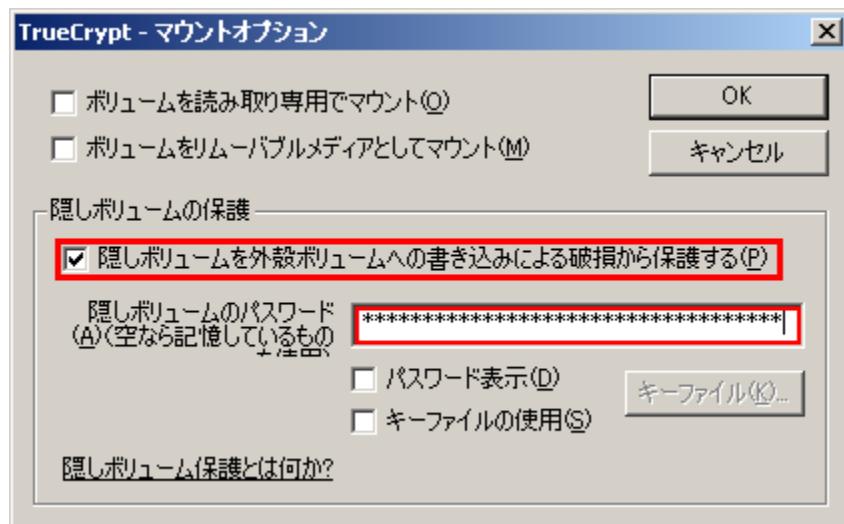
隠しボリュームを破損から守る

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と、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。

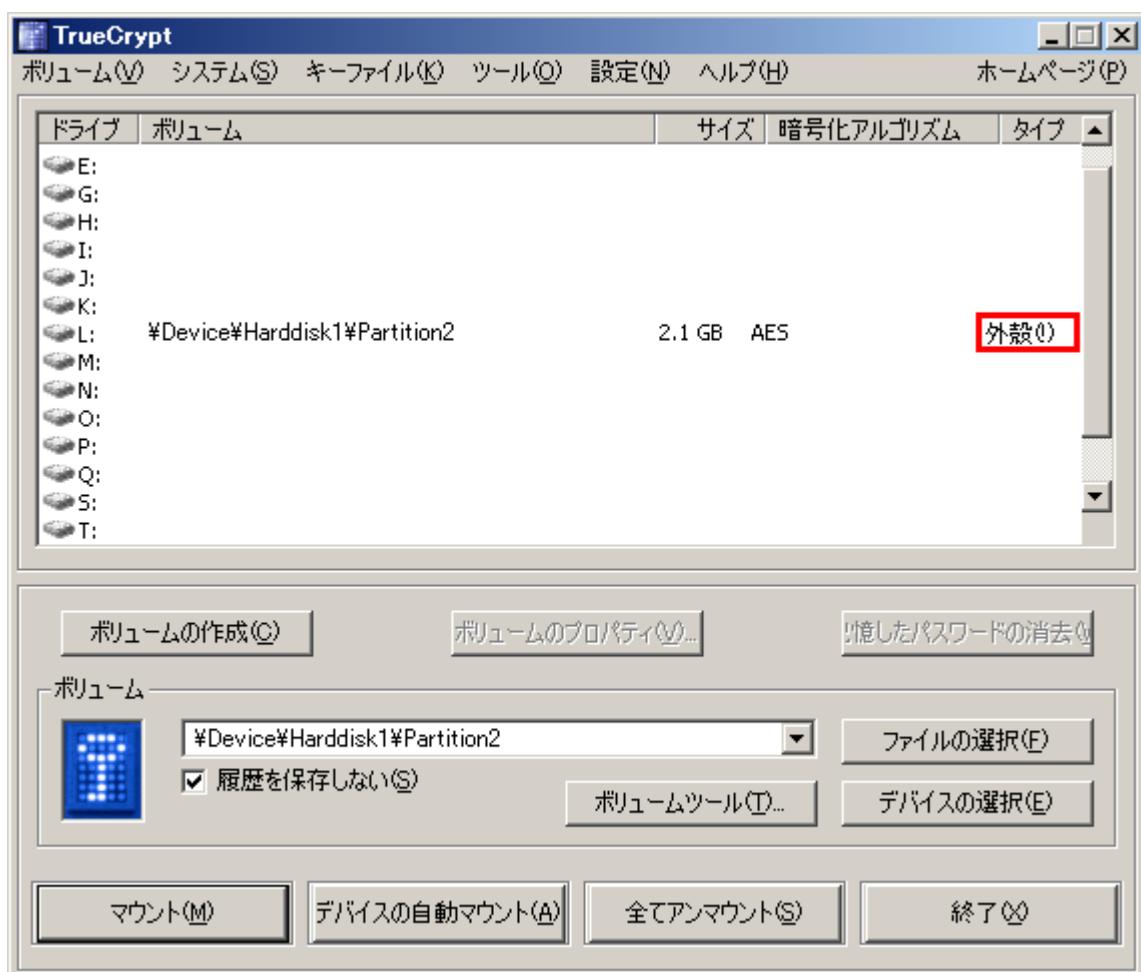


両方のパスワードが正しいものでなくてはいけません。そうでなければ、外殻ボリュームはマウントされません。隠しボリューム保護が有効な場合、TrueCrypt は隠しボリュームをマウントするのではなく(RAM にある)ヘッダーを復号し、隠しボリュームのサイズを(復号されたヘッダーから)得るだけです。そして、外殻ボリュームがマウントされ、(外殻ボリュームがアンマウントされるまで)隠しボリューム領域へのどんなデータ保存も拒否されます。TrueCrypt は外殻ボリュームのファイルシステム(クラスタ割り当て情報、空き領域情報など)をいっさい変更しません。ボリューム

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 ドライバー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という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。

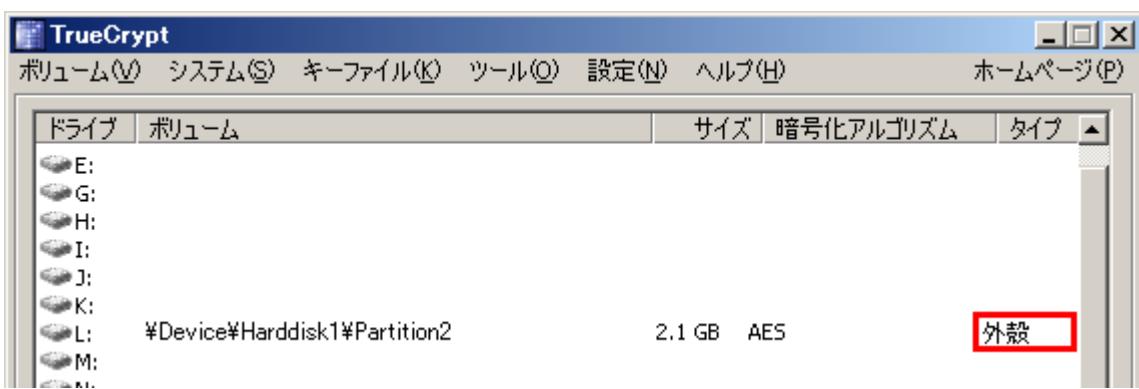


さらに、「ボリュームプロパティ」の「隠しボリューム保護」フィールドでは「はい(破損は防止されました!)」と表示されます。

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。

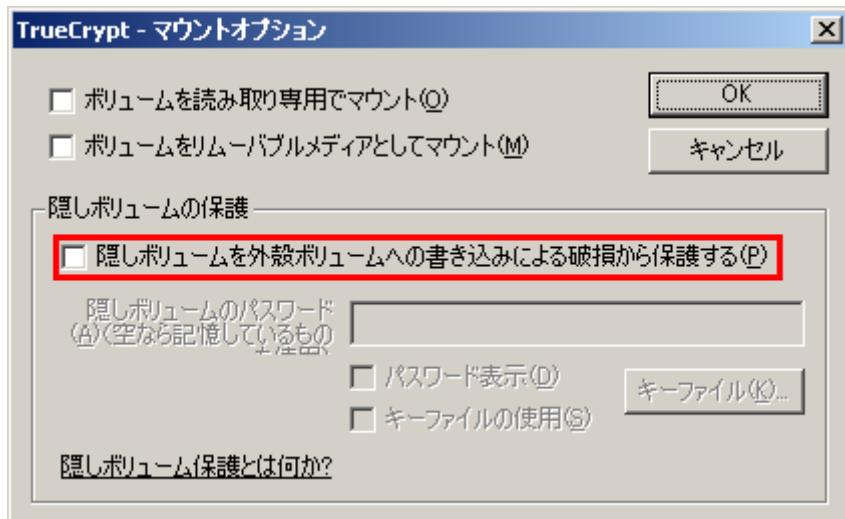
隠しボリュームが破損から保護されているかどうかを調べるには、いくつかの方法があります。

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ト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。



キヤッショ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)

隠しボリューム区画づくりの前の安全策

- 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暗号化された内容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。
- 隠しボリュームをつくろ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)

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。

システム暗号化はブート前認証をともないます。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。ブート前認証は、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)の最初のシリンドーにある 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は必要)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は必要)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。

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るべきです。(「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(複合する)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。

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。

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。:.:コンピューターに複数の OS がインストールされているなら、ブート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ーのセカンダリまたは外付けドライブとして接続し、そのコンピューターの 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 -> ブート前認証なしでマウントする」を選択し、ブート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シリンドーの元の(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。最初のシリンドー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を使うには、それを CD/DVD ドライブに挿入しコンピューターを再起動してください。TrueCrypt レスキューディスクは、通常はシステムドライブの最初のシリンドーに記録されているものとおなじ TrueCrypt ブートローダーを持っていることに留意してください。だから、TrueCrypt レスキューディスクから起動する場合には、標準の TrueCrypt ブートローダーの画面が表示されます。正規の TrueCrypt ブートローダーと TrueCrypt レスキューディスクとの違いは、Repair Option(修復オプション) メニューで多くのオプションが提供されているという点です。(正規の TrueCrypt ブートローダーでは「Permanently decrypt system partition/drive - システムパーティション/ドライブの暗号化を解除」だけです) TrueCrypt ブートローダー画面が表示されないとか修復メニューの全オプションが選択可能になっていなかつたりした場合(下記参照)は、BIOS で CD/DVD からの起動の前にハードディスクからの起動を試みるように設定されている可能性があります。もしそうなら、コンピューターを再起動して BIOS 開始画面が表示されたらすぐに F2 か Delete キーを押し、BIOS 設定画面が表示されるまで待ってください。BIOS 設定画面が表示されないなら、コンピューターを再起動しすぐに繰り返し F2 か Delete キーを押してください。BIOS 設定画面が表示されたら、BIOS で起動順を CD/DVD ドライブが最初になるように設定してください。(この手順については、BIOS かマザーボードの説明書を参照してください) それから、コンピューターを再起動してください。それでレスキューディスクから TrueCrypt ブートローダーが起動するはずです。修復オプションを選択するにはキーボードの F8 を押してください。

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。

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、メインウィンドーの「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集めはじめます。収集されたデータは可能なかぎ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けっして直接には暗号化キーとして使われないことを知っておいてください。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つた場合には)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つてしまうかもしれませんからです。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のパーティション/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 スペ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。

スペースファイルは 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(スペースファイルの)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 のエクスプローラー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、このようになります)

警告: ダイナミックな(スペースファイルの)TrueCrypt ボリュームでの速度は通常のボリュームよりも大きく悪化します。また、ダイナミックな(スペースファイルの)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充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、(性能はあがりますが)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憶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

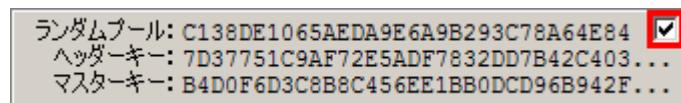
TrueCrypt はハードウェア/ソフトウェア・レイドと同様に Windows のダイナミックボリュームをサポートします。Windows のダイナミックボリュームを TrueCrypt ボリュームとしてフォーマットする場合には(Windows のディスク管理ツールを使って)ダイナミックボリュームを作成したあと、システムの再起動が必要です。そうすれば TrueCrypt ボリューム作成ウィザードの「デバイス選択」に目的のボリュームが表示され、選択できるようになります。

「デバイス選択」ウインドーで、ダイナミックボリュームは单一のデバイス(項目)としては表示されません。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。

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。キャッシュになければ、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とも **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いければ、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(キャッシング)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。キャッシング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 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

この機能はひんぱ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。 トランザクションモードでは、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」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 → お気に入りボリュームをマウントを選択してください。

お気に入り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として登録」を選択してください。

ボリューム → お気に入りボリュームをマウント

この機能は、以前に「お気に入り」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: ブート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

ブート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るべきです。(「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 -> ブート前認証なしでマウントする

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ブート前認証なしで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: 複数のパーティションを同時にマウントする必要があれば、「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、「ブート前認証なしでシステム暗号化されたパーティションをマウントする」を有効にしてください。

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

TrueCrypt ボリュームにあるすべてのファイルをバックアップするだけの空き領域がない場合、この機能を使って、少なくともボリュームヘッダーだけでもバックアップをとっておくことを強くおすすめします。ここにはマスターキーが記録されています。(バックアップしたファイルのサイズは 1024 バイトになるはずです) ボリュームヘッダーが破損すると、ほとんどの場合はボリュームはマウントできなくなります。

ボリュームヘッダーをバックアップするには、「デバイスの選択」か「ファイルの選択」をクリックし、ボリュームを選択してください。それから「ツール -> ボリュームヘッダのバックアップ」をクリックしてください。ヘッダーをリストア(復旧)するには、同じ手順で最後に「ボリュームヘッダのリストア」を選択してください。

TrueCrypt のボリュームヘッダーのバックアップは暗号化されたボリュームヘッダーの正確なコピーです。バックアップコピーにはいっさいの追加情報は含まれません。TrueCrypt ボリュームヘッダーバックアップは正しいパスワードを知っているか正しいキーファイルを用意しなければ、復号することはできません。

注意: 標準のボリュームヘッダーと隠しボリュームのボリュームヘッダーが格納される領域とがバックアップ(バックアップファイルにコピー)されます。そのボリュームに隠しボリュームがなかつ

たとしてもです。(隠しボリュームのみせかけの拒否を確実にするため)しかし、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」->「ボリュームヘッダのリストア」)

警告: ボリュームヘッダーをリストアすると、ボリュームのパスワードはバックアップ作成時に有効だったものに置き替えられます。さらに、バックアップ作成時にボリュームをマウントするのにキーファイルが必要だった場合には、ボリュームヘッダーをリストア後にボリュームを再マウントするのに同じキーファイルが必要になります。

ボリュームヘッダー・バックアップ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ために、新しいバックアップを作る必要があるかもしれません。しかしながら、ボリュームヘッダーは変更されないので、ボリュームヘッダー・バックアップは最新の状態のままということになります。

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key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)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。

ツール->ボリュームヘッダーのリストア

TrueCrypt ボリュームがマウントできなくなった場合にはヘッダーが破損している可能性があります。ボリュームヘッダーをバックアップしておけば、この機能で復旧できます。

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」->「ボリュームヘッダのリストア」)

警告: ボリュームヘッダーをリストアすると、ボリュームのパスワードはバックアップ作成時に有効だったものに置き替えられます。さらに、バックアップ作成時にボリュームをマウントするのにキーファイルが必要だった場合には、ボリュームヘッダーをリストア後にボリュームを再マウントするのに同じキーファイルが必要になります。

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ー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ことがあります。エクスプローラウィンドーが 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ー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つ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。

システム暗号化されたパーティションをブート前認証なしでマウントする

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ブート前認証なしで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便利な理由があります。:

- 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せん) TrueCrypt はキーファイル自体に改変を加えることは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、「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。

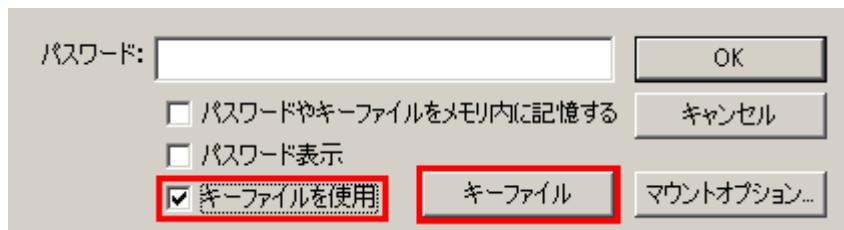
重要: 総当たり攻撃に対抗するため、ひとつのボリュームに対するキーファイルの大きさは少なくとも 30 バイトが必要です。ボリュームが複数のキーファイルを使うなら、そのうちのひとつは 30 バイト以上が必要です。30 バイトという制限は、キーファイルの平均情報量を増大させます。ファイルの先頭 1024 キロバイトの平均情報量が少ないと、(ファイルサイズに関わりなく)キーファイルとしては使われません。平均情報量という意味がよくわからなければ、TrueCrypt にランダムな内容のファイルを生成させ(キーファイル->ランダムキーファイルの生成を選択)、それをキーファイルとして使うことをすすめます。

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トするのに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つ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「キーファイルを使う」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」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。キーファイルとキーファイル検索パスでは、該当のファイル/フォルダーをキーファイルダイアログウィンドウにドラッグすることでも選択できます。

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(フォルダ一)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(読み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。

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。

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 項目は憶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)ということがわかつてしまふかもしれません。

この問題に対処する必要があるなら、BartPE を使うことをすすめます。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開封し、(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で可能になります。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、それらが読み取可能な場合のみに動作します。(USB メモリスティ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 が常駐していざ 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も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」ダイアログき「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、アメリカ政府各部局、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する Information Assurance の要求を満たすと考えるアメリカ政府各部局、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)

Whirlpool

Whirlpool ハッシュアルゴリズムは Vincent Rijmen (AES encryption algorithm の共同作者)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 競技に似て、EU 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。

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。

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。

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
- Mac OS X 10.4 Tiger
- Mac OS X 10.5 Leopard
- 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。 <code>/l</code> が省略され <code>/a</code> 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プを鳴らします。
<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 or /k</code>	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。

/cache or /c	y 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。n の場合(/c n)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 /w を使ってください)
/history or /h	y 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; n: マウントしたボリュームの履歴を保存しない。(例 /h n)
/wippecache or /w	ドライバに記憶したパスワードをすべて消去
/password or /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 /p "My Password"). 空パスワードを表すには /p ""としてください。 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 /q を使うことを検討してください。
/quit or /q	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) preferences が指示されていれば(/q preferences) プログラム設定が読み込まれます。 /q background は TrueCrypt 常駐(トレイアイコン)を開始します。 /q 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。
/silent or /s	/q 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。
/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 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):

`/noisochk` 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イ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。

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 {rm|ro|sm|ts}] [/p password] [/q
[background|preferences]] [/s] [/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しすてむ)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ることになります。

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。

ボリュームとボリュームヘッダーのバックアップ

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。このため、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以外のどんなデータについても同様です)

非システムボリューム

注意: ファイルのバックアップに加えて、マスターキーを含むボリュームヘッダーをバックアップ(ボリュームヘッダーバックアップのサイズは 1024 バイト)することも強くすすめます。ボリュームヘッダーが破損すると、多くの場合はマウントができなくなります。ボリュームヘッダーのバックアップとリストアについては、メインプログラム ウィンドウの章、プログラムメニューの節、ツール -> ボリュームヘッダーのバックアップとツール -> ボリュームヘッダーのリストアを参照してください。

TrueCrypt ボリュームと TrueCrypt ボリュームヘッダーを安全にバックアップするには、以下の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。
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. マウントされたバックアップボリュームへ直接に、バックアップ元ボリュームのヘッダーのバックアップを作成し保存してください。その後、バックアップボリュームをアンマウントしてください。
4. 同様に、バックアップ元ボリュームをマウントし、バックアップボリュームのヘッダーのバックアップをバックアップ元ボリュームに作成してください。
5. バックアップボリュームをマウントし、マウントされたバックアップ元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るでしょう。

- 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区画づくりの前の安全策の節を参照)¹

- 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。
- ボリュームヘッダーのバックアップを作成したこと、およびそれがどこに保存されているかということ。

バックアップ元ボリュームのヘッダーが破損した場合には、バックアップボリュームをマウントし、そこに保存されたヘッダーバックアップを使ってバックアップ元ボリュームのボリュームヘッダーを復旧することができます。(他も同様)

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、ブート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。

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。(クリ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。
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(前の手順のように通常の TrueCrypt ボリュームとして)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。
 - b. OKをクリック。
 - c. 「システム -> ブート前認証なしでマウント」を選択。

¹この場合、特にバックアップボリュームがファイル型である場合、隠しボリュームはホストボリュームのほんの少しの領域しか使わず、外殻ボリュームはほとんど全部をファイルで埋められているべきです。(そうでなければ、敵対者は隠しボリュームについてのみせかけの拒否を疑うかもしれません)

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。

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(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)
- 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。

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とあまりに膨大になってしまいます。

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(通常ハードディスクに置かれる)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(文書化されたものも、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)

ですから、Windows XP/Vista ユーザーには、スワップファイル機能を無効にすること、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無効にすることを強くおすすめします。これをするにはデスクトップか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->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 としてください。

知る限りでは、Windows 2000 ではこの方法では完全に無効にはできません。Windows 2000 ユーザーには、コンピュータをシャットダウンするつどにページングファイルをクリアするようセキュリティの設定を変更することをおすすめします。(詳細は Windows のマニュアルまたは www.microsoft.com を参照してください)

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。

ハイバネーションモード

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には、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key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。したがって、システム暗号化をしないなら、少なくとも機密データを扱ったり TrueCrypt ボリュームをマウントするセッションの間だけでもハイバネーション機能を無効にするか、ハイバネーションの起動を抑止することを強くおすすめします。

解決できそうな案: 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には、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。

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(メモリダンプ)が可能です。このメモリ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、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ダ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

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)他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ーの使用は、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。

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を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、メモリダンプファイルがシステムドライブ(通常はそうなっています)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のかはシステム暗号化の章を参照)

Windows レジストリ

TrueCrypt の「もっともらしい否認」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)がわかつ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)

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、WindowsXP/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)

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をあるメモリー領域(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

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。

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²⁾)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ディ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。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 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含む)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** は自然にはプロセスを停止せず、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。

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へ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へファイルを移動させてください。

データの破損

ハードウェアやソフトウェアのエラーや誤動作で、TrueCrypt ボリュームのファイルが破損することもあります。ですから、重要ファイルは定期的にバックアップをとることをおすすめします。(も

²⁾聞くところでは、通常の動作温度(26-44 °C) d h

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。

もちろん、TrueCrypt ボリュームに記録された暗号化データにかぎらず、すべての重要なデータについて言えることです)

TrueCrypt ボリュームにあるすべてのファイルをバックアップするだけの空き領域がない場合、少なくともボリュームヘッダーだけでもバックアップをとっておくことを強くおすすめします。ここにはマスターキーが記録されています。(バックアップしたファイルのサイズは 1024 バイトになるはずです)

詳細はボリュームとボリュームヘッダーのバックアップを参照してください。

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ってボリュームをマウントすることができます。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)に置かないことをすすめます。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。

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れば、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。

「隠しボリューム区画づくりの前の安全策」も参照してください。

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や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やアンチウィ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できます。

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。アンチウィ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。アンチウィ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、臨時にウィ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(ドライプリリストで)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という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ます。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。やってられないとか、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と、*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と、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います。

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。アンチウィ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を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 Macromedia 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、ブート前認証(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。

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)のあるバージョンはデータをドライブの最初のシリンドーに書込みます。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。

- 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。
- 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。

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充分な領域をドライブの最初のシリンド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

- TrueCrypt は現在のところ、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。
- 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トブルな ASCII キャラクターでなくてはいけません。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 のいくつかの組み込みツール(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。
- 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: パスワードを忘れてしまいました。TrueCrypt ボリュームのファイルを復元する方法はありますか?

A: TrueCrypt は正しいパスワードまたは暗号化に使ったキーなしで、暗号化されたデータを部分的でも完全にでも復元する機能はまったく持っていません。復元するたった一つの方法はパスワードやキーをクラックして暗号を破ることですが、パスワード/キーファイルの質や長さ、キーのサイズ、ソフトやハードの効率性、その他の要素によって、数千年、数百万年かかるかもしれません。

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、そもそ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ないません。唯一の方法はパスワードやキーを破ることですが、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ナー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、フォルダーナー、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充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: 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: OS を再インストールしても元からある 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。

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セクター(ボリュームの最後からの第3セクター)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: 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。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。「デバイス選択」ウインドーで、ダイナミックボリュームは単一のデバイスとしては表示されません。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憶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: 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: TrueCrypt ボリュームの最大サイズは 8589934592 GB です。。しかし、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、最大 1PB(1,048,576 GB)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: トラベラーモードで TrueCrypt を実行しようとすると、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できません。

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はありますか？

ボリュームとボリュームヘッダーのバックアップを参照してください。

Q: ボリュームヘッダーのバックアップをどこに保存すればいいでしょうか？

ボリュームとボリュームヘッダーのバックアップ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」で次のオプションを有効にしてください。
 - TrueCrypt を開始
 - お気に入りボリュームをマウント
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> で入手することもできます。

Q: Windows のファイルセレ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、ファイルセレ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。ただし、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)を暗号化する場合だけです。

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 Windows OS 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 - ハードディスクはまったく使いませんし、ハードディスクが存在する必要もありません)、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: Windows がインストールされているパーティション/ドライブを暗号化することも検討してください。(その手順についてはシステム暗号化を参照)

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)

ハードウェアやソフトウェアのエラーや誤動作で、TrueCrypt ボリュームのファイルが破損することもあります。ですから、重要ファイルは定期的にバックアップをとることをすすめます。(もちろん、TrueCrypt ボリュームに記録された暗号化データにかぎらず、すべての重要なデータにつ

いて言えることです)TrueCrypt ボリュームにあるすべてのファイルをバックアップするだけの空き領域がない場合、少なくともボリュームヘッダーだけでもバックアップをとっておくことを強くおすすめします。ここにはマスターキーが記録されています。(バックアップしたファイルのサイズは 1024 バイトになるはずです) ボリュームヘッダーが破損すると、ほとんどの場合はボリュームはマウントできなくなります。ボリュームヘッダーをバックアップするには、「ツール -> ボリュームヘッダーのバックアップ」をクリックしてください。

「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。

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)に管理者がリセットする方法はありますか?

A: 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。同様に、ブート前認証でもパスワードをリセットすることができます。(「システム -> レスキューディスク作成」と TrueCrypt 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)

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: 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。

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: 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。

Q: Windows を TrueCrypt 隠しボリュームにインストールすることはできますか？

A: はい、ただし直接ではありません。Virtual PC , VirtualBox, VMware, など(VirtualBOX OSE はフリーでオープンソースであり、Virtual PC と VMware の一部のエディションはフリーです)の仮想マシンソフトウェアで起動する OS を含むディスクイメージ格納する予定にしている TrueCrypt ボリュームになら、隠しボリュームを作ることができます。これで TrueCrypt 隠しボリュームに Windows をインストールしておくことができます。

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」の下の「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いで、デバイスがまとめて暗号化されている)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」の下の「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る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.bak (TrueCrypt ブートローダーが書き込まれる前のドライブの最初のシリコンダー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ければ、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 が左のオペラントと結果のビットサイズ。(左のオペラントが 1-bit 値で、右のオペラントが 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)、またはブート前認証中に、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シリンドーの最後の 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シリンドーおよび TrueCrypt レスキューディスクにあります)
2. ボリュームの最後から 1536 バイトの位置から 512 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) もしそのボリュームに隠しファイルがあれば、この時点でそのヘッダーを読み込んだことになります。(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)
注意: システム暗号化では、このステップおよび関連するすべてのステップは省略されます。
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 はこれらをかけ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ません - 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、ヘッダーアクセスキーが生成され、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(ボリュームヘッダー)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

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。

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)に戻って継続します。

しかし、今回は(1)で読んだデータの替わりに(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。こ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。(ボリュームヘッダー領域は、ヘッダーキーで暗号化されます) 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・ロガウェイが設計した XEX モード[12]がありますが、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

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

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

$K2$ は第二キー

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さを非常に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なります。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を基礎としている場合は2000回)繰り返さなくてはいけません。これは徹底したパスワード探索(総当たり攻撃)に要する時間を非常に増大させます。[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キーを導出するように指示を受けます。その後、このキーは三つの256-bitキーに分割され、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 亂数発生機構(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. $l =$ 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. $M = H(B_0 \| B_1 \| \dots \| B_q)$ [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. $B_i = B_i \wedge M$

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。

$$8. \quad R = B_0 \parallel B_1 \parallel \dots \parallel B_q$$

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:

$$\begin{aligned} (B_0 \parallel B_1) &= R \\ B_0 &= B_0 \wedge H(B_0 \parallel B_1) \\ B_1 &= B_1 \wedge H(B_0 \parallel B_1) \\ R &= B_0 \parallel B_1 \end{aligned}$$

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混合されるファイルです。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生成する組み込みのキーファイル生成機能を使って、キーファイルを生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。(巨大なファイルを処理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個づつロード、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 2⁸ 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

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はドライブの最初の論理シリナーに保管されます) 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(オプションのクイックフォーマットとダイナミックが無効になっていれば) ランダム値で満たされます。 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満たす(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。

TrueCrypt ボリュームフォーマット 仕様:

オフセット (bytes)	サイズ (bytes)	暗号化 ¹	備考
0	64	非暗号化 ²	ソルト
64	4	暗号化	ASCII 文字列 “TRUE”
68	2	暗号化	ボリュームヘッダーフォーマットバージョン
70	2	暗号化	ボリュームを開く最小プログラムバージョン
72	4	暗号化	(復号された) 256-511 バイトの CRC-32 チェックサム
76	8	暗号化	ボリューム作成日時
84	8	暗号化	ヘッダー作成/変更日時
92	8	暗号化	予約(0 をセット)
100	8	暗号化	ボリュームのサイズ
108	8	暗号化	暗号化データのオフセットバイト
116	8	暗号化	暗号化領域のサイズ
124	132	暗号化	予約(0 をセット)
256	Var.	暗号化	連結された第一、第二マスターキー ³
512	Var.	暗号化	データ領域(実際のボリュームの内容)

byte #0(ソルト)、byte #256(第二キー)、byte #288(マスター暗号化キー)のフィールドはボリューム生成過程の間、乱数発生機構(乱数発生機構参照)で生成された乱数が入れられます。

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最後から 1536 バイトの位置にあります。(ホスト/外殻ボリュームのヘッダーはボリュームの先頭にあります - 隠しボリューム参照)隠しボリュームのヘッダーのフォーマットについては、次の表で説明します。

オフセット (bytes)	サイズ (bytes)	暗号化状態	備考
0	64	非暗号化	ソルト
64	4	暗号化	ASCII 文字列 “TRUE”
68	2	暗号化	ボリュームヘッダーフォーマットバージョン
70	2	暗号化	ボリュームを開く最小プログラムバージョン
72	4	暗号化	(復号された) 256-511 バイトの CRC-32 チェックサム
76	8	暗号化	ボリューム作成日時
84	8	暗号化	ヘッダー作成/変更日時
92	8	暗号化	隠しボリュームのサイズ
100	8	暗号化	ボリュームのサイズ
108	8	暗号化	暗号化データのオフセットバイト
116	8	暗号化	暗号化領域のサイズ
124	132	暗号化	予約(0 をセット)
256	Var.	暗号化	連結された第一、第二マスターキー

TrueCrypt ボリュームヘッダーはつねに 512 バイトです。隠しボリュームのヘッダーも 512 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。

¹ボリュームヘッダーの暗号化領域はヘッダーキー(およびLRW モードでの第二キー)で暗号化されます。詳細は暗号化アルゴリズム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ソルト(ランダムデータの連続であるため)は秘密にする必要がなく、暗号化されている必要がないことに留意してください。

³ボリュームが複数の暗号化方式のカスケードで暗号化されている場合には、連結されたマスターキー(XTS モードの場合には、第二キー)がここに保存されます。

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]
- 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->テストベクターをクリック)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++ およびアセンブラーで書かれています)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/downloads.php>

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/license.php>

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

5.1a

2008年3月17日

機能改善:

- システムパーティション/ドライブを暗号化した場合のブート速度の向上(約10%) (*Windows Vista/XP/2008/2003*)
- その他の細かい改善 (*Linux and Mac OS X*)

非互換性の解消:

- 特定のハードウェア設定のコンピューターによって、システムパーティションが暗号化されていると、ハイバネーションからの復帰に失敗することがあった。注意: この現象が発生すると、RAMの内容が暗号化されずにハイバネーションファイルに書き込まれる。システムパーティション/ドライブを復号(「システム -> システムパーティション/ドライブの暗号化を解除」を選択)することで、そのデータを削除することができ、その後に再暗号化すればよい。(*Windows Vista/XP/2008/2003*)

補足: 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ーの使用は、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。

- アップルのあるコンピューターのBIOSのバグがブート前認証のパスワード入力とTrueCryptブートローダーの制御を妨害することへの対策 (*Windows Vista/XP/2008/2003*)

バグ修正:

- Windowsでシステムパーティションし/ドライブの暗号化を解除すると、オリジナルのパーティションテーブルが復旧しない。注意: これは、暗号化ドライブのパーティションを区切り直し、Windowsで暗号化を解除した場合の問題である。(*Windows Vista/XP/2008/2003*)
- その他の小さいバグ修正 (*Windows, Mac OS X, and Linux*)

5.1

2008年3月10日

新機能:

- システムパーティションが暗号化されている場合には、ハイバネーションができるようにした。(TrueCrypt の前バージョンではシステムパーティションが暗号化されていてもハイバネーションが発生しないようにしていた)(*Windows Vista/XP/2008/2003*)
- システム暗号化キーの有効範囲内のパーティション(たとえば、稼動中ではない他の OS が載った暗号化システムドライブにあるパーティション)をブート前認証なしでマウントできる。 (*Windows Vista/XP/2008/2003*)
- 新規ボリューム作成のコマンドラインオプション (*Linux and Mac OS X*)

機能改善:

- AES 暗号化/復号の速度改善(ハードウェアによるが 30~140%) (*Windows*)
- システムパーティション/ドライブの暗号化をした場合のブート速度改善 (*Windows Vista/XP/2008/2003*)
- システム暗号化をした場合の TrueCrypt ブートローダーを圧縮し、小容量で保存することにした。非カスケード暗号(AES, Serpent, Twofish)が使われていれば、TrueCrypt ブートローダーはそのバックアップをドライブの最初のシリンドラーに保管することができ、実際にそうなるようにした。TrueCrypt ブートローダーが破損した場合には、自動的にそのバックアップが代替として機能する。

この改善の結果、次の問題は発生しなくなった。：ある種の不適切な設計のアクティベーションソフトウェア(あるサードパーティ製ソフトウェアのアクティベーションに使われる)はドライブの最初のシリンドラーに書込みし、TrueCrypt ブートローダーを破損する。この場合には TrueCrypt ブートローダーを修復するために TrueCrypt レスキューディスクを使わなければならなかった。TrueCrypt をこのバージョンにアップグレードすれば、この問題は発生しなくなる。(システムパーティション/ドライブが非カスケード暗号, AES, Serpent, Twofish, で暗号化されている場合)

注意: システムパーティション/ドライブがすでに非カスケード暗号(AES, Serpent, Twofish)で暗号化されている場合は、このバージョンの TrueCrypt にアップグレードすれば、自動的に TrueCrypt ブートローダーのバックアップがドライブの最初にシリンドラーに作成される。

- TrueCrypt ブートローダー(AES)の必要最小メモリーを 42KB から 27KB に減らした。このため、BIOS が大きなメモリーを使うコンピューターでもシステムパーティション/ドライブの暗号化が可能になった。 (AES アルゴリズムを使った場合) (*Windows Vista/XP/2008/2003*)
- その他の細かい改善 (*Windows, Mac OS X, and Linux*)

非互換性の解消:

- コンピューターによって、システム暗号化事前テスト中に、Windows がログオン画面の表示に失敗することがあった。これは今後発生しない。 (*Windows Vista/XP/2008/2003*)

バグ修正:

- あるシステムでは、新しくマウントされた非システムボリュームのドライブ文字が正しく割り当てられなかつたが、これは今後発生しない。 (*Windows*)
- その他の小さいバグ修正 (*Windows, Mac OS X, and Linux*)

5.0a

2008年2月12日

機能改善:

- TrueCrypt ブートローダーの必要メモリーを 18KB に減らした。この改善の結果、大部分のコンピュータでは後記の問題がおきなくなった。TrueCrypt ブートローダー 5.0 ではいくつかのコンピュータでシステムパーティション/ドライブの暗号化ができなかった。(システムブート前認証暗号化テスト時に、TrueCrypt ブートローダーが「暗号化のためのメモリーが不足です」というメッセージを出す)

バグ修正:

- 特定ブランドのオーディオカードを実装したコンピュータで、システム暗号化テスト時またはシステムパーティション/ドライブが暗号化されたときに、サウンドカードドライバのロードができなかつた。これは、今後は発生しない。(Windows Vista/XP/2003)
- ネットワーク越しにマウントされた TrueCrypt ボリュームにアクセスできる。(Windows)
- 前のバージョンで作成した TrueCrypt レスキューディスクはいくつかのコンピュータを起動できなかつた。これは、今後は発生しない。(Windows Vista/XP/2003)
注意: TrueCrypt 5.0 で作成した TrueCrypt レスキューディスクで起動できなければ、TrueCrypt のこのバージョンにアップデートし、新しい TrueCrypt レスキューディスクを作ってください。(「システム -> レスキューディスクの作成」を選択)
- その他の小さいバグ修正(Windows, Mac OS X と Linux)

5.0

2008年2月5日

新機能:

- システムパーティション/ドライブ(OS がインストールされるドライブ)の暗号化とブート前認証(システムを使ったりファイルの読み書きをする場合には、システム起動前に正しいパスワードを入力する必要がある)ができるようになった。詳細はシステム暗号化の章を参照。
- パイプラインプロセスにより、読み書き速度を 100%まで向上。(Windows)
- Mac OS X 対応。
- TrueCrypt Linux 版にグラフィカルユーザーインターフェースをつけた。
- TrueCrypt ボリューム作成ウィザードで、NTFS ボリューム内に隠しボリュームをつくることができるようになった。
- 動作モードを XTS とした。これはフィリップ・ロガウェイによって 2003 年に設計され、最近に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 は LRW モードより早く安全です。(XTS モードについての詳細は「技術詳細」の「動作モード」を参照)

注意: TrueCrypt のこのバージョンで作成されたボリュームは XTS モードのみで暗号化されます。しかし、TrueCrypt の前のバージョンで作成したボリュームも TrueCrypt のこのバージョンでマウントできます。

- SHA-512 ハッシュアルゴリズム(新しいボリューム作成には使われなくなった SHA-1 の後継)

注意: HMAC-SHA-512(PRF)で導出されたヘッダーキーで既存のボリュームを再暗号化するには、「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。

機能改善、バグ修正、セキュリティ拡張:

- TrueCrypt Linux 版は Linux カーネルの変更(カーネル更新)に影響されないように、設計しなおした。
 - たくさんの小さい改善、バグ修正およびセキュリティ拡張(Windows と Linux)
- TrueCrypt 旧バージョンを使っているなら、このバージョンにアップグレードすることを強くすすめます。

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

私たちは以下の皆さんに感謝します:

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 と共に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>.

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、配布することができます。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