フルディスク暗号化のプロテクションプロファイル

紛失または盗難にあったハードディスクのリスクの軽減

原文タイトル：

Protection Profile for Full Disk Encryption

Mitigating the Risk of a Lost or Stolen Hard Disk

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。
http://www.niap-ccevs.org/pp/pp_fde_v1.0.pdf

Information Assurance Directorate

NSA 情報保証局

2011 年 12 月 1 日
バージョン 1.0

平成 24 年 3 月 13 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

表一覧

改定履歴

バージョン	日付	説明
1.0	2011年12月1日	初回リリース

1 はじめに（イントロダクション）

1.1 TOE の PP の概要

本PPは、紛失または盗難にあった機密データが含まれたハードディスク（例えば、ラップトップに収容されたディスクやポータブルの外付けハードディスクドライブ)を敵対者が入手するという脅威に対処する。本プロテクションプロファイル（PP）で定義されている評価対象（TOE）は、フルディスク暗号化製品である。NISTで定義されている通り、「*フルディスク暗号化（FDE）*は、完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用されるハードドライブ上のすべてのデータを暗号化し、FDE製品への認証が成功した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] ソフトウェア暗号化製品では、マスタブートレコード（MBR）と初期ブート可能なパーティションについて、ドライブの一部が暗号化されない状態で残ることに注意すること。本プロテクションプロファイルでは、用語「ディスク暗号化」は、利用者データが含まれる可能性がある情報が書き込まれていない限り、ソフトウェアディスク暗号化製品でMBR及びブート可能なパーティションについて、ドライブの一部が暗号化されない状態で残ることを許可するように変更された、NISTのフルディスク暗号化の定義と解釈されるだろう。

1.1.1 TOE の利用と主要なセキュリティ機能

TOEは、保存されているデータを保護するために使用される。一連の対策方針とセキュリティ機能要件は、敵対者による事前のアクセスなしに電源オフの状態で紛失または盗難にあったデバイス（一般的にラップトップ）に限定される。

ハードディスクはデータ暗号化鍵（DEK）を使用して暗号化される。DEKは鍵の暗号化鍵（KEK）を使用してマスキングされる。KEKは複数のコンポーネント（サブマスクと呼ばれ、認証要素から導出される）から導出するか、または1つのサブマスクから取得することができる。格納デバイスの暗号化における最大のセキュリティ対策方針は、敵対者に非常に大きい鍵空間で暗号解読を実行せざるを得なくすることである。

本PPに適合するTOEは、主な機能を実装する。認証機能が確立したら、TOEの利用者の認証要素を収集してKEKを形成する。ディスク暗号化機能が、DEKを使用して格納デバイスに書き込まれたすべてのデータを暗号化及び復号する。両方の機能を備えている必要があるため、例えば、製品を本PPに適合させる必要があるハードドライブ開発者は、その製品またはハードドライブと共に評価している付属の製品のいずれかが認証機能に対応していることを保証しなければならない。評価のスポンサーは、評価チームが保証アクティビティを実施するために必要となるすべての情報を提供しなければならない。

ベンダは、サポートされるすべての運用環境（例えば、製品でサポートされるすべてのO/S）でTOEを正しくインストール及び管理するため、構成ガイダンス（AGD_PRE、AGD_OPR）を提供することが必要となる。

1.1.2 許可と認証

ハードディスクの許可された利用者は、コンピュータのブート時に1つ以上の認証要素を提供する。これらの認証要素によって、ディスクドライブ上のデータへのアクセスを利用

[1] NIST「GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES」、NIST Special Pub 800-111、2007 年 11 月。

者に許可するかどうかが決まる。認証要素は、個々の利用者ごとに一意である必要はない。つまり、ディスク暗号化機能の認証要素は、ハードディスク上に保存された情報へのアクセスが許可された利用者のコミュニティに所有者が所属していることを証明するためにのみ必要である。

利用者が正しい認証要素を提供すると、オペレーティングシステムが復号され、多くの場合、オペレーティングシステムの通常のログインプロンプトが利用者に表示される。基盤となるOSに対する利用者の識別と認証、及びTOE管理機能については、以降の節で説明する。

認証要素は、次のいずれかで構成される必要がある。

- 管理者が提供するパスフレーズ、または
- 外付けトークン認証要素として定義される、外付けトークン（例えば、USBデバイス）に含まれたビット文字列、または
- パスフレーズと外付けトークン認証要素の組み合わせ。

また、上記のいずれかに加えて、次のもので構成される場合もある。

- セキュリティターゲット（ST）作成者が定義した認証要素

ST作成者が追加の認証要素を定義する場合は、それらの追加の認証要素を完全に文書化しなければならず、パスフレーズ認証要素及び／または外付けトークン認証要素の強度を低下させてはならない。すべての認証要素は、保護対象の鍵と同じサイズ（ビット長）のサブマスクを提供することを条件付けなければならない。また、KEKを生成するため、XOR関数を使用して組み合わせなければならない。

パスフレーズ認証要素は、TOE文書に含まれたガイダンス及び米国政府機関から提供されたすべてのガイダンスを使用して管理者が生成したパスフレーズであるべきである。TOEは、辞書に載っている語から選択した、1文字から8文字の長さの単語が9以上含まれたパスフレーズをサポートしなければならない。利用者がパスフレーズを入力すると、NIST 800-132を満たす承認された鍵導出機能を使用してTOEが入力されたパスフレーズを条件付けし、KEKの入力として使用されるサブマスクを生成する。

外付けトークン認証要素は、TOEで生成する必要はない。TOEで生成する場合は、附属書Cの該当する要件を含めて、FIPSで承認されたランダムビット生成器を使用してTOEで認証要素を生成すること、及び認証要素がDEKに選択された鍵サイズ以上になることを特定しなければならない。この場合、KEKの形成時に外付けトークン認証要素をサブマスクとして直接使用してもよい。

1.1.3 暗号化

鍵または認証要素を生成、処理、及び保護するために使用される暗号文が十分に堅牢であり、実装に重要な誤りがない場合、紛失または盗難にあった、認証要素またはKEKが保存されていない電源がオフになったハードドライブを入手した敵対者は、データを入手するためには、KEKまたはDEKの暗号化鍵空間をすべて試す必要がある（パスフレーズが提供する強度がディスク暗号アルゴリズムAESの潜在的鍵空間よりも弱く、パスフレーズが敵対者に知られていない唯一の認証要素である場合、提供される保護はAESの鍵空間ではなくパスフレーズの強度に比例することに注意すること）。

ハードディスクはDEKを使用して暗号化される。DEKは、KEKまたは中間鍵によってマスキングすることができる。中間鍵を使用する場合は、中間鍵がKEKによってマスキングされ

て、DEKが中間鍵によって暗号化される。すべての中間鍵が、KEK及びDEKと同じ強度要件を満たさなければならない。

一部の製品では、暗号操作が製品（TOE）の1つのコンポーネントに存在せず、暗号操作をホストOSと格納デバイスに分割することができる。KEKはディスク暗号化製品のさまざまな種類の認証要素から取得されたサブマスクから構成できるため、格納デバイスの暗号化自体がディスクコントローラ上のハードウェアに実装されている場合でも、KEKを構成するコードは通常、ブート環境でブート時に実行される。TOEを適合STで記述する場合、製品開発者はTOEの該当する部分に適切な要件を課していることを確認するべきである。説明を適用上の注記またはTSS節に含めることができ、含めるべきである。

DEKは、KEKによって（XOR関数またはAESを使用して）マスキングされる。DEKは決定論的ランダムビット生成器（DRBG）を使用して生成され、128ビットまたは256ビットのいずれかになる。DRBGを適切にシードすることにより、少なくともDEKの鍵サイズと等しいノイズサンプルが確保される。DRBGアルゴリズムの入力として使用するエントロピーは、1つ以上のハードウェアベースのソースによって提供されなければならない。

暗号化されていない鍵及び鍵とする材料は、シャットダウン時にゼロ化され、利用者が一定の時間非アクティブになった後で運用環境によってゼロ化を開始してもよい。もし電源がオフの状態で敵対者がデバイスを回復させた場合、暗号化されていない鍵または鍵とする材料は利用できない。例えば、オペレーティングシステムのメモリイメージ、スワップ領域などから暗号化されていない鍵及び／または鍵とする材料が取得される可能性がある休止状態だけでなく、利用者がデバイスを使った作業を完了したときには、利用者またはTOEアクションによってデバイスの電源がオフになることが必須である。

1.1.4 管理

1.1.6で詳しく説明するように、TOEの基本要件では、TOEに管理役割を保持することを必要としない。ただし、システム全体にTOEの利用者のサブセットであるTOEの管理の概念を保持する。以降の節では、用語「管理者」はこの意味で使用されている。

TOEの管理者は、必要な構成ガイダンスに正しく従わなければならない。TOEでは、運用環境のホストO／Sによって提供される認証システムを使用してこの役割を確立するか、または独自のメカニズムを実装することができる。後者の場合、附属書Cの情報をセキュリティターゲットに含める必要がある。TOEは、次の管理機能を実行できなければならない。

- データ暗号化鍵を作成する
- DEKをラップするために使用される認証要素から生成したサブマスクから、鍵の暗号化鍵を生成する

附属書Cの制約に従う限り、追加機能をTOEで提供して、STで特定することができる。

1.1.5 許可された利用者

許可された利用者は、データ侵害のリスクを最小限に抑えるため、利用者ガイダンスに従わなければならない。認証は、保護されたディスクの保護を解除する正しい認証要素を所有し、TOEに提供することにより確定される。所有しているデバイスをセキュリティで保護し、TOEの認証要素を保護することが、ハードディスクの許可された利用者の責任である。許可された利用者は、ハードドライブの電源がオンになっているときに、ハードドライブに利用者の物理的な制御を残したままにしてはならない。許可された利用者は、ハードドライブにパスフレーズ及び／または外付けトークンを残したり保存してはならない。また、複数の要素を使用する場合は、一緒に残したり保存してはならない。外付けトーク

ンは、認証が成功した後でシステムから取り外さなければならない。利用者には、セキュアなTOEを維持するために適切なガイダンスが提供される。

1.1.6 TOE と TOE のサポート環境

TOEのサポート環境は重要である。TOEは、ハードウェアとソフトウェアの組み合わせ（例えば、ソフトウェアミドルウェアを使用したハードドライブの暗号化）であるか、まったくのソフトウェアソリューションであるかのいずれかである。そのため、TOEは、その実行ドメインと適切な使用のために、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）に大きく依存することとなる。ベンダは、必要な機能を備えた運用環境を特定し、運用環境を正しく設定する方法について指示を提供するために、インストールと構成に関して十分な指示を提供することが求められる。

場合によっては、TOEがセキュリティ対策方針に対処できるよう、TOEベンダは運用環境に特定の構成ガイダンスを提供することが必要となる。これらの指示には、次のものが含まれる。

- 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で、利用者が一定の時間非アクティブになった後でシステムの電源を完全にオフにするための、休止／スリープ機能を設定する方法の指示
- システムの電源を完全にオフにするようには設定できない休止／スリープ機能を無効にする方法の指示
- TOE認証要素を運用環境（オペレーティングシステム）の識別情報及び認証情報の一部またはその代わりに使用する機能を無効にする方法の指示

TOEの許可された利用者とは、TOEの有効な認証要素を所有する利用者のことである。TOEでは、特定の管理アクティビティ（FMT要件に定義された）をTOEの許可された利用者のサブセットによって実行することが必要となる。本PPでは、識別機能と認証機能を提供することによりこれらの管理機能を管理者の役割に制限する場合は、TOEに要件は発生しない。このことは、TOEベンダが適合となる際に、さまざまな方法があることを示す。例えば、次のような方法がある。

1. TOEに、権限を持つ管理者の概念を含めない。管理ユーティリティを起動できれば誰でもTOEを設定できる。この場合、PPに適合するためには、TOEベンダは、TOEの許可された利用者のサブセットだけが管理ユーティリティを実行できる運用環境を設定するため、管理者が使用する指示を詳述したAGD_OPE/PREガイダンスの一部として指示を提供しなければならない。
   例えば、ガイダンスに、管理者が許可した利用者だけが管理ユーティリティを実行できるよう運用環境にアクセス制御メカニズムを設定していることを記述する。これにより、本PPのベースライン要件を反映する。
2. TOEに、権限を持つ管理者（1人または一連の管理者）の概念を含めるが、運用環境を使用して識別機能と認証機能を実行し、権限を持つ管理者のTOE内表現と一致するある程度の表示をTOEに渡す。この場合、ST作成者は、TOEで提供される機能を指定するため、要件を追加する必要がある（附属書Cで提供されるテンプレートを使用）。ベンダは、TOEに情報を渡すのを支援するために必要な、運用環境の構成または設定を記述する必要がある。
3. TOEに、ハードディスクを収容しているシステムのどの利用者がTOEで提供される管理機能を使用することが許可されるのかを決定する、独自の識別機能と認証機能を含める。この場合、ST作成者は、附属書Cで提供されるI&Aテンプレート情報をSTの本文に使用して、この機能を特定する必要がある。

2　セキュリティ課題記述

本プロテクションプロファイル（PP）は、敵対者による事前のアクセスなしに電源オフの状態でハードディスクが紛失または盗難にあったという状況に対処するために作成されている。

2.1　脅威

脅威は、脅威エージェント、資産、及びその資産に対するその脅威エージェントの有害なアクションから成る。脅威エージェントとは、紛失または盗難にあっ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のことである。例えば、次の表の脅威の T.UNAUTHORIZED_DISK_ACCESS がある。脅威エージェントは、紛失または盗難のあったハードディスクの所有者（許可されていない利用者）である。資産とは格納デバイス上のデータのことであり、有害なアクションとはハードディスクからこれらのデータを入手するよう試みることである。この脅威のため、ハードドライブを使用してデータを暗号化／復号できる利用者を許可するという、ディスクエンクリプタの最初の機能要件（TOE）が推進されている。KEK、DEK、中間鍵、認証要素、サブマスク、鍵または認証要素を作成するための乱数または他の値を所有することで、許可されていない利用者が暗号化を無効にできるようになるため、鍵とする材料はデータと同じように重要であると見なされ、鍵とする材料も「表 1：脅威」で対処の対象となるその他の資産となっている。

この時点で、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評価対象（TOE）または運用環境に取り込むことが可能な、紛失または盗難にあったハードディスクの所有者から製品（TOE）を保護することは、一般的に期待されないことを再度強調することが重要である。適合TOEである程度の保護が提供される特定の領域として、TOEに更新を提供する場合がある。ただし、この領域以外では、本PPでは対策は規定されていない。同様に、これらの要件では、敵対者がハードディスクを入手し、ブートデバイス（例えば、MBR、ブートパーティション）の暗号化されていない部分を侵害してから、改ざんされたコードが実行されるよう元の利用者が回復できるようにするという、「紛失して発見された」ハードディスクの問題には対処していない。

表 1：脅威

脅威	脅威の説明
T.KEYING_MATERIAL_ COMPROMISE	攻撃者は、TOEが永続記憶域に書き込んだ暗号化されていない鍵とする材料（KEK、DEK、認証要素、サブマスク、及び鍵を導き出す乱数または他の値）を入手し、これらの値を使用して利用者データにアクセスすることが可能。
T.INCOMPLETE_SHUTDOWN	運用環境が省電力モードになって、データまたは鍵とする材料が永続記憶域に暗号化されていない状態で保持される可能性がある。
T.KEYSPACE_EXHAUST	許可されていない利用者が総当り攻撃を試みて、暗号化鍵または認証要素を判断し、データまたはTOE資源に不正アクセスを行うことが可能。

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コードに不適切にアクセス（表示、変更、または削除）し、鍵とする材料または利用者データにアクセスすることが可能。
T.UNAUTHORIZED_DISK_ACCESS	紛失したハードディスクにアクセスできる許可されていない利用者が、TOEセキュリティ方針では許可されないデータにアクセスすることが可能。
T.UNAUTHORIZED_UPDATE	悪意のある部外者がTOEのセキュリティ機能を侵害する可能性がある製品の更新をエンドユーザに提供するよう試みる。
T.UNSAFE_AUTHFACTOR_VERIFICATION	利用者が入力した認証要素の検証を実施するため、攻撃者が安全でない方法を利用し、その結果、KEK、DEK、または利用者データを入手することが可能。

2.2 前提条件

セキュリティ課題の定義のこの節では、セキュリティ機能を提供できるようにするために運用環境に課す前提条件を示す。もし、これらの前提条件を満たさない運用環境にTOEを配置した場合、そのTOEがすべてのセキュリティ機能を提供できるとは限らない。前提条件は、運用環境の物理的な利用者と接続性に対して課すことができる。

表 2：TOE 前提条件

前提条件	前提条件の説明
A.AUTHORIZED_USER	許可された利用者は、パスフレーズ及び外付けトークンをディスクとは別の安全な場所に保存するなど、提供されるすべての利用者ガイドに従う。
A.ET_AUTH_USE_ONLY	認証要素が含まれた外付けトークンは、外付けトークン認証要素を保存する以外の目的には使用しない。
A.PASSPHRASE_BASED_AUTH_FACTOR	権限を持つ管理者は、保護対象のデータの機密性を反映してパスフレーズ認証要素が十分な強度とエントロピーを備えていることを確認する。
A.PLATFORM_I&A	TOEは、TOEをインストールしても影響を受けない、個別の利用者識別と認証をサポートしているプラットフォームにインストールされる。
A.SHUTDOWN	許可された利用者は、未使用時にはホストシステムの電源を完全にオフにすることが求められる。
A.STRONG_EXT_AUTH_FACTOR	TOEで生成されない外付けトークン認証要素はすべて、本PPに示された要件を満たすランダムビット生成器によって生成される。
A.TRAINED_ADMINISTRATORS	権限を持つ管理者は、適切なトレーニングを受けて、すべての管理者ガイダンスに従う。

3　セキュリティ対策方針

セキュリティ対策方針とは、第3章の脅威、組織のセキュリティ方針、及び前提条件から導き出す、評価対象（TOE）及び運用環境の要件のことである。第4章で、TOEのセキュリティ対策方針をより形式的にセキュリティ機能要件（SFR）として再度説明する。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3にTOEのセキュリティ対策方針を示す。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及び／または特定された組織のセキュリティ対策に適合するため、示した意図を反映している。TOEでは、セキュリティ機能要件を満たすことにより、これらの対策方針に対処する必要がある。

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は、ハードディスク上のデータを復号できるよう、利用者の認証要素を含まなければならない。
O.CORRECT_TSF_OPERATION	TOEは、運用環境におけるTSFの正しい動作を保証するため、TSFをテストするための機能を提供する。
O.ENCRYPT_ALL	TOEは、ハードドライブに保存されているすべてのデータを暗号化する（MBR及びMBRが指すブート可能なパーティションは除外してもよいことに注意すること）。
O.EXTERNAL_AUTH_FACTOR_PROTECTION	TOEは、認証用に使用した後は、外付けトークン認証要素にアクセスできないことを確実にしなければならない。
O.DEK_SECURITY	TOEは、認証要素を所有しない脅威エージェントがDEKを入手して利用者データにアクセスすることができないように、1つ以上のサブマスク（認証要素から導出した）から作成した鍵の暗号化鍵（KEK）を使用してDEKをマスキングする。
O.KEY_MATERIAL_COMPROMISE	TOEは、KEKまたはDEKを見つけるために鍵とする材料が利用される可能性を低減するため、必要がなくなり次第、すぐにこの材料をゼロ化する。
O.MANAGE	TOEは、TOEのセキュリティの管理において権限を持つ管理者を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許可されない利用を禁止する。
O.OWNERSHIP	TOEは、TOEの操作時に利用者データにアクセスできるようになる前に、所有権が得られている（つまり、DEKが作成され、認証要素が確立され、デフォルトの認証要素が変更され、KEKが導出されたサブマスクから形成され、DEKがKEKと関連付けられている）ことを確実にしなければならない。

O. SAFE_AUTHFACTOR_ VERIFICATION	TOEは、KEK、DEK、または利用者データが意図せず公開されない方法で、認証要素の検証を実施しなければならない。
O.TRUSTED_UPDATE	TOEは、TOEのファームウェア／ソフトウェアを更新して、製品の更新を対象となるソースから入手したことを検証する機能を管理者に提供しなければならない。

3.2 運用環境のセキュリティ対策方針

TOEの運用環境は、セキュリティ機能（TOEのセキュリティ対策方針で定義された）を正しく提供するためにTOEを支援する、技術的及び手続き的な手段を実装する。この部分的なソリューションは運用環境のセキュリティ対策方針と呼ばれ、運用環境で達成するべき目標を示した一連の記述から成る。

この節では、IT領域によってまたは技術的または手続き的な手段以外によって対処するセキュリティ対策方針を定義する。2.3節で特定されている前提条件は、環境のセキュリティ対策方針として組み込まれている。これらの前提条件は、主に手続き的または管理上の手段によって満たされる、追加の要件を課す。表4に、環境のセキュリティ対策方針を示す。

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	権限を持つ管理者は、パスフレーズ認証要素がNSA／NISTのパスフレーズガイダンスに適合することを確認する。
OE.PLATFORM_I&A	運用環境は、TOEで使用される認証要素とは無関係に機能する、個別の利用者識別メカニズムと認証メカニズムを提供する。
OE.POWER_SAVE	利用者の選択によってシステムをシャットダウンするのと同じ方法で一定時間後にシステムの電源をオフにする、1つ以上のメカニズムが存在するように、運用環境を構成しなければならない（O.SHUTDOWN）。この要件に適合しないメカニズム（例えば、スリープ、休止）は、管理者が無効にできなければならない。
OE.RESTRICTED_FUNCTIONS	管理機能は権限を持つ管理者に限定される。
OE.SINGLE_USE_ET	認証要素が含まれた外付けトークンは、外付けトークン認証要素を保存する以外の目的には使用しない。
OE.STRONG_ENVIRONMENT_CRYPTO	運用環境は、TOEの要件及び機能に適切な暗号化関数機能を提供する。
OE.TRAINED_USERS	許可された利用者は、適切なトレーニングを受けて、TOE及び認証要素を保護するためのすべてのガイダンスに従う。

3.3 セキュリティ対策方針の根拠

TOEの対策方針に対するセキュリティ対策方針の根拠は、第6章に示す。表 5に、セキュリティ対策方針と前提条件のマッピングを示す。

表 5：セキュリティ対策方針と前提条件のマッピング

前提条件	前提条件に対処する対策方針	根拠
A.AUTHORIZED_USER 許可された利用者は、パスフレーズ及び外付けトークンをディスクとは別の安全な場所に保存するなど、提供されるすべての利用者ガイドに従う。	OE.TRAINED_USERS 許可された利用者は、適切なトレーニングを受けて、TOE及び認証要素を保護するためのすべてのガイダンスに従う。	OE.TRAINED_USERSは、TOEを正しく使用する方法について利用者がトレーニングを受けることを確実にする。
A.ET_AUTH_USE_ONLY 認証要素が含まれた外付けトークンは、外付けトークン認証要素を保存する以外の目的には使用しない。	OE.SINGLE_USE_ET 認証要素が含まれた外付けトークンは、外付けトークン認証要素以外のものを含まない。 OE.TRAINED_USERS 許可された利用者は、適切なトレーニングを受けて、TOE及び認証要素を保護するためのすべてのガイダンスに従う。	OE.SINGLE_USE_ETは、外付けトークンに外付けトークン認証要素のみが含まれることを必要とすることにより、対策方針に対処する。 OE.TRAINED_USERSは、利用者が外付けトークンに追加の情報を保持しないことを義務付けることにより、貢献する。
A.PASSPHRASE_BASED_AUTH_FACTOR 権限を持つ管理者は、パスフレーズ認証要素がパスフレーズの方針に適合し、保護対象のデータの機密性を反映して十分な強度とエントロピーを備えていることを確認する。	OE.TRAINED_USERS 許可された利用者は、適切なトレーニングを受けて、TOE及び認証要素を保護するためのすべてのガイダンスに従う。 OE.PASSPHRASE_STRENGTH 権限を持つ管理者は、パスフレーズ認証要素がNSA／NISTのパスフレーズガイダンスに適合することを確認する。	OE.TRAINED_USERSは、管理者がトレーニングを受けて、提供されるガイダンスに従うことを確実にすることにより、この方針を満たす。 OE.PASSPHRASE_STRENGTHは、保護対象のデータの機密性を反映して管理者が十分な強度とエントロピーを備えたパスフレーズを作成することを確実にすることにより、この方針を満たす。
A.PLATFORM_I&A TOEは、TOEをインストールしても影響を受けない、個別の利用者識別と認証をサポートしているプラットフォームにインストールされる。	OE.PLATFORM_I&A 運用環境は、TOEで使用される認証要素とは無関係に機能する、個別の利用者識別メカニズムと認証メカニズムを提供する。	OE.PLATFORM_I&Aは、1)システムの利用者向けのI&Aメカニズムを運用環境に実装すること、及び、2)それらのメカニズムがTOEの認証要素の入力に取って代わられないことを確実にする。

A.SHUTDOWN 許可された利用者は、未使用時にはホストシステムの電源を完全にオフにすることが求められる。	OE.TRAINED_USERS 許可された利用者は、適切なトレーニングを受けて、TOEをシャットダウンして認証要素を保護するためのガイダンスに従う。	OE.TRAINED_USERSは、システムを正しくシャットダウンする方法を利用者に指示し、そうすることの重要性を説明することにより、この方針を満たす。
A.STRONG_EXT_AUTH_FACTOR TOEで生成されない外付けトークン認証要素はすべて、本PPに示された要件を満たすランダムビット生成器によって生成される。	OE.STRONG_ENVIRONMENT_CRYPTO 運用環境は、TOEの要件及び機能に適切な暗号化関数機能を提供する。	運用環境は、前提条件を満たすよう、OE.STRONG_ENVIRONMENT_CRYPTOを通じて、TOEに適した機能と動作を保証する暗号化関数を提供しなければならない。
A.TRAINED_ADMINISTRATORS 権限を持つ管理者は、適切なトレーニングを受けて、すべての管理者ガイダンスに従う。	OE.TRAINED_USERS 許可された利用者は、適切なトレーニングを受けて、TOE及び認証要素を保護するためのすべてのガイダンスに従う。	OE.TRAINED_USERSは、TOEのセキュリティを設定及び維持するために、管理者がトレーニングを受けて、適切なガイダンスに従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分けられる。セキュリティ機能要件（SFR）はセキュリティ対策方針を正式に具体化したものであり、4.1節の適用上の注意で提供している。

セキュリティ保証要件（SAR）は通常、PPに挿入され、SFRとは別にリストアップされる。CEMは、選択されたSARに基づいて評価を実施する際に参照される。コモンクライテリアのセキュリティ保証要件の性質及びTOEとして識別される特定のテクノロジーのために、本PPではより固有のアプローチを行っている。前後関係及び完全性のためにSARを4.2節に示しているが、各SFR及びSARに関して評価者がこのTOEで実施する必要があるアクティビティの大部分は、「保証アクティビティ」に詳述している。保証アクティビティは、評価を完了するために実施しなければならないアクティビティの規範を記述したものである。保証アクティビティは本PPの2箇所に示しており、特定のSFRに関連するPPは4.1節に、SFRに関連しないPPは4.2節に示している。保証アクティビティは、可読性、理解性、及び利便性のために並べて示される、固有の評価方法である。

保証アクティビティは本PPの2箇所に示しており、特定のSFRに関連するPPは4.1節に、SFRに関連しないPPは4.2節に示している。

SFRに直接関連するアクティビティについては、各SFRの後に1つ以上の保証アクティビティを示し、実施する必要があるアクティビティを詳述している。

SFRに関連しないアクティビティを必要とするSARについては、4.2節に、そのSARに関連する特定の保証アクティビティが記述されているSFRへのポインタと共に、実施する必要がある追加の保証アクティビティを示している。

プロテクションプロファイルを将来繰り返すことにより、実際の製品評価から習得した知識に基づいて、より詳細な保証アクティビティを提供することが可能である。

4.1　セキュリティ機能要件

セキュリティ機能要件（SFR）は、TOEのセキュリティ対策方針を翻訳したものである。セキュリティ機能要件は通常、より詳細なレベルの抽象的概念であるが、完全な翻訳である必要がある（セキュリティ対策方針に完全に対処していなければならない）。CCでは、いくつかの理由からこの標準言語への翻訳を必要としている。

- 評価対象について正確な記述を提供するため。TOEのセキュリティ対策方針は通常、自然言語で説明されるため、標準言語への翻訳によってTOEの機能がより正確に記述されるようにする。
- 2つのSTを比較できるようにするため。ST作成者が異なると、セキュリティ対策方針の記述に異なる用語が使用される可能性があるため、標準言語によって同じ用語と概念が使用されるようにする。これにより、容易に比較できるようにする。

表 6：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.1(3) 暗号鍵生成（パスフレーズ条件付け）
暗号サポートクラス（FCS）	FCS_CKM_EXT.4 暗号鍵とする材料の破棄
暗号サポートクラス（FCS）	FCS_COP.1(1) ディスク暗号化

暗号サポートクラス（FCS）	FCS_COP.1(2) 署名検証
暗号サポートクラス（FCS）	FCS_COP.1(2) 暗号技術的ハッシュ
暗号サポートクラス（FCS）	FCS_COP.1(2) 鍵のマスキング
暗号サポートクラス（FCS）	FCS_RBG_EXT.1 拡張：ランダムビット生成
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
識別及び認証のクラス（FIA）	FIA_AUT_EXT.1 拡張：FDE利用者認証
セキュリティ管理クラス（FMT）	FMT_SMF.1 管理機能の特定
TSFクラスの保護	FPT_TUD_EXT.1 高信頼更新
TSFクラスの保護	FPT_TST_EXT.1 TSFのテスト

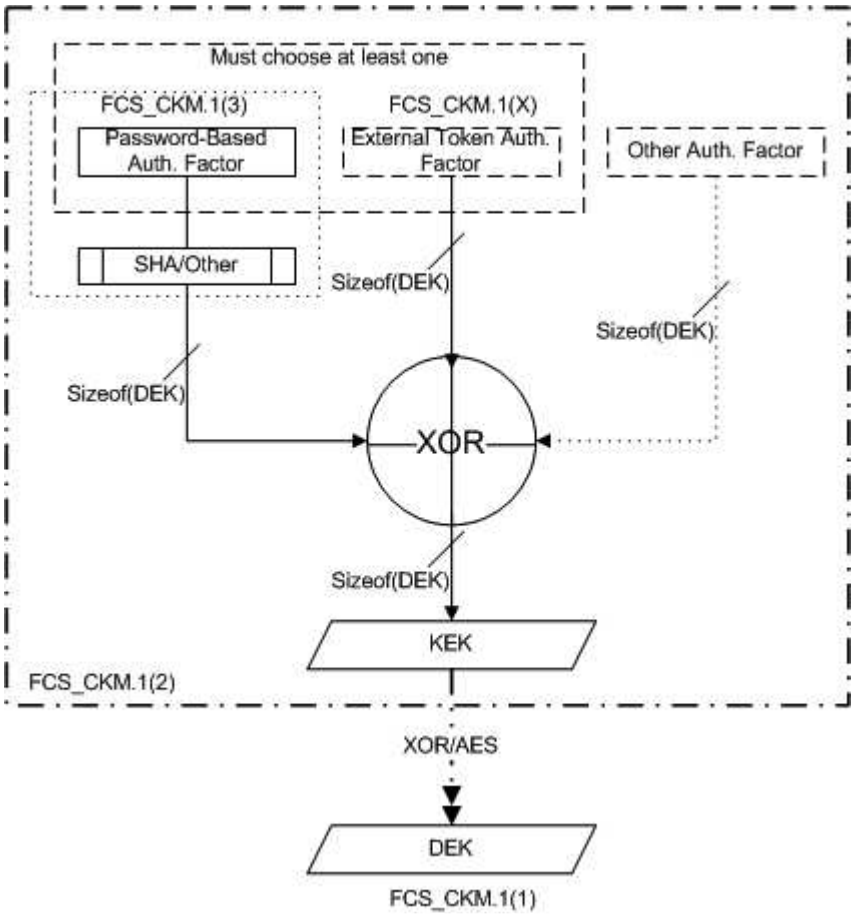
4.1.1 クラス：暗号サポート（FCS）

これらの機能要件で対処する主な脅威は、鍵空間に対する総当り攻撃及び暗号コンポーネントの障害である。

暗号要件では、アルゴリズムを記述した規格について言及する。これらの規格の大部分は、米NISTから入手できるSpecial Publication（800-xxx）またはFederal Information Processing Standards（FIPS、連邦情報処理規格）である。保証要件では、これらの要件の実装をどのように検証するのかを詳述する。制度ごとに、暗号保証アクティビティを満たしていると見なすためのプロセスを指定するオプションがある。

暗号鍵の管理（FCS_CKM）

適合実装には、鍵の暗号化鍵（KEK）及びデータ暗号化鍵（DEK）の少なくとも2つの鍵が含まれる。以下の要件は、鍵をどのように生成するのかを特定している。この生成はやや複雑であるため、次の図にこの節における要件の概要を示す。



上記の図に示すように、DEKの生成はFCS_CKM.1(1)で指定されているのに対し、KEKの生成は、（任意） FCS_CKM.1(3)及び／または（任意） FCS_CKM.1(X)の他の1つ以上のコンポーネントで指定されている入力を使用してFCS_CKM.1(2)で指定されている。KEKは、認証要素から導出されたサブマスクから生成される。TOEでは、パスフレーズベース認証要素（FCS_CKM.1(3)）または認証要素（FCS_CKM.1(X)）が含まれた外付けトークンのいずれかをサポートする必要がある。両方をサポートすることも可能である。外付けトークン認証要素に関する注記：TOEは要素を生成する必要はないが、要素を生成せずに要素を使用することができる。FCS_CKMは鍵の生成を取り扱うため、もしTOEが外付けトークン認証要素も生成できることを主張する必要がある場合は、附属書CのFCS_CKM.1(X)コンポーネント（及び関連する脅威、対策方針、及び根拠）をSTの本文に含めなければならない。

TOEがこれらの認証要素の少なくとも1つをサポートする限り、TOEは他の認証要素（上記の図の右側に表示）もサポートすることができる。これらの他の認証要素は、FCS_CKM.1(2)で指定されている。また、FCS_CKM.1(2)では、KEKを形成するためにさまざまな認証要素をどのように組み合わせるのかも指定している。この予備情報とともに、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、以下の**[標準なし]**に合致する、**FCS_RBG_EXT.1**に指定された**ランダムビット生成器**及び指定された暗号鍵サイズ**[選択：128ビット、256ビット]**を使用して、**DEK**暗号鍵を生成しなければならない。

適用上の注意：

この要件は、AESの鍵空間を総当たり以外の方法では、DEKを回復できないことを確実にすることを意図している。TOEの鍵生成機能は、TOEデバイスに実装されたRBGを使用する。128ビットまたは256ビット（または両方）のいずれか使用できる。ST作成者は、デバイスに適したものを選択する。デバイス上のすべての利用者データを再度暗号化しなくても認証要素（特にパスワード認証要素）を変更できるように、KEKに加えてDEKも使用する。

TOEが中間鍵を使用する場合、この要件は中間鍵に対しても適用される。

保証アクティビティ：

評価者は、TSSをレビューして、FCS_RBG_EXT.1で記述されている機能がどのように起動されるのかがTSSに記述されていることを確認しなければならない。評価者は、FCS_RBG_EXTのRBG機能の記述から可能な限り、必要となる鍵サイズが利用者データの暗号化／復号（FCS_COP.1(1)）に使用される鍵サイズ及びモードと同一であることを確認しなければならない

FCS_CKM.1(2)

暗号鍵生成（KEK）

FCS_CKM.1.1(2)

詳細化：TSFは、指定された暗号鍵**導出**アルゴリズム**[選択：なし、排他的OR （XOR)]**に従って**KEK**暗号鍵を導き出さなければならない。**次の入力を使用する[選択**：

FCS_CKM.1(3)の定義に従って条件付けされたパスワード認証要素から導出されたサブマスク

外付けトークン認証要素

FCS_CKM.1(1)の指定に従ってDEKと同じサイズのサブマスクを生成する[選択、次から1つを選択：他の入力なし、[割付：他の認証要素及び関連するサブマスク導出方法のリスト]]

各認証要素の効果的な強度及び次の**[標準なし]**を満たす指定された暗号鍵サイズ**[選択：128ビット、256ビット]**を維持する。

適用上の注意：

これらの要件は、認証要素を使用してKEKを作成する方法を定義することを意図している。各割付と選択について、以下にST作成者向けの特別なガイダンスを示しているが、以下のガイダンスはこのコンポーネントの要点の概要を記述したものである。ST作成者は、パスフレーズ認証要素または外付けトークン認証要素のいずれか、またはその両方を選択し、さらに追加の認証要素を定義することもできる。追加の認証要素を定義する場合は、それらの認証要素からサブマスクを生成する方法も記述しなければならない。割付に課される条件は、生成されるサブマスクがDEKと同じサイズであるということだけである。

複数の認証要素を使用することが望ましい。複数の認証要素を使用する場合は、XORを使用して生成されるサブマスクを組み合わせなければならない。

1番目の選択に関して、1つの認証要素のみ使用する場合、ST作成者は「なし」を選択する。複数の認証要素を使用する場合は、ST作成者は「XOR」を選択する（他の組み合わせ方法は本PPに適合しない）。

2番目の選択に関して、ST作成者は使用する認証要素を選択する。複数の認証要素を選択できるが、最初の2つ（パスフレーズベースまたは外付けトークンベース）から少なくとも1つを選択しなければならないことに注意すること。条件付きのパスフレーズ以外の追加の認証要素または外付けトークンに含まれる認証要素を使用する場合、ST作成者は、この2番目の選択の選択肢に含まれている割付を使用してそれらの要素を指定する（または「他の入力なし」を選択する）。

暗号鍵のサイズの選択に関しては、生成されるKEKのサイズを選択する。このサイズは、FCS_CKM.1(1)でDEKに指定されたビット長と同じでなければならない。

KEKを形成するために使用する認証要素が1つしかないため（KEKの構成は別の場所に指定）、またはKEKはXOR関数を使用して形成されるため、「標準なし」が必要となることに注意すること。

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での要件の実装が文書化されていることを確認するため、STのTSSを検査することを必要とする。評価者は、まずTSS節を検査して、STに指定されている認証要素が記述されていることを確認しなければならない。パスフレーズベースの要素に関しては、TSS節の検査はFCS_CKM.1(3)の保証アクティビティの一部として実施される。外付けトークン認証要素に関しては、認証要素はTOEが生成する必要があるかどうかをTSSに記述しなければならない（この場合、附属書CのFCS_CKM.1(X)に関連する保証アクティビティが適用される）。記述しない場合は、外付けトークン認証要素がSTに示された最小長の要件を満たすことを確実にするために、TSS節にTOE（または管理者）が使用する手段を特定しなければならない。許容可能な手段には、管理者による長さの検証や、実行時にTOEが実行する入力評価チェックが含まれる。さらにこの場合、評価者は、TOEが使用できる外付けトークン認証要素の特性（例えば、認証要素の生成方法、認証要素が満たさなければならない形式や規格）を管理者ガイダンスで説明していることを検証しなければならない。

他の認証要素が特定されている場合は、TSSで、それらの要素ごとに、要素をTOEに入力する方法、認証要素からサブマスクを生成する方法（このプロセスが適合する関連する規格を含む）、及びサブマスクの長さが必要なサイズ（この要件で特定される）を満たしていることを確認するために実施する検証を特定する。

認証要素が1つのみの場合は、必然的に何も組み合わせられないため、この場合に関連する保証アクティビティはない。認証

要素から生成されるサブマスクをまとめてXOR処理してKEKを形成する場合は、TSS節でその実行方法（例えば、順序付けの要件がある場合、実行されるチェック）を指定しなければならない。また、評価者は、TSSに生成される出力の長さをDEKと同じにする方法がTSSに記述されていることも確認しなければならない。

評価者は、以下のテストも実施しなければならない。

- テスト1 [条件付]：複数の認証要素がある場合、必要な認証要素を提供できなかったときに、暗号化されたデータにアクセスできないことを確認する。
- テスト2 [条件付]：TOEが複数の異なる形式の複数の外付けトークンをサポートする場合、評価者は、TOEに認証情報を提供する際に各形式が適切に使用されることを確認する。

FCS_CKM.1.1(3)

詳細化：サブマスクを生成するために使用するパスフレーズに、一連の{大文字、小文字、及び[割付：*その他のサポートされる文字*]で**最大[割付：8以上の正の整数]文字の最大[割付：9以上の正の整数]の単語を**含まれなければならない。**また、条件付き関数の出力がDEKのサイズ（ビット数）と等しくなるよう、次のように条件付けなければならない。[選択：**

- **128ビットDEKに[選択：SHA-1、SHA-256、SHA-512]を使用する；**
- **256ビットDEKに[選択：SHA-256、SHA-512]を使用する**
- **FCS_RBG_EXT.1に指定されたランダムビット生成器を使用して生成されたソルトによるNIST SP 800-132、反復回数[割付：*1000以上*]、及び[選択：SHA-1、SHA-256、SHA-512]を使用したHMACを使用する；**

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る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なランダムな方法で、辞書に載っている語から取得される一連の単語である。この要件は、パスフレーズの構成に要件を課すものである。辞書から単語を選択するのに特定の方法は必要とならない（ただし一般的に、暗号を使用したランダムな方法で行われる）。取得される文字列は、基盤となるOSによって決定されるスキームでエンコードされた一連の文字列から成る。この順序を、KEKへの入力として使用されるサブマスクを形成する、ビットの文字列に条件付けられなければならない。条件付けは、識別されたハッシュ関数のいずれかまたはNIST SP 800-132に記述されたプロセスを使用して行うことができる。使用する方法は、ST作成者が選択する。800-132の条件付けが指定されている場合、ST作成者は実行する繰返しの回数（C）を記載する。この値は10000以上でなければならない。また、800-132は、承認されたハッシュ関数と共にMACから成る擬似乱数関数（PRF）を使用することを必要とする。

ST作成者は、使用するハッシュ関数を選択する。また、附属書

CからHMAC及びハッシュ関数に適切な要件を含める。

本PPの後続版では、SHA-1は、暗号ハッシュとして承認されたアルゴリズムではなくなっているだろう。また、SP 800-132を使用した条件付けが必要となるだろう。

保証アクティビティ：　このコンポーネントの2つの側面で評価が必要となる。辞書に載っている語から選択した、1文字から8文字の長さの単語が9以上含まれたパスフレーズがサポートされること、及び入力となる文字が選択された条件付け関数の影響を受けるということである。これらのアクティビティについて、以下の説明で別々に対処する。

最大8文字の単語が9以上含まれた長さのパスフレーズのサポート

評価者は、TSS節をチェックして、この割付の記述でSTに指定されている最大数の単語長のパスフレーズを許可する能力があること、及び指定されている数が要件に示されている数以上であることがTSSに特定されていることを確認しなければならない。また、評価者は、操作ガイダンスをチェックして、パスフレーズを生成する管理者向けの指示が含まれており、TOEにパスフレーズを入力する方法がガイダンスに示されていることを確認しなければならない。

さらに、上記の分析に加えて、評価者は、AGD_PREガイダンスに従って設定されたTOEで以下のテストを実施しなければならない。

- テスト1：9以上（または最初の割付でSTに指定された数のいずれか大きい数）の単語が含まれたパスフレーズをTOEがサポートすることを確認する。また、このテストで、2番目の割付に指定された数（または8のいずれか大きい数）以下の単語がサポートされることを検証するべきである。
- テスト2：ベンダから提供される操作ガイダンスに指定された長さと一致する、より短い長さのパスフレーズをTOEがサポートすることを確認する（例えば、ガイダンスに5つ以上の単語をパスフレーズに含めることが指定されている場合、このテストで、5つの単語が含まれたパスフレーズがTOEによって受け入れられることを少なくとも確認する）。
- テスト3 [条件付]：ST作成者が追加のサポートされる文字を3番目の割付に記載している場合、指定された特殊文字に関して、AGD_OPRまたはAGD_PREガイダンスの指定に従って構成されたパスフレーズのサポートがTOEに含まれることを確認する。例えば、ガイダンスでパスフレーズに特殊文字を含めることを指定している場合、もしTOEが文字と数字しかサポートしていないなら、このテストは失敗するだろう。

パスフレーズの条件付け

SHAベースのパスフレーズ条件付けに関して、評価者は次のアクティビティを実施する。評価者は、パスフレーズをまずエンコードしてからSHAアルゴリズムに送るメソッドが、TSSに記述されていることをチェックしなければならない。

アルゴリズム（パディング、ブロッキングなど）の設定が記述されていなければならない。また評価者は、これらの設定がこのコンポーネントの選択及びハッシュ関数自体に関するFCS_COP.1(3)の選択でサポートされていることを検証しなければならない。評価者は、FCS_CKM.1(2)に記述された関数への入力となり、FCS_CKM.1(1)に指定されたDEKと同じ長さとなるサブマスクを、ハッシュ関数の出力を使用してどのように形成するかの記述がTSSに含まれていることを検証しなければならない。

800-132ベースのパスフレーズ条件付けに関しては、必要となる保証アクティビティは、該当する附属書Cの要件について保証アクティビティを行う際に実施する。KEKを形成するために使用されるサブマスクの形成時にマスター鍵の操作を実行する場合は、そのプロセスをTSSに記述しなければならない。

入力したパスフレーズからのサブマスクの形成について、系統立てられたテストは必要ない。

FCS_CKM_EXT.4　暗号鍵のゼロ化

FCS_CKM_EXT.4.1　TSFはすべての平文の秘密鍵及びプライベート鍵とCSPについて、必要がなくなったときにゼロ化しなければならない。

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において、「セキュリティに関する情報であって、その開示または変更が、暗号モジュールのセキュリティを侵害し得るもの（例えば、秘密鍵及びプライベート鍵、及びパスワードやPINなどの認証データ）」として定義されている。

上記のゼロ化は、鍵／暗号クリティカルセキュリティパラメタを他の場所に移動させる際に、平文の鍵／暗号クリティカルセキュリティパラメタのための、それぞれの中間格納領域（すなわち、このようなデータのパスに含まれる、例えば、メモリバッファのような記憶域）に適用される。

保証アクティビティ：　評価者は、TSSをチェックして、秘密鍵（対称暗号化のために使用される鍵）、プライベート鍵、及び鍵生成のために使用されるCSPのそれぞれについて、いつそれらがゼロ化されるのか（例えば、使用後直ちに、システムのシャットダウン時など）、及び実行されるゼロ化処理のタイプ（ゼロで上書き、ランダムなパターンで3回上書きなど）がTSSに記述されていることを確認しなければならない。保護対象を格納するためにさまざまな種類のメモリを利用している場合、評価者はTSSをチェックして、データが格納されるメモリに関してゼロ化手順（例えば、

flashに格納された秘密鍵はゼロで1 回上書きされ、一方、内蔵ハードドライブに格納された秘密鍵は、各書き込み動作前に変更されるランダムパターンを使って3回上書きされる）がTSSに記述されていることを確認しなければならない。

暗号操作（FCS_COP）

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、**FIPS PUB 197「Advanced Encryption Standard (AES)」及び[選択：NIST SP 800-38A、NIST SP 800-38C、NIST SP800-38E]**を満たす**[選択：CBC、CCM、CFB128、CTR、OFB、XTS]モード**及び暗号鍵サイズ**[選択：128ビット、256ビット]**で使用される、特定された暗号アルゴリズム**AES**に従って、**暗号化と復号**を実行しなければならない。

適用上の注意： この要件は、ST作成者がハードディスク上の該当する情報のAES暗号化に選択することができる、承認されたAESモードを特定することを意図している。1番目の選択に関して、ST作成者は、TOE実装でサポートされるモード（1つまたは複数）を示すべきである。2番目の選択では、FCS_CKM.1(1)で指定された鍵サイズと同一となる、使用する鍵サイズを示す。3番目の選択では、1番目の選択で選択されたモード（1つまたは複数）に同意しなければならない。複数のモードがサポートされる場合は、このコンポーネントを繰り返すとSTで明確にすることができる。

本PPの将来のバージョンには、NISTによってレビュー及び承認された新しい暗号モードが含まれる可能性がある。

保証アクティビティ: 複数のモードがサポートされる場合、評価者はTSS及びガイダンス証拠資料を検査して、エンドユーザが特定のモード／鍵サイズをどのように選択するのかを決定する。次に、評価者は、必要に応じて、モード／鍵サイズの各組み合わせを次の節に示されている方法でテストする。これらのテストには、評価施設のスキームで許容可能なアルゴリズムのリファレンス実装が必要となるものがあることに注意すること。

● ***CBC、CRB128、CTR、OFBモード***

上記のモードのすべてのテストで、
http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdfから入手可能な「*The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)*」[AESAVS]を参照する。

評価者は、TSFでサポートされる鍵サイズとモードごとに一連の既知の答えを使用したテストを実施しなければならない。入力は1つの鍵、IV、及び暗号化する平文または復号する暗号文である。
http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip
のサポートされる鍵長でこれらのモードのすべてのテストベクター（暗号化と復号の両方）を使用して、これらのテストを実

施しなければならない。

評価者は、サポートされる鍵長とモードごとに、複数ブロックのメッセージのテストを実施しなければならない。このテストを実施するため、評価者は暗号化用に10のデータセットを生成し、復号用に10のデータセットを生成する。各データセットは、鍵、IV、及び平文（暗号化の場合）または暗号文（復号の場合）から成る。

ブロック長は128ビットでなければならない。平文／暗号文の長さは、ブロック長* *i*でなければならない。ここで、*i*はデータセット数を示し、*i*の範囲は1～10となる（そのため、メッセージの範囲は128ビット～1280ビットとなる）。

評価者は、サポートされるモードごとにモンテカルロテストを実施しなければならない。評価者は、暗号化には10セットの初期値（鍵、IV、及び平文の値）を生成し、復号には10セットの初期値（鍵、IV、及び暗号文の値）を生成しなければならない。平文／暗号文の長さは128ビットでなければならない。各初期値のセットを使用して、100のテストを生成及び実施する。100のテストの値（初期値のセットごと）を生成するためのアルゴリズムは、[AESAVS]のSection 6.4.xに含まれており、テストするモードによって異なる。

● ***CCMモード***

CCMモードテストでは、以下から入手可能な「*The CCM Validation System (CCMVS)*」[CCMVS]を参照する。
http://csrc.nist.gov/groups/STM/cavp/documents/mac/CCMVS.pdf

評価者は、TSSを検査して、ペイロード、関連データ、ナンス、及びタグの長さ（及び鍵長）が指定されていることを確認しなければならない。これらの値を、次の節で説明するテストを実施する際に使用しなければならない。複数の値がサポートされる場合、評価者は操作ガイダンスを検査して、利用者がどのように値を選択するのかを決定しなければならない。

評価者は、TSFでサポートされる鍵長ごとに、次の5つのテストを実施しなければならない。

評価者は、可変関連データテストを実施しなければならない。サポートされる関連データ長ごとに、評価者は10セットの入力データを作成しなければならない。入力データセットごとに同じ鍵とナンスを使用し、同じタグ（MAC）長でなければならない。10セットごとに、一意の文字列の関連データ及びペイロードデータを使用しなければならない。評価者は、入力用に正しい暗号文を計算し、サポートされるすべての関連データ長について、TSFがすべての入力セットに同じ値を計算することを確認しなければならない。入力セットの例（256ビットの鍵用）を以下のアーカイブからVADT256.txtファイルで参照できる。

http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip

評価者は、可変ペイロードテストを実施しなければならない。サポートされるペイロード長ごとに、評価者は10セットの入力データを作成しなければならない。入力データセットごとに同じ鍵とナンスを使用し、同じタグ（MAC）長でなければならない。

10セットごとに、一意の文字列の関連データ及びペイロードデータを使用しなければならない。評価者は、入力用に正しい暗号文を計算し、サポートされるすべてのペイロード長について、TSFがすべての入力セットに同じ値を計算することを確認しなければならない。入力セットの例（256ビットの鍵用）を以下のアーカイブからVPT256.txtファイルで参照できる。
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip

評価者は、可変ナンステストを実施しなければならない。サポートされるナンス長ごとに、評価者は10セットの入力データを作成しなければならない。入力データセットごとに同じ鍵を使用し、同じタグ（MAC）長でなければならない。10セットごとに、一意のナンス、及び一意の文字列の関連データとペイロードデータを使用しなければならない。評価者は、入力用に正しい暗号文を計算し、サポートされるすべてのナンス長について、TSFがすべての入力セットに同じ値を計算することを確認しなければならない。入力セットの例（256ビットの鍵用）を以下のアーカイブからVNT256.txtファイルで参照できる。
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip

評価者は、可変タグテストを実施しなければならない。サポートされるタグ長ごとに、評価者は10セットの入力データを作成しなければならない。入力データセットごとに同じ鍵とナンスを使用しなければならない。10セットごとに、一意の文字列の関連データ及びペイロードデータを使用しなければならない。評価者は、入力用に正しい暗号文を計算し、サポートされるすべてのタグ長について、TSFがすべての入力セットに同じ値を計算することを確認しなければならない。入力セットの例（256ビットの鍵用）を以下のアーカイブからVTT256.txtファイルで参照できる。
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip

評価者が実施しなければならない最後のテストは、検証プロセステストである。このテストは、TSFでサポートされる関連データ長、ペイロード長、ナンス長、及びタグ長の組み合わせごとに実施する。組み合わせごとに、15セットの入力データをTSFに指定する。入力データは、鍵、関連データ、ペイロード

データ、ナンス、及び暗号文から成る。評価者は、さまざまなエラータイプのために、暗号文の値の3分の1から3分の2がMACのチェックに合格しないことを確認するべきである。入力をTSFに指定したら、評価者は誤ったMAC値及び渡される値をTSFが正しく識別していることを検証する。入力セットの例（256ビットの鍵用）を以下のアーカイブからVTT256.txtファイルで参照できる。
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip

● ***XTSモード***

XTSモードテストでは、以下から入手可能な「*The XTS-AES Validation System (XTSVS)*」[XTSVS]を参照する。
http://csrc.nist.gov/groups/STM/cavp/documents/aes/XTSVS.pdf

評価者はまず、上記の「*CBCモード*」節に示すテストを実施する。これらのテストを完了したら、評価者はTSSを検査してXTSモードでサポートされるデータ長の範囲が示されていることを確認し、tweak値（128ビットの文字列またはデータユニットのシーケンス番号）の形式を検査する。

次に、評価者は、サポートされる鍵長ごとにテストセットを作成する。所定の鍵長について、評価者は5以上のデータ長サンプルをテストに選択する。データ長ごとに、評価者は100の暗号化テストと100の復号テストを作成する。各テストを、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）の値を使用して実施する。

テストセットの例を
http://csrc.nist.gov/groups/STM/cavp/documents/aes/XTSTestVectors.zipで参照することができる

FCS_COP.1(2) **暗号操作（署名検証）**

FCS_COP.1.1(2) **詳細化**：TSFは、以下に従って**TOE更新の暗号署名検証**を実施しなければならない。***[選択：***

(1) 2048ビット以上の鍵サイズ（係数）の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（係数）の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の楕円曲線デジタル署名アルゴリズム（ECDSA）]

であって、以下に準拠するもの：

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、（FIPS PUB 186-3、「Digital Signature Standard」に定義されている通り）「NIST curves」P-256、P-384、及び[選択：P-521、他の曲線なし]を実装しなければならない。**

適用上の注意：

ST作成者は、デジタル署名を実行するように実装されるアルゴリズムを選択するべきである。もし複数のアルゴリズムが利用可能であれば、この要件は、機能性を特定するために繰返し記述されるべきである。選択されたアルゴリズムに関して、ST作成者は適切な割付／選択を行い、そのアルゴリズムに実装するパラメタを特定するべきである。

楕円曲線に基づくスキームでは、鍵サイズは基点の位数の$\log_2$をとった値を意味する。デジタル署名のための望ましいアプローチとして、楕円曲線が本PPの将来の版で要求されるだろう。

保証アクティビティ：

この要件は、TOEの製造元から提供された更新をTOEにインストールする前に、それらの更新に添付されたデジタル署名を検証するために使用する。このコンポーネントは更新機能に使用されるため、以下に示す保証アクティビティに対する追加の保証アクティビティは、本書の他の保証アクティビティの節で対応する。

以下の保証要件は、デジタル署名アルゴリズムの実装のみを取り扱うものである。評価者は、コンポーネントで選択されたアルゴリズム（1つまたは複数）に適切なテストを実施する。

これらのアルゴリズムで必要となるハッシュ関数及び／または乱数の生成をSTに指定しなければならない。従って、これらの関数に関連する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節に含まれる。さらに、TOEで必要となる機能のみ、デジタル署名を検証する。もし本PPで必要とされる機能の実装をサポートするためにTOEがデジタル署名を生成する場合は、評価と検証のスキームを参照して必要な保証アクティビティを決定しなければならない。

すべてのアルゴリズムについて、評価者はTSSをチェックして、署名検証の全体的なフローが記述されていることを確認する。これには、少なくとも、デジタル署名の検証に使用するデータの形式と一般的な場所（例えば、「ハードディスクドライブ上のファームウェア」、「記憶場所0x00007A4B」）、運用環境から受け取ったデータをデバイスに移動させる方法、及びデジタル署名アルゴリズムの一部としてではなく実行されるすべての処理（例えば、証明書失効リストの検査）が含まれるべきである。

以下の各節では、評価者がデジタル署名スキームのタイプごとに実施しなければならないテストを示す。要件内の割付と選択

に基づいて、評価者はそ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。

以下に示すスキームに関して、鍵生成／ドメインパラメタ生成のテスト要件はないことに注意するべきである。これは、この機能が更新の配布におけるデジタル署名の検査に限定されるために、エンドデバイスでこの機能が必要であるとは想定されないからである。このことは、ドメインパラメタが既に生成されて、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格納域にカプセル化されているべきであることを意味する。もし鍵生成／ドメインパラメタ生成が必要な場合、評価者は、評価と検証のスキームを参照して、必要となる保証アクティビティ及び追加コンポーネントが正しく特定されていることを確認しなければならない。

同様に、本PPのベースライン要件を満たすために署名生成が必要となるとは想定されていない。もし署名生成が必要な場合は、評価と検証のスキームを参照して、必要となる保証アクティビティ及び追加コンポーネントが正しく特定されていることを確認しなければならない。

- ***RSA***

署名生成／検証関数の実装に関して、ANSI X9.31及びPKCS #1（バージョン1.5及び／またはバージョン2.1 PSS）の2つのオプションがある。

これらのオプションの少なくとも1つを実装しなければならない。実装したバージョンごとに、以下に示すようにテストしなければならない。PKCS #1バージョン2.1 PSSを選択した場合、評価者はTSSをチェックして、ソルトの長さが指定されていることを確認しなければならない。

TOEが複数の係数サイズをサポートする場合、評価者はすべての係数サイズに対して以下のテストを実施しなければならない。TOEが複数のハッシュアルゴリズムをサポートする場合、評価者はすべてのハッシュアルゴリズムに対して以下のテストを実施しなければならない。このことは、もし実装で2つの係数サイズと2つのハッシュアルゴリズムを選択できるようにする場合は、評価者は以下のテストを4回実施することを意味する。

評価者は、3つのグループのデータを生成しなければならない。各グループのデータは、係数及びその係数と一致する4セットのテストベクターから成る。テストベクターは、公開されている指数*e*、擬似ランダムに生成されたメッセージ、及び関連するプライベート鍵を使用するメッセージの署名（*e*及び係数*n*と一致する）から成る。このことは、TSFでサポートされる係数サイズ／ハッシュアルゴリズムごとに最小12のテストベクターが存在することを意味する。

テストベクターの4分の3で、正しい署名を生成した後で（ただ

しTSFに「フィード」しない)、署名検証エラー機能をテストするため、評価者は公開鍵、メッセージ、または署名を変更する（それぞれの少なくとも2つを変更することを確実にする)。次に、評価者はTSFを使用してテストベクターを実行し、結果が正しいことを検証しなければならない。

さらに、実装するアルゴリズムが「*Public Key Cryptography Standards (PKCS) #1 v2.1:RSA Cryptography Standard-2002*」に記載されているRSASSA-PKCS1-v1_5であるか、または「X9.31, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)*」に記載されているRSAアルゴリズムである場合、評価者は http://csrc.nist.gov/groups/STM/cavp/documents/dss/SigVer15EMTest.zip（PKCS #1バージョン1.5の実装用）または http://csrc.nist.gov/groups/STM/cavp/documents/dss/SigVer931IRTest.zip（X9.31の実装用）で提供される適切な追加のテストベクターを使用して、実装がこれらのテストに適切に合格することを検証しなければならない。

● ***DSA***

評価者は、TSSを検査して、（L, N）に使用される値が指定されており、使用されるハッシュアルゴリズムが指定されていることを確認する。評価者は、特定の（L,N）に使用さ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Section 5.6.1の表2及び表3に明記された必須の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）の強度が、USBフラッシュドライブで使用される対称（データ）暗号アルゴリズムと同程度となることを確認しなければならない（例えば、もし128ビットのAESを使用して利用者データを暗号化する場合、少なくとも（3072, 256）の（L,N）が必要とされる)。

評価者は、サポートされる（L,N）とハッシュの組み合わせごとに以下のテストを実施する。評価者は、鍵ペアを生成しなければならない。

次に、評価者は、15の1024ビットメッセージを擬似ランダムに生成し、プライベート鍵を使用してそれらのメッセージに署名する。半分程度のメッセージに関して、正しい署名を生成した後で（ただしTSFに「フィード」しない)、署名検証エラー機能をテストするため、評価者は公開鍵、メッセージ、または署名を変更する（それぞれの少なくとも2つを変更していることを確認する)。次に、評価者はTSFを使用してテストベクターを実行し、結果が正しいことを検証しなければならない。

● ***ECDSA***

評価者は、TSSを検査して、実装に使用する曲線（1つまたは複数）が指定され要件と一致しており、サポートされるハッシュ（1つまたは複数）が指定されていることを確認しなければな

らない。評価者は、TSFで実装される曲線とハッシュペアごとに、以下のテストを実施しなければならない。

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、1つの擬似ランダムメッセージ、1つの公開／プライベート鍵ペア（d,Q）、及び1つの署名（r,s）から成る。半分程度のメッセージに関して、正しい署名を生成した後で（ただしTSFに「フィード」しない）、署名検証エラー機能をテストするため、評価者は公開鍵、メッセージ、または署名を変更する（それぞれの少なくとも2つを変更していることを確認する）。次に、評価者はTSFを使用してデータを実行し、結果が正しいことを検証しなければならない。

FCS_COP.1(3) **暗号操作（暗号ハッシュ）**

FCS_COP.1.1(3) **詳細化**：TSFは、以下の*FIPS Pub 180-3「Secure Hash Standard」を満たす* **[選択：SHA-1、SHA 224、SHA 256、SHA 384、SHA 512]**及び**メッセージダイジェストサイズ[選択：160、224、256、384、及び512]ビット**に従って、**暗号ハッシュサービス**を実行しなければならない。

適用上の注意： この要件は、ハッシュ関数を特定することを意図している。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に対応していなければならない。ハッシュの選択は、FCS_COP.1(1)及びFCS_COP.1(2)（128ビットの鍵向けのSHA 256、256ビットの鍵向けのSHA 512)で使用されるアルゴリズムの全体的な強度と一致するべきである。

本PPの後続版では、もはや暗号ハッシュとしての承認されたアルゴリズムではなくなっているだろう。

保証アクティビティ： 評価者は、AGD文書をチェックし、必要なハッシュサイズに機能を設定するために行う必要があるすべての設定が記述されていることを確認する。評価者は、ハッシュ関数とその他のTSF暗号化関数（例えば、デジタル署名検証関数）の関連付けがTSSに文書化されていることをチェックしなければならない。

暗号ハッシュテストでは、
http://csrc.nist.gov/groups/STM/cavp/documents/shs/SHAVS.pdfから入手可能な「*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することができる。1番目のモードはバイト指向のモードである。このモードでは、TSFは整数のバイト長であるメッセージのみハッシュする。例えば、ハッシュされるメッセージの長さ（ビット単位）は8で割り切ることができる。2番目のモードはビット指向のモードである。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。モードごとにテストが異なるため、以降の節ではビット指向のテストとバイト指向のテストについて示す。

評価者は、以下のすべてのテストを、TSFで実装され、本PPの要件を満たすために使用されるハッシュアルゴリズムごとに実施しなければならない。

- **短いメッセージのテスト－ビット指向モード**

評価者は、*m*+1のメッセージから成る入力セットを作成する。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、連続的に0～*m*ビットの範囲となる。メッセージテキストは、擬似ランダムに生成されなければならない。評価者は、各メッセージのメッセージダイジェストを算出し、メッセージがTSFに提供されるときに正しい結果が生成されることを確認する。

- **短いメッセージのテスト－バイト指向モード**

評価者は、*m/8*+1のメッセージから成る入力セットを作成する。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、連続的に0～*m*/8バイトの範囲となり、各メッセージは整数のバイト長となる。メッセージテキストは、擬似ランダムに生成されなければならない。評価者は、各メッセージのメッセージダイジェストを算出し、メッセージがTSFに提供されるときに正しい結果が生成されることを確認する。

- **選択した長いメッセージのテスト － ビット指向モード**

評価者は、*m*のメッセージから成る入力セットを作成する。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512 + 99**i*となる。ここで$1 \le i \le m$である。メッセージテキストは、擬似ランダムに生成されなければならない。評価者は、各メッセージのメッセージダイジェストを算出し、メッセージがTSFに提供されるときに正しい結果が生成されることを確認する。

- **選択した長いメッセージのテスト－バイト指向モード**

評価者は、*m/8*のメッセージから成る入力セットを作成する。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512 + 8*99**i*となる。ここで$1 \le i \le m/8$である。メッセージテキストは、擬似ランダムに生成されなければならない。評価者は、各メッセージのメッセージダイジェストを算出し、メッセージがTSFに提供されるときに正しい結果が生成されることを確認する。

- **擬似ランダムに生成されたメッセージのテスト**

このテストは、バイト指向の実装のみを対象とする。評価者は、

*n*ビット長のシードをランダムに生成する。ここで、*n*はテスト対象のハッシュ関数によって生成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に示されたアルゴリズムに従って、100のメッセージ及び関連するダイジェストのセットを作成する。評価者は、メッセージがTSFに提供されるときに正しい結果が生成されることを確認する。

FCS_COP.1(4) **暗号操作（鍵のマスキング）**

FCS_COP.1.1(4) **詳細化**：TSFは、**[選択：XORの場合、「なし」；AESの場合、「FIPS PUB 197, *Advanced Encryption Standard (AES)*及びNIST SP 800-38A」]**を満たす、指定された暗号アルゴリズム**[選択：XOR；ECBモードで使用されるAES]**及び暗号鍵サイズ**[選択：128ビット、256ビット]**に従って、**鍵のマスキング**を実行しなければならない。

適用上の注意： 1番目の選択に関して、ST作成者は、KEKを使用してDEKをマスキングする方法として、KEK及びDEKをXOR処理するか、またはAESをECBモードで使用する方法のいずれかを選択する。XORを選択する場合、ST作成者は最後の選択で「なし」を選択する。それ以外の場合、FIPS 197及びSP 800-38Aへの参照を選択する。2番目の選択は、KEKのサイズを反映するように行うべきである。

保証アクティビティ： DEKのマスキング方法に「XOR」を使用する場合、評価者はXORの使用がTSSに記述されていることを検証しなければならない。AESを使用する場合は、次の保証アクティビティを実施する。

評価者は、KEKを使用してAESでDEKをマスキングする方法／アルゴリズムをベンダが記述していることを確認しなければならない（例えば、FIPS文書で指定されたオプションが識別されている、入力をパディングする方法、出力の切り詰めなど）。

評価者は、以下のテストを実施しなければならない。複数のモードがサポートされる場合、評価者はTSS及びガイダンス証拠資料を検査して、エンドユーザがECB及び指定された鍵サイズをどのように選択するのかを決定する。次に、評価者は、必要に応じて、各鍵サイズを次の節に示されている方法でテストする。これらのテストには、評価施設のスキームで許容可能なアルゴリズムのリファレンス実装が必要となるものがあることに注意すること。

● ***ECBモード***

ECBモードテストでは、
http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdfから入手可能な「*The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)*」[AESAVS]を参照する。

評価者は、TSFでサポートされる鍵サイズごとに一連の既知の答えを使用したテストを実施しなければならない。入力は1つの鍵及び暗号化する平文または復号する暗号文である。

http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip のサポートされる鍵長でECBモードのすべてのテストベクター（暗号化と復号の両方）を使用して、これらのテストを実施しなければならない。

評価者は、サポートされる鍵長ごとに、複数ブロックのメッセージのテストを実施しなければならない。このテストを実施するため、評価者は暗号化用に10のデータセットを生成し、復号用に10のデータセットを生成する。各データセットは、鍵及び平文（暗号化の場合）または暗号文（復号の場合）から成る。ブロック長は128ビットでなければならない。平文／暗号文の長さは、ブロック長* iでなければならない。ここで、iはデータセット数を示し、iの範囲は1～10となる（そのため、メッセージの範囲は128ビット～1280ビットとなる）。

評価者は、モンテカルロテストを実施しなければならない。評価者は、暗号化には10セットの初期値（鍵及び平文の値）を生成し、復号には10セットの初期値（鍵及び暗号文の値）を生成しなければならない。平文／暗号文の長さは128ビットでなければならない。各初期値のセットを使用して、100のテストを生成及び実施する。100のテストの値（初期値のセットごと）を生成するためのアルゴリズムは、[AESAVS]のsection 6.4.1に含まれている。

拡張：暗号操作（ランダムビット生成器）（FCS_RBG_EXT）

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、1つ以上の独立したTSFハードウェアベースのノイズ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初期化された[選択、次から1つを選択[選択：Hash_DRBG （任意）、HMAC_DRBG（任意）、CTR_DRBG （AES）、Dual_EC_DRBG （任意）]を使用したNIST Special Publication 800-90； FIPS Pub 140-2 Annex C； AESを使用したX9.31 Appendix 2.4] に従ってすべてのランダムビット生成（RBG）サービスを実行しなければならない。

FCS_RBG_EXT.1.2 決定論的RBGは、少なくともそのRBGが生成する鍵及び認証要素の最大長と等しい、かつ、最小[選択、次から1つを選択：128ビット、256ビット]のエントロピーによって初期化されなければならない。

適用上の注意： NIST Special Pub 800-90, Appendix Cは、FIPS-140の将来のバージョンで要求される可能性がある最小エントロピーの測定について記述している。可能であれば、直ちにこれを使用するべきであり、本PPの将来の版ではこれが要求されるだろう。

FCS_RBG_EXT.1.1の最初の節について、ST作成者はRBGサービスが適合する規格（NIST SP 800-90またはFIPS Pub 140-2 Annex Cのいずれか）を選択するべきである。

SP 800-90は、4つの異なる乱数生成手法を含んでいる。これらの手法は基盤となる暗号プリミティブ（ハッシュ関数／暗号）に依存する。ST作成者は、使用される関数を選択し（もしSP 800-90を選択した場合）、要件またはTSSの中で使用される特定の基盤となる暗号プリミティブを含める。Hash_DRBGまたはHMAC_DRBGに関しては、識別されたハッシュ関数のいずれか（SHA-1、SHA-224、SHA-256、SHA-384、及びSHA-512）が許可されるが、CTR_DRBGに関してはAESに基づく実装のみが許可される。

Dual_EC_DRBGに関しては800-90で定義されたすべての曲線が許可されるが、ST作成者は選択した曲線だけでなく使用されるハッシュアルゴリズムも含めなければならない。

FIPS Pub 140-2 Annex Cに関して、現在、「*NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms*」、Section 3に記述された手法のみが有効であることに注意すること。ここで使用されるAES実装の鍵長が利用者データを暗号化するために使用するものと異なる場合、FCS_COP.1は、異なる鍵長を反映するように調整するか、または繰返し記述することが必要になるかもしれない。FCS_RBG_EXT.1.2における選択について、ST作成者はRBGを初期化するために使用されるエントロピーの最小ビット数を選択する。

ST作成者は、TOEのベースライン要件に基本的なすべての関数が含まれることも確実にする。

将来的に、「*A Method for Entropy Source Testing:Requirements and Test Suite Description*」に記述された要件の大部分が本PPで要求されるだろう。以下の保証アクティビティは、現在、要求されるアクティビティのサブセットのみ反映している。

保証アクティビティ：　評価者は、TSS節をレビューして、TOEで使用されるRBG（1つまはた複数）を含んでいる製品のバージョン番号を確認しなければならない。評価者は、エントロピーを収集するハードウェアベースのノイズ源がTSSに記述されていることも確認しなければならない。さらに、評価者は、RBGで使用される基本的なすべての関数及びパラメタがTSSにリストアップされていることを検証する。

評価者は、エントロピー入力を取得する方法に加えて、使用されるエントロピー源の識別、各エントロピー源からエントロピーがどのように生成／収集されるのか、及び各エントロピー源からどれだけのエントロピーが生成されるのかを含めた、RBGモデルの記述がTSSに含まれていることを検証しなければならない。また、評価者は、エントロピー源の正常性テスト、エントロピー源の正常性を判断する上で正常性テストが十分である根拠、及びエントロピー源故障の既知のモードについても、TSSに記述されていることを確認しなければならない。最後に、評価者は、時間条件及び／または環境条件による出力と分散の

独立性の観点でRBG出力の記述がTSSに含まれていることを確認しなければならない。

RBGが適合を主張している規格に関係なく、評価者は以下のテストを実施しなければならない。

テスト1：評価者は、*エントロピー源テストスイート*を使用して、各エントロピー減についてエントロピーの推量を決定しなければならない。評価者は、すべてのエントロピー源から取得されたすべての結果の最小値であるエントロピー推定量がTSSに含まれることを確実にしなければならない。

評価者は、RBGが適合する規格に従って、以下のテストも実施しなければならない。

- **FIPS 140-2, Annex Cに適合する実装**

この節に含まれるテストについての参考文献は、「*The Random Number Generator Validation System (RNGVS)*」[RNGVS]である。評価者は、次の2つのテストを実施しなければならない。「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り生成されることに注意すること。正しさの証明は各制度に任されている。

評価者は、可変シードテストを実施しなければならない。評価者は、TSF RBG関数に128（シード、DT）ペアのセットをそれぞれ128ビットで提供しなければならない。また、評価者は、すべての128（シード、DT）ペアに一定の（AESアルゴリズムに適切な長さの）鍵を提供しなければならない。DTの値は、セットごとに1ずつ増加される。シードの値は、セット内で反復してはならない。評価者は、TSFから返される値が期待値と一致していることを確認する。

評価者は、モンテカルロテストを実施しなければならない。このテストでは、TSF RBG関数に初期シードとDTの値をそれぞれ128ビットで提供する。また、評価者は、テストを通して一定の（AESアルゴリズムに適切な長さの）鍵を提供しなければならない。評価者は、DTの値を毎回1ずつ増加させ、NIST - Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3の指定に従って生成された後続の新しいシードを使用して、TSF RBGを10000回呼び出す。評価者は、10000回目に生成された値が期待値と一致することを確認する。

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

評価者は、RNG実装について15回試行しなければならない。もしRNGが設定可能であれば、評価者はそれぞれの設定について15回試行しなければならない。また、評価者は、RNG機能を設定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ければならない。

もしRNGが予測耐性を備えている場合、それぞれの試行は(1)drbgのインスタンス化、(2)ランダムビットの1番目のブロックの生成、(3)ランダムビットの二番目のブロックの生成、(4)終了処理（ゼロ化）、から成る。評価者は、ランダムビットの2番目のブロックが期待値であることを検証する。評価者は、それぞれの試行について8つの入力値を生成しなければならない。1番目はカウンタ（0 –14）である。次の3つは、インスタンス化操作のためのエントロピー入力、ナンス、及び個別化文字列である。次の2つは、生成の初回呼び出しのための追加入力とエントロピー入力である。最後の2つは、生成の2回目の呼び出しのための追加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。「ランダムビットの1ブロックを生成する」とは、返されるビット長が（NIST SP 800-90で定義された）出力ブロック長と等しくなるランダムビットを生成するという意味である。

もしRNGが予測耐性を備えていない場合、それぞれの試行は(1)drbgのインスタンス化、(2)ランダムビットの1番目のブロックの生成、(3)初期化、(4)ランダムビットの2番目のブロックの生成、(5)終了処理（ゼロ化）、から成る。評価者は、ランダムビットの2番目のブロックが期待値であることを検証する。評価者は、それぞれの試行について8つの入力値を生成しなければならない。1番目はカウンタ（0 –14）である。次の3つは、インスタンス化操作のためのエントロピー入力、ナンス、及び個別化文字列である。5番目の値は、生成の初回の呼び出しのための追加入力である。6番目と7番目は、初期化の呼び出しのための追加入力とエントロピー入力である。最後の値は、生成の2回目の呼び出しのための追加入力である。

以下に、評価者が生成／選択する入力値のいくつかに関して詳しい情報を示す。

エントロピー入力：エントロピー入力値の長さは、シード長と等しくなければならない。

ナンス：ナンスがサポートされている（dfなしのCTR_DRBGがナンスを使用しない）場合、ナンスビット長はシード長の半分となる。

個別化文字列：個別化文字列の長さは、シード長以下でなければならない。もし実装が1つの個別化文字列のみサポートするなら、両方の値について同じ長さが利用可能である。もし複数の文字列の長さをサポートするなら、評価者は2つの異なる長さの個別文字列を使用しなければならない。実装が個別文字列を使用しない場合は、値を提供する必要はない。

追加入力：追加入力のビット長は、個別化文字列長と同じデフォルト値及び制約条件を持つ。

4.1.2　クラス：利用者データ保護（FDP）

このファミリは、保存されたすべてのデータの暗号化を必要とする。

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)に従ってフルディスク暗号化を実行しなければならない。
FDP_DSK_EXT.1.2	FCS_CKM.1(2)及びFCS_COP.1(4)に指定されている通りに導出されたKEK（または中間鍵）を用いてDEKがマスキングされる場合、DEKは電源がオフになっているハードディスク上にのみ存在する。
FDP_DSK_EXT.1.3	TSFは、利用者の操作なしに、すべてのデータを暗号化しなければならない。
FDP_DSK_EXT.1.4	平文の鍵とする材料は、ハードディスク上の永続記憶域に書き込んではならない。
適用上の注意：	「フルディスク暗号化」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ディスク上にあるすべてのデータを暗号化し、FDE製品への認証が成功した後にのみデータへのアクセスを許可するプロセス」と定義されており、認証要素を受け入れて処理するために必要なコードが含まれるMBR及び関連するブート可能なパーティションは除外される。 この要件は、重要なファイルの暗号化が、そのファイルを保護するための利用者の選択に依存しないことを特定することを意図している。FDP_DSK_EXT.1に指定されたディスク暗号化は、利用者に対して透過的に行われ、データを保護するという決定は利用者の裁量には含まれない。このことが、ディスク暗号化をファイル暗号化と区別する特徴となっている。 この要件は、利用者データが含まれた明示的に格納されているファイルに対処するだけでなく、ディスク上のスワップファイル、レジストリ、及びその他の運用環境格納領域に格納されているデータチャンクも含む。すべてのリムーバブルメディアの暗号化は必要とされない。ただし、すべてのハードドライブの暗号化が必要とされる。
保証アクティビティ：	評価者は、この要件の保証アクティビティを実施する際、STのTSS節を参照しなければならない。評価者は、データをディスクに書き込む方法及び暗号化機能を適用する場所について、記述が包括的であることを確認することに焦点を当てる。例えば、もし暗号化をハードドライブ自体に格納されたファームウェアとハードウェアに直接実装するなら、TOEが設定されて機能を開始したら、ハードディスクに送られるすべてのデータが暗号化され、ハードディスクから受け取るすべてのデータが復号されることを、TSSの記述で主張することができる。ただし、もし暗号化／復号機能の実装をホストオペレーティングシステム

上のソフトウェアのみで行うなら、ディスクにアクセスするすべての方法がこれらの機能を通過することをTSSで主張しなければならない。

このことは、TOEに含まれるすべてのデバイスに当てはまる。もし暗号化／復号をディスクコントローラまたはディスクドライブ自体に実装するなら、どのような状況でPPに適合する方法でTOEを使用する（つまり、すべてのハードドライブを暗号化する）のかを（ST及び管理者ガイダンスの両方に）明確にしなければならない。

レビューの実施時に、評価者は、MBRの読み込み及び認証機能を実行するTOEの部分に関して、電源オン時に発生するアクティビティがTSSに記述されていることを確認しなければならない。TOEの初期化、及びTOEを初回確立するときにすべてのディスクが完全に暗号化されることを確実にするために実施するアクティビティについて、TSSでカバーしなければならない。ディスクの暗号化されない領域（例えば、MBRに関連する部分）についても記述されなければならない。

評価者は、DEKをラップ解除してTOEに格納する方法を含め、FCS要件の暗号化関数を使用して暗号化機能を実行する方法についても、記述でカバーされていることを確認しなければならない。評価者は、電源オフの各シナリオ（FCS_CKM_EXT.4の保証アクティビティを参照）について、DEKがKEKでラップされるのをTOEがどのように確実にするのか、TSSに記述されていることを確認しなければならない。

評価者は、システムで利用できる他の機能（例えば、DEKの再生成）により、暗号化されていないデータまたは鍵とする材料をディスク上に格納しないことをどのように確実にするのか、TSSに記述されていることを確認しなければならない。

もしTOEが複数のディスク暗号化をサポートする場合、評価者は、管理者ガイダンスを検査して、初期化手順がプラットフォーム上の暗号化されるすべてのディスクのニーズに対応していることを確認しなければならない。

評価者は、TSSをレビューして、鍵とする材料が暗号化されない状態でハードディスクに書き込まれないことが主張されていることを確認する。通常の利用では、ディスクへの書き込みはすべて暗号化されるため、1つのアプローチとして、ディスクの暗号化されない部分にデータが書き込まれるという例外的なケースに関して論証を行って、鍵とする材料がそれらの領域に書き込まれるのを防ぐ方法を詳述するというアプローチがある。

評価者は、AGDガイダンスをレビューして、必要なすべての準備手順を含め、FED機能を有効にするために必要な初期手順が記述されていることを確認しなければならない。このガイダンスに、すべてのプラットフォームで、暗号化が有効になっている場合は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実にするための十分な指示が記述されなければならない。

評価者は、以下のテストアクティビティを実施しなければならない。

- テスト1：初期化アクティビティを実行し、すべてのディスクが暗号化されることを確認する。デバイスで暗号化されないことが判明している領域について、それらの領域に利用者データまたは重要なTSFデータを書き込むことができないことを（例えば、TSSまたは操作ガイダンスで）正当化する。ディスクの検査は、いくつかの方法で実施することができる。ドライブを物理的に取り外して別のコンピュータに差し込むというのが1つの方法である。また、許容可能な検査方法の例として、暗号化されたハードドライブを収容するシステムを外部デバイスから起動して、暗号化されたデバイスに直接アクセスするという方法もある。
- テスト2：ディスクへの書き込み時に、データ（OSのページファイルに保存される可能性があるデータを含め）が暗号化されることを確認する。これをテストする範囲は前のテストと一致する。つまり、システムの電源を「正常」にオンにし、データがディスクに書き込まれた後で、前のテストで示された方法を使用して、これらのデータが暗号化されない状態でデバイスに存在することがないことを確認することが許容可能である。

4.1.3 クラス：識別と認証（FIA）

拡張：FDE利用者認証（FIA_AUT_EXT）

FIA_AUT_EXT.1	**拡張：FDE利用者認証**
階層関係：	他のコンポーネントなし。
FIA_AUT_EXT.1.1	TSFは、利用者認証を実行するために、FCS_CKM.1.1(2)及びFCS_COP.1(4)に定義された通りにメカニズムを提供しなければならない。
FIA_AUT_EXT.1.2	TSFは、FIA_AUT_EXT.1.1で提供されるメカニズムを使用して、デバイスの利用者データへのアクセスを許可する前に、利用者認証を実行しなければならない
FIA_AUT_EXT.1.3	TSFは、デバイスの暗号化されていないデータへのアクセスを許可する前に、利用者が入力した認証要素が有効であることを検証し、[選択：他のアクティビティなし、外付けトークンにアクセスできなくなったことを確実にしなければならない]。
FIA_AUT_EXT.1.4	TSFは、各認証要素の検証方法が、KEKまたはDEKを導出するために使用されるKEK、DEK、またはCSPの効果的な強度を公開または低減しないことを確実にしなければならない。
適用上の注意：	この要件は、利用者にディスクの復号を許可し、システムにア

クセスできるようにするメカニズムを特定することを意図している。このことが個々の利用者の認証とは見なされないことに注意すること。認証要素は、複製して、ハードディスクの許可された利用者すべてに提供することができる。または、利用者が個々の利用者に固有の認証要素を持つこともできる。

ベンダは、本質的にKEKのチェーン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る鍵は、KEKによって暗号化されるDEKの要件を満たさなければならない。すべての中間鍵は、別の鍵によって暗号化される必要がある。ST作成者は、FCS_CKM及びFCS_COPの要件の繰返しによって、これをSTに含めなければならない。

ハードディスクの認証要素を紛失した場合は、DEKをTOEからエクスポートした、または認証要素をバックアップした（または、紛失していない別の認証要素のセットでDEKを暗号化した）のなら、データを回復することができる。暗号化したDEKがTOEで破損している場合、データを回復するためには、認証要素のバックアップは十分ではないだろう。

FIA_AUT_EXT.1.3の選択に関して、外付けトークン認証要素の使用がサポートされない場合、STは「他のアクティビティなし」を選択するべきである。ただし、FCS_CKM.1.1(3)でSTに外付けトークンを選択する場合は、「外付けトークンにアクセスできなくなったことを確実にしなければならない」を選択する必要がある。意図する実装では、ハードディスクを収容するシステムにトークンが残される（従って、TOEが提供する保護をくぐり抜ける）可能性を低減するため、利用者が完全にアクセスできるようになる前に、トークンを取り外すことを利用者に強制するべきである。ただし、いかなる場合も、使用される認証要素の検証が必要となる。

エレメント1.3及び1.4は、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が提供する、認証要素の検証に関するものである。認証要素が有効でない場合、TSFがKEKを形成し、KEKを使用してDEKのマスクを解除し、利用者に無意味な情報を示すよう試行するのは望ましくない。ただし、認証要素が有効であることを、攻撃者が他の要件をくぐり抜けることが可能になるような方法でチェックするべきでない。この操作は通常、ホスト上で行われるため、攻撃者に監視／逆アセンブルされる可能性がある。よって、この操作はこの脅威を考慮して設計しなければならない。

利用者認証は、その利用者をデバイスにアクセスできるようにするとき（つまり、USBポートに差し込んで、基盤となるOSによって認識されるとき）にのみ実行する必要がある。上記の要件は、すべてのデバイスまたはファイルアクセスの前に利用者認証を実行する必要があることを意味すると解釈するべきではない。ただし、利用者が自身のパスワードベースの認証要素を変更することを希望する場合は、変更を完了する前に利用者認証機能を呼び出す必要がある。

保証アクティビティ：　評価者は、TSS節をチェックして、TOEを初期化する方法、つまり電源オン、MBRのアクセス、及び認証アクティビティを実行するコードの読み込みを含む一連のイベントが、TSSに記述されていることを確認しなければならない。もし操作ガイダンスに異なるセットアップモード（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、認証要素を入力する前に、これらのモードによってハードディスク上のデータへのアクセスが許可されないことがTSSに記述されていることを確認しなければならない。 もし外付けトークン認証要素がサポートされる場合、評価者は、利用者にハードディスクへのアクセスを許可する前に、外付けトークンにアクセスできないことをTOEがどのように確実にするのか、TSSの記述をチェックしなければならない。評価者は、操作ガイダンスをチェックして、ハードディスクが動作している間、認証要素を保護することができるよう、ディスクにアクセスするために外付けトークンを使用した後で、外付けトークンを物理的に取り外さなければならないことを利用者に通達していることも確認しなければならない。

評価者は、利用者にドライブ上のデータへのアクセスを許可する前に、認証要素をどのように検証するのかについて、TSSに記述されていることをチェックしなければならない この記述は、使用される方法によってDEK、KEK、またはその他の鍵とする材料が公開されないことを評価者が判断できるよう、十分に詳細なものでなければならない。「公開」には、DEKまたはKEKの弱体化の概念も含まれる。もし別の認証要素を使用してKEKを作成するためのサブマスクを提供するなら、各認証要素をチェックする別の方法を使用することは必要とならない。評価者は、認証要素を認証するために使用するメカニズムの分析について、テスト報告書（ATE_IND）に文書化しなければならない。

評価者は、以下のテストを実施しなければならない：

- テスト 1：ハードドライブデバイス上の暗号化されていないデータへのアクセスを許可する前に、認証要素の入力が求められることを確認する。サポートされる認証要素ごとに、認証要素を誤って入力すると、正しくない認証が提供されたことを示す通知が TOE から表示されることを確認する。
- テスト 2 [条件付]：外付けトークン認証要素が必要な場合、デバイスの暗号化されていないデータへのアクセスを許可する前に、TOE が認証要素を読み取ったら、外付けトークン認証要素にアクセスできなくなることを確認する。
- テスト 3 [条件付]：バイパスまたは別のブートモードを提供する場合、テストを実施して、そのモードが要件と一致している（つまり、暗号化されていないデータへのアクセスの前に、適切な認証要素が入力される必要がある）ことを確認する。

- テスト4：認証要素を正しく入力してデバイスへのアクセスを取得した後で、既に入力した認証要素とは別の識別及び認証が、利用しているプラットフォームによって要求されることを確認する。

4.1.4 クラス：セキュリティ管理（FMT）

この節の主な目的は、不注意な利用者がディスクエンクリプタをセキュアでない状態にすることを防ぐために、管理者が実施しなければならない（または実施してはならない）重要なアクティビティを示すことである。適合TOEの管理モデルは、本PPの1.1.4節に記述されている。追加機能をTOEで提供する場合は、附属書Cの適切な管理要件及びI&A要件をSTに含めるべきである。

TSFデータの管理（FMT_MTD）

FMT_MTD.1(3) **TSFデータの管理（すべての対称鍵の読み出しに関して）**

FMT_MTD.1.1(3) **詳細化**：TSFは、*すべてのプリシェアード鍵、対称鍵、及びプライベート鍵の読み出し*を**防止**しなければならない。

適用上の注意： この要件は、「通常」のインタフェースを通して（保存された、または一時的に）識別された鍵はどの利用者または管理者も読み出し及び表示できないことを意図している。もちろん、権限を持つ管理者は、メモリを直接読み出してこれらの鍵を表示できるが、そのようなことはしないと信じられている。

保証アクティビティ： 評価者は、TSSを検査して、プリシェアード鍵、対称鍵、及びプライベート鍵がどのように保存されるのかが詳述されていることを確認し、適用上の注意に概説されているように、その目的のために特別に設計されたインタフェースを通してこれらの鍵を表示できないことを確認しなければならない。もし、これらの値が平文で保存されないなら、それらをどのように保護または不可視化するのかをTSSに記述しなければならない。

管理機能の特定（FMT_SMF）

FMT_SMF.1 **管理機能の特定**

FMT_SMF.1.1 TSFは、次の管理機能を実行できなければならない：

a) **暗号化操作のため、ハードドライブを初期化するときにDEKを生成する。**

b) **利用者が入力した認証要素、具体的に、[選択、次から1つまたは両方を選択：パスフレーズベースの認証要素、外付けトークン認証要素]及び[選択：他の要素なし、[割付：他の認証要素]]から導き出されたサブマスクから形成されたKEKを使用してDEKをラップする。**

c) **パスワードベースの認証要素を変更する。**

d) **[選択：次から1つを選択：他の機能なし、[選択：デフォルトの認証要素を変更する、利用者認証パスフレーズを生成する、外付けトークン認証要素を生成する、**

暗号機能を設定する、鍵エスクロー機能を無効にする、[割付：TSFが提供する他の管理機能]]。]

適用上の注意：

この要件は、TOEが持つ管理機能を示すことを意図している。これは、記載されている機能をTOEが実行できなければならないことを意味する。項目(a)及び(b)は、操作上の使用に必要となる鍵とする材料を規定する。項目(c)は、利用者が自身の認証要素を変更できるようにする。また、項目(d)は、TOEに含めることが可能であるがPPに適合するためには必須ではない機能を特定するために使用する。

上記の項目(b)に関して、FCS_CKM.1(2)によってKEKの形成に影響する適切な認証要素をST作成者が特定するべきである。実装の観点から、これにより、認証要素がDEKにバインドされてエンドユーザに提供できるようになる。これらの認証要素は、利用者の管理下で入力または生成されなければならない。エスクロー機能は存在してもよいが、DEK／KEKの生成時に回復鍵またはエスクロー鍵が生成されないように、エスクロー機能を無効にしなければならない（または機能を無効にしておかなければならない）。

上記の項目(c)に関して、パスワードベースの認証要素のみが変更可能でなければならない。もし、他の認証要素を変更可能にする場合は、ST作成者は項目(d)の割付を使用するべきである。また、これらの追加機能をサポートするため、適切な保証アクティビティと根拠も追加する必要がある。

上記の項目(d)で、もし管理機能を提供（または主張）しない場合は、「他の機能なし」を選択するべきである。以下に、他の一般的なオプションを示す：

- 「利用者認証パスフレーズを生成する」を選択する場合、ST作成者は、パスフレーズを生成するためにTOEによって使用されるパラメタを識別する、附属書C「C.6 *認証パスフレーズの生成*」の情報を含める必要がある。
- 「外付けトークン認証要素を生成する」を含める場合、附属書CのC.4の要件をSTに含めなければならない。
- TOEで暗号化機能（例えば、DEKの鍵サイズ）を設定可能にする場合、「暗号化機能を設定する」を含める。提供される機能の詳細は、この要件内に箇条書きで記述するかTSSに含めることができる。
- TOEに鍵エスクロー機能を含める場合、エスクロー鍵が生成されないよう、利用者がこの機能をオフにするための機能をTOEが提供しなければならない。
- 「他の管理機能」を指定する場合、評価を監督する国家制度を参照して、STが本PPへの適合を主張できるよう、必要となる可能性がある保証アクティビティ及び他の機能要件が適切に特定されていることを確認しなければならない。

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、ST作成者が行う選択によって決定される。この節では、上記のコンポーネントにおける選択の保証アクティビティ（「他の管理機能」の割付を除く）について説明する。STで機能を選択しない場合は、示されている保証アクティビティを実施する必要がないことを理解するべきである。以下の節は、容易に参照できるよう、「必須のアクティビティ」と「条件付きのアクティビティ」に分かれている。

必須のアクティビティ

上述の機能を管理者（TOEの利用者のセットのサブセットである、特権を持つグループ）に制限する（運用環境からの大きな支援と共に）ことが、本PPに適合する製品の要件であるが、TOE実装によっては、それを行うための要件及び関連する保証アクティビティがSTの他の場所に課される。本PPの1.1.4節に詳述したように、実行することが可能なさまざまなシナリオがあり、相互に関連付けられる保証アクティビティは、類似しているが範囲と実装の点で異なる。

通則

評価者は、TSS及びAGDガイダンスをレビューして、管理を実行するために必要なTOE以外の製品がすべて識別されていることを確認しなければならない。例えば、もし管理機能がJavaアプレットやWebブラウザインタフェースを通して提供されるなら、配置する必要があるものの詳細がTSSで提供される。

DEKの生成

評価者は、AGDガイダンスをレビューして、DEKを生成するための指示が記述されていることを確認しなければならない。この指示が、TOEが適合を主張するすべての環境をカバーしており、DEKを正常に生成または再生成するために存在しなければならない前提条件を含んでいなければならない。TSSをチェックして、DEKの生成方法に関する記述がAGDガイダンスの指示と一致していることを確認する。また、プラットフォームが異なっていることから生じる差分を考慮に入れる。新しいDEKを生成及びインストールしたときに既存のデータで発生する処理についても、TSSに記述しなければならない。評価者は、以下のテストも実施しなければならない。

- テスト1：「クリーン」インストール時に、管理者がDEKを生成することができる。
- テスト2：ディスクが既に暗号化された状態で、ディスク（1つまたは複数）に新しいDEKを生成して、新しいDEKが以前のDEKとは異なることを検証する。
- テスト3：TSS及びAGD_OPR／AGD_PREガイダンスの情報を使用して、DEK再生成プロセスの機能として、TOEの利用者に表示される機能性に関して行われてい

る主張を検証する（例えば、新しいDEKを生成した後でも、以前のDEKを使用して暗号化されたファイルが表示される）。

適切な認証要素のサブマスクから形成されたKEKを使用するDEKの保護

STは、TOEでサポートされる認証要素を特定し、TOEの機能を正しく使用するために必要となる認証要素の数及び組み合わせに関して要件を提供する（これはFCS_CKM要件で行われる）。この要件は、認証要素から生成されたKEKを使用したDEKの最初のラッピング（または新しいDEKのラッピング）に関するものである。認証要素は、ディスクごとまたは利用者ごとにすることができる。評価者は、AGDガイダンスをレビューして、サポートされる認証要素ごとに、この操作で認証要素がどのようにTSFに入力されるのか、ガイダンスに詳述されていることを確認しなければならない。評価者は、TSS節をレビューして、さまざまな認証要素を組み合わせてKEKを形成する方法、及びKEKを使用してDEKをマスキングする方法がTSSに記述されていることを確認しなければならない。また、このプロセスと「通常」の操作で使用されるプロセス（つまり、TOEが一度確立された場合）に相違点があるかどうかも明確になっていなければならない。この記述に、FCS_CKM.1*要件の保証アクティビティに記述されている情報を含めることもできる。サポートされる認証要素がプラットフォームによって異なる場合、AGDガイダンスで、各プラットフォームの最小要件及び各プラットフォームで適用される認証要素に関するその他の制限が明確になっていなければならない。評価者は、以下のテストも実施しなければならない。

- テスト4：サポートされる最小数の認証要素ごとに、DEKを確立し、管理者が認証要素を入力して暗号化されたDEKを生成できることを確認する。このテストを実施する回数は、サポートされるプラットフォームの数及び必要となる認証要素の違いによって異なる。例えば、TOEがプラットフォームAではパスフレーズベース認証要素のみをサポートし、プラットフォームBではパスフレーズベース認証要素と外付けトークン認証要素の両方を要求するとする。また、プラットフォームCではパスフレーズベース認証要素、外付けトークンベース認証要素、及び網膜スキャンベース認証要素をサポートするが、（プラットフォームCでは）外付けトークン認証要素の最小限の使用を要求するとする。評価者は、少なくとも次のテストを実施する：プラットフォームAでパスフレーズベース認証要素を使用したテスト。プラットフォームBでパスフレーズベース認証要素と外付けトークン認証要素の組み合わせを使用したテスト。プラットフォームCで外付けトークン認証要素を使用したテスト。プラットフォームCで外付けトークンベース、パスフレーズベース、及び網膜スキャンベース認証要素の組み合わせを使用したテスト。

パスフレーズベース認証要素の変更

評価者は、操作ガイダンスを検査して、パスフレーズベース認証要素を変更する方法が記述されていることを確認しなければならない。また、評価者は、TSSを検査して、このアクティビティの実行時にホスト及びハードディスクデバイスで実行される一連のアクティビティが記述されていることを確認し、この変更時にKEK及びDEKが公開されないことを確認しなければならない。評価者は、以下のテストも実施しなければならない：

- テスト5：評価者は、ハードディスクデバイス用のパスフレーズ認証要素を確立しなければならない。評価者は、利用者データをホストからデバイスに転送しなければならない。評価者は、「認証要素の変更」機能を使用してデバイスのパスワードを変更し、現在の認証要素の入力を求めるプロンプトが表示されることを確認しなければならない。評価者は、現在の認証要素について正しくない値を入力し、認証要素が変更されないことを観察しなければならない。評価者は、現在の認証要素について正しい値を入力すると、デバイス上のデータにアクセスできることを確認しなければならない。また、評価者は、古い認証要素を使用して（認証要素の変更が成功した後で）、デバイス上の利用者データへのアクセスが提供されなくなることを確認しなければならない。

条件付きのアクティビティ

上記の要件の項目(d)には、TOEで提供することが可能であるが本PPに適合するためには必須ではない機能を特定する、複数の節が含まれる。ただし、この機能を提供する場合は、附属書Cの該当する要件を含めて上記の関連する選択を行うことにより、TOEは適合を主張することができる。適用上の注意に示されているように、割付を行う場合は、PPへの適合を主張できることを判断するために、評価を監督する国家制度を参照する必要がある。

ハードディスクデバイスが、デフォルトの認証要素が設定された状態で到着する場合がある。その場合は、それらの認証要素を変更するメカニズムが存在するよう、選択(d)を選択する。操作ガイダンスに、利用者がデバイスの所有者となったときに、利用者がこれらの要素を変更する方法を記述しなければならない。TSSに、存在するデフォルトの認証要素を記述しなければならない。評価者は、以下のテストも実施する：

- テスト6：[条件付]TOE がデフォルトの認証要素を提供する場合、評価者は、操作ガイダンスに記述されているように、デバイスの所有者となる過程でこれらの要素を変更しなければならない。次に、評価者は、（古い）認証要素がデータのアクセスには有効でなくなったことを確認しなければならない。

項目(d)のアクティビティのうち2つは、認証要素として外付けトークンに格納されるパスフレーズとビット文字列の生成に関するものである。これらのケースごとに、附属書Cから追加の要件をSTに含める。これらの要件に関連するのは、認証要素をどのように生成するかの細部に対応する保証アクティビティである。この要件に関して、評価者は、AGD情報をレビューして、必要な特性を備えた認証要素を生成できるよう、認証要素メカニズムを呼び出す手順が詳述されており、十分に明確であることを確認しなければならない。これらのメカニズムに関連するテストは、これらの特定のメカニズムの保証アクティビティの一部として特定される。

一部のTOEでは、使用される基盤となる暗号化に関する選択があるかもしれない。例えば、DEKのビット長や、AESに使用される暗号化モードに関する選択があるかもしれない。繰返しとなるが、PPへの適合を主張するために、この機能をTOEに提供する必要はない。ただし、機能を提供する場合は、STで特定し、上記の要件の「暗号化機能を設定する」を選択する。

この選択に関して、評価者は、暗号化機能のどの部分が設定可能であるのかSTから確認しなければならない。これにより、暗号化機能に関して、FCS要件、TSSの関連する記述、及びTOEに関連する追加の文書を確認することが必要となる。この情報を持って、評価者は、AGD文書をレビューして、主張されているすべてのメカニズムの操作に関する指示が記述されていることを確認しなければならない。評価者は、以下のテストも実施しなければならない：

- テスト 7 [条件付]：サポートされる設定可能な暗号化モードごとに、評価者は、AGD の指示に従って、TOE の機能が想定どおりに動作する（つまり、ハードディスクが適切に暗号化／復号される）ことを確認する。詳細をこの保証レベルで検証することは必要とされない（つまり、TOE で AES の 128 ビット鍵または 256 ビット鍵を許可する場合、評価者は、鍵長を決定するためにデバッガでプロセスを実行する必要はない）が、比較分析をいくつか実施する必要がある。例えば、もし複数の AES モードをサポートしている場合、同じ DEK で異なるモードを選択すると、異なる暗号文がハードディスクに生成されるべきである。

TOEが鍵エスクローをサポートする場合は、そのことがTSSに記述されていなければならない。また、TSSには、エスクローとする材料をエスクローホルダーに提供する方法を含め、この機能を無効にする方法についても記述されていなければならない。この記述を評価者がテストに使用して、エスクロー機能が実際に無効になったかどうかを確認できることを意図している（例えば、もし新しいKEK／DEKが生成されると材料がネットワーク接続経由で第三者に送信されることがTSSに示されている場合、評価者は、機能を無効にし、ネットワークモニタを接続し、新

しいKEK／DEKが生成されるとネットワーク接続が確立されるかどうかを確認することができる）。この機能を無効にするためのガイダンスが、AGD文書に記述されていなければならない。

- テスト 8 [条件付] TOE がエスクロー機能を提供し、その効果が TOE インタフェースに表示される場合、評価者は、エスクロー機能が無効になっていること、またはベンダから提供されたガイダンスに従ってエスクロー機能を無効にできることを確認するテストを作成しなければならない。

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：TSFシステムファイル保護**
FPT_TUD_EXT.1.1	TSFは、管理者にTOEのファームウェア／ソフトウェアの現在のバージョンを照会する機能を提供しなければならない。
FPT_TUD_EXT.1.2	TSFは、管理者がTOEのファームウェア／ソフトウェアに対して更新を開始する機能を提供しなければならない。
FPT_TUD_EXT.1.3	TSFは、TOEのファームウェア／ソフトウェアの更新をインストールする前に、TSFによって実装されたデジタル署名メカニズムを使用して、それらの更新を検証しなければならない。
適用上の注意：	3番目のエレメントで参照されるデジタル署名メカニズムは、FCS_COP.1(2)で指定されているメカニズムである。
保証アクティビティ：	TSFの更新は、認証局によって署名される。更新検証メカニズムで使用される証明書をデバイスにどのように格納するかの記述と共に、認証局の定義がTSSに含まれる。評価者は、この情報がTSSに含まれていることを確認する。 また、評価者は、TSS（または操作ガイダンス）に、更新の候補の取得方法、更新のデジタル署名の検証に関連する処理、及び成功（署名が検証された）または失敗（署名を検証できなかった）の場合にとるアクションについて記述されていることを確認する。処理を実行するソフトウェア／ファームウェアの場所もTSSに記述されていなければならず、これらの場所を評価者が検証しなければならない。評価者は、以下のテストを実施しなければならない： • テスト1：評価者は、製品の現在のバージョンを確認するため、バージョン検証アクティビティを実施する。以下のテストで説明されている更新テストの後で、評価者は、このアクティビティを再度実施して、バージョンが更新のバージョンと正確に一致することを検証する。 • テスト2：評価者は、操作ガイダンスに記述された手順を使用して正規の更新を取得し、TOEに正しくイン

ストールされることを検証する。更新が想定どおりに機能することを実証するため、他の保証アクティビティのテストのサブセットを実施する。

- テスト3：評価者は、正規の更新を取得または生成し、TOEにインストールするよう試みる。評価者は、TOEが更新を拒否することを検証する。

拡張：TSFテスト（FPT_TST_EXT.1）

FPT_TST_EXT.1	**拡張：TSFテスト**
FPT_TST_EXT.1.1	TSFは、TSFの正しい動作を実証するため、初期スタートアップ（電源オン）時に一連のセルフテストを実施しなければならない。
保証アクティビティ：	NIST SP 800-90に従ってFCS_RBG_EXT.1を実装する場合、評価者は、NIST SP 800-90のSection 11.3と一致する正常性テストがTSSに記述されていることを検証しなければならない。 TSSに、FCS_COPのすべての機能について、既知の答えを使用したセルフテストを記述しなければならない。 評価者は、TSFの正しい動作に影響する、暗号化機能以外のいくつかの機能に関して、それらの機能をテストする方法がTSSに記述されていることを検証しなければならない。TSSには、これらの各機能に関して、機能／コンポーネントの正しい動作を検証する方法が記述される。評価者は、識別されたすべての機能／コンポーネントがスタートアップ時に適切にテストされることを確認しなければならない。

4.2 セキュリティ保証要件

3.1節のTOEのセキュリティ対策方針は、2.1節で特定された脅威に対処するために構成されている。4.1節のセキュリティ機能要件（SFR）は、セキュリティ対策方針を正式に具体化したものである。

4.1節の序論で示したように、この節にはCCからのSARの一式が含まれているが、評価者が実行する保証アクティビティについて、4.1節とこの節の両方に詳述する。

ファミリごとに、開発者がどのような追加書類／アクティビティを提供する必要があるのかを明確にするため、開発者アクションエレメントに「開発者向け注意事項」を提供している。その内容／プレゼンテーションエレメント及び開発者アクティビティエレメントに関して、（4.1節に既に含まれている保証アクティビティに対する）追加の保証アクティビティは、エレメントごとではなくファミリとしてまとめて記述されている。さらに、この節に記述されている保証アクティビティは、4.1節に記述されているものを補完している。

表 7に要約しているTOEセキュリティ保証要件は、本PPの第3章で特定された脅威と方針に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するものである。4.2節に、この節のセキュリティ保証要件を選択するための正当化を簡潔に示す。

表 7：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	準備手続き
テスト	ATE_IND.1	独立テスト－適合
脆弱性評定	AVA_VAN.1	脆弱性分析
ライフサイクルサポート	ALC_CMC.1	TOEのラベル付け
	ALC_CMS.1	TOEのCM範囲

4.2.1 ADV クラス：開発

本PPに適合するTOEでは、TOEの情報は、エンドユーザが入手可能なガイダンス文書及びSTのTOE要約仕様（TSS）の部分に含まれる。TOE開発者は、TSSを記述する必要はないが、機能要件に関してTSSに含まれる製品の記述に同意しなければならない。4.1節に含まれている保証アクティビティは、TSS節の適切な内容を決定するために十分な情報をST作成者に提供しなければならない。

4.2.1.1 ADV_FSP.1 基本機能仕様

この機能仕様はTSFIを記述している。本PPで提供される保証レベルでは、これらのインタフェースの正式または完全な仕様を設定する必要はない。さらに、本PPに適合するTOEは、TOE利用者によって直接呼び出されない運用環境のインタフェースを必然的に備えており、この保証レベルでは、そのようなインタフェースの間接的なテストのみが可能であるため、インタフェースを特定して記述するのは、それ自体としてあまり意味がない。本PPのこのファミリのアクティビティでは、機能要件に応えてTSSに示されるインタフェース及びAGD文書に示されるインタフェースを理解することに焦点を当てるべきである。特定された保証アクティビティを満たすために、追加の「機能仕様」文書は必要とならない。

TOEのインタフェースを理解する際、対抗するべき脅威とは、攻撃者が、電源がオフにな

っているハードディスクを発見してディスク上のデータを入手しようとすることであると見なすことが重要である。このことは、TOEが機能している（つまり、認証要素が正しく入力されて、TOEがシステムとディスク間で転送されるデータを暗号化及び復号している）ときには、攻撃者はシステムにアクセスできないことを意味するため、最も信頼できない利用者インタフェースは、システムのブート時に利用者に表示されるインタフェースである。
これらの「利用者インタフェース」に加えて、管理者インタフェース（TOEがどのように設定されているのか）も記述する必要がある。

場合によっては、ハードディスク上のインタフェース（例えば、ハードドライブを取り外して別のコンピュータに二次デバイスとして装着する）など、直接呼び出すことができるインタフェースがあるかもしれないが、そのような場合に、開発者がこのタイプのインタフェース仕様を提供したり、評価者が完全なUSBまたはSCSインタフェース実装を検査する（例えば、エラーを探す）必要はない。評価する必要が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、記載された保証アクティビティを実施するために必要となる情報を通じて特徴付けられる。

開発者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ければならない。

ADV_FSP.1.2D　開発者は機能仕様からSFRまでの追跡を提供しなければならない。

開発者向け注意事項：　この節の序論で示した通り、機能仕様は、AGD_OPRとAGD_PRE文書に含まれた情報に加えてSTのTSSで提供される情報から成る。機能要件における保証アクティビティは、関連文書とTSS節に存在するべき証拠を指すものである。保証アクティビティはSFRと直接関連するため、エレメントADV_FSP.1.2Dの追跡は既に暗黙的になされており、追加の文書は必要ない。

内容とプレゼンテーションエレメント：

ADV_FSP.1.1C　機能仕様は、SFR適用及びSFRサポートの各TSFIの目的と使用方法を記述しなければならない。

ADV_FSP.1.2C　機能仕様は、SFR適用及びSFRサポートの各TSFIに関連するすべてのパラメタを識別しなければならない。

ADV_FSP.1.3C　機能仕様は、SFR非干渉としての暗黙的なインタフェースの分類について、根拠を提供しなければならない。

ADV_FSP.1.4C　追跡は、機能仕様においてTSFIに対するSFRの追跡を実証しなければならない。

評価アクションエレメント：

ADV_ FSP.1.1E　評価者は、証拠の内容とプレゼンテーションに関して、提供された情報がすべての要件を満たすことを*確認しなければならない*。

ADV_ FSP.1.2E　評価者は、機能仕様が正確で完全なSFRの具体化であることを確認しなければならない。

保証アクティビティ：　このコンポーネントに関連する特定の保証アクティビティはない。評価アクティビティを支援するために提供されるインタフェース文書は4.1節に記述されており、AGD、ATE、及びAVAのSARに関して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（ハードディスクをホストする製品）がセキュリティ機能において役割を果たすことができることを、管理者がどのように検証するのかについての記述が含まれなければならない。文書は、格式張った様式でなく、管理者が読みやすいものであるべきである。

ガイダンスは、STで主張されている通り、製品がサポートするすべての運用環境について提供されなければならない。
このガイダンスは、以下を含む。

- その環境において、TOEを正しくインストールするための指示、及び
- 製品として及び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

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。このようなガイダンスの要件は、4.1節で特定される保証アクティビティに含まれている。

既に述べた領域に加えて、ガイダンスでは、どの省電力モード、休止モード、及びスリープモードがOE.POWER_SAVEに適合するのかを特定し、無効にするようには適合しないモードを無効にする方法について指示を提供する。

4.2.2.1　AGD_OPE.1 利用者操作ガイダンス

開発者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ければならない。
開発者向け注意事項：　開発者は、このコンポーネントの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ガイダンスの詳細を確定するべきである。これによって、許容可能なガイダンスの準備に必要な情報が提供される。

内容とプレゼンテーションエレメント：

AGD_OPE.1.1C　利用者操作ガイダンスは、適切な警告を含め、セキュアな処理環境で管理するべき、利用者がアクセス可能な機能と権限について、利用者の役割ごとに記述しなければならない。

AGD_OPE.1.2C　利用者操作ガイダンスは、TOEにより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どのように使用するのかについて、利用者の役割ごとに記述しなければならない。

AGD_OPE.1.3C　利用者操作ガイダンスは、利用可能な機能とインタフェース、

特に利用者の管理下にあるすべてのセキュリティパラメタについて、必要に応じてセキュアな値を示し、利用者の役割ごとに記述しなければならない。

AGD_OPE.1.4C　利用者操作ガイダンスは、TSFの制御下にあるエンティティのセキュリティ特性の変更を含む、利用者がアクセス可能で実行が必要な機能に関連する各タイプのセキュリティ関連イベントについて、利用者の役割ごとに明確に提示しなければならない。

AGD_OPE.1.5C　利用者操作ガイダンスは、TOEの操作のすべての可能なモード（障害や操作誤りの後の操作を含む）、それらの結果、及びセキュアな運用を維持するために必要なことを識別しなければならない。

AGD_OPE.1.6C　利用者操作ガイダンスは、STに記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を、利用者の役割ごとに記述しなければならない。

AGD_OPE.1.7C　利用者操作ガイダンスは、明確で、合理的なものでなければならない。

評価アクションエレメント：

AGD_OPE.1.1E　評価者は、証拠の内容とプレゼンテーションに関して、提供された情報がすべての要件を満たすことを*確認しなければならない*。

保証アクティビティ：　操作時に、ガイダンスに記述されたアクティビティは、利用者（非管理者）が実行するアクティビティと、管理者が実行するアクティビティの、2つの大きなカテゴリに分類される。非管理者の利用者に必要な大部分の手順が、4.1節の保証アクティビティで参照されることに注意するべきである。ただし、利用者向けのガイダンスに2つの追加の警告を提供しなければならない。ガイダンスは、格納デバイスの電源がオンになっているときに、格納デバイスに利用者の物理的な制御を残したままにしてはならないことを、許可された利用者に対して警告しなければならない。さらに、ガイダンスは、複数の要素を相互に使用する場合は、デバイスにパスフレーズ認証要素及び／または外付けトークン認証要素を残したり保存してはならないことを、許可された利用者に対して示さなければならない。

管理機能に関して、複数の情報が4.1節に記述されているが、次のような追加情報が必要である。

文書に、TOEの更新が対象となるソース（多くの場合、TOEベンダ）から取得されたことを検証するプロセスを記述しなければならない。この検証プロセスは、許可された利用者によって開始されるが、デバイス上のTSFによって実行される。評価者は、このプロセスが次のステップを含むことを検証しなければならない：

1. 署名済みの更新を証明書の所有者から受け取ったこと

を確認するための、FCS_COP.1(2)メカニズムによって使用される証明書を入手するための指示。これは、最初に製品とともに提供しても、他の方法で入手して初期設定の一部としてドライブ上にインストールしてもよい。最初にドライブに提供しない場合は、入手した証明書をエンドユーザが信頼できることをどのように判断するのか、ガイダンスで指示を提供しなければならない。

2. 更新自体を入手するための指示。これには、更新にアクセスできるようにするための指示を含めるべきである（例えば、特定のディレクトリ内の配置）。
3. 更新プロセスを開始するための指示と、そのプロセスが成功したかどうかを見定めるための指示。

TOEが外付けトークン認証要素の使用をサポートする場合、評価者は、認証要素が含まれた外付けトークンデバイスに利用者がいかなるデータも保存しないことが、ガイダンスに記述されていることもチェックしなければならない。

4.2.2.2 AGD_PRE.1 準備手続き

開発者アクションエレメント：

AGD_PRE.1.1D 開発者は、準備手続きを含め、TOEを提供しなければならない。

開発者向け注意事項： 操作ガイダンスと同様に、開発者は準備手続きに関して必要となる内容を決定するために、保証アクティビティに目を向けるべきである。

内容とプレゼンテーションエレメント：

AGD_ PRE.1.1C 準備手続きには、開発者の配付手続きに従って配付されたTOEのセキュアな受入れに必要なすべてのステップを記述しなければならない。

AGD_ PRE.1.2C 準備手続きには、TOEのセキュアな設置、及びSTに記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述しなければならない。

評価アクションエレメント：

AGD_ PRE.1.1E 評価者は、証拠の内容とプレゼンテーションに関して、提供された情報がすべての要件を満たすことを*確認しなければならない*。

AGD_ PRE.1.2E 評価者は、TOEを操作のためにセキュアに準備できることを確実にするために、準備手続きを*適用しなければならない*。

保証アクティビティ： 上記の序論で示した通り、特にTOE機能要件をサポートするように運用環境を設定する場合に、文書に関して大きな期待があ

る。評価者は、TOE用に提供されるガイダンスがSTでTOEに主張されているすべてのプラットフォーム（つまり、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）に適切に対処していることを確認しなければならない。

評価者は、次のガイダンスが提供されることを確認しなければならない。

- システム（及び特にラップトップ）が通常、省電力、休止、スリープ／スタンバイ、自動シャットダウンなど、利用者の非アクティブな状態を対象とする多くのモードをサポートする。ガイダンスで2つの領域をカバーする必要がある。

  1番目の領域では、利用者が一定の時間非アクティブになった後でシステムの電源が完全にオフになるよう、プラットフォームを設定するために実行する必要があるステップに対処する。電源がオフになった時点で、鍵とする材料は消去され、ハードディスクは脅威モデルが想定する初期状態になる。電源オフのプロセスが開始される前に、利用者が非アクティブであるために、画面ロックなどの機能がアクティブになることは許可されるが、そのような機能は電源オフの代わりにはならず、この要件を満たさない。

  一部のモードでは、システムの電源は完全にはオフにならず、オペレーティングシステムは完全にはシャットダウンしない。代わりに、そのモードに入る前に中止した箇所から利用者が作業を開始できるよう、システム（揮発性メモリまたはディスク）にある程度の状態が保存される。適合TOEは、プラットフォームの電源が完全にはオフにならず、オペレーティングシステムが完全にはシャットダウンしないモードに入ることは許可されない。そのため、ガイダンスでカバーする必要がある2番目の領域では、鍵とする材料が暗号化されずに存在するような、システムのメインメモリに電源がまだなお適用される状態にシステムがなったままになるモードを無効にするために必要なステップを詳述する。この電源オフの状態に入ったら、KEKが再構成されてDEKが再度ラップ解除されるよう必要な認証要素をまず入力しないと、利用者がハードディスクにアクセスできない状況でなければならない。ガイダンスには、モードを再度有効にする機能をTOE管理者に制限するための指示も提供しなければならない。

- TOE認証要素を、TOEの基盤となる識別と認証のメカニズムの代わりに使用することはできない。評価者は、ガイダンスを検査して、プラットフォームの識別と認証のメカニズムの代わりまたはその一部として認証要素を使用する機能が存在する場合、この機能を無効にする方法について指示が提供され、この機能は適合TOEには使用されないという警告が管理者に提供されることを確認しなければならない。

- 製品のセットアップ時にすべてのハードドライブが暗号化されるよう、またこのような設定のみが適合TOE

の設定に許可されるよう、製品をどのように設定するのかを詳述した指示と情報が管理者に提供される。

- 序論の部分で示したように、TOEの管理は、TOEのすべての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及び運用環境）でこの機能を提供しなければならないが、機能の実装責任は、完全に運用環境の責任である場合から完全にTOEの責任である場合までさまざまである。責任を負う機能を提供するように運用環境を構成するよう、高レベルでガイダンスに適切な指示が含まれなければならない。もし管理利用者を一般の利用者から分離できるようにするメカニズムをTOEが提供しない場合は、指示によって、例えば、OSのI&Aメカニズムの OS設定をカバーし、利用者の一意（OSベース）の識別情報を提供する。また、更なるガイダンスで、TOE管理者だけが管理用の実行可能ファイルにアクセスできるよう、TOE管理識別情報（1つまたは複数）を使用したOSのDACメカニズムの設定についてインストーラに指示する。

  もしTOEがこの機能性の一部またはすべてを提供するなら、附属書Cの該当する要件をSTに含め、それらの要件に関連する保証アクティビティにより、TOEと運用環境の両方に必要なガイダンスについて詳細を提供する。

  評価者は、以下のテストも実施しなければならない。

  - テスト1 [条件付]：すべてのTOE利用者からの管理者である利用者の分離を運用環境の設定のみで実施する場合、評価者は、STで主張される設定ごとに、管理者ガイダンスに従ってシステムを設定した後で管理者でない利用者がTOE管理機能にアクセスできないことを確認する。

4.2.3 ATE クラス：テスト

テストは、システムの機能の観点とともに、設計上または実装上の弱点を利用する観点でも指定される。前者はATE_INDファミリを使用して行われ、後者はAVA_VANファミリを使用して行われる。本PPで特定される保証レベルでは、TSSに示される設計情報の利用可能性によって制限される通りに、テストは公開される機能性とインタフェースに基づく。評価プロセスの主な出力の1つは、以下の要件で特定されているテスト報告書である。

4.2.3.3 ATE_IND.1 独立テスト – 適合

テストは、TSSに記述された機能及び提供される管理（設定と操作を含む）文書を確認するために実施される。追加のテストが4.2節のSARに対して特定されているが、テストの焦点は、4.1節で特定された要件を満たしていることを確認することである。保証アクティビティでは、これらのコンポーネントに関連する最小限のテストアクティビティを識別する。評価者は、テスト計画とテスト結果を文書化したテスト報告書と、本PPへの適合を主張するプラットフォーム／TOEの組み合わせに焦点を当てた範囲の論証を作成する。

開発者アクションエレメント：

ATE_IND.1.1D　開発者は、テスト用のTOEを提供しなければならない。

内容とプレゼンテーションエレメント：

ATE_IND.1.1C　TOEはテストに適してなければならない。

評価アクションエレメント：

ATE_IND.1.1E　評価者は、証拠の内容とプレゼンテーションに関して、提供された情報がすべての要件を満たすことを*確認しなければならない*。

ATE_IND.1.2E　評価者は、TSFが特定された通りに機能することを確認するため、TSFのサブセットを*テストしなければならない*。

保証アクティビティ：　評価者は、システムのテスト面を文書化したテスト計画と報告書を準備しなければならない。テスト計画は、本PPの保証アクティビティの本文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に記載されているテストごとにテストケースは必要とはならないが、評価者は、STの該当する各テスト要件がカバーされていることをテスト計画に文書化しなければならない。

テスト計画では、テスト対象のプラットフォームを特定し、テスト計画には含まれないがSTには含まれるプラットフォームに関して、プラットフォームのテストを行わないことを正当化する。この正当化では、テスト対象のプラットフォームとテスト対象でないプラットフォームの違いに対処し、その違いが実施するテストに影響しないことを論証しなければならない。その違いによる影響がないと単に主張するのは不十分で、根拠が提供されなければならない。この正当化を記述する際、評価者は、特に省電力機能と休止機能を扱うOSベースのメカニズムとハードウェアベースのメカニズムを考慮しなければならない。もしSTで主張されているすべてのプラットフォームがテストされるのであれば、根拠は必要ない。

テスト計画には、テスト対象となる各プラットフォームの構成を記述し、AGD文書に含まれているもの以外で必要となるセットアップについても記述する。評価者は、各プラットフォームのインストールとセットアップについて、テストの一部または標準プレテスト条件として、AGD文書に従うことが求められることに注意するべきである。これは、特別なテストドライバーやツールを含むかもしれない。各ドライバーまたはツールに関して、ドライバーまたはツールがTOE及びプラットフォームが提供する機能性のパフォーマンスを低下させないという論証（単なる主張ではなく）を提供する。

テスト計画には、テスト目的の概要及びこの目的を達成するた

めに従うテスト手順を特定する。これらの手順は、特定の手順の目標、目標を達成するために使用するテストステップ、及び期待される結果を含む。テスト報告書（単なるテスト計画の注釈付きのバージョンかもしれないが）は、テスト手順が実行された際に行われたアクティビティを詳述し、テストの実際の結果を含む。これは、累積的な報告でなければならない。もしテストが不合格に終わったら、調整され、テストを適切に再実施し、報告書には、単なる「合格」の結果だけでなく、「不合格」と「合格」の結果（及び論点を補強する例証）を示す。

テストアクティビティを実施する際、評価者は、TSSのすべての情報を考慮して、テストケースがさまざまな操作シナリオをカバーすることを確認する。例えば、DEKを再生成する場合、評価者は、TSS及びAGD_PREまたはAGD_OPRガイダンスを検査して、ディスク上のすべての情報が暗号化されたままになっており（FDP_DSK_EXT.1）、鍵とする材料が利用できる状態で残っていない（FCS_CKM_EXT.4）ことを確認するべきである。

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初版のために、評価機関は、これらのタイプの製品で検出された脆弱性を検出するため、オープンソースを調査することが求められる。ほとんどの場合、これらの脆弱性は、基本的な攻撃者の巧妙さを超えた巧妙さを必要とする。侵入ツールが作成されて評価機関に配付されるまで、評価者はTOEのそれらの脆弱性をテストすることは求められない。評価機関は、ベンダから提供された文書に記載されているこれらの脆弱性の可能性についてコメントすることが求められる。この情報は、侵入テストツールの開発や将来のプロテクションプロファイルの開発のために使用される。

4.2.4.1 AVA_VAN.1 脆弱性調査

開発者アクションエレメント：

AVA_VAN.1.1D 開発者は、テスト用のTOEを提供しなければならない。

内容とプレゼンテーションエレメント：

AVA_VAN.1.1C TOEはテストに適してなければならない。

評価アクションエレメント：

AVA_VAN.1.1E 評価者は、証拠の内容とプレゼンテーションに関して、提供された情報がすべての要件を満たすことを*確認しなければならない*。

AVA_VAN.1.2E 評価者は、TOEの潜在的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*実施しなければならない*。

AVA_VAN.1.3E 評価者は、TOEが基本的な攻撃の可能性を持つ攻撃者による攻撃に対して耐性があることを確認するため、特定された潜在的脆弱性に基づいてテストを*実施しなければならない*。

保証アクティビティ：　ATE_INDと同様に、評価者はこの要件に関して、報告書を作成して到達した結論を文書化しなければならない。この報告書は、物理的に、ATE_INDに述べている全体的なテスト報告書に含めても、別文書でもよい。評価者は、公知の情報を検索して、一般的なディスク暗号化製品で見つかった脆弱性及び特定のTOEに関連する脆弱性を判断しなければならない。評価者は、参照した情報源及び見つかった脆弱性を報告書に文書化する。見つかった各脆弱性について、評価者は脆弱性を確認するために、適切であれば、不適合性に関連する根拠を提供するか、（ATE_INDで提供されるガイドラインを使用して）テストを策定する。適合性は、脆弱性を利用するために必要とされる攻撃ベクトルを評価することにより決まる。例えば、もし脆弱性がブートアップ時に鍵の組み合わせを押すことによって検知できれば、テストは本PPの保証レベルに適しているだろう。もし、脆弱性の悪用に、例えば、電子顕微鏡や液体窒素が必要となるならば、テストは適しておらず、適切な正当化を策定することになるだろう。

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よりも、エンドユーザに見えるライフサイクルの側面に限定される。これは、製品の全体的な信頼に貢献するために開発者が果たす重要な役割を軽減するということではなく、むしろ、この保証レベルでの評価に利用できるようにする情報を反映したものである。

4.2.5.1　ALC_CMC.1　TOE のラベル付け

このコンポーネントは、同じベンダの他の製品やバージョンと区別することができたり、エンドユーザが購入する際に容易に指定することができるといった、TOEの識別を目的としている。

開発者アクションエレメント：

ALC_CMC.1.1D　開発者は、TOE及びTOEの参照情報を提供しなければならない。

内容とプレゼンテーションエレメント：

ALC_CMC.1.1C　TOEは、その一意の参照情報でラベル付けされなければならない。

評価アクションエレメント：

ALC_CMC.1.1E　評価者は、証拠の内容とプレゼンテーションに関して、提供された情報がすべての要件を満たすことを*確認しなければならない*。

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明確に特定する識別子（製品名、バージョン番号など）がSTに含まれていることを確認しなければならない。さらに、評価者は、AGDガイダンス及びテスト用に受け取ったTOEサンプルをチェックして、バージョン番号がSTに含まれているバージョン番号と一致することを確認しなければならない。もしベンダがTOEを公表するWebサイトを保持しているなら、評価者は、そ

のWebサイトの情報を検査して、STの情報が製品を区別するのに十分であることを確認しなければならない。

4.2.5.2 ALC_CMS.1 TOE の CM 範囲

TOEの範囲及び関連する評価証拠要件を考慮すると、このコンポーネントの保証アクティビティは、ALC_CMC.1に記載されている保証アクティビティでカバーされる。

開発者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ければならない。

内容とプレゼンテーションエレメント：

ALC_CMS.2.1C 構成リストは、TOE自体、及びSARが要求する評価証拠を含まなければならない。

ALC_CMS.2.2C 構成リストは、構成要素を一意に識別しなければならない。

評価アクションエレメント：

ALC_CMS.2.1E 評価者は、証拠の内容とプレゼンテーションに関して、提供された情報がすべての要件を満たすことを*確認しなければならない*。

保証アクティビティ： 本PPの「セキュリティ保証要件が要求する評価証拠」とは、STの情報及びAGD要件の元で管理者と利用者に提供されるガイダンスに限定される。TOEが明確に識別されること、及びこの識別がST及びAGDガイダンスと一致していることを確認する（ALC_CMC.1の保証アクティビティで実施しているように）ことによって、評価者はこのコンポーネントで必要となる情報を暗黙的に確認する。

5　適合主張

適合主張はPPまたは評価に合格しようとするセキュリティターゲット（ST）が適合するべき要件の情報源を示す。適用上の注意は、満たすべき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）の節で提供される。

5.1　PP 適合主張

本PPは、CC 3.1のCCパート2拡張及びCCパート3適合に適合する。

本PPへの適合を主張するSTは、CCパート1（CCMB-2006-09-001）の付属書D3で定義された正確PP適合の最低基準を満たさなければならない。

正確PP適合とは、PPの要件が満たされており、STはPPを具体化したものであることを意味する。STはPPよりも広範囲であってもよく、その場合、評価を監督する国家制度が追加部分を承認することとなる。STでは、運用環境では最大でPPと同じことを行うが、TOEでは最小でもPPと同じことを行うことを特定する。本PPでは、保証アクティビティは、特定された要件の目的をさらに明確にし、ベンダが要件を満たす方法についての期待を説明するために提供されている。ST及び記述されたTOEが本PPのすべての記述（場合によっては、それ以上）を含むだけでなく、保証アクティビティで示された期待を満たすことも確認することにより、STの評価者が正確PP適合を確認することが求められる。

5.2　PP 適合主張の根拠

本PPは、別のPPへの適合は主張しない。

6 根拠

この章では、このセキュリティターゲットで定義されているセキュリティ対策方針とセキュリティ機能要件の根拠、及び保証要件の根拠について説明する。

6.1 セキュリティ機能要件の根拠

この節では、4.1節で定義されているTOEセキュリティ機能要件の根拠について説明する。TOEで実装される要件が脅威を低減または方針を実施する度合いを明確に示すために、以下で要件から、対策方針、該当する脅威／方針までを明確にする。表 8に、セキュリティ機能要件、セキュリティ対策方針、及び脅威／方針のマッピング、及び要件が脅威を軽減または方針にどのように対処するのか根拠を示す。

表 8：脅威／方針／対策方針／SFR のマッピング／根拠

脅威／方針	対策方針	根拠
T.KEYING_MATERIAL_ COMPROMISE 攻撃者は、TOEが永続記憶域に書き込んだ暗号化されていない鍵とする材料（KEK、DEK、認証要素、サブマスク、及び鍵を導き出す乱数または他の値）を入手し、これらの値を使用して利用者データにアクセスすることが可能。	O.DEK_SECURITY TOEは、（認証要素から導出した） 1つ以上のサブマスクから作成した鍵の暗号化鍵（KEK）を使用してDEKをマスキングするので、認証要素を持たない脅威エージェントがDEKを入手して利用者データにアクセスすることができない。 （FCS_CKM.1(2)、FCS_CKM.1(3)、FCS_COP.1(4)、FCS_RBG_EXT.1） O.EXTERNAL_AUTH_FACTOR_ PROTECTION TOEは、認証用に使用した後は、外付けトークン認証要素にアクセスできないことを確実にしなければならない。 （FIA_AUT_EXT.1） O.KEY_MATERIAL_COMPRO M ISE TOEは、KEKまたはDEKを見つけるために鍵とする材料が利用される可能性を低減すため、必要がなくなり次第、すぐにこの材料をゼロ化する。 （FCS_CKM_EXT.4） O.MANAGE TOEは、TOEのセキュリティの管理において権限を	FCS_CKM.1(3)は、パスフレーズ認証要素を使用する場合、適切なKEKが導出されることを確実にするため、パスフレーズ認証に十分に条件付けするという要件を課す。 FCS_CKM.1(2)は、KEKをどのように導出するのかを特定し、KEKの鍵長を特定する要件である。この要件は、パスフレーズ以外の認証要素を許可するが、各認証要素の効果的な強度を維持することを義務付けている。つまり、別の認証要素を導入しても、条件付けしたパスフレーズの強度は低下しないということである。 FCS_COP.1 (4)は、DEKをマスキングするための暗号操作の安全な実装を確実にする。 FCS_RBG_EXT.1は、鍵とする材料が堅牢に生成されることを確実にする。この要件は、パスフレーズ認証要素を使用している場合、またはTOEが外付けトークン認証要素を生成している場合に、この対策方針を満たすためにのみ機能する。 FCS_CKM_EXT.4は、必要がなくなったら鍵とする材料を利用できなくすることを確実にすることにより、この対策方針を満たすために機能する。これにより、見つかった鍵とする材料を試してそこからKEKを導出することができるような攻撃を低減する。 FIA_AUT_EXT.1は、外付けトークン上の認証要素に対処する。これらの認証要素は、一度使用されたら消去し

	持つ管理者を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許可されない利用を禁止する。 （FMT_SMF.1）	てはならない点で、他の鍵とする材料とは異なる。ただし、これらの認証要素を引き続き保護し、使用後は「取り外す」必要があるため、FIA_AUT_EXT.1では、ホストシステムで認証要素が使用された後で、ホストシステムから外付けトークンにアクセスできなくすることが必要となる。 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実にする。これらの機能には、DEKの生成、保護、及び削除、認証要素の生成と設定、及び暗号化機能の設定が含まれる。ST作成者は、他の管理機能を組み込むことを選択してもよい。
T.INCOMPLETE_SHUTDOWN 運用環境が省電力モードになって、データまたは鍵とする材料が永続記憶域に暗号化されていない状態で保持される可能性がある。	O.KEY_MATERIAL_COMPROM ISE TOEは、KEKまたはDEKを見つけるために鍵とする材料が利用される可能性を低減すため、必要がなくなり次第、すぐにこの材料をゼロ化する。 （FCS_CKM_EXT.4） OE.POWER_SAVE 利用者の選択によってシステムをシャットダウンするのと同じ方法で一定時間後にシステムの電源をオフにする、1つ以上のメカニズムが存在するように、運用環境を構成しなければならない（O.SHUTDOWN）。この要件に適合しないメカニズム（例えば、スリープ、休止）は、管理者が無効にできなければならない。 OE.TRAINED_USERS 許可された利用者は、適切なトレーニングを受けて、TOE及び認証要素を保護するためのすべてのガイダンスに従う。	FCS_CKM_EXT.4では、必要がなくなった場合またはシャットダウン時に、すべての鍵とする材料がゼロ化されることが必要となる。これは、鍵とする材料が暗号モジュールの内部または外部（例えば、メモリ内）のいずれに存在するかに関係なく適用される。ほぼ確実に、TSFで必要がなくなると、ほとんどの鍵とする材料はゼロ化されるが、それでも鍵とする材料が存在する場合は、マシンのシャットダウン（手動で、または非アクティブであるために自動で）時に鍵とする材料がゼロ化される。 OE.POWER_SAVEは、TOEの保護機能を呼び出すことができるよう設定することが可能なプラットフォームを提供することにより、脅威を低減する。 同様に、OE.TRAINED_USERSは、利用者が鍵のゼロ化機能が呼び出される方法で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 許可されていない利用者が総当り攻撃を試みて、暗号化鍵または認証要素を判断し、データまたはTOE資源に不正アクセスを行うことが可能。	O.DEK_SECURITY TOEは、認証要素を所有しない脅威エージェントがDEKを入手して利用者データにアクセスすることができないように、1つ以上のサブマスク（認証要素から導出した）から作成した鍵の暗号化鍵（KEK）を使用してDEKをマスキングする。 （FCS_CKM.1(2)、FCS_CKM.1(3)、FCS_RBG_EXT.1、FCS_COP.1(4)、FCS_COP.1(3)、FMT_MTD.1）	FCS_CKM.1(2)及びFCS_CKM.1(3)は、KEK／認証要素の推測を困難にするようランダム化（FCS_RBG_EXT.1、FCS_COP.1(3))することを確実にし、これらの値のいずれかを推測するのがDEKを推測するのと同じように困難になるように適切な長さにするのを確実にするよう、KEK及び認証要素条件付けにそれぞれ要件を課す。DEKは、DEKの長さに相当する強度を提供する手法（FCS_COP.1(4))を使用してラップされるため、この方法が総当り以上の攻撃を提供しないことを確実にする。誰も鍵を読み出しできないようにすることにより、鍵を推測するために必要な作業要素を減らすような情報を攻撃者が入手する可能性を低減することもできる。
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コードに不適切にアクセス（表示、変更、または削除）することが可能。	O.CORRECT_TSF_OPERATION TOEは、運用環境におけるTSFの正しい動作を保証するため、TSFをテストするための機能を提供する。（FPT_TST_EXT.1） O.TRUSTED_UPDAE TOEは、TOEのファームウェア／ソフトウェアを更新して、製品の更新を対象となるソースから入手したことを検証する機能を管理者に提供しなければならない。 （FCS_COP.1(2)、FCS_COP.1(3)、FPT_TUD_EXT.1）	FPT_TST_EXT.1では、TOEを操作に組み込む前に、TOEで(暗号モジュール及びその他のコンポーネントの両方に関して）セルフテストを実施することが必要となる。 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しないが、TSFの基盤となるメカニズムが正しく動作することを確実にすることにより、TSFの侵害に対してある程度の保護を提供する。 暗号の使用が検証された更新（FCS_COP.1(2)、FCS_COP.1(3)、FPT_TUD_EXT.1）で、暗号を使用した強力なメカニズムによって更新が署名され、インストール前に管理者が暗号を検証することを確実にすることにより、悪意のある攻撃者が更新プロセスで破損したTOEを置き換えることを試みる可能性を低減する。
T.UNAUTHORIZED_DISK_ACCESS 紛失したハードディスクにアクセスできる許可されていない利用者が、TOEセキュリティ方針では許可されないデータにアクセスすることが可能。	O.ENCRYPT_ALL TOEは、ハードドライブに保存されているすべてのデータを暗号化する（MBR及びMBRが指すブート可能なパーティションは除外してもよいことに注意すること）。 （FDP_DSK_EXT.1 FCS_CKM.1(1) FCS_COP.1(1)）	FDP_DSK_EXT.1は、TOEがすべての利用者データを含め、フルディスク暗号化を実行することを確実にする。「フルディスク暗号化」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ディスク上にあるすべてのデータを暗号化し、FDE製品への認証が成功した後にのみデータへのアクセスを許可するプロセス」と定義されており、認証要素を受け入れて処理するために必要なコードが含まれるMBR及び関連するブート可能なパーティション

	O.AUTHORIZATION TOEは、ハードディスク上のデータを復号できるよう、利用者の認証要素を含まなければならない。（FIA_AUT_EXT.1 FCS_CKM.1(2) FCS_COP.1(4)） O.DEK_SECURITY TOEは、認証要素を所有しない脅威エージェントがDEKを入手して利用者データにアクセスすることができないように、1つ以上のサブマスク（認証要素から取得した）から作成した鍵の暗号化鍵（KEK）を使用してDEKをマスキングする。 （FCS_CKM.1(2)、 FCS_CKM.1(3)、 FCS_COP.1(4)、 FCS_RBG_EXT.1、 FMT_MTD.1) O.EXTERNAL_AUTH_FACTOR_ PROTECTION TOEは、認証用に使用した後は、外付けトークン認証要素にアクセスできないことを確実にしなければならない。（FIA_AUT_EXT.1） O.KEY_MATERIAL_COMPROM ISE TOEは、KEKまたはDEKを見つけるために鍵とする材料が利用される可能性を低減すため、必要がなくなり次第、すぐにこの材料をゼロ化する。（FCS_CKM_EXT 4） O.OWNERSHIP TOEは、TOEの操作時に利用者データにアクセスできるようになる前に、所有権が得られている（つまり、DEKが作成され、認証要素が確立され、デフォルトの認証要素が変更され、KEKが取得されたサ	は除外される。これにより、デバイスを紛失した場合でも、データが公開されないことを確実にする。 すべてのデータを暗号化するという要件に加えて、FCS_CKM.1(1)及びFCS_COP.1(1)は、暗号化を実行するために使用する鍵の品質、及びディスク暗号化操作に使用するアルゴリズムと鍵長も特定する。これにより、保護が容易に破られないようにし、データの保護を確実にする。 FIA_AUT_EXT.1では、利用者にハードドライブの暗号化されていないデータへのアクセスを許可する前に、FCS_CKM.1(2)及びFCS_COP.1(4)で特定されるメカニズムによって利用者が許可されることが必要となる。これにより、許可されていない利用者が、データにアクセスするために、暗号化メカニズムを呼び出すことができないことを確実にする。 鍵または認証要素が侵害された場合、ディスク上のデータを容易に回復することができる。FMT_MTD.1、FCS_CKM.1(2)、FCS_CKM.1(3)、FCS_COP.1(4)、FCS_RBG_EXT.1、及びFCS_CKM_EXT.4はすべて、鍵または認証要素を取得するのがDEKを推測するのと同じように暗号処理が困難であることを確実にする。 同様に、FIA_AUT_EXT.1は外付けトークン上の認証要素に対処する。これらの認証要素は、一度使用されたら消去してはならない点で、他の鍵とする材料とは異なる。ただし、これらの認証要素を引き続き保護し、使用後は「取り外す」必要があるため、FIA_AUT_EXT.1では、ホストシステムで認証要素が使用された後で、ホストシステムから外付けトークンにアクセスできなくし、外付けトークンがデータの不正アクセスに使用できないことを確実にすることが必要となる。 FMT_SMF.1は、TOEが一度操作に組み込まれたら、暗号化をディスクドライブに確立する方法がないことを確実にすることにより、脅威に対処する。さらに、デフォルトの認証要素が存在する場合、利用者が認証要素を変更してデータの自明な侵害を

	ブマスクから形成され、DEKがKEKと関連付けられている）ことを確実にしなければならない。（FMT_SMF.1）	防止することができる、メカニズムと適切なガイダンスが存在する。
T. UNAUTHORIZED_UPDATE 悪意のある部外者がTOEのセキュリティ機能を侵害する可能性がある製品の更新をエンドユーザに提供するよう試みる。	O.TRUSTED_UPDATE TOEは、TOEのファームウェア／ソフトウェアを更新して、製品の更新を対象となるソースから入手したことを検証する機能を管理者に提供しなければならない。（FCS_COP.1(2)、FCS_COP.1(3)、FPT_TUD_EXT.1）	更新は、AGD要件及びFPT_TUD_EXT.1で特定されているように検証される。この検証では、FCS_COP.1(3)で特定されているハッシュメカニズム及びFCS_COP.1(2)で特定されているデジタル署名メカニズムを使用する必要がある。これらの暗号メカニズムを使用して更新を検証することにより、更新が対象となるソースから入手されることを確実にする。
T.UNSAFE_AUTHFACTOR_VERIFICATION 利用者が入力した認証要素の検証を実施するために攻撃者が安全でない方法を利用し、その結果、KEK、DEK、または利用者データを入手することが可能。	O. SAFE_AUTHFACTOR_VERIFICATION TOEは、KEK、DEK、または利用者データが意図せず公開されない方法で、認証要素の検証を実施しなければならない。（FIA_AUT_EXT.1）	FIA_AUT_EXT.1では、利用者がUSBフラッシュドライブ上のデータにアクセスできるようになる前に、TSFが認証要素を検証することが必要となる。また、攻撃者にDEKまたはKEKを推測できるような機会を提供しない方法でこれを実行することも必要となる。

6.2 セキュリティ保証要件の根拠

特定の保証要件が、フルディスク暗号化デバイスの優れた商習慣と一致する、達成可能なレベルの保証を提供するために選択されている。そのため、ベンダが合理的なソフトウェアエンジニアリング実践に従い、必要となる支援ガイダンス文書を提供できることを前提として、最小限の追加タスクがベンダに課せられる。選択した保証レベルは、第2章で定義されているセキュリティ課題の定義と脅威に見合ったものである。この文書は、絶え間なく変化する脅威環境及び開発ベストプラクティスの進歩と共に進化し、必要に応じて新しい要件や保証アクティビティを含めることを意図している。これらの進歩は、実際の評価結果及びベンダのコンソーシアムによって推進されるであろう。

附属書 A：サポート表と参照情報

[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] NSA Glossary of Terms Used in Security and Intrusion Detection, Greg Stocksdale, NSA Information Systems Security Organization, April 1998. Need to update to CNSS 4009

[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（高度暗号規格）
AF	Authorization Factor（認証要素）
CAVS	Cryptographic Algorithm Validation System（暗号アルゴリズム検証システム）
CC	Common Criteria（コモンクライテリア）
CM	Configuration Management（構成管理）
COTS	Commercial Off-The-Shelf（民生品）
DEK	Data Encryption Key（データ暗号化鍵）
DRBG	Deterministic Random Bit Generator（決定論的ランダムビット生成器）
DoD	Department of Defense（米国国防総省）
EAL	Evaluation Assurance Level（評価保証レベル）
FDE	Full Disk Encryption（フルディスク暗号化）
FIPS	Federal Information Processing Standards（連邦情報処理規格）
ISSE	Information System Security Engineer（情報システムセキュリティエンジニア
IT	Information Technology（情報技術）
KEK	Key Encryption Key（鍵の暗号化鍵）
MBR	Master Boot Record（マスタブートレコード）
OSP	Organization Security Policy（組織のセキュリティ方針）
PP	Protection Profile（プロテクションプロファイル）
PUB	Publication（出版）
RGB	Random Bit Generator（ランダムビット生成器）
SAR	Security Assurance Requirements（セキュリティ保証要件）
SF	Security Function（セキュリティ機能）
SFR	Security Functional Requirement（セキュリティ機能要件）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）
TSFI	Target Security Functionality Interface （ターゲットセキュリティ機能インタフェース）
TSS	TOE Summary Specification（TOE要約仕様）
TOE	Target of Evaluation（評価対象）

附属書 B：NIST SP 800-53／CNSS 1253 のマッピング

NIST SP 800-53／CNSS 1253の管理策のいくつかは、適合TOEで全体的または部分的に対処するものである。 本節では対処する要件を概説しており、TOEを運用構成に組み込む場合にどのような追加のテスト（存在する場合）が必要となるのかを認証員が判断するために使用できる。

適用上の注意：このバージョンでは、簡単なマッピングのみを提供する。将来のバージョンでは、情報が追加されて認証チームに更なる情報が提供されるだろう。この追加の情報は、TOEによって提供される適合の度合い（例えば、完全に管理策を満たす、部分的に管理策を満たす）を記述したマッピングを管理するためのSFRについての詳細を含むだろう。さらに、特定された保証アクティビティの総合的なレビュー、及びSARへの適合の一環として発生するそれらの評価アクティビティが要約されて、適合がどのように決定されたか（例えば、文書のレビュー、ベンダのアサーション、テスト／検証の度合い）に関する情報が認証チームに提供されるだろう。この情報は、認証チームに対して、指定された管理策への適合の度合いを判断するために実施する必要がある追加のアクティビティ（ある場合）にはどのようなものがあるのかを示すだろう。

STでは選択を行って割付を埋めるため、STを完成して評価するまでは最終的な筋書きを完成できるとは限らない。したがって、この情報はPPだけでなくSTにも含めるべきである。また、特定の実装に基づいて評価者が実施したアクティビティについて、ある程度の解釈（例えば、「修正」）が必要になるかもしれない。制度では、監督担当者（例えば、認証員）がこの種の情報を提供したり、または評価者が保証アクティビティの一部として実施する場合もあるだろう。検証アクティビティは、評価チームの作業以外に実行する必要がある活動（ある場合）を認証チームが決定できるよう、提供されなければならない重要な情報である。

ID	名称	適用可能なセキュリティ機能要件
CM-5	Access Restrictions for Change （変更のためのアクセス制限）	FPT_TUD_EXT.1
IA-5	Authenticator Management （認証コードの管理）	FCS_CKM.1.1(3)、FIA_AUT_EXT.1、FMT_SMF.1
IA-7	Cryptographic Module Authentication （暗号モジュールの認証）	FIA_AUT_EXT.1
MP-4	Media Storage （記憶媒体の保管）	FDP_DSK_EXT.1
SC-12	Cryptographic Key Establishment and Management （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	Use of Cryptography （暗号化の利用）	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	Protection of Information at Rest （残存情報の保護）	FDP_DSK_EXT.1
SI-6	Security Functionality Verification （セキュリティ機能の検証）	FPT_TST_EXT.1

附属書 C：追加の要件

本PPの概要で示した通り、TOEで実装でき、本PPに適合するいくつかの機能がある。これらの機能は必須ではなく、運用環境への依存（例えば、TOEの管理者の識別と認証）を引き起こすものである。ただし、TOEでこのような機能を実装する場合は、ST作成者はこの附属書から該当する情報を取得してSTに含めることとなる。ST作成者は、附属書Cの要件と関連する可能性があるが記載されていない要件（例えば、FMTのような要件）もSTに含めなければならない。この附属書に含まれていない要件については、本PPへの適合主張を行う前に、評価を監督する国家制度によるレビューと承認を受けることとなる。

C.1　TOE の識別と認証

PPの本文では、TOEは識別と認証（I&A）を実行することが必要とされていない。TOEが認証要素を受け入れて処理できる必要があるが、「従来の」I&Aとしては処理されない。TOEは管理機能を提供する必要があるが、TOEが運用環境を使用してTOE管理機能へのアクセスを制御することは許容可能であり、このことは現在PPで特定されている。

ただし、TOEがある程度のI&A機能を提供する場合は、ST作成者が以下の情報を使用してその機能を特定するべきである。TOEで提供される機能を記述した情報を以下から取得し、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）、及び800-53／CISSP 1253の情報がSTに含まれることを確実にする。

TOEが「管理者」の概念を保持し、この保持された識別情報に基づき管理機能へのアクセスを強制的に適用するが、この識別情報を確立する独自のメカニズムを提供しない場合（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から渡される情報を利用する）、以下の要件のサブセットを含める必要がある。この場合、ST作成者は、以下の情報の該当するサブセットを含め、PPの本文を適切に調整しなければならない。これらは、本PPに適合するSTとなっていることを判断するため、評価を監督する国家制度によってレビューされることとなる。

TOEに対してI&Aを実行する利用者や、利用者が実行可能な管理機能（例えば、管理者がパスフレーズベースの認証要素用のパスフレーズを作成することに制限されている、暗号化を有効にしたり無効にしたりすることもできる）に関して、TOEが詳細を提供する必要はない。このような機能を実装し、ベンダがSTでその機能を主張することを希望する場合は、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を作成して、PPの維持管理組織に提案する必要がある。

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	正式な組織方針の参考文献
P.I_AND_A	公共のオブジェクトを除く管理対象のリソースにアクセスする前に、すべての利用者を識別及び認証しなければならない。	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、TOE管理機能へのアクセスを許可する前に、権限を持つ管理者を識別及び認証する。

O.IDAUTHの追加に加えて、ST作成者は、環境に関する対策方針OE.RESTRICTED_FUNCTIONSをTOE:O.RESTRICTED_FUNCTIONSの対策方針に変更して、STの本文の該当する表に記載しなければならない。

表 C.1-3：セキュリティ対策方針と脅威、方針のマッピングへの追加

脅威／方針	脅威と方針に対処する対策方針	根拠
P.I_AND_A 公共のオブジェクトを除く管理対象のリソースにアクセスする前に、すべての利用者を識別及び認証しなければならない。	O.IDAUTH TOEは、TOE管理機能へのアクセスを許可する前に、権限を持つ管理者を識別及び認証する。	A.PLATFORM_I&Aでは、利用者が必要な認証要素を正しく入力した後で、基盤となるOSが識別と認証を実行することが必要となる。ただし、認証要素を持つ利用者のサブセットのみが、TOE管理機能を実行することを許可される。 O.IDAUTHは、管理機能を呼び出す前に権限を持つTOE管理者がTOEにI&Aを実行することを必要とすることにより、この制限を実行する。

上記の根拠の追加に加えて、ST作成者は、環境上の対策方針OE.RESTRICTED_FUNCTIONSをセキュリティ対策方針と脅威のマッピングに含まれるTOE:O.RESTRICTED_FUNCTIONSの対策方針に変更しなければならない（変更のある項目は対策方針を実行するエンティティだけであるため、記載されている内容をそのまま残すことが可能である）。

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	対策方針に対処する要件	根拠
O.RESTRICTED_FUNCTIONS 管理機能は権限を持つ管理者に限定される。	FIA_UID.2 FIA_UAU.2 FMT_MOF.1 FMT_MTD.1	TOE利用者は、有効な認証要素を持つ個人として定義される。これにより、ディスク上の情報の復号を許可する。この一連の利用者は、基盤となるOSに対してI&Aを実行することもできる。ただし、TOEに関しては、権限を持つ管理者のみがTOEにアクセスするための有効なI&A資格情報を持つ。TOEに正常にログインできる利用者はすべて管理者であるため、I&Aが正しく完了するまで管理機能を実行できないという要件は、対策方針を実施する上で十分である。 「管理者の代わりとなるTSF仲介アクション」はFMT_SMFで定義されている管理機能を示しており、ブート前に実行される機能（例えば、KEKの形成）やハードディスクとの間で直接行われる暗号操作ではないことに注意するべきである。

利用者識別（FIA_UID）

FIA_UID.2　　アクション前の利用者識別

FIA_UID.2.1　　**詳細化**：TSFは、**権限を持つ管理者**の代わりにその他のすべてのSTF仲介アクションを許可する前に、その各**管理者**が正しく識別されることを要求しなければならない。

適用上の注意：　　DEKはKEKによって暗号化する必要があり、KEKは認証要素から取得された鍵によって暗号化する必要があるため、ディスク暗号化を一度初期化したら、管理者はTOEを管理するために有効な認証要素を所有する必要がある。

保証アクティビティ：　　識別と認証はTOEによって両方が連続的に実行されるため、このコンポーネントとFIA_UAU.2の両方の保証アクティビティがFIA_UAU.2保証アクティビティ節で説明されている。

利用者認証（FIA_UAU）

FIA_UAU.2　　アクション前の利用者認証

FIA_UAU.2.1 **詳細化**：TSFは、**権限を持つ管理者**の代わりにその他のすべてのSTF仲介アクションを許可する前に、その各**管理者**が正しく認証されることを要求しなければならない。

保証アクティビティ： FIA_UID.2で示すように、ここに示す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、AGDガイダンスで、TOEで管理者がどのように確立されるかについての記述をレビューしなければならない。それらの記述は、利用者の識別子を作成するための指示や、利用者の初期認証情報であるだろう。評価者は、I&Aメカニズムを呼び出すための指示、及び認証情報を変更する（例えば、利用者が自身のパスフレーズを変更する）ための指示（機能が提供されている場合）もガイダンスに含まれていることを確認しなければならない。また、構成ガイダンスに、I&A機能を実行するためにTOEで使用される情報を保護するために必要となる、プラットフォームの構成情報も含まれるだろう。

評価者は、TSS節をレビューして、機能と使用に関してI&Aメカニズムの記述と一致していることを確認しなければならない。TSS節には、I&Aプロセスが正しく完了するまで、実際の管理機能が不正な呼び出しからどのように保護されるのかも詳述する。この分析の一環として、評価者は、管理に使用される非TOE製品を識別するTSS節内の情報を使用して、TOEに対して最初にI&Aを実行せずには、TOEを管理するためにこれらの製品を直接呼び出すことができない仕組みを詳述した記述が存在することを確認しなければならない。

評価者は、以下のテストも実施しなければならない。

- テスト1：管理者の識別情報を確立することができ、TOE管理機能を呼び出すために、この識別情報を使用してTOEに正常にログインできることを確認する。
- テスト2：利用者の識別情報及び／または認証情報を誤って入力した場合、利用者はTOE管理機能を呼び出すことができないことを確認する。
- テスト3：I&Aプロセスをバイパスして、TOE管理機能を直接呼び出すことができないことを確認する。

C.3 FCS_CKM.1 補助要件

規格を参照するFCS_CKM要件のいくつかの節では、PPの本文に特定されている以外の追加の暗号機能をTOEが実装することを必要としている。STの作成時に、ST作成者がこのような規格を参照する選択を選ぶ場合、この選択に追加のSFR及び関連する保証アクティビティを含め、この保証アクティビティをSTの本文に含める必要がある。

これらの要件をSTに含める場合、ST作成者は、これらの機能がサポートする既存のFCS_COP要件を判断し、要件根拠の節の該当する対策方針を適切に更新する（多くの場合、これはO.AUTHORIZATIONである）。これらの要件は補助要件であるため、対策方針の更新は必要とならない。

C.3.1 HMAC関数

HMAC関数は、NIST SP 800-90のHMAC_DRBG関数及びNIST SP 800-132のPRFを実装するために使用される。SHA関数の使用も必要となるため、この要件をSTで使用する場合は、C.1.2のハッシュ要件及び該当する選択も含めなければならないことに注意すること。RBG関数はUSBフラッシュドライブに実装する必要があるため、この要件を満たすメカニズムをUSBフラッシュドライブに実装しなければならないことに注意するべきである。1つの鍵長／ハッシュ関数／ブロックサイズ／出力MAC長だけを使用することが求められる。これらのパラメタのいずれかを設定できる場合、この要件をSTに繰返し記述してこれを反映するべきである。

FCS_COP.1	**暗号操作（鍵付暗号ハッシュ）**
FCS_COP.1.1	**詳細化：**TSFは、以下の**FIPS 198-1**に合致する、**[The Keyed-Hash Message Authentication Code（鍵付ハッシュメッセージ暗号コード）]**と暗号鍵サイズ**[選択：128ビット、256ビット]**に従って、**鍵付暗号ハッシュサービス**を実行しなければならない。
適用上の注意：	この要件における選択は、DEKのサイズに対して特定される鍵サイズと一致しなければならない。
保証アクティビティ：	評価者は、TSSを検査して、HMAC関数によって使用される次の値をTSSが特定していることを確認しなければならない：鍵長、使用されるハッシュ関数、ブロックサイズ、及び使用される出力MSC長。 また、評価者は、以下から入手可能な「The Keyed-Hash Message Authentication Code Validation System （HMACVS)」[HMACVS]を参照して、ランダムメッセージテストを実施しなければならない。: http://csrc.nist.gov/groups/STM/cavp/documents/mac/HMACVS.pdf テストでは、評価者は15セットのテストデータを作成しなければならない。各セットは1つの鍵とメッセージデータで構成されなければならない。評価者は、TSFによって生成されるHMACが期待値と一致することを確認しなければならない。

C.4 認証要素の生成

TOEは、外付けトークン認証要素またはパスフレーズベース認証要素のいずれかを生成することは必要とされない。ただし、TOEがこのサービスを提供する場合は、TOEがこの機能を主張し、FMT_SMF.1.1の項目「d」で行った該当する選択に、管理者がこのような認証要素を生成する利用者であることを反映するためには、以下のコンポーネントをSTに含める必要がある。

FCS_CKM_EXT.1(X)	**暗号鍵生成（外付けトークンのサポート）**
FCS_CKM_EXT.1.1(X)	TSFは、FCS_CKM.1(1)の指定に従って少なくともDEKのサイズと等しいエントロピーによって初期化された[選択：128ビット、256ビット]の認証要素を生成するFCS_RBG_EXT.1の指定に従って、ランダムビット生成器で生成された外付けトークン認証要素を

取得しなければならない。

FCS_CKM_EXT.1.2(X)　TSFは、外付けデバイスに認証要素を保存できなければならない。

適用上の注意：　選択では、FCS_CKM.1(1)でDEKに指定されているものと同一のビット数を示すべきである。

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、管理者が外付けトークン認証要素を生成するために必要なステップが記述されていることを確認する。評価者は、STのTSS部分をレビューして、生成機能がRBGをどのように使用するのか、及びRBG関数がどのように初期化されるのかを含め、外付けトークン認証要素の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節（または管理者ガイダンス文書）をレビューして、RBGによって生成される値がどのようにトークンに転送されるのかも確認する。使用されるRBGはTOEが提供しなければならず、FCS_RBG_EXT.1に指定されている要件を満たさなければならないことに注意するべきである。

評価者は、以下のテストを実施しなければならない。

- テスト1：管理者ガイダンスに従って、外付けトークン認証要素を作成する。可能であれば、認証要素に含まれるビット数を確認する。外付けトークン認証要素を使用して暗号化されたディスクにアクセスできることを確認する。

附属書 D：文書の表記法

英国式の綴りを米国式の綴りに置き換えたことを除き、本PPで使用している表記、書式、及び表記法は、コモンクライテリア（CC）のバージョン3.1と一致している。PPの読者に役立つよう、厳選された表現の選択についてここで説明する。

PPの利用者に役立つよう、厳選された表現の選択についてここで説明する。CCによって、機能要件及び保証要件に対してさまざまな操作を実行することが可能である；*詳細化*、*選択*、*割付*、*及び繰返し*は、CC 3.1のパート1の附属書C4に定義されている。これらの各操作を本PPに使用している。

詳細化の表記法

詳細化操作は、要件に詳細を追加する、つまり要件をさらに制限するために使用される。セキュリティ要件の詳細化は、エレメント番号及び太字で示される要件内の追加テキストの後に、「詳細化」という**太字**の語句で示されている。詳細化で元の要件が「低下」することはない。詳細化された要件を満たすTOEは、PP／STの文脈の詳細化されていない要件も満たさなければならない（CC 3.1パート1、附属書C.4.4を参照）。詳細化は、CCの語句の削除で構成される場合もある。その場合、削除は~~取り消し線~~のテキストで示される。

選択の表記法

選択操作は、CCで提供される要件を記述した1つ以上のオプションを選択するために使用される（CC 3.1パート1、附属書C.4.3を参照）。PP作成者が行った選択では、選択内容が**太字**で示されており、括弧と語句「選択」が削除されている。ST作成者が指定する選択は、角括弧及び選択を行うことを示す[選択：]という表示で示されている。

割付の表記法

割付操作は、パスフレーズ長などの指定されていないパラメタに特定の値を指定するために使用される（CC 3.1パート1、附属書C.4.2を参照）。値が**太字**で表示されている割付はPP作成者が作成した割付を示し、括弧と語句「割付」は削除されている。ST作成者が指定する割付は、角括弧及び割付を行うことを示す[割付：]という表示で示されている。

繰返しの表記法

繰返し操作は、コンポーネントがさまざまな操作で繰り返される場合に使用される（CC 3.1パート1、附属書C.4.1を参照）。コンポーネントIDの後に、括弧内に繰返し回数（iteration_number）が示されている。

繰返し操作は、すべてのコンポーネントで実行することができる。PP／ST作成者は、同じコンポーネントに基づいた複数の要件を含めることにより、繰返し操作を実行する。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返しと異ならなければならない。これは、割付と選択を異なる方法で指定したり、詳細化を異なる方法で適用することにより実現される。

繰返しの例に、3つの異なる暗号アルゴリズムの実装が必要であるため、3回繰り返されるFCS_COP.1がある。

根拠を明確にすると共に、これらの要件との間で追跡を行うことができるよう、さまざまな繰返しは一意に識別されるべきである。

拡張要件の表記法

拡張要件は、CCが作成者のニーズを満たす適切な要件を提供しない場合に認められている。**拡張要件**は識別されなければならず、CCのクラス／ファミリ／コンポーネントモデルを使用して要件を明確に示すために必要である。拡張要件は、コンポーネント内に挿入された「EXT」で示される。

前提条件、脅威、組織のセキュリティ方針、及び対策方針の命名法：

前提条件：TOEセキュリティ環境の前提条件は、先頭が「A.」でその後にすべて大文字の説明ラベルが続く、所定の名称である（例えば、A.TRAINED_ADMINISTRATORS）。

脅威：TOEセキュリティ環境の脅威は、先頭が「T.」でその後にすべて大文字の説明ラベルが続く、所定の名称である（例えば、T.ACCIDENTAL_ADMIN_ERROR）。

方針の記述：方針の記述は、先頭が「P.」でその後にすべて大文字の説明ラベルが続く、所定の名称である（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は、先頭が「O.」でその後にすべて大文字の説明ラベルが続く、所定の名称である（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は、先頭が「OE.」でその後にすべて大文字の説明ラベルが続く、所定の名称である（例えば、OE.NO_EVIL）。

運用上の注意

運用上の注意には、TOEの作成に関連したりTOEの使用に役立つと考えられる、追加の補足情報が含まれている。また、コンポーネントに許可されている操作に関連する助言も含まれている。

保証アクティビティ

保証アクティビティは、脅威を低減するためにTOEに課される機能要件についての共通評価方法論として機能する。アクティビティは、TSSの記載に従って評価者がTOEの特定の側面を分析するための指示を含んでおり、ST作成者にこの情報をTSS節に含めるという暗黙的な要件を課している。

附属書 E：用語集

PP全体に渡って使用される用語に適用されている、いくつかの定義がある：

管理者 ー TOEを設定することができる利用者。

認証要素（AF） ー 利用者がハードディスクを使用することが許可されたコミュニティに所属していることを確立するために、利用者によって提示される値。この値はKEKとして使用される（条件付け及び／または組み合わせの後で）。従って、各要素はKEKを生成するために必要となるため、すべてのAFが利用者によって正しく提示されなければならない。これらのAFは、利用者の特定の識別情報を確立するためには使用されないことに注意すること。*外付けトークン認証要素*は、外付けトークンに保存される認証要素である。

許可された利用者 ー TOEを使用するために管理者によって認証要素を提供された利用者。

データ暗号化鍵（DEK）ーハードドライブを暗号化するために暗号アルゴリズムによって使用される鍵。

決定論的ランダムビット生成器（DRBG）ー秘密の初期シード値から一連のビットを生成する暗号アルゴリズム。シード値を知らない場合は、DRBGのセキュリティレベルに応じて、出力順序を予測できないようにするべきである。

エントロピー源ーこの暗号化関数は、1つ以上のノイズ源から出力を累積することにより、ランダムビット生成器にシードを提供する。機能には、一定の出力を推測するために必要となる最小限の作業の測定、及びノイズ源が正しく動作していることを確認するためのテストが含まれる。

FIPSで承認された暗号化関数 ー 1) 連邦情報処理規格（FIPS）に規定されている、または2) FIPSで採用されてFIPSの附属書またはFIPSによって参照される文書に規定されている、セキュリティ機能（例えば、暗号アルゴリズム、暗号鍵管理手法、認証手法）

フルディスク暗号化（FDE） ー 完全ディスク暗号化とも呼ばれる。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して、FDE製品への認証が成功した後にのみデータへのアクセスを許可するプロセスのこと。ソフトウェア暗号化製品では、マスタブートレコード（MBR）とブート可能なパーティションについて、ドライブの一部が暗号化されない状態で残ることに注意すること。本プロテクションプロファイルでは、ディスク暗号化とは、利用者データが含まれる可能性がある情報が書き込まれていない限り、ソフトウェアディスク暗号化製品でMRB及びブート可能なパーティションについてドライブの一部が暗号化されない状態で残ることを許可するように変更された、NIST定義となるだろう。複数のドライブを使用する場合、「フルディスク暗号化」の概念では、すべてのドライブを暗号化することが要求される。

運用環境 ー 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すべてを含め、TOEの機能とセキュリティ方針をサポートするTOE境界の外側に存在するハードウェアとソフトウェア。

鍵の暗号化鍵（KEK） ー DEKを暗号化するために使用される鍵。注意：間接の別の階層を追加することが可能である。例えば、DEKを暗号化し、KEKによって暗号化される中間鍵など。

鍵とする材料 ー KEK、DEK、中間鍵、認証要素、及び鍵を取得するために使用する乱数または他の値。

マスタブートレコード（MBR） ー MBRは通常、ハードドライブの1番目のセクタに存在する。MBRは、パーティションテーブルを確認することによって決定した、ブート可能なパーティションを読み込む。

ノイズ源 ー 決定論的ではないエントロピーを生成するアクティビティが含まれる、RBGのコンポーネント。

運用環境 – TOEが動作する環境。

永続記憶域 ー 電源がオフになった後にデータを長時間保持するデータ格納域。

ランダムビット生成器（RBG）ー エントロピー源及び鍵とする材料を生成するために必要なランダムビットを取得するために呼び出されるDRBGから成る暗号化関数。

許可されていない利用者 ー TOEに対して有効な認証要素を所有していない利用者。

揮発性メモリー 電源がオフになると内容が失われるメモリ。

ゼロ化 ー この用語は、記憶場所を逆参照することと記憶場所を定数でアクティブに上書きすることを区別するために使用されている。鍵とする材料は、必要がなくなったら上書きする必要がある。

附属書 F：PP の識別情報

タイトル：	フルディスク暗号化のプロテクションプロファイル （紛失または盗難にあったハードディスクのリスクの軽減）
バージョン：	1.0
スポンサー：	National Security Agency （NSA）
CCのバージョン：	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3、2009年7月
評価レベル：	評価保証レベル（EAL） 1
キーワード：	認証要素、認証サブシステム、DEK、ディスク暗号化、 暗号化サブシステム、エントロピー、KEK、ノイズ源