



Central department of security and information systems

---

# TRUECRYPT Security target

---

Date of Creation	: October 22, 2007
Project name	: TRUECRYPT
Type of Document	: Security target
Reference	: SPM030-ST-2.00
Classification	: public
Number of Pages	: 64 (including 2 headers)
Comments	: none

## 序文

特に教育の現場での、本書の複製、および/または二次利用は、次の3つの条件を満たすことによって、国防総局情報セキュリティ中央局(SGDN/DCSSI)によって許可されている。

- 本書の配布を無償とすること。

- 本書を複製する場合には、完全性に注意を払うこと(原書に忠実であること): 修正、改ざんは認めない。

- 本書の複製版には、例えば「本書は、国防総局情報セキュリティ中央局(SGDN/DCSSI) (<http://www.ssi.gouv.fr/en>)によって策定されたものである。」など、出自を明らかにする文言を含めること。

## 目次

<b>1. ST 概説</b> .....	<b>7</b>
1.1. ST 識別 .....	7
1.2. TOE 識別 .....	7
1.3. TOE の概要 .....	8
1.3.1. TOE のタイプ .....	8
1.3.2. TOE の使用 .....	8
1.3.3. TOE のセキュリティ特性と特徴 .....	9
1.3.4. TOE とソフトウェア環境 .....	10
1.4. TOE 記述 .....	10
1.4.1. TRUECRYPT の概要 .....	10
1.4.2. TOE 範囲 .....	18
<b>2. 適合主張</b> .....	<b>20</b>
2.1. CC 適合 .....	20
2.2. PP 適合 .....	20
2.3. 保証パッケージ適合 .....	20
<b>3. セキュリティ課題定義</b> .....	<b>21</b>
3.1. 資産 .....	21
3.2. ユーザ .....	22
3.3. 脅威 .....	22
3.4. 組織のセキュリティ方針 (OSP) .....	22
3.5. 前提条件 .....	23
<b>4. セキュリティ対策方針</b> .....	<b>24</b>
4.1. TOE のセキュリティ対策方針 .....	24
4.2. 運用環境のセキュリティ対策方針 .....	25
4.3. 根拠 .....	25
4.3.1. 脅威 .....	25
4.3.2. 組織のセキュリティ方針 (OSP) .....	26
4.3.3. 前提条件 .....	26
4.3.4. 課題定義とセキュリティ対策方針の対応表 .....	26
<b>5. セキュリティ要件</b> .....	<b>28</b>
5.1. 序章 .....	28
5.1.1. 対象 .....	28
5.1.2. オブジェクト .....	28
5.1.3. 操作 .....	29
5.1.4. ユーザ .....	31
5.2. セキュリティ機能要件 .....	31
5.2.1. FCS クラス: 暗号化によるサポート .....	31
5.2.2. FDP クラス: ユーザデータの保護 .....	34
5.2.3. FIA クラス: 識別と認証 .....	38
5.2.4. FMT クラス: セキュリティ管理 .....	40
5.2.5. FPT クラス: TSF の保護 .....	44
5.2.6. FRU クラス: 資源使用 .....	45
5.3. セキュリティ保証要件 .....	45

5.4. 根拠.....	46
5.4.1. 保証要件.....	46
5.4.2. 機能要件.....	46
5.4.3. セキュリティ対策方針と要件の対応表.....	48
5.5. 依存性.....	50
5.5.1. セキュリティ機能要件の依存性.....	50
5.5.2. セキュリティ保証要件の依存性.....	51
<b>6. TOE 要約仕様.....</b>	<b>53</b>
6.1. TOE セキュリティ機能.....	53
6.2. TOE 要約仕様と機能要件との対応付け.....	56
6.2.1. 対応表.....	56
6.2.2. 根拠.....	57
<b>付録 A 定義と頭字語.....</b>	<b>62</b>
6.3. 略語と頭字語.....	62
6.4. 定義.....	62
<b>付録 B 参考文献.....</b>	<b>64</b>



## 表

表 1. 脅威に対するセキュリティ対策方針根拠 .....	26
表 2. セキュリティ対策方針に対する脅威.....	26
表 3. 組織のセキュリティ方針に対するセキュリティ対策方針根拠 .....	26
表 4. セキュリティ対策方針に対する組織のセキュリティ方針.....	27
表 5. 前提条件に対する環境のセキュリティ対策方針根拠 .....	27
表 6. 環境のセキュリティ対策方針に対する前提条件.....	27
表 7. TOE 機能要件に対するセキュリティ対策方針.....	48
表 8. セキュリティ対策方針に対する TOE 機能要件.....	48
表 9. 機能要件の依存性.....	50
表 10. 保証要件の依存性.....	52
表 11. セキュリティ機能に対する機能要件.....	56
表 12. 機能要件に対するセキュリティ機能.....	57

## 1. ST 概説

---

この ST の TOE は、TRUECRYPT 全てではなくそのサブセットである。

TRUECRYPT は、ストレージデバイスに格納された情報の機密性を保護するためのソフトウェアである。そのメカニズムは暗号化によって提供される。

本章は、以下の 4 つの項で構成されている。

- 第 1.1 項では、本 ST(セキュリティ・ターゲット)の識別を提供する。
- 第 1.2 項では、TOE の識別を提供する。
- 第 1.3 項では、TOE の調達を考えている顧客に、自身のニーズに適合しているかを確認できるよう、TOE の概要について説明する。
- 第 1.4 項では、評価者と認証者を対象に、TOE の詳細を提供する。

### 1.1.

#### ST 識別

タイトル	:TRUECRYPT security target
バージョン	:2.0
著者	:Silicomp-AQL
リファレンス	:SPM030-ST-2.00
発行日	:2007 年 10 月 22 日

### 1.2.

#### TOE 識別

開発者(名称)	:TrueCrypt Foundation
製品名	:TRUECRYPT
製品のバージョン	:4.2a
TOE の評価対象	:TOE の評価範囲は、次のような暗号アルゴリズムに限定する。AES-256、TWOFISH、AES-TWOFISH、SHA-1、および RIPE-MD 160(第 1.4.2 項参照)。
対象プラットフォーム	:マイクロソフト・ウィンドウズ XP をベースにした PC プラットフォーム(第 1.4.2 項参照)。

### 1.3. TOE の概要

TOE は自動的に大量データを暗号化するソフトウェアである。本 TOE では、ファイル内やマウントされた物理的なディスクに仮想暗号化ディスク(TrueCrypt ボリューム)を生成することを可能にする。TrueCrypt は、フロッピー・ディスクや USB キーなどの全体、または一部を暗号化することもできる。

この TOE は、ユーザがデータを操作(参照、修正、保存)するために使用するアプリケーションと、暗号化ディスクが格納されているストレージデバイスを透過的に中継する。ユーザが明示的に TOE を操作するのは、ユーザが最初に暗号化ディスクにアクセスするためにディスクをアクティブにすると、ディスクをインアクティブにするときだけである。

ディスクをアクティブにするには、ユーザの認証が必要である。(ディスクが)一旦アクティブになると、暗号化ディスクは他のディスクと何ら変わることなくアクセスすることができる。

作業中は、TOE はユーザに対し透過的にディスク上に保存される(もしくは読み込まれる)データの暗号化(復号)を実施する。

本 ST は、本セキュリティ評価において TOE に課せられるセキュリティ要件を定義する。

#### 1.3.1. TOE のタイプ

本 TOE では以下の 2 つのケースにおいて、コンピュータのデバイス(一般的には、取り外し可能なストレージデバイス)全体、または一部に保存されているデータの機密性を保護することができる。

1. TOE が動作していないとき。
2. TOE は動作中だが、正規ユーザが認証されていない状態。

ここでは TOE に対し認証済みの正規ユーザが、TOE を操作している間の脅威については考慮していない。

本 TOE の主要な目的は、コンピュータやデバイスの盗難対応である。ただし、本製品によって提供されるデータの機密性保護に対する、運用リスクはこの限りではない(例えば、暗号化が適用されない領域へ機密性の高い情報を書き込む、或いはデバイスに復号した情報を書き込む場合など)。デバイス内のデータの機密性は、コンピュータの稼動中はその状態如何にかかわらず保証される。仮に突然シャット・ダウンしてしまった場合でも、オペレーティング・システムが RAM のメモリ・イメージを生成しないよう設定されていれば、RAM に一時的に書き込まれた重要データの機密性も維持される。

簡単のため、TOE により保護されるデータを含むデバイスの一部(全部の場合もあるが)を、曖昧にならない限り本項以降では「暗号化ディスク」と称する。

#### 1.3.2. TOE の使用

組織や管理部門の IT 資産は、その他の資産と同様盗難の対象となりうる。このリスクは、機器が持ち運びやすくなり、以前に比べると職場以外でこれら機器を使用することが多くなった昨今一層拍車がかかっている。本 TOE は自動的に大量データを暗号化するアプリケーションであり、それによりデータの機密性が保護され、データが盗難にあった場合の影響を低減する。

TOE の使用方法をより適切に示すには、本自動暗号化アプリケーションを金庫か、頑丈な箱と比較するのがよい。金庫の第一の目的は、一旦閉めたら、その内容物が盗まれないように保護することである。同様に暗号化アプリケーションの目的は、一旦暗号化しその後ディスクを「インアクティブ」にしたら、その中のデータを保護することである。

さらに類似点を述べるならば、業務中社内に人がいるときに、金庫の扉が開けられその内容物が人により取り扱われる。従ってその内容物へのアクセスは、組織のポリシーや物理的な手段によって管理される（金庫が設置されている場所の入退室管理や監視カメラの設置など）。即ち金庫により提供される保護機能は、取り扱われている最中の内容物を対象としているのではなく、内容物が金庫に格納された間のみ（データがディスクに格納されている間のみ）を対象としている。つまり金庫のセキュリティの重要な側面は、その開閉時における以下を考慮することとなる。

- 金庫を開けることができるのは誰か？ どのような条件で？
- 金庫を閉めることができるのは誰か？ どのような条件で？
- その条件には、どのような制限が盛り込まれているか？

同様に、ディスク暗号化アプリケーションは、(ワークステーションの記憶領域で)アプリケーションにより展開され一旦公開されたデータを保護することはできない。特にディスク共有の問題は、オペレーティング・システムとネットワーク権限管理に帰着することが多い。そのような事は全く考慮されていないわけではないが、その点は本 TOE の対象外とする。

### 1.3.3. TOE のセキュリティ特性と特徴

TOE の重要な役割は、デバイス、またはコンピュータ本体が盗難にあった際に格納されているデータの機密性を保護する一方で、許可されたユーザがデータを閲覧できるようにすることである。

- **ディスクに格納されたデータの機密性の保護。** TOE の重要な役割は、ディスクに保存されているデータの機密性を保護することである。この機密性の保護は、他のアプリケーションやコンピュータのオペレーティング・システムによって生成された一時的なデータにも適用されなければならない。

またこの機能が正しく動作するには、TOE には以下の機能が要求される。

- **ユーザ認証。** ディスクや認証の設定の修正をする前には、ユーザは認証される必要がある。

TOE は暗号化ディスクがアクティブのときに、ディスクへ保存され、読み出されるデータを透過的に暗号化 / 復号する。暗号化ディスクをアクティブにするには、ユーザはパスワードや鍵ファイルなどの認証データに基づく認証が要求される。

操作時には、TOE は「暗号化ディスク」に対応する暗号鍵を使用する。その暗号鍵は TOE により生成される。

認証データや暗号鍵は TOE によって保護されるべきユーザ・データではないが、以下を考慮すればその機密性は保証されなければならない。

- 認証メカニズムの有効性は、認証データの機密性に依存する。
- 暗号化メカニズムの有効性は、暗号鍵の機密性に依存する。

これらデータが開示されてしまうと、ユーザデータの機密性を保証することはできない。これらデータの機密性は、第 1.3.1 項で特定されたケースにおいて、TOE により保証される。

TOE は、暗号化されたデータをディスク、またはパーティション (USB メモリ、フロッピー・ディスクなどを含む) に格納することができる。「暗号化ディスク」がアクティブにならない限り、このディスクやパーティションはフォーマットされていないように見えるため (そこに何が格納されているかを判別することは不可能である。一見すると無作為な数字が含まれているようにしか見えない)、セキュリティが強化される。これはラップトップ・コンピュータに格納されているデータを保護するために使用されることが多いソリューションである。

最終的に、この TOE は、「暗号化ディスク」を、さらに別の「暗号化ディスク」に隠すことができる。これにより文字通り力づくでユーザの認証データを取得しようとする攻撃者から、機密性の高い情報を保護することができる。

#### **1.3.4. TOE とソフトウェア環境**

TRUECRYPT 製品は、Windows 2000/XP/2003、および Linux 環境で動作する。

本評価では、Windows XP 環境のみを評価対象としている。

本 TOE は、セキュリティ機能<sup>1</sup>を実行するために外部のソフトウェアやマイクロ・プログラムを必要としない。

本 TOE は、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 キー、その他データを格納する全てのデバイスに格納されたデータを暗号化し、その機密性を保証する。

「暗号化ディスク」は、CD や DVD にも保存することができる。

「暗号化ディスク」は、オペレーティング・システムから独立しており、TOE が動作できる全ての環境でマウントすることができる。

### **1.4. TOE 記述**

#### **1.4.1. TRUECRYPT<sup>2</sup>の概要**

TRUECRYPT は、「Encryption for the Masses」、すなわち E4M v2.02a をベースに TrueCrypt Foundation によって開発されたオープン・ソースの自動即時暗号化ソフトウェアである。TRUECRYPT は、マイクロソフトの Windows XP/2000/2003 (32 ビット、および 64 ビット)、および Linux 環境で動作する。

<sup>1</sup> ユーザ認証手続きや TOE の操作 (暗号化と復号) に関しては鍵ファイルも利用できる。これらの鍵ファイルは、外部媒体 (USB キー、スマートカードなど) に格納することができる。ただし、ここではそれら外部媒体に関する如何なる要件にも触れない。

<sup>2</sup> この項では、評価対象である TOE 範囲を考慮せず、TRUECRYPT を 1 つの製品として紹介する。

TRUECRYPTは、コンテナに格納されている機密性の高いデータを保護する。暗号化されるのはデータごとではなくコンテナ全体である。以降の各章では、このコンテナが「暗号化ディスク」を構成しているものとする。

## ファイルとパーティション

TRUECRYPTでは、2通りの「暗号化ディスク」を管理することができる。

- コンテナ・ファイルは、どのような拡張子、サイズも定義できる。コンテナ・ファイルは、どのようなデバイスにも格納できる普通のファイルである。
- パーティション・ファイルは、物理的なパーティション(ディスク全体を指すことが多い)であり、コンテナとして機能する。ハードディスク全体、USBハードディスク、フロッピー・ディスク、USBキー、その他全てのデータ格納用デバイスのデータも暗号化することができる。

### **1.4.1.1. 「暗号化ディスク」の作成プロセス**

本項では、「暗号化ディスク」の作成プロセスを説明する。このプロセスは、以下の7段階で構成される。

- 第1段階: ユーザによるパラメタの選択
- 第2段階: 乱数生成
- 第3段階: パスワードの処理
- 第4段階: ヘッダ鍵の生成
- 第5段階: ヘッダの生成
- 第6段階: ヘッダの暗号化
- 第7段階: 暗号化ディスクのフォーマット

#### **第1段階: ユーザによるパラメタの選択**

ユーザは、「暗号化ディスク」の作成に必要な情報を提供する。これには次のような情報が含まれる。

- ユーザのパスワード
- 鍵ファイル
- 暗号アルゴリズムのシーケンス
- ハッシュ関数アルゴリズム
- 「暗号化ディスク」のサイズ
- 「暗号化ディスク」のファイル・システム
- 「暗号化ディスク」のクラスタ・サイズ

#### **第2段階: 乱数生成**

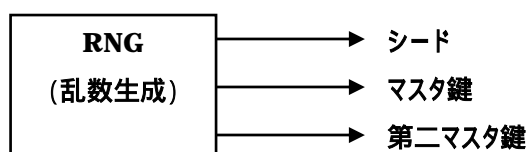


図 1: 乱数生成

乱数生成器は、次のようなデータを生成する。

- マスタ鍵
- 第二マスタ鍵(32 バイト)
- シード(64 バイト)

マスタ鍵と第二マスタ鍵は、「暗号化ディスク」のデータを暗号化するために使用される。シードはヘッダ鍵を生成するために使用される。

### 第 3 段階: パスワードの処理

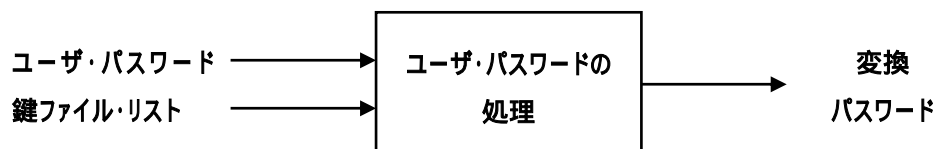


図 2: パスワードの処理

第 3 段階には、鍵ファイルを使用したパスワードの変換が含まれる。鍵ファイルはバイナリ・データを含むファイルであり、一連の加算によりパスワードと連結される。鍵ファイルは TRUECRYPT により生成することもできるし、ユーザが指定することもできる。また最初の 1Mb のデータのみが使用される。

注: 鍵ファイルの使用は任意である。ファイルが使用されない場合パスワードは変換されない。

### 第 4 段階: ヘッダ鍵の生成

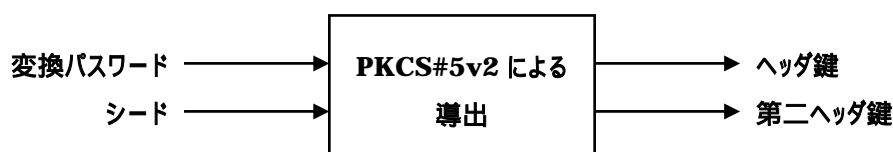


図 3: PKCS#5v2 による(鍵)導出

第 4 段階では、「暗号化ディスク」のヘッダを暗号化するためのヘッダ鍵が生成される。そのため、乱数生成器は 64 バイトのシードを生成する。このシードと変換パスワードは PKCS#5v2 に従い処理され、ヘッダ鍵と第二ヘッダ鍵を構成する一連のバイトが生成される。

### 第 5 段階: ヘッダの生成

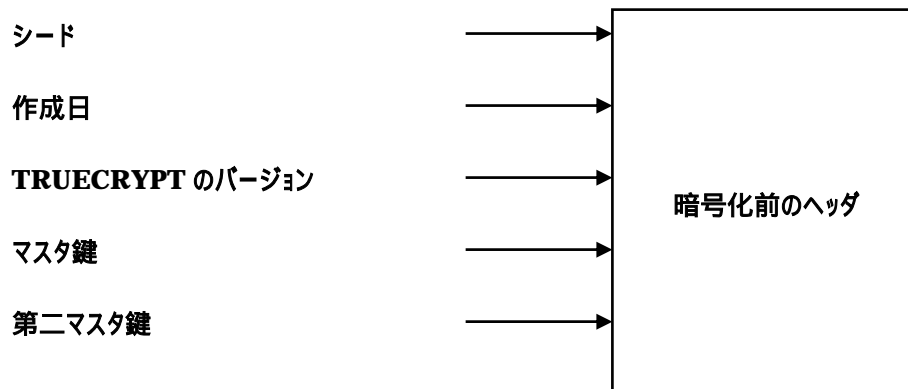


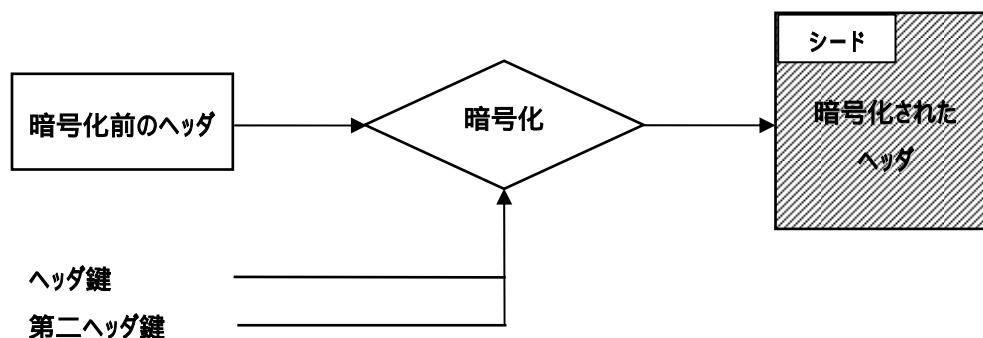
図 4: ヘッダの生成

第 5 段階では、TRUECRYPT ボリューム・ヘッダが生成される。暗号化ディスクのヘッダは暗号化ディスクの最初のセクタ(セクタ 0)に格納され、サイズは 512 バイトである。この段階で、暗号化ディスクのデータを暗号化するためのマスタ鍵と第二マスタ鍵が乱数生成器によって生成される。

このヘッダには、次のような情報が含まれる。

- ヘッダ鍵を生成するために使用されたシード
- ASCII 文字列: TRUE
- 暗号化ディスクのヘッダ フォーマット バージョン
- 暗号化ディスクをオープン可能なプログラムの最小バージョン
- 256 から 511 バイト(マスタ鍵と第二マスタ鍵)の CRC32 チェックサム
- マスタ鍵
- 第二マスタ鍵

### 第 6 段階: ヘッダの暗号化



第 6 段階では、ヘッダ鍵と第二ヘッダ鍵を使用して TRUECRYPT ボリューム・ヘッダが暗号化される。シード(すなわち、最初の 64 バイト)を除く、全てのヘッダが暗号化される。

## 第 7 段階：暗号化ディスクのフォーマット

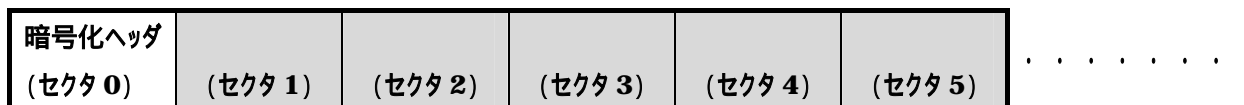


図 5：暗号化ディスクのフォーマット

第 7 段階では、暗号化ディスクが作成されフォーマットされる。

- 暗号化ディスクの最初の 512 バイト(セクタ 0)に、暗号化ヘッダが書き込まれる。
- 次に、QuickFormat が無効化されている場合は、これまでの段階で生成した乱数鍵ではない鍵を使用し暗号化された乱数データを、残りのセクタに埋め込む。

### 1.4.1.2. 暗号化ディスクのマウントとアンマウント

標準的なディスクと同様格納されているデータにアクセスするには、「暗号化ディスク」は TRUECRYPT によりマウントされなければならない。「暗号化ディスク」のデータアクセスは認証完了後のみ可能となる。

「暗号化ディスク」をアンマウントすれば、このディスクに格納されている全てのデータへのアクセスが不可能になる。

### 1.4.1.3. 認証

認証は、「暗号化ディスク」の生成プロセス(第 1.4.1.1.項)の第 2、第 3 段階で説明した、認証データ(パスワードと鍵ファイル)によるヘッダ鍵の生成に基づき実施される。

認証データを使用し生成されたヘッダ鍵により、ヘッダを復号できた場合に限りユーザの認証は成功する。

### 1.4.1.4. 隠し「暗号化ディスク」

TRUECRYPT では、TRUECRYPT の「暗号化ディスク」を他の「暗号化ディスク」に秘匿する機能も備えている。

QuickFormat 機能が無効化されている場合、TRUECRYPT の通常の「暗号化ディスク」作成中は、その「空き」領域は実際のデータと無関係のデータにより埋められる。TRUECRYPT の「暗号化ディスク」に保護すべきデータがインポートされると、そのデータがデータと置き換わる。ハッカーは TRUECRYPT の「暗号化ディスク」に機密性の高いデータが格納されているか、あるいは「空き」領域のままなのかを知ることは不可能であることに注目していただきたい。

最初の外殻「暗号化ディスク」(ボリューム)を作成すると、隠し「暗号化ディスク」はその外殻の「空き」領域に相当する場所に格納される。

双方の「暗号化ディスク」(すなわち外殻「暗号化ディスク」と隠し「暗号化ディスク」)には、それぞれ異なるパスワードが設定される。この 2 つの異なるパスワードにより、隠し「暗号化ディスク」は秘匿可能となる。即ちユーザが入力したパスワードによって、TRUECRYPT はそれに対応した「暗号化ディスク」を表示する。

従って、攻撃者がユーザのパスワードを暴力で獲得したとしても、ユーザは外殻「暗号化ディスク」のパスワードを与えればよい。ハッカーがそのパスワードを使用しても外殻「暗号化ディスク」のみが表示され、機密性の高いデータを格納している隠し「暗号化ディスク」は「空き」領域と見なされる。またユーザは、念のため外殻「暗号化ディスク」に偽の重要そうに見えるデータを格納しておいてもよい。

#### 1.4.1.5. 「暗号化ディスク」の構造

TRUECRYPT の「暗号化ディスク」は、特徴的なデータや識別可能なデータを保持していない。TRUECRYPT ファイルの構造や中身を分析したところで、攻撃者は TRUECRYPT ファイルが TRUECRYPT ファイルであることを同定することはできない。すなわち、攻撃者の目には、この「暗号化ディスク」はでたらめなデータの寄せ集めしか見えない。

暗号化ディスクのヘッダ・フォーマットの仕様は、以下の表に示した通りである。

指数(バイト)	サイズ(バイト)	暗号処理	説明
0	64	平文	シード
64	4	暗号化	ASCII 文字列で「TRUE」
68	2	暗号化	「暗号化ディスク」のヘッダ フォーマット バージョン
70	2	暗号化	「暗号化ディスク」をオープンできる最小プログラム バージョン
72	4	暗号化	(復号された)256 から 511 バイトの CRC32 チェックサム
76	8	暗号化	「暗号化ディスク」作成日時
84	8	暗号化	ヘッダの作成 / 変更日時
92	8	暗号化	予約(0 で初期化)
100	156	暗号化	未使用
256	可変	暗号化	二次鍵(LRW モード)
288	可変	暗号化	マスタ鍵
512	可変	暗号化	データ・セクタ(「暗号化ディスク」の中身)

最初の 64 バイトのみが平文である。ただし疑似乱数として生成されているため、それ以降のファイルの中身と区別することはできない。指数#0(シード)、指数#256(二次鍵)、および指数#288(マスタ暗号鍵)として設定されたフィールドには、「暗号化ディスク」作成時に乱数生成器によって生成されたランダムな値が含まれる。

TRUECRYPT の「暗号化ディスク」の空き領域に隠し「暗号化ディスク」が収納されている場合、隠し「暗号化ディスク」のヘッダは、「暗号化ディスク」の末尾から指数#1536 に当たる部分に設定される(収納する側のボリューム・ヘッダは最前部に設定される)。隠し「暗号化ディスク」のヘッダのフォーマットの仕様は次の表のとおりである。

指数(バイト)	サイズ(バイト)	暗号処理	説明
0	64	平文	シード
64	4	暗号化	ASCII 文字列で「TRUE」
68	2	暗号化	「暗号化ディスク」のヘッダ フォーマット バージョン
70	2	暗号化	「暗号化ディスク」をオープンできる最小プログラム バージョン
72	4	暗号化	(復号された)256 から 511 バイトの CRC32 チェックサム
76	8	暗号化	「暗号化ディスク」作成日時
84	8	暗号化	ヘッダの作成 / 変更日時
92	8	暗号化	予約(0 で初期化)
100	156	暗号化	未使用
256	可変	暗号化	二次鍵(LRW モード)
288	可変	暗号化	マスタ鍵

#### 1.4.1.6. 自動即時暗号化と復号

自動即時暗号化とは、ユーザを介さずにデータがディスクにロード、または保存される直前に自動的に暗号化、または復号することである。ユーザは認証なしで「暗号化ディスク」に格納されているデータを読む(すなわち、復号する)ことはできない。

「暗号化ディスク」のファイル(例えば、ファイル名、ディレクトリ名、ディレクトリの全体的な内容、フリースペース、メタデータなど)は、全て暗号化される。

ファイルは、(例えば、単純にドラッグアンドドロップなどで)他の一般的なディスクから取り出したり保存するのと同じように、TRUECRYPT で実装した「暗号化ディスク」から取り出したり、保存することができる。ファイルは「暗号化ディスク」から取り出す、コピーされる最中に TRUECRYPT により(RAM メモリで)自動的に復号される。同様に、「暗号化ディスク」に書き込む、コピーする最中に(ディスクに書き込む直前に)RAM メモリで自動的に暗号化される。

#### 1.4.1.7. 暗号化ディスクに格納されているデータの保護

TRUECRYPT では、復号されたデータをディスクに保存することはない。復号されたデータは一時的に RAM メモリに格納される(この RAM メモリにデータを永続的に格納してはならない)。「暗号化ディスク」がマウントされているときも、このディスクに格納されているデータは常に暗号化されている。従って、シャット・ダウン後にオペレーティング・システムを再起動させても、「暗号化ディスク」はアンマウントされているため格納されているファイルにアクセスすることはできない。(オペレーティング・システムのシャット・ダウンなしに)突然の電源断が発生した場合も、「暗号化ディスク」に格納されているファイルにアクセスすることはできない。「暗号化ディスク」に格納されているデータへ再度アクセスするには、新たな認証が必要である。

特にマスタ鍵など、メモリに一時的に格納される秘密情報は使用後「ゼロクリア」される。関連するメモリ・ページをロックし、この情報がディスクにスワップされないようにする保護手段も講じられている。ただし TRUECRYPT は、(例えば、システムの物理的なメモリが不足している場合など)仮想ファイル・システムより復号された情報がスワップされるのを防ぐことはできない。従って機密性の高い情報を処理する必要がある場合は、Windows XP のスワップを

無効化することを推奨する。

#### 1.4.1.8. 管理者の権限<sup>3</sup>

自動即時暗号化 / 復号をセットアップするために、TRUECRYPT のインストールには Windows オペレーティング・システムの管理者権限が必要である。

従って、TRUECRYPT は管理者権限でインストールされなければならない。

TRUECRYPT を管理者権限でインストール後、権限がないユーザは TRUECRYPT を使用することができるようになる。一般的なユーザ権限でできることは、次のとおりである。

- 既存の「暗号化ディスク」のマウントとアンマウント
- ファイル・タイプの「暗号化ディスク」の作成

管理者権限がない場合、ユーザは以下の作業ができない。

- パーティション・タイプの「暗号化ディスク」の生成
- NTFS の生成
- TRUECRYPT のインストール、またはアンインストール
- 物理パーティションの「暗号化ディスク」のパスワードや鍵ファイルの変更
- 物理パーティションのヘッダの保存 / リストア
- TRUECRYPT を「トラベラーモード」で実行すること(第 1.4.1.11 項参照)

#### 1.4.1.9. 暗号化アルゴリズム

次の表は、TRUECRYPT に実装されている暗号アルゴリズムをリストにまとめたものである。「 」で区別されたアルゴリズムのみが今回の評価対象である。

対称鍵の暗号アルゴリズム		
AES	AES-256-LRW(256 ビット)	
BLOWFISH	BLOWFISH-LRW(448 ビット)	
CAST5	CAST5-LRW(448 ビット)	
SERPENT	SERPENT-LRW(256 ビット)	
DES3	DES3-LRW(168 ビット)	
TWOFISH	TWOFISH-LRW(256 ビット)	
AES-BLOWFISH	BLOWFISH 適用後、別の鍵で AES を適用	
AES-BLOWFISH-SERPENT	SERPENT、BLOWFISH 適用の順で、最後に別の鍵で AES を適用	
AES-TWOFISH	TWOFISH 適用後、別の鍵で AES を適用	
AES-TWOFISH-SERPENT	SERPENT、TWOFISH 適用の順で、最後に別の鍵で AES を適用	
SERPENT-AES	AES 適用後に、別の鍵で SERPENT を適用	
SERPENT-TWOFISH-AES	AES、TWOFISH 適用の順で、最後に別の鍵で SERPENT を適用	
TWOFISH-SERPENT	SERPENT 適用後、別の鍵で TWOFISH を適用	

<sup>3</sup> この TOE では、管理者の役割を識別していない。本項では、TOE がインストールされている (Windows の) オペレーティング・システムの管理者権限について説明する。

完全性、認証、およびハッシュ計算アルゴリズム	
CRC32	ボリューム、およびそれに対応する IV マスタ鍵のエラー管理アルゴリズム
SHA1	ハッシュ・アルゴリズム (160 ビット)
RIPEMD160	ハッシュ・アルゴリズム (160 ビット)
HMAC-SHA-1	ボリューム・パスワードの導出に使用する認証アルゴリズム
HMAC-RIPEMD160	ボリューム・パスワードの導出に使用する認証アルゴリズム
疑似乱数生成器	
PRNG	所有者

#### 1.4.1.10. 標準

次の表は、TRUECRYPT によって使用される標準のリストである。

標準	
PKCS#5	<i>RSA Laboratories, PKCS#5 v2.0 Password-based Cryptography Standard, 25 March 1999</i> TRUECRYPT では、ユーザ・パスワードの導出、すなわち PKCS5-PBKDF2 アルゴリズムを使用する。
FIPS 46-3	<i>NIST, Data Encryption Standard (DES), 25 October, 1999</i>
FIPS 197	<i>NIST, Advanced Encryption Standard (AES), Publication 197, 26 November, 2001</i>
FIPS 198	<i>NIST, The Keyed-Hash Message Authentication Code (HMAC), 6 March, 2002</i>
FIPS 180-2	<i>NIST, Secure Hash Standard, 1 August, 2002</i>
NIST SP800-38A	<i>Morris Dworkin, Recommendation for Block Cipher Modes of Operation</i>

#### 1.4.1.11. その他の機能

TRUECRYPT ボリュームは CD や DVD にも保存することができる。従って CD や DVD に保存する前に、ハードディスク上にコンテナ・ファイルを作成する必要がある。

TRUECRYPT は、「トラベラー」モードで使用することもできる。この場合オペレーティング・システムには何もインストールする必要はないが、TRUECRYPT を管理者権限で動作させる必要がある。この「トラベラー」モードのためには以下を作成する必要がある。

- 「暗号化ディスク」
- 全ての TRUECRYPT 実行ファイルが含まれるディレクトリ
- アプリケーションを実行し「暗号化ディスク」を自動的にマウントする autorun.inf ファイル

最後に、TRUECRYPT では「暗号化ディスク」のヘッダの保存とリストアップができる。これらの機能は、評価対象のセキュリティ機能には含まれない。

### 1.4.2. TOE 範囲

#### 1.4.2.1. TOE の論理的範囲

ソフトウェアの全てのコンポーネントが評価対象である。ただし、この評価対象は次の暗号アルゴリズムに限定される。



## 2. 適合主張

---

### 2.1. CC 適合

この ST は、コモン・クライテリア ([CC2]、および [CC3]) バージョン 3.1 のパート 2・パート 3 適合である。

### 2.2. PP 適合

この ST は、いずれの PP<sup>4</sup>にも適合するものはない。

### 2.3. 保証パッケージ適合

本 ST における評価保証レベルは、以下のコンポーネントで拡張された EAL2+ (EAL2 追加) である。

- ADV\_FSP.4
- ADV\_TDS.3
- ADV\_IMP.1
- ALC\_TAT.1
- AVA\_VAN.3

---

<sup>4</sup> 本書は、PP CDISK (自動即時暗号化アプリケーション) をベースに記載されたものである。ただし、この PP は CC 3.0 に適合しているため、この ST が適合性を主張することはできない。特に機能要件を再使用することができない。従って、本 ST は PP から再使用可能な情報のみに基づき記載されている。

## 3. セキュリティ課題定義

---

### 3.1. 資産

この TOE の一番の目的は、ユーザがデータを保存したデバイスやコンピュータが盗難にあった場合に、このデータを保護することである。データ自身は秘密鍵(マスタ鍵)によって暗号化され機密性が保護されている。この秘密鍵は別の秘密鍵(認証データから導出されたヘッダ鍵)で(同じく)暗号化されている。それぞれの資産に必要な保護のタイプは、*保護*の部で説明されている。コモン・クライテリアで識別されている資産は、次の 2 タイプである。

- **TSF データ**: TOE のために TOE により作成され、TSF の機能に影響するデータ。
- **ユーザ・データ**: ユーザのためにユーザにより作成され、TSF の機能に影響を与えないデータ。

これらの資産のタイプは、対応する機能要件のクラスが存在する。

#### 3.1.1. TSF データ

##### **D.DONNEES\_AUTH**

認証データに代表されるこの資産は、ユーザにより提供される識別(ユーザ・パスワードと鍵ファイル)を検証するために使用される。

*保護*: 機密性

##### **D.CLE\_ENTETE**

ヘッダ鍵に代表されるこの資産は、マスタ鍵を含むヘッダ・データの暗号化に使用される。この鍵は認証データから導出される。

*保護*: 機密性

##### **D.CLE\_MAITRE**

マスタ鍵に代表されるこの資産は、ユーザ・データを暗号化するために使用される。

*保護*: 機密性

#### 3.1.2. ユーザ・データ

##### **D.DONNEES\_UTILISATEUR**

ユーザ・データに代表されるこの資産は、TOE によりディスク上での機密性が保護される。暗号化されていないデータが対象である(既に暗号化されているデータは、機密性の高い資産ではない)。

*保護*: 機密性

### 3.2. ユーザ

運用環境における TOE は、直接的、または間接的に、以下の役割を取り扱う。

#### ユーザ

コンピュータのディスク上に機密性を保護すべきデータを保持するユーザ。

#### 適用上の注釈:

TOE の導入と構成を実施するセキュリティ管理者は、(データに関する)セキュリティ上の問題に関与しない。従って、TOE の機能ではこの役割を必要としない。

### 3.3. 脅威

本項における脅威とは、TOE により提供されるサービスではなく、TOE のセキュリティを脅かすものである。(例えば公共の場で盗む等)外部に持ち出された機器を狙う人や泥棒等、TOE が運用される環境外においては様々な人が脅威となりうる。正規のユーザは、攻撃者とは見なさない。

#### T.ACCS\_DONNEES

攻撃者は、例えば部分的な、或いは全てのディスク・イメージを(何回かにわたり)採取する、もしくはデバイスや機器を盗んだ後に、ディスクに格納されている機密性の高いデータを獲得する。

#### 適用上の注釈:

実装方法に依存するが、ディスク・イメージには特定の暗号鍵などその他の資産も含まれる可能性がある。

以下は、この脅威における攻撃シナリオの例である。

- 攻撃者は機密性が保護されていない(暗号化による保護がされていない)重要なデータを取得する。
- 攻撃者は重要なデータを保護するための対称暗号メカニズムにより使用されるマスタ鍵の取得に成功する。そしてこの鍵を使用して復号し、ユーザの機密性の高いデータにアクセスする。
- 攻撃者は暗号され保護されている(マスタ鍵は暗号化されたヘッダに格納されている)マスタ鍵を取得するために、暗号化に使用されているヘッダ鍵を発見する。このヘッダ鍵を使用してマスタ鍵にアクセスし、ユーザの機密性の高いデータを復号することができる。
- 攻撃者はヘッダ鍵を計算するために使用される認証データ(パスワードや鍵ファイル)の発見に成功する。この情報を使用してヘッダ鍵、マスタ鍵の順にアクセスし、ユーザの機密性の高いデータを取得する。

### 3.4. 組織のセキュリティ方針(OSP)

#### OSP.CRYPT

TOE の暗号化のメカニズムは、標準的な強度レベル([CRYPT])を考慮し、DCSSI が定める暗号化の要件に適合しなければならない。

### 3.5. 前提条件

#### A.ENV\_OPERATIONNEL

運用環境は、正規ユーザが重要なデータにアクセス可能な状況において、攻撃者にディスクにたいするアクセスを許容してはならない。

## 4. セキュリティ対策方針

---

### 4.1. TOE のセキュリティ対策方針

#### **O.ARRET\_UTILISATEUR**

TOE は、ユーザの要求に基づき機密性の高い情報(ユーザ・データや暗号鍵)をアクセス不可にしなければならない。

##### *適用上の注釈:*

このセキュリティ対策方針は、データを効果的に保護するために、ユーザが TOE を停止しディスクをインアクティブにすることを許可することを意味する。このセキュリティ対策方針では、データのセキュアな消去に関しては考慮していない。

#### **O.CRYPTO**

TOE は、標準強度レベル([CRYPT])に関する DCSSI 暗号化フレームの要件に適合した暗号化機能と暗号化鍵操作機能を実装しなければならない。

#### **O.PROTECTION\_DES\_DONNEES\_ENREGISTREES**

TOE は、格納されているデータにアクセスできるようになる前に、ユーザが認証されていることを保証しなければならない。

##### *適用上の注釈:*

このセキュリティ対策方針を満たすためには、格納されているデータへのアクセスを許可する暗号鍵が利用可能になる前に、ユーザが認証されていることを保証しなければならない。

マスタ鍵は保護されなければならない。これらマスタ鍵は、認証なしでアクセスされてはならない。

#### **O.ROBUSTESSE**

TOE(の装置、またはディスク)が突然(不定期に)シャット・ダウンした場合でも、機密性の高いデータにアクセスできてはならない。

##### *適用上の注釈:*

このセキュリティ対策方針は、異常発生時においても暗号化されるべきデータが暗号化されずに、永続的に記録されないことを保証するものである。現実的に、盗難や不正コピーの前には TOE を直ぐにシャット・ダウンする可能性が高い。その場合にデバイスに暗号化されていないユーザのデータが存在してしまうことも起こりうる。

#### **O.CLES\_CHIFFREMENT**

TOE は、ユーザの重要なデータの機密性を確保することができる暗号化鍵(マスタ鍵)を生成しなければならない。

## 4.2. 運用環境のセキュリティ対策方針

### OE.ENV\_OPERATIONNEL.1

ユーザが認証された場合、運用環境は機密性の高いデータ、鍵、および認証データの機密性を保証しなければならない。

#### *適用上の注釈:*

装置は、傍受やデータの許可されていない通信に対し効果的な保護(適切に設定されたファイアウォール、更新されたウイルス定義ファイルを持つウイルス対策ソフトウェア、スパイウェア対策ソフトウェアなどを使用)を提供しなければならない。

共存するアプリケーションは TOE の円滑な稼動を妨げてはならない。即ち特にそれらアプリケーション経由での、TOE より保護されているファイルに対する操作は、TOE の外部にファイルの全部、または一部を複製してはならない。ただしユーザが明示的に要求した場合や、要求したオペレーションの明示的な結果である場合は除く。

### OE.ENV\_OPERATIONNEL.2

ユーザは、信頼のおける環境(ユーザが一人の場合、また知る必要のある人物のみと一緒にいるときなど)である場合に限り、機密性の高いデータにアクセスしなければならない。

## 4.3. 根拠

### 4.3.1. 脅威

**T.ACCES\_DONNEES**: TOE は、機密性の高いユーザ・データ(**D.DONNEES\_UTILISATEUR** で定義された資産)を暗号化しディスクに格納する(**OB.DU** オブジェクト)。従って資産の保護は暗号化されたデータの保護に帰着する。

この脅威は、ディスクに格納された(暗号化された)データの機密性を保証する

**O.PROTECTION\_DES\_DONNEES\_ENREGISTREES** により対抗される。**O.ROBUSTESSE** も、例えば一時的にでも暗号化されていないユーザ・データがディスクに格納されないことを保証することで、この脅威への対抗に寄与する。

更に **O.ARRET\_UTILISATEUR** は、ユーザがデータが格納されているディスクをインアクティブにすることにより、明示的にデータを保護できることを保証する。

最後に、**O.CRYPTO** は実装された暗号化の機能と使用した暗号鍵を管理することによって、暗号的な分析(攻撃)によるディスクへの不正なアクセス防止を保証する。

**O.CLE\_CHIFFREMENT** は、TOE が使用する暗号化鍵の可用性を保証する。従って、ディスクに格納されている暗号化されたユーザ・データの暗号的な分析の防止に寄与する。鍵の品質は、鍵の生成が TOE の暗号化機能の一部として実装されているため、**O.CRYPTO** によって保証されている。

#### 4.3.2. 組織のセキュリティ方針(OSP)

**OSP.CRYPTO**:このOSPは、**O.CRYPTO** 対策方針で直接対応されている。

#### 4.3.3. 前提条件

**A.ENV\_OPERATIONNEL**:この前提条件は、**OE.ENV\_OPERATIONNEL.1** と **OE.ENV\_OPERATIONNEL.2** により直接対応されている。

TOE が動作し、正規ユーザがディスクをアクティブにしていれば、ユーザのワークステーションのアプリケーションは、そこに格納されているデータを自在に操作することができる。**OE.ENV\_OPERATIONNEL.1** は、これらのアプリケーションが、ユーザが知らない間にディスクと同じデバイス上にデータが複製されないこと、および一般的にユーザのワークステーションがデータの機密性を喪失させる原因にならないことも保証する。

**OE.ENV\_OPERATIONNEL.2** では、正規のユーザは適切なセキュリティの知識を有しトレーニングを受けているため、従ってそれらが TOE の運用環境において正しく活用されると確信できる。

#### 4.3.4. 課題定義とセキュリティ対策方針の対応表

脅威	セキュリティ対策方針	根拠
T.ACCES_DONNEES	O.ROBUSTESSE、 O.PROTECTION_DES_DONNEES_ENGREGISTREE、 O.CRYPTO、O.CLES_CHIFFREMENT、 O.ARRET_UTILISATEUR	第 4.3.1 項

表 1: 脅威に対するセキュリティ対策方針根拠

セキュリティ対策方針	脅威
O.ARRET_UTILISATEUR	T.ACCES_DONNEES
O.CRYPTO	T.ACCES_DONNEES
O.PROTECTION_DES_DONNEES_ENGREGISTREE	T.ACCES_DONNEES
O.ROBURSTESSE	T.ACCES_DONNEES
O.CLES_CHIFFREMENT	T.ACCES_DONNEES
OE.ENV_OPERATIONNEL.1	
OE.ENV_OPERATIONNEL.2	

表 2: セキュリティ対策方針に対する脅威

組織のセキュリティ方針(OSP)	セキュリティ対策方針	根拠
OSP.CRYPTO	O.CRYPTO	第 4.3.2 項

表 3: 組織のセキュリティ方針に対するセキュリティ対策方針根拠

セキュリティ対策方針	組織のセキュリティ方針 (OSP)
O.ARRET_UTILISATEUR	
O.CRYPTO	OSP.CRYPTO
O.PROTECTION_DES_DONNEES_ENGREGISTREE	
O.ROBURSTESSE	
O.CLES_CHIFFREMENT	
OE.ENV_OPERATIONNEL.1	
OE.ENV_OPERATIONNEL.2	

表 4: セキュリティ対策方針に対する組織のセキュリティ方針

前提条件	環境のセキュリティ対策方針	根拠
A.ENV_OPERATIONNEL	OE.ENV_OPERATIONNEL.1 OE.ENV_OPERATIONNEL.2	第 4.3.3 項

表 5: 前提条件に対する環境のセキュリティ対策方針根拠

環境のセキュリティ対策方針	前提条件
OE.ENV_OPERATIONNEL.1	A.ENV_OPERATIONNEL
OE.ENV_OPERATIONNEL.2	A.ENV_OPERATIONNEL

表 6: 環境のセキュリティ対策方針に対する前提条件

## 5. セキュリティ要件

### 5.1. 序章

#### 5.1.1. サブジェクト

TSP は、次のようなサブジェクトを扱う。

サブジェクト	セキュリティ属性	値
S.API	-	-
S.DISK	S.DISK_HEADER_STATUS(ディスク・ヘッダ)	ACTIVATED/DEACTIVATED
S.DISK	S.DISK_HEADER_STATUS(ディスクの状態)	ACTIVATED/DEACTIVATED
S.DISK	S.DISK_ID(ディスク ID)	ファイルかパーティション ID

TOE によって扱われるディスクは、以下の 3 つのセキュリティ属性を有す S.DISK サブジェクトで表現される。

- S.DISK\_HEADER\_STATUS セキュリティ属性。暗号化ディスクのヘッダに格納されたデータがアクセス可能かどうかを示す。
- S.DISK.STATUS セキュリティ属性。ヘッダ以外の部分がアクティブかインアクティブかを示す。
- S.DISK.ID セキュリティ属性。ディスクに対応するファイルかパーティションの ID を示す。

認証されたユーザは、自身を本サブジェクトと関連付ける (結合) できる場合に限り、ヘッダに格納されているデータにアクセス可能 (S.DISK\_HEADER\_STATUS = ACTIVATED) である。ヘッダに格納されているデータにアクセス可能な場合、以下の操作ができる。

- 認証データの修正、もしくは、
- ディスクを実際にマウントし、ユーザ・データにアクセスする (S.DISK\_HEADER\_STATUS = ACTIVATED)。

S.API 一般サブジェクトは、全てのアプリケーションがアクセス可能な入力ポイントに対応し、アクティブなディスクのデータへのアクセスを許可する。

#### 5.1.2. オブジェクト

TSP は、次のようなオブジェクトを扱う。

オブジェクト	セキュリティ属性	値
S.DISK	「5.1.1 サブジェクト」参照	「5.1.1 サブジェクト」参照
OB_MASTER_KEY (マスタ鍵)	OB.MASTER_KEY.DISK_ID (ディスク ID)	ファイルかパーティション ID
	OB.MASTER_KEY.STATUS (鍵のアクセス可能性)	ACTIVATED/DEACTIVATED (平文 / 暗号化状態)

オブジェクト	セキュリティ属性	値
<i>OB.HEADER_KEY</i> (ヘッダ鍵)	-	-
<i>OB.DU</i> (暗号化されたユーザ・データ)	<i>OB.DU_DISK_ID</i> (ディスク ID)	ファイルかパーティション ID
<i>OB.VD</i> (認証データ)	<i>OB.VD_DISK_ID</i> (ディスク ID)	ファイルかパーティション ID

S.DISK サブジェクトは、S.DISK を対象とする操作が存在するという意味において、オブジェクトでもある。

マスタ暗号鍵(*OB.MASTER\_KEY*)は、暗黙的にディスクに対応する。従って、ディスク上にユーザ・データ(*D.DONNEES\_UTILISATEUR*)を保存することは、*OB.DU* オブジェクトの生成、改変を意味し、その *OB.DU* オブジェクトに対応するディスク ID(*OB.DU\_DISK\_ID*)により、そのデータがどのマスタ鍵(言い換えればどのディスク上で)暗号化されたのかが判る。*OB.DU* オブジェクトは *D.DONNEES\_UTILISATEUR* と同じデータを表現しているが、しかし TOE により一度暗号化されたものである。

マスタ鍵(*OB.MASTER\_KEY*)自体は、特定のセキュリティ属性と関連付けられる必要のないヘッダ鍵(*OB.HEADER\_KEY*)による暗号化メカニズムにより保護される。ヘッダ鍵は暗号化されたディスクには格納されない。ヘッダ鍵は認証プロセス時に、認証データから導出される。

マスタ鍵(*OB.MASTER\_KEY*)は、その鍵が復号された場合(アクティブになった場合)に限り使用することができる。*OB.MASTER\_KEY.STATUS* のセキュリティ属性が持つことのできる 2 つの値(*ACTIVATED/DEACTIVATED*)はそれに対応している。従って、マスタ鍵がディスク・ヘッダに格納されている限り、ヘッダ・データのアクセス可能性は、マスタ鍵のアクセス可能性と同じである。

- *S.DISK.HEADER\_STATUS* = *ACTIVATED* *OB.MASTER\_KEY.STATUS* = *ACTIVATED*
- *S.DISK.HEADER\_STATUS* = *DEACTIVATED* *OB.MASTER\_KEY.STATUS* = *DEACTIVATED*

TOE によって扱われるのであれば、そのディスクに対応する認証データ(*OB.VD*)は、ディスクのユーザを認証するためのデータである。ヘッダ鍵を導出するには、パスワードや鍵ファイルが使用される。

- パスワードは、ユーザがディスクを作成したときに選択される。
- 鍵ファイルは、ユーザがディスクを作成したときに選択される。鍵ファイルには、TOE の乱数生成器によって生成されたランダムな値を含ませることができる。

認証データは、認証後ディスクをインアクティブにしたときのみ修正することができる。

### 5.1.3. 操作

TSP の操作は、以下の通りである。

操作	サブジェクト	オブジェクト
S.DISK -> OP.CREATE ( <i>OB.MASTER_KEY</i> , <i>OB.VD</i> )	S.DISK	<i>OB.MASTER_KEY</i> , <i>OB.VD</i>

操作	サブジェクト	オブジェクト
S.DISK -> OP.MODIFY(OB.VD)	S.DISK	OB.VD
S.DISK -> OP.MOUNT(S.DISK, OB.VD)	S.DISK	S.DISK, OB.VD
S.DISK -> OP.USE(S.DISK, OB.MASTER_KEY)	S.API	S.DISK, OB.MASTER_KEY
S.API -> OP.DECIPHER(S.DISK, OB.DU)	S.API	S.DISK, OB.DU
S.API -> OP.CIPHER(S.DISK, OB.DU)	S.API	S.DISK, OB.DU
S.API -> OP.DISMOUNT(S.DISK)	S.API	S.DISK

*OP.CREATE* は、「暗号化ディスク」の作成に対応する。

- ディスクのマスタ鍵(OB.MASTER\_KEY)は、ランダムに生成される。
- ディスクの作成時、ユーザは作成ディスクの暗号アルゴリズムを選択する。
- ディスクの生成時、ユーザは最終的にはディスク所有者を識別する手段となる認証データ(OB.VD)を選択する。
  - + このデータは、ヘッダ鍵の計算にも使用される。
  - + このヘッダ鍵により、ヘッダ・データ(特にマスタ鍵)を暗号化することができる。
  - + 認証メカニズムは、この導出メカニズムがベースになっている。認証データは、導出されたヘッダ鍵が暗号化されたディスクのヘッダを正しく復号することができる場合有効と見なすことができる。

一度選択されたデータは、認証終了後(すなわち、S.DISK.HEADER\_STATUS = ACTIVATED、および OB.MASTER\_KEY.STATUS = ACTIVATED の場合)で、暗号化されたディスクがインアクティブにされたとき(S.DISK\_STATUS = DEACTIVATED の場合)、データ生成者のみが修正(*OP.MODIFY*)できる。認証データが修正される際はヘッダのみが取り出される。ディスクはマウントされないため、ユーザ・データにアクセスすることはできない(S.DISK.STATUS = DEACTIVATED)。

*OP.MOUNT* 操作は、ユーザによる S.DISK ディスクのアクティブに対応している。このディスクをアクティブにするには、ユーザは OB.VD 認証データを提供しなければならない。この操作により、S.DISK.STATUS セキュリティ属性の値が、ACTIVATED に変更される。

*OP.USE* 操作は、ディスクの暗号化、または復号時における OB.MASTER\_KEY マスタ鍵の使用に対応している。これは TOE「内部」のオペレーションであり、TOE 外部のインタフェースの一部ではない。

*OP.DECIPHER* 操作は、TOE が管理するディスク上に格納されているデータの読み出しに対応している。TOE は、そのディスク上に格納されているデータを暗号化された状態で読み出し、これはディスクが作成された際に選択された暗号アルゴリズムに基づく復号操作である。

*OP.CIPHER* 操作は、TOE が管理するディスク上へのデータの書込みに対応している。TOE は、そのディスク上に格納されているデータを暗号化された状態で書き込み、これはディスクが作成された際に選択された暗号アルゴリズムに基づく暗号化操作である。



## 5.2.1.1. FCS\_CKM - 暗号鍵管理

暗号鍵は、そのライフサイクル全般を通して管理されなければならない。FCS\_CKM ファミリーはこのライフサイクルをサポートすることを意図し、暗号鍵の生成、暗号鍵へのアクセスや暗号鍵の廃棄に関する要件を定義する。

**FCS\_CKM.1 / ヘッド鍵 暗号鍵生成**

**FCS\_CKM.1.1 / ヘッド鍵:** TSF は、以下の[割付: DCSSI の暗号化要件(「CRYPTO」)、および PKCS#5 v2.0]に合致する、指定された暗号鍵生成アルゴリズム[割付: 以下の表]

ヘッド鍵	TrueCrypt がヘッド鍵と二次ヘッド鍵(LRW モード)の生成に使用する手法は、PKCS#5 v2.0 で定められている PBKDF2 である。
------	---

と指定された暗号鍵長[割付: 以下の表]に従って、暗号鍵を生成しなければならない。

暗号鍵	256 ビット
二次(暗号)鍵	256 ビット

**FCS\_CKM.1 / マスタ鍵 暗号鍵生成**

**FCS\_CKM.1.1 / マスタ鍵:** TSF は、以下の[割付: DCSSI の暗号化要件(「CRYPTO」)]に合致する、指定された暗号鍵生成アルゴリズム[割付: 以下の表]

マスタ鍵	マスタ暗号鍵と二次(暗号)鍵(LRW モード)の生成には、乱数生成器(RNG)が使用される。
------	--

と指定された暗号鍵長[割付: 以下の表]に従って、暗号鍵を生成しなければならない。

暗号鍵	256 ビット
二次(暗号)鍵	256 ビット

**FCS\_CKM.3 / ヘッド鍵 暗号鍵アクセス**

**FCS\_CKM.3.1 / ヘッド鍵:** TSF は、以下の[割付: DCSSI の暗号化要件(「CFYPTO」)、および PKCS#5]に合致する、指定された暗号鍵アクセス方法[割付: 鍵導出]に従って、[割付: ヘッド鍵アクセス]を行わなければならない。

**FCS\_CKM.3 / マスタ鍵 暗号鍵アクセス**

**FCS\_CKM.3.1 / マスタ鍵:** TSF は、以下の[割付: **DCSSI の暗号化要件 ('CFYPTO')**]に合致する、指定された暗号鍵アクセス方法[割付: **鍵の復号**]に従って、[割付: **マスタ鍵アクセス**]を行わなければならない。

*適用上の注釈:*

ヘッダ鍵は、暗号化されたマスタ鍵を含む TrueCrypt ボリューム・ヘッダの復号のために使用される。

**FCS\_CKM.4 / 暗号鍵廃棄**

**FCS\_CKM.4.1:** TSF は、以下の[割付: **なし**]に合致する、指定された暗号鍵破棄方法[割付: **上書き**]に従って、暗号鍵を破棄しなければならない。

*適用上の注釈:*

データの各バイトは、「0xFF」に続き、「0x0」を上書きすることによって削除される。この削除操作は、機密性の高いデータを使用する必要がなくなった時点で即座に実行される。

## 5.2.1.2. FCS\_COP - 暗号化操作

暗号化の操作が正しく機能するためには、指定されたアルゴリズムに適合し、指定されたサイズの暗号鍵が使用されなければならない。

識別された暗号化の操作には、データの暗号化 / 復号、セキュア・ハッシュ(メッセージ・ダイジェスト)、暗号鍵の暗号化 / 復号などがある。

**FCS\_COP.1 / 暗号化操作****FCS\_COP.1.1:**

TSF は、[割付: 以下の表]

<b>PKCS#5</b>	<b>RSA</b> ラボラトリ、 <b>PKCS#5 v2.0</b> 、パスワード・ベースの暗号化標準、 <b>1999年3月25日</b> 。 TrueCrypt では、ユーザ・パスワードからの鍵導出に、 <b>PKCS-5PBKDF2</b> アルゴリズムを使用している。
<b>FIPS 46-3</b>	<b>NIST</b> 、データ暗号化規格( <b>DES</b> )、 <b>1999年10月25日</b> 。
<b>FIPS 197</b>	<b>NIST</b> 、共通鍵(秘密鍵)暗号アルゴリズム( <b>AES</b> )、パブリケーション <b>197</b> 、 <b>2001年11月26日</b> 。
<b>FIPS 198</b>	<b>NIST</b> 、鍵付きハッシュ・メッセージ認証コード( <b>HMAC</b> )、 <b>2002年3月6日</b> 。
<b>FIPS 180-2</b>	<b>NIST</b> 、セキュア・ハッシュ標準、 <b>2002年8月1日</b> 。
<b>NIST S.P. 800-38A</b>	<b>Morris Dworkin</b> 、ブロック暗号の運用モードの推奨
<b>DCSSI</b>	<b>DCSSI</b> の暗号化要件 (' <b>CRYPTO</b> ')

に合致する、特定された暗号アルゴリズム[割付: 以下の表]

<b>AES-256</b>	AES-256-LRW(256 ビット)
<b>BLOWFISH</b>	BLOWFISH-LRW(448 ビット)
<b>TWOFISH</b>	TWOFISH-LRW(256 ビット)
<b>DES3</b>	DES3-LRW(168 ビット)
<b>AES-TWOFISH</b>	Twofish のあとに AES を適用(別々の鍵を使用)
<b>SHA1</b>	ハッシュ・アルゴリズム(160 ビットのハッシュ値)
<b>RIPE-MD 160</b>	ハッシュ・アルゴリズム(160 ビットのハッシュ値)

と暗号鍵長[割付: 以下の表]

<b>AES-256</b>	256 ビット
<b>BLOWFISH</b>	448 ビット
<b>TWOFISH</b>	256 ビット
<b>DES3</b>	168 ビット
<b>SHA1</b>	-
<b>RIPE-MD 160</b>	-

に従って、[割付: 完全性、および / または検証用の暗号化チェックサムの生成、セキュア・ハッシュ(メッセージ・ダイジェスト)の計算、データの暗号化、および / または復号、暗号鍵の暗号化、および / または復号、および乱数の生成]を実行しなければならない。

### 5.2.2. FDP クラス: 利用者データ保護

本項では、TOE のセキュリティ機能要件とユーザ・データの保護に関するセキュリティ機能方針について説明する。

ユーザ・データとは、TSF の動作には何ら影響を与えない、ユーザが使用するために、ユーザ自身が作成したデータのことである。従って、以下のデータの保護が対象となる。

- **D.DONNEES\_UTILISATEUR**(保護すべきユーザ・データ)

このデータは、**OB.DU** オブジェクトと対応している。

#### 5.2.2.1. FDP\_ACC - アクセス制御方針

本項では、アクセス制御 SFP を(名前で)識別し、アクセス制御方針の制御範囲を定義する。

この制御範囲は、次のような 3 つのグループで構成されている。

- + 制御方針の制御下のサブジェクト
- + 制御方針の制御下のオブジェクト、および
- + 制御方針によって管理されるとオブジェクト、サブジェクト間の操作。

識別されたアクセス制御 SFP を定義する規則は、FDP\_ACF.1 コンポーネントで定められる。

**FDP\_ACC.1 / サブセットアクセス制御**

FDP\_ACC.1.1: TSF は、[割付: 以下の表で識別されているサブジェクト、オブジェクト、および操作]に対して [割付: **SFP.TOE\_ACCESS\_CONTROL**]を実施しなければならない。

サブジェクト	<b>S.API, S.DISK</b>
オブジェクト	<b>OB.MASTER_KEY, OB.DU, OB.VD</b>
操作	<b>S.DISK -&gt; OP.CREATE(OB.MASTER_KEY, OB.VD) S.DISK -&gt; OP.MODIFY(OB.VD) S.DISK -&gt; OP.MOUNT(OB.VD) S.API -&gt; OP.USE(OB.MASTER_KEY) S.API -&gt; OP.DECIPHER(OB.DU) S.API -&gt; OP.CIPHER(OB.DU) S.API -&gt; OP.DISMOUNT(S.DISK)</b>

## 5.2.2.2: FDP\_ACF - アクセス制御機能

本項では、アクセス制御方針の制御範囲を特定している FDP\_ACC.1 コンポーネントを実装するセキュリティ機能に関連した規則を記述する。

**FDP\_ACF.1 / セキュリティ属性によるアクセス制御**

FDP\_ACF.1.1: TSF は、以下の [割付: 以下の表] に基づいて、オブジェクトに対して、 [割付: **SFP.TOE\_ACCESS\_CONTROL**]を実施しなければならない。

サブジェクト	<b>S.API, S.DISK</b>
オブジェクト	<b>OB.MASTER_KEY, OB.HEADER_KEY OB.DU, OB.VD</b>
操作	<b>S.DISK -&gt; OP.CREATE(OB.MASTER_KEY, OB.VD) S.DISK -&gt; OP.MODIFY(OB.VD) S.DISK -&gt; OP.MOUNT(OB.VD) S.API -&gt; OP.USE(OB.MASTER_KEY) S.API -&gt; OP.DECIPHER(OB.DU) S.API -&gt; OP.CIPHER(OB.DU) S.API -&gt; OP.DISMOUNT(S.DISK)</b>

FDP\_ACF.1.2: TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: 以下の表]。

R1	OP.CREATE	S.DISK -> OP.CREATE (OB.MASTER_KEY、OB.VD)は常に許可される	TRUE
R2	OP.MODIFY	S.DISK -> OP.MODIFY(OB.VD)は右記の条件が満たされれば許可される	S.DISK = OB.VD.DISK_ID、および S.DISK.STATUS = DEACTIVATED、および S.DISK.HEADER_STATUS = ACTIVATED
R3	OP.USE	S.API -> OP.USE(S.DISK、OB.MASTER_KEY)は右記の条件が満たされれば許可される	S.DISK.ID = OB.MASTER_KEY.DISK.ID、および S.DISK.HEADER_STATUS = ACTIVATED、および OB.MASTER_KEY.STATUS = ACTIVATED
R4	OP.MOUNT	S.DISK -> OP.MOUNT(S.DISK、OB.VD)は右記の条件が満たされれば許可される	S.DISK.ID = OB.VD.DISK_ID、および S.DISK.STATUS = DEACTIVATED、および S.DISK.HEADER_STATUS = ACTIVATED、および OB.MASTER_KEY.STATUS = ACTICATED
R5	OP.CIPHER	S.API -> OP.CIPHER(S.DISK、OB.DU)は右記の条件が満たされれば許可される	S.DISK.ID = OB.DU.DISK_ID、および S.API -> OP.USE(OB.MASTER_KEY)が許可されており、かつ S.DISK.STATUS = ACTIVATED
R6	OP.DECIPHER	S.API -> OP.DECIPHER (S.DISK、OB.DU)は右記の条件が満たされれば許可される	S.DISK.ID = OB.DU.DISK_ID、および S.API -> OP.USE(OB.MASTER_KEY)が許可されており、かつ S.DISK.STATUS = ACTIVATED
R7	OP.DISMOUNT	S.API -> OP.DISMOUNT (S.DISK)は右記の条件が満たされれば許可される	S.DISK.STATUS = ACTIVATED

**適用上の注釈:**

- R1: 全てのユーザに対し、新たな暗号化ディスクの作成が許可されている。
- R2: 暗号化ディスクに格納された認証データの修正は、ユーザが認証されディスクがアンマウントされたのちに許可される。認証されたユーザはヘッダ・データにアクセスし、修正することができる。ただし、ディスクはマウントされない。
- R3: 暗号化ディスクに格納されているマスタ鍵の使用は、ヘッダ・データにアクセスでき認証が終了(すなわち、

マスタ鍵にアクセスすることができるようになった)後に許可される。

- R4: 暗号化ディスクのマウントは、アクティブでない暗号化ディスクへの認証後許可される。認証によりヘッダを復号するヘッダ鍵が生成され(S.DISK.HEASER\_STATUS = ACTIVATED)、マスタ鍵にアクセスできる(OB.MASTER\_KEY.STATUS = ACTIVATED)ようになる。これにより、ディスクがマウントされ(S.DISK.STATUS = ACTIVATED)データの暗号化や復号が可能となる。
- R5: 暗号化ディスクへのユーザ・データの書き込みは、ディスクに格納されているマスタ鍵が使用可能であり(OP.USE)、ディスクがマウントされた場合(S.DISK.STATUS = ACTIVATED)のみに限られる。
- R6: 暗号化ディスクからのユーザ・データの読み出しは、ディスクに格納されているマスタ鍵を使用可能であり(OP.USE)、ディスクがマウントされた場合(S.DISK.STATUS = ACTIVATED)のみに限られる。
- R7: ディスクのアンマウントは、既にアクティブな(S.DISK.STATUS = ACTIVATED)全ての暗号化ディスクにおいて許可される。

**FDP\_ACF.1.3:** TSF は、次の追加規則、[割付: **TOE** は、**S.DISK.ID = OB.DU.DISK\_ID** および **S.DISK.STATUS = ACTIVATED** になるような **S.DISK** が存在した場合においてのみ、**S.API** の、**OB.DU** へのアクセスを許可しなければならない]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

*適用上の注釈:*

アプリケーション(S.API)は、一旦ユーザ・データ(OB.DU)を格納している暗号化ディスク(S.DISK)がアクティブになったら(S.DISK.STATUS = ACTIVATED)、このユーザ・データへのアクセスが明示的に許可される。

**FDP\_ACF.1.4:** TSF は、[割付: **S.DISK** が、**S.DISK.ID = OB.DU.DISK\_ID**、および **S.DISK.STATUS = DEACTIVATED**の場合は、**S.API**の、**OB.DU**へのアクセスを拒否しなければならない]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

*適用上の注釈:*

暗号化ディスク(S.DISK)がインアクティブ(S.DISK.STATUS = DEACTIVATED)にされている場合、いかなるアプリケーション(S.API)もその暗号化ディスクのユーザ・データ(OB.DU)にアクセスできてはならない。

### 5.2.2.3: FDP\_RIP - 残存情報保護

#### **FDP\_RIP.1 / サブセット残存情報保護**

**FDP\_RIP.1.1:** TSF は、[割付: マスタ鍵(OB.MASTER\_KEY)、ヘッダ鍵(OB.HEADER\_KEY)、認証データ(OB.VD)]のオブジェクト[選択:からの資源の割当て解除]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

*適用上の注釈:*

認証データはグローバル変数に格納され、アプリケーションが動作する際にメモリ領域が割り当てられる。認証データは、実際にはそのメモリ領域が開放されないとしても、使用する必要がなくなった時点でメモリから削除しなければ

ならない。

ヘッダ鍵はローカル変数に格納される。従ってヘッダ鍵はスタックに格納され削除される。

マスタ鍵の場合、メモリ領域はダイナミックに割り当てられる。従って割り当てを解除する際、TOE はデータがアクセス不可になることを保証しなければならない。

#### *適用上の注釈:*

この機能要件では、攻撃者にユーザ・データへのアクセスを許可してしまいかねない重要なデータの保護を保証している。また暗号鍵を安全に削除するための要件は、FCS クラスのコンポーネントで扱われている(暗号サポート)。

### **5.2.3. FIA クラス: 識別と認証**

本項では、ユーザより要求された識別を確立、管理する機能に関する要件を記述する。

正しいセキュリティ属性(例えば、身元、グループ、役割、セキュリティ・レベル、完全性など)がユーザに関連付けられることを保証するには、識別と認証が必要である。

曖昧なく許可ユーザを識別し、ユーザのセキュリティ属性をサブジェクトと正しく関連付けることは、規定されたセキュリティ方針の実施に不可欠である。このクラスファミリーには、ユーザの識別の決定と検証、TOE の使用に関する権限の決定、及び許可ユーザとセキュリティ属性との適切な関連付けなどが含まれる。

#### 5.2.3.1: FIA\_UID - 利用者識別

本項では、TSF を介する必要があるアクションを実施する前に、ユーザが自身の識別を要求される条件について記述する。

#### **FIA\_UID.1 / ディスク所有者 識別のタイミング**

**FIA\_UID.1.1 / ディスク所有者:** TSF は、利用者が識別される前に利用者を代行して実行される[割付: 新たなディスクの作成、アクティブなディスク上のデータの読み出しと書き込み、アクティブなディスクのプロパティの表示、TOE の各種設定の変更とアンマウント]を許可しなければならない。

**FIA\_UID.1.2 / ディスク所有者:** TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

#### *適用上の注釈:*

ユーザは、アクセスしたい「暗号化ディスク」を指定することにより TOE に識別される。このようにして、ユーザは「暗号化ディスク」の所有者、または正規のユーザとして識別される。ユーザは、格納されているデータにアクセスするために、「暗号化ディスク」を復号する権利があると主張する。

ユーザのパスワードは、既存の「暗号化ディスク」のマウント、認証データ(パスワードと鍵ファイル)の修正、またはヘッダ鍵を導出するアルゴリズム(PKCS#5 アルゴリズム)を変更する場合において要求される。

それ以外のアクションは、TOE への識別、または認証を要求されない。

#### 5.2.3.2: FIA\_UAU - 利用者認証

本項では、TSF が扱うユーザの認証メカニズムのタイプを明らかにする。このファミリでは、ユーザの認証メカニズムに基づく必要なセキュリティ属性も定義する。

#### **FIA\_UAU.1 / ディスク所有者 認証のタイミング**

**FIA\_UAU.1.1 / ディスク所有者:** TSF は、利用者が認証される前に利用者を代行して行われる[割付: **新たなディスクの作成、アクティブなディスク上のデータの読み出しと書き込み、アクティブなディスクのプロパティの表示、TOE の各種設定の変更とアンマウント**]を許可しなければならない。

**FIA\_UAU.1.2 / ディスク所有者:** TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

##### *適用上の注釈:*

ユーザの認証は、鍵ファイルに含まれる他のデータと組み合わせることもできるパスワードによって実行される。

ユーザのパスワードは、既存の「暗号化ディスク」のマウント、認証データ(パスワードと鍵ファイル)の修正、またはヘッダ鍵を導出するアルゴリズム(PKCS#5 アルゴリズム)を変更する場合において要求される。

それ以外のアクションは、TOE への識別、または認証を要求されない。

#### 5.2.3.3: FIA\_SOS - 秘密についての仕様

本項では、提供された秘密に品質尺度を適用し、その尺度に対応する秘密を生成するメカニズムに関する要件を定義する。

#### **FIA\_SOS.1 / パスワード 秘密の検証**

**FIA\_SOS.1.1 / パスワード** TSF は、秘密が[割付:**パスワードは 12 文字以上で構成される**]に合致することを検証するメカニズムを提供しなければならない。

##### *適用上の注釈:*

パスワードが作成される際には、ユーザには次のようなメッセージが表示される。

「適切なパスワードは、大文字、小文字、数字、@ ^ \$ \* + などの特殊文字を組み合わせたものである。20 文字以上(より長ければより良い)で構成されるパスワードを推奨する。パスワードの最大長は 64 文字である。」

しかしながら TOE がチェックするのは、単に選択されたパスワードが 12 文字(20 文字ではない)以上であるかどうかである。もしそれに違反した場合は警告メッセージが表示される。しかしこれを無視し、12 文字より短いパスワードを選択することも可能である。

#### 5.2.4. FMT クラス: セキュリティ管理

本項では、様々な TSF (セキュリティ属性、TSF データ、およびその機能) の管理的な側面を定義する。異なる管理役割とその相互作用、例えば権限の分離などが指定できる。

本項では、次のような要件がカバーされる:

- + TSF データの管理 (例えば、ユーザへのメッセージなど)。
- + セキュリティ属性の管理 (例えば、アクセス制御や権限リストなど)。
- + TSF 機能の管理 (例えば、機能の選択および TSF のふるまいに影響する規則や条件など)。
- + セキュリティ役割の定義。

##### 5.2.4.1: FMT\_MOF - TSF における機能の管理

本項では、TSF の管理機能の制御を許可されているユーザを定義する。

#### FMT\_MOF.1 / ディスク所有者 セキュリティ機能のふるまいの管理

**FMT\_MOF.1.1 / ディスク所有者:** TSF は、機能[割付:以下の表][選択: のふるまいを決定する]能力を[割付: ディスクを作成するユーザ(ディスク所有者)]に制限しなければならない。

暗号化	暗号アルゴリズムの選択 (AES、Twofish、など)
ハッシュ関数	暗号アルゴリズムの選択 (SHA-1、RIPEMD-160、など)
認証 (Authentication)	鍵ファイルの使用、鍵ファイルの生成、パスワードの導出、など

#### 適用上の注釈:

暗号アルゴリズムは、暗号化ディスク時に所有者によって選択される。これはそれ以降修正することはできない。

認証データは、暗号化ディスク作成時に所有者によって選択される。この場合は認証後であれば(そのときの認証データを入力し)変更できる。

ヘッダ鍵計算機能により使用されるハッシュ・アルゴリズムは、暗号化ディスク作成時に所有者により選択される。この場合も、認証後であれば変更できる。

##### 5.2.4.2: FMT\_MSA - セキュリティ属性の管理

本項では、許可ユーザにより管理されるセキュリティ属性について説明する。本セキュリティ・ターゲットにより識別されているセキュリティ属性は、次の表の通りである。

<b>S.DISK</b>	S.DISK.HEADER_STATUS S.DISK.STATUS S.DISK.ID
<b>OB.MASTER_KEY</b>	OB.MASTER_KEY.DISK_ID OB.MASTER_KEY.STATUS
<b>OB.DU</b>	OB.DU.DISK_ID
<b>OB.VD</b>	OB.VD.DISK_ID

### FMT\_MSA.2 / セキュアなセキュリティ属性

**FMT\_MSA.2.1:** TSF は、セキュアな値だけが[割付: **上記表の属性**]として受け入れられることを保証しなければならない。

*適用上の注釈:*

ディスクの ID は、一意でなければならない(2 つのディスクに同じ ID が設定されてはならない)。

S.DISK.HEADER\_STATUS、S.DISK.STATUS の値、および OB.MASTER\_KEY.STATUS のセキュリティ属性は曖昧さなく TOE の状態を識別しなければならない。

### FMT\_MSA.3 / 静的属性初期化

**FMT\_MSA.3.1:** TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択: **制限的**]デフォルト値を与える[割付: **SFP.TOE\_ACCESS\_CONTROL**]を実施しなければならない。

*適用上の注釈:*

デフォルト値には、次のような制限的な値が選択されなければならない。

- + S.DISK.STATUS = DEACTIVATED
- + S.DISK.HEADER STATUS = DEACTIVATED
- + OB.MASTER KEY.STATUS = DEACTIVATED

**FMT\_MSA.3.2:** TSF は、オブジェクトや情報が生成されるとき、[割付: **なし**]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

#### 5.2.4.3: FMT\_MTD - TSF データの管理

本項では、許可ユーザによる TSF データの管理に関する要件を考える。TSF データとして以下のデータが識別されている。

- + 認証データ(D.DONNEES\_AUTH)
- + ヘッド鍵(D.CLE\_ENTETE)
- + マスタ鍵(D.DLE\_MAITRE)

**FMT\_MTD.1 / 認証データ TSF データの管理**

**FMT\_MTD.1.1 / 認証データ:** TSF は、[割付: 認証データ]を[選択: 改変]する能力を[割付: ディスク所有者]に制限しなければならない。

*適用上の注釈:*

認証データを修正することができるのは、ディスクの所有者だけである。

**FMT\_MTD.1 / マスタ鍵 TSF データの管理**

**FMT\_MTD.1.1 / マスタ鍵:** TSF は、[割付: マスタ鍵(D.CLE\_MAITRE)]を[選択: 問い合わせ、生成]する能力を[割付: ディスク所有者]に制限しなければならない。

*適用上の注釈:*

ユーザがディスクを作成時、ディスクのフォーマットが開始されマスタ鍵が生成される。このマスタ鍵は、TOE の乱数生成器によって生成された一般的な乱数をベースにして生成される。

**FMT\_MTD.1 / ヘッド鍵 TSF データの管理**

**FMT\_MTD.1.1 / ヘッド鍵:** TSF は、[割付: ヘッド鍵(D.CLE\_ENTETE)]を[選択: 問い合わせ、改変]する能力を[割付: ディスクの所有者として認証されたユーザ]に制限しなければならない。

*適用上の注釈:*

ヘッド鍵は認証データと乱数生成器によって提供されたシードによって計算される。従って認証データを知っているディスクの所有者のみがヘッド鍵を生成することができる。ヘッド鍵を修正する場合、ユーザは、

- + 認証データ(パスワードと鍵ファイル)
- + ハッシュ・アルゴリズム

を修正すればよい。

上記データを修正するには、ユーザは認証されなければならない。認証データが修正されるたびに新たなシードが生成されるため、新たな認証データが以前のデータと同一であってもヘッド鍵は修正される。従って、ヘッド鍵は実際には認証データを変更しなくても修正できる。

**FMT\_MTD.2 / 認証データ TSF データにおける限界値の管理**

**FMT\_MTD.2.1 / 認証データ:** TSF は、[割付: 認証データ]に限界値を指定することを[割付: なし]に制限しなければならない。

*適用上の注釈:*

パスワードと鍵ファイルのサイズ制限は、ユーザのみが修正できる。

**FMT\_MTD.2.2 / 認証データ:** TSF は、TSF データが指示された限界値に達するか、それを超えた場合、以下のアクションをとらねばならない。:[割付: 以下参照]

\*パスワードに対して:

- + パスワード長が 0 の場合は、パスワードは拒否される。
- + パスワード長が 12 文字以下の場合、警告メッセージが表示される。
- + パスワード長が 64 文字以上の場合、最初の 64 文字のみが使用される。

\*鍵ファイルでは、1 メガバイトを超えた場合、最初の 1 メガバイトのみが使用される。

#### FMT\_MTD.3 / セキュアな TSF データ

**FMT\_MTD.3.1:** TSF は、[割付: 5.2.4.3 で指定された TSF データ]としてセキュアな値だけが受け入れられることを保証しなければならない。

*適用上の注釈:*

TSF データがセキュアであると判断されるには;

- + パスワードは、所定の条件を満たしていなければならない。特に TrueCrypt では、「適切なパスワードは、大文字、小文字、数字、@ ^ \$ \* + などの特殊文字を組み合わせたものである。20 文字以上(より長ければより良い)で構成されるパスワードを推奨する。パスワードの最大長は 64 文字である」である。
- + 使用するパスワードや鍵ファイルは、容易に推測できてはならない。
- + 使用される乱数生成器はセキュアでなければならない。
- + ヘッド鍵を導出するハッシュ・アルゴリズムはセキュアでなければならない。

#### 5.2.4.4: FMT\_SMF - 管理機能の特定

本項では、TOE によって提供される管理機能の仕様に関する要件について考える。TOE によって提供される管理機能には次のようなものがある。

- + セキュリティ属性の管理
- + TSF データの管理
- + セキュリティ機能の管理

この TOE の唯一の管理機能は、認証データを修正する機能である。

#### FMT\_SMF.1 / 管理機能の特定

**FMT\_SMF.1.1:** TSF は、以下の管理機能を実行することができなければならない。:[割付: パスワードと鍵ファイルの管理機能]

#### 5.2.4.5: FMT\_SMR - セキュリティの役割

本項では、ユーザにさまざまな役割を割り当てる際の要件について説明する。この TOE では、2 つのユーザ役割が識別されている: ディスクを所有するユーザ(または認証データを知っているユーザ)と、その他のユーザ。

#### FMT\_SMR.1 セキュリティの役割

**FMT\_SMR.1.1:** TSF は、役割[割付: ディスク所有者とその他のユーザ]を維持しなければならない。

**FMT\_SMR.1.2:** TSF は、利用者を役割に関連付けなければならない。

*適用上の注釈:*

ディスクに対応したパスワードによりユーザを認証することにより、TSF はユーザと役割を対応付ける(ディスクの所有者かどうか)ことができる。

### 5.2.5. FPT クラス:TSF の保護

本項では、TSF によって提供されるメカニズムの完全性と管理、および TSF データの完全性に関する要件を定義する。

#### 5.2.5.1: FPT\_FLS - フェールセキュア

ここでは TOE が常に、TSF におけるさまざまな障害が発生した際も、SFR を保証するための要件を定義する。

#### **FPT\_FLS.1 セキュアな状態を保持する障害**

**FPT\_FLS.1.1:** TSF は、以下の種別の障害が生じたときはセキュアな状態を保持しなくてはならない: [割付: 以下参照]。

- + ホスト・マシンのホット/ウォーム/コールド・リセット。
- + (電源断により)ホスト・コンピュータがオフになったとき。
- + ユーザが、ログ・オフを選択した場合。
- + パワー・セーブ・モードに移行。
- + スクリーン・セーバが開始された場合。

*適用上の注釈:*

セキュアな状態とは、特にユーザ・データへのアクセスを制御するセキュリティ属性の制限的な値に対応していなければならない。

- + S.DISK.STATUS = DEACTIVATED
- + S.DISK.HEADER\_STATUS = DEACTIVATED
- + OB.MASTER\_KEY.STATUS = DEACTIVATED

これらの値は、ディスクがアンマウントされておりこのディスクに格納されているデータを保護している鍵にアクセス不可な状態を示している。

以下のような事象が発生した場合においては、ディスクが自動的にアンマウントされるように設定することもできる。

- + ウィンドウズ・セッションの終了。
- + スクリーン・セーバの開始。
- + パワー・セーブ・モードに移行。
- + ユーザが設定した制限時間に達した場合(この時刻設定は「暗号化ディスク」ではなく、アプリケーションに対するものである)。

また、ディスクに格納されたファイルやディレクトリがウィンドウズのアプリケーションによってオープンされている場合でも、「暗号化ディスク」を強制的にアンマウントするかしないかを選択することもできる。

### 5.2.6. FRU クラス: 資源使用

本項では、リソースの可用性について考える。

#### 5.2.6.1: FRU\_FLT - 耐障害性

ここでは、リソースに所定の不具合が発生した場合でも、TOE が正確に機能することを保証するための要件を中心に説明する。

#### FRU\_FLT.1 / 機能削減された耐障害性

**FRU\_FLT.1.1:** TSF は、以下の障害[割付:以下のリスト]が生じたとき、[割付: **S.API** -> **DISMOUNT (S.DISK)**の操作]の動作を保証しなければならない。

- + ホスト・マシンのホット/ウォーム/コールド・リセット。
- + (電源断により)ホスト・コンピュータがオフになったとき。
- + ユーザが、ログ・オフを選択した場合。
- + パワー・セーブ・モードに移行。
- + スクリーン・セーバが開始された場合。

#### 適用上の注釈:

以下のような事象が発生した場合においては、ディスクが自動的にアンマウントされるように設定することもできる。

- + ウィンドウズ・セッションの終了。
- + スクリーン・セーバの開始。
- + パワー・セーブ・モードに移行。
- + ユーザが設定した制限時間に達した場合(この時刻設定は「暗号化ディスク」ではなく、アプリケーションに対するものである)。

また、ディスクに格納されたファイルやディレクトリがウィンドウズのアプリケーションによってオープンされている場合でも、「暗号化ディスク」を強制的にアンマウントするかしないかを選択することもできる。

## 5.3. セキュリティ保証要件

このセキュリティ・ターゲットが対象とする評価保証レベルは、EAL+2(または EAL2 追加)で、ADV\_FSP.4、ADV\_TDS.3、ADV\_IMP.1、ALC\_TAT.1、およびAVA\_VAN.3によって拡張される。

製品のユーザ・ガイドでは、ホスト・マシンのスタンバイ・モード、休止モード、およびこれらのモードで考えられるセキュリティ関連の問題に関する警告が提供されなければならない。

このユーザ・ガイドには、作成される可能性のある一時的なファイル(例えばキャッシュ・メモリに関する設定、機密性の高い情報を処理する場合の、ウィンドウズ XP のスワップ機能の無効化、など)管理に関する推奨策も含められ

ている。

## 5.4. 根拠

### 5.4.1. 保証要件

このセキュリティ・ターゲットが対象とする評価保証レベルは、EAL+2(またはEAL2追加)で、次のようなコンポーネントによって拡張される。

- + ADV\_FSP.4(ADV\_IMP.1コンポーネントを選択するためにはADV\_TDS.3の選択が要求され、ADV\_TDS.3の選択にはEAL2のADV\_FSP.2の代わりにADV\_FSP.4が要求される)
- + ADV\_TDS.3(ADV\_IMP.1コンポーネントを選択するためにはEAL2のADV\_TDS.1の代わりにADV\_TDS.3の選択が要求される)
- + ADV\_IMP.1
- + ALC\_TAT.1(ADV\_IMP.1とADV\_TDS.3コンポーネントの選択により、ADV\_TAT.1コンポーネントの選択が必要になる)
- + AVA\_VAN.3

CCにより要求される全ての保証コンポーネントの依存性は満たされている。

### 5.4.2. 機能要件

#### 5.4.2.1: TOEセキュリティ対策要件

#### **O.ARRET\_UTLISATEUR**

FDP\_ACC.1コンポーネントは、ユーザのデータへアクセスを不可にするとともに、「暗号化ディスク」のアンマウント(S.API -> DISMOUNT(S.DISK))を許可する、アクセス制御セキュリティ方針を識別する。

FDP\_ACF.1コンポーネントでは、アンマウント操作に関する制御方針に関し定義している。全てのユーザはディスクが既にマウント済みの場合(S.DISK.STATUS = MOUNTED)にのみ、このディスクをアンマウントできなければならない。

「暗号化ディスク」、および機密性の高いデータの所有者以外が、マスタ鍵または認証データを修正することができる場合ユーザは機密性の高いデータにもアクセスすることができるが、許可ユーザがそのアクセスを不可にすることもできる。

FDP\_RIP.1は、ディスクがアンマウントされているとき、鍵や認証データを再使用することができないことを確認する。もし鍵や認証データの痕跡が残されていると、攻撃者はそれを利用してユーザ・データにアクセスする可能性がある。

FCS\_CKM.4は、特に暗号鍵の削除を保証するコンポーネントである。

これらコンポーネントの集合は、セキュリティ対策要件(O.ARRET\_UTLIISATEUR)に完全に対応している。

## O. CRYPTO

FCS\_CKM.1 / ヘッダ鍵、および FCS\_CKM.1 / マスタ鍵のコンポーネントでは、暗号化鍵の管理に関するセキュリティ要件が定められている。いずれの要件でも、この鍵管理を実施する場合には、DCSSI暗号化フレームに対応する要件に適合すべきである旨が記載されている。

FCS\_CKM.3 / ヘッダ鍵、および FCS\_CKM.3 / マスタ鍵コンポーネントでは、暗号化鍵のアクセス手法に関する要件が定められている。ヘッダ鍵は認証データから導出され、マスタ鍵復号のためにヘッダがヘッダ鍵により復号される。いずれの要件でも、この鍵アクセス手法を実施する場合には、DCSSI暗号化フレームに対応する要件に適合すべきである旨が記載されている。

FCS\_CKM.4 コンポーネントには、機密性の高いデータの削除に関する要件が含まれている。

FCS\_COP.1 コンポーネントには、暗号化操作に関する要件が含まれている。DCSSI暗号化フレームは、暗号化操作が遵守しなければならない標準の一部である。

FMT\_MTD.3 コンポーネントでは、暗号化鍵がセキュアと見なすための要件を定義している。この要件を満たすには、その値はDCSSIの推奨に適合している値が望ましい。

これらコンポーネントの集合は、セキュリティ対策要件(O.CRYPTO)に完全に対応している。

## O.PROTECTION\_DES\_DONNEES\_ENREGISTREES

FDP\_ACC.1、および FDP\_ACF.1 コンポーネントは、セキュリティ方針とアクセス制御機能が、「暗号化ディスク」がマウント(S.DISK.STATUS = ACTIVATED)されている場合に限り、機密性の高いデータ(OB.DU オブジェクト)へのアクセスを許可するよう要求する。

FIA\_UAU.1 / ディスク所有者コンポーネントでは、事前の認証を要求する「暗号化ディスク」に対するアクションを規定する。特に「暗号化ディスク」をマウントするには、ユーザの認証が必要である。

FIA\_UID.1 / ディスク所有者コンポーネントではユーザの識別が考慮される。直接的な識別は存在しないが、「暗号化ディスク」を選択することにより、ユーザは「暗号化ディスク」をマウントする許可を与えられているユーザとして間接的に識別される。またこのコンポーネントは、FIA\_UAU.1 / ディスク所有者コンポーネントが要求する依存性を満たすことができる。

FIA\_SOS.1 / パスワードコンポーネントには、機密性の高いデータへのアクセスのための認証を行いアクセス制御するパスワードの品質を検証する要件が含まれている。FMT\_MTD.3 コンポーネントも、TSFデータである認証データが容易に推測することはできないセキュアな値を受け入れることを規定している。

FMT\_MTD.2 / 認証データコンポーネントでは、ユーザが認証データの仕様(文字数)を修正する権利を所有していないことを定めている。ただしこのコンポーネントの重要性は限定されている。パスワードには強い制約がなく、それを直接修正し既に作成済みのディスクに対応するように再生成することも可能である。

FMT\_MTD.1 / 認証データ、FMT\_MTD.1 / ヘッダ鍵、および FMT\_MTD.1 / マスタ鍵コンポーネントでは、許可ユーザのみが認証データを修正し、機密性の高いデータへのアクセスを制御するヘッダ鍵やマスタ鍵を取り出し、修正することができるよう規定する。

FMT\_MSA.2、および FMT\_MSA.3 コンポーネントには、セキュリティ方針で使用されるセキュリティ属性に関する

要件が明示されており、これらの属性により全てのユーザに対して機密性の高いデータへのアクセスが許可されないようになっている。

FMT\_MOF.1 / ディスク所有者コンポーネントでは、ディスク作成者のみが、機密性の高いデータを保護するために使用される暗号アルゴリズムと認証パラメタ(パスワードと鍵ファイル)を選択することができることを規定する。

FMT\_SMF.1 コンポーネントでは、格納されたデータへのアクセス制御に使用される認証パスワードを管理する機能について定めている。

FMT\_SMR.1 コンポーネントは、次のような 2 つの役割を区別することができる。

- + 「暗号化ディスク」の所有者は、認証パスワードを知っており、鍵ファイルを所有している。
- + その他のユーザ。格納されたデータの保護のために、ある特定のアクセスは「暗号化ディスク」の所有者のみに許可される。

これらコンポーネントの集合は、セキュリティ対策方針(O.PROTECTION\_DES\_DONNEES\_ENREGISTREES)に完全に対応する。

## O.ROBUSTESS

FPT\_FLS.1 コンポーネントは、システムの障害もしくは不具合が発生した場合でも、TSF がデータの機密性を保証し適切に動作し続けることを規定する。

このコンポーネントは、同種の変性を規定する FRU\_FLT.1 コンポーネントと密接に関係するが、FRU\_FLT.1 は重要な資産にのみ対応している。

これらコンポーネントの集合は、このセキュリティ対策要件(O.ROBUSTESS)に完全に対応する。

## O.CLE\_CHIFFREMENT

FCS\_CKM.1 / ヘッダ鍵、および FCS\_CKM.1 / マスタ鍵コンポーネントでは、それぞれ機密性の高いデータを暗号化するために使用されるヘッダ鍵とマスタ鍵の生成について定めている。

これらコンポーネントの集合は、このセキュリティ対策要件(O.CLE\_CHIFFREMENT)に完全に対応する。

### 5.4.3. セキュリティ対策方針と要件の対応表

セキュリティ対策方針	TOE の機能要件	根拠
O.ARRET_UTILISATEUR	FDP_ACF.1、FDP_ACC.1、 FDP_RIP.1、FCS_CKM.4	第 5.4.2.1 章
O.CRYPTO	FCS_CKM.1 / ヘッダ 鍵、 FCS_CKM.1 / マスタ 鍵、 FCS_CKM.3 / ヘッダ 鍵、 FCS_CKM.3 / マスタ 鍵、 FCS_CKM.4、FCS_COP.1、 FMT_MTD.3	第 5.4.2.1 章

O.PROTECTION_DES_DONNEES_ENREGISTREES	FDP_ACC.1、FDP_ACF.1、 FIA_UID.1 / ディスク所有者、 FIA_UAU.1 / ディスク所有者、 FIA_SOS.1 / パスワード、 FMT_MSA.2、FMT_MSA.3、 FMT_MTD.1 / ヘッダ鍵、 FMT_MOF.1 / ディスク所有者、 FMT_SMF.1、 FMT_SMR.1、FMT_MTD.1 / 認証データ、 FMT_MTD.1 / マスタ鍵、 FMT_MTD.2 / 認証データ、 FMT_MTD.3	第 5.4.2.1 章
O.ROBUSTESS	FRU_FLT.1、FPT_FLS.1	第 5.4.2.1 章
O.CLE_CHIFFREMENT	FCS_CKM.1 / ヘッダ鍵、 FCS_CKM.1 / マスタ鍵、 FMT_MTD.3	第 5.4.2.1 章

表 7: TOE 機能要件に対するセキュリティ対策方針

TOE 機能要件	セキュリティ対策方針
FCS_CKM.1 / ヘッダ鍵	O.CRYPTO、O.CLE_CHIFFREMENT
FCS_CKM.1 / マスタ鍵	O.CRYPTO、O.CLE_CHIFFREMENT
FCS_CKM.3 / ヘッダ鍵	O.CRYPTO
FCS_CKM.3 / マスタ鍵	O.CRYPTO
FCS_CKM.4	O.ARRET_UTILISATEUR、O.CRYPTO
FCS_COP.1	O.CRYPTO
FDP_ACC.1	O.ARRET_UTILISATEUR、 O.PROTECTION_DES_DONNES_ENREGISTREE
FDP_ACF.1	O.ARRET_UTILISATEUR、 O.PROTECTION_DES_DONNES_ENREGISTREE
FDP_RIP.1	O.ARRET_UTILISATEUR
FIA_UID.1 / ディスク所有者	O.PROTECTION_DES_DONNES_ENREGISTREE
FIA_UAU.1 / ディスク所有者	O.PROTECTION_DES_DONNES_ENREGISTREE
FIA_SOS.1 / パスワード	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_MOF.1 / ディスク所有者	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_MSA.2	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_MSA.3	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_MTD.1 / 認証データ	O.PROTECTION_DES_DONNES_ENREGISTREE

FMT_MTD.1 / マスタ鍵	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_MTD.1 / ヘッダ鍵	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_MTD.2 / 認証データ	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_MTD.3	O.CRYPTO、 O.PROTECTION_DES_DONNES_ENREGISTREE、 O.CLE_CHIFFREMENT
FMT_SMF.1	O.PROTECTION_DES_DONNES_ENREGISTREE
FMT_SMR.1	O.PROTECTION_DES_DONNES_ENREGISTREE
FPT_FLS.1	O.ROBUSTESSE
FRU_FLT.1	O.ROBUSTESSE

表 8: セキュリティ対策方針に対する TOE 機能要件

## 5.5. 依存性

### 5.5.1. セキュリティ機能要件の依存性

TOE セキュリティ機能要件	CC の依存性	依存性を満たす要件
FCS_CKM.1 / ヘッダ鍵	(FCS_COP.1 または FCS_CKM.2)、 (FCS_CKM.4)、および (FMT_MSA.2)	FCS_CKM.4、FCS.COP.1、 FMT_MSA.2
FCS_CKM.1 / マスタ鍵	(FCS_COP.1 または、 FCS_CKM.2)、 (FCS_CKM.4)、および (FMT_MSA.2)	FCS_CKM.4、FCS.COP.1、 FMT_MSA.2
FCS_CKM.3 / ヘッダ鍵	(FDP_ITC.1 または、 FCS_CKM.1)、 (FCS_CKM.4)、および (FMT_MSA.2)	FCS_CKM.1 / ヘッダ鍵、 FCS.CKM.4、および FMT_MSA.2
FCS_CKM.3 / マスタ鍵	(FDP_ITC.1 または、 FCS_CKM.1)、 (FCS_CKM.4)、および (FMT_MSA.2)	FCS_CKM.1 / ヘッダ鍵、 FCS.CKM.4、および FMT_MSA.2
FCS_CKM.4	(FDP_ITC.1 または、 FCS_CKM.1)、 (FCS_CKM.4)、および (FMT_MSA.2)	FCS_CKM.1 / ヘッダ鍵、FMT_MSA.2
FCS_COP.1	(FDP_ITC.1 または、 FCS_CKM.1)、 (FCS_CKM.4)、および (FMT_MSA.2)	FCS_CKM.1 / ヘッダ鍵、 FCS.CKM.4、および FMT_MSA.2
FDP_ACC.1	(FDP_ACF.1)	FDP_ACF.1
FDP_ACF.1	(FDP_ACC.1)、および (FMT_MSA.3)	FDP_ACC.1、FMT_MSA.3
FDP_RIP.1	依存性はなし	

FIA_UID.1 / ディスク所有者	依存性はなし	
FIA_UAU.1 / ディスク所有者	(FIA_UID.1)	FIA_UID.1 / ディスク所有者
FIA_SOS.1 / パスワード	依存性はなし	
FMT_MOF.1 / ディスク所有者	(MFT_SMF.1)、および (FMT_SMR.1)	FMT_SMF.1、FMT_SMR.1
FMT_MSA.2	(ADV_SPM.1)、および (FDP_IFC.1 または、 FDP_ACC.1)、 (FMT_MSA.1)、および (FMT_SMR.1)	FDP_ACC.1、および FMT_SMR.1
FMT_MSA.3	(FMT_MSA.1)、および (FMT_SMR.1)	FMT_SMR.1
FMT_MTD.1 / 認証データ	(FMT_SMF.1)、および (FMT_SMR.1)	FMT_SMF.1、FMT_SMR.1
FMT_MTD.1 / マスタ鍵	(FMT_SMF.1)、および (FMT_SMR.1)	FMT_SMF.1、FMT_SMR.1
FMT_MTD.1 / ヘッド鍵	(FMT_SMF.1)、および (FMT_SMR.1)	FMT_SMF.1、FMT_SMR.1
FMT_MTD.2 / 認証データ	(FMT_MTD.1)、および (FMT_SMR.1)	FMT_MTD.1 / 認 証 デ ー タ 、 FMT_SMR.1
FMT_MTD.3	(FMT_MTD.1)	FMT_MTD.1 / 認証データ、 FMT_MTD.1 / マスタ鍵、 FMT_MTD.1 / ヘッド鍵
FMT_SMF.1	依存性はなし	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1 / ディスク所有者
FPT_FLS.1	依存性はなし	
FRU_FLT.1	(FPT_FLS.1)	FPT_FLS.1

表 9: 機能要件の依存性

## 5.5.1.1: 依存性が満たされない根拠

**FMT\_MSA.2** から **FMT\_MSA.1**、および **FMT\_MSA.3** から **FMT\_MSA.1** の依存性は満たされない。管理者役割やユーザ役割がなく、セキュリティ属性に直接アクセスできる役割はない。これらのセキュリティ属性は、セキュリティ機能により自動的に定義される。

従って、セキュリティ属性にアクセス可能なユーザを識別する **FMT\_MSA.1** コンポーネントは不要である。

## 5.5.2. セキュリティ保証要件の依存性

要件	CC の依存性	依存性を満たす要件
ADV_IMP.1	(ADV_TDS.3)、および (ALC_TAT.1)	ADV_TDS.3、および ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4

ALC_DVS.1	依存性はなし	
ALC_FLR.3	依存性はなし	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ADV_ARC.1	(ADV_FSP.1)、および(ADV_TDS.1)	ADV_TDS.3、および ADV_FSP.4
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	依存性はなし	
ALC_CMC.2	(ALC_CMS.1)	ALC_CMS.2
ALC_CMS.2	依存性はなし	
ALC_DEL.1	依存性はなし	
ASE_CCL.1	(ASE_ECD.1)、(ASE_INT.1)、および(ASE_REQ.1)	ASE_ECD.1、ASE_INT.1、および ASE_REQ.2
ASE_ECD.1	依存性はなし	
ASE_INT.1	依存性はなし	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1)、および(ASE_OBJ.1)	ASE_ECD.1、および ASE_OBJ.2
ASE_SPD.2	依存性はなし	
ASE_TSS.1	(ASE_INT.1)、および(ASE_REQ.1)	ASE_INT.1、ASE_REQ.2
ATE_COV.1	(ADV_FDP.2)、および(ATE_FUN.1)	ADV_FDP.2、ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.1
ATE_IND.2	(ADV_FSP.2)、(AGD_OPE.1)、(AGD_PRE.1)、および(ATE_FUN.1)	ADV_FSP.4、AGD_OPE.1、AGD_PRE.1、および ATE_FUN.1
AVA_VAN.3	(ADV_ARC.1)、(ADV_FSP.2)、(ADV_IMP.1)、(ADV_TDS.3)、(AGD_OPE.1)、および(AGD_PRE.1)	ADV_IMP.1、ADV_TDS.3、ADV_ARC.1、ADV_FSP.4、AGD_OPE.1、および AGD_PRE.1

表 10: 保証要件の依存性

## 6. TOE 要約仕様

---

### 6.1. TOE セキュリティ機能

#### 6.1.1. 暗号化操作

##### **SF.RANDOM\_GEN**

このセキュリティ機能は、乱数生成を実現する。乱数生成器は、暗号化のマスタ鍵、二次鍵(LRW モード)、ロード、および鍵ファイルを生成するために使用される。

##### **SF.MASTER\_KEY\_GEN**

このセキュリティ機能は、ディスクのマスタ鍵の生成を実現する。

##### **SF.CIPHERING**

このセキュリティ機能は、暗号鍵と「暗号化ディスク」に対応するアルゴリズムを使用し事前にマウントされた「暗号化ディスク」上への暗号化されたデータの書き込みを実現する。

##### **SF.DECIPHERING**

このセキュリティ機能は、暗号鍵と「暗号化ディスク」に対応するアルゴリズムを使用し事前にマウントされた「暗号化ディスク」上への暗号化されたデータの読み込みを実現する。

##### **SF.HASH\_CALC**

このセキュリティ機能は、「暗号化ディスク」に対応するハッシュ計算アルゴリズムに基づき、「暗号化ディスク」に関連するデータのハッシュ計算を実現する。

##### **適用上の注釈:**

このセキュリティ機能は、乱数生成器と PKCS#5 標準に基づいたヘッダ鍵導出関数の双方に使用される。

#### 6.1.2. アクセス制御

##### **SF.PLAUSIBLE\_DENIABILITY**

このセキュリティ機能は、隠し「暗号化ディスク」と、この隠し「暗号化ディスク」を判別可能な特徴がないことに基づき、信頼できる見せ掛けのシステムを作ることを可能とする。

隠し「暗号化ディスク」の原理は、TrueCrypt「暗号化ディスク」(の空き領域内)の中にもう一つに TrueCrypt「暗号化ディスク」を作成することである。外殻「暗号化ディスク」がマウントされている場合でも、隠し「暗号化ディスク」がその内部にあるかどうかを証明することは不可能である。隠し「暗号化ディスク」のパスワードは、外殻「暗号化ディスク」のパスワードと同じではない。

## SF.PASSWORD\_MGT

このセキュリティ機能によって、許可ユーザは自身のパスワードはもとより、パスワードに関連付けられた「鍵ファイル」を管理することができる。

- + 「暗号化ディスク」を作成する際のパスワードの生成、
- + パスワードの修正、
- + パスワードの品質管理、
- + 鍵ファイルの管理。

鍵ファイルとは、その内容がパスワードと組み合わせられるファイルである。鍵ファイルの使用はオプションである。ユーザが鍵ファイルの使用を選択した場合、「暗号化ディスク」はパスワードと適切な「鍵ファイル」が TOE に提示されるまでマウントすることはできない。

このセキュリティ機能は、ユーザがどの鍵ファイルを使用するか決定することを可能とし、ユーザが要求すればそれを生成することもできる。

## SF.MASTER\_KEY\_ACCESS

このセキュリティ機能は、PKCS#5 標準をベースにユーザの認証データからヘッダ鍵の導出を行う。次にこのヘッダ鍵は、マスタ鍵を含むヘッダに含まれるデータへのアクセスを可能にする。

### 6.1.3. 暗号化されたディスクの管理

## SF.DISK\_CREATION

このセキュリティ機能は、「暗号化ディスク」の作成を可能にする。

- + 割り当てられたメモリ・ゾーンをフォーマットする。
- + 設定時に「クイック・フォーマット」が選択されている場合には、この「暗号化ディスク」は、フォーマットされラダムデータで上書きされる。
- + マスタ鍵を含むヘッダが生成される。

## SF.DISMOUNT

このセキュリティ機能は、ユーザの要求により「暗号化ディスク」のアンマウントを許可する。

## SF.AUTO\_DISMOUNT

このセキュリティ機能は、次のような事象が発生した場合、既にマウント済みの「暗号化ディスク」を自動的にアンマウントできる。

- + OS の停止
- + 電源断

設定を適切に行えば、このセキュリティ機能は次のような事象が発生した場合、「暗号化ディスク」をアンマウント

することができる。

- + ウィンドウズ・セッションの終了
- + スクリーン・セーバの開始
- + パワー・セーブ・モードに移行
- + ユーザの設定時間が経過後(この時間は「暗号化されたディスク」ではなく、アプリケーションに対応している)

「暗号化ディスク」にウィンドウズのアプリケーションによって開かれたファイルやディレクトリが含まれる場合でも、この「暗号化ディスク」を強制的にアンマウントすることもできる。

## SF.DISK\_MGT

このセキュリティ機能は、「暗号化ディスク」がマウントされている場合のリストを管理する。この管理機能にはマウントされたディスクのリストへの追加と、ディスクがアンマウントされた場合のそれらの削除が含まれる。

### 6.1.4. TOE データの保護

## SF.CLEANNING

このセキュリティ機能は、保護されていない領域に一時的に格納された機密性の高いデータの削除を可能にする。例えば、RAM に含まれるパスワードはオペレーティング・システムの SWAP 領域にスワップアウトされる可能性がある。

この機能は、「暗号化ディスク」がアンマウントされると、キャッシュ領域のパスワードを削除するために自動的に呼び出される。

### 適用上の注釈:

このキャッシュとは、ドライバがロードされると(グローバル変数として)静的に割り当てられたメモリ領域のことである。キャッシュには、メモリ領域をロックする特別な機能は使われない。従ってこのキャッシュは、SWAP にスワップアウトされる可能性がある。

## SF.DATA\_LOCK

このセキュリティ機能は、機密性の高いデータを含むことがあるメモリをロックすることができる(例えば、RAM の内容をオペレーティング・システムの SWAP ファイルにスワップアウトすべきではない)。

### 注:

「TrueCrypt.exe」、および「TrueCrypt Format.exe」実行ファイルでは、VirtualLock API がこれに対応する。

TrueCrypt.sys ドライバでは、「ExAllocatePoolWithTag」メモリ割り当て関数の「NonPagedPool」パラメタに対応する。

## 6.2. TOE 要約仕様と機能要件との対応付け

### 6.2.1. 対応表

機能要件	TOE セキュリティ機能	根拠
FCS_CKM.1 / ヘッド鍵	SF.MASTER_KEY_ACCESS、SF.HASH_CALC	第 6.2.2 章
FCS_CKM.1 / マスタ鍵	SF.RANDOM_GEN、SF.MASTER_KEY_GEN、 SF.HASH_CALC	第 6.2.2 章
FCS_CKM.3 / ヘッド鍵	SF.MASTER_KEY_ACCESS	第 6.2.2 章
FCS_CKM.3 / マスタ鍵	SF.MASTER_KEY_ACCESS	第 6.2.2 章
FCS_CKM.4	SF.CLEANNING	第 6.2.2 章
FCS_COP.1	SF.CIPHERING、SF.DECIPHERING、 SF.HASH_CALC	第 6.2.2 章
FDP_ACC.1	SF.MASTER_KEY_ACCESS、SF.DISMOUNT、 SF.AUTO_DISMOUNT、 SF.PLAUSIBLE_DENIABILITY、SF.DATA_LOCK	第 6.2.2 章
FDP_ACF.1	SF.MASTER_KEY_ACCESS、SF.DISMOUNT、 SF.AUTO_DISMOUNT、 SF.PLAUSIBLE_DENIABILITY、SF.DATA_LOCK	第 6.2.2 章
FDP_RIP.1	SF.CLEANINNG	第 6.2.2 章
FIA_UID.1 / ディスク所有者	SF.MASTER_KEY_ACCESS	第 6.2.2 章
FIA_UAU.1 / ディスク所有者	SF.MASTER_KEY_ACCESS、 SF.PLAUSIBLE_DENIABILITY	第 6.2.2 章
FIA_SOS.1 / パスワード	SF.PASSWORD_MGT	第 6.2.2 章
FMT_MOF.1 / ディスク所有者	SF.DISK_CREATION、SF.PASSWORD_MGT	第 6.2.2 章
FMT_MSA.2	SF.DISK_CREATION	第 6.2.2 章
FMT_MSA.3	SF.DISK_CREATION	第 6.2.2 章
FMT_MTD.1 / 認証データ	SF/PASSWORD_MGT	第 6.2.2 章
FMT_MTD.1 / マスタ鍵	SF.MASTER_KEY_ACCESS	第 6.2.2 章
FMT_MTD.1 / ヘッド鍵	SF/PASSWORD_MGT、 SF.MASTER_KEY_ACCESS	第 6.2.2 章
FMT_MTD.2 / 認証データ	SF.PASSWORD_MGT	第 6.2.2 章
FMT_MTD.3	SF.RANDOM_GEN、SF.MASTR_KEY_GEN、 SF.PASSWORD_MGT、 SF.MASTER_KEY_ACCESS	第 6.2.2 章
FMT_SMF.1	SF.PASSWORD_MGT	第 6.2.2 章
FMT_SMR.1	SF.MASTER_KEY_ACCESS、	第 6.2.2 章

	SF.DISK_CREATION	
FPT_FLS.1	SF.AUTO_DISMOUNT、SF.DISK_MGT	第 6.2.2 章
FRU_FLT.1	SF.AUTO_DISMOUNT、SF.DISK_MGT	第 6.2.2 章

表 11: セキュリティ機能に対する機能要件

TOE セキュリティ機能	機能要件
SF.RANDOM_GEN	FCS_CKM.1 / マスタ鍵、FMT_MTD.3
SF.MASTER_KEY_GEN	FCS_CKM.1 / マスタ鍵、FMT_MTD.3
SF.CIPHERING	FCS_COP.1
SF.DECIPHERING	FCS_COP.1
SF.HASH_CALC	FCS_CKM.1 / ヘッダ鍵、FCS_CKM.1 / マスタ鍵、 FCS_COP.1
SF.PLAUSIBLE_DENIABILITY	FDP_ACC.1、FDP_ACF.1、FIA_UAU.1 / ディスク所有者
SF.PASSWORD_MGT	FIA_SOS.1 / パスワード、FMT_MOF.1 / ディスク所有者、 FMT_MTD.1 / 認証データ、FMT_MTD.1 / ヘッダ鍵、 FMT_MTD.2 / 認証データ、FMT_MTD.3、FMT_SMF.1
SF.MASTER_KEY_ACCESS	FCS_CKM.1 / ヘッダ鍵、FCS_CKM.3 / ヘッダ鍵、 FCS_CKM.3 / マスタ鍵、FDP_ACC.1、FDP_ACF.1、 FIA_UID.1 / ディスク所有者、FIA_UAU.1 / ディスク所有者、 FMT_MTD.1 / マスタ鍵、FMT_MTD.1 / ヘッダ鍵、 FMT_MTD.3、FMT_SMR.1
SF.DISK_CREATION	FMT_MOF.1 / ディスク所有者、FMT_MSA.2、 FMT_MSA.3、FMT_SMR.1
SF.DISMOUNT	FDP_ACC.1、FDP_ACF.1
SF.AUTO_DISMOUNT	FDP_ACC.1、FDP_ACF.1、FPT_FLS.1、FRU_FLT.1
SF.DISK_MGT	FPT_FLS.1、FRU_FLT.1
SF.CLEANNING	FCS_CKM.4、FDP_RIP.1
SF.DATA_LOCK	FDP_ACC.1、FDP_ACF.1

表 12: 機能要件に対するセキュリティ機能

### 6.2.2. 根拠

TOE 要約仕様の根拠は、SFR が TOE のセキュリティ機能により対応されていることを検証する。

#### 6.2.2.1: FCS クラス:暗号サポート

##### FCS-CKM - 暗号鍵管理

**FCS\_CKM.1 / ヘッダ鍵:** マスタ鍵へのアクセスを可能にするヘッダ鍵生成のプロセスは、セキュリティ機能 SF.MASTER\_KEY\_ACCESS により総合的に管理される。このセキュリティ機能自体は、ハッシュ計算を実行



**FCS\_CKM.1 / マスタ鍵:** 以下のセキュリティ機能を組み合わせることにより、この要件に準拠するマスタ鍵生成が保証される。

- + SF.MASTER\_KEY\_GEN では、乱数生成器を使用し鍵を生成する。
- + SF.RANDOM\_GEN は、SF.HASH\_CALC と共に乱数を生成する。

**FCS\_CKM.3 / ヘッド鍵:** マスタ鍵のアクセス制御のため、セキュリティ機能 SF.MASTER\_KEY\_ACCESS は、まずヘッド鍵へのアクセスを制御する。実際このセキュリティ機能では、認証データからヘッド鍵を導出する計算を実施する。従って、この認証データが正しくなければ、ヘッドを復号するヘッド鍵を正しく算出することができない。この場合、ヘッド鍵へのアクセスは失敗となる。

**FCS\_CKM.3 / マスタ鍵:** セキュリティ機能 SF.MASTER\_KEY\_ACCESS は、事前のヘッド鍵の計算を通してマスタ鍵へのアクセスを制御する。ヘッド鍵は認証データより導出される。従って認証データが正しくなければ、ヘッドを復号するヘッド鍵を正しく算出することができない。ヘッドを復号することができないため、このヘッドに含まれるマスタ鍵へのアクセスは不可能となる。

**FCS\_CKM.4:** SF.CLEANNING のセキュリティ機能は、セキュアな機密性の高いデータ削除を可能とする。この機能は暗号鍵の削除を対象とする。

#### *FCS\_COP - 暗号操作*

**FCS\_COP.1:** 暗号操作は、このSFRの要件に対応するSF.CIPHERING、SF.DECIPHERING、およびSF.HASH\_CALCにより実現される。

#### **6.2.2.2: FDP クラス:利用者データ保護**

##### *FDP\_ACC - アクセス制御方針*

**FDP\_ACC.1:** 次のようなセキュリティ機能によって、アクセス制御が実現される。

- + SF.MASTER\_KEY\_ACCESS は、ヘッド鍵へのアクセスを制御する。それにより機密性の高いデータを復号するマスタ鍵へのアクセスが制御される。
- + SF.DISMOUNT、およびSF.AUTO\_DISMOUNT は、ユーザの要求、もしくはあるイベント(電源断、オペレーション・システムのシャット・ダウン等)に基づき自動的に、アクセスを拒絶する。
- + SF.PLAUSIBLE\_DENIABILITY は、「暗号化ディスク」所有者に対し、隠し「暗号化ディスク」に基づく補足的なアクセス制御を提供する。すなわち、機密性の高い情報が漏えいされるリスクを伴わずに、攻撃者に対し「セキュリティ」(外殻「暗号化ディスク」)パスワードを提供することができる。従って、このセキュリティ機能は機密性の高いデータが格納される隠し「暗号化ディスク」のアクセス制御にも関わっている。
- + SF.DATA\_LOCK は、セキュリティが確保されていない領域にデータを格納することを禁じ、機密性の高いデータへのアクセスを阻止することを可能とする。

*FDP\_ACF* - アクセス制御機能

**FDP\_ACF.1**: 次のようなセキュリティ機能によって、アクセス制御が実現される。

- + SF.MASTER\_KEY\_ACCESS は、ヘッダ鍵へのアクセスを制御する。それにより機密性の高いデータを復号するマスタ鍵へのアクセスが制御される。
- + SF.DISMOUNT、および SF.AUTO\_DISMOUNT は、ユーザの要求、もしくはあるイベント(電源断、オペレーション・システムのシャット・ダウン等)に基づき自動的に、アクセスを拒絶する。
- + SF.PLAUSIBLE\_DENIABILITY は、「暗号化ディスク」所有者に対し、隠し「暗号化ディスク」に基づく補足的なアクセス制御を提供する。すなわち、機密性の高い情報が漏えいされるリスクを伴わずに、攻撃者に対し「セキュリティ」(外殻「暗号化ディスク」)パスワードを提供することができる。従って、このセキュリティ機能は機密性の高いデータが格納される隠し「暗号化されたディスク」のアクセス制御にも関わっている。
- + SF.DATA\_LOCK は、セキュリティが確保されていない領域にデータを格納することを禁じ、機密性の高いデータへのアクセスを阻止することを可能とする。

*FDP\_RIP* - 残存情報保護

**FDP\_RIP.1**: SF.CLEANNING のセキュリティ機能は、セキュリティが確保されていない領域に一時的に格納される機密性の高いデータの削除を可能にする。暗号鍵や認証データが機密性の高いデータと見なされる。

**6.2.2.3: FIA クラス** - 識別と認証*FIA\_UID* - 利用者識別

**FIA\_UID.1 / ディスク所有者**: ユーザに自身の識別を明示的に要求するセキュリティ機能はない。ただし、ユーザが「暗号化ディスク」をマウントするよう要求した場合、このユーザは自身をディスクの正規ユーザとして識別されることになる。従って、セキュリティ機能 SF.MASTER\_KEY\_ACCESS 認証前の「暗号化ディスク」の選択が識別に相当する。

*FIA\_UAU* - 利用者認証

**FIA\_UAU.1 / ディスク所有者**: パスワードや関連する鍵ファイルが要求される認証は、セキュリティ機能 SF.MASTER\_KEY\_ACCESS により実施される。これらのデータ(パスワードや鍵ファイル)は、ヘッダ鍵を導出するために使用される。マスタ鍵の復号が成功すればヘッダ鍵が正しかったことになり、パスワードや鍵ファイルも同様となる。

直接ではないが、SF.PLAUSIBLE\_DENIABILITY も、ユーザの識別と認証に関与していると考えることができる。実際、このセキュリティ機能は攻撃者の識別に有効である。攻撃者とは、機密性の高いデータへのアクセスを許可されていないが、「有効な」(外殻「暗号化ディスク」)パスワードを入手したユーザである。

*FIA\_SOS* - 秘密についての仕様

**FIA\_SOS.1 / パスワード**: このセキュリティ要件は、新規パスワードの品質を検証し、それによりパスワードを登

録、および修正することができるセキュリティ機能 SF.PASSWORD\_MGT により、完全に対応されている。

#### 6.2.2.4: FMT クラス: セキュリティ管理

##### *FMT\_MOF - TSF における機能の管理*

**FMT\_MOF.1 / ディスク所有者:** 暗号化のアルゴリズムは、セキュリティ機能 SF.DISK\_CREATION を使用しディスクを作成するユーザ、すなわちディスクの所有者が、「暗号化ディスク」を作成したときに選択される。

セキュリティ機能 SF.PASSWORD\_MGT は、ユーザが認証されたあとの認証データの修正を許可しない。従って、「暗号化ディスク」に関連のパスワードを持っていないユーザが、この認証データを修正することは不可能である。

##### *FMT\_MSA - セキュリティ属性の管理*

**FMT\_MSA.2:** セキュリティ属性は、「暗号化ディスク」が作成されたときに割り当てられる。この「暗号化ディスク」は、セキュリティ機能 SF.DISK\_CREATION により作成される。この機能は属性値がセキュアな値となることを保証する。

**FMT\_MSA.3:** セキュリティ属性は、「暗号化ディスク」が作成されたときに割り当てられる。この「暗号化ディスク」の作成は、デフォルトの属性値がアクセス制御方針に関連する制限的な値であることを保証するセキュリティ機能 SF.DISK\_CREATION により作成される。またこれらのデフォルト値は、TOE によって固定されるためユーザが修正することはできない。

##### *FMT\_MTD - TSF データの管理*

**FMT\_MTD.1 / 認証データ:** セキュリティ機能 SF.PASSWORD\_MGT は、認証データを修正する許可を得ているユーザを確認することができる。

**FMT\_MTD.1 / マスタ鍵:** セキュリティ機能 SF.MASTER\_KEY\_ACCESS は、マスタ鍵へのアクセスが許可されているユーザを確認することができる。認証データを所有するユーザのみが、マスタ鍵へのアクセスを許可するヘッダ鍵を生成することができる。

**FMT\_MTD.1 / ヘッダ鍵:** セキュリティ機能 SF.PASSWORD\_MGT では、事前認証(旧パスワードの要求)により、「暗号化ディスク」に対応する認証データの修正が、「暗号化されたディスク」の所有者のみ許可されることを保証する。

セキュリティ機能 SF.MASTER\_KEY\_ACCESS は、ヘッダ鍵が認証データから計算されることを保証する。

**FMT\_MTD.2 / 認証データ:** SF.PASSWORD\_MGT の認証データの管理機能では、認証データの制限値(パスワードと鍵ファイルのサイズ)に関する要件を特に考慮しなければならない。

**FMT\_MTD.3:** この機能要件では、TSF データがセキュアであることを要求する。

- + セキュリティ機能 SF.RANDOM\_GEN は、乱数の生成に関与している。これらの乱数は、TSF データである暗号鍵や鍵ファイルの生成に使用される。従って、この乱数生成器は、セキュリティが確保された乱数を生成すると見なされる統計的に正しい性質を所有していなければならない。

- + セキュリティ機能 SF.MASTER\_KEY\_GEN は、セキュアと見なされる正しい暗号化の属性を保持しなければならないマスタ鍵の生成に参与している。
- + セキュリティ機能 SF.PASSWORD\_MGT は、認証データの管理に参与している。セキュアと見なされるには、この認証データは、特に、容易に推測できてはならない。
- + セキュリティ機能 SF.MASTER\_KEY\_ACCESS は、(ランダムに生成された)シードと認証データから生成されるヘッダ鍵に参与している。この鍵のセキュアと見なされるためには次のような条件が必要である。
  - \* 入力データ(シードと認証データ)がセキュアと見なされる。
  - \* 特に、PKCS#5 v2.0 に準拠する導出メカニズム(仕様と実装)がセキュアと見なされる。

#### *FMT\_SMF* - 管理機能の特定

**FMT\_SMF.1:** パスワードの管理機能は、セキュリティ機能 SF.PASSWORD\_MGT によって保証される。

#### *FMT\_SMR* - セキュリティ管理役割

**FMT\_SMR.1:** この機能では、2通りのユーザ・タイプが識別される。この2通りのタイプは、SFRで識別される2通りの役割に対応している。一方が、パスワードを所有する「暗号化ディスク」の所有者であり、もう一方はその他のユーザである。

これらの2通りの役割は次のような方法で、TOEによって管理されている。ディスクを認証するためのパスワード所有者は、ディスク所有者として識別される。パスワードを持っていない者はその他のユーザと見なされる。

従って、

- + セキュリティ機能 SF.DISK\_CREATION により「暗号化ディスク」が作成されると、ユーザはパスワードを選択し「暗号化ディスク」の所有者となる。
- + セキュリティ機能 SF.MASTER\_KEY\_ACCESS は、正常に認証されたユーザにディスク所有者の役割を割り当てることができる。

#### **6.2.2.5: FPT クラス:TSF の保護**

##### *FPT\_FLS* - フェールセキュア

**FPT\_FLS.1:** セキュリティ機能 SF.AUTO\_DISMOUNT は、障害時において、マウントされている全ての「暗号化ディスク」を、自動的にアンマウントすることができる。この自動的なアンマウント機能により対象となる全ての S.DISK が、S.DISK.STATUS = DESACTIVATED となるセキュアな状態になる。

#### **6.2.2.6: FRU クラス:資源利用**

##### *FRU\_FLT* - 耐障害性

**FRU\_FLT.1:** セキュリティ機能 SF.AUTO\_DISMOUNT は、不具合、または障害時でも「暗号化ディスク」をアンマウントすることができる。

## 付録 A 定義と頭字語

---

付録 A では、本書で使用されている主な用語を定義する。コモン・クライテリア(CC)で使用されている用語については、第 4 章の「CC1」を参照のこと。

### 6.3. 略語と頭字語

CC	コモン・クライテリア(Common Criteria)
EAL	評価保証レベル(Evaluation Assurance Level)
IT	情報技術(Information Technology)
OS	オペレーティング・システム(Operating System)
OSP	組織的なセキュリティ方針(Organizational Security Policy)
PP	プロテクション・プロファイル(Protection Profile)
SF	セキュリティ機能(Security Function)
SFR	セキュリティ機能要件(Security Function Requirement)
ST	セキュリティ・ターゲット(Security Target)
TOE	評価対象(Target of Evaluation)

### 6.4. 定義

#### 評価対象(TOE)

評価の対象となる製品とそれに関連する一連の文書。

#### セキュリティ・ターゲット(ST)

TOE 評価の対象を記載した文書。評価対象の要件に適合する製品とその文書は、DCSSI が発行する認証書によって証明される。

#### ディスク

TOE によって暗号化されたデータを含む不揮発性記憶域。

#### ディスク・イメージ

不揮発性の大容量記憶域に格納される(暗号化された)データの集合。

#### 解釈

コモン・クライテリアに対する補足(明確化、是正、または追加)。解釈に関するリストは、

<http://www.commoncriteriaportal.org> から利用可能である。

#### マシーン

不揮発性の大容量記憶域の暗号化アプリケーションを稼動する装置(ラップトップ・コンピュータ、ネットワーク・サーバなど)。

### 大容量記憶域

大容量記憶域という用語には、コンピュータを介してアクセスする全ての情報格納システム(データとプログラム)が含まれる。この情報格納システムには、ハードディスク、フロッピー・ディスク、磁気ストライプ、Iomega 社の Zip ディスク、CD、DVD、USB キーなどがある。

### デバイス

物理的なデバイスには、不揮発性の大容量記憶域が収容されている。このデバイスは、必ずしも TOE によって管理されなければならないわけではないが、保護領域という意味では TOE の一部となることもできる。

---

**付録 B 参照文献**

---

- [CC1] *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model. Version 3.1, June 2006. CCIMB-2006-06-001.*
- [CC2] *Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Requirements. Version 3.1, June 2006. CCIMB-2006-06-002.*
- [CC3] *Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements. Version 3.1, June 2006. CCIMB-2006-06-003.*
- [CEM] *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology. Version 3.1, June 2006. CCIMB-2006-06-004.*
- [CRYPTO] *Mécanismes de cryptographie: règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard (Cryptographic mechanisms: rules and recommendations concerning the choice and sizing of cryptographic mechanisms of standard robustness) Version 1.02, 19 November 2004. DCSSI.*
- [QS-QR] *Définition des paquets d'assurance pour la qualification standard et pour la qualification renforcée suivant les CC version 3, (Definition of assurance packets for standard qualification and for reinforced qualification according to the CC version 3). Note circulated at the evaluation launch meeting, 8 February 2006, DCSSI.*
- [QUA-STD] *Processus de qualification d'un produit de sécurité – Niveau standard. (Qualification Process for a security product) Version 1.0, July 2003. DCSSI, 001591 /SGDN /DCSSI /SDR.*
-