ソフトウェア完全ディスク暗号化の
プロテクションプロファイル

ハードディスクの盗難・紛失リスクの低減

本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。

正式な文書は、以下の URL よりダウンロード可能です。

https://www.niap-ccevs.org/pp/pp_swfde_v1.0.pdf

Information Assurance Directorate

2013 年 2 月 14 日
バージョン 1.0

平成 25 年 11 月 12 日　翻訳 暫定第 0.1 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

目次

改版履歴

バージョン	日付	説明
1.0	2013 年 2 月 14 日	初版リリース

1 PP 概論

1.1 TOE の PP の概要

本 PP は、紛失したり盗まれたりしたハードディスク（例えば、ラップトップまたはポータブルな外付けハードディスクドライブ）であって機密性のあるデータが含まれるものを敵対者が入手するという脅威に対処するものである。本プロテクションプロファイル（PP）に定義される評価対象（TOE）は、ハードディスクデバイス上のデータを暗号化する、ソフトウェアによる全ディスク暗号化製品である。NIST は以下のように定義している。*「完全ディスク暗号化（FDE）*は、全ディスク暗号化とも呼ばれ、コンピュータの OS を含め、コンピュータをブートするために使われるハードドライブ上のすべてのデータを暗号化することによって、FDE 製品への認証成功後にのみデータへのアクセスを許可するプロセスである。」[1] ソフトウェアによる暗号化製品は、ドライブ上のマスタブートレコード（MBR）及び最初のブート可能パーティションの部分を暗号化せずに残すことに注意されたい。本プロテクションプロファイルでは、「ディスク暗号化」という用語は NIST の定義による完全ディスク暗号化であるが、利用者データを含む可能性のある情報が書き込まれていない限りはドライブの MBR 及びブート可能パーティションをソフトウェアディスク暗号化製品が暗号化しないことを許可するように変更したものと解釈されることとする。

1.1.1 TOE の利用方法と主要なセキュリティ機能

TOE は、データを安全に保護するために用いられる。一連の対策方針とセキュリティ機能要件は、敵対者によって全く事前にアクセスされずに電源を切られた状態で紛失または盗まれたデバイス（通常はラップトップ）に限定される。

ハードディスクは、データ暗号鍵（DEK）を用いて暗号化される。DEK は、鍵暗号化鍵（KEK）を用いてマスクされる。KEK は、複数のコンポーネント（サブマスクと呼ばれ、認可ファクタから導出される）または単一のサブマスクから得られる。ストレージデバイス暗号化の最も重要なセキュリティ対策方針は、敵対者へ膨大な鍵空間に対する総当り的な暗号解読の実行を強制することである。

本 PP に適合する TOE は、以下のような主要な機能を実装する。認可機能は、TOE の利用者が KEK を形成するための認可ファクタを確立し、次にそれを収集する。ディスク暗号化機能は、DEK を用いてストレージデバイスへ書き込まれるすべてのデータの暗号化と復号を担当する。評価のスポンサーは、保証アクティビティを行うために評価チームによって必要とされるすべての情報の配付に責任を持つ。

さらにベンダは、サポートされているすべての運用環境で（例えば、製品によってサポートされているすべての O/S で）TOE を正しくインストールし管理するための構成ガイダンス（AGD_PRE、AGD_OPR）を提供することが求められる。

1.1.2 認可と認証

ハードディスクの正当な利用者は、コンピュータのブート時に 1 つ以上の認可ファクタを提供する。これらの認可ファクタによって、利用者がディスクドライブ上のデータへのアクセスを認可されているかどうかが判定される。認可ファクタは、個別の利用者ごとに一意である必要はない。換言すれば、ディスク暗号化機能の認可ファクタはその所有者が、ハードディスク上に保存された情報へのアクセスを認可された利用者のコミュニティの一員であることを立証するためにだけ必要とされる。

利用者が正しい認可ファクタを提供した後で、オペレーティングシステムは復号され、多

[1] NIST, “GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES”, NIST Special Pub 800-111, November 2007.

くの場合には利用者に通常のオペレーティングシステムのログインプロンプトが提示される。基盤となる OS への利用者の識別と認証と、TOE 管理機能に関しては、以下のセクションで論ずる。

認可ファクタは、以下のいずれかで構成されなくてはならない（must）。

- 管理者によって提供されたパスフレーズ、または
- プラットフォーム外部のトークン（例えば、USB デバイス）に収容されたビット列（外部トークン認可ファクタとして定義される）、または
- パスフレーズと外部トークン認可ファクタの組み合わせ。

さらに、上記のいずれかに加えて、以下から成り立っていてもよい。

- セキュリティターゲット（ST）作成者によって定義された認可ファクタ（例えば、（耐破壊性保護が組み込まれた）TPM 中に保護され、PIN によって保護されたビット列（TPM 保護認可ファクタとして定義される）。

ST 作成者が追加的な認可ファクタを定義する場合、それらは十分に文書化されなくてはならず、またパスフレーズまたは外部トークン認可ファクタあるいはその両方の強度を減少させてはならない。すべての認可ファクタは、それらが保護する鍵と同一のサイズ（ビット長）のサブマスクを提供するように調整されなくてはならず、また XOR 関数を用いて結合され KEK を作成しなくてはならない（must）。

パスフレーズ認可ファクタは、TOE 文書に含まれるガイダンスに加えて利用者のエンタープライズによって提供されるガイダンスを用いて管理者によって生成されたパスフレーズであるべきである（should）。TOE は、1 文字から少なくとも 8 文字までの長さの単語の辞書から選択された少なくとも 9 語のパスフレーズをサポートしなくてはならない（must）。パスフレーズが利用者によって入力されると、TOE はハッシュ関数、または NIST 800-132 を満たす認定された鍵導出関数を用いて、KEK への入力として用いられるサブマスクを作成する。

TPM 認可ファクタと外部トークン認可ファクタは、いずれも TOE によって提供されるビット列に過ぎない。外部トークンまたは TPM そのものは、いずれも TOE の一部とはみなされない。しかし、外部トークンはコンピューティングプラットフォームの一部ではないため、それについては追加的な運用上の考慮点が存在するという理由から、本 PP ではこれらは区別される（もちろん、PIN で保護された認可ファクタと共に TPM を含む外部トークンを用いることは許容可能であり、この場合には両方の認可ファクタに関する前提条件のすべてが満たされる必要があることになる）。本 PP においては、TPM 認可ファクタと外部トークン認可ファクタの両方に適用される前提条件またはコメントには、「外部認可ファクタ」という用語が用いられる。

外部認可ファクタは、TOE によって生成されなくともよい。TOE によって生成される場合には、FIPS 認定ランダムビット生成器を用いて TOE によって認可ファクタが生成されることを規定するために附属書 C から適切な要件を取り込まなくてはならず、また DEK に選択された鍵サイズと少なくとも同じ大きさであることが必要となる。この場合には、外部トークン認可ファクタが、サブマスクとして KEK の形成に直接利用されてもよい。

1.1.3 暗号化

鍵または認可ファクタを生成、取り扱い、及び保護するために用いられる暗号が十分に堅牢であり、さらに実装に重大なミスがなければ、電源が切られた状態で認可ファクタまたは KEK のない紛失または盗まれたハードドライブを入手した敵対者は、データを取得するために KEK または DEK の暗号鍵空間を総当たりする必要がある（has to）。（ディスク暗号化アルゴリズムである AES の潜在的鍵空間よりも弱い強度しかパスフレーズが提供せず、さらにパスフレーズのみが敵対者にとって未知の認可ファクタである場合には、提供される保護は AES 鍵の鍵空間ではなく、パスフレーズの強度に対応するものになる、ということに注意されたい。）

ハードディスク上のデータは DEK を用いて暗号化される。DEK は、KEK または中間鍵のいずれかによってマスクできる。中間鍵を用いる場合、中間鍵は KEK によってマスクされ、DEK は中間鍵によって暗号化される。あらゆる中間鍵は KEK 及び DEK と同一の強度要件を満たさなくてはならず、また要件の繰返しを用いて ST 中に規定されなくてはならない（must）。

DEK は KEK によってマスクされる（XOR 演算または AES を用いて）。DEK は、決定論的ランダムビット生成器（DRBG）を用いて生成され、128 ビットまたは 256 ビットのいずれかである。適切にシードが与えられた DRBG によって、少なくとも DEK の鍵サイズと同等の雑音がサンプリングされることが確実となる。DRBG アルゴリズムへの入力として用いられるエントロピーは、少なくとも 1 つのハードウェアベースまたはソフトウェアベースの雑音源によって提供されなくてはならない（must）。DEK と IV（訳注：初期化ベクトル）のペアがシステム上で一意であることは重要であり、暗号操作が行われる粒度のレベル（例えば、ブロック、セクタ、ドライブ全体）は実装依存である。したがって、複数のドライブまたはドライブ上の複数のブロックが同一の DEK によって暗号化される場合、コンピュータ全体で異なる IV が用いられるべきである（should）。

暗号化されていない鍵及び鍵マテリアル（認可ファクタを含む）は、もはや使われなくなった際にゼロ化されることになり、また永続的ストレージに書き込まれることはない。いかなる暗号化されていない鍵または鍵マテリアルも、敵対者が電源の切られた状態のハードディスクデバイスを回収した場合に平文で利用できてはならない（should not）。

1.1.4 管理

1.1.6 でさらに論ずるように、TOE の基本要件には TOE が管理的役割を維持することは要求されていない。しかし、システム全体は TOE の管理者という概念を維持している。これは、TOE の利用者のサブセットである。「管理者」という用語は、以下のセクションではこの意味で用いられる。

TOE の管理者は、あらゆる必要とされる構成ガイダンスに正しくしたがわなくてはならない（shall）。この役割を確立するために、TOE は運用環境中のホスト O/S によって提供される認証システムに依存することもできるし、独自のメカニズムを実装することもできる。後者の場合、附属書 C からの情報がセキュリティターゲットに含まれなくてはならない。TOE は、以下の管理機能を強制できなくてはならない（shall）。

- DEK の作成、
- 既存の DEK の変更、
- パスフレーズベースの認可ファクタの変更、
- 認可ファクタから作成されたサブマスクからの鍵暗号化鍵（DEK をラップするために用いられる）の生成。

附属書 C の制約が遵守される限り、追加的な機能を TOE が提供したり、ST に規定したりすることもできる。

1.1.5 正当な利用者

正当な利用者は、データ危殆化のリスクを最小化するために利用者ガイダンスを厳守しなくてはならない（shall）。認可は、保護されたディスクのロックを解除するための正しい認可ファクタを所有し、TOE に提供することによって判定される。自分が所有している間、デバイスと TOE の認可ファクタをセキュアに保護することは､正当な利用者の責任である。正当な利用者は、電源が入っている状態でハードドライブを自分の物理的制御下から逸脱させてはならない（must not）。正当な利用者は、パスフレーズまたは外部トークンまたは TPM の PIN をハードドライブとともに、また複数のファクタが用いられる場合にはこれらを一緒に放置／保存してはならない（shall not）。外部トークンは、認可が成功した後はシステムから取り外されるべきである（should）。利用者には、セキュアな TOE を維持するための適切なガイダンスが提供される。

1.1.6 TOE とその支援環境

TOE の支援環境は重要である。TOE は純粋にソフトウェアによるソリューションであるため、その実行ドメイン及びその適切な使用は、TOE 運用環境（システムハードウェア、ファームウェア､及びオペレーティングシステム）に全面的に依存しなくてはならない（must）。ベンダには、運用環境に必要な機能を特定するために十分なインストール及び構成の指示を提供すること、そしてその構成方法に関する指示を提供することが期待される。

TOE の最も重要な目的は、基盤となるプラットフォームのハードドライブ上のデータを確実に暗号化することである。しかし、TOE によって利用される暗号サービスの一部が、運用環境によって提供される場合もあるかもしれない。例えば認可ファクタからの KEK の形成など、文書本体に含まれる暗号または鍵生成／操作の要件は TOE によって実装されなくてはならない（must）。TOE または運用環境のいずれによって行われてもよい暗号または鍵生成／操作の要件は、附属書 C に含まれている。TOE がこれらの機能を行う場合、ST 作成者はこれらのコンポーネントを ST の本体へ移し、ST 中の脅威と対策方針に適切な調整を行う。

附属書 C のセクション C.1 は、本 PP の附属書 C 中の他の要件とは多少異なっている。附属書 C.1 中の要件は、TOE または運用環境のいずれかによって満たされなくてはならない（must）。この意味で、これらは附属書 C の他の要件のように「オプショナル」ではない。TOE が依存する C.1 中の要件を運用環境が「満たしている」かどうかを開発者／評価チームが判定するために必要な証拠資料を判定することは、評価スキームに任されている。ST には、そのプラットフォームが割付けられた C.1 中の要件を満たすかどうかの判定ができるように、TOE が評価されるべきプラットフォームが十分な詳細と共に列挙されなくてはならない（must）。

場合によっては、TOE がそのセキュリティ対策方針を満たせるようにするため、具体的な運用環境の構成ガイダンスを TOE ベンダが提供する必要がある場合もあるだろう。そのような例を、以下に挙げる。

- その製品がサポートするすべてのオペレーティングシステムについて、利用者のインアクティビティが一定期間続いた後にシステムが完全にパワーダウンするように電源管理状態（例えば、休止状態／スリープ）を構成する方法の指示、
- システムを完全にパワーダウンするように構成できない電源管理状態（例えば、休止状態／スリープ）を禁止する方法の指示、
- 運用環境（オペレーティングシステム）の識別と認証情報の一部、またはそれに

代わるものとして TOE の認可ファクタを利用する任意の機能を無効化する方法を記述した指示。

1 つ以上の基盤となるプラットフォームの電源管理モード中で正しく情報を保護できる機能を TOE が有する場合、附属書 C.5 中の要件を用いることができることに注意すべきである（should）。

TOE の正当な利用者は、TOE の有効な認可ファクタを所有している利用者である。TOE は、TOE の正当な利用者のサブセットによって特定の管理アクティビティ（FMT 要件中に定義される）が行われることを要求する。本 PP では、識別と認証の機能を提供してこれらの管理機能を管理的役割に制約することに関して TOE には何ら要件を課さないが、これは TOE ベンダが適合するための方法が多数存在することを意味する。以下にその例を挙げる。

1. TOE には、正当な管理者の概念が含まれない。管理ユーティリティを呼び出すことができるものは誰でも、TOE を構成できる。この場合、PP へ適合するためには、TOE ベンダは AGD_OPE/PRE ガイダンスの一部として、TOE の正当な利用者のサブセットのみが管理ユーティリティを実行できるように運用環境を構成するために管理者が用いる手順を詳述する指示を提供しなくてはならない（must）。そのガイダンスには例えば、管理者の許可した利用者のみが管理ユーティリティを実行できるような、運用環境中のアクセス制御メカニズムの構成が記述されることだろう。この場合は、A.PLATFORM_I&A に規定される本 PP の基本要件を反映している。
2. TOE には正当な管理者（または管理者のセット）の概念が含まれるが、識別と認証の機能を実行した後に正当な管理者の TOE 内部表現とマッチ可能な何らかの情報を TOE へ渡すことについては、運用環境に依存している。この場合、ST 作成者は（附属書 C に提供されるテンプレートを用いて）要件を追加して、TOE によって提供される機能を規定する必要があるだろう。ベンダは、情報を TOE へ渡すことをサポートするために必要な運用環境の構成または設定があれば、それを記述する必要があるだろう。
3. TOE には、ハードディスクを収容するシステムのどの利用者に TOE によって提供される管理機能の利用が認可されているかを判定するために用いられる、それ自身の識別と認証の機能が含まれる。この場合、ST 作成者は附属書 C に提供される I&A を ST 本体に用いて、この機能を規定する必要があるだろう。

2 セキュリティ課題定義

本プロテクションプロファイル（PP）は、敵対者によって事前にアクセスされずに電源を切られた状態でハードディスクが紛失または盗まれた状況に対処するために作成される。

2.1 脅威

脅威は、脅威エージェントと資産、そしてその資産への脅威エージェントの敵対的なアクションによって構成される。

脅威エージェントは、紛失または盗まれたハードディスクを敵対者が入手した場合に資産をリスクにさらすエンティティである。例えば、下図における脅威は T.UNAUTHORIZED_DISK_ACCESS である。脅威エージェントは、紛失または盗まれたハードディスクの所有者（権限のない利用者）である。資産はストレージデバイス上のデータであり、敵対的なアクションはハードディスクからこれらのデータを入手しようとする試みである。この脅威によって、ハードディスクへアクセスするために TOE を使用できる人物を認証し、データを暗号化／復号するというディスク暗号化装置（TOE）に関する機能要件が必要とされる。KEK、DEK、中間鍵、認可ファクタ、サブマスク、及び乱数もしくは鍵または認可ファクタの作成に寄与するその他の任意の値を所有することによって権

限のない利用者が暗号を解読できる可能性があるため、鍵マテリアルはデータと同様の重要度を持つとみなされ、脅威テーブルにおいて対処されるもうひとつの資産となる。

この時点で、評価対象（TOE）または運用環境へ悪意のあるコードまたは悪用可能なハードウェアコンポーネントを導入できる、紛失または盗まれたハードディスクの所有者に対して、製品（TOE）が防御を行えるとは一般的には期待されないことは重要なので、再度強調しておきたい。TOE が物理的に保護され、運用環境がロジックをねらった攻撃に対して十分な保護を利用者が確実に提供することが前提となる。多少の保護が適合 TOE によって提供される具体的な領域のひとつは、TOE への更新の提供である。しかしこの領域を除いて、本 PP では一切の対策は義務付けられない。同様に、これらの要件は「紛失後に見つかった」ハードディスクの問題にも対処しない。これは、敵対者がハードディスクを入手してブートデバイスの暗号化されていない部分（例えば、MBR、ブートパーティション）を危殆化し、そして元の利用者が取り戻すように仕向けて、危殆化されたコードを実行させようとすることである。

表 1：脅威

脅威	脅威の説明
T.KEYING_MATERIAL_ COMPROMISE	攻撃者が、TOE が永続的なメモリへ書き込んだ暗号化されていない鍵マテリアル（KEK、DEK、認可ファクタ、サブマスク、及び乱数または鍵が導出されるその他の値）を入手し、これらの値を使って利用者データへのアクセスができるおそれがある。
T.PERSISTENT_INFORMATION	運用環境が省電力モードに入り、データまたは鍵マテリアルが永続的なメモリ中で暗号化されずに残るおそれがある。
T.KEYSPACE_EXHAUST	権限のない利用者がブルートフォース攻撃を行って暗号鍵または認可ファクタを明らかにし、データまたは TOE リソースへの不正なアクセスができるおそれがある。
T.TSF_ COMPROMISE	悪意のある利用者またはプロセスが、TSF データまたは実行可能形式のコードを不適切な形でアクセス（閲覧、変更、または削除）できるようにして、鍵マテリアルまたは利用者データへのアクセスができるおそれがある。
T.UNAUTHORIZED_DISK_ACCESS	紛失したハードディスクへのアクセスを得た権限のない利用者が、TOE のセキュリティ方針に従えば彼らには権限のないデータへアクセスできるおそれがある。
T.UNAUTHORIZED_UPDATE	悪意のある人物が、TOE のセキュリティ機能を危殆化させるおそれのある製品への更新をエンドユーザへ供給することを試みるおそれがある。

T.UNSAFE_AUTHFACTOR_VERIFICATION	攻撃者が、認可ファクタの検証を行うための安全でない手法を利用して、KEK、DEK、または利用者データの暴露を招くおそれがある。

2.2 前提条件

セキュリティ課題を定義するこのセクションでは、セキュリティ機能を供給可能とするために運用環境に対して課される前提条件を示す。TOE がこれらの前提条件を満たさない運用環境に配置された場合、TOE はもはやそのセキュリティ機能のすべてを提供することはできないかもしれない。前提条件は、物理的、人的、及び運用環境の接続性に課すことができる。

表 2：TOE の前提条件

前提条件	前提条件の説明
A.AUTHORIZED_USER	正当な利用者は、パスフレーズや外部トークンをセキュアに保ち、ディスクとは別個に保管することを含め、提供されたすべての利用者ガイダンスを遵守すること。
A.ET_AUTH_USE_ONLY	認可ファクタを含む外部トークンは、外部トークン認可ファクタの保存以外のいかなる他の目的にも用いられないこと。
A.PASSPHRASE_BASED_AUTH_FACTOR	正当な管理者は、パスフレーズ認可ファクタが、保護されるデータの機密性を反映した十分な強度とエントロピーを持つことを確実にする責任を負うこと。
A.PLATFORM_I&A	TOE は、個別の利用者の識別と認証をサポートするプラットフォーム上にインストールされること。この I&A 機能は、TOE によって影響されてはならない（shall）。
A.PROTECT_INTEGRITY	利用者は、TOE の物理的な保護に正当な注意を払い、IT 環境がロジックをねらった攻撃に対して十分に保護されていることを確実にすること。
A.SHUTDOWN	正当な利用者は、機密性のある情報が不揮発性ストレージに残るようなモードにマシンを放置しないこと（例えば、電源を切るか、「休止状態」などの電源管理状態にする）。
A.STRONG_OE_CRYPTO	運用環境において実装され TOE によって利用されるすべての暗号機能は、本 PP の附属書 C に列挙された要件を満たすこと。これには、外部トークン認可ファクタの RBG による生成も含まれる。
A.TRAINED_ADMINISTRATORS	正当な管理者は、適切に教育され、すべての

	管理ガイダンスを遵守すること。

3 セキュリティ対策方針

セキュリティ対策方針は、評価対象（TOE）及び運用環境に関する要件であって、脅威、組織のセキュリティ方針、そしてセクション 2 の前提条件から導出されたものである。セクション 4 では、TOE に関するセキュリティ対策方針を、セキュリティ機能要件（SFR）として、より形式的に再び述べる。TOE は、SFR に対して評価される。

3.1 TOE のセキュリティ対策方針

表 4（訳注：表 3 の間違い）に、TOE のセキュリティ対策方針を特定する。これらのセキュリティ対策方針は、特定された脅威に対抗する、または特定された任意の組織のセキュリティ方針に準拠する、あるいはその両方の言明された意図を反映している。TOE は、セキュリティ機能要件を満たすことによって、これらの対策方針を満たす必要がある（has to）。

表 3：TOE のセキュリティ対策方針

対策方針	対策方針の説明
O.AUTHORIZATION	TOE がハードディスク上のデータを復号できるためには、利用者から認可ファクタを取得しなくてはならない（must）。
O.CORRECT_TSF_OPERATION	TOE は、その運用環境における TSF の正しい動作を確実にするため、TSF をテストする機能を提供すること。
O.ENCRYPT_ALL	TOE は、ハードドライブ上に保存されたすべてのデータを暗号化すること。（MBR 及びそれが参照するブート可能パーティションはこれから除外されるかもしれないことに注意されたい。）
O.DEK_SECURITY	TOE は、1 つ以上のサブマスク（これはさらに認可ファクタから導出される）から作成された鍵暗号化鍵（KEK）を用いて DEK をマスクし、認可ファクタを持たない脅威エージェントが DEK を入手することによって利用者データへアクセスできることのないようにすること。
O.KEY_MATERIAL_COMPROMISE	TOE は、鍵マテリアルが必要なくなった際にはすぐにそれをゼロ化し、そのようなマテリアルが KEK または DEK の発見のために使われる可能性を減少させること。
O.MANAGE	TOE は、正当な管理者を TOE のセキュリティ管理の面でサポートするために必要なすべての機能及び設備を提供し、これらの機能及び設備の不正な利用を制限すること。
O.OWNERSHIP	TOE は、TOE が動作中に任意の利用者データがアクセスできるようになる前に、所有権が

	得られている（すなわち、DEK が作成され、認可ファクタが確立され、任意のデフォルト認可ファクタが変更され、KEK が導出されたサブマスクから形成され、そして DEK が KEK と関連付けられている）ことを確実にしなくてはならない（shall）。
O. SAFE_AUTHFACTOR_VERIFICATION	TOE は、KEK や DEK または利用者データが不用意に暴露されないように、認可ファクタの検証を行わなくてはならない（shall）。
O.TRUSTED_UPDATE	TOE は、管理者に TOE のファームウェア／ソフトウェアを更新する機能と、製品への更新が意図されたソースから受信されたことを検証する機能を提供しなくてはならない（shall）。

3.2 運用環境のセキュリティ対策方針

TOE の運用環境は、TOE がそのセキュリティ機能（これは、TOE のセキュリティ対策方針によって定義される）を正しく提供できるように支援する、技術的及び手続的手段を実装する。このパートごとのソリューションは、運用環境のセキュリティ対策方針を形成し、また運用環境が達成すべき目標を記述する一連の言明によって構成される。

このセクションでは、IT ドメインもしくは非技術的または手続き的手段によって対処されるべきセキュリティ対策方針を定義する。セクション 2.2 中に特定された前提条件は、環境へのセキュリティ対策方針として組み込まれている。これによって環境に対する追加的な要件が課されるが、これらは主に手続き的または管理的手段によって満たされる。表 5（訳注：表 4 の間違い）に、環境のセキュリティ対策方針を特定する。

表 4：運用環境のセキュリティ対策方針

対策方針	対策方針の説明
OE.PASSPHRASE_STRENGTH	正当な管理者は、パスフレーズ認可ファクタが TOE を利用するエンタープライズからのガイダンスに準拠していることを確実にする責任を負うこと。
OE.PLATFORM_I&A	運用環境は、TOE によって用いられる認可ファクタとは独立して動作する、個別の利用者の識別と認証メカニズムを提供すること。
OE.POWER_SAVE	運用環境は、利用者がシステムのシャットダウンを選択したサイト同一の方法で、一定の時間が経過した後にシステムの電源を落とすメカニズムが少なくとも 1 つ存在するように、構成可能でなくてはならない（must）（O.SHUTDOWN）。この要件に適合しない任意のメカニズム（例えば、スリープ、休止状態）は、管理者によって無効にできなくては

	ならない（must）。
OE.RESTRICTED_FUNCTIONS	管理機能は、正当な管理者に限定されること。
OE.SINGLE_USE_ET	認可ファクタを含む外部トークンは、外部トークン認可ファクタの保存以外のいかなる他の目的にも用いられないこと。
OE.STRONG_ENVIRONMENT_ CRYPTO	運用環境は、TOE の要件及び機能ならびに附属書 C に対応した暗号機能を提供すること。
OE.TRAINED_USERS	正当な利用者は、適切に教育されるとともに TOE 及び認可ファクタをセキュアに保つためのすべてのガイダンスを遵守すること。

3.3 セキュリティ対策方針の根拠

TOE 対策方針に関するセキュリティ対策方針の根拠はセクション 6 に含まれている。表 6 に、セキュリティ対策方針から前提条件への対応付けを示す。

表 6：セキュリティ対策方針から前提条件への対応付け

前提条件	前提条件へ対処する対策方針	根拠
A.AUTHORIZED_USER 正当な利用者は、パスフレーズや外部トークンをセキュアに保ち、ディスクとは別個に保管することを含め、提供されたすべての利用者ガイダンスを遵守すること。	OE.TRAINED_USERS 正当な利用者は、適切に教育されるとともに TOE 及び認可ファクタをセキュアに保つためのすべてのガイダンスを遵守すること。	OE.TRAINED_USERS は、利用者に TOE を正しく使うための方法が教育されることを確実にする。
A.ET_AUTH_USE_ONLY 認可ファクタを含む外部トークンは、外部トークン認可ファクタの保存以外のいかなる他の目的にも用いられないこと。	OE.SINGLE_USE_ET 認可ファクタを含む外部トークンには、外部トークン認可ファクタの以外の何ものも含まれないこと。 OE.TRAINED_USERS 正当な利用者は、適切に教育されるとともに TOE 及び認可ファクタをセキュアに保つためのすべてのガイダンスを遵守すること。	OE.SINGLE_USE_ET は、外部トークン上に外部トークン認可ファクタのみが存在することを要求することによって、対策方針を満たす。 OE.TRAINED_USERS は、利用者が外部トークン上へ追加的な情報を置かないことを供給することによって、これに寄与する。
A.PASSPHRASE_BASED_AUTH_FACTOR 正当な管理者は、パスフレーズ認可ファクタがパスフレーズ方針に適合し、保護されるデータの機密	OE.TRAINED_USERS 正当な利用者は、適切に教育されるとともに TOE 及び認可ファクタをセキュアに保つためのすべての	OE.TRAINED_USERS は、管理者が教育され提供されるガイダンスを順守することを確実にすることにより、この方針を

前提条件	前提条件へ対処する 対策方針	根拠
性を反映した十分な強度とエントロピーを持つことを確実にする責任を負うこと。	ガイダンスを遵守すること。 OE.PASSPHRASE_STRENGTH 正当な管理者は、パスフレーズ認可ファクタが TOE を利用するエンタープライズからのガイダンスに準拠していることを確実にする責任を負うこと。	満たす。 OE.PASSPHRASE_STRENGTH は、保護されるデータの機密性を反映した十分な強度とエントロピーを持つパスフレーズを管理者が作成することを確実にすることによって、この方針を満たす。
A.PLATFORM_I&A TOE は、個別の利用者の識別と認証をサポートするプラットフォーム上にインストールされること。この I&A 機能は、TOE によって影響されてはならない（shall）。	OE.PLATFORM_I&A 運用環境は、TOE によって用いられる認可ファクタとは独立して動作する、個別の利用者の識別と認証メカニズムを提供すること。	OE.PLATFORM_I&A は、1) システムの利用者のための I&A メカニズムが運用環境上に実装されることを確実にし、また 2) これらのメカニズムが TOE への認可ファクタの入力によって取って代わられない（例えば、シングルサインオン機能を通して）ことを確実にする。
A.PROTECT_INTEGRITY 利用者は、TOE の物理的な保護に正当な注意を払い、IT 環境がロジックをねらった攻撃に対して十分に保護されていることを確実にすること。	OE.TRAINED_USERS 正当な利用者は、適切に教育されるとともに TOE をシャットダウンし認可ファクタをセキュアに保つためのすべてのガイダンスを遵守すること。	OE.TRAINED_USERS は、ロジックを狙った攻撃への暴露を最小化するように運用環境を構成し運用する方法に関するガイダンスを利用者へ提供することによって、この前提条件を満たす。さらにガイダンスでは、たとえディスクが暗号化されていたとしても、TOE を物理的に保護する為の対策を取ることを利用者へ指示する。
A.SHUTDOWN 正当な利用者は、機密性のある情報が不揮発性ストレージに残るようなモードにマシンを放置しないこと（例えば、電源を切るか、「休止状態」などの電源管理状態にする）。	OE.TRAINED_USERS 正当な利用者は、適切に教育されるとともに TOE をシャットダウンし認可ファクタをセキュアに保つためのすべてのガイダンスを遵守すること。	OE.TRAINED_USERS は、正しくシステムの電源を切るか、または機密性のある情報が不揮発性のメモリ中に残らないことを確実にする電源管理モードにマシンが入っていることを確実にする方法を指示することによっ

前提条件	前提条件へ対処する 対策方針	根拠
		て、この前提条件を満たす。ガイダンスでは、そうすることの重要性も説明される。
A.STRONG_OE_CRYPTO 運用環境において実装され TOE によって利用されるすべての暗号機能は、本 PP の附属書 C に列挙された要件を満たすこと。これには、外部トークン認可ファクタの RBG による生成も含まれる。	OE.STRONG_ENVIRONMENT_ CRYPTO 運用環境は、TOE の要件及び機能ならびに附属書 C に対応した暗号機能を提供すること。	TOE が、運用環境に実装された暗号機能を利用することは許容可能である。しかし、例えば RBG の特徴や DEK を使った暗号化の許容されるモードなど、そのような暗号機能に特有の要件がいくつか存在する。そのような特有の要件は附属書 C に取り込まれており、運用環境がこれらの規定された機能を提供することによって、この前提条件を満たすことが期待される。
A.TRAINED_ADMINISTRATORS 正当な管理者は、適切に教育され、すべての管理ガイダンスを遵守すること。	OE.TRAINED_USERS 正当な利用者は､適切に教育されるとともに TOE 及び認可ファクタをセキュアに保つためのすべてのガイダンスを遵守すること。	OE.TRAINED_USERS は、管理者が教育され適切なガイダンスを遵守して TOE の構成及び維持管理を行うことを確実にする。

4 セキュリティ要件

セキュリティ要件は、機能要件と保証要件に大別される。セキュリティ機能要件（SFR）は、セキュリティ対策方針の形式的な具体化であり、セクション 4.1 の適用上の注意が提供される。

セキュリティ保証要件（SAR）は、典型的には SFR とは分離して PP へ挿入され列挙される。そして、選択された SAR に基づいた評価中には CEM が参照される。コモンクライテリアのセキュリティ保証要件と、TOE として特定される特有の技術の性質のため、よりカスタム化されたアプローチが本 PP では取られている。本 PP でも SAR は文脈と完全性に応じてセクション 4.3（訳注：4.2 の間違い）に列挙されているが、評価者が SFR と SAR のそれぞれについてこの TOE に行う必要のあるアクティビティの大半は、「保証アクティビティ」のパラグラフに詳述されている。保証アクティビティは、評価が完了されるためには行われなくてはならないアクティビティの規範的な記述である。保証アクティビティは本 PP の 2 か所に配置されている｡具体的な SFR と関連付けられたものはセクション 4.1 に配置され、SFR と独立したものはセクション 4.3（訳注：4.2 の間違い）に詳述されてい

る。保証アクティビティは、実際にはカスタム化された評価の方法論であり、読みやすさと理解しやすさ、そして便宜のため SFR と共に提示されていることに注意されたい。

将来のプロテクションプロファイルの繰り返しでは、より詳細な保証アクティビティを、実際の製品評価から得られた教訓に基づいて提供することになるかもしれない。

4.1 セキュリティ機能要件

表 5：TOE セキュリティ機能要件

機能クラス	機能コンポーネント
暗号サポートクラス（FCS）	FCS_CKM.1(1) 暗号鍵生成（DEK）
暗号サポートクラス（FCS）	FCS_CKM.1(2) 暗号鍵生成（KEK）
暗号サポートクラス（FCS）	FCS_CKM_EXT.4 暗号鍵マテリアルの破壊
利用者データ保護クラス（FDP）	FDP_DSK_EXT.1 拡張:ディスク上のデータの保護
識別と認証クラス（FIA）	FIA_AUT_EXT.1 拡張：FDE 利用者の認可
セキュリティ管理クラス（FMT）	FMT_SMF.1 管理機能の仕様
TSF の保護クラス	FPT_TUD_EXT.1 高信頼更新
TSF の保護クラス	FPT_TST_EXT.1 TSF のテスト

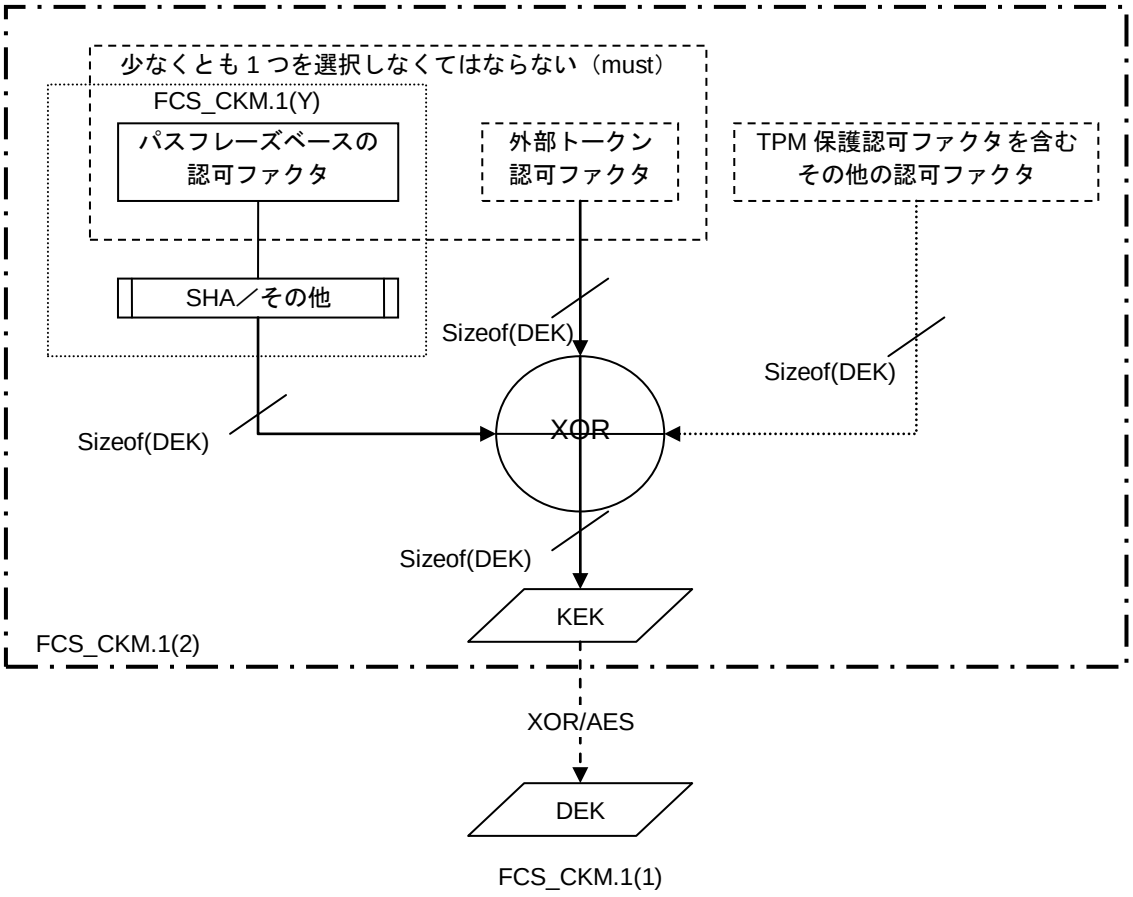
4.1.1 クラス：暗号サポート（FCS）

これらの機能要件によって対処される主な脅威は、鍵空間及び暗号コンポーネントの故障に対するブルートフォース攻撃である。

保証要件は、これらの要件が検証されるべき実装を詳述する。それぞれのスキームは、暗号保証アクティビティが満たされたとみなすことのできるプロセスを規定する選択肢を有する。

暗号鍵の管理（FCS_CKM）

適合する実装には、少なくとも鍵暗号化鍵（KEK）及びデータ暗号化鍵（DEK）の 2 つの鍵が含まれること。以下の要件では、鍵が作成される方法を規定する。この作成は多少込み入ってはいるが、以下の説明でこのセクション中の要件の概要を提供する。



上の図に示すように、DEK の生成は FCS_CKM.1(1) 中に規定される一方で、パスフレーズまたは外部トークン認可ファクタあるいはその両方を用いた KEK の生成は FCS_CKM.1(2) 中で規定されている。パスフレーズは、セクション C.4「認可ファクタ」中の FCS_CKM.1(Y) に規定されているように条件付けられなくてはならない（must）。KEK は、認可ファクタから導出されたサブマスクから生成される。TOE は、パスフレーズベースの認可ファクタ（FCS_CKM.1(Y)）または認可ファクタを含む外部トークンのいずれかをサポートすることが求められる。これらの両方をサポートしてもよい。外部認可ファクタに関する注意：TOE には、そのようなファクタの生成は求められないが、生成できなくてもそれらを使うことはできる。FCS_CKM は鍵の生成を取り扱うため、TOE が外部トークン認可ファクタを生成する能力の認定も主張したい場合には、附属書 C から FCS_CKM.1(X) コンポーネント（及び関連する脅威、対策方針、そして根拠）を ST の本体中に取り込まなくてはならない（must）。

TOE がこれらの認可ファクタのうち少なくとも 1 つをサポートする限り、TPM ベースの認可ファクタ（上の図の右側に示されている）を含め、その他の認可ファクタをサポートすることもできる。これらは FCS_CKM.1(2) に規定されている。また FCS_CKM.1(2) には、さまざまな認可ファクタを結合して KEK を形成する方法も規定されている。この背景を踏まえて、鍵生成要件を以下に示す。

FCS_CKM.1(1)	**暗号鍵生成（DEK）**
FCS_CKM.1.1(1)	**詳細化**：TSF は、**FCS_RBG_EXT.1 に規定されるランダムビット生成器及び**以下 [**標準なし**] に適合する規定された暗号鍵サイズ **[選択**：**128 ビット、256 ビット]** を用いて、**DEK** 暗号鍵を

生成しなくてはならない（shall）。

適用上の注意：

この要件の意図は、AES の鍵空間の総当たりよりも少ない労力で DEK が回復できないことを確実にすることである。TOE の鍵生成機能は、TOE デバイス上に実装された RBG を利用する。128 ビットまたは 256 ビットのいずれかが許可される。ST 作成者は、デバイスに適切な選択を行う。DEK は、デバイス上の利用者データをすべて再暗号化する必要なく認可ファクタ（特に、パスフレーズ認可ファクタ）が変更できるよう、KEK に加えて使われる。

FCS_RBG_EXT.1 は、附属書 C に含まれる。TOE 中の DEK 生成ルーチンが、ランダムビット生成器などのサポート暗号機能を呼び出すことは受容可能であり、その場合にも本 PP には適合する。

TOE が中間鍵を利用する場合、この要件は中間鍵について繰り返される。

保証アクティビティ：

評価者は TSS をレビューし、FCS_RBG_EXT.1 によって記述される機能が呼び出される方法が記述されていることを判定しなくてはならない（shall）。RBG が運用環境によって提供されている場合には、評価者は（ST 中に特定されるプラットフォームのそれぞれについて）この機能を呼び出すために TOE によって使われるインタフェースが TSS に記述されていることをチェックして確実にする。評価者は、FCS_RBG_EXT 中の RBG 機能の記述または運用環境に利用可能な文書を用いて、要求されている鍵サイズが利用者データの暗号化／復号に用いられる鍵サイズ及びモードと同一であることを判定する（FCS_COP.1(1)、これは附属書 C に含まれている要件でもある）。

FCS_CKM.1(2) **暗号鍵生成（KEK）**

FCS_CKM.1.1(2) **詳細化**：TSF は、規定された暗号**導出**アルゴリズム **[選択：なし、排他的論理和（XOR）]** にしたがって、**以下の入力 [選択**：

FCS_CKM.1(Y) に定義されるように作成され調整されたパスフレーズ認可ファクタから導出されたサブマスク、

DEK と同一のビット長である外部トークン認可ファクタ、

[選択：その他の入力なし、DEK と同一のビット長である TMP 保護された認可ファクタ、 [割付：その他の認可ファクタのリスト及び関連付けられたサブマスク導出手法] であって FCS_CKM.1(1) に規定される DEK と同一のサイズのサブマスクを作成するもの]

を利用して、各認可ファクタの実効強度及び規定された暗号鍵サイズ **[選択：128 ビット、256 ビット]** を**維持**して、以下 **[標準なし]** を満たす **KEK 暗号鍵を導出**しなくてはならない（shall）。

適用上の注意：

これらの要件は、KEK の作成に認可ファクタが用いられる方法を定義することを意図している。割付と選択のそれぞれについて ST 作成者への具体的なガイダンスは後述するが、以下はこのコンポーネントのポイントの高レベル記述である。ST 作成者は、

パスフレーズ認可ファクタ、または外部トークン認可ファクタ、あるいはその両方を選択する。次に ST 作成者は、TPM 保護された認可ファクタを選択するか、追加的な認可ファクタを定義する選択肢を有する。何らかの追加的な認可ファクタが定義された場合には、これらの認可ファクタからサブマスクが作成される手法もまた記述されなくてはならない（must）。そのような割付に課される唯一の条件は、作成されるサブマスクが DEK と同一のサイズであることのみであり、サブマスクの形成に暗号操作が用いられる場合には追加的な FCS_COP.1 の繰り返しを用いてこれらの暗号操作が規定される。複数の認可ファクタを用いることが望ましい。2 つ以上の認可ファクタが用いられる場合、作成されるサブマスクは XOR を用いて結合されなくてはならない（must）。

最初の選択については、1 つの認可ファクタのみが用いられる場合 ST 作成者は「なし」を選択する。2 つ以上の認可ファクタが用いられる場合には、ST 作成者は「XOR」を選択する（その他の結合手法は本 PP に適合しない）。

2 番目の選択については、ST 作成者は用いられる認可ファクタを選択する。2 つ以上の選択は可能だが、少なくとも 2 つ（パスフレーズベース、外部トークンベース）のうち 1 つは選択されなくてはならない（must）。調整されたパスフレーズまたは TOE に対して外部的なもの以外の追加的な認可ファクタが用いられる場合には、ST 作成者はこの 2 番目の選択中の選択の内部の割付を用いて、これらのファクタを規定する（または「その他の入力なし」を選択する）。パスフレーズベースが選択された場合、ST 作成者は附属書 C から FCS_CKM.1(Y) を ST 本体へ取り入れる。TPM 保護または外部認可ファクタについては、その外部デバイス／TPM に含まれる認可ファクタは調整されず、直接利用される。

暗号鍵サイズに関しては、作成される KEK のサイズが選択されるが、これは FCS_CKM.1(1) 中の DEK に関して規定されたものと同一のビット長でなくてはならない（must）。

KEK を形成するために用いられる認可ファクタはただ 1 つしか存在しない（その作成方法は別の場所で規定される）か、あるいは KEK が XOR 関数を用いて形成されるかのどちらかであるため、「標準なし」が必要であることに注意されたい。

保証アクティビティ：

このコンポーネントの保証アクティビティは、TOE の要件の実装が文書化されていることを判定するために ST の TSS の調査を求めている。評価者は、まず TSS セクションを調査して ST 中に規定された認可ファクタが記述されていることを確証しなくてはならない（shall）。パスフレーズベースのファクタについては、TSS セクションの調査は FCS_CKM.1(Y) 保証アクティビティの一部として行われる。外部認可ファクタについては、その認可ファクタが TOE によって生成されなくてはならない（must）かどうかが TSS に詳述されていなくてはならない（shall）（この場合には附属書 C 中の FCS_CKM.1(X) と関連付けられた保証アクティビティが適用される）。そうでない場合に

は、外部認可ファクタが ST に列挙された最小の長さの要件を満たしていることを確実にするため TOE（または管理者）によって取られる対策が TSS セクションに規定されなくてはならない（shall）。受容可能な手段には、管理者による長さの検証または TOE によってランタイムに行われる入力適合性チェックである。さらにこの場合に評価者は、TOE によって用いられることが可能な外部認可ファクタの特徴（例えば、どのように認可ファクタが生成されなくてはならないか、認可ファクタが満たさなくてはならないフォーマットまたは標準、用いられる TPM デバイスの構成）が管理ガイダンスに論じられていることを検証しなくてはならない（shall）。

その他の認可ファクタが規定されている場合には、そのファクタのそれぞれについて、そのファクタが TOE へ入力される方法、その認可ファクタからサブマスクが作成される方法（このプロセスが準拠する関連する標準があればそれを含め）、及びサブマスクの長さが要求されるサイズを満たしていることを確実にするために行われる検証（この要件に規定されているように）が TSS に規定される。

ただ 1 つの認可ファクタしか存在しない場合、当然のことながら結合は行われないため、この場合に関連する保証アクティビティは存在しない。認可ファクタから作成されるサブマスクが互いに XOR されて KEK を形成する場合、TSS セクションにはこれが行われる方法（例えば、順序の要件が存在するかどうか、行われたことをチェックするかどうかなど）が特定されなくてはならない（shall）。また評価者は、作成された出力の長さが DEK の長さと同一であるかどうかが TSS に記述されていることを確認しなくてはならない（shall）。

また評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 1 [条件付き]：2 つ以上の認可ファクタが存在する場合、要求される認可ファクタを提示しなければ暗号化されたデータへアクセスできないことを確証する。
- テスト 2 [条件付き]: TOE が異なるフォーマットの複数の外部トークンをサポートしている場合、評価者は各フォーマットを使って TOE への認可情報の提供に成功できることを確認する。

FCS_CKM_EXT.4　暗号鍵のゼロ化

FCS_CKM_EXT.4.1　TSF は、すべての平文の共通暗号鍵及び秘密暗号鍵ならびに CSP を、もはや必要とされなくなった際にゼロ化しなくてはならない（shall）。

適用上の注意：　「暗号クリティカルセキュリティパラメタ」は FIPS 140-2 に、「セキュリティ関連情報（例えば、共通暗号鍵及び秘密暗号鍵、ならびにパスワードや PIN などの認証データ）であって、その開示または変更が暗号モジュールのセキュリティの危殆化をもたらす可能性のあるもの」と定義されている。

上に示したゼロ化は、平文の鍵／暗号クリティカルセキュリテ

ィパラメタのすべての中間ストレージ領域（すなわち、メモリバッファなど任意のストレージであって、そのようなデータのパスに含まれるもの）に、その鍵／暗号クリティカルセキュリティパラメタが別の場所へ転送された際に適用される。

保証アクティビティ：　評価者は、共通鍵（共通鍵暗号化に用いられる鍵）、秘密鍵、及び鍵の生成に用いられる CSP のそれぞれについて、それらがゼロ化される時点（例えば、使用直後、システムのシャットダウン時、など）、及び行われるゼロ化手続きの種類（ゼロで上書き、ランダムパターンで 3 度上書き、など）が TSS に記述されていることをチェックして確証しなくてはならない（shall）。保護されるべきマテリアルの保存に異なる種類のメモリが用いられている場合、評価者はデータが保存されるメモリに関するゼロ化手続き（例えば、「フラッシュメモリ上に保存される共通鍵はゼロで 1 度上書きすることによってゼロ化されるが、内部ハードドライブ上に保存される共通鍵は書き込みごとに変化するランダムパターンを 3 度上書きすることによってゼロ化される」）が TSS に記述されていることをチェックして確証しなくてはならない（shall）。

4.1.2 クラス：利用者データ保護 (FDP)

このファミリは、すべての保存されたデータの暗号化を規定する。

拡張：ディスク上のデータの保護（FDP_DSK_EXT）

FDP_DSK_EXT.1	**拡張：ディスク上のデータの保護**
FDP_DSK_EXT.1.1	TSF は、FCS_COP.1.1(1) にしたがって完全ディスク暗号化を行わなくてはならない（shall）。
FDP_DSK_EXT.1.2	DEK は、FCS_CKM.1(2) 及び FCS_COP.1(4) に規定されているとおり導出された KEK（または中間鍵）によってマスクされている場合にのみ、電源の切られたハードディスク上に存在することができる。
FDP_DSK_EXT.1.3	TSF は、利用者の介在なく、すべてのデータを暗号化しなくてはならない（shall）。
FDP_DSK_EXT.1.4	一切の平文の鍵マテリアルは、永続的ストレージに書き込まれてはならない（shall not）。

適用上の注意：　「完全ディスク暗号化」は、本 PP の用語集に「コンピュータの OS を含め、コンピュータのハードドライブ上のすべてのデータを暗号化し、FDE 製品への認証成功後にのみデータのアクセスを許可するプロセス」として定義されている（MBR 及び認可ファクタの受け入れと処理に必要なコードを含む関連したブート可能パーティションを例外として）。

この要件の意図は、あらゆる重要なファイルの暗号化が、そのファイルを保護するという利用者の選択に依存しないことを規定することである。FDP_DSK_EXT.1 に規定されたディスク暗号化は利用者に透過的に行われ、そのデータを保護するという決定は利用者の裁量外である。これは、ディスク暗号化をファイル暗号化と区別する特徴である。

この要件は、明示的に保存された利用者データを含むファイルだけでなく、スワップファイルやレジストリ、そして他のディスク上の運用環境保存領域に保存されたデータのかたまりも含めて対処している。すべてのリムーバブルメディアの暗号化は要求していない。しかし、すべてのハードドライブの暗号化は要求している。

FDP_DSK_EXT.1.4 の意図が、TOE が平文の鍵マテリアルを永続的ストレージに書き込むことはない、ということであることには注意すべきである（should）。ほとんどの場合、TOE はメモリ上の鍵マテリアルが（例えば）ディスク上のスワップスペースに書き込まれることをコントロールすることはできない。これらのディスクの領域は DEK によって暗号化されるため、この FDP_DSK_EXT.1.4 への例外は受容可能である。

保証アクティビティ：

評価者は、この要件に関する保証アクティビティを行う際に、ST の TSS セクションを参照しなくてはならない（shall）。評価者は、データがディスクへ書き込まれる方法、及び暗号化機能が適用されるポイントに関して、記述が包括的であることを確証することに焦点を当てる。暗号化／復号機能の実装は完全にホストオペレーティングシステム上のソフトウェアで実装されているため、TSS にはディスクへアクセスするすべての手段がこれらの機能を通過することを立証しなくてはならない（must）。これは、TOE が実行されるプラットフォームに含まれるすべてのハードドライブについて成り立たなくてはならない（must）。

評価者は、レビューを行うにあたって、MBR のロードと認証機能を実行する TOE の部分に関連した電源投入時に行われるアクティビティの記述が TSS に含まれていることを判定しなくてはならない（shall）。また TSS には、TOE の初期化と、TOE が最初に確立された際にすべてのディスクが完全に暗号化されていることを確証するために行われるアクティビティがカバーされているべきであり、また暗号化されていないディスクの領域（例えば、MBR と関連した部分）も記述されなくてはならない（shall）。

評価者は、DEK がアンラップされ TOE に保存される方法を含め、暗号化機能を行うために FCS 要件中の暗号化機能が用いられる方法もまた、記述でカバーされていることを確証しなくてはならない（shall）。運用環境によって提供されている暗号機能については、評価者は TSS をチェックして、（ST 中に特定されるプラットフォームのそれぞれについて）この機能を呼び出すために TOE によって使われるインタフェースが TSS に記述されていることを確証しなくてはならない（shall）。評価者は、電源断シナリオのそれぞれについて（FCS_CKM_EXT.4 に関する保証アクティビティを参照）、DEK が KEK によってラップされることを TOE が確実にする方法が TSS に記述されていることを確証しなくてはならない（shall）。

評価者は、システム中で利用できる他の機能（例えば、DEK の再生成）が、どのようにして暗号化されていないデータまたは鍵マテリアルがディスク上に存在しないことを確実にするのか、TSS に記述されていることを確証しなくてはならない（shall）。

TOE が複数のディスク暗号化をサポートしている場合、評価者は管理ガイダンスを調査して、プラットフォーム上のすべてのディスクが暗号化されるという必要に初期化手続きが対処していることを確証しなくてはならない（shall）。

評価者は TSS をレビューして、鍵マテリアルが暗号化されずにハードディスクへ書き込まれることはない、ということが立証されていることを判断する。通常の利用ではディスクへのすべての書き込みは暗号化されることになるため、ひとつのアプローチとして、まずディスクの暗号化されない部分へデータが書き込まれる例外的な場合に関する議論を行い、その後これらの領域に鍵マテリアルが書き込まれることが防止される方法を詳述することが考えられる。

評価者は AGD ガイダンスをレビューして、準備的な手順があればそれを含めて、FDE 機能を有効化するために必要な初期化手順が記述されていることを判定しなくてはならない（shall）。ガイダンスには、すべてのプラットフォームについて、暗号化が有効化された際にすべてのハードドライブデバイスが暗号化されることを確証するために十分な指示が提供さてなくてはならない（shall）。

評価者は、下記のテストアクティビティを実施しなくてはならない（shall）。

- テスト 1 : 初期化アクティビティをたどることによって、すべてのディスクが暗号化されることを確証する。暗号化されていないことが判明したデバイスの領域に関しては、一切の利用者データや機密性のある TSF データがこれらの領域へ書き込まれることがないという正当化が（例えば TSS または操作ガイダンスに）提供される。ディスクの調査は、いくつかの方法で行うことができる。物理的にドライブを取り外し、そして別のコンピュータへ挿入するのがひとつの手法である。あるいは、暗号化されたハードドライブを含むシステムを外部デバイスからブートし、その後暗号化されたドライブへ直接アクセスすることも、受容可能な調査手法のもうひとつの例である。
- テスト 2 : データ（OS のページファイルに保存される可能性のあるデータを含む）が、ディスクへの書き込みの際に暗号化されることを確証する。これがテストされる範囲は、先ほどのテストと一貫していること。すなわち、システムを「通常通り」電源投入し、データをディスクへ書き込み、そして先ほどのテストで述べた手法を使ってこれらのデータがデバイス上で暗号化されない形で出現しないことを確証することは受容可能である。

4.1.3 クラス：識別と認証 (FIA)

拡張：FDE 利用者の認証（FIA_AUT_EXT）

FIA_AUT_EXT.1	**拡張：FDE 利用者の認証**
FIA_AUT_EXT.1.1	TSF は、FCS_CKM.1.1(2) 及び FCS_COP.1(4) に定義されるメ

カニズムを用いて、利用者の認証を行わなくてはならない（shall）。

FIA_AUT_EXT.1.2　TSF は、デバイスからの利用者データへのアクセスを許可する前に、FIA_AUT_EXT.1.1 に提供されるメカニズムを用いて利用者認証を行わなくてはならない（shall）。

FIA_AUT_EXT.1.3　TSF は、デバイスからの暗号化されないデータへのアクセスを許可する前に、認可ファクタが有効であることを検証しなくてはならない（shall）。

FIA_AUT_EXT.1.4　TSF は、認可ファクタのそれぞれについて、その検証手法によって KEK、DEK、もしくは KEK または DEK の導出に用いられる CSP が暴露されたり、その実効強度が減少したりしないことを確証しなくてはならない（shall）。

適用上の注意：　この要件の意図は、利用者にディスクの復号が認可され、それによって利用者のシステムへアクセスできるようになるメカニズムを特定することである。これは、個別の利用者の認証とはみなされないことに注意されたい。認可ファクタはコピーされ、ハードディスクのすべての正当な利用者へ提供されてもよい。あるいは、利用者は利用者に一意の認可ファクタを持っていてもよい。

本 PP の将来のバージョンでは、外部トークン認可ファクタが用いられる際には、ブートプロセスが停止して利用者がトークンを取り外さないと継続しないことが求められるかもしれない。

ベンダは、本質的には KEK の連鎖である中間鍵を作成することができる。別の鍵によって暗号化された鍵は、KEK によって暗号化された DEK に関する要件を満たさなくてはならない（must）。すべての中間鍵は、別の鍵によって暗号化する必要がある（has to）。ST 作成者は、FCS_CKM 及び FCS_COP 要件の繰り返しによって、このことを ST へ取り込むべきである（should）。

ハードディスクの認可ファクタが失われたとすると、DEK が TOE からエクスポートされていた場合、または認可ファクタがバックアップされていた場合（あるいは、DEK が異なるセットの認可ファクタによって暗号化され、その認可ファクタが失われていなかった場合）ににみデータを回復することが可能となる。暗号化された DEK が TOE 中で損傷している場合には、認可ファクタのバックアップだけではデータを回復するには十分でないかもしれない。

エレメント 1.3 及び 1.4 は、利用者がデバイス上の情報にアクセスできるようになる前に利用者によって提供された認可ファクタを検証することを取り扱っている。認可ファクタが有効でない場合、TSF が KEK の形成を試み、それを使って DEK のマスクを解除し、その後利用者にでたらめなデータを提示することは望ましくない。しかし、認可ファクタが有効であることのチェックは、攻撃者が他の要件を回避できるような形で行われるべきではない（should not）。この操作は典型的にはホスト上で行われるため、攻撃者によって監視／逆アセンブルされるおそ

れがあり、したがってこの脅威を意識して設計されなくてはならない（must）。

利用者の認証は、デバイスが利用者にアクセス可能となった際（すなわち、システムのブート時）にのみ行うことが必要とされる。上記の要件は、利用者の認証がすべてのデバイスまたはファイルアクセスに先立って行われる必要があることを意味するものと解釈されるべきではない（should not）。しかし、利用者が自分のパスフレーズベースの認可ファクタの変更を望んだ場合には、利用者認可機能はその変更が完了する前に呼び出される必要があることになる。

保証アクティビティ：

評価者は、TSS セクションをチェックして、TOE がどのように初期化されるか、すなわち、電源投入を含む事象のシーケンス、MBR アクセス、及び認可アクティビティを行うコードのロードが記述されているかどうかを判定しなくてはならない（shall）。操作ガイダンスに異なる起動モード（例えば、ブートプロセス中に特定のファンクションキーを押す）が記述されている場合、評価者はこれらのモードが認可ファクタの入力前にどのようにハードディスクへのアクセスを禁止しているかが TSS に記述されていることを確証しなくてはならない（shall）。

評価者は、利用者にドライブ上のデータへのアクセスまたは自分のパスワードの変更を許可する前にどのように認可ファクタが検証されるかが TSS に記述されていることをチェックしなくてはならない（shall）。この記述は、DEK や KEK または他の鍵マテリアルを暴露させないために用いられる 1 つまたは複数の手法を評価者が特定できる程度に詳細でなくてはならない（shall）。「暴露」には、DEK または KEK を弱体化させる概念も含まれる。KEK を作成するためのサブマスクを提供するために別個の認可ファクタが用いられる場合、各認可ファクタを別個の手法でチェックすることは必要とされない。評価者は、テスト報告中に認可ファクタを認証するために用いられるメカニズムの自分の分析を文書化しなくてはならない（shall）（ATE_IND）。

運用環境内で実装されている暗号機能については、評価者は TSS をチェックして、（ST 中に特定されるプラットフォームのそれぞれについて）この機能を呼び出すために TOE によって使われるインタフェースが TSS に記述されていることを確証しなくてはならない（shall）。

評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 1: ハードドライブデバイス上の暗号化されないデータへの一切のアクセスを許可する前に、認可ファクタが要求されることを確証する。
- テスト 2: サポートされている認可ファクタのそれぞれについて、認可ファクタを正しく入力しないと TOE から正しくない認可が行われたという通知が行われることを確証する。
- テスト 3 [条件付き] : 何らかのバイパスまたは代替ブートモードが提供されている場合、そのモードが要件と一貫して

いる（すなわち、暗号化されていないデータへのアクセスの前に適切な認可ファクタが入力される必要がある）ことを確証するテストを行う。

- テスト 4: 認可ファクタを正しく入力してデバイスへアクセスできるようになった後でも、基盤となるプラットフォームに対しては、すでに入力された認可ファクタとは異なる識別と認証が要求されることを確証する。

4.1.4 クラス：セキュリティ管理 (FMT)

このセクションの主要な意図は、不注意な利用者がディスク暗号化装置をセキュアでない状態にすることを防止するために、管理者によって行われなくてはならない（must）（または行われることができてはならない（must not））重要なアクティビティを規定することである。適合 TOE の管理モデルは、本 PP のセクション 1.1.4 に記述されている。TOE によって追加的な機能が提供されている場合、附属書 C からの適切な管理及び I&A 管理が ST に取り込まれるべきである（should）。

管理機能の仕様（FMT_SMF）

FMT_SMF.1	**管理機能の仕様**
FMT_SMF.1.1	TSF は、下記のセキュリティ管理機能を実施できなくてはならない（shall）。 a) **ディスクドライブが暗号化された操作に初期化された際、または管理者のコマンドによって、DEK を生成すること** b) **利用者の入力した認可ファクタ、具体的には [選択：1 つ以上のパスフレーズベースの認可ファクタ、外部トークン認可ファクタ] 及び [選択：その他のファクタなし、TPM 保護された認可ファクタ、[割付：その他の認可ファクタ]] から導出されたサブマスクから形成された KEK を用いて DEK をラップすること** c) **[選択：以下から 1 つを選択：その他の機能なし、[選択：パスフレーズベースの認可ファクタの変更、デフォルトの認可ファクタの変更、外部認可ファクタの生成、暗号機能の構成、鍵回復機能の無効化、[割付：TSF によって提供されるその他の管理機能]]]**
適用上の注意：	この要件の意図は、TOE の有する管理機能を明示することである。これは、TOE が列挙された機能を行うことができなくてはならないことを意味する。項目 (a) 及び (b) は運用での使用に必要な鍵マテリアルを確立し、項目 (c) は TOE に取り込まれてもよいが、PP への適合には必要ではない機能を規定するために使われる。 項目 b については、FCS_CKM.1(2) にしたがって KEK の形成に寄与する適切な認可ファクタが ST 作成者によって規定されるべきである（should）。実装の観点からは、これは認可ファクタを DEK へ束縛し、そのファクタがエンドユーザへ提供できるようにするものである。これらの認可ファクタは、利用者の制御下で入力または生成されなくてはならない（must）。鍵回復機能は存在してもよいが、DEK/KEK が生成される際には回復鍵が存

在しないよう、無効化され（または、無効化できる能力を持た）なくてはならない（must）。項目 b で「パスフレーズベースの認可ファクタ」が選択されている場合には、ST 作成者は項目 c でも「パスフレーズベースの認可ファクタの変更」を選択しなくてはならない。

項目 d（訳注：項目 c の間違い）では、その他の管理機能が提供されない（または主張されない）場合には、「その他の機能なし」が選択されるべきである（should）。その他の共通の選択肢は以下の通り。

- 「外部認可ファクタの生成」が含まれる場合には、附属書 C の C.4 中の要件が ST に取り込まれなくてはならない（must）。
- TOE が暗号機能（例えば、DEK の鍵サイズ）を構成可能としている場合には、「暗号機能の構成」が含まれることになり、さらに提供される機能の詳細がこの要件に箇条書きとして書き込まれるか、あるいは TSS 中に取り込むことができる。
- TOE に鍵回復機能が実際に含まれている場合、回復鍵が生成されないように利用者がこの機能をオフにできる機能を TOE が提供しなくてはならない（must）。
- 「その他の管理機能」に割付が行われている場合、ST が本 PP への適合を主張できるために必要とされる可能性のある保証アクティビティやその他の機能要件が適切に規定されていることを確約するため、評価を監督する国家スキームの意見を求めなくてはならない（must）。

保証アクティビティ：

このこのコンポーネントの保証アクティビティは、ST 作成者によって行われた選択に基づいて行われる。このセクションでは、上記のコンポーネント中の選択（「その他の管理機能」への割付を除く）に関する保証アクティビティを記述する。ある機能が ST 中で選択されていない場合、注記された保証アクティビティを行う必要がないことは理解されるべきである（should）。以下のセクションは、参照を容易とするために「必要なアクティビティ」と「条件付きアクティビティ」に分かれている。

必要とされるアクティビティ

上記の機能を管理者（TOE の利用者のセットのサブセットである特権グループ）に限定する（運用環境から多大な助力を得て行われる可能性がある）のは本 PP に適合した製品の要件であるが、そうするための要件及び関連する保証アクティビティは、特定の TOE の実装に応じて、ST 中の別の場所で課される。本 PP のセクション 1.1.4 に詳述したように、実装可能と思われるシナリオは幅広く、またそれぞれに関連付けられる保証アクティビティは、似通ってはいるものの、範囲と実装の面で異なっている。

概要

評価者は TSS と AGD ガイダンスをレビューし、管理を行うために必要な非 TOE 製品がすべて特定されていることを判定しなくてはならない（shall）。例えば、管理機能が Java アプレットまたはウェブブラウザインタフェース経由で提供されている場合、何を準備する必要があるかの詳細が TSS 中に提供される。

DEK の生成

評価者は AGD ガイダンスをレビューし、DEK を生成するための指示が存在することを判定しなくてはならない（shall）。この指示には、TOE が適合を主張する環境のすべてがカバーされ、さらに DEK の生成または再生成が成功するために存在しなくてはならない前提条件が含まれていなくてはならない（must）。TSS は、DEK の生成方法の記述が AGD ガイダンス中の指示と一貫していることを確実にするためにチェックされ、また異なるプラットフォームに起因する違いがあれば考慮される。また TSS には、新たな DEK が生成されインストールされた際、既存のデータに発生する処理（もしあれば）が記述されなくてはならない（shall）。また評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 1 :「クリーン」な設置上で、管理者が DEK を生成できること。
- テスト 2 : すでに暗号化されたディスクに対して、新たな DEK を生成し、その新たな DEK が以前の DEK と異なることを検証する。
- テスト 3 : TSS 及び AGD_OPR/AGD_PRE ガイダンス中の情報を用いて、DEK 再生成プロセスの機能として TOE の利用者に可視である機能に関して行われたあらゆる主張（例えば、新たな DEK が生成された後でも以前の DEK で暗号化されたファイルが依然として可視である）が検証される。

DEK を適切な認可ファクタからのサブマスクから形成された KEK で保護する

ST には、TOE によってサポートされる認可ファクタが規定され、また TOE 機能を使えるために必要なファクタの数（及び組み合わせ）に関する要件が提供される（これは、FCS_CKM 要件によって行われる）。この要件は、認可ファクタから作成された KEK での DEK の初期ラッピング（または新たな DEK のラッピング）に対応する。認可ファクタは、ディスクごとであっても、利用者ごとであってもよい。評価者は AGD ガイダンスをレビューして、サポートされている各認可ファクタについて、この操作に関してそのファクタが TSF へ入力される方法がガイダンスに詳述されていることを判定しなくてはならない（shall）。評価者は、TSS セクションをレビューして、さまざまなファクタが結合されて KEK が形成される方法と、DEK をマスクするために KEK が使われる方法が記載されていることを判定しなくてはならない（shall）。また、「通常」の操作（すなわち、TOE が確立された後）中に用いられるプロセスとこのプロセスとの間に何らかの違いがあるかどうか、明確になっていなくてはならない

（shall）。また、この記述は FCS_CKM.1* 要件に関する保証アクティビティに記述された情報を包含していてもよい。サポートされた認可ファクタがプラットフォームによって異なる場合には、各プラットフォームでの最低要件と、該当する認可ファクタに関するその他の制限が AGD に明確にされなくてはならない（shall）。また評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 4 : 認可ファクタの受容可能な組み合わせのそれぞれについて、DEK を確立し、そして DEK が暗号化されることになる認可ファクタを管理者が入力できることを確証する。

このテストを行う回数は、実装によって許可される認可ファクタの数によって異なる。認可ファクタは、特に異なる環境で異なる認可ファクタがサポートされている場合（例えば、TPM のある環境とない環境）には、サポートされているさまざまな運用環境（TOE に主張されている）上でテストされるべきである（should）。

条件付きアクティビティ

上記要件の項目 c に含まれるいくつかの選択には、TOE によって提供されてもよいが本 PP へ適合するためには必要とされない機能が規定されている。しかし、その機能が提供される場合、TOE は附属書 C から適切な要件を取り込み、上記の対応する選択を行うことによって適合を主張することができる。適用上の注意にも述べたように、割付がなされた場合、PP への適合が主張できるかどうかを判定するために評価を監督する国家スキームの意見を求める必要がある。

パスフレーズベースの認可ファクタが TOE によって用いられる場合には、「パスワードベースの認可ファクタの変更」項目が選択され、以下の保証アクティビティが行われなくてはならない（shall）。評価者は操作ガイダンスを調査して、パスフレーズベースの認可ファクタが変更される方法が記述されていることを確証しなくてはならない（shall）。また評価者は TSS を調査して、このアクティビティが行われた際にホスト上及びディスクデバイス上で行われる一連のアクティビティが記載されていることを確証し、さらにこの変更中に KEK 及び DEK が暴露されないことを確証しなくてはならない（shall）。また評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 5 [条件付き] : 評価者は、ハードディスクデバイスのパスフレーズ認可ファクタを確立しなくてはならない（shall）。次に評価者は、利用者データをホストからデバイスへ転送しなくてはならない（shall）。次に、「認可ファクタの変更」機能を用いてデバイス上のパスフレーズを変更し、またその際に現在の認可ファクタが求められることを確証しなくてはならない（shall）。現在の認可ファクタとして正しくない値を入力し、認可ファクタへ何の変更も行われないことを確認しなくてはならない（shall）。現在の認可ファクタとして正しい値を入力した際に、デバイス上のデ

ータへ依然としてアクセスできることを確証しなくてはならない（shall）。また評価者は、（認可ファクタの変更が成功した後で）古い認可ファクタを用い、もはやそれによってデバイス上の利用者データへのアクセスが提供されないことを示さなくてはならない（shall）。

ハードディスクデバイスに、デフォルトの認可ファクタが組み込まれて到着する場合もあるかもしれない。その場合には、これらの認可ファクタを変更するメカニズムが存在するように、セクション d（訳注：c の間違い）の選択が行われなくてはならない（must）。操作ガイダンスには、利用者がデバイスの所有権を取得した際にこれらのファクタを変更する手法が記述されなくてはならない（shall）。TSS には、存在するデフォルト認可ファクタが記述されなくてはならない（shall）。また評価者は、下記のテストを実施する。

- テスト 6: [条件付き] TOE がデフォルトの認可ファクタを提供する場合、操作ガイダンス中に記述されるようにデバイスの所有権を取得する途上で、評価者はこれらのファクタを変更しなくてはならない（shall）。次に評価者は、（古い）認可ファクタがもはやデータアクセスに有効ではないことを確認しなくてはならない（shall）。

セクション d（訳注：c の間違い）のアクティビティのうち 2 つは、認可ファクタ（パスフレーズと、外部トークンに保存されるべきビット列）の生成に関するものである。これらの場合のそれぞれについて、附属書 C から追加的要件が ST に取り込まれる。これらの要件と関連付けられるのは、認可ファクタの生成方法の詳細をカバーした保証アクティビティである。この要件について、評価者は AGD 情報をレビューし、認可ファクタメカニズムを呼び出すための指示が、必要な特徴のある認可ファクタが生成できるほど十分に詳細かつ明瞭であることを確証しなくてはならない（shall）。これらのメカニズムと関連付けられたテストは、特定のメカニズムの保証アクティビティの一部として規定される。

一部の TOE では、例えば DEK のビット長や AES で用いられる暗号化モードなど、基盤となる暗号に関する選択が行えるかもしれない。ここでも、TOE が PP への適合を主張するためにはこの機能が提供される必要はない（not have to）。しかし、この機能が提供される場合、それが ST に規定されるとともに選択「暗号機能の構成」が上記の要件中で選択される。

この選択に関して、評価者は ST から暗号機能のどの部分が構成可能なのかを判定しなくてはならない（shall）。これには、FCS 要件だけではなく、TSS 中の関連する記述も、さらには暗号機能に関して TOE と関連付けられた追加的な文書も、調査が必要とされることになる。この情報を得た上で、評価者は AGD 文書をレビューし、主張されるメカニズムのすべてを操作するための指示が存在することを判定しなくてはならない（shall）。また評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 7 [条件付き] : サポートされている構成可能な暗号モードのそれぞれについて、評価者は AGD の指示にしたがって、TOE 機能が期待されたとおり動作する（すなわち、ハードディスクが適切に暗号化／復号される）ことを判定する。この保証レベルでは詳細の検証は必要とされない（すなわち、TOE が 128 ビットまたは 256 ビットの AES 鍵を許可している場合、評価者は鍵の長さを判定するためにデバッガ内でプロセスを実行する必要はない）が、多少の比較分析が行われることは必要とされる。例えば、異なる AES モードがサポートされている場合、同一 DEK で異なるモードを選択すると、ハードディスクには異なる暗号文が存在することになるはずである（should）。

TOE が鍵回復をサポートしている場合、このことが TSS に言明されなくてはならない（must）。また TSS には、この機能を無効化する方法が記述されなくてはならない（shall）。これには、回復の所有者へ回復マテリアルが提供される方法の記述も含まれる。ここでの意図は、この記述をテスト中に評価者が用いて鍵回復機能が本当に無効化されているかどうかを判定できるようにするためである（例えば、KEK/DEK が生成される際にネットワーク接続を介して第三者へ鍵マテリアルが送信されると TSS に言明されている場合、ネットワークモニタを接続して、新たな KEK/DEK が生成された際にネットワーク接続が行われているかどうかを観察する）。この機能を無効化するためのガイダンスは、AGD 文書内に記述されなくてはならない（shall）。

- テスト 8 [条件付き] TOE が鍵回復機能を提供し、その効果が TOE インタフェースにおいて可視である場合には、評価者はベンダによって提供されたガイダンスにしたがって鍵回復機能が無効化されている、または無効化可能であることを確証するテストを考案しなくてはならない（shall）。

4.1.5 クラス：TSF の保護（FPT）

拡張：高信頼更新（FPT_TUD_EXT.1）

FPT_TUD_EXT.1	**拡張：高信頼更新**
FPT_TUD_EXT.1.1	TSF は、TOE ファームウェア／ソフトウェアの現在のバージョンを問い合わせる能力を管理者へ提供しなくてはならない（shall）。
FPT_TUD_EXT.1.2	TSF は、TOE ソフトウェアの更新を開始する能力を管理者へ提供しなくてはならない（shall）。
FPT_TUD_EXT.1.3	TSF は、デジタル署名メカニズム及び [選択 : 公開ハッシュ、その他の機能なし] を用いて、TOE のファームウェア／ソフトウェア更新を、そのインストール前に検証する手段を提供しなくてはならない（shall）。
適用上の注意：	3 番目のエレメントにおいて参照されているデジタル署名メカニズムは、附属書 C の FCS_COP.1(2) に規定されているものである。参照されている公開ハッシュは、附属書 C の FCS_COP.1(3) に規定された機能のひとつによって生成される。

このコンポーネントによって TOE へ更新機能そのものの実装が要求されるが、運用環境内で利用可能な機能を用いて暗号チェックを行うことは許容可能である。

保証アクティビティ： TSF の更新は、権限のあるソースによって署名され、また関連付けられたハッシュが存在するかもしれない。権限のあるソースの定義は、更新検証メカニズムによって用いられる証明書が運用環境にインストールされる方法の記述とともに、TSS 中に含まれる。評価者は、この情報が TSS に含まれ、また更新資格情報のインストールに対応する任意の指示が、操作ガイダンスに詳述されていることを確証する。また評価者は、更新候補が取得される方法、更新のデジタル署名の検証（及び、場合によってはハッシュの計算）に関連した処理、ならびに成功の（署名が検証され、場合によってはハッシュも検証された）場合と不成功の（署名が検証できず、場合によってはハッシュが正しくなかった）場合に行われるアクションが、TSS（または操作ガイダンス）に記述されていることを確証する。デジタル署名／ハッシュが運用環境によって行われる場合、評価者は TSS をチェックして、（ST 中に特定されるプラットフォームのそれぞれについて）この機能を呼び出すために TOE によって使われるインタフェースが TSS に記述されていることを確証しなくてはならない（shall）。

また処理を行うソフトウェアの場所も、TSS に記述され評価者によって検証されなくてはならない（must）。評価者は、以下のテストを行わなくてはならない（shall）（オプションのハッシュが TOE によってサポートされている場合には、評価者はデジタル署名のみのテスト以外に、デジタル署名とハッシュの有効と無効の異なる組み合わせについてテスト 2 と 3 を行う）。

- テスト 1 : 評価者は、バージョン検証アクティビティを行って製品の現在のバージョンを判定する。以下のテストに記述されている更新テストの後、評価者はこのアクティビティを再び行って、バージョンが更新のバージョンと正しく対応していることを検証する。
- テスト 2 : 評価者は、操作ガイダンスに記述されている手順を用いて本物の更新を取得し、その TOE へのインストールが成功していることを検証する。その他の保証アクティビティテストのサブセットを行い、更新が期待されたとおり機能していることを例証する。
- テスト 3 : 評価者は、偽物の更新を取得または作成し、TOE へそれをインストールしようと試みる。評価者は、TOE がその更新を拒否することを検証する。

拡張：TSF のテスト（FPT_TST_EXT.1）

FPT_TST_EXT.1	**拡張：TSF のテスト**
FPT_TST_EXT.1.1	TSF は、最初の起動中（電源投入時）に一連のセルフテストを実行し、TSF の正しい動作を例証しなくてはならない（shall）。
保証アクティビティ：	FCS_RBG_EXT.1 が TOE によって NIST SP 800-90 にしたがっ

て実装されている場合、評価者は NIST SP 800-90 のセクション 11.3 と一貫したヘルステストが TSS に記述されていることを検証しなくてはならない（shall）。

何らかの FCS_COP 機能が TOE によって実装されている場合、これらの機能に関する既知解セルフテストが TSS に記述されなくてはならない（shall）。

評価者は、TSF の正しい動作に影響する非暗号機能の何らかのセットと、これらの機能がテストされる方法が TSS に記述されていることを検証しなくてはならない（shall）。TSS には、これらの機能のそれぞれについて、その機能／コンポーネントの正しい動作が検証される手法が記述される。評価者は、特定された機能／コンポーネントがすべて起動時に十分にテストされていることを判定しなくてはならない（shall）。

4.2 セキュリティ保証要件

セクション 3.1 中の TOE に関するセキュリティ対策方針は、セクション 2.1 中に特定された脅威へ対処するために構築された。セクション 4.1 のセキュリティ機能要件（SFR）は、セキュリティ対策方針の形式的な実体化である。

セクション 4.1 に示されているように、このセクションには CC からの SAR の完全なセットが含まれている一方で、評価者によって行われるべき保証アクティビティはこのセクションと共にセクション 4.1 の両方にも記述されている。

それぞれのファミリについて、「開発者への注意」が開発者アクションエレメントについて提供され、（もしあれば）開発者によって提供される必要のある追加的文書／アクティビティを説明している。内容／提示及び評価者アクティビティエレメントについては、エレメントごとにではなく、ファミリ全体について追加的アクティビティ（セクション 4.1 にすでに含まれているものに加えて）が記述されている。さらに、このセクションに記述された保証アクティビティは、セクション 4.1 に規定されたものとは相補的な関係にある。

表 10 に要約されている TOE セキュリティ保証要件は、本 PP のセクション 3 に特定されている脅威及び方針へ対処するために必要な管理及び評価アクティビティを特定している。セクション 4.3 には、このセクション中のセキュリティ保証要件を選択するための簡潔な正当化が提供されている。

表 6：TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネントの記述
開発	ADV_FSP.1	基本機能仕様
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	利用者準備ガイダンス
試験	ATE_IND.1	独立テスト—適合
脆弱性の評定	AVA_VAN.1	脆弱性分析
ライフサイクルサポート	ALC_CMC.1	TOE のラベリング
	ALC_CMS.1	TOE CM カバレージ

4.2.1 ADV クラス：開発

本 PP に適合する TOE については、TOE に関する情報は ST の TOE 要約仕様（TSS)部分とともに､エンドユーザに利用可能なガイダンス文書にも含まれている｡TOE 開発者が TSS を作成することは要求されてはいないが､TOE 開発者は TSS に含まれている製品の記述を、機能仕様に関して一致させなくてはならない（must)。セクション 4.1 に含まれる保証アクティビティは､TSS セクションにふさわしい内容を判定する上で ST 作成者に十分な情報を提供すべきである（should)。

4.2.1.1 ADV_FSP.1 基本機能仕様

機能仕様には、TSFI が記述される。本 PP によって提供される保証のレベルにおいては、これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 PP に適合する TOE は必然的に TOE の利用者（管理ユーザを含む）によって直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、この保証レベルではそのようなインタフェースそれ自体を規定することにはあまり意味がない。そのようなインタフェースは間接的なテストしかできないためである｡本 PP のこのファミリに関するアクティビティは、機能仕様へ対応した形で TSS に提示されるインタフェースと、AGD 文書に提示されるインタフェースのの理解に焦点を絞るべきである（should)。規定された保証アクティビティを満たすために、追加的な「機能仕様」文書が必要とされるべきではない（should not)。

TOE へのインタフェースを理解するにあたって、対抗されるべき脅威が、攻撃者が電源の入っていないハードディスクを発見してディスク上のデータを得ようとすることである、ということを考慮することは重要である。このことは、TOE が動作中の（すなわち、認可ファクタの入力に成功し TOE がシステムとディスク間で転送されるデータの暗号化と復号を行っている）場合には攻撃者がシステムへアクセスできないことを意味するため、主要な信頼できない利用者とのインタフェースは、システムのブート時に利用者へ提示されるものとなる。これらの「利用者」インタフェースに加えて、管理インタフェース（TOE を構成する方法）も記述される必要がある。

場合によっては、例えばハードディスク上のインタフェースなどの直接呼び出し可能な他のインタフェース（ハードドライブを取り外して別のコンピュータの補助デバイスとして接続するなど）が存在するかもしれないが、これらの場合でも開発者がこの種のインタフェース仕様を配布したり、評価者が（例えばエラーを見つけるために）USB または SCSI インタフェースの実装全体を調査したりすることは必要とされない。評価される必要のあるインタフェースは、独立した抽象的なリストとしてではなく、列挙された保証アクティビティを行うために必要な情報を通して特徴づけされる。

開発者のアクションエレメント：

ADV_FSP.1.1D	開発者は、機能仕様を提供しなくてはならない（shall)。
ADV_FSP.1.2D	開発者は、機能仕様から SFR への追跡を提供しなくてはならない（shall)。
開発者への注意：	このセクションの概論で述べたように、機能仕様は AGD_OPR 及び AGD_PRE 文書に含まれる情報と、ST の TSS に提供される情報との組み合わせで構成されている。機能仕様中の保証アクティビティは、文書及び TSS セクションに存在すべき証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

内容及び提示エレメント：

ADV_FSP.1.1C　機能仕様には、SFR を強制する TSFI 及び SFR をサポートする TSFI のそれぞれについて、その使用目的と使用方法が記述されなくてはならない（shall）。

ADV_FSP.1.2C　機能仕様には、SFR を強制する TSFI 及び SFR をサポートする TSFI のそれぞれに関連付けられるすべてのパラメタが特定されなくてはならない（shall）。

ADV_FSP.1.3C　機能仕様には、SFR 非干渉と分類されているインタフェースについて、その根拠が提供されなくてはならない（shall）。

ADV_FSP.1.4C　追跡は、機能仕様における SFR から TSFI への追跡を例証するものでなくてはならない（shall）。

評価者のアクションエレメント：

ADV_ FSP.1.1E　評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを確認しなくてはならない（shall）。

ADV_ FSP.1.2E　評価者は、機能仕様が SFR の正確かつ完全な実体化であることを判定しなくてはならない（shall）。

保証アクティビティ：

このコンポーネントに関連付けられた具体的な保証アクティビティは存在しない。評価アクティビティをサポートするために提供されるインタフェース文書はセクション 4.1 に記述されており、また AGD、ATE、及び AVA SAR に関するその他のアクティビティが記述されている。

4.2.2 AGD クラス：ガイダンス文書

ガイダンス文書は、開発者のセキュリティターゲットと共に提供される。ガイダンスには、運用環境（ハードディスクを収容する製品）がセキュリティ機能にそれ自身の役割を果たすことができることを管理者が検証する方法の記述が含まれなくてはならない（must）。この文書は、管理者によって読解可能な非形式的なスタイルであるべきである（should）。

ST で主張されているように、製品のサポートするすべての運用環境についてガイダンスが提供されなくてはならない（must）。このガイダンスには、以下が含まれる。

- その環境への TOE のインストールを成功させるための指示、及び
- 製品として、また、より大規模な運用環境のコンポーネントとして、TOE のセキュリティを管理するための指示。

また、特定のセキュリティ機能に関するガイダンスも提供される。そのようなガイダンスに関する要件は、セクション 4.1 に規定された保証アクティビティに含まれている。

すでに述べた領域に加えて、ガイダンスにはどの電源管理モード（例えば、休止状態、スリープ）が OE.POWER_SAVE に適合しているかが規定され、また適合していない電源管理モードを無効化するための指示が提供される。

4.2.2.1 AGD_OPE.1 利用者操作ガイダンス

開発者のアクションエレメント：

AGD_OPE.1.1D　開発者は、利用者操作ガイダンスを提供しなくてはならない（shall）。

開発者への注意：　開発者は、このコンポーネントに関する保証アクティビティをレビューして、評価者がチェックすることになるガイダンスの詳細を確認すべきである（should）。これによって、受容可能なガイドラインの作成に必要な情報が提供されることになる。

内容及び提示エレメント：

AGD_OPE.1.1C　利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用者にアクセス可能な機能及び特権であってセキュアな処理環境において制御されるべきものが、適切な警告を含めて記述されなくてはならない（shall）。

AGD_OPE.1.2C　利用者操作ガイダンスには、利用者の役割のそれぞれについて、TOE によって提供される利用可能なインタフェースをセキュアな方法で利用する方法が記述されなくてはならない（shall）。

AGD_OPE.1.3C　利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用可能な機能及びインタフェース、特に利用者の制御下にあるすべてのセキュリティパラメタが、該当する場合にはセキュアな値を示しつつ、記述されなくてはならない（shall）。

AGD_OPE.1.4C　利用者操作ガイダンスには、利用者の役割のそれぞれについて、利用者にアクセス可能な機能であって、TSF の制御下でエンティティのセキュリティ的な特徴の変更を含めて、実行される必要のあるものに関連するセキュリティ関連事象のすべての種類が明示されなくてはならない（shall）。

AGD_OPE.1.5C　利用者操作ガイダンスには、TOE のすべてのあり得る運用モード（故障または操作エラー後の運用を含めて）と、その結果及びセキュアな運用を維持することへの影響が特定されなくてはならない（shall）。

AGD_OPE.1.6C　利用者操作ガイダンスには、利用者の役割のそれぞれについて、ST に記述されているように運用環境に関するセキュリティ対策方針を達成するために遵守されるべきセキュリティ対策が記述されなくてはならない（shall）。

AGD_OPE.1.7C　利用者操作ガイダンスは、明確かつ妥当なものでなくてはならない（shall）。

評価者のアクションエレメント：

AGD_OPE.1.1E　評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない（shall）*。

保証アクティビティ：　運用中、ガイダンスに記述されるべきアクティビティは大きく 2 つに分類される。一方は（管理者ではない）利用者によって行われるもの、他方は管理者によって行われるものである。非管理ユーザに必要とされる大部分の手続きは、セクション 4.1 の保証アクティビティ中で参照されていることに注意すべきである（should）。しかし、2 つの追加的な警告が、利用者へのガイダンス中に提供されなくてはならない（shall）。ガイダンスでは、正当な利用者に対して、ストレージデバイスに電源が入っている間はそれを自分の物理的な制御下から逸脱させてはならない（must not）という警告が与えられなくてはならない（shall）。

さらに、正当な利用者がパスフレーズまたは外部トークン認可ファクタあるいはその両方を、デバイスとともに、また複数のファクタが用いられる場合にはこれらを一緒に放置／保存してはならない（shall not）ことが言明されなくてはならない（shall）。

管理機能に関しては、いくつかはすでにセクション 4.1 に述べたが、追加的情報が以下のように必要とされる。

文書には、TOE への更新が意図されたソース（ほとんどの場合は TOE のベンダ）からのものであることを検証するためのプロセスが記述されなくてはならない（must）。この検証プロセスは正当な利用者によって開始されるが、デバイス上の TSF によって行われる。評価者は、このプロセスに以下の手順が含まれることを検証しなくてはならない（shall）。

1. FCS_COP.1(2) メカニズムによって、署名された更新が証明書の所有者から受信されていることを確証するために用いられる証明書を取得するための指示。これは、製品と共に最初から供給されていてもよいし、何らかの別の手段によって取得され、最初の構成の一部としてドライブへインストールされてもよい。ドライブ上に最初から供給されていなかった場合、ガイダンスには取得した証明書がエンドユーザによって信頼できるものと判定される方法について指示が与えられなくてはならない（shall）。
2. 更新そのものを取得するための指示。これには、更新をアクセス可能とするための指示（例えば、特定のディレクトリへの格納）が含まれるべきである（should）。
3. 更新プロセスを開始するため、及びそのプロセスが成功したか失敗したかを判別するための指示。

TOE が外部トークン認可ファクタの使用をサポートしている場合、認可ファクタを含む外部トークンデバイス上に一切のデータを置かないよう、ガイダンスで利用者に言明されていることもチェックして確証しなくてはならない（shall）。

4.2.2.2 AGD_PRE.1 準備手続き

開発者のアクションエレメント：

AGD_PRE.1.1D　開発者は、TOE の準備手続きを含めて TOE を提供しなくてはならない（shall）。

開発者への注意：　操作ガイダンスと同様に、開発者は保証アクティビティを見た上で準備手続きに関して必要とされる内容を判定すべきである（should）。

内容及び提示エレメント：

AGD_ PRE.1.1C　準備手続きには、開発者の配付手続きにしたがって配付された TOE をセキュアに受領するために必要なすべての手順が記述されなくてはならない（shall）。

AGD_ PRE.1.2C　準備手続きには、TOE のセキュアな設置に必要なすべての手順と、ST に記述された運用環境に関するセキュリティ対策方針に

したがった運用環境のセキュアな準備に必要なすべての手順が記述されなくてはならない（shall）。

評価者のアクションエレメント：

AGD_ PRE.1.1E　評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない（shall）*。

AGD_ PRE.1.2E　評価者は、TOE が運用のためにセキュアに準備できることを確認するために、準備手続きを*適用しなくてはならない（shall）*。

保証アクティビティ：　上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の構成にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、TOE を収容できると ST が主張しているすべてのプラットフォーム（すなわち、ハードウェアとオペレーティングシステムの組み合わせ）へ十分に対応していることをチェックして確証しなくてはならない（shall）。

評価者は、以下のガイダンスが提供されていることをチェックして確証しなくてはならない（shall）。

- システム（そして特にラップトップ）は、電源管理モード（例えば、休止状態、スリープ／スタンバイ、自動シャットダウン）として利用者のインアクティビティの状態に対処するいくつかのモードをサポートしているのが一般的である。ガイダンスでカバーされる必要のある領域は 2 つ存在する。

  第 1 は、一定期間の利用者のインアクティビティ後にシステムが完全にパワーダウンするようにプラットフォームを構成するために、行われなくてはならない（must）手順に対応する。ここで重要なのは、パワーダウン時に鍵マテリアルが消去され、ハードディスクが脅威モデルの想定する初期状態にあることである。パワーダウンプロセスが開始する前に利用者のインアクティビティによって画面ロックなどの機能がアクティブとなることは許容可能であるが、そのような機能はパワーダウンの代替とはならず、したがってこの要件を満たさない。

  一部のモードは完全にはシステムをパワーダウンしたりオペレーティングシステムをシャットダウンしたりしない。その代わりに、利用者がそのモードに入る前の状態から作業を開始できるように、システムによって何らかの状態が（揮発性メモリまたはディスクへ）保存されている。適合 TOE は、コンピュータを危殆化した状態に放置する一切のモードに入ることを許可されていない。したがって、電力管理状態によって、コンピュータが完全な電源オフ状態と同様に良好に保護されている（すなわち、電源管理モード中ですべてのデータは暗号化され、利用者認証は通常の電源オン時と同様に行われる）ことを確実にしなくてはならない（must）。TOE がこの要件に適合する製品の提供を主張していない場合には、プラットフォームを完全にパワーダ

ウンさせずオペレーティングシステムをシャットダウンさせない任意のモードに TOE が入れないことを例証するガイダンスが TOE に含まれていなくてはならない（must）。したがってガイダンスでカバーされる必要のある 2 番目の領域では、鍵マテリアルが暗号化されずにメインメモリへ依然として電力が供給されているような状態にシステムを放置する任意のモードを無効とするために必要な手順が詳述される。このパワーダウン状態に入った後、最初に必要とされる認可ファクタを入力して KEK を再構築し DEK をアンラップしなければ利用者によるハードディスクのアクセスができないことが事実でなくてはならない（shall）。またガイダンスには、このようなモードを再び有効化する機能を TOE 管理者に限定するための指示が提供されなくてはならない（shall）。

- TOE 認可ファクタを、基盤となる TOE の識別と認証メカニズムの代用として使うことはできない。評価者はガイダンスを調査して、プラットフォームの識別と認証メカニズムの代わりに、またはその一部として認可ファクタを利用する機能が存在する場合、この機能を無効化する方法に関する指示が提供され、また適合 TOE ではこの機能が使われてはならないことを示す警告が管理者へ与えられることを確証しなくてはならない（shall）。
- 製品の設定時にすべてのハードドライブが暗号化されるように製品を構成する方法と、またこれが適合 TOE に対して唯一の許容される構成であることをを詳述した指示及び情報が管理者には与えられる。
- 概論マテリアルに示したように、TOE の管理は TOE の全利用者のグループのサブセットである、1 人以上の管理者によって行われる。システム全体（TOE プラス運用環境）がこの機能を提供することが事実でなくてはならない（must）が、その機能を実装する責任は、完全に運用環境の責任から、完全に TOE の責任まで変動する可能性がある。高レベルにおいては、ガイダンスには運用環境が責任を持つ機能の部分を提供できるように運用環境を構成するための適切な指示が含まれていなくてはならない（must）。利用者全体から管理ユーザを分離するためのメカニズムを TOE が提供しない場合には、例えば、OS の I&A メカニズムが一意の（OS ベースの）利用者の識別を提供するような OS の構成をカバーするような指示と、1 つまたは複数の TOE 管理識別情報を用いた OS の DAC メカニズムの構成を設置者に指示するようなさらなるガイダンスとが与えられ、TOE 管理者のみが管理用実行可能形式へアクセスできるようにする。

  TOE がこの機能の一部または全部を提供する場合には、適切な要件が附属書 C から ST へ取り込まれ、これらの要件と関連付けられた保証アクティビティが TOE と運用環境の両方に必要とされるガイダンスの詳細を提供する。

  また評価者は、下記のテストを実施しなくてはならない

（shall）。

- テスト 1 [条件付き]：すべての TOE 利用者からの管理ユーザの分離が運用環境の構成を通してのみ行われる場合、評価者は、ST 中に主張されるすべての構成について、管理ガイダンスにしたがってシステムを構成した後には非管理ユーザが TOE の管理機能へアクセスできないことを確証する。

4.2.3 ATE クラス：テスト

テストは、システムの機能的側面と、設計または実装の弱点を利用する側面について規定される。前者は ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 PP に規定された保証レベルにおいては、テストは TSS 中に提示された設計情報の利用可能性によって制約された、通知された機能及びインタフェースに基づいて行われる。評価プロセスの主要なアウトプットのひとつは、以下の要件に規定されるテスト報告である。

4.2.3.1 ATE_IND.1 独立テスト—適合

テストは、TSS に記述された機能と、提供された管理（構成及び操作を含む）文書を確認するために行われる。テストで重視されるのは、セクション 4.1 に規定された要件が満たされていることの確認であるが、いくつかの追加的テストがセクション 4.3 中の SAR について規定されている。保証アクティビティは、これらのコンポーネントと関連付けられた最小テストアクティビティを特定する。評価者は、テストの計画及び結果、ならびに本 PP への適合を主張するプラットフォーム／TOE に絞られたカバレージの論拠を文書化した、テスト報告を作成する。

開発者のアクションエレメント：

ATE_IND.1.1D 開発者は、テストに用いられる TOE を提供しなくてはならない（shall）。

内容及び提示エレメント：

ATE_IND.1.1C TOE は、テストに適切なものでなくてはならない（shall）。

評価者のアクションエレメント：

ATE_IND.1.1E 評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない（shall）*。

ATE_IND.1.2E 評価者は、TSF が規定されたように動作していることを確認するために TSF のサブセットを*テストしなくてはならない（shall）*。

保証アクティビティ： 評価者は、システムのテストの側面を文書化したテスト計画とテスト報告を作成しなくてはならない（shall）。テスト計画は、本 PP の保証アクティビティの本体に含まれるすべてのテストアクションをカバーする。保証アクティビティ中に列挙されたテストのそれぞれについて 1 つのテストケースを用意する必要はないが、ST 中の該当するテスト要件のそれぞれがカバーされていることを評価者はテスト計画中に文書化しなくてはならない（must）。

テスト計画にはテストされるプラットフォームが特定され、そしてテスト計画には含まれていないが ST に含まれているプラットフォームについては、そのプラットフォームをテストしな

いことについての正当化をテスト計画が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、行われようとしているテストにその違いが影響しないという論拠が示されなくてはならない（must）。単にその違いが影響しないと主張するだけでは十分ではない。根拠が提供されなくてはならない（must）。評価者は特に、パワーセービング機能や休止状態などの電源管理モードを取り扱う OS ベースのメカニズムを、この正当化を作成する際に考慮しなくてはならない（shall）。ST 中のすべてのプラットフォームがテストされる場合には、根拠は必要とされない。

テスト計画にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。テストの一部としての、または標準的なテスト前の条件としての、各プラットフォームの設置及び設定について、評価者が AGD 文書にしたがうことが期待されていることには注意すべきである（should）。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の性能に悪影響を与えないという、（単なる主張ではなく）論拠が提供される。

テスト計画には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も特定される。これらの手順には、その手順の目標、その目標を達成するために用いられるテスト工程、及び期待される結果が含まれる。テスト報告（テスト計画へ単に注釈を加えたものであってもよい）には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなくてはならず（shall）、したがって失敗に終わったテストの実行が存在し、修正がインストールされ、そして次にテストの再実行が成功した場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果（及びそれを支持する詳細）が示される。

テストアクティビティを行うにあたって、評価者はテストケースがさまざまな運用シナリオを確実にカバーするように、TSS 中のすべての情報を考慮することになる。例えば、DEK が再生成された際、評価者は TSS 及び任意の AGD_PRE または AGD_OPR ガイダンスを調査して、ディスク上のすべての情報が暗号化されたままでなくてはならず（FDP_DSK_EXT.1）、そして鍵マテリアルが利用できる状態で放置されていない（FCS_CKM_EXT.4）ことを確証すべきである（should）。

4.2.4 AVA クラス：脆弱性評定

本プロテクションプロファイルの第一世代については、オープンソースの調査を行って、これらの種類の製品にどのような脆弱性が発見されているのかを見出すことが評価ラボに期待される。多くの場合、これらの脆弱性には基本的な攻撃者を越える巧妙さが必要とされる。ペネトレーションツールが作成されて評価ラボへあまねく配付されるまでは、評価者はこれらの脆弱性のテストを TOE で行うことが期待できないことになる。ラボには、ベ

ンダによって提供された文書を考慮して、これらの脆弱性の存在する可能性についてコメントすることが期待される。この情報はペネトレーションテストツールの開発と、将来のプロテクションプロファイルの開発に用いられることになる。

4.2.4.1 AVA_VAN.1 脆弱性調査

開発者のアクションエレメント：

AVA_VAN.1.1D 開発者は、テストに用いられる TOE を提供しなくてはならない（shall）。

内容及び提示エレメント：

AVA_VAN.1.1C TOE は、テストに適当なものでなくてはならない（shall）。

評価者のアクションエレメント：

AVA_VAN.1.1E 評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない（shall）*。

AVA_VAN.1.2E 評価者は、TOE 中に潜在する脆弱性を特定するために、パブリックドメインソースの検索を*行わなくてはならない（shall）*。

AVA_VAN.1.3E 評価者は、基本的な攻撃能力を有する攻撃者によって行われる攻撃に TOE が耐えられることを判定するために、特定された潜在する脆弱性に基づいて、ペネトレーションテストを*実施しなくてはならない（shall）*。

評価アクティビティ： ATE_IND と同様に、評価者は報告を作成し、この要件に関連する自分たちの結論を文書化しなくてはならない（shall）。この報告は、物理的には ATE_IND に言及される全体的なテスト報告の一部であってもよいし、あるいは別個の文書であってもよい。評価者は、公開された情報の検索を行って、一般的なディスク暗号化製品に発見された脆弱性と、特定の TOE に関する脆弱性を特定する。評価者は、参考としたソースと発見された脆弱性を報告の中に文書化する。発見された脆弱性のそれぞれについて、評価者はそれが該当しないことを示す根拠を提供するか、あるいはそのほうが適切であれば脆弱性を確認するためのテストを策定する（ATE_IND に提供されるガイドラインを用いて）かのどちらかを行う。適切かどうかは、その脆弱性を利用するために必要とされる攻撃ベクトルの評定によって判定される。例えば、ブート時にあるキーの組み合わせを押すことによって脆弱性が検出できる場合、本 PP の保証レベルにおいてはテストが適当と思われる。例えば、脆弱性の悪用に電子顕微鏡と液体窒素が必要とされる場合には、テストは適当ではなく、適切な根拠が策定されることになる。

4.2.5 ALC クラス：ライフサイクルサポート

本 PP に適合する TOE に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの調査ではなく、ライフサイクルのエンドユーザに可視の側面に限定される。これは、製品の全体的な信頼度の向上において開発者の手腕が果たす重要な役割を減じようとするものではない。そうではなく、この保証レベルにおける評価に関して利用可能とされるべき情報を反映したものなのである。

4.2.5.1 ALC_CMC.1 TOE のラベル付け

このコンポーネントは、TOE を同一ベンダの他の製品またはバージョンから区別でき、またエンドユーザによって調達される際に容易に指定できるように、TOE を識別することを目標としている。

開発者のアクションエレメント：

ALC_CMC.1.1D　開発者は、TOE 及び TOE への参照情報を提供しなくてはならない（shall）。

内容及び提示エレメント：

ALC_CMC.1.1C　TOE は、その一意の参照情報によってラベル付けされなくてはならない（shall）。

評価者のアクションエレメント：

ALC_CMC.1.1E　評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない（shall）*。

保証アクティビティ：　評価者は ST をチェックして、ST の要件を満たすバージョンを具体的に特定する識別情報（製品名／バージョン番号など）が含まれていることを確証しなくてはならない（shall）。さらに、評価者は AGD ガイダンス及びテスト用の TOE サンプルをチェックして、バージョン番号が ST 中のものと一貫していることを確証しなくてはならない（shall）。ベンダが TOE を宣伝するウェブサイトを維持管理している場合、評価者はそのウェブサイト上の情報を調査して、ST 中の情報がその製品を識別するために十分であることを確証しなくてはならない（shall）。

4.2.5.2 ALC_CMS.1 TOE の CM カバレージ

TOE の適用範囲とそれに関連した評価証拠の要件を考慮して、このコンポーネントの保証アクティビティは ALC_CMC.1 に関して列挙された保証アクティビティによってカバーされる。

開発者のアクションエレメント：

ALC_CMS.2.1D　開発者は、TOE の構成リストを提供しなくてはならない（shall）。

内容及び提示エレメント：

ALC_CMS.2.1C　構成リストには、以下が含まれなくてはならない（shall）：TOE そのもの、及び SAR によって要求される評価証拠。

ALC_CMS.2.2C　構成リストには、構成要素が一意に識別されなくてはならない（shall）。

評価者のアクションエレメント：

ALC_CMS.2.1E　評価者は、提供された情報が証拠資料の内容及び提示のすべての要件を満たしていることを*確認しなくてはならない（shall）*。

保証アクティビティ：　本 PP において「SAR によって要求される評価証拠」は、ST 中の情報と、AGD 要件の下で管理者及び利用者に提供されたガイダンスとの組み合わせに限られる。TOE が具体的に識別され、その識別が ST 及び AGD ガイダンスの内容と一貫していることを確証する（ALC_CMC.1 に関する評価アクティビティ中で行わ

れるように）ことによって、評価者は暗黙にこのコンポーネントによって要求される情報を確認する。

5 適合主張

適合主張は、PP またはセキュリティターゲット（ST）によって満たされ、評価をパスした要件の集合の源を示している。適用上の注意は、満たされなくてはならない（must）特定の要件をさらに明確にするため、セキュリティ機能要件（SFR）及びセキュリティ保証要件（SAR）のセクション中で提供される。

5.1 PP 適合主張

OSPP は、CC バージョン 3.1 に適合し、CC パート 2 拡張及びパート 3 へ適合する。

本 PP への適合を主張する ST は、CC パート 1 のセクション D3（CCMB-2006-09-001）に定義される正確 PP 適合の最低基準を満たさなくてはならない（shall）。

正確 PP 適合は、PP 中の要件が満たされ、ST が PP の具体化であることを意味している。ST は PP よりも適用範囲が広くてもよいが、そのような場合には評価を監督する国家スキームが追加を承認することになる。ST は、TOE が少なくとも PP と同一の動作をすることを規定するが、運用環境は高々PP と同じ動作をする。本 PP では、規定された要件の意図と、ベンダが要件を満たすための方法に関する期待とを、さらに明確化し説明するための保証アクティビティを提供する。ST の評価者には、ST 及びその記述された TOE が本 PP 中のすべて（場合によってはそれよりもさらに多く）の言明を含むだけでなく、保証アクティビティによって言明される期待を満たすことを判定することによって、正確 PP 適合を確約することが期待される。

5.2 PP 適合主張の根拠

本 PP は、他の PP への適合を主張しない。

6 根拠

このセクションでは、このセキュリティターゲットで定義されるセキュリティ対策方針及びセキュリティ機能要件の根拠と共に、保証要件の根拠を記述する。

6.1 セキュリティ機能要件の根拠

このセクションでは、セクション 4.1 で定義される TOE セキュリティ機能要件の根拠を記述する。TOE によって実装される要件が脅威を低減したり方針を実装したりできる程度に明確な表現を提供するため、以下の本文では要件から、対策方針を通して、該当する脅威／方針までの追跡を行う。表 9（訳注：表 7 の間違い）に、セキュリティ機能要件からセキュリティ対策方針を通して脅威／方針までの対応付けを、その脅威がどのように脅威を軽減または方針に対処するのかという関連する根拠と共に、示した。

以下の表には、附属書 C 中のいくつかの要件、特にセクション C.1 中の要件への参照が含まれていることに注意すべきである（should）。これは、附属書 C 中の他の要件とは異なり、TOE が規定されたセキュリティ方針を満たすためには、これらの要件が TOE または運用環境のいずれかによって実装されなくてはならない（must）ためである。脅威が低減される程度の理解を助けるため、これらのコンポーネントはこの表に入れられている。この表に入っているからと言って、TOE がこれらの附属書 C セクション C.1 の要件を実装しなければならない（must）というわけではない。

表 7：脅威／方針／対策方針／SFR の対応付け／根拠

脅威／方針	対策方針	根拠
T.KEYING_MATERIAL_ COMPROMISE 攻撃者が、TOE が永続的なメモリへ書き込んだ暗号化されていない鍵マテリアル（KEK、DEK、認可ファクタ、サブマスク、及び乱数または鍵が導出されるその他の値）を入手し、これらの値を使って利用者データへのアクセスができるおそれがある。	O.DEK_SECURITY TOE は、1 つ以上のサブマスク（これはさらに認可ファクタから導出される）から作成された鍵暗号化鍵（KEK）を用いて DEK をマスクし、認可ファクタを持たない脅威エージェントが DEK を入手することによって利用者データへアクセスできることのないようにすること。 (FCS_CKM.1(2), FCS_CKM.1(3), FCS_COP.1(4), FCS_RBG_EXT.1) O.KEY_MATERIAL_COMPROMISE TOE は、鍵マテリアルが必要なくなった際にはすぐにそれをゼロ化し、そのようなマテリアルが KEK または DEK の発見のために使われる可能性を減少させること。 (FCS_CKM_EXT.4) O.MANAGE TOE は、正当な管理者を TOE のセキュリティ管理の面でサポートするために必要なすべての機能及び設備を提供し、これらの機能及び設備の不正な利用を制限すること。(FMT_SMF.1)	FCS_CKM.1(3) は、パスフレーズ認可ファクタが用いられた場合、それが十分な KEK が導出されることを確実にするように調整されるという要件を課す。 FCS_CKM.1(2) は、KEK が導出される方法を規定し、また KEK の鍵の長さを規定する要件である。この要件は、パスフレーズ以外の認可ファクタを許可しているが、それぞれの認可ファクタの実効強度が維持されることを義務付けている。換言すれば、他の認可ファクタを導入することによって、調整されたパスフレーズの強度が弱まることはないのである。 FCS_COP.1(4) は、DEK のマスクに用いられる暗号操作の健全な実装を確証している。 FCS_RBG_EXT.1 は、鍵マテリアルが堅牢に生成されることを確証している。パスフレーズ認可ファクタが用いられる場合、または TOE が外部トークン認可ファクタを生成している場合には、この要件はこの対策方針を満たす役割のみを果たすことになる。 FCS_CKM_EXT.4 は、鍵マテリアルがもはや必要なくなった際には利用不可能となることを確証することによって、

脅威／方針	対策方針	根拠
		この対策方針を満たす役割を果たしている。これによって、発見された任意の鍵マテリアルから KEK を導出しようという試みるという攻撃が低減される。 FMT_SMF.1 は、TOE の重要な側面を管理するために必要な機能を TSF が提供することを確証する。これらの機能には、DEK の生成、保護、及び削除、認可ファクタの生成及び構成、ならびに暗号機能の構成が含まれる。ST 作成者は、その他の管理機能を取り込むことを選択することもできる。
T.PERSISTENT_INFORMATION 運用環境が省電力モードに入り、データまたは鍵マテリアルが永続的なメモリ中で暗号化されずに残るおそれがある。	O.KEY_MATERIAL_COMPROMISE TOE は、鍵マテリアルが必要なくなった際にはすぐにそれをゼロ化し、そのようなマテリアルが KEK または DEK の発見のために使われる可能性を減少させること。(FCS_CKM_EXT.4) OE.POWER_SAVE 運用環境は、利用者がシステムのシャットダウンを選択したサイト同一の方法で、一定の時間が経過した後にシステムの電源を落とすメカニズムが少なくとも１つ存在するように、構成可能でなくてはならない（must）（O.SHUTDOWN）。この要件に適合しない任意のメカニズム（例えば、スリープ、休止状態）は、管理者によって無効にで	FCS_CKM_EXT.4 は、もはや必要なくなった際またはシャットダウンの際に、すべての鍵マテリアルがゼロ化されることを要求している。これは、暗号モジュール内部の鍵マテリアルにも、暗号モジュール外部（例えば、メモリ）の鍵マテリアルにも適用される。ほとんどの場合、TSF が必要としなくなった際に大部分の鍵マテリアルはゼロ化されることになるが、鍵マテリアルがいまだに存在する状況や、マシンがシャットダウンされる（手作業またはインアクティビティのため）際には鍵マテリアルはゼロ化される。 OE.POWER_SAVE は、TOE の保護機能が呼び出されるように構成できるプラットフォーム

脅威／方針	対策方針	根拠
	きなくてはならない（must）。 OE.TRAINED_USERS 正当な利用者は、適切に教育されるとともに TOE 及び認可ファクタをセキュアに保つためのすべてのガイダンスを遵守すること。	を提供することによって、脅威を低減する。 同様に、OE.TRAINED_USERS は鍵ゼロ化機能が呼び出されるような方法で利用者がシステムをシャットダウンすることを確実にすることによって、脅威を低減する。
T.KEYSPACE_EXHAUST 権限のない利用者がブルートフォース攻撃を行って暗号鍵または認可ファクタを明らかにし、データまたは TOE リソースへの不正なアクセスができるおそれがある。	O.DEK_SECURITY TOE は、1 つ以上のサブマスク（これはさらに認可ファクタから導出される）から作成された鍵暗号化鍵（KEK）を用いて DEK をマスクし、認可ファクタを持たない脅威エージェントが DEK を入手することによって利用者データへアクセスできることのないようにすること。(FCS_CKM.1(2), FCS_CKM.1(3), FCS_RBG_EXT.1, FCS_COP.1(4), FCS_COP.1(3))	FCS_CKM.1(2) と FCS_CKM.1(3) は、KEK 及び認可ファクタの調整が（それぞれ）KEK/認可ファクタの推定をより困難とするためにランダム化され (FCS_RBG_EXT.1, FCS_COP.1(3))、これらの値のひとつの推定が DEK の推定と同程度に困難であることを確実にするために適切な長さであることを確実にする要件を課す。DEK は、DEK の長さと同等の強度を提供するテクニックを用いてラップされ (FCS_COP.1(4))、したがってこの経路ではブルートフォースよりも優れた攻撃が提供されないことを確実にする。誰にも鍵を読むことができなくすることには、鍵を推定するために必要とされるワークファクタを低下させるような情報を攻撃者が取得する確率を低下させる意味もある。
T.TSF_COMPROMISE 悪意のある利用者またはプロセスが、TSF データまたは実行可能形式	O.CORRECT_TSF_OPERATION TOE は、その運用環境における TSF の正しい動	FPT_TST_EXT.1 は、TOE が運用へ投入される前に、（暗号モジュールと、その他のコンポー

脅威／方針	対策方針	根拠
のコードを不適切な形でアクセス（閲覧、変更、または削除）できるようにしてしまうおそれがある。	作を確実にするため、TSF をテストする機能を提供すること。(FPT_TST_EXT.1) O.TRUSTED_UPDATE TOE は、管理者に TOE のファームウェア／ソフトウェアを更新する機能と、製品への更新が意図されたソースから受信されたことを検証する機能を提供しなくてはならない（shall）。(FCS_COP.1(2), FCS_COP.1(3), FPT_TUD_EXT.1)	ネントの両方について）セルフテストが TOE 上で実行されることを要求する。悪意のある利用者またはプロセスに対して直接的な保護を提供するものではないが、TSF の基盤となるメカニズムが適切に動作していることを確実にすることによって、TSF の危殆化に対する多少の保護を提供する。 暗号学的に検証された更新 (FCS_COP.1(2), FCS_COP.1(3), FPT_TUD_EXT.1) は、悪意のある攻撃者が更新プロセスを通して TOE を損傷したバージョンで置き換えようと試みる可能性を、暗号学的に強力なメカニズムによって更新が署名され、インストールされる前に管理者によって検証されることを確実にすることによって低減させる。
T.UNAUTHORIZED_DISK_ACCESS 紛失したハードディスクへのアクセスを得た権限のないが利用者が、TOE のセキュリティ方針に従えば彼らには権限のないデータへアクセスできるおそれがある。	O.ENCRYPT_ALL TOE は、ハードドライブ上に保存されたすべてのデータを暗号化すること。（MBR 及びそれが参照するブート可能パーティションはこれから除外されるかもしれないことに注意されたい。）(FDP_DSK_EXT.1 FCS_CKM.1(1) FCS_COP.1(1)) O.AUTHORIZATION TOE がハードディスク上のデータを復号できるためには、利用者から認可ファクタを取得しなく	FDP_DSK_EXT.1 によって、すべての利用者データを含め、TOE が完全ディスク暗号化を行うことが確実となる。「完全ディスク暗号化」は、本 PP の用語集に「コンピュータの OS を含め、コンピュータのハードドライブ上のすべてのデータを暗号化し、FDE 製品への認証成功後にのみデータのアクセスを許可するプロセス」として定義されている（MBR 及び認証ファクタの受け入れと処理に

脅威／方針	対策方針	根拠
	てはならない（must）。(FIA_AUT_EXT.1 FCS_CKM.1(2) FCS_COP.1(4)) O.DEK_SECURITY TOE は、1 つ以上のサブマスク（これはさらに認可ファクタから導出される）から作成された鍵暗号化鍵（KEK）を用いて DEK をマスクし、認可ファクタを持たない脅威エージェントが DEK を入手することによって利用者データへアクセスできることのないようにすること。(FCS_CKM.1(2), FCS_CKM.1(3), FCS_COP.1(4), FCS_RBG_EXT.1,) O.KEY_MATERIAL_COMPROMISE TOE は、鍵マテリアルが必要なくなった際にはすぐにそれをゼロ化し、そのようなマテリアルが KEK または DEK の発見のために使われる可能性を減少させること。(FCS_CKM_EXT.4) O.OWNERSHIP TOE は、TOE が動作中に任意の利用者データがアクセスできるようになる前に、所有権が得られている（すなわち、DEK が作成され、認可ファクタが確立され、任意のデフォルト認可ファクタが変更され、KEK が導出されたサブマスクから形成され、そして DEK が KEK と関連付けられている）ことを確実にしなくてはならない（shall）。(FMT_SMF.1)	必要なコードを含む関連したブート可能パーティションを例外として）。（原文の「authentication factors」は「authorization factors」の間違いと思われますが、そのまま訳してあります）これによって、デバイスを紛失した場合であっても、データが暴露されないことが確実となる。 すべてのデータが暗号化されるという要件を持つことに加えて、FCS_CKM.1(1) と FCS_COP.1(1) では暗号化を行うために用いられる鍵の品質と共に、ディスク暗号化操作中に用いられるアルゴリズムと鍵の長さが規定されている。これによって保護が簡単に破られないことが確実となり、したがってデータは確実に保護される。 FIA_AUT_EXT.1 は、FCS_CKM.1(2) と FCS_COP.1(4) に規定されるメカニズムによって、利用者がハードドライブの暗号化されないデータへのアクセスを許可される前に認可されなくてはならない（must）ことを要求している。これによって、権限のない利用者がデータへアクセスするために復号メカニズムを呼び出すことはできないことが確実となる。 鍵または認可ファクタが危殆化した場合には、

脅威／方針	対策方針	根拠
		ディスク上のデータは容易に回復されてしまう。FCS_CKM.1(2)、FCS_CKM.1(3)、FCS_COP.1(4)、FCS_RBG_EXT.1、そしてFCS_CKM_EXT.4のすべてによって、鍵または認可ファクタを取得するコストが、DEKの推測と暗号学的に同程度に困難であることが確実となる。 FMT_SMF.1は、TOEが運用に投入された後では、ディスクドライブ上で暗号化が確立されていないウィンドウが存在しないことを確実にすることによって、脅威へ対処する。また、デフォルト認可ファクタが存在する場合、利用者がこれらの認可ファクタを変更できるようなメカニズムと適切なガイダンスが存在し、それによってデータの自明な危殆化を防ぐことができる。
T. UNAUTHORIZED_UPDATE 悪意のある人物が、TOEのセキュリティ機能を危殆化させるおそれのある製品への更新をエンドユーザへ供給することを試みるおそれがある。	O.TRUSTED_UPDATE TOEは、管理者にTOEのファームウェア／ソフトウェアを更新する機能と、製品への更新が意図されたソースから受信されたことを検証する機能を提供しなくてはならない（shall）。(FCS_COP.1(2), FCS_COP.1(3), FPT_TUD_EXT.1)	更新は、AGD要件とFPT_TUD_EXT.1に規定されているように検証される。この検証は、FCS_COP.1(3) に規定されるハッシュメカニズムや、FCS_COP.1(2)に規定されるデジタル署名メカニズムを利用するために必要とされる。これらの暗号メカニズムを用いて更新を検証することにより、更新が意図されたソースからのものであることが確実となる。

脅威／方針	対策方針	根拠
T.UNSAFE_AUTHFACTOR_VERIFICATION 攻撃者が、利用者の入力した認可ファクタの検証を行うための安全でない手法を利用して、KEK、DEK、または利用者データの暴露を招くおそれがある。	O. SAFE_AUTHFACTOR_VERIFICATION TOE は、KEK や DEK または利用者データが不用意に暴露されないように、認可ファクタの検証を行わなくてはならない（shall）。 (FIA_AUT_EXT.1)	FIA_AUT_EXT.1 は、利用者が USB フラッシュドライブ上のデータへアクセスできるようになる前に、TSF が認可ファクタを検証することを要求している。また、これが DEK または KEK の推測の手掛かりを攻撃者へ与えないような方法で行われることも要求している。

6.2 セキュリティ保証要件の根拠

完全ディスク暗号化デバイスの良好な商慣習と一貫した保証の達成可能なレベルを提供するために、特定の保証要件が選択された。それゆえ、ベンダが適度なソフトウェアエンジニアリング習慣にしたがい、必要な支援ガイダンス文書を提供できると想定して、最低限の追加的タスクがベンダへ課される。選択された保証レベルは、セクション 2 に定義されるセキュリティ課題定義と脅威に対応したものである。この文書は、今後も変化し続ける脅威環境と共に、また開発ベストプラクティスの進歩と共に進化することが意図されており、任意の新たな要件または保証アクティビティが適宜取り込まれることになる。これらの進歩は、実際の評価結果とベンダのコンソーシアムによって推進されることになる。

附属書A： 参考表と参照資料

[1] Common Criteria for Information Technology Security Evaluation, CCMB-2007-09, Version 3.1, September 2007.

[2] Draft Consistency Instruction Manual, for Basic Robustness Environments, Release 4.0, CC version 3.1, 2008

[3] Federal Information Processing Standard Publication (FIPS-PUB) 140-2, Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001 (CHANGE NOTICES (12-03-2002)

[4] Federal Information Processing Standard Publication (FIPS-PUB) 180-2, Secure Hash Standard, August 1 2002

[5] Federal Information Processing Standard Publication (FIPS-PUB) 197, Specification for the Advanced Encryption Standard (AES), November 26, 2001

[6] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, 2001 Edition

[7] NIST Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

[8] NIST Special Pub 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised) , March 2007

[9] NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, April 2008

[10]

[11] RFC 2898 Password-Based Cryptography Specification, Version 2.0, September 2000

[12] RFC 3394 Advanced Encryption Standard (AES) Key Wrap Algorithm, September 2002

略語

AES	Advanced Encryption Standard
AF	認可ファクタ
CAVS	暗号アルゴリズム検証システム
CC	コモンクライテリア
CM	構成管理
COTS	市販（COTS）の
DEK	データ暗号化鍵
DRBG	決定論的ランダムビット生成器
DoD	（米国）国防省
EAL	評価保証レベル
FDE	完全ディスク暗号化
FIPS	連邦情報処理規格
ISSE	情報システムセキュリティエンジニア

IT	情報技術
KEK	鍵暗号化鍵
MBR	マスタブートレコード
OSP	組織のセキュリティ方針
PP	プロテクションプロファイル
PUB	公開
RGB	ランダムビット生成器
SAR	セキュリティ保証要件
SF	セキュリティ機能
SFR	セキュリティ機能要件
ST	セキュリティターゲット
TOE	評価対象
TSF	TOE セキュリティ機能
TSFI	TOE セキュリティ機能インタフェース
TSS	TOE 要約仕様
TOE	評価対象

附属書B： NIST SP 800-53/CNSS 1253 との対応付け

NIST SP 800-53/CNSS 1253 管理策のいくつかは、適合 TOE によって完全または部分的に対処されている。このセクションは対処されている要件を概説し、また TOE がその運用構成に組み込まれた際に（もしあれば）どんな追加的テストが必要かを検定員が判定するために利用することができる。

適用上の注意：このバージョンでは、単純な対応付けのみが提供されている。将来のバージョンでは、検定チームへさらに情報を提供する追加的な説明文が含まれることになる。追加的情報には、SFR から管理策への対応付けに関する詳細が含まれ、TOE によって提供される適合の程度が論じられることになる（例えば、完全に管理策を満たす、部分的に管理策を満たす）。さらに、規定された保証アクティビティの包括的なレビューと、SAR を満たす過程で行われる評価アクティビティがまとめられ、適合が判定される方法（例えば、文書レビュー、ベンダの主張、テスト／検証の程度）に関する情報を検定チームへ提供することになる。この情報は、規定された管理策への適合の程度を判定するために（もしあれば）どんな追加的アクティビティを行う必要があるかを検定チームへ示すことになる。

ST は選択に関して選択を行い、また割付に記入することになるため、ST が完成し評価されるまで最終的なストーリーは必ずしもでき上がらないかもしれない。したがって、この情報は PP に加えて ST にも含まれるべきである（should）。また、特定の実装に基づいて評価者によって行われるアクティビティには何らかの必要な解釈（例えば、「変更」）が存在するかもしれない。スキームは、監督者（例えば、検証者）にこの種の情報を記入させるかもしれないし、あるいは評価者に評価アクティビティの一環として行わせるかもしれない。評価チームの作業に加えて検定チームが（もしあれば）何をする必要があるかを判定できるように、評価アクティビティは提供されなくてはならない（must）必須の情報である。

識別子	名称	該当する SFR
CM-5	変更のためのアクセス制限	FPT_TUD_EXT.1
IA-5	認証子の管理	FCS_CKM.1.1(Y), FIA_AUT_EXT.1, FMT_SMF.1
IA-7	暗号モジュールの認証	FIA_AUT_EXT.1
MP-4	記録媒体の保管	FDP_DSK_EXT.1
SC-12	暗号鍵の確立と管理	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM_EXT.4, FMT_SMF.1
SC-13	暗号の使用	FCS_CKM.1.1(3), FCS_COP.1.1(1), FCS_COP.1.1(2), FCS_COP.1.1(3), FCS_COP.1.1(4), FCS_RBG_EXT.1, FMT_SMF.1
SC-28	情報の安全な保護	FDP_DSK_EXT.1
SI-6	セキュリティ機能の検証	FPT_TST_EXT.1

附属書C： 追加的要件

本 PP の概論で示したように、ベースライン要件（TOE によって行われなくてはならない（must）もの）は本 PP の本体に含まれている。TOE が依然として本 PP に適合するような形で ST に含めることのできる追加的要件が存在する。これらの要件が、この附属書に含まれる。この附属書には、2 つの別個の種類の要件がある。セクション C.1 中のものは、TOE または運用環境のいずれかによって実装されることが要求され、運用環境で実装され TOE（及びその他の多くのセキュリティ製品）によって利用されることが可能な基本的暗号機能を取り扱う。TOE がこの機能を運用環境に依存せず実装することを選択した場合には、これらの要件は ST 作成者によって ST の本体へ移動されることになる。

それに対してセクション C.2 中及びそれ以降の要件は、要求はされないが、TOE によって実装され得るものである。その場合、ST 作成者はこの附属書から適切な情報を取り出し、それを自分の ST へ取り込むことになる。ST 作成者は、附属書 C と関連付けられるかもしれないが列挙されない要件（例えば、FMT タイプの要件）も、ST に確実に取り込む責任があることに注意されたい。この附属書に含まれない要件は、評価を監督する国家スキームによるレビュー及び承認を受けてから、本 PP への適合主張が行えるようになる。

C.1 主要な暗号要件

本 PP の本体で述べたように、TOE がディスク暗号化／復号プロセスをサポートする暗号機能を直接実装しても、あるいはそれが運用環境に存在する場合にはその機能を利用（例えば、オペレーティングシステムの暗号提供インタフェース、サードパーティ製の暗号ライブラリ、またはハードウェア暗号アクセラレータの呼び出し）しても、どちらでも受容可能である。このセクション中の要件は、TOE がそのセキュリティ対策方針を満たすために、TOE または運用環境のどちらかに存在しなくてはならない（must）暗号機能を規定する。その機能が TOE 中に存在する場合には、これらの要件は、保証アクティビティとともに、ST 作成者によって ST の本体へ移動されることになる。

その機能が TOE によって利用されるだけであり、運用環境によって提供される場合には、開発者はこれらの機能を ST に列挙される各運用環境中で特定することになる。この特定は、評価者が（各操作が呼び出される手段が特定されることを要求する）TSS 中の情報と運用環境中の機能に関する情報とを組み合わせてスキーム特定のアクティビティを行い、TOE について列挙された各運用環境でこのセクションの要件が満たされることを検証できるものであるべきである（should）。評価者は運用環境をチェックして、これらの機能が提供され、インタフェースが運用環境文書中に存在することを確認する。暗号サービスの呼び出しは評価者によって本 PP の本体に記述された保証アクティビティが行われる際にテストされることになる。

注意：運用環境中に実装される暗号の承認に関して課される追加的な国家スキームの方針が存在するかもしれない。これには、基盤となるプラットフォームが評価または検証されることが含まれるかもしれない。追加的な「認定」の必要性は、スポンサーとなるスキームによって検証されるべきである（should）。

C.1.1 対称（ディスク）暗号化

この要件は、ディスク上のデータを暗号化及び復号するために用いられる対称暗号化／復号アルゴリズムを規定するために用いられる。

FCS_COP.1(1)	**暗号操作（ディスク暗号化）**
FCS_COP.1.1(1)	**詳細化**：TSF は、**[選択：CBC、XTS] で用いられる AES** 及び暗号鍵サイズが **[選択：128 ビット、256 ビット]** であって、**FIPS**

PUB 197, “Advanced Encryption Standard (AES)” 及び [選択：NIST SP 800-38A、NIST SP 800-38E] を満たす規定された暗号アルゴリズムにしたがって**暗号化及び復号**を行わなくてはならない（shall）。

FCS_COP.1.2(1)　プラットフォーム上の TOE によって用いられる DEK/IV ペアは、一意でなくてはならない（must）。

適用上の注意：　この要件の意図は、承認された AES モードであって ST 作成者がハードディスク上の適切な情報の AES 暗号化に選択できるものを規定することである。最初の選択では、ST 作成者は TOE の実装によってサポートされる 1 つ以上のモードを指定すべきである（should）。2 番目の選択では、FCS_CKM.1(1) に関して規定されたものと同一の、使用する鍵サイズを指定する。3 番目の選択は、最初の選択で選択された 1 つ以上のモードと一致しなくてはならない（must）。複数のモードがサポートされている場合、このコンポーネントが繰り返されれば ST ではより明確となるかもしれない。

CBC と XTS はブロックモード暗号化方式であるため、データの最初のブロックを暗号化するために IV を必要とする。1 つ以上のディスクが IV を必要とする別個の暗号化可能セグメントに分割される方式を TOE が用いている場合には、所与のプラットフォームでデータの暗号化に用いられるすべての DEK/IV ペアは一意でなくてはならない（must）。

本 PP の将来のバージョンでは、新しい暗号モードが NIST によってレビューされ承認されるのにしたがって含まれることになるかもしれない。

保証アクティビティ　複数のモードがサポートされている場合、評価者は TSS とガイダンス文書を調査して、エンドユーザによって特定のモード／鍵サイズが選択される方法を判定する。次に評価者は、各モード／鍵サイズの組み合わせを、以下のセクションに見出される方法で、適宜テストする。これらのテストの一部は、評価機関のスキームに受容可能なアルゴリズムの参照実装を必要とすることになるだろう。

評価者は、ST に列挙されたサポートされているプラットフォームのそれぞれについて、ディスクが暗号化されるプロセスを確実にしなくてはならない（shall）。複数のディスクがサポートされている場合には、この記述はその場合もカバーしなくてはならない（shall）。この記述は、いつ IV が使われる必要があるか、そしてシステムに存在する可能性のある IV の数が明確となるように、ディスクが暗号化可能な部分に分割される方法（または分割されるかどうか）をカバーしなくてはならない（shall）。またこの記述は、システム上で使われるすべての DEK/IV ペアが一意であることを評価者が判定できるように IV の生成をカバーしなくてはならない（shall）。

- ***CBC モード***

CBC モードに関するテストは、

http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf から入手できる The tests for CBC mode are referenced in The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) [AESAVS] に参照されている。

評価者は、TSF によってサポートされている鍵サイズとモードのそれぞれについて、一連の既知解テストを実行しなくてはならない（shall）。入力は鍵と IV、そして暗号化されるべき平文または復号されるべき暗号文である。サポートされている鍵の長さでのこれらのモードに関するすべてのテストベクトル（暗号化と復号の両方）は、http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip から得られるものを利用してこれらのテストを行わなくてはならない（shall）。

評価者は、サポートされている鍵の長さとモードのそれぞれについて、複数ブロックメッセージテストを行わなくてはならない（shall）。このテストを行うために、評価者は暗号化について 10 個、復号について 10 個のデータセットを生成する。各データセットは、鍵と IV、そして平文（暗号化の場合）または暗号文（復号化の場合）から構成される。ブロック長は 128 ビットでなくてはならない（shall）。平文／暗号文の長さは、ブロック長 * i でなくてはならない（shall）。ここで i はデータセット番号であり、i は 1 から 10 の範囲である（したがってメッセージは 128 ビットから 1280 ビットの範囲となる）。

評価者は、サポートされているモードのそれぞれについて、モンテカルロテストを行わなくてはならない（shall）。評価者は 10 セットの暗号化の初期値（鍵、IV、及び平文の値）と、10 セットの復号の初期値（鍵、IV、及び暗号文の値）を生成しなくてはならない（shall）。平文／暗号文の長さは 128 ビットとする（shall）。初期値のセットのそれぞれを用いて 100 通りのテストが生成され、行われる。100 通りのテスト値（初期値のセットのそれぞれについて）を生成するアルゴリズムは [AESAVS] のセクション 6.4.x に含まれており、テストされるモードに依存する。

- ***XTS モード***

XTS モードテストは、http://csrc.nist.gov/groups/STM/cavp/documents/aes/XTSVS.pdf から取得できる The XTS-AES Validation System (XTSVS) [XTSVS] を参照する。

評価者はまず、上記の CBC モードのセクションに特定されるテストを実施する。これらのテストを完了した後、評価者は TSS を調査して XTS モードでサポートされているデータ長の範囲が特定されていることと、tweak 値のフォーマット（128 ビットのビット列またはデータユニットのシーケンス番号）を確認する。

次に評価者は、サポートされている鍵の長さのそれぞれについて、テストセットを考案する。所与の鍵の長さに対して、評価者はテストされる少なくとも 5 通りのデータ長のサンプルを選択する。それぞれのデータ長について、評価者は 100 通りの暗

号化テストと 100 通りの復号テストを考案する。各テストは一意の鍵、tweak、及び平文（暗号化の場合）または暗号文（復号の場合）の値と共に行われる。テストセットの例は、http://csrc.nist.gov/groups/STM/cavp/documents/aes/XTSTestVectors.zip で見ることができる。

C.1.2 署名の検証

この要件は、TOE への更新に関する署名の検証を行うために利用される。

FCS_COP.1(2)	**暗号操作（署名の検証）**
FCS_COP.1.1(2)	**詳細化**：TSF は、**TOE 更新に関する暗号署名の検証**を、***[選択：*** ***(1) 2048 ビット以上の鍵サイズ（法）を用いたデジタル署名アルゴリズム（DSA)、*** ***(2) 2048 ビット以上の鍵サイズ（法）を用いた RSA デジタル署名アルゴリズム（rDSA）、または*** ***(3) 256 ビット以上の鍵サイズを用いた楕円曲線デジタル署名（ECDSA）]*** であって、以下を満たすものにしたがって行わなくてはならない（shall）。 **デジタル署名アルゴリズムの場合**： • **[FIPS PUB 186-3, “Digital Signature Standard”** **RSA デジタル署名アルゴリズムの場合**： • **FIPS PUB 186-3, “Digital Signature Standard”** **楕円曲線デジタル署名アルゴリズムの場合**： • **FIPS PUB 186-3, “Digital Signature Standard”** • **TSF は、「NIST 曲線」P-256、P-384、及び [選択：P-521、その他の曲線なし]（FIPS PUB 186-3, “Digital Signature Standard” の定義による）を実装しなくてはならない（shall）。**
適用上の注意：	ST 作成者は、デジタル署名を行うために実装されたアルゴリズムを選択すべきである（should）。2 つ以上のアルゴリズムが利用できる場合、この要件はその機能を規定するために繰り返されるべきである（should）。選択されたアルゴリズムについて、ST 作成者は適切な割付／選択を行ってそのアルゴリズムに実装されているパラメタを規定すべきである（should）。 楕円曲線ベースの方式に関しては、鍵サイズは基点の位数の 2 の対数を示す。デジタル署名に関する好ましいアプローチとして、本 PP の将来の版では楕円曲線が要求されることになるだろう。
保証アクティビティ：	この要件は、TOE 製造業者からの更新に添付されたデジタル署名を、これらの更新を TOE へインストールする前に検証するために用いられる。このコンポーネントは更新機能において用いられるため、以下に列挙された追加的な保証アクティビティは

この文書の別の保証アクティビティのセクションにおいてカバーされている。以下の保証要件は、デジタル署名アルゴリズムに関する実装のみに適用される。評価者は、コンポーネント中で選択されたアルゴリズムに適切なテストを行う。

これらのアルゴリズムによって必要とされるハッシュ関数または乱数生成あるいはその両方は、ST の中で規定されなくてはならない（must）。したがってこれらの機能と関連付けられた保証アクティビティは、関連する暗号ハッシュ及びランダムビット生成のセクションに含まれる。また、TOE に必要とされる唯一の機能は、デジタル署名の検証である。TOE が本 PP によって要求される何らかの機能の実装をサポートするためにデジタル署名を生成する場合には、それを認識している評価及び検証スキームに問い合わせて必要な保証アクティビティを判定しなくてはならない（must）。

任意のアルゴリズムについて、評価者は TSS をチェックして署名の検証の全体的な流れが記述されていることを確証する。これには少なくとも、デジタル署名の検証に用いられるデータのフォーマットと一般的な場所の特定（例えば、「メモリのロケーション 0x00007A4B」ではなく「ハードドライブデバイス上のファームウェア」）、運用環境から受信されたデータがデバイス上に持ち込まれる方法、そして任意の処理であってデジタル署名アルゴリズムの一部ではないもの（例えば、証明書失効リストのチェック）が含まれるべきである（should）。

以下の各セクションには、デジタル署名方式の種類のそれぞれについて評価者が行わなくてはならない（must）テストが含まれている。要件中の割付と選択に基づいて、評価者はこれらの選択に対応する特定のアクティビティを選択する。

以下に示した方式については、鍵生成／ドメインパラメタ生成に関するテスト要件は存在しないことに注意すべきである（should）。これは、配付された更新のデジタル署名のチェックに機能が制限されているため、この機能がエンドデバイスに必要とされるとは予期されていないためである。これは、ドメインパラメタがすでに生成され、ハードドライブのファームウェアまたはオンボードの不揮発性ストレージの中にカプセル化されているべきであることを意味する。鍵生成／ドメインパラメタ生成が必要とされる場合、評価者と検証スキームに相談して必要とされる保証アクティビティの正しい仕様と任意の追加的なコンポーネントが確認されなくてはならない（must）。

同様に、署名の生成が本 PP のベースライン要件を満たすために必要とされることは予期されていない。署名の生成が必要とされる場合、評価者と検証スキームに相談して必要とされる保証アクティビティの正しい仕様と任意の追加的なコンポーネントが確認されなくてはならない（must）。

- ***RSA***

署名生成／検証機能の実装には、ANSI X9.31 と PKCS #1（バージョン 1.5 またはバージョン PSS、あるいはその両方）という、

2 つの選択肢が存在する。これらの選択肢のうち、少なくとも 1 つが実装されなくてはならない（must）。実装されたバージョンのそれぞれが、以下に示すようにテストされなくてはならない（must）。PKCS #1 バージョン PSS が選択されている場合には、評価者は TSS をチェックしてソルト長が規定されていることを確証しなくてはならない（shall）。

TOE が 2 つ以上の法のサイズをサポートしている場合には、評価者はすべての法のサイズについて以下のテストを行わなくてはならない（shall）。TOE が 2 つ以上のハッシュアルゴリズムをサポートしている場合、評価者はすべてのハッシュアルゴリズムについて以下のテストを行わなくてはならない（shall）。これはつまり、実装で 2 つの法サイズと 2 つのハッシュアルゴリズムの選択が許可されている場合、評価者は以下のテストを 4 回行うことになる。

評価者は、3 グループのデータを生成しなくてはならない（shall）。データの各グループは、法と、その法と両立する 4 セットのテストベクトルから構成される。テストベクトルは、公開鍵指数 *e*、疑似ランダム的に生成されたメッセージ、及び関連付けられた秘密鍵を用いたメッセージの署名（*e* 及び法 *n* と両立するもの）から構成される。つまり、TSF によってサポートされている法のサイズ／ハッシュアルゴリズムのそれぞれについて、最低でも 12 個のテストベクトルが存在することになる。

テストベクトルの 3/4 において正しい署名が生成された（しかしまだ TSF に「供給」されてはいない）後、評価者は公開鍵、メッセージ、または署名（少なくともそれぞれの 2 つについて確実に行うこと）を変更し、署名検証失敗機能がテストされるようにする。次に評価者は、TSF を通してテストベクトルを実行し、結果が正しいことを検証しなくてはならない（shall）。

さらに、実装されているアルゴリズムが *Public Key Cryptography Standards (PKCS) #1 v2.1: RSA Cryptography Standard-2002* に規定される RSASSA-PKCS1-v1_5、または X9.31, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)* に記述される RSA アルゴリズムである場合、http://csrc.nist.gov/groups/STM/cavp/documents/dss/SigVer15EMTest.zip （PKCS #1 Version 1.5 の実装について）または http://csrc.nist.gov/groups/STM/cavp/documents/dss/SigVer931IRTest.zip （X9.31 の実装について）から得られる追加テストベクトルを用いて、評価者はこれらのテストを実装がパスすることを検証しなくてはならない（shall）。

- ***DSA***

評価者は TSS を調査して、(L, N) に用いられる値が与えられ、用いられるハッシュアルゴリズムが規定されていることを確証する。評価者は、特定の (L,N) に用いられるハッシュアルゴリズムが、SP 800-57, *Recommendation for Key Management --Part I: General (Revised)* のセクション 5.6.1 の表 2 及び表 3 に規定される、必要な強度を提供することを検証する。また評

価者は、選択された (L,N) が USB フラッシュドライブ上で用いられる対称（データ）暗号化アルゴリズムと同等の強度を持つことを確証しなくてはならない（shall）（例えば、利用者データの暗号化に 128 ビット AES が用いられる場合には、少なくとも (3072, 256) の (L,N) が必要とされる）。

評価者は、サポートされている (L,N) とハッシュの組み合わせのそれぞれについて、以下のテストを行う。評価者は、鍵ペアを生成しなくてはならない（shall）。次に評価者は、疑似ランダム的に 1024 ビットのメッセージ 15 個を生成し、秘密鍵でそれらに署名する。メッセージの約半分において正しい署名が生成された（しかしまだ TSF に「供給」されてはいない）後、評価者は公開鍵、メッセージ、または署名（少なくともそれぞれの 2 つについて確実に行うこと）を変更し、署名検証失敗機能がテストされるようにする。次に評価者は、TSF を通してテストベクトルを実行し、結果が正しいことを検証しなくてはならない（shall）。

- ***ECDSA***

評価者は、TSS を調査して実装に用いられている 1 つまたは複数の曲線が規定されていて要件と一貫していること、及びサポートされている 1 つまたは複数のハッシュが規定されていることを判定しなくてはならない（shall）。評価者は、TSF によって実装されている曲線とハッシュのペアのそれぞれについて、以下のテストを実施しなくてはならない（shall）。

評価者は、15 セットのデータを生成する。各データセットは、疑似ランダムなメッセージ、公開鍵／秘密鍵のペア (d,Q)、及び署名 (r,s) から構成される。メッセージの約半分において正しい署名が生成された（しかしまだ TSF に「供給」されてはいない）後、評価者は公開鍵、メッセージ、または署名（少なくともそれぞれの 2 つについて確実に行うこと）を変更し、署名検証失敗機能がテストされるようにする。次に評価者は、TSF を通してデータを実行し、結果が正しいことを検証しなくてはならない（shall）。

C.1.3 暗号ハッシュ

この要件は、署名の検証、パスフレーズの調整など、さまざまな高レベルのアクティビティを行うために用いられるハッシュを規定する。

FCS_COP.1(3)	**暗号操作（暗号ハッシュ）**
FCS_COP.1.1(3)	**詳細化** : TSF は、**[選択** : **SHA-1、SHA 224、SHA 256、SHA 384、SHA 512]** にしたがい、**メッセージダイジェストのサイズが [選択** : **160、224、256、384、及び 512] ビット**の、以下 *FIPS Pub 180-3, "Secure Hash Standard"* を満たす**暗号ハッシュサービス**を行わなくてはならない（shall）。
適用上の注意：	この要件の意図は、ハッシュ機能を規定することである。ハッシュの選択は、メッセージダイジェストサイズの選択をサポートしなくてはならない（must）。ハッシュの選択は、FCS_COP.1(1) と FCS_COP.1(2) に用いられるアルゴリズム

の全体的な強度と一貫している（128 ビットの鍵については SHA 256、256 ビットの鍵については SHA 512）べきである（should）。

本 PP のこれ以降の版では、もはや SHA-1 は暗号ハッシュの承認されたアルゴリズムではなくなってしまうことになるだろう。

保証アクティビティ：

評価者は AGD 文書をチェックして、必要とされるハッシュのサイズに機能を構成するために行われる必要のある任意の構成が存在することを判定する。評価者は、ハッシュ機能と他の TSF 暗号機能（例えば、デジタル署名検証機能）との関連が TSS に文書化されていることをチェックしなくてはならない（shall）。

暗号ハッシュのテストは、http://csrc.nist.gov/groups/STM/cavp/documents/shs/SHAVS.pdf から入手できる The Secure Hash Algorithm Validation System (SHAVS) [SHAVS] を参照する。

TSF ハッシュ関数は、2 つのモードのいずれかで実装できる。第 1 のモードは、バイト指向モードである。このモードでは、TSF は長さがバイトの整数倍であるメッセージのみをハッシュする。すなわち、ハッシュされるべきメッセージのビット長が 8 で割り切れる必要がある。第 2 のモードは、ビット指向モードである。このモードでは、TSF は任意の長さのメッセージをハッシュする。各モードについて異なるテストが存在するため、ビット指向とバイト指向のテストについて、以下のセクションで指示を与える。

評価者は、TSF によって実装され、本 PP の要件を満たすために用いられているハッシュアルゴリズムのそれぞれについて、以下のテストのすべてを行わなくてはならない（shall）。

- ***ショートメッセージテスト—ビット指向モード***

評価者は *m*+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは、0 から *m* ビットまでシーケンシャルに変化する。メッセージの本文は、疑似ランダム的に生成されなくてはならない（shall）。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が生じることを確証する。

- ***ショートメッセージテスト—バイト指向モード***

評価者は *m*/8+1 個のメッセージからなる入力セットを作り上げる。ここで *m* はハッシュアルゴリズムのブロック長である。メッセージの長さは 0 から *m*/8 バイトまでシーケンシャルに変化し、各メッセージは整数個のバイトとなる。メッセージの本文は、疑似ランダム的に生成されなくてはならない（shall）。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が生じることを確証する。

- ***選択されたロングメッセージテスト—ビット指向モード***

評価者は *m* 個のメッセージからなる入力セットを作り上げる。

ここで *m* はハッシュアルゴリズムのブロック長である。*i* 番目のメッセージの長さは 512 + 99**i* となる。ここで 1 ≤ *i* ≤ *m*。メッセージの本文は、疑似ランダム的に生成されなくてはならない（shall）。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が生じることを確証する。

- ***選択されたロングメッセージテスト—バイト試行モード***

評価者は *m*/8 個のメッセージからなる入力セットを作り上げる。ここで *m* はハッシュアルゴリズムのブロック長である。*i* 番目のメッセージの長さは 512 + 8*99**i* となる。ここで 1 ≤ *i* ≤ *m*。メッセージの本文は、疑似ランダム的に生成されなくてはならない（shall）。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が生じることを確証する。

- ***疑似ランダム的に生成されたメッセージテスト***

このテストは、バイト指向の実装にのみ行われる。評価者は、*n* ビットの長さのシードをランダムに生成する。ここで *n* はテストされるハッシュ機能によって作り出されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムにしたがって 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が生じることを確証する。

C.1.4 鍵のマスク

この要件は、KEK を用いて DEK をマスクするために用いられる操作を規定する。中間鍵が用いられる場合、ST 作成者はこの要件を繰り返して、これらの場合に用いられるマスクを規定する。

FCS_COP.1(4)	**暗号操作（鍵のマスク）**
FCS_COP.1.1(4)	**詳細化**：TSF は、規定された暗号アルゴリズム **[選択：XOR、ECB モードで用いられる AES、AES キーラップ、パディング付きの AES キーラップ]** 及び暗号鍵サイズ **[選択:128 ビット、256 ビット]** であって、**[選択：XOR については「なし」、ECB モードで用いられる AES については “FIPS PUB 197, Advanced Encryption Standard (AES) and NIST SP 800-38A”、キーラップについては NIST SP 800-38F]** を満たすものにしたがって鍵のマスクを行わなくてはならない（shall）。
適用上の注意：	最初の選択では、ST 選択者は DEK をマスクするために KEK が用いられる手法を選択する。これは KEK と DEK の XOR 演算、ECB モードでの AES の利用、または NIST SP 800-38F に規定される 2 つの AES ベースのキーラップ手法のいずれかである。この選択に基づいて、最後の選択を用いて適切な参照が選択されるべきである（should）（「なし」は XOR に用いられる）。2 番目の選択は、KEK のサイズを反映して行われるべきである（should）。 NIST SP 800-38F は現在、公開前の状態である。公式に公開さ

れた後では、公開されたバージョンが本 PP を用いた新たな評価に適用される。

保証アクティビティ：

DEK のマスク手法が「XOR」を利用する場合、評価者は XOR の利用が TSS に言明されていることを検証しなくてはならない（shall）。

ECB モードでの AES が利用される場合には、以下の保証アクティビティが行われることになる。

評価者は、AES を用いて DEK をマスクするために KEK が利用される手法／アルゴリズムをベンダが記述していることを確証しなくてはならない（shall）（例えば、FIPS 文書によって規定される任意のオプションが特定されていること、入力のパディング手法、出力の切り詰めなど）。

評価者は、下記のテストを実施しなくてはならない（shall）。複数のモードがサポートされている場合、評価者は TSS とガイダンス文書を調査して、エンドユーザによって ECB と規定された鍵サイズが選択される方法を判定する。次に評価者は鍵サイズをそれぞれ、以下のセクションに見出される方法で、適宜テストする。これらのテストの一部は、評価機関のスキームに受容可能なアルゴリズムの参照実装を必要とすることになるだろう。

ECB モードテストは、http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf から入手できる The tests for CBC mode are referenced in The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) [AESAVS] を参照する。

評価者は、TSF によってサポートされている鍵サイズのそれぞれについて、一連の既知解テストを実行しなくてはならない（shall）。入力は、鍵と暗号化されるべき平文または復号されるべき暗号文である。サポートされている鍵の長さでの ECB モードに関するすべてのテストベクトル（暗号化と復号の両方）は、http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip から得られるものを利用してこれらのテストを行わなくてはならない（shall）。

評価者は、サポートされている鍵の長さのそれぞれについて、複数ブロックメッセージテストを行わなくてはならない（shall）。このテストを行うために、評価者は暗号化について 10 個、復号について 10 個のデータセットを生成する。各データセットは、鍵と平文（暗号化の場合）または暗号文（復号化の場合）から構成される。ブロック長は 128 ビットでなくてはならない（shall）。平文／暗号文の長さは、ブロック長 * i でなくてはならない（shall）。ここで i はデータセット番号であり、i は 1 から 10 の範囲である（したがってメッセージは 128 ビットから 1280 ビットの範囲となる）。

評価者は、モンテカルロテストを行わなくてはならない（shall）。評価者は 10 セットの暗号化の初期値（鍵及び平文の値）と、10 セットの復号の初期値（鍵及び暗号文の値）を生成しなくてはならない（shall）。平文／暗号文の長さは 128 ビットとする

（shall）。初期値のセットのそれぞれを用いて 100 通りのテストが生成され、行われる。100 通りのテスト値（初期値のセットのそれぞれについて）を生成するアルゴリズムは [AESAVS] のセクション 6.4.1 に含まれている。

AES キーラップまたはパディング付きの AES キーラップが用いられる場合には、以下の保証アクティビティが行われなくてはならない（shall）。

評価チームは TSS をチェックして、キーラップとアンラップが行われる方法が記述されていることを確証しなくてはならない（shall）。この記述は、暗号操作が実行される方法を指摘するために 800-38F のセクションを参照してもよい。

C.1.5 ランダムビット生成

この要件は、DEK の作成を含め、いくつかの暗号操作において必要とされるランダムビット生成機能に関する要件を規定する。

FCS_RBG_EXT.1 **拡張：暗号操作（ランダムビット生成）**

FCS_RBG_EXT.1.1 TSF は、すべてのランダムビット生成（RBG）サービスを [選択、1 つを選択 : [選択 : Hash_DRBG（任意）、HMAC_DRBG（任意）、CTR_DRBG（AES）、Dual_EC_DRBG（任意）] を用いた NIST Special Publication 800-90 ; FIPS Pub 140-2 Appendix C ; AES を用いた X9.31 Appendix 2.4] にしたがい、[選択、1 つまたは両方を選択 : ソフトウェアベースの雑音源、ハードウェアベースの雑音源] からエントロピーを蓄積するエントロピー源によってシードを供給されて、実施しなくてはならない（shall）。

FCS_RBG_EXT.1.2 決定論的 RBG は、最小で [選択、1 つを選択 : 128 ビット、256 ビット] のエントロピーであって、それが生成する鍵及び認可ファクタの最も長いビット長と少なくとも等しいエントロピーによってシードを供給されなくてはならない（shall）。

適用上の注意 : NIST Special Pub 800-90 の附属書 C には、FIPS-140 の将来のバージョンでおそらく必要とされることになる最小エントロピー量が記述されている。可能であれば直ちにこれを用いるべきであり、また本 PP の将来の版では必要とされることになる。

FCS_RBG_EXT.1.1 の最初の選択に関しては、ST 作成者は RBG サービスが適合する標準（800-90 または 140-2 Annex C のいずれか）を選択すべきである（should）。

SP 800-90 には、4 つの異なる乱数生成手法が含まれる。これらはそれぞれ、基盤となる暗号プリミティブ（ハッシュ関数／暗号）に依存している。ST 作成者は利用される関数を選択し（800-90 が選択されている場合）、要件または TSS に用いられる具体的な基盤となる暗号プリミティブを取り込む。特定されたハッシュ関数（SHA-1, SHA-224, SHA-256, SHA-384, SHA-512）はいずれも Hash_DRBG または HMAC_DRBG に許可されるが、CT_DRBG には AES ベースの実装のみが許可される。800-90 に定義された任意の曲線が Dual_EC_DRBG に許可される一方で、ST 作成者は選択された曲線だけではなく、利用

されるハッシュアルゴリズムも含めなくてはならない（must）。

FIPS Pub 140-2 の附属書 C については、現在のところ *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms* のセクション 3 に記述されている手法のみが有効であることに注意されたい。ここで用いられる AES 実装の鍵の長さが利用者データの暗号化に用いられるものと異なる場合には、異なる鍵の長さを反映するために FCS_COP.1 が調整されるか、繰り返される必要があるかもしれない。FCS_RBG_EXT.1.2 の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。

また ST 作成者は、任意の基盤となる機能が TOE のベースライン要件に含まれていることを確証する。

将来には、*A Method for Entropy Source Testing: Requirements and Test Suite Description* に記述される要件の大部分が本 PP によって要求されることになる。以下の保証アクティビティは、現在のところ要求されるアクティビティのサブセットのみを反映している。

保証アクティビティ：

附属書 G、エントロピーの文書化及び評定にしたがって、文書が作成されなくてはならない（shall）（そして評価者はアクティビティを行わなくてはならない（shall））。

評価者は、RBG が準拠する標準にしたがって、以下のテストを行わなくてはならない（shall）。

- ***FIPS 140-2 の附属書 C へ適合する実装***

このセクションに含まれるテストの参照情報は、*乱数生成検証システム（RNGVS）* [RNGVS] である。評価者は、以下の 2 つのテストを実施しなくてはならない（shall）。「期待値」は、正しいことが知られているアルゴリズムの参照実装によって作成されたものであることに注意されたい。正しさの証明は、各スキームに任されている。

評価者は、可変シードテストを行わなくてはならない（shall）。評価者は 128 セットの (Seed, DT) ペア（それぞれ 128 ビット）を TSF RBG 機能に提供しなくてはならない（shall）。また評価者は、128 ペアの (Seed, DT) すべてについて一定である（AES アルゴリズムに適切な長さの）鍵も提供しなくてはならない（shall）。DT の値は、各セットについて 1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない（shall not）。評価者は、TSF によって返される値が期待値と一致することを確証する。

評価者は、モンテカルロテストを行わなくてはならない（shall）。このテストについては、シード及び DT の初期値（それぞれ 128 ビット）が TSF の RBG 機能に提供される。また評価者は、テストを通して一定である（AES アルゴリズムに適切な長さの）鍵も提供しなくてはならない（shall）。次に評価者は TSF の RBG

を、繰返しのたびに DT の値を 1 ずつ増やしながら、そして *NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms* のセクション 3 に規定されるように次回の繰返しの際の新たなシードを作成して、10,000 回呼び出す。評価者は、作成された 10,000 番目の値が期待値と一致することを確証する。

- ***NIST Special Publication 800-90 に適合する実装***

評価者は、RNG 実装の 15 回のトライアルを行わなくてはならない（shall）。RNG が構成可能な場合、評価者は各構成について 15 回のトライアルを行わなくてはならない（shall）。また評価者は、RNG 機能を構成するための適切な指示が操作ガイダンスに含まれていることも確認しなくてはならない（shall）。

RNG が有効な予測困難性を持つ場合、1 回のトライアルは (1) DRBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) ランダムなビットの 2 番目のブロックを生成し、 (4) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各トライアルに 8 つの入力値を生成しなくてはならない（shall）。最初はカウント (0〜14) である。次の 3 つはエントロピー入力とノンス、そしてインスタンス化操作の個別化文字列である。次の 2 つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の 2 つは、2 番目の生成呼出しへの追加的入力とエントロピー入力である。これらの値は、ランダムに生成される。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が（NIST SP 800-90 に定義される）Output Block Length と等しいランダムなビットを生成することを意味する。

RNG が予測困難性を持たない場合、1 回のトライアルは (1) RDBG をインスタンス化し、 (2) ランダムなビットの最初のブロックを生成し、 (3) シードを再供給し、 (4) ランダムなビットの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各トライアルに 8 つの入力値を生成しなくてはならない（shall）。最初はカウント (0〜14) である。次の 3 つはエントロピー入力とノンス、そしてインスタンス化操作の個別化文字列である。5 番目の値は、最初の生成呼出しへの追加的入力である。6 番目と 7 番目は、シードを再供給する呼出しへの追加的入力とエントロピー入力である。最後の値は、2 回目の生成呼出しへの追加的入力である。

以下のパラグラフには、評価者によって生成／選択されるべき入力値のいくつかについて、より多くの情報が含まれている。

エントロピー入力：エントロピー入力値の長さは、シードの長さと等しくなくてはならない（must）。

ノンス：ノンスがサポートされている場合（df のない

CTR_DRBG はノンスを利用しない)、ノンスのビット長はシードの長さの半分となる。

個別化文字列：個別化文字列の長さは、シードの長さ以下でなくてはならない（must)。実装が 1 通りの個別化文字列の長さしかサポートしていない場合には、両方の値に同一の長さが使用できる。2 通り以上の文字列の長さがサポートされている場合、評価者は 2 つの異なる長さの個別化文字列を用いなくてはならない（shall)。実装が個別化文字列を用いない場合、値を供給する必要はない。

追加的入力：追加的入力のビット長は、個別化文字列の長さと同一のデフォルトと制約を持つ。

C.2 TOE の識別と認証

PP 本体では、TOE が識別と認証（I&A）を行うことは要求されていなかった。TOE は認可ファクタを受領し処理できることを必要とされるが、これは「伝統的」な I&A としては取り扱われない。TOE は管理機能の提供を要求されるが、TOE が TOE の管理機能へのアクセスの制御を運用環境に依存することは受容可能であり、これが現在のところ本 PP に規定されているものである。

しかし、TOE が何らかのレベルの I&A 機能を提供する場合には、ST 作成者は以下の情報を用いることによって、それを規定すべきである（should)。TOE によって提供される機能を記述する情報は、セキュリティ課題記述の情報、対策方針、根拠、要件（及び関連する保証アクティビティ)、そして 800-53/CISSP 1253 の情報が ST に含まれることを確証するために、以下から得られる。

TOE が「管理者」の概念を維持管理しており、この維持管理された識別情報に基づいて管理機能へのアクセスを強制しているが、この識別情報を確立するためにそれ自身のメカニズムを提供してはいない場合（例えば、利用者の識別情報を確立するためにオペレーティングシステムによって渡される情報に依存している場合）には、以下の要件のサブセットが含まれることが必要となるであろう。この場合、ST 作成者は以下の情報の適切なサブセットを含めることと、PP の本体において適切な調整を行うことをしなくてはならない（must)。これらは、評価を監督する国家スキームによってレビューされ、それらが本 PP に適合する ST に帰着することが判定される。

TOE に I&A を行う利用者、及び利用者が行える管理機能に関して TOE が何らかの粒度を提供するという要件は存在しない（例えば、パスフレーズベースの認証を行うためのパスフレーズの作成に制限される管理者と、暗号化を有効化及び無効化できる管理者の違い)。そのような機能が実装されており、ベンダがその機能の ST 中での主張を望む場合には、脅威、対策方針、根拠、SFR、及び保証アクティビティへの適切な追加が起草され、PP 維持管理組織へ提案される必要がある。

表 C.1-1：組織のセキュリティ方針への追加

方針	方針の説明	形式的な組織のセキュリティ方針の参照情報
P.I_AND_A	すべての利用者は、公共オブジェクトを例外として、任意の制御されたリソースへのアクセスを行う前に識別され認証されなくてはならない（must)。	DODI 8500.2 Enclosure 4, Attachment 4 IAIA-2

表 C.1-2：TOE のセキュリティ対策方針への追加

対策方針	対策方針の説明
O.IDAUTH	TOE は、正当な管理者に TOE 管理機能へのアクセスを許可する前に、彼らを識別し認証すること。

O.IDAUTH に加えて、ST 作成者は環境の対策方針 OE.RESTRICTED_FUNCTIONS を TOE の対策方針 O.RESTRICTED_FUNCTIONS へ変更し、それを ST の本体の中の適切な表へ配置することも行わなくてはならない（must）。

表 C.1.-3：セキュリティ対策方針から脅威及び方針への対応付けへの追加

脅威／方針	脅威及び方針に対処する対策方針	根拠
P.I_AND_A すべての利用者は、公共オブジェクトを例外として、任意の制御されたリソースへのアクセスを行う前に識別され認証されなくてはならない（must）。	O.IDAUTH TOE は、正当な管理者に TOE 管理機能へのアクセスを許可する前に、彼らを識別し認証すること。	A.PLATFORM_I&A は、利用者が必要とされる認可ファクタを正しく入力した後に、基盤となる OS が識別と認証を行うことを要求する。しかし、認可ファクタを所有する利用者のサブセットのみが TOE 管理機能を行うことが許可される。 O.IDAUTH は、正当な TOE 管理者が任意の管理機能を呼び出す前に TOE への I&A を行うことを要求することによって、この制約を実装する。

上記の根拠を追加することに加えて、ST 作成者はセキュリティ対策方針から脅威への対応付けの中で環境の対策方針 OE.RESTRICTED_FUNCTIONS を TOE の対策方針 O.RESTRICTED_FUNCTIONS に変更することも行わなくてはならない（must）（変更される要素は対策方針を実装する責任を持つエンティティだけなので、文章はそのまま残してかまわない）。

表 C.1-4：TOE セキュリティ機能要件の根拠への追加

対策方針	対策方針へ対処する要件	根拠
O.RESTRICTED_FUNCTIONS 管理機能は、正当な管理者に限定されること。	FIA_UID.2 FIA_UAU.2 FMT_MOF.1	TOE の利用者は、有効な認可ファクタを所有する個人と定義される。これによってディスク上の情報の復号が許可される。この利用者のセットはまた、基盤となる OS への I&A も行うことができる。しかし TOE に関しては、正当な管理者のみが TOE へアクセスするための有効な

		I&A 資格情報を所有する。TOE へのログインを成功できるすべての利用者は管理者であるため、I&A が成功する前には一切の管理機能が行えないことという要件は、対策方針を実装するのに十分である。「その管理者の代理として…TSF 仲介アクション」は FMT_SMF に定義される管理機能を指しているのであって、ブート以前に行われる機能（例えば、KEK の形成）やハードディスクへの、またはハードディスクからのデータにその場で適用される暗号操作を指しているのではないことに注意すべきである（should）。

利用者の識別 (FIA_UID)

FIA_UID.2	**任意のアクション以前の利用者の識別**
FIA_UID.2.1	**詳細化**: TSF は、その**管理者**の代理としてあらゆるその他の TFS 仲介アクションが許可される前に、それぞれの**正当な管理者**の識別成功を要求しなくてはならない（shall）。
適用上の注意：	ディスク暗号化が初期化された後には、DEK は KEK によって暗号化される必要があり、したがって認可ファクタから導出された鍵によって暗号化される必要があるため、管理者が TOE を管理するには有効な認可ファクタを所有する必要があることに注意されたい。
保証アクティビティ：	識別と認証は両方とも TOE によってシーケンシャルに行われるため、このコンポーネントと FIA_UAU.2 の両方に関する保証アクティビティは FIA_UAU.2 の保証アクティビティのセクションで議論される。

利用者の認証（FIA_UAU）

FIA_UAU.2	**任意のアクション以前の利用者の認証**
FIA_UAU.2.1	**詳細化**: TSF は、その**管理者**の代理としてあらゆるその他の TFS 仲介アクションが許可される前に、それぞれの**正当な管理者**の認証を要求しなくてはならない（shall）。
保証アクティビティ：	FIA_UID.2 の項で述べたように、この保証アクティビティは FIA_UID.2 と FIA_UAU.2 の両方のコンポーネントをカバーする。 評価者は、どのように管理者が TOE に関して確立されるかという議論について、AGD ガイダンスをレビューしなくてはならない（shall）。利用者の識別子と、利用者に対する初期認証情報を作成するための指示が存在することだろう。評価者は、ガイダンスに I&A メカニズムを呼び出すための指示と、（その機能が提供されている場合）認証情報を変更する（例えば、利用者が自分のパスフレーズを変更する）ための指示もガイダンスに含まれていることを判定しなくてはならない（shall）。また構成ガイダンスには、TOE が I&A 機能を実行するために用いる情報を保

護するために必要なプラットフォームの構成があれば、それに関する情報も含まれることになる。

評価者は TSS セクションをレビューして、その I&A メカニズムの機能と利用に関する記述が一貫していることを判定しなくてはならない（shall）。また TSS セクションには、I&A プロセスが成功して完了する前の呼び出しから実際の管理機能が保護される方法が詳述されることになる。この分析の一環として、評価者は管理に用いられる非TOE製品を特定するTSSセクションの情報を利用して、まず TOE への I&A を行わないと、TOE の管理を行うためにこれらの製品を直接呼び出すことができないことを詳述した議論が存在することを確証しなくてはならない（shall）。

また評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 1 : 管理者の ID が確立でき、それを使った TOE へのログインが成功して TOE 管理機能の呼び出しができることを確証する。
- テスト 2 : 利用者 ID または認証情報、あるいはその両方を間違って入力すると、利用者が TOE 管理機能を呼び出すことができないことを確証する。
- テスト 3 : TOE 管理機能を、I&A プロセスをバイパスして直接呼び出すことができないことを確証する。

C.3 暗号サポート要件

標準を参照する鍵管理暗号要件中のいくつかの選択は、PP 本体に規定されたもの以上の追加的な暗号機能を TOE が実装することを要求する。ST の作成途中で、ST 作成者がそのような標準を参照する選択を選択した場合、このセクションには ST の本体に必要とされる追加的な SFR 及び関連する保証アクティビティが含まれる。

これらの要件が ST に含まれる場合には、ST 作成者はこれらの機能がサポートする既存の FCS_COP 要件を判定し、適切な対策方針から要件への根拠のセクション（ほとんどの場合、それは O.AUTHORIZATION になる）を適切に更新することになる。これらの要件はサポート要件なので、対策方針の更新は必要ない。

C.3.1 HMAC 機能

HMAC 機能は、NIST SP 800-90 の HMAC_DRBG や、NIST SP 800-132 における PRF を実装するために用いられる。これには SHA 機能の利用も必要とされるため、この要件が ST に用いられる場合には、適切な選択を行った C.1.2 のハッシュ要件も含まれなくてはならないことに注意されたい。RBG 機能は USB フラッシュドライブ上に実装される必要があるため、この要件を満たすメカニズムは USB フラッシュドライブ上に実装されなくてはならない（must）ことに注意すべきである（should）。鍵の長さ／ハッシュ機能／ブロックサイズ／出力 MAC 長は、1 種類だけ利用されることが期待される。これらのパラメタのいずれかが構成可能な場合には、それを反映してこの要件は ST 中で繰り返されるべきである（should）。

FCS_COP.1	**暗号操作（鍵付き暗号ハッシュ）**
FCS_COP.1.1	**詳細化**：TSF は、**[鍵付きハッシュメッセージ認証コード]** 及び暗号鍵サイズ **[選択：128 ビット、256 ビット]** にしたがい、FIPS

198-1 を満たす**鍵付きハッシュサービス**を行わなくてはならない（shall）。

適用上の注意：　この要件の選択は、DEK のサイズとして規定された鍵サイズと一貫していなくてはならない（must）。

保証アクティビティ：　評価者は TSS を調査して、HMAC 関数に用いられる以下の値が規定されていることを確証しなくてはならない（shall）：鍵の長さ、利用されるハッシュ関数、ブロックサイズ、そして利用される出力 MAC 長。

また管理者は、http://csrc.nist.gov/groups/STM/cavp/documents/mac/HMACVS.pdf から利用可能な鍵付きハッシュメッセージ認証コード検証システム (HMACVS) [HMACVS] に参照されるランダムメッセージテストも行わなくてはならない（shall）。

このテストのため、評価者は 15 セットのテストデータを作成しなくてはならない（shall）。各セットは、鍵とメッセージデータで構成されなくてはならない（shall）。評価者は、TSF によって作成される HMAC が期待値と一致することを確証しなくてはならない（shall）。

C.4 認可ファクタ

このセクションの要件は、FCS_CKM.1.1(2) 中の選択に依存する適切な機能と追加的機能を規定するために用いられる。パスフレーズが選択された場合、このセクションにはパスフレーズの作成と調整に関する要件であって TOE が満たさなくてはならない（must）ものが含まれる (FCS_CKM.1(Y))。また、パスフレーズが TOE で実装されている場合、ST 作成者は ST 作成時に PP 本体の FIA_AUT_EXT.1 要件をこの附属書中のものに置き換えてパスフレーズの変更がセキュアな方法で行われることを確実にし、そして FMT_SMF.1.1c 中で選択「パスフレーズベースの認可ファクタの変更」が行われる（そして関連する保証アクティビティが行われる）ことを確実にする。認可ファクタの提供に TPM が用いられる場合には、以下の前提条件が、運用環境の対策方針と関連付けとともに、ST へ組み込まれなくてはならない（must）。

前提条件	前提条件の説明
A.TPM_PIN_ANTI-HAMMER	TPM デバイス上に保存された認可ファクタは PIN によって保護されなくてはならず、またブルオートフォース推測攻撃を防止するために TPM デバイスは耐破壊性機能を実装しなくてはならない（must）。

前提条件	前提条件に対処する対策方針	根拠
A.TPM_PIN_ANTI-HAMMER TPM デバイス上に保存された認可ファクタは PIN によって保護されなくてはなら	OE.PROTECT_TPM_AF 運用環境は、任意の TPM ベースの認可ファクタが利用組織に適切な強度の PIN に	TPM によって実装された PIN は、それが保護する 128 ビットまたは 256 ビットの認可ファクタよりもかなり

ず、またブルオートフォース推測攻撃を防止するために TPM デバイスは耐破壊性機能を実装しなくてはならない（must）。	よって保護されていることを確実にし、またこの TPM に PIN に対するブルートフォース攻撃を低減する耐破壊性対策が実装されていることを確実にする。	短いため、攻撃者はブルートフォースによって PIN が保護している認可ファクタを推測するよりもはるかに少ない労力でブルートフォースによって PIN を推測できる。運用環境は耐破壊性対策が実施されていること、またそれによってこれらの種類の攻撃が低減されていることを、確実にしなくてはならない（must）。

TOE には、外部認可ファクタまたはパスフレーズベースの認可ファクタのどちらの生成も必要とされない。しかし、TOE がこれらのサービスを提供する場合には、この機能の認定を主張するためにこのセクション中のコンポーネントが TOE の ST へ取り込まれること、及び管理者がそのような認可ファクタの生成を行うことを反映して FMT_SMF.1.1 の項目「c」から適切な選択が行われることが必要とされる。

FCS_CKM.1(Y) **暗号鍵生成（パスフレーズの形成及び調整）**

FCS_CKM.1.1(Y) **詳細化：TSF は、サブマスクを生成するために用いられる** { 大文字、小文字、及び [割付：その他のサポートされる文字] } **のセット中の最大 [割付：8 以上の正の整数] 文字の長さの少なくとも [割付：9 以上の正の整数] 語のパスフレーズをサポートしなくてはならず（shall）、またそのパスフレーズは [選択：**

- **128 ビットの DEK については [選択：SHA-1、SHA-256、SHA-512] を用いて、**
- **256 ビットの DEK については [選択：SHA-256、SHA-512] を用いて、**
- **FCS_RBG_EXT.1 に規定されるランダムビット生成器を用いて生成されたソルトと共に NIST SP 800-132、繰り返し回数 [割付：1000 以上の数]、及び [選択：SHA-1、SHA-256、SHA-512] を用いた HMAC を用いて**

] 調整関数の出力が DEK の（ビット数での）サイズと等しくなるように調整されなくてはならない（shall）。

適用上の注意： パスフレーズは、パスフレーズから導出されたサブマスクを生成するために必要なエントロピーを提供するようにランダムな方法で単語の辞書から取られた単語のシーケンスである。理想的にはこれは TOE によって行われるが、このバージョンの PP には TOE がこのような方法でパスフレーズを構成できるという要件は存在しない。そうではなく、このコンポーネントはパスフレーズの構成に関して TOE がサポートしなくてはならない要件をパスフレーズに課している。結果として作成される文字列は、基盤となる OS によって決定される方式でエンコードされた文字のシーケンスから構成される。このシーケンスは、KEK へ

の入力として用いられるサブマスクを形成するビット列へ調整されなくてはならない（must）。調整は、特定されたハッシュ関数のいずれか、または NIST SP 800-132 に記述されるプロセスを用いて行うことができる。使用される手法は、ST 作成者によって選択される。800-132 による調整が規定された場合には、ST 作成者は行われる繰返し（C）の回数を記入する。この値は、少なくとも 1000 でなくてはならない（must）。また 800-132 では、HMAC と承認されたハッシュ関数から構成された疑似ランダム関数（PRF）の利用も要求されている。ST 作成者は利用されるハッシュ関数を選択し、また附属書 C から適切な HMAC 及びハッシュ関数の要件を取り込む。

本 PP のこれ以降の版では、SHA-1 はもはや暗号ハッシュの承認されたアルゴリズムではなくなることが予想され、また SP 800-132 を用いた調整が必要とされることになる。

保証アクティビティ：

このコンポーネントには、評価を必要とする 2 つの側面が存在する。1～8 文字の単語の辞書から選ばれた少なくとも 9 単語からなるパスフレーズがサポートされていることと、入力される文字が選択された調整関数の対象となることである。これらのアクティビティは、以下の本文で別個に対処される。

少なくとも 9 つの少なくとも 8 文字までの単語の長さのパスフレーズのサポート

評価者は TSS セクションをチェックして ST 中に規定されたこの割付の言明中の最大数の単語からなるパスフレーズを受け付ける機能が存在すること、及び規定された数が少なくとも要件中に示された数であることを判定しなくてはならない（shall）。また評価者は操作ガイダンスをチェックして、管理者がそのようなパスフレーズを生成するための指示が存在し、またパスフレーズが TOE へ入力される方法がガイダンスに示されていることを判定しなくてはならない（shall）。

上記の分析以外にも、評価者は AGD_PRE ガイダンスにしたがって構成された TOE 上で以下のテストを行わなくてはならない（shall）。

- テスト 1：少なくとも 9（あるいは、ST 中で 3 番目の割付に規定された数と、いずれか大きいほう）単語からなるパスフレーズを TOE がサポートしていることを確証する。またこのテストは、2 番目の割付（あるいは、8 といずれか大きいほう）に規定された数までの長さの単語がサポートされていることも検証すべきである（should）。
- テスト 2: ベンダによって供給される操作ガイダンス中に規定されたものと一貫したより短い長さのパスフレーズを TOE がサポートしていることを確証する（例えば、パスフレーズの最小の長さは 5 単語であるとガイダンスに規定されている場合、このテストは少なくとも 5 単語のパスフレーズが TOE によって受け入れられることを判定することになる）。

- テスト 3 [条件付き]：ST 作成者が最初の割付に追加的なサポート文字を記入した場合、規定された特殊文字に関して AGD_OPR または AGD_PRE ガイダンスに含まれるガイダンスに規定されるように構成されたパスフレーズのサポートが TOE に含まれていることを確証する。例えば、パスフレーズには特殊文字が含まれなくてはならない（must）とガイダンスに規定されている場合に、TOE が文字と数字しかサポートしていなかったとすればこのテストは失敗することになる。

パスフレーズの調整

SHA ベースのパスフレーズの調整に関しては、評価者は以下のアクティビティを行う。評価者は、パスフレーズがまずエンコードされてそれから SHA アルゴリズムへ供給される手法が TSS に記述されていることをチェックしなくてはならない（shall）。アルゴリズムの設定（パディング、ブロック化など）が記述されていなくてはならず、またこれらがこのコンポーネントと共に FCS_COP.1(3) 中のハッシュ関数そのものに関する選択によってサポートされていることを評価者は検証しなくてはならない（shall）。評価者は FCS_CKM.1(2) に記述される関数へ入力されることになるサブマスクを形成するためにハッシュ関数の出力が用いられる方法の説明が TSS に含まれており、また FCS_CKM.1(1) に規定される DEK と同じ長さであることを検証しなくてはならない（shall）。

800-132 ベースのパスフレーズの調整に関しては､必要とされる保証アクティビティは適切な附属書 C の要件に関する保証アクティビティが行われる際に行われる。KEK を形成するために使われることになるサブマスクの形成に、何らかのマスター鍵の操作が行われる場合には、それが TSS に記述されなくてはならない（shall）。

入力されたパスフレーズからサブマスクを形成するための明示的なテストは、必要とされない。

FIA_AUT_EXT.1 **拡張：FDE 利用者の認証**

FIA_AUT_EXT.1.1 TSF は、FCS_CKM.1.1(2) 及び FCS_COP.1(4) に定義されるメカニズムを用いて、利用者の認証を行わなくてはならない（shall）。

FIA_AUT_EXT.1.2 TSF は、デバイスからの利用者データへのアクセスを許可する前に、FIA_AUT_EXT.1.1 に提供されるメカニズムを用いて利用者認証を行わなくてはならない（shall）。

FIA_AUT_EXT.1.3 TSF は、デバイスからの暗号化されないデータへのアクセスを許可する前に、認可ファクタが有効であることを検証しなくてはならない（shall）。

FIA_AUT_EXT.1.4 TSF は、認可ファクタのそれぞれについて、その検証手法によって KEK、DEK、もしくは KEK または DEK の導出に用いられる CSP が暴露されたり、その実効強度が減少したりしないことを確証しなくてはならない（shall）。

FIA_AUT_EXT.1.5 TSF は、FMT_SMF.1(c) に規定されるように利用者へパスフレーズベースの認可ファクタの変更を許可する前に、FIA_AUT_EXT.1.1 に提供されるメカニズムを用いて利用者の認証を行わなくてはならない（shall）。

適用上の注意： この要件の意図は、利用者にディスクの復号が認可され、それによって利用者のシステムへアクセスできるようになるメカニズムを特定することである。これは、個別の利用者の認証とはみなされないことに注意されたい。認可ファクタはコピーされ、ハードディスクのすべての正当な利用者へ提供されてもよい。あるいは、利用者は利用者に一意の認可ファクタを持っていてもよい。

本 PP の将来のバージョンでは、外部トークン認可ファクタが用いられる際には、ブートプロセスが停止して利用者がトークンを取り外さないと継続しないことが求められるかもしれない。

ベンダは、本質的には KEK の連鎖である中間鍵を作成することができる。別の鍵によって暗号化された鍵は、KEK によって暗号化されたDEKに関する要件を満たさなくてはならない（must）。すべての中間鍵は、別の鍵によって暗号化する必要がある。ST 作成者は、FCS_CKM 及びFCS_COP 要件の繰り返しによって、このことを ST へ取り込むべきである（should）。

ハードディスクの認可ファクタが失われたとすると、DEK が TOE からエクスポートされていた場合、または認可ファクタがバックアップされていた場合（あるいは、DEK が異なるセットの認可ファクタによって暗号化され、その認可ファクタが失われていなかった場合）ににみデータを回復することが可能となる。暗号化された DEK が TOE 中で損傷している場合には、認可ファクタのバックアップだけではデータを回復するには十分でないかもしれない。

エレメント 1.3 及び 1.4 は、利用者がデバイス上の情報にアクセスできるようになる前に利用者によって提供された認可ファクタを検証することを取り扱っている。認可ファクタが有効でない場合、TSF が KEK の形成を試み、それを使って DEK のマスクを解除し、その後利用者にでたらめなデータを提示することは望ましくない。しかし、認可ファクタが有効であることのチェックは、攻撃者が他の要件を回避できるような形で行われるべきではない（should not）。この操作は典型的にはホスト上で行われるため、攻撃者によって監視／逆アセンブルされるおそれがあり、したがってこの脅威を意識して設計されなくてはならない（must）。

利用者の認証は、デバイスが利用者にアクセス可能となった際（すなわち、システムのブート時）にのみ行うことが必要とされる。上記の要件は、利用者の認証がすべてのデバイスまたはファイルアクセスに先立って行われる必要があることを意味するものと解釈されるべきではない（should not）。しかし、利用者が自分のパスフレーズベースの認可ファクタの変更を望んだ場合には、利用者認可機能はその変更が完了する前に呼び出さ

れなくてはならないことになる。

保証アクティビティ： 評価者は、TSS セクションをチェックして、どのように TOE が初期化されるか、すなわち、電源投入を含む事象のシーケンス、MBR アクセス、及び認可アクティビティを行うコードのロードが記述されているかどうかを判定しなくてはならない（shall）。操作ガイダンスに異なる起動モード（例えば、ブートプロセス中に特定のファンクションキーを押す）が記述されている場合、評価者はこれらのモードが認可ファクタの入力前にどのようにハードディスクへのアクセスを禁止しているかが TSS に記述されていることを確証しなくてはならない（shall）。

評価者は、利用者にドライブ上のデータへのアクセスまたは自分のパスワードの変更を許可する前にどのように認可ファクタが検証されるかが TSS に記述されていることをチェックしなくてはならない（shall）。この記述は、DEK や KEK または他の鍵マテリアルを暴露させないために用いられる 1 つまたは複数の手法を評価者が特定できる程度に詳細でなくてはならない（shall）。「暴露」には、DEK または KEK を弱体化させる概念も含まれる。KEK を作成するためのサブマスクを提供するために別個の認可ファクタが用いられる場合、各認可ファクタを別個の手法でチェックすることは必要とされない。評価者は、テスト報告中に認可ファクタを認証するために用いられるメカニズムの自分の分析を文書化しなくてはならない（shall）（ATE_IND）。

運用環境内で実装されている暗号機能については、評価者は TSS をチェックして、（ST 中に特定されるプラットフォームのそれぞれについて）この機能を呼び出すために TOE によって使われるインタフェースが TSS に記述されていることを確証しなくてはならない（shall）。

評価者は、下記のテストを実施しなくてはならない（shall）。

- テスト 1: ハードドライブデバイス上の暗号化されないデータへの一切のアクセスを許可する前に、認可ファクタが要求されることを確証する。
- テスト 2: サポートされている認可ファクタのそれぞれについて、認可ファクタを正しく入力しないと TOE から正しくない認可が行われたという通知が行われることを確証する。
- テスト 3 [条件付き] : 何らかのバイパスまたは代替ブートモードが提供されている場合、そのモードが要件と一貫している（すなわち、暗号化されていないデータへのアクセスの前に適切な認可ファクタが入力される必要がある）ことを確証するテストを行う。
- テスト 4: 認可ファクタを正しく入力してデバイスへアクセスできるようになった後でも、基盤となるプラットフォームに対しては、すでに入力された認可ファクタとは異なる識別と認証が要求されることを確証する。

FCS_CKM_EXT.1(X)　暗号鍵の生成（外部トークン認可ファクタの生成）

FCS_CKM_EXT.1.1(X)　TSF は、FCS_RBG_EXT.1 に規定されるランダムビット生成器であって、FCS_CKM.1(1) に規定される DEK のサイズと少なくとも等しいエントロピーによってシードを供給された [選択：128 ビット、256 ビット] の認可ファクタを作成するものによって生成された外部認可ファクタを導出しなくてはならない（shall）。

FCS_CKM_EXT.1.2(X)　TSF は、認可ファクタを [選択：外部デバイス、TPM] 上に保存できなくてはならない（shall）。

適用上の注意：　最初の選択には、FCS_CKM.1(1) において DEK に規定されたものと同一のビット数を指定すべきである（should）。2 番目の選択は、生成された認可ファクタを TOE が保存できなくてはならないデバイスの種類を規定するために使われるべきである（should）。TOE が認可ファクタの生成のみを行い、認可ファクタの適切なデバイス上への保存を運用環境に依存している場合には、このコンポーネントの最初のエレメントだけを含む新たなコンポーネントを作成し、それを ST に取り込むことは受容可能である。この場合にも、すべての保証アクティビティが適用される。

保証アクティビティ：　評価者はガイダンス文書をレビューして、管理者が外部認可ファクタを生成するために必要な手順が記述されていることを確認する。評価者は ST の TSS の部分をレビューして、生成機能が RBG を利用する方法と RBG 機能がシードを供給される方法とを含め、外部認可ファクタ生成プロセスが記述されていることを確認する。最後に、評価者は TSS セクション（または管理ガイダンス文書）をレビューして、RBG によって生成された値がこのセクションに規定されたデバイスへ転送される方法を判定する。この要件が ST 中で主張されるためには、利用される RBG は TOE によって提供されるとともに FCS_RBG_EXT.1 に規定される要件を満たさなくてはならないことには注意すべきである（should）。

以下のテストが、評価者によって行われなくてはならない（must）。

- テスト 1：管理ガイダンスにしたがって、外部トークン認可ファクタを作成する。可能であれば、認可ファクタに含まれるビット数を確認する。外部認可ファクタをその「コンテナ」へロードする。すると外部認可ファクタを用いて暗号化されたディスクがアクセスできるようになることを確証する。

C.5 プラットフォームの電源管理モードのサポート

すでに述べたように、TOE が動作するプラットフォームでは、ときには利用者による完全なシャットダウン以外の 1 つまたは複数の「パワーダウン」モードがサポートされているかもしれない。これらのモードでデータが揮発性メモリに残される場合には、そのデバイス（例えば、ラップトップ）がこの状態で攻撃者によって持ち去られた際に、セキュリティ方針の抜け穴となってしまうおそれがある。

一部の TOE では、メモリからディスクへ転送される情報が FDP.DSK_EXT.1.1 にしたがっ

て暗号化され、プラットフォームが低電力モードにある間にも情報が正しく保護される（そして機密性のある情報はメモリ上に維持されない）ような機能を提供しているかもしれない。このような場合には、ST 作成者が以下の要件を用いてこの機能を規定すべきである（should）。

C.5.1 電源管理機能

FDP_PM_EXT.1 **電源管理状態でのデータの保護**

FDP_PM_EXT.1.1 TSF は、FDP_DSK_EXT.1.1 に示された [割付：この機能が提供されるパワーダウン状態] 状態への移行中にディスクドライブへ保存されたすべてのデータを保護しなくてはならない（shall）。

FDP_PM_EXT.1.2 FDP_HIB_EXT.1.1 に示された状態から電源オン状態への復帰に当たって、TSF は任意のデータを復号する前に FIA_AUT_EXT.1.1 に規定された方法で利用者を認可しなくてはならない（shall）。

適用上の注意： 最初の選択に関しては、TOE によって適切に保護される状態について管理ガイダンスに用いられているものと同じ名前を用いて、ST 作成者はこの状態を記入する。

運用環境ベースの資格情報を用いて指定された状態からデバイスをアンロックすることは十分ではないことに注意すべきである（should）。ここでの意図は、指定された状態からの復帰を（認可の観点から）完全な電源オフ状態からの復帰と等価とすることである。

保証アクティビティ： 評価者は TSS を調査して、この機能によってサポートされている状態が記述されていることを確証しなくてはならない（shall）。各状態について、評価者はその状態に入る方法と、その状態に入る際の TSF のアクションの記述が TSS に含まれていることを確証する。また TSF には、その状態から抜ける方法と、この運用状態への移行中に要件がどのように満たされるかも記述されなくてはならない（shall）。

評価者は管理ガイダンスをチェックして、TOE によってサポートされている状態が記述され、これらのモードと TOE の正しい構成に関する情報が提供されていることを判定しなくてはならない（shall）。

以下のテストは、サポートされている状態のそれぞれについて評価者によって行われなくてはならない（must）。

- テスト 1：操作ガイダンスにしたがって、プラットフォームの低パワー状態が保護されるように運用環境と TOE を構成する。低パワー状態に入る。通常の電源状態への復帰に当たって、認可ファクタの正しくない入力によってシステムへのアクセスが可能とならないことと、認可ファクタの正しい入力によってシステムへのアクセスが可能となることを確認する。ここでの意図は、デバイスからの暗号化されないデータへのアクセスを許可する前にシステムによって行われるアクティビティが TOE による認可ファクタの有効性の検証のみであるように、利用者はまず認可ファクタを

求められるべきであるということである。

附属書D： 文書の表記

英国式つづりを米国式つづりに置き換えた以外には、本 PP に用いられる記法、様式、及び表記はコモンクライテリア（CC）のバージョン 3.1 と一貫している。PP の読者を助けるため、選択された表記法についての議論をここで行う。

PP の読者を助けるため、選択された表記法についての議論をここで行う。CC では、機能及び保証要件に対していくつかの操作を行うことを許可している。*詳細化*、*選択*、*割付*、及び*繰返し*が CC 3.1 のパート 1 の附属書 C4 に定義されている。これらの操作のすべてが、本 PP で用いられている。

詳細化の表記

詳細化の操作は、要件に詳細を付け加え、これによってさらに要件を制約するために用いられる。セキュリティ要件の詳細化は、エレメント番号の後に**太字**で表記された「詳細化」という単語と、太字で表記された要件中の追加的な本文によって示される。詳細化によって、元の要件を「弱める」ことはできない。詳細化された要件を満たす TOE は、PP/ST の文脈で詳細化されていない要件もまた満たさなくてはならない（must）（CC 3.1 のパート 1、附属書 C.4.4 を参照）。また詳細化は CC の文言の削除によって行われてもよく、これは本文の~~取り消し~~線によって示される。

選択の表記

選択の操作は、CC によって要件の言明中に提供された 1 つ以上の選択肢を選択するために用いられる（CC 3.1 のパート 1、附属書 C.4.3 を参照）。PP 作成者によってなされた選択は**太字**で表記されたその選択と、大かっこ及び「選択」の文字を削除して示される。ST 作成者によって記入されるべき選択は、大かっこ中に選択が行わるべきことを示す指示によって示される： [選択：]。

割付の表記

割付の操作は、例えばパスフレーズの長さのように、まだ規定されていないパラメタへ特定の値を割り付けるために用いられる（CC 3.1 のパート 1、附属書 C.4.2 を参照）。**太字**で示された値は、その割付が PP 作成者によってなされたことを示し、大かっこと「割付」の文字は削除される。ST 作成者によって記入されるべき割付は、大かっこ中に割付が行わるべきことを示す指示によって示される： [割付：]。

繰返しの表記

繰返しの操作は、変化する操作と共にコンポーネントが繰り返される場合に用いられる（CC 3.1 のパート 1、附属書 C.4.1 を参照）。繰返し回数（iteration number）は、コンポーネントの識別子に引き続く括弧の中で示される。

繰返しの操作は、すべてのコンポーネント上で実行できる。PP/ST 作成者は、同一のコンポーネントに基づく複数の要件を取り込むことによって、繰り返し操作を行う。コンポーネントの各繰返しは、そのコンポーネントの他のすべての繰り返しとは異なっていなくてはならず、これは割付及び選択を異なる方法で完成させることによって、または異なる方法で詳細化を適用することによって、実現される。繰返しの例は FCS_COP.1 であり、3 つの異なる暗号アルゴリズムの実装を要求するために 3 回繰り返されている。

異なる繰返しは、これらの要件への、及びこれらの要件からの明確な根拠と追跡を可能とすることによって一意に特定されるべきである（should）。

拡張要件の表記

拡張要件は、作成者のニーズを満たす適切な要件を CC が提供していない場合に許可される。

拡張要件は特定されなくてはならず、またその要件を関連付けるにあたって CC のクラス／ファミリ／コンポーネントモデルを利用することが要求される。拡張要件は、コンポーネント中に「EXT」を挿入することによって示される。

前提条件、脅威、組織のセキュリティ方針、及び対策方針の名前の表記：

前提条件：TOE セキュリティ環境の前提条件には、「A.」で始まりそれ以降にすべて大文字の記述的なラベルが続く名前を与えられる（例えば、A.TRAINED_ADMINISTRATORS）。

脅威：TOE セキュリティ環境の脅威には、「T.」で始まりそれ以降にすべて大文字の記述的なラベルが続く名前が与えられる（例えば、T.ACCIDENTAL_ADMIN_ERROR）。

方針の言明：方針の言明には、「P.」で始まりそれ以降にすべて大文字の記述的なラベルが続く名前が与えられる（例えば、P.AUTH_FACTORS）。

TOE のセキュリティ対策方針：セキュリティ対策方針には、「O.」で始まりそれ以降にすべて大文字の記述的なラベルが続く名前が与えられる（例えば、O.CRYPTOGRAPHY）。

運用環境のセキュリティ対策方針：運用環境のセキュリティ対策方針には、「OE.」で始まりそれ以降にすべて大文字の記述的なラベルが続く名前が与えられる（例えば、OE.NO_EVIL）。

適用上の注意

1 適用上の注意には、TOE の構築または使用に関連する、または役立つと考えられる追加的なサポート情報が含まれる。また適用上の注意には、コンポーネントの許可された操作に関するアドバイスも含まれる。

保証アクティビティ

保証アクティビティは、TOE に課された機能要件が脅威を低減するための共通評価方法として役立つ。このアクティビティには、TSS に文書化された TOE の特定の側面を評価者が分析するための指示が含まれているため、ST 作成者にはこの情報を TSS セクションへ取り込むという暗黙の要件が課される。

附属書E： 用語集

これらの定義は、この PP 全体で用いられる用語に適用される。

管理者 - TOE を構成する能力のある利用者。

認可ファクタ (AF) - 利用者がハードディスクを使用する権限のあるコミュニティに属していることを立証するために TOE へ提出される値であって、KEK として（調整または結合あるいはその両方が行われた後に）用いられる。したがって、各ファクタは KEK の生成に必要とされるため、すべての AF は利用者によって正しく提示されなくてはならない（must）。これらの AF は、利用者の特定の識別情報を立証するためには用いられないことに注意されたい。外部トークン認可ファクタは、外部トークン上に保存されるものである。TPM 保護認可ファクタは、TPM 上に保存されるものである（TPM は運用環境の一部であって、TOE の一部ではない）。外部認可ファクタは、外部トークン認可ファクタか、TPM 保護認可ファクタのいずれかである。

正当な利用者 - 管理者によって TOE を使用するための認可ファクタが与えられている利用者。

データ暗号化鍵 (DEK) - ハードドライブを暗号化するために暗号化アルゴリズムによって用いられる鍵。

決定論的ランダムビット生成器 (DRBG) - 秘密の初期シード値からビットのシーケンスを作り出す暗号アルゴリズム。シード値の知識がないと、出力されたシーケンスは DRGB のセキュリティレベルまで予測不能となるはずである（should）。

エントロピー源 - この暗号機能は、1 つ以上の雑音源からの出力を蓄積することによってランダムビット生成器にシードを供給する。この機能には、所与の出力を推測するために必要とされる最低限の労力の計量と、雑音源が適切に動作していることを確実にするためのテストが含まれる。

FIPS 承認済み暗号機能 - セキュリティ機能（例えば、暗号アルゴリズム、暗号鍵管理テクニック、あるいは認証テクニック）であって、 1) 連邦情報処理規格 (FIPS) に規定されているか、 2) FIPS に採用され、FIPS の附属書または FIPS によって参照される文書のどちらかに規定されているもの。

完全ディスク暗号化 (FDE) - 全ディスク暗号化とも呼ばれ、コンピュータの OS を含め、ハードドライブ上のすべてのデータを暗号化することによって、FDE 製品への認証成功後にのみデータへのアクセスを許可するプロセスである。ソフトウェアによる暗号化製品は、ドライブ上のマスタブートレコード（MBR）及びブート可能パーティションの部分を暗号化しないことがある。本プロテクションプロファイルでは、ディスク暗号化は NIST の定義を、利用者データを含む可能性のある情報が書き込まれていない限りはドライブの MBR 及びブート可能パーティションをソフトウェアディスク暗号化製品が暗号化しないことを許可するように変更したものとする。複数のドライブが利用される場合、「完全ディスク暗号化」の概念はすべてのドライブが暗号化されることを要求する。

運用環境 - TOE 境界の外部に存在するハードウェア及びソフトウェアであって、TOE の機能及びセキュリティ方針をサポートするもの。すべてのハードウェア、関連するファームウェア、及びオペレーティングシステムを含む。

鍵暗号化鍵 (KEK) - DEK を暗号化するために用いられる鍵。注意：別の間接化の層を付け加えることもできる。例えば、DEK を暗号化し KEK によって暗号化される中間鍵。

鍵マテリアル - KEK、DEK、中間鍵、認可ファクタ及び乱数、または鍵が導出されるその他の値。

マスタブートレコード (MBR) - 通常、MBR はハードディスクの最初のセクタに存在する。MBR は、パーティションテーブルを調べることによって判定したブート可能パーティションをロードする。

雑音源 - RBG のコンポーネントであって、非決定論的なエントロピーを作り出すアクティビティを含むもの。

運用環境 - その中で TOE が運用される環境。

永続的メモリ - 電源が切られた後でも長期間データを保持するデータストレージ。

ランダムビット生成器 (RBG) - エントロピー源と DRBG によって構成される暗号機能であって、鍵マテリアルを作り出すために必要とされるランダムビットを得るために呼び出される。

権限のない利用者 - TOE への有効な認可ファクタを所有しない利用者。

揮発性メモリ - 電源が切られた後にその内容が失われるメモリ。

ゼロ化 - この用語は、メモリロケーションを参照しないことと、それを定数によって積極的に上書きすることとを区別するために用いられる。鍵マテリアルは、それがもはや必要なくなった際には上書きされる必要がある。

附属書F： PP 識別情報

タイトル :	Protection Profile for Software Full Disk Encryption−Mitigating the Risk of a Lost or Stolen Hard Disk （ソフトウェア完全ディスク暗号化のプロテクションプロファイル—ハードディスクの盗難・紛失リスクの低減）
バージョン :	1.0
スポンサー :	（米国）国家安全保障局 (NSA)
CC のバージョン :	Common Criteria for Information Technology Security Evaluation (CC) Version 3.1R3, July 2009. （情報技術セキュリティ評価のためのコモンクライテリア（CC）バージョン 3.1 改訂第 3 版、2009 年 7 月）
評価レベル :	評価保証レベル (EAL) 1
キーワード :	認可ファクタ、認可サブシステム、DEK、ディスク暗号化、暗号化サブシステム、KEK

附属書G： エントロピーの文書化と評価

エントロピー源の文書は、それを読んだ後の評価者が完全にエントロピー源を理解し、それがエントロピーを供給すると信頼できる理由を理解できるように、十分に詳細であるべきである（should）。この文書には、設計の記述、エントロピーの正当化、運用条件、及びヘルステストという、複数の詳細なセクションが含まれるべきである（should）。この文書は、TSS の一部である必要はない。

設計の記述

文書には、すべてのエントロピー源コンポーネントの相互作用を含めた、エントロピー源の全体的な設計が含まれなくてはならない（shall）。これにはエントロピー源の動作が記述され、どのように動作するのか、どのようにエントロピーが作り出されるのか、そしてどのように未処理（生の）データをエントロピー源の内部からテスト目的で取り出すことができるのか、などが含まれることになる。この文書では、エントロピー源の設計の概略が説明され、ランダム性がどこから由来し、次にどこへ渡されるのか、任意の生の出力の後処理（ハッシュ、XOR など）、保存されるのか（保存されるとすればどこに）、そして最後に、どのようにしてエントロピー源から出力されるのかを示すべきである（should）。処理に課される条件があれば（例えば、ブロッキング）、それもエントロピー源の設計の中で記述されるべきである（should）。図や例を利用することが望ましい。

また、この設計にはエントロピー源のセキュリティ境界の内容の説明と、境界外部の敵対者がエントロピー量に影響を与えられないことがどのようにしてセキュリティ境界によって確実とされるのかという説明が含まれなくてはならない（must）。

エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、エントロピー源が確率的な挙動を示すことがなぜ確信できるのか（確率分布の説明と、その分布が特定のエントロピー源によって得られるという正当化を行うことは、これを記述する方法のひとつである）という、技術的な議論が存在すべきである（should）。この議論には、期待されるエントロピー量の記述と、十分なエントロピーが TOE のランダム化シード供給プロセスへ与えられると確信できる理由の説明が含まれることになる。この議論は、エントロピー源がエントロピーを含むビットを作り出すと信頼できる理由の正当化の一部となる。

運用条件

また文書には、エントロピー源がランダムデータを生成すると期待される運用条件の範囲も含まれることになる。これには、これらの条件の下でエントロピー源が動作し続けることを確実にするために、システムの設計に取り入れられた対策が明確に記述されることになる。同様に、文書にはエントロピー源が不調または一貫しない動作となることがわかっている条件も記述されなくてはならない（shall）。エントロピー源の故障または機能低下を検出するための手法が、含まれなくてはならない（shall）。

ヘルステスト

さらに具体的に、すべてのエントロピー源ヘルステストとその根拠が文書化されることになる。これには、ヘルステストの記述、各ヘルステストが行われる頻度及び条件（例えば、起動時、連続、またはオンデマンド）、各ヘルステストに期待される結果、そしてそれぞれのテストがエントロピー源の 1 つ以上の故障を検出するために適当であると信じられる理由を示す根拠が含まれることになる。