USB フラッシュドライブ用のプロテクションプロファイル
不正操作、放置または盗難にあったUSBフラッシュドライブのリスクの低減

原文タイトル：

Protection Profile for USB Flash Drives

Mitigating the Risk of a Manipulated, Misplaced, or Stolen USB Flash Drive

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_usb_fd_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

図一覧

改訂履歴

バージョン	日付	説明
1.0	2011年12月01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 概要

1 本書は、USB フラッシュドライブ用の第一世代の標準プロテクションプロファイル(PP）である。本 PP では、1）組織が 2 つのデバイス間で情報を転送する、2）単一利用者がデバイスにファイルを保存する、という USB フラッシュドライブの 2 つの使用シナリオを取り扱う。本 PP は、攻撃者が放置または盗難 USB フラッシュドライブを入手し、機密データを抽出する、またはホスト環境に侵入するために使用できる悪意のあるシステムファイルをデバイスに配置しようとする主な脅威を取り扱っている。本プロテクションプロファイル（PP）で定義する評価対象（TOE）は、USB フラッシュドライブ及びドライブ上のデータにアクセスし、ドライブを管理するために使用される関連ソフトウェアである。

1.1.1 評価対象（TOE）の用途及び主なセキュリティ機能

2 本 PP に適合する USB フラッシュドライブは、デバイスに保存された利用者データをデバイスのプロセッサによって暗号化しなければならない。TOE には、利用者が USB フラッシュドライブと相互作用するためにベンダによって提供されるソフトウェアが含まれる。このソフトウェアはホストデバイスに常駐し、USB フラッシュドライブ自体に常駐することもあり、2 つの環境間の相互作用の量は実装によって異なる。すべての暗号操作（デバイスに保存された利用者データの暗号化と復号、データ暗号鍵（DEK）をマスクするための鍵暗号鍵（KEK）の生成、DEK をマスクするための操作）は、ホストでなく、USB フラッシュドライブのプロセッサによって実行されなければならない。

3 USB フラッシュドライブに保存されるデータは、DEK を使用して暗号化される。DEK は、鍵暗号鍵（KEK）を使用してマスクされる。KEK は、（認証要素から導出する「サブマスク」と呼ぶ）複数のコンポーネントから導出したり、単一のサブマスクから取得したりすることができる。USB フラッシュドライブを暗号化する最大のセキュリティ対策方針は、攻撃者に膨大な鍵空間で暗号を解読する作業を強いることである。なお、これを実現できるのは、USB フラッシュドライブの許可された利用者が意図せずに認証要素を USB フラッシュドライブに保存しない場合のみである。

4 デバイスにはシステムファイルの保護領域がある。USB フラッシュドライブを攻撃ベクトルとして使用する既知の攻撃は、USB フラッシュドライブをホストに挿入すると自動的に実行される USB デバイス上のシステムファイルの置換に依存する。本 PP に適合する USB フラッシュドライブは、更新が許可された配付元から来たことを保証するデジタル署名を通じてチェックできる更新を、USB フラッシュドライブ上のシステムファイルにインストールするだけでよい。さらに、適合デバイスは、最初にデジタル署名をチェックせずにシステムファイルを置換することはない。最新のファームウェアが使用されていることを保証するために役立ち、USB フラッシュドライブ上の製品のバージョンを決定するために使用できるインタフェースが、利用者に提供される。

5 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）及びローカルファイルストレージとファイル転送の 2 つの使用例のために 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）を提供する必要がある。

1.1.2 許可

6 USB フラッシュドライブが初期化され、暗号化が有効にされた後で、ホストから USB フラ

ッシュドライブにデータを転送する前に 1 つまたは複数の認証要素を確立しなければならない。利用者が USB フラッシュドライブの復号を要求し、利用者のホストにデータを転送するには、この認証要素を USB フラッシュドライブに提示しなければならない。認証要素は利用者ごとに一意である必要はない。認証要素は、所有者が USB フラッシュドライブに保存されているデータを要求することが許可された利用者のコミュニティに属することを確立するためにのみ必要である。各認証要素はサブマスクを導出するために使用され、サブマスクは KEK を導出するために使用される。

7 すべての適合 TOE は、パスワード認証要素をサポートしなければならない。これは、サブマスクを生成するために条件付けられる。また、適合 TOE はオプションで以下をサポートできる。

- ホストに保存される「ホスト分割認証要素」と呼ぶランダムに生成されるビット列。この場合、認証要素は直接サブマスクとしても機能する。
- USBフラッシュドライブ上の改ざんから保護されたストレージでランダムに生成されるビット列。これは、利用者が正しいPINを提供する場合のみ提供される。この場合、PINが認証要素であり、ランダムに生成されるビット列がサブマスクである。これらの認証要素では、PINは、間違ったPINを連続して入力する（回数は設定可能）とデバイスがロックされる防衛手段に支配される。

次に、これらのオプションの認証要素から生成されるサブマスクがパスワードベースのサブマスクと組み合わされ、この組合せからKEKが導出される。

通常、ホスト分割認証要素は、USBフラッシュドライブが特定のデバイスの外付ストレージとして使用される場合にサポートされる。理想的には、ホスト分割認証要素は、ホストデバイス上のTrusted Platform Module（TPM）によって保護される。しかしながら、ホストではディスク暗号化がまだ使用され、分割、その残り、または追加認証要素の残りを保護する。

8 ST の執筆者が追加認証要素とサブマスクを生成する手段を定義する場合は、認証要素と手段を完全に記載しなければならず、パスワード及び/または他の認証要素から生成されるサブマスクの強度を減らしてはならない。すべての認証要素は、マスクする DEK と同じサイズ（ビット長）のサブマスクを生成するように条件付けなければならず、XOR 機能を使用して KEK を生成するように組み合わせなければならない。

9 現在のプラクティスを反映するために、ベンダは管理者が外部で生成できる 32 文字以上のパスワードを持つ機能をサポートしなければならない。利用者がパスワードを入力すると、パスワードは KEK の入力として提供される前に USB フラッシュドライブ上の TSF によって条件付けられる。大きいパスフレーズ（256 文字以上）が望ましい。「附属書 C」のパスフレーズ認証要素の要件がサポートされる場合は、代わりにこの要件を ST に入れるべきである。長いランダム文字列のパスワードを思い出して入力するより、単語が並んだパスフレーズを記憶して入力する方が利用者にとって容易であるため、本 PP の将来の世代では、パスフレーズのサポートが必須になる。

10 他のオプションの認証要素のいずれかを使用する場合、ST 執筆者は附属書 C から該当する内容を含める。ホスト分割認証要素は、USB フラッシュドライブに常駐する RBG によって生成されなければならない。USB フラッシュドライブのメモリに常駐する PIN で保護されたサブマスクは、USB フラッシュドライブ上の RBG によって生成されなければならない。PIN 認証要素は運用環境で設定し、選択することができるが、サブマスクは USB フラッシュドライブ上の乱数発生器によって生成されなければならない。下記に示すように、DEK は USB フラッシュドライブに常駐する RBG によって生成されなければならない。

1.1.3 暗号化

11 USB フラッシュドライブは、製造施設を出るとき、暗号化が有効になっていない場合がある。利用者または管理者がドライブを初期化し、暗号化をオンにしたら、デバイス上のデータは暗号化されたままでなければならない。さらに、デバイスの最初の利用者がデバイスを初期化するとき、DEK を生成できなければならない。暗号化が有効になり、DEK が利用者の認証要素から導出した KEK でマスクされるまで、すなわち利用者がデバイスの所有権を取得するまで、データはデバイスに保存できない。最初の利用者が所有権を取得し、デバイスを初期化した後で DEK を再生成できることが望ましいが、必須ではない。

12 パスワード変更の認証要素は必須の機能であるため、利用者がパスワードを変更するには 2 個の鍵（DEK と KEK）が必要である。KEK を使用して DEK をマスクするとは、利用者がデバイス上のデータを再び暗号化せずにパスワード認証要素を変更する（したがって新しい KEK を導出する）ことができることを指す。

13 鍵、サブマスク、または認証要素を生成、処理、及び保護するために使用する暗号方式が十分に堅牢であり、実装に重大な誤りがないなら、認証要素、サブマスク、または KEK なしに放置または盗難 USB フラッシュドライブを入手する攻撃者は、データを取得するために KEK または DEK の鍵空間を総当りしなければならない。なお、パスワードは、データ暗号化アルゴリズム（AES）で可能な個数の鍵を総当りすることに比べ、強度が劣るかもしれない。さらに、パスワードが攻撃者に未知の唯一の認証要素であるなら、鍵空間は AES を総当りするまたは可能な個数のパスワードを総当りするために必要な最小の作業になる。そのため、今後のプロテクションプロファイルでは、パスフレーズ及び他のより強力な認証要素/サブマスクのサポートが要求されるだろう。

14 USB フラッシュドライブに転送されるデータは、DEK を使用して暗号化される。DEK は、（XOR 演算を通じて、または AES を使用して）KEK によってマスクされる。DEK は、USB フラッシュドライブに装備される決定性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 ビットのいずれかである。正しいシードで生成した DRBG により、ノイズのサンプルが DEK の鍵サイズ以上になることが保証される。DRBG アルゴリズムの入力として使用されるエントロピーは、1 つ以上のハードウェアベース情報源から提供されなければならない。

15 USB フラッシュドライブをデバイスから取り出す際は（シャットダウン）、暗号化されていない鍵関連情報（改ざん防止モジュールで保護された PIN 保護方式サブマスクを除く）または利用者データが永続メモリに常駐してはならない。永続メモリは、USB フラッシュドライブの電源を切った後でも状態を維持するメモリと定義される。シャットダウンの定義については、いくつかのシナリオがある。USB フラッシュドライブが急にホストコンピュータから取り出されるとき。USB フラッシュドライブが安全にハードウェアを取り出すためにオペレーティングシステムを使用して取り出されるとき。ホストコンピュータがオフになるとき（電源オフ、スリープモード、休止モード）。すべての場合が制御されるわけではないため、以下のように定める。1）鍵関連情報は使用したらただちに消去する、または揮発性メモリに保存する、及び 2）利用者データは暗号化されていない形でデバイスに保存しない。

1.1.4 TOE ファームウェア/ソフトウェアの更新

16 PP に適合する USB フラッシュドライブは、要件に規定されているデジタル署名を使用して、TOE ファームウェア及びソフトウェアの更新（存在する場合）が、信頼される配付元（多くの場合、製品ベンダ）から来ていることを暗号方式で検証する機能を備える。更新の検証に使用する公開鍵は、更新の署名の検証を実行する際に必要な「信頼の連鎖」チェック

を制限するために、USB フラッシュドライブに装備されていなければならない。この証明書は「システムファイル」として取り扱われ、更新できるが、そのときの最新の証明書によって検証された後に限られる。このような更新をサポートするために、利用者は使用中のファームウェア/ソフトウェアの現在のバージョンを USB フラッシュドライブに問い合わせ、ファームウェア/ソフトウェアの更新を開始することができる。USB フラッシュドライブは、署名を検証できない変更を拒否する。チェックに関連する暗号操作は、USB フラッシュドライブ自体の暗号機能によって実行される。ホストデバイスで動作する暗号機能には依存しない。

1.1.5 管理

17 TOE の基本要件では、TOE が管理者の役割を維持することは要求されない（TOE の管理者とは、特定の責任を持ち、一般の利用者より「信用」が大きい TOE の利用者の部分集合が存在することを指す）。通常、管理者は、一般の利用者が使用できない TOE の機能を呼び出す特権を保有する。ただし、USB フラッシュドライブの場合は、デバイスが一旦使用されたら、管理者が関与する必要はない。TOE の更新であっても、デバイスを所有する（管理者でない）利用者が実行できるべきである。

18 ただし、本 PP の基底要件では、パスワードベースの認証要素のみが必須である。本 PP の要件では 150 ビットのエントロピーを持つ、推測が困難なパスワードが許容されているにもかかわらず、信頼できない利用者は、歴史的にエントロピーが低く、推測しやすいパスワードを作成する傾向があった。本 PP で規定される保護が容易に破られないことを保証したい組織は、利用者が良いパスワードを選ぶことの重要性を理解することを保証し、利用者がそれに従うための方針を実施するべきである。管理者がパスワードを作成する（それから利用者に提供する）方法もあるが、ほとんどの USB フラッシュドライブには利用者が本人の認証要素を変更する機能があるため、利用者が強いパスワードの必要性に納得しない限り、USB フラッシュドライブの所有権を取得すると、管理者から提供されたパスワードを好みのパスワードに変更する。

19 利用者に幾分の裁量を許すとしても、すべての利用者が良い認証要素を選ぶことを信用するための解決方法は、TOE によってパスワード対策を強制することである。この要件は現在の USB フラッシュドライブでは広く実装されていないため、附属書 C に記載されているオプションの要件である。

1.1.6 許可された利用者

20 データの不正入手のリスクを最小限に抑えるために、許可された利用者には利用者ガイダンスを守ることが期待される。許可は、TOE を所有し、保護された USB フラッシュドライブのロックを解除する正しい認証要素を提供することで決定される。USB フラッシュドライブと TOE の認証要素の安全を図り、保護するのは、公式に保有している間の USB フラッシュドライブの許可された利用者の責任である。許可された利用者は、パスワード及び/または保護されていない認証要素を USB フラッシュドライブに残したり、保存したりしてはならない。また、複数の要因を使用する場合は、相互に残したり、保存したりしてはならない。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。

1.1.7 TOE 以外の利用可能なハードウェア/ソフトウェア/ファームウェア

21 TOE は、パスワードベースの認証要素用のインタフェース、高信頼更新機能用のインタフェース、及びホストと USB デバイス間の通信メカニズムの提供について運用環境（ホストデバイス）に依存する。ベンダには、必要な機能を持つ運用環境を識別するための十分なインストール/設定手順を提供し、正しくセキュアな方法で運用環境を設定し、更新する方

法に関する手順を提供することが期待される。

22 場合によっては、TOE ベンダは、TOE がセキュリティ対策方針を達成できるように、運用環境の具体的な設定ガイダンスを提供しなければならない。このようなガイダンスは TOE の操作ガイダンスと見なされ、TOE の最終利用者に提供される文書に記載されるべきである。

2 セキュリティ課題記述

23 保護するべき主な資産は、USBフラッシュドライブに保存されるデータである。したがって、脅威モデルは、USBフラッシュドライブを使用してデータを保存したり、転送したりするときに、データが意図せず、または意図的に不正入手される方法に集中する。

2.1 脅威

24 脅威は、脅威エージェント、資産及びその資産に対する脅威エージェントの有害なアクションから構成される。

25 主な脅威エージェントは、脅威エージェントが USB フラッシュドライブを盗んだり、放置 USB フラッシュドライブを入手したりする場合に、その資産を危険にさらすエンティティである。例えば、次の表には T.UNAUTHORIZED_ACCESS が含まれている。脅威エージェントは、放置または盗難 USB フラッシュドライブの所有者（許可されていない利用者）である。資産は、利用者データである。有害なアクションは、USB フラッシュドライブから利用者データを入手しようとすることである。この脅威から USB フラッシュドライブの最初の機能要件（TOE）が生じ、利用者がデータを復号するために必要な鍵または鍵分割を所有する必要が生じる。KEK、DEK、認証要素、サブマスク、及び乱数または鍵または認証要素の生成に関与するその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を解読できるため、鍵関連情報は重要性において利用者データと同等と見なされ、脅威の表では「その他の資産」に含まれる。

26 本 PP では、TOE には、USB フラッシュドライブの利用者データファイルに常駐する悪意のあるソフトウェアに関連するすべての脅威に対して保護することは期待されない。例えば、TOE には、利用者が暗号化や伝送用に選択するデータ内のマルウェアを検出する責任はない（それはホスト環境の責任である）。USB フラッシュドライブがホストシステムで動作するようになった後で、ホスト上の潜在的に悪意のあるソフトウェアによるデータに対する脅威も、本 PP の脅威モデルには含まれない。例えば、本 PP には、（悪意のあるアクションまたは使用後のデータの消し忘れによる）パスワードベースの認証要素を取得する悪意のあるホストに対処する要件はない。

27 USB フラッシュドライブを外付ストレージとして使用するときは、USB フラッシュドライブがそれらのデータの唯一の保存場所として使用されている場合でも、ホスト上でディスク全体の暗号化が使用されるべきである。USB フラッシュドライブがホストに接続されるときに調べられ、または変更されるファイルの一時コピーが作られるリスクがある。このような残留物は、ホストの電源が切れた後も（例えばオペレーティングシステムのページファイルに）永続し、暗号化または消去しないと、開示されることになる。また、利用者がホスト経由で USB フラッシュドライブに認証要因を提供するとき、利用者の認証要因が意図せず永続メモリにスワップされるリスクもある。

表 1：脅威

脅威	脅威の説明
T.KEYING_MATERIAL_COMPROMISE	攻撃者はTOEによってUSBフラッシュドライブ上の永続メモリに書き込まれた暗号化されていない鍵関連情報（KEK、DEK、認証要素、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、これらの値を使用して利用者データにアクセスすることができる。

T.KEYSPACE_EXHAUST	許可されていない利用者は、利用者データやTSFデータへの無許可アクセスの取得を目指して暗号鍵または認証要素を決定するためにブルートフォース攻撃を試みることがある。
T.TSF_COMPROMISE	悪意のある利用者またはプロセスは、鍵関連情報や利用者データにアクセスするために、TSFデータまたは実行コード（例えばUSBフラッシュドライブ上のファームウェア）を使用して不適切にアクセス（表示、変更、または削除）することがある。
T.MALWARE_PROPOGATION	ホストデバイス上の悪意のあるエンティティは、TOEが挿入されるホストにそれ自体を自動的に転送し、そのホストの完全性とセキュリティ機能を無効にする（悪意のある）システムファイルをUSBフラッシュドライブに配置する。
T.UNAUTHORIZED_ACCESS	放置または盗難USBフラッシュドライブにアクセスできる許可されていない利用者は、USBフラッシュドライブに保存されるデータにアクセスできることがある。
T.UNAUTHORIZED_UPDATE	悪意のあるパーティは、TOEのセキュリティ機能を無効にすることができる製品の更新を最終利用者に提供しようとする。
T.UNSAFE_AUTHFACTOR_VERIFICATION	攻撃者は、安全でない方法を利用して利用者が入力した認証要素の検証を実行できる。その結果、KEK、DEK、または利用者データが開示される。

2.2 前提条件

28 セキュリティ問題の定義の本節では、セキュリティ機能を提供するために運用環境に関する前提条件を示す。これらの前提条件を満たさない運用環境に TOE が配置される場合、TOE はすべてのセキュリティ機能を提供できない場合がある。前提条件には、運用環境の物理的、人為的、及び接続的側面がある。

表 2：TOE の前提条件

前提条件	前提条件の説明
A.AUTHORIZED_USER	許可された利用者は、提供されるすべてのガイダンスに従う。
A.PASSWORD_BASED_AUTH_FACTOR	許可された利用者には、保護対象データの機密性を反映する十分な強度とエントロピーがパスワード認証要素にあることを保証する責任がある。

3 セキュリティ対策方針

29 セキュリティ対策方針は、第 2 章の脅威、組織のセキュリティ方針、及び前提条件から導出する評価対象（TOE）と運用環境に関する要件である。第 4 章では、TOE に関する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）と言い換えている。TOE は、SFR に対して評価される。

3.1 TOE に関するセキュリティ対策方針

30 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、識別された脅威に対抗し、識別された組織のセキュリティ方針に適合するために、記載されている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で、これらの対策方針に適合しなければならない。

表 3：TOE に関するセキュリティ対策方針

対策方針	対策方針の説明
O.AUTHORIZED_USER	TOEは、USBフラッシュドライブ上のデータを暗号化及び復号できるように、認証要素を取得しなければならない。
O.CORRECT_TSF_OPERATION	TOEは、TSFがその運用環境で正しく動作することを保証するためにTSFをテストする機能を提供する。
O.ENCRYPT_ALL	TOEは、USBフラッシュドライブに保存されるすべての利用者データを暗号化する。
O.DEK_SECURITY	TOEは、認証要素を持たない脅威エージェントがDEKを取得して利用者データにアクセスできないように、（認証要素から導出した）1つまたは複数のサブマスクから作成された鍵暗号鍵（KEK）を使用してDEKをマスクする。
O.OWNERSHIP	TOEは、利用者データをTOEに保存する前に、所有権が取得された（すなわち、DEKが作成され、認証要素が確立され、既定の認証要素が変更され、KEKが導出したサブマスクから生成され、DEKがKEKに関連付けられている）ことを保証しなければならない。
O.KEY_MATERIAL_COMPROMISE	TOEは、暗号化/マスクされていない鍵または鍵関連情報がUSBフラッシュドライブ上の永続メモリに書き込まれないことを保証しなければならない。
O.PROPAGATION_PREVENTION	TOEは、USBフラッシュドライブが悪意のあるソフトウェアを自動的に拡散するメカニズムとして使用されることを防止するメカニズムを実装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開示されないように、認証要素の検証を実行しなければならない。
O.TRUSTED_UPDATE	TOEは、TOEファームウェア/ソフトウェアを更新し、製品の更新が意図した配付元から受信されることを検証する機能を利用者に提供しなければならない。

3.2 運用環境に関するセキュリティ対策方針

31 TOE の運用環境は、TOE が（TOE に関するセキュリティ対策方針で定義される）そのセキュリティ機能を正しく提供するための技術的及び手続き的対策を実装する。運用環境に関するセキュリティ対策方針は、運用環境が達成するべき対策方針を記述する 1 組の文から構成される。

32 本節では、IT ドメインによって、または技術的または手続き的でない対策によって対処するべきセキュリティ対策方針を定義する。2.2 節で規定されている前提条件は、環境に関するセキュリティ対策方針として組み込まれる。これらの前提条件から環境に関する追加要件が生じ、追加要件は手続き的または管理的対策を通じて満たされる。表 4 に、運用環境に関するセキュリティ対策方針を示す。

表 4：運用環境に関するセキュリティ対策方針

対策方針	対策方針の説明
OE.TRAINED_USERS	許可された利用者は正しく訓練され、強いパスワードの作成を含むすべての利用者ガイダンスに従う。

3.3 セキュリティ対策方針根拠

33 本節では、前節で定義したセキュリティ対策方針の根拠について説明する。表 5 に、セキュリティ対策方針と脅威の対応関係を示す。

表 5：セキュリティ対策方針と脅威の対応関係

脅威/方針	脅威と方針に対応する対策方針	根拠
T.KEYING_MATERIAL_COMPROMISE 攻撃者はTOEによってUSBフラッシュドライブ上の永続メモリに書き込まれた暗号化されていない鍵関連情報（KEK、DEK、認証要素、及び乱数または鍵が導出されるその他の値）を入手し、これらの値を使用して利用者データにアクセスすることができる。	O.DEK_SECURITY TOEは、認証要素を持たない脅威エージェントがDEKを取得して利用者データにアクセスできないように、（認証要素から導出した）1つまたは複数のサブマスクから作成された鍵暗号鍵（KEK）を使用してDEKをマスクする。 O.KEY_MATERIAL_COMPROMISE TOEは、暗号化/マスクされていない鍵または鍵関連情報がUSBフラッシュドライブ上の永続メモリに書き込まれないことを保証しなければならない。	O.DEK_SECURITYは、DEKがKEKによって保護され、DEKを直接不正入手することができないことを保証することで、この脅威を軽減する。さらに、O.KEY_MATERIAL_COMPROMISEは、USBフラッシュドライブ上の永続メモリに平文の鍵関連情報が書き込まれないため、USBフラッシュドライブを回復する悪意のあるエンティティがDEKを不正入手するために使用できる関連情報を取得できないことを保証する。
T.KEYSPACE_EXHAUST 許可されていない利用者は、利用者データやTSFデータへの無許可アクセスの取得を目指して暗号鍵または認証要素を決定するためにブルートフォース攻撃を試みることがある。	O.DEK_SECURITY TOEは、認証要素を持たない脅威エージェントがDEKを取得して利用者データにアクセスできないように、（認証要素から導出した）1つまたは複数のサブマスクから作成された鍵暗号鍵（KEK）を使用してDEKをマスクする。	O.DEK_SECURITYは、脅威エージェントがTOEにアクセスするために鍵またはパスワード空間を総当りする必要があることを保証することで、この脅威に対抗する。
T.TSF_COMPROMISE 悪意のある利用者またはプロセスは、鍵関連情報や利用者データにアクセスするために、TSFデータまたは実行コード（例えばUSBフラッシュドライブ上のファームウェア）を使用して不適切にアクセス（表示、変更、または削除）することがある。	O.CORRECT_TSF_OPERATION TOEは、TSFが運用環境で正しく動作することを検証する機能を提供しなければならない。O.TRUSTED_UPDATE TOEは、製品の更新が意図した配付元から受信されることを検証しなければならない。	O.CORRECT_TSF_OPERATIONは、TOEがそのコンポーネントが正しく動作することを検証することを保証する。コンポーネントが正しく動作しないと、情報がアクセスされるべきでないときにアクセスされることになる場合がある。 O.PROPAGATION_PREVENTION及びO.TRUSTED_UPDATEは、許可されていない利用者がTSFを変更しようとする試みが成功しないことを保証する。

	O.PROPAGATION_PREVENTION TOEは、USBフラッシュドライブが悪意のあるソフトウェアを自動的に拡散するメカニズムとして使用されることを防止するメカニズムを実装しなければならない。	
T.MALWARE_PROPOGATION 許可されていない利用者は、TOEが挿入されるホストにそれ自体を自動的に転送し、そのホストの完全性とセキュリティ機能を無効にする（悪意のある）システムファイルをUSBフラッシュドライブに配置する。	O.PROPAGATION_PREVENTION TOEは、USBフラッシュドライブが悪意のあるソフトウェアを自動的に拡散するメカニズムとして使用されることを防止するメカニズムを実装しなければならない。	O.PROPAGATION_PREVENTIONは、自動的にホストで実行される悪意のあるファイルをUSBフラッシュドライブに導入できる手段がないことを保証することで、この脅威に対抗する。
T.UNAUTHORIZED_ACCESS 放置または盗難USBフラッシュドライブにアクセスできる許可されていない利用者は、USBフラッシュドライブによって転送されるデータにアクセスできることがある。	O.AUTHORIZED_USER TOEは、USBフラッシュドライブ上のデータを復号できるように、利用者から認証要素を取得しなければならない。 O.ENCRYPT_ALL TOEは、USBフラッシュドライブに保存されるすべての利用者データを暗号化する。 O.DEK_SECURITY TOEは、認証要素を持たない脅威エージェントがDEKを取得して利用者データにアクセスできないように、（認証要素から導出した）1つまたは複数のサブマスクから作成された鍵暗号鍵（KEK）を使用してDEKをマスクする。 O.OWNERSHIP TOEは、利用者データをTOEに保存する前に、所有権が取得された（すなわち、DEKが作成され、認証要素が確立され、既定の認証要素が変更され、KEKが導出したサブマスクから生成され、DEKがKEKに関連付けられている）ことを保証しなければならない。	O.AUTHORIZATIONは、USBフラッシュドライブの許可された利用者から得られた、データを復号するために必要な認証要素を使用して、この脅威に対抗する。 O.ENCRYPT_ALLは、USBフラッシュドライブに書き込まれるときにすべての利用者データが暗号化されることを保証することで、この脅威に対抗する。 O.DEK_SECURITYは、USBフラッシュドライブに保存されない認証要素から導出したKEKでデータ暗号鍵がマスクされることを保証することで、この脅威に対抗する。 この対策方針は、許可されていない利用者が、KEKを生成するために使用される鍵関連情報にアクセスできないことも保証する。 O.OWNERSHIPは、USBフラッシュドライブ上に暗号化が確立されていない時間がなく、そのドライブに利用者データを書き込むことができることを保証することで、脅威に対抗する。さらに、既定の認証要素が存在する場合は、データが簡単に不正入手されないように利用者がこれらの認証要素を変更できるメカニズム

		と適切なガイダンスがある。
T.UNAUTHORIZED_UPDATE 悪意のあるパーティは、TOEのセキュリティ機能を無効にすることができる製品の更新を最終利用者に提供しようとする。	O.TRUSTED_UPDATE TOEは、TOEファームウェア/ソフトウェアを更新し、製品の更新が意図した配付元から受信されることを検証する機能を利用者に提供しなければならない。	O.TRUSTED_UPDATEは、第三者から受信される更新が、最終利用者に識別される配付元から来ていることを検証できることを保証することで、脅威に対抗する。
T.UNSAFE_AUTHFACTOR_VERIFICATION 攻撃者は、安全でない方法を利用して利用者が入力した認証要素の検証を実行できる。その結果、KEK、DEK、または利用者データが開示される。	O.SAFE_AUTHFACTOR_VERIFICATION TOEは、KEK、DEK、または利用者データが意図せず開示されないように、認証要素の検証を実行しなければならない。	O.SAFE_AUTHFACTOR_VERIFICATIONは、認証要素の検証がKEK、DEK、または利用者データを開示せずに実行されることを保証することで、脅威に対抗する。これには、KEKの実効強度を減らそうとする（例えば、多重認証要素使用例で認証要素の1つを開示する）攻撃に対する対抗手段が含まれる。

34 表 6 に、セキュリティ対策方針と前提条件の対応関係を示す。

表 6：セキュリティ対策方針と前提条件の対応関係

前提条件	前提条件に対応する対策方針	根拠
A.AUTHORIZED_USER 許可された利用者は、提供されるすべての利用者ガイダンスに従う。	OE.TRAINED_USERS 許可された利用者は正しく訓練され、強いパスワードの作成を含むすべての利用者ガイダンスに従う。	OE.TRAINED_USERSは、利用者が利用者ガイダンスに従ってTOEを正しく使用する方法について訓練されることを保証する。
A.PASSWORD_BASED_AUTH_FACTOR 許可された利用者は、パスワード認証要素がパスワード方針に適合し、保護対象データの機密性を反映する十分な強度とエントロピーがパスワード認証要素にあることを保証する責任がある。	OE.TRAINED_USERS 許可された利用者は正しく訓練され、強いパスワードの作成を含むすべての利用者ガイダンスに従う。	OE.TRAINED_USERSは、利用者が保護対象データの機密性を反映する十分な強度とエントロピーを持つパスワードを作成することを保証することで、この方針を満たす。

4 セキュリティ要件及び根拠

35 セキュリティ要件は、機能要件と保証要件に分割される。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、4.1 節の適用上の注意で提供される。4.2 節は、SFR からセキュリティ対策方針への必須の追跡である。

36 セキュリティ保証要件（SAR）は、通常、PP に挿入され、SFR とは別に記載される。次に、選択した SAR に基づいて、評価中に CEM が参照される。共通基準セキュリティ保証要件及び TOE として識別される具体的な技術の性質上、本 PP ではより柔軟に変更できる方法を採る。4.3 節では文脈と完全さのために SAR が記載されているが、この TOE で各 SFR と SAR に関して評価者が実行する必要があるほとんどのアクティビティは、「保証アクティビティ」の段落に詳述されている。保証アクティビティは、評価を実施するために行わなければならないアクティビティの正式の説明である。本 PP では、保証アクティビティを 2 か所で取り扱っている。特定の SFR に関連する保証アクティビティは 4.1 節で取り扱い、SFR に依存しない保証アクティビティは 4.3 節で取り扱う。なお、保証アクティビティは実際に柔軟に変更できる評価方法であり、読みやすさ、理解、及び便利のためにインライン方式で記載してある。

37 SFR に直接関連するアクティビティについては、SFR ごとに 1 つまたは複数の保証アクティビティが記載され、適合デバイスに必要な保証を達成するために実行する必要があるアクティビティが詳述されている。

38 SFR に依存しない活動が必要な SAR については、実施する必要がある追加の保証アクティビティと SAR に関連する具体的な保証アクティビティが記載された SFR へのポインタが 4.3 節に記載されている。

39 将来のプロテクションプロファイルでは、実際の製品評価から学習したレッスンに基づいて、より詳細な保証アクティビティが提供されるだろう。

4.1 セキュリティ機能要件

40 セキュリティ機能要件（SFR）は、TOE 用セキュリティ対策方針の翻訳である。通常は、より詳細なレベルの抽象化であるが、完全な翻訳でなければならない（セキュリティ対策方針を完全に取り扱わなければならない）。CC では、いくつかの理由で標準化された言語に翻訳することが必要である。

- 評価対象の正確な記述を提供するため。通常、TOE に関するセキュリティ対策方針が自然言語で作成されるため、標準化された言語に翻訳することで、TOE の機能のより正確な記述が強制される。
- 2 つの ST を比較できるようにするため。異なる ST 執筆者がセキュリティ対策方針を記述する際に異なる用語を使用する場合があるので、標準化された言語を使用することで同じ用語と概念の使用が強制される。そのため、比較が容易になる。

4.1.1 クラス：暗号サポート（FCS）

41 これらの機能要件で取り扱う主な脅威は、鍵空間に対するブルートフォース攻撃及び暗号コンポーネントの故障である。

42 暗号要件は、アルゴリズムを記述する規格を参照する。これらの規格のほとんどが NIST の Special Publication（800--xxx）または連邦情報処理規格（FIPS）から入手できる。保証要件は、これらの要件の実装を検証する方法を詳述する。スキームごとに、暗号保証アクティ

ビティを適合と見なすプロセスを特定するオプションがある。以下に規定するすべての暗号機能が、USB フラッシュドライブに実装されなければならない。

暗号鍵管理（FCS_CKM）

43 適合する実装には、鍵暗号鍵（KEK）及びデータ暗号鍵（DEK）の少なくとも 2 個の鍵が含まれる。以下の要件は、鍵の生成方法を規定する。DEK の生成は、FCS_CKM.1(1)に規定されている。KEK は、FCS_CKM.1(2)で説明されているように 1 つまたは複数の認証要素から導出したサブマスクから作成される。認証要素は、必要なパスワードベースの認証要素（サブマスクを生成するための条件付けは FCS_CKM.1(3)に規定されている）及び（オプションで）ホスト分割認証要素（FCS_CKM.1(X1)）及び/または PIN 保護方式のサブマスク（FCS_CKM.1(X2)）から構成される。KEK の形成に寄付するサブマスクが導出される他の認証要素は、前述の認証要素から導出されるサブマスクと（XOR 関数を使用して）組み合わされる限り許される。

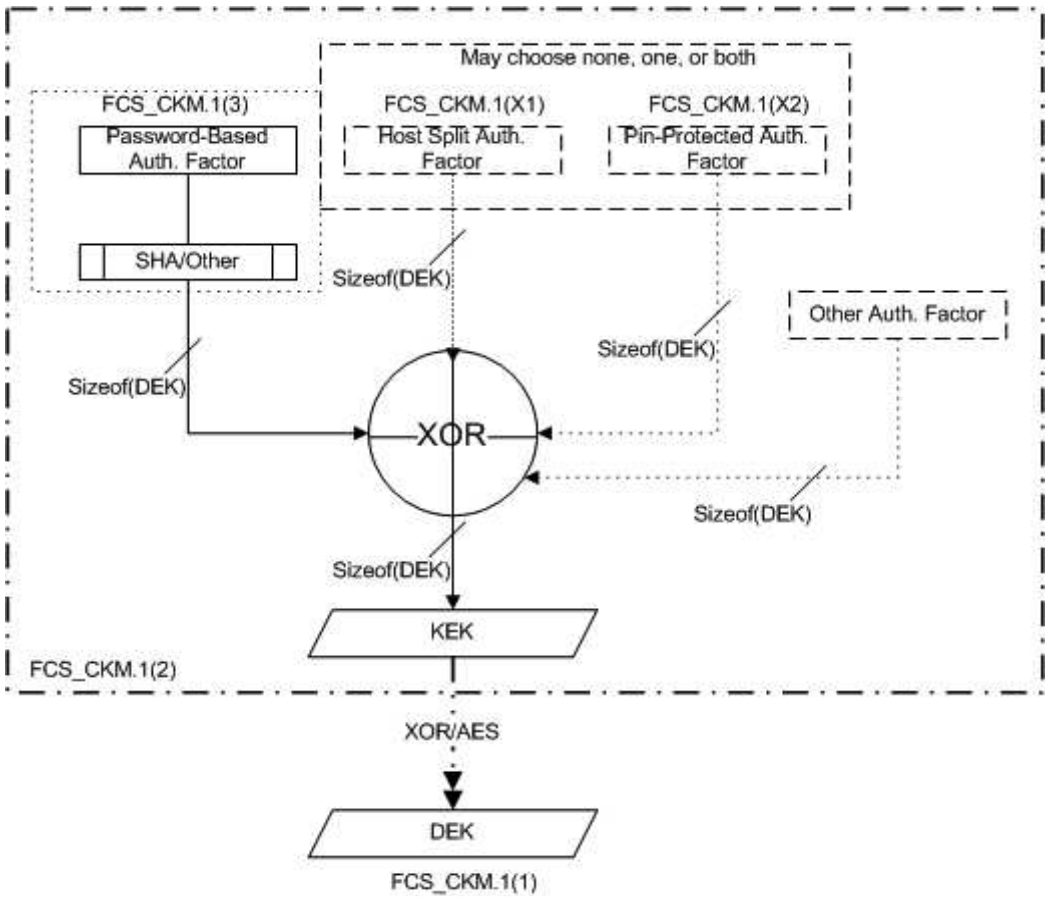

図 1：KEK 導出オプション

KEKを形成するために使用されるサブマスクを導出する際の認証要素の使用については、FCS_CKM.1(2)で取り扱われている。TOEは、（パスワードに加えて）ホスト分割またはPIN認証要素を使用してもよい。これらの認証要素がTOEによって使用される場合、STは、STの本文に「附属書Cの認証要素の生成」に記載されている該当する要件を使用するべきである。

以下にKEKとDEKの生成に関連する要件について説明する。

FCS_CKM.1(1) **暗号鍵生成（DEK）**

FCS_CKM.1.1(1) **詳細化**：TSFは、以下を満たす**FCS_RBG_EXT.1に規定されたランダムビット生成器**及び規定されている暗号鍵サイズ**[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**[規格なし]。**

適用上の注意：

44 この要件の意図は、DEK が AES の鍵空間の総当り以下の作業では回復できないことを保証することである。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（またはその両方）が許される。ST 執筆者は、デバイスに適したものを選択する。DEK は、デバイス上のすべての利用者データを再び暗号化せずに認証要素（特にパスワード認証要素）を変更できるように、KEK に加えて使用される。

保証アクティビティ：

45 評価者は、FCS_RBG_EXT.1 によって記述されている機能を呼び出す方法が TSS に記述されていることを決定するために、TSS をレビューする。FCS_RBG_EXT での RBG 機能の記述から可能な範囲で、評価者は、要求される鍵サイズが利用者データの暗号化/復号に使用される鍵のサイズとモードと同じであることを決定する（FCS_COP.1(1)）。

FCS_CKM.1(2) **暗号鍵生成（KEK）**

FCS_CKM.1.1(2) **詳細化**：TSFは、**以下の入力を持つ**規定された暗号鍵**導出**アルゴリズム**[選択：なし、排他的論理和（XOR）]**に従って、**KEK**暗号鍵を**導出**しなければならない。

FCS_CKM.1(3)に定義されている条件付けされたパスワード認証要素から導出されるサブマスク、

[選択、次のうち1つまたは複数：

なし、

ホスト分割認証要素（それ自体がサブマスク）、

PIN保護方式のサブマスク、

[選択、次のうち1つを選択：他の入力なし、[割付：他の認証要素及び以下を満たす**各認証要素の実効強度**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、FCS_CKM.1(1)に規定されているようにDEKと同じサイズのサブマスクを生成する関連付けられたサブマスク導出方法のリスト]]：[規格なし]。**

適用上の注意： これらの要件は、KEKを生成するために使用される認証要素を使用して、サブマスクを導出する方法を定義するためのものである。割付及び選択ごとにST執筆者に対する具体的なガイダンスを以下に提供するが、以下はこのコンポーネントの要点に関する高レベルの記述である。ST執筆者は、追加の認証要素を定義するオプションを含めて、TOEによってサポートされる（パスワードに追加する）認証要素を選択する。追加の認証要素を

定義する場合は、こ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。このような割付に課される唯一の条件は、生成されるサブマスクのサイズがDEKと同じサイズであることである。複数の認証要素の使用が望ましい。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結合しなければならない。

最初の選択では、パスワード認証要素のみを使用する場合、ST執筆者は「なし」を選択する。複数の認証要素を使用する場合、ST執筆者は「XOR」を選択する（他の結合方法は本PPに適合しない）。なお、XOR関数は、USBフラッシュドライブで実行されなければならない。

2番目の選択では、ST執筆者は使用されるオプションの認証要素を選択する。なお、複数の認証要素を選択できる。条件付けされたパスワードのほかに追加の認証要素を使用する場合、ST執筆者は、この2番目の選択のうち、選択の中にある割付を使用して、これらの要因を指定する（または「他の入力なし」を選択する）。ホスト分割認証要素またはPIN認証要素を選択する場合、ST執筆者は、選択した認証要素/サブマスクの生成に関する附属書Cからの該当する要件もSTに記載しなければならない。

暗号鍵のサイズの選択では、生成されるKEKのサイズが選択される。これは、FCS_CKM.1(1)でDEK用に指定したビット長と同じでなければならない。

なお、「規格なし」が必要なのは、ただ1つの認証要素を使用してKEKを形成する(その組成は他の場所で規定される）、またはXOR機能を使用してKEKが形成されるからである。

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には、TOEの要件の実装が文書化されていることを決定するために、STのTSSを検査することが伴う。評価者は、最初にTSS節を検査して、STに規定された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。パスワードベースの要因の場合、TSS節の検査は、FCS_CKM.1(3)保証アクティビティの一環として実行される。ホスト分割認証要素及びPIN認証要素については、これらが含まれる場合、そのサブマスク生成がTOEによって実行されるなら、附属書Cから取った保証アクティビティの一環としてサブマスク生成を検査してもよい。サブマスク生成がTOEによって実行されない場合は、その保存と検索のみを記述しなければならない。その保存と検索は、それらの要件に関する保証アクティビティの一環として検査される。

他の認証要素が指定される場合、TSSは、要因ごとに要因をTOEに入力する方法、（このプロセスが準拠するかもしれない関連規格を含めて）認証要素からサブマスクを生成する方法、及びサブマスクの長さが（この要件に規定された）必要なサイズを満たすことを保証するために実行される検証を指定する。

ただ1つの認証要素しかない場合は、当然、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がXOR演算を経てKEKを形成する場合、TSS節はその実行方法（例えば、順序付け要件があるかどうか、実行されるチェックなど）を示さなければならない。評価者は、生成される出力の長さがDEKの長さと同じであることがTSSに記述されていることも確認しなければならない。

- テスト 1[条件付き]：複数の認証要素がある場合は、必要な認証要素を提供しないと TOE にアクセスできないことを確認する。

FCS_CKM.1(3)　　暗号鍵生成（パスワードの条件付け）

FCS_CKM.1.1(3)　　**詳細化：サブマスクを生成するために使用されるパスワードは、{大文字、小文字、数字、及び次の特殊文字**："!"、"@"、"#"、"$"、"%"、"^"、"&"、"*"、"("、及び")"、及び[割付：サポートされる他の特殊文字]}**の集合の中から最大[割付：32以上の正整数個の]文字を含み、以下のように条件付けされなければならない。[選択：**

- **128ビットDEK用に[選択：SHA-1、SHA-256、SHA-512]を使用する、**
- **256ビットDEK用に[選択：SHA-256、SHA-512]を使用する、**
- **FCS_RBG_EXT.1で規定されているようにランダムビット生成器を使用して生成されるソルトでNIST SP 800-132、[割付：繰返しの数]の繰返しカウント、及び[選択：SHA-1、SHA-256、SHA-512]を使用するHMACを使用する、**

]これは、条件付け機能から出力されるサブマスクのサイズ（ビット数）がDEKのサイズに等しくなるようにするものである。

適用上の注意：　　パスワードは、ホストマシン上で文字の並びとして表現され、文字の符号化はTOE及び基礎となるOSに依存する。この並びは、KEKの入力として使用されるサブマスクを形成するビット列に条件付けされなければならない。条件付けは、識別されるハッシュ関数のいずれか、またはNIST SP 800-132に記載されているプロセスを使用して実行できる。使用する方法は、ST執筆者によって選択される。 800-132条件付けを指定する場合、ST執筆者は実行される繰返しの数（C）を入力する。この値は、10000以上でなければならない。また、800-132では、承認されたハッシュ関数を持つHMACから構成される擬似ハッシュ関数（PRF）の使用が要求される。ST執筆者は、附属書CからのHMAC及びハッシュ関数に関する該当する要件も含めて、使用されるハッシュ関数を選択する。

通常、利用者が記憶できる長さが短いパスワードは、基礎となるKEK/DEKと同じ「強度」を提供するために十分な長さがないため、KEKのエントロピー源としては劣っている。ただし、本書の執筆時点ではこれが最も便利な認証要素であるため、パスワードは唯一の認証要素として許される。おそらく、本PPの将

来の版では、基礎となる鍵強度と同等の十分なエントロピーを含んでいるパスフレーズが要求されるだろう。

USBフラッシュドライブは、鍵導出機能（または800-132に規定された条件付けによって要求される暗号操作）によって要求されるハッシュ関数を実装しなければならないことに注意するべきである。

おそらく、本PPの今後の刊行では、SHA-1は暗号ハッシュに承認されるアルゴリズムではなくなり、SP 800-132を使用した条件付けが要求されるだろう。

保証アクティビティ：　このコンポーネントには、評価が必要な2つの側面がある。32文字以上のパスワードがサポートされる。入力する文字は、選択した条件付け機能に支配される。これらのアクティビティについては、以下で個別に取り扱う。

32文字のパスワードの長さのサポート

評価者は、この割付文の中のSTに指定されている最大文字数のパスワードを受け付ける機能が存在することがTSS節に指定されており、指定されている値が32以上であることを決定するために、TSS節をチェックしなければならない。また、評価者は、このようなパスワードを生成する管理者用の指示が存在し、パスワードをTOEに入力する方法がガイダンスに記載されていることを決定するために、運用ガイダンスもチェックしなければならない。

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で以下のテストも実行しなければならない。

- テスト1：TOEが、最大32及び最初の割付に関してSTに指定された値に等しい文字長を持つパスワードをサポートすることを確認する。
- テスト2：TOEが、ベンダから提供される運用ガイダンスに規定されている内容と一致する短い長さのパスワードをサポートすることを確認する（例えば、ガイダンスにパスワードの長さが16文字以上と規定されている場合、このテストではTOEが最低でも16文字のパスワードを受け付けることを決定する）。
- テスト3：TOEが、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ているように構成されたパスワードのサポートを備えていることを確認する。例えば、パスワードが特殊文字を含まなければならないとガイダンスに規定されている場合、このテストはTOEが英数字しかサポートしていない場合に失敗する。

パスワード条件付け

SHAベースのパスワード条件付けについては、評価者は以下のアクティビティを実行する。評価者は、最初にパスワードを符

号化し、それからSHAアルゴリズムに渡す方法がTSSに記載されていることをチェックしなければならない。アルゴリズムの設定値（パディング、ブロッキングなど）が記述されなければならず、評価者は、これらがこのコンポーネントでの選択及びハッシュ関数自体に関するFCS_COP.1(3)での選択によってサポートされることを検証しなければならない。評価者は、ハッシュ関数の出力を使用してFCS_CKM.1(2)に記載されている関数に入力されるサブマスクを形成する方法の記述がTSSに含まれており、FCS_CKM.1(1)に規定されているようにDEKと同じ長さであることを検証しなければならない。

800-132ベースのパスワード条件付けについては、必要な保証アクティビティは、該当する附属書C要件の保証アクティビティを実行するときに実行される。KEKを形成するために使用されるサブマスクを形成するときにマスター鍵の操作が実行される場合は、そのプロセスをTSSに記載しなければならない。

入力されるパスワードからのサブマスクの形成を明示的にテストする必要はない。

FCS_CKM.2 **暗号鍵配付（高信頼更新）**

FCS_CKM.2.1 **詳細化**：TSFは、以下を満たす規定された暗号鍵配付方法*USBフラッシュドライブ上のシステムファイル*に従って、**TOEシステムファイルの更新を検証するために使用される公開鍵**を配付しなければならない。*規格なし*。

適用上の注意： システムファイルの更新プロセス中に更新の検証に使用される公開鍵は、USBフラッシュドライブに配付されなければならない。

保証アクティビティ： この要件の検証に関連するアクティビティは、FPT_SFP_EXT.1及びFPT_TUD_EXT.1に関する保証アクティビティに含まれる。これ以上の保証アクティビティは要求されない。

暗号操作（FCS_COP）

FCS_COP.1(1) **暗号操作（データ暗号化）**

FCS_COP.1.1(1) **詳細化**：TSFは、以下を満たす**[選択：CBC、CCM、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、規定された暗号アルゴリズムAESに従って、**データの暗号化と復号**を実行しなければならない。**FIPS PUB 197、「Advanced Encryption Standard(AES)」及び*選択：NIST SP 800-38A、NIST SP 800-38C、NIST SP 800-38E]**。

適用上の注意：

46 この要件の意図は、ST 執筆者が USB フラッシュドライブ上の該当する情報の AES 暗号化に選択できる、承認された AES モードを規定することである。最初の選択では、ST 執筆者は、TOE 実装によってサポートされているモードを指定するべきである。2 番目の選択は、使用される鍵サイズを指定する。これは、FCS_CKM.1(1)用に規定されている鍵サイズと同じ

である。3 番目の選択は、最初の選択で選んだモードと一致しなければならない。複数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、複数モードがサポートされることが ST でより明確になる。

47 本 PP の将来の版では、NIST によってレビューされ、承認されるときに、新しい暗号モードが含まれることがある。

保証アクティビティ：

48 複数のモードがサポートされる場合、評価者は、最終利用者が特定のモード/鍵サイズを選択する方法を決定するために、TSS とガイダンス文書を検査する。次に、評価者は、適宜、以下の節に記載されている方法で各モード/鍵サイズの組合せをテストする。なお、これらのテストの一部では、評価施設のスキームが受け入れることができるアルゴリズムの参照実装が要求される。

CBC モード

49 CBC モードテストに関する参考文献は *The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)* [AESAVS]であり、これは http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf から入手できる。

50 評価者は、TSF によってサポートされる鍵サイズごとに、1 組の答えがわかっているテストを実行する。入力は、鍵、IV、及び暗号化される平文または復号される暗号文のいずれかである。http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip からサポートされる鍵の長さにある CBC モード用のすべてのテストベクター（暗号化及び復号の両方）を使用して、これらのテストを実行しなければならない。

51 評価者は、サポートされる鍵の長さごとにマルチブロックメッセージテストを実行しなければならない。このテストを実行するために、評価者は、暗号化用に 10 のデータセットと復号用に 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（暗号化用）または暗号文（復号用）から構成される。ブロックの長さは、128 ビットでなければならない。平文/暗号文の長さは、ブロックの長さ*i でなければならない。ここで、i はデータセット番号を表し、1～10 の範囲にある（したがって、メッセージは 128 ビットから 1280 ビットの範囲にある）。

52 評価者は、モンテカルロテストを実行しなければならない。評価者は、暗号化用に 10 組の開始値（鍵、IV、及び平文の値）を生成し、復号用に 10 組の開始値（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。各組の開始値を使用して 100 個のテストが生成され、実行される。（開始値の組ごとに）100 個のテスト値を生成するためのアルゴリズムは[AESAVS]の 6.4.2 節に記載されている。

CCM モード

53 CCM モードテストに関する参考文献は The CCM Validation System (CCMVS) [CCMVS]であり、これは http://csrc.nist.gov/groups/STM/cavp/documents/mac/CCMVS.pdf から入手できる。

54 評価者は、ペイロード、関連データ、ナンス、タグの長さ（及び鍵の長さ）が指定されていることを確認するために、TSS を検査しなければならない。これらの値は、次の節で記述するテストの作成に使用されなければならない。複数の値がサポートされる場合、評価者は、利用者が値を選択する方法を決定するために、運用ガイダンスを検査しなければならない。

55 評価者は、USB フラッシュドライブによってサポートされる鍵の長さごとに以下の 5 つのテストを実行しなければならない。

56 評価者は、可変関連データテストを実行しなければならない。サポートされる関連データの長さごとに、評価者は、10 組の入力データを考案しなければならない。各組の入力データは、同じ鍵とナンスを使用し、同じタグ（MAC）長を持たなければならない。10 組のそれぞれについて、関連データとペイロードデータの一意の文字列を使用しなければならない。評価者は、入力用の正しい暗号文を計算し、それから TSF がサポートされるすべての関連データ長についてすべての入力セットに対して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 ビット鍵用）は、
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip アーカイブにある VADT256.txt ファイルに含まれている。

57 評価者は、可変ペイロードテストを実行しなければならない。サポートされるペイロードの長さごとに、評価者は、10 組の入力データを考案しなければならない。各組の入力データは、同じ鍵とナンスを使用し、同じタグ（MAC）長を持たなければならない。10 組のそれぞれについて、関連データとペイロードデータの一意の文字列を使用しなければならない。評価者は、入力用の正しい暗号文を計算し、それから TSF がサポートされるすべてのペイロード長についてすべての入力セットに対して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 ビット鍵用）は、
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip アーカイブにある VPT256.txt ファイルに含まれている。

58 評価者は、可変ナンステストを実行しなければならない。サポートされるナンスの長さごとに、評価者は、10 組の入力データを考案しなければならない。各組の入力データは、同じ鍵を使用し、同じタグ（MAC）長を持たなければならない。10 組のそれぞれについて、一意のナンス及び関連データとペイロードデータの一意の文字列を使用しなければならない。評価者は、入力用の正しい暗号文を計算し、それから TSF がサポートされるすべてのナンス長についてすべての入力セットに対して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 ビット鍵用）は、
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip アーカイブにある VNT256.txt ファイルに含まれている。

59 評価者は、可変タグテストを実行しなければならない。サポートされるタグの長さごとに評価者は、10 組の入力データを考案しなければならない。各組の入力データは、同じ鍵とナンスを使用しなければならない。10 組のそれぞれについて、関連データとペイロードデータの一意の文字列を使用しなければならない。評価者は、入力用の正しい暗号文を計算し、それから TSF がサポートされるすべてのタグ長についてすべての入力セットに対して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 ビット鍵用）は、
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip
アーカイブにある VTT256.txt ファイルに含まれている。

60 評価者が実行しなければならない最後のテストは、復号検証プロセステストである。このテストは、TSF によってサポートされる関連データ長、ペイロード長、ナンス長、及びタグ長の組合せごとに実行される。組合せごとに、15 組の入力データが TSF に提供される。入力データは、鍵、関連データ、ペイロードデータ、ナンス、及び暗号文から構成される。評価者は、暗号文の 1/3～2/3 の値が様々なエラータイプにより、MAC チェックに合格しないことを確認するべきである。入力が TSF に提供され、評価者は、TSF が合格値だけでなく、エラーのある MAC 値を正しく識別することを検証する。入力セットの例（256 ビット鍵用）は、
http://csrc.nist.gov/groups/STM/cavp/documents/mac/ccmtestvectors.zip

アーカイブにある VTT256.txt ファイルに含まれている。

XTS モード

61 XTS モードテストに関するの参考文献は The XTS-AES Validation System (XTSVS) [XTSVS]であり、これは http://csrc.nist.gov/groups/STM/cavp/documents/aes/XTSVS.pdf から入手できる。

62 評価者は、最初に上記の CBC モードの節に記載されているテストを実行する。それらのテストが完了したら、評価者は、XTS モードでサポートされている範囲のデータ長が指定されていることと調整値（128 ビット列またはデータ単位順序番号）のフォーマットを確認するために、TSS を検査する。

63 次に、評価者は、サポートされる鍵の長さごとに、テストセットを考案する。ある鍵の長さについて、評価者は、テストする 5 つ以上のデータ長のサンプルを選択する。鍵の長さごとに、評価者は、100 個の暗号化テストと 100 個の復号テストを考案する。各テストは、一意の鍵、調整、及び平文（暗号化用）または暗号文（復号用）の値で実行される。テストセットの例は、http://csrc.nist.gov/groups/STM/cavp/documents/aes/XTSTestVectors.zip に含まれている。

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**を実行しなければならない。**[選択**：

(1) 鍵サイズ（法）が2048ビット以上のデジタル署名アルゴリズム（DSA）、

(2) 鍵サイズ（法）が2048ビット以上のRSAデジタル署名アルゴリズム（rDSA）、または

(3) 鍵サイズ（法）が256ビット以上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：

- **IPS 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」**
- **SF は、(FIPS PUB 186-3、「Digital Signature Standard」に定義されている通り）「NIST曲線」 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：

64 ST 執筆者は、デジタル署名を実施するよう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(及び関連する FCS_CKM.1(2)要件）は、機能性を特定するために繰り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 執筆者は適切な割付／選択を行い、そのアルゴリズムについて実装されたパラ

メタを特定するべきである。

65 楕円曲線に基づくスキームに関して、鍵サイズは *base point* の位数の *log2* をとった値を意味する。デジタル署名の望ましいアプローチとして、必要なすべての規格及び他の補足情報が完全に確立された後で、楕円曲線が要求されるだろう。

保証アクティビティ：

66 この要件は、TOE に更新をインストールする前に、TOE 製造者か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される。このコンポーネントは更新機能で使用されるため、下記の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取り扱う。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。評価者は、コンポーネント内で選択されるアルゴリズムに該当するテストを実行する。

67 これらのアルゴリズムによって要求されるハッシュ関数または乱数生成は、USB フラッシュドライブに装備され、それらの関数に関連する保証アクティビティは、このコンポーネントに続く暗号ハッシュ及びランダムビット生成の節に記載されている。また、TOE によって要求される唯一の機能は、デジタル署名の検証である。本 PP によって要求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、必要な保証アクティビティを決定するために、その件に詳しい評価及び検証機関（スキーム）に相談しなければならない。

68 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、署名検証の全体的な流れが TSS に記載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を検証する場合に使用されるデータのフォーマットと一般的位置（例えば、「USB デバイス上のファームウェア」、「メモリ位置 0x00007A4B」など）の識別、運用環境からデータを受信する方法をデバイスに提供する方法、及びデジタル署名アルゴリズムには含まれないが、実行される処理（例えば、証明書失効リストのチェック）を含めるべきである。

69 以下の各節では、デジタル署名スキームのタイプごとに評価者が実行しなければならないテストを示す。要件で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具体的なアクティビティを選択する。デジタル署名スキームのタイプごとに、FIPS 186-3 及び FIPS 186-2 に適合するためのテストの節が提供されている。

70 なお、下記のスキームでは、鍵生成/ドメインパラメタ生成のテスト要件がないことに注意するべきである。それは、この機能が、配付される更新内のデジタル署名のチェックに制限されるため、エンドデバイスに必要とは想定されないからである。すなわち、ドメインパラメタは既に生成され、USB フラッシュドライブのファームウェアまたは搭載された不揮発性ストレージにカプセル化されているはずである。鍵生成/ドメインパラメタ生成が要求される場合は、評価及び検証機関（スキーム）に相談して、必要な保証アクティビティ及び追加コンポーネントの正しい仕様を確認しなければならない。

71 同様に、本 PP の基底要件を満たすために署名生成が要求されることは想定されない。署名生成が要求される場合は、評価及び検証機関（スキーム）に相談して、必要な保証アクティビティ及び追加コンポーネントの正しい仕様を確認しなければならない。

RSA

72 署名生成/検証機能を実装する場合は、ANSI X9.31 及び PKCS #1（バージョン 1.5 及び/またはバージョン PSS）という 2 つのオプションがある。少なくともこれらのオプションのいずれかを実装しなければならない。実装された各バージョンは、下記のようにテストされなければならない。PKCS#1 バージョン PSS が選択される場合、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。

73 TOE が複数の法サイズをサポートする場合、評価者は、すべての法サイズについて次のテストを実行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ついて次のテストを実行しなければならない。すなわち、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される場合、評価者は、次のテストを 4 回実行することになる。

74 評価者は、3 つのデータグループを生成する。各データグループは 1 つの法から構成され、その法と共に 4 組のテストベクターが構成される。テストベクターは、公開指数 e、擬似ランダム生成メッセージ、及び（e 及び法 n と一貫した）関連の秘密鍵を使用するメッセージ用署名から構成される。すなわち、TSF によってサポートされる法サイズハッシュアルゴリズムごとに最低でも 12 個のテストベクターが存在する。

75 正しい署名が生成された（ただし TSF には「提供」されない）後で、評価者は、署名検証失敗機能がテストされるように、テストベクターの 3/4 において、公開鍵、メッセージ、または署名を変更する（必ずそれぞれ 2 回以上行う）。次に、評価者は、TSF を通じ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。

76 加えて、実装されたアルゴリズムが「*Public Key Cryptography Standards (PKCS) #1 v2.1:RSA Cryptography Standard-2002*」に規定されている 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 Version 1.5 を実装の場合）または、
http://csrc.nist.gov/groups/STM/cavp/documents/dss/SigVer931IRTest.zip（X9.31 を実装の場合）からの該当する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合格することを検証しなければならない。

DSA

77 評価者は、（L, N）に使用される値が与えられ、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ために、TSS を検査する。 評価者は、SP 800-57「*Recommendation for Key Management --Part I:General (Revised)*」の 5.6.1 節の表 2 と表 3 に規定されているように、特定の（L,N）に使用されるハッシュアルゴリズムが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で使用される対称（データ）暗号化アルゴリズムに相当する強度を備えていることを確認しなければならない。例えば、利用者データを暗号化するために 128 ビット AES を使用する場合は、少なくとも（3072,256）の（L,N）が要求される）。

78 評価者は、サポートされる（L,N）とハッシュの組合せごとに次のテストを実行する。評価者は、鍵ペアを生成しなければならない。評価者は、擬似ランダム的に 15 個の 1024 ビットメッセージを生成し、秘密鍵でメッセージに署名する。正しい署名が生成された（ただし TSF には「提供」されない）後で、評価者は、署名検証失敗機能がテストされるように、メッセージの約半数について、公開鍵、メッセージ、または署名を変更する（必ずそれぞれ 2 回以上行う）。次に、評価者は、TSF を通じ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

79 評価者は、実装に使用される曲線が指定され、サポートされるハッシュが指定されていることを決定するために、TSS を検査しなければならない。評価者は、TSF によって実装される曲線、ハッシュペアごとに次のテストを実行しなければならない。

80 評価者は、15 組のデータを生成する。各データセットは、擬似ランダムメッセージ、公開/秘密鍵ペア（d,Q）、及び署名（r,s）から構成される。正しい署名が生成された（ただし TSF には「提供」されない）後で、評価者は、署名検証失敗機能がテストされるように、メッセージの約半数について、公開鍵、メッセージ、または署名を変更する（必ずそれぞれ 2 回以上行う）。次に、評価者は、TSF を通じてデータを実行し、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、以下に合致する［**選択**：**SHA-1、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、256、384、512**］**ビット**に従って、**暗号ハッシュサービス**を実施しなければならない：***FIPS Pub 180-3*、「*Secure Hash Standard*」**

適用上の注意：

81 この要件の意図は、高信頼更新及びシステムファイル保護に関連するデジタル署名チェック、及びパスワードの条件付けにおいて使用されるハッシュ関数を規定することである（FCS_CKM.1(3)を参照)。ハッシュ選択は、メッセージダイジェストサイズ選択をサポートしなければならない。ハッシュ選択は、FCS_COP1(1)及び FCS_COP.1(2)用に使用されるアルゴリズム（128 ビット鍵の場合は SHA 256、256 ビット鍵の場合は SHA 512）の全体的強度と一貫しているべきである。おそらく、本 PP の今後の刊行では、SHA-1 は暗号ハッシュに承認されるアルゴリズムではなくなるだろう。

保証アクティビティ：

82 評価者は、必要なハッシュサイズ用の機能を設定するために行う必要がある設定が存在することを決定するために、AGD 文書をチェックする。評価者は、ハッシュ関数とその他の TSF 暗号機能（例えばデジタル署名検証機能）の関連性が TSS に記載されていることをチェックしなければならない。

83 暗号ハッシュテストに関する参考文献は The Secure Hash Algorithm Validation System (SHAVS) [SHAVS]であり、これは http://csrc.nist.gov/groups/STM/cavp/documents/shs/SHAVS.pdf から入手できる。

84 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。最初のモードは、バイト指向モードである。このモードでは、TSF は、長さが整数バイトであるメッセージのみをハッシュする。すなわち、ハッシュ対象メッセージの長さ（ビット単位）は 8 で割り切れる。2 番目のモードは、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。モードごとに異なるテストがあるため、以下の節ではビット指向テストとバイト指向テストの区別を明記する。

85 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使用されるハッシュアルゴリズムごとに、以下のすべてのテストを実行しなければならない。

短いメッセージテスト　－　ビット指向モード

86 評価者は、m+1 個のメッセージ（m はハッシュアルゴリズムのブロック長)から構成される入力セットを考案する。メッセージの長さは、順番に 0～*m* ビットの範囲にある。メッセージ文は、擬似ランダム的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計算し、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。

短いメッセージテスト　－　バイト指向モード

87 評価者は、*m/8*+1 個のメッセージ（m はハッシュアルゴリズムのブロック長）から構成される入力セットを考案する。メッセージの長さは順番に 0～m/8 バイトの範囲にあり、各メッセージは整数バイトである。メッセージ文は、擬似ランダム的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計算し、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。

選択された長いメッセージテスト　－　ビット指向モード

88 評価者は、*m* 個のメッセージ（*m* はハッシュアルゴリズムのブロック長）から構成される入力セットを考案する。*i* 番目のメッセージの長さは、512 + 99**i*（ただし $1 \le i \le m$）である。メッセージ文は、擬似ランダム的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計算し、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。

選択された長いメッセージテスト　－　バイト指向モード

89 評価者は、*m/8* 個のメッセージ（*m* はハッシュアルゴリズムのブロック長）から構成される入力セットを考案する。*i* 番目のメッセージの長さは、512 + 8*99**i*（ただし $1 \le i \le m/8$）である。メッセージ文は、擬似ランダム的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計算し、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。

擬似ランダム的に生成されるメッセージテスト

90 このテストはバイト指向実装専用である。評価者は、*n* ビット長のシードをランダムに生成する（*n* は、テストされる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）。次に、評価者は、[SHAVS]の図 1 に提供されているアルゴリズムに従って、1 組の 100 個のメッセージ及び関連ダイジェストを作成する。次に、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（鍵マスキング）**
FCS_COP.1.1(4)	**詳細化**：TSFは、以下を満たす規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、**鍵マスキング**を実行しなければならない。**FIPS PUB 197、*Advanced Encryption Standard (AES)*及びNIST SP 800-38A" for AES+**。

適用上の注意：

91 最初の選択では、ST 執筆者は、KEK を使用して DEK をマスクする方法を選択する。方法は、KEK と DEK の XOR 演算、または ECB モードでの AES の使用のいずれかである。XOR を選択する場合、ST 執筆者は、最後の選択で「なし」を選択する。そうでない場合は、FIPS 197 及び SP 800-38A への参照を選択する。KEK のサイズを反映するために、2 番目の選択を行うべきである。

保証アクティビティ：

92 DEK マスキング方法で「XOR」が使用されている場合、評価者は、XOR の使用が TSS に記載されていることを検証しなければならない。AES が使用される場合は、以下の保証アクティビティが実行される。

93 評価者は、ベンダが KEK を使用して AES を使用する DEK をマスクする方法/アルゴリズムを記述している(例えば、FIPS 文書に規定されているオプション、入力を埋め込む方法、出力を切り詰める方法などが指定されている）ことを確認しなければならない。

94 評価者は、以下のテストを実行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、最終利用者が ECB 及び指定された鍵サイズを選択する方法を決定するために、TSS とガイダンス文書を検査する。次に、評価者は、適宜、以下の節に記載されている方法で各鍵サイズをテストする。なお、これらのテストの一部では、評価施設のスキームが受け入れることができるアルゴリズムの参照実装が要求される。

ECB モード

95 ECB モードテストに関する参考文献は The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) [AESAVS]であり、これは http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf から入手できる。

96 評価者は、TSF によってサポートされる鍵サイズごとに、1 組の答えがわかっているテストを実行する。入力は、鍵及び暗号化される平文または復号される暗号文のいずれかである。http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip からサポートされる鍵の長さにある ECB モード用のすべてのテストベクター（暗号化及び復号の両方）を使用して、これらのテストを実行しなければならない。

97 評価者は、サポートされる鍵の長さごとにマルチブロックメッセージテストを実行しなければならない。このテストを実行するために、評価者は、暗号化用に 10 のデータセットと復号用に 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（暗号化用）または暗号文（復号用）から構成される。ブロックの長さは、128 ビットでなければならない。平文/暗号文の長さは、ブロックの長さ*i でなければならない。ここで、i はデータセット番号を表し、1～10 の範囲にある（したがって、メッセージは 128 ビットから 1280 ビットの範囲にある）。

98 評価者は、モンテカルロテストを実行しなければならない。評価者は、暗号化用に 10 組の開始値（鍵及び平文の値）を生成し、復号用に 10 組の開始値（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。各組の開始値を使用して 100 個のテストが生成され、実行される。（開始値の組ごとに）100 個のテスト値を生成するためのアルゴリズムは[AESAVS]の 6.4.1 節に記載されている。

拡張：暗号操作（ランダムビット生成）（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、[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）]を使用するNIST Special Publication 800-90、FIPS Pub 140-2 Annex C、AESを使用するX9.31 Appendix 2.4]に従って、少なくとも1個の独立したTSFハードウェアに基づく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シードされた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	決定性RBGは、少なくともそれが生成する鍵と認証要素の最も大きいビット長に等しい、最低でも[選択、1つを選択：128ビ

ット、256ビット]のエントロピーによってシードされなければならない。

適用上の注意：

99 IST Special Pub 800-90、Appendix C には、おそらく FIPS-140 の将来の版で要求されるであろう最小エントロピー値が記載されている。可能であれば、これをただちに使用するべきであり、本 PP の将来の刊行で要求されるだろう。

100 FCS_RBG_EXT.1.1 の最初の選択では、ST 執筆者は、RBG サービスが適合する規格（800-90 または 140-2 Annex C のいずれか）を選択するべきである。

101 SP800-90 には、4 つの異なる乱数生成方法が含まれている。各方法は、基礎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 執筆者は、使用される関数を選択し（800-90 が選択される場合）、使用される特定の基礎となる暗号プリミティブを要件または TSS に記載する。Hash_DRBG または HMAC_DRBG については指定されたハッシュ関数（SHA-1、SHA-224、SHA-256、SHA-384、SHA-512）が許されるが、CT_DRBG については AES に基づく実装のみが許される。Dual_EC_DRBG については 800-90 に定義されている任意の曲線が許されるが、ST 執筆者は選択した曲線を記載するだけでなく、使用されるハッシュアルゴリズムも記載しなければならない。

102 なお、現在 FIPS Pub 140-2 Annex C では、*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 に記載されている方法のみが有効である。ここで AES 実装に使用された鍵長が利用者データを暗号化するために使用される鍵長と異なる場合は、異なる鍵長を反映するために FCS_COP.1 を調整するか、繰り返さなければならないことがある。FCS_RBG_EXT.1.2 における選択では、ST 執筆者は、RBG をシード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。

103 また、ST 執筆者は、TOE の基底要件に基礎となる関数が含まれていることを確認する。

104 将来は、*A Method for Entropy Source Testing:Requirements and Test Suite Description* に記載されているほとんどの要件が、本 PP によって要求されるだろう。現在、以下の保証アクティビティは、要求されるアクティビティの部分集合のみを反映している。

保証アクティビティ：

105 評価者は、TOE で使用される RBG を含んでいる製品のバージョン番号を決定するために、TSS 節をレビューする。また評価者は、エントロピーが収集されるハードウェアベースのノイズ源が TSS に記載されていることと、このノイズ源が USB フラッシュドライブに搭載さ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、RBG に使用されるすべての基礎となる関数とパラメタが TSS に記載されていることを検証する。

106 評価者は、エントロピー入力を取得する方法、使用されるエントロピー源を識別する方法、各エントロピー源からエントロピーを生成し、収集する方法、及び各エントロピー源によって生成されるエントロピーの量など、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、エントロピー源ヘルステスト、エントロピー源のヘルスを決定するためにヘルステストが十分である根拠、及びエントロピー源の故障の既知のモードが TSS に記載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検証しなければならない。

107 RBG が適合を主張する規格にかかわらず、評価者は次のテストを実行する。

- 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源のエントロピー見積りを決定する。評価者は、すべてのエントロピー源から得られるすべての結果の最小値であるエントロピー見積りが、TSS に含まれていることを確認しなければならない。

108 また、評価者は、RBG が適合する規格に応じて、以下のテストを実行しなければならない。

FIPS 140-2、Annex Cに適合する実装

109 本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、以下の 2 つのテストを実行しなければならない。なお、「期待値」は、正しいと知られているアルゴリズムの標準実装により生成される。正しさの証明は各認証機関（スキーム）に任されている。

110 評価者は、可変シードテストを実行しなければならない。評価者は、TSF RBG 機能に対する 128 ペア（シード、DT）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 ペア（シード、DT）に対して一定の値の（AES アルゴリズムについて適切な長さの）鍵を提供しなければならない。DT の値は、それぞれのセットについて 1 ずつ増加される。セットの中で、シードの値は重複してはならない。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。

111 評価者は、モンテカルロテストを実行しなければならない。このテストでは、それぞれ 128 ビットの初期シードと DT 値を TSF RBG 関数に与える。また、評価者は、テストを通して一定の値の（(AES アルゴリズムについて適切な長さの）鍵を提供しなければならない。評価者は、（毎回）DT の値を 1 ずつ増加させつつ、TSF RBG を 10000 回呼び出して、次の繰り返しで使用される新しいシードは、*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 で指定されるように生成される。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

112 評価者は、RBG 実装について、15 回試行を実施しなければならない。もし、RBG が設定変更可能であれば、評価者は設定ごとに 15 回試行を行わなければならない。また、評価者は、RBG 機能性を設定変更するために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。

113 RBG が予測耐性を備えている場合、それぞれの試行は(1)drbg の具体化、(2)ランダムビット列の 1 番目のブロックの生成、(3)ランダムビット列の 2 番目のブロックの生成、(4)終了処理（ゼロ化）、から成り立つ。評価者は、ランダムビット列の 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、整数カウンタ（0-14）である。次の 3 つは、具体化操作のためのエントロピー入力、ナンス（Nonce）、及び個別化文字列である。次の 2 つは、（乱数）生成の初回の呼び出しについての追加入力とエントロピー入力である。最後の 2 つは、（乱数）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。「ランダムビット列の 1 ブロックを生成する」とは、（NIST SP 800-90 で定義された）出力ブロック長に等しい返されたビット数のランダムビット列を生成するという意味である。

114 RBG が予測耐性を備えていない場合、それぞれの試行は(1)drbg の具体化、(2)ランダムビット列の 1 番目のブロックの生成、(3)初期化、(4)ランダムビット列の 2 番目のブロックの生

成、(5)終了処理（ゼロ化）、から成り立つ。評価者は、ランダムビット列の 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、整数カウンタ（0-14）である。次の 3 つは、具体化操作のためのエントロピー入力、ナンス（Nonce）、及び個別化文字列である。5 番目の値は、初回生成呼び出しへの追加入力である。6 番目と 7 番目は、再シード呼び出しへの追加入力及びエントロピー入力である。最後の値は、2 番目の生成呼び出しへの追加入力である。

115 次の段落は、評価者によって生成／選択される入力値のいくつかについての詳細情報を含んでいる。

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

117 **ナンス（Nonce）**：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。

118 **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、実装がある個別化文字列の長さのみをサポートするなら、両方の値について同じ長さが利用可能である。もし、複数の長さの文字列がサポートされているなら、評価者は 2 つの異なる長さの個別化文字列を使用しなければならない。もし、実装が個別化文字列を使用しないなら、値を提供する必要はない。

119 **追加入力**：追加入力文字列のビット長は、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）

120 このファミリは、保存されるすべての利用者データの暗号化を要求する。

拡張：USBフラッシュドライブ上のデータの保護（FDP_DSK_EXT）

FDP_DSK_EXT.1	**拡張：USBフラッシュドライブ上のデータの保護**
FDP_DSK_EXT.1.1	TSFは、FCS_COP.1.1(1)に従って、利用者データの暗号化を実行しなければならない。
FDP_DSK_EXT.1.2	DEKは、FCS_CKM.1(2)及びFCS_COP.1(4)に規定されているように導出されるKEKでマスクされる場合、USBフラッシュドライブ上の永続メモリのみに存在しなければならない。
FDP_DSK_EXT.1.3	TSFは、利用者の介入なしにすべての利用者データを暗号化しなければならない。
FDP_DSK_EXT.1.4	USBフラッシュドライブの保護領域に書き込まれるPIN保護方式のサブマスクを除き、TOEによって使用される平文鍵関連情報は、USBフラッシュドライブ上の永続メモリに書き込まれなければならない。

適用上の注意：

121 「データ暗号化」は、本 PP の用語では「USB フラッシュドライブに書き込まれるすべての利用者データを暗号化するプロセス」と定義される。

122 この要件の意図は、利用者データの暗号化がそれらのデータを保護しようとする利用者に依存しないことを規定することである（例えば、ファイル単位の暗号化スキームは許容されない）。データ暗号化は利用者には透過的に実行され、データを保護する決定は利用者の裁量外である。

123 USB フラッシュドライブ上の領域に保存される、フラッシュドライブの正常動作に必要なデータとファイルも保護されなければならない。これは、FPT_SFP_EXT によって取り扱われる。

保証アクティビティ：

124 評価者は、この要件に関する保証アクティビティを実行するとき、ST の TSS を参照しなければならない。評価者は、データをデバイスに書き込む方法と暗号化関数を適用するポイントの記述が包括的であることを確認することに集中する。

125 レビューを行う際、評価者は、認証要素を生成するために使用される情報を利用者から収集するソフトウェアの読み込みに関連する USB フラッシュドライブの挿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決定しなければならない。また、TSS は、TOE の初期化、及び TOE が最初に確立されるとき、USB フラッシュドライブが完全に暗号化されていることを確認するために実行されるアクティビティを取り扱うべきである。TOE によってオプションの認証要素がサポートされる場合、評価者は、これらの認証要素を入手する方法、及びこれらの認証要素からサブマスクを導出する方法が TSS に記載されていることをチェックしなければならない。

126 評価者は、DEK のマスクを解除し、TOE に保存する方法など、FCS 要件で暗号機能がどのように使用されるいるかについても、記述に含まれていることを確認しなければならない。

127 評価者は、鍵関連情報が平文の形で USB フラッシュドライブに書き込まれないことを決定するために TSS をレビューする。通常の使用では USB フラッシュドライブへのすべての書き込みが暗号化されるため、1 つの方法として、データがデバイスの暗号化されていない部分に書き込まれる例外事例に関する議論を行い、鍵関連情報がこれらの領域に書き込まれない理由を詳述することである。

128 評価者は、以下のテストアクティビティを実行しなければならない。

- テスト1：初期化アクティビティに従うと、USBフラッシュドライブが暗号化されることを確認する。暗号化されていないことが判明したデバイスの領域については、（例えばTSSまたは運用ガイダンスに）これらの領域には利用者データを書き込むことができない正当化が提供されていることを確認する。
- テスト2：USBフラッシュドライブに書き込まれるとき、利用者データが暗号化されること確認する。これをテストする程度は前のテストとの対応で決まる。すなわち、USBフラッシュドライブを「普通に」差し込み、利用者データをUSBフラッシュドライブに書き込み、それらのデータが暗号化されていないように見えないことを保証することは許容される。

4.1.3 クラス：識別及び認証（FIA）

拡張：USB フラッシュドライブ利用者許可（FIA_AUT_EXT）

FIA_AUT_EXT.1　　拡張：USBフラッシュドライブ利用者許可

FIA_AUT_EXT.1.1　　TSFは、利用者許可を実行するために、FCS_CKM.1.1(2)、

FCS_CKM.1.1(3)、及びFCS_COP.1(4)に定義されているメカニズムを提供しなければならない。

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に提供されているメカニズムを使用して利用者許可を実行しなければならない。

FIA_AUT_EXT.1.3 TSFは、FMT_SMF.1(c)に規定されているように、利用者にパスワードベースの認証要素の変更を許可する前に、FIA_AUT_EXT.1.1に提供されているメカニズムを使用して利用者許可を実行しなければならない。

FIA_AUT_EXT.1.4 TSFは、USBフラッシュドライブ上の利用者データを復号する前に、利用者が入力する認証要素が有効であることを検証しなければならない。

FIA_AUT_EXT.1.5 TSFは、各認証要素の検証方法によって、KEKまたはDEKを導出するために使用されるKEK、DEK、またはCSPの実効強度が開示されたり、低下することがないことを確認しなければならない。

適用上の注意：

129 この要件の意図は、USB フラッシュドライブを復号し、自分のデータにアクセスする許可を利用者に与えるメカニズムを規定することである。なお、これは個別利用者の認証とは見なされない。認証要素は、クローンして、USB フラッシュドライブのすべての許可された利用者に提供することができる。あるいは、利用者が利用者固有の認証要素を持つこともできよう。ただし、利用者が一般に USB データにアクセスできるようになる前に認証要素が「認証」されること、及びこの認証に使用される方法によって鍵または鍵関連情報が不正に入手されることがないことは要求されない。この認証の手段は、使用される認証要素によって異なる場合がある。

130 エレメント 1.4 及び 1.5 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、利用者から提供される認証要素の検証を取り扱う。認証要素が有効でない場合、TSF が KEK を形成し、それを使用して DEK のマスクを解除し、利用者に意味のないデータを提供しようと試みることは望ましくない。ただし、認証要素が有効かどうかのチェックは、攻撃者が他の要件を迂回できるような方法で行ってはならない。通常、この操作はホスト上で実行されるため、攻撃者によって監視/分解されることがあるので、この脅威を考慮して設計しなければならない。

131 利用者許可は、デバイスが利用者からアクセスできるようになる（すなわち、USB ポートに差し込まれ、基礎となる OS によって認識される）ときに実行すればよい。上記の要求が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許可を実行しなければならないことを意味すると解釈するべきではない。ただし、利用者がパスワードベースの認証要素を変更したい場合には、変更を行う前に利用者許可機能が呼び出されなければならない。

保証アクティビティ：

評価者は、TOEを初期化する方法、すなわち、USBフラッシュドライブの挿入及び検出、USBフラッシュドライブから読み込まれるソフトウェア（存在する場合）、パスワードの入力及びKEKの形成、及びDEKのマスク解除及びUSBフラッシュドライブの暗号化されている部分へのアクセスなどのイベントシーケンスが記載されていることを決定するために、TSS節をチェックしなければならない。変更前の許可機能（FIA_AUT_EXT.1.3）は、FMT_SMF.1の下でテストされる。

評価者は、利用者がUSBフラッシュドライブ上のデータにアクセスする許可を得る前に認証要素を検証する方法がTSSに記載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、または他の鍵関連情報が開示されないことを評価者が決定することができるように十分に詳細でなければならない。「開示」には、DEKまたはKEKの強度低下の意味も含まれる。KEKを作成するためのサブマスクを提供するために別の認証要素が使用される場合、各認証要素をチェックするために個別の方法を持つことは要求されない。評価者は、認証要素を認証するメカニズムの分析をテスト報告書（ATE_IND）に記載しなければならない。

評価者は、次のテストを実行しなければならない。

- テスト 1：USB フラッシュドライブ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、（適宜）認証要素の入力が要求されることを確認する。サポートされる認証要素ごとに、間違った認証要素を入力すると、間違った認証要素が提供されたことが TOE から通知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）

132 本節の主な意図は、安全な方法でデバイスを使用するために実行しなければならない（または実行できてはならない）重大なアクティビティを記載することである。これらの機能の一部は他の種類の TOE では「管理者」機能と見なされるかもしれないが、USB フラッシュドライブの場合は、デバイスの最終利用者がこれらの機能すべてを実行できることが期待される。適合する TOE の管理モデルについては、本 PP の 1.1.5 節に記述されている。

133

TSFデータの管理（FMT_MTD）

FMT_MTD.1	**TSFデータの管理（すべての対称鍵の読み取りに関して）**
FMT_MTD.1.1	**詳細化：**TSFは、デバイス外部の利用者によるUSBデバイス上のすべての鍵関連情報の読み取りを**防止**しなければならない。

適用上の注意：

134 要件の意図は、USB デバイス外部のエンティティが、デバイスに提供されているインタフェースを通じて、デバイス上に含まれ、または処理される鍵関連情報の読み取りまたは表示を実行できないことである。これには、マスクされた鍵を読み取る機能も含まれる。

保証アクティビティ：

135 評価者は、ホストから見えるデバイスへのインタフェースが TSS に詳述されていることを決定するために、TSS を検査しなければならない。これは、TSS で直接規定するか、または ST の読者が参照を使用できる限り参照することができる。インタフェースには、デバイスドライバが使用できるインタフェース及び（オプションで）デバイスドライバによってエクスポートされるインタフェースがある。評価者は、どのインタフェースによっても外部エンティティが USB デバイスから鍵（マスクされた鍵または平文の鍵）を取得できないという議論があることについて TSS を検査し、主張される機能（またはその欠如）に関してインタフェースの記述を検査することで議論を検証しなければならない。

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、以下の管理機能を実行できなければならない。

a) **USBフラッシュドライブを初めて使用するときにDEKを生成する。**

b) **利用者が入力する認証要素から導出されるサブマスクから形成されるKEKを使用してDEKを保護する。特に条件付けされたパスワードベースの認証要素及び[選択：他の入力なし、PIN保護方式の保存されたサブマスク、ホスト分割認証要素/サブマスク、[割付：他の認証要素/サブマスク]]。**

c) **パスワードベースの認証要素を変更する。**

d) **[選択、次のうち1つを選択：他の機能なし、[選択：既定の認証要素を変更する、認証要素を生成する、認証要素入力を設定する、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によって提供される他の管理機能]]。**

適用上の注意：

136 この要件の意図は、TOE が備える管理機能を表現することである。すなわち、TOE は、リストされる機能を実行できなければならない。項目(a)及び(b)は運用で使用するために必要な鍵関連情報を確立し、項目(c)は利用者が自分の認証要素を変更できるようにし、項目(d)は TOE に含めることはできるが、PP に適合するために必須ではない機能の特定に使用される。

137 項目 b については、FCS_CKM.1(2)で規定される KEK の形成にサブマスクを提供する適切な認証要素を、選択文と割付文に規定するべきである。実装の観点からは、これにより、最終利用者に認証要素を提供できるように、認証要素が DEK に拘束される。これらの認証要素は、利用者の制御の下で入力または生成されなければならない。エスクロー機能が存在することもあるが、エスクロー鍵を回復できない、または DEK/KEK が生成されるときにエスクロー鍵が生成されるように、エスクロー機能が無効にされなければならない（または無効にする機能を持たなければならない）。

138 項目(c)については、パスワードベースの認証要素のみが変更可能である。他の認証要素が変更可能な場合は、ST 執筆者は項目(d)での割付を使用するべきである。また、この追加機能をサポートするために、適切な保証アクティビティ及び根拠も追加する必要があるだろう。

139 項目(d)では、他の管理機能が提供されない（または主張されない）なら、「他の機能なし」を選択するべきである。いくつかの他の共通オプションが与えられる。

- TOEによってホスト分割認証要素またはPIN保護方式のサブマスクが実装される場合は、附属書Cからの該当する要件と共に「認証要素を生成する」を含めなければならない。
- TOEが暗号機能の設定可能性（例えばDEKの鍵サイズ）を提供する場合は、「暗号機能を設定する」を記載し、提供される具体的な機能を箇条書きにしてこの要件またはTSSに記載できる。
- TOEが鍵エスクロー機能を備えている場合、TOEは、エスクロー鍵が生成されないように、利用者がこの機能をオフにする機能を提供しなければならない。
- 「他の管理機能」が割り付けられる場合は、STが本PPへの適合を主張できるように保証アクティビティ及び他の機能要件が適切に規定されていることを確認するために、評価を監督する国の認証機関（スキーム）に相談しなければならない。

保証アクティビティ：

140 このコンポーネントの保証アクティビティは、ST 執筆者が行った選択によって駆動されるだろう。本節では、ST でのすべての可能な選択に関する保証アクティビティについて記述する。機能が ST で選択されない場合は、記載されている保証アクティビティを実行する必要がないと理解されるべきである。以下の節は、参照しやすいように、「必須アクティビティ」と「条件付きアクティビティ」に分割されている。

141 **必須アクティビティ**

142 DEK の生成

143 評価者は、AGD ガイダンスをレビューし、DEK を生成する手順が存在することを決定しなければならない。手順は TOE が適合を主張しているすべての環境を網羅し、正常に DEK を生成するために存在しなければならない前提条件を含まなければならない。DEK が生成される方法の記述が AGD ガイダンスの手順と一貫していること、及び異なるプラットフォームから生じる違いが考慮されていることを確認するために、TSS が確認される。

144 適切な認証要素からのサブマスクから形成される KEK で DEK の保護

145 ST は、TOE によってサポートされる認証要素を特定し、正常に TOE 機能を使用するためにいくつの要素及びどの組合せが必要かに関する要件を提供する（これは FCS_CKM 要件で行われる）。この要件は、それらの認証要素から導出されるサブマスクから生成される KEK による DEK の最初の保護（または新しい DEK の保護）を取り扱う。評価者は、サポートされる認証要素ごとに、ガイダンスがこの操作のためにその要素を TSF 入力する方法を詳述していること決定するために、AGD ガイダンスをレビューしなければならない。評価者は、様々な認証要素用のサブマスクを導出し、組み合わせて KEK を形成する方法、及び KEK を使用して DEK をマスクする方法が TSS 節に記載されていることを決定するために、TSS 節をレビューしなければならない。このプロセスと「通常の」操作中（すなわち、TOE で暗号化が確立された後）に使用されるプロセスの違いがあるかどうかも明確にしなければならない。また、この記述に、FCS_CKM.1* 要件に関する保証アクティビティに記述される情報を含めることもできよう。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は、AGD ガイダンスは各プラットフォームの最低要件及び適用する認証要素に関する他の制限事項を明記しなければならない。評価者は、次のテストも実行しなければならない。

- テスト 1：サポートされる最小数の認証要素のそれぞれについて、DEK を確立し、DEK を暗号化するための認証要素を管理者が入力できることを確認する。このテストを実行する回数は、サポートされるプラットフォームの数及び必要な認証要素の違いによって異なる。サポートされる認証要素とサポートされるプラットフォームのすべての組合せをテストすることは要求されないが、代表的なサンプルを使用しなければならない。また、評価者はテスト報告書にこのサンプルの正当化を提供しなければならない。

146 パスワードベースの認証要素を変更する

147 評価者は、パスワードベースの認証要素を変更する方法が記載されていることを確認するために、運用ガイダンスを検査しなければならない。また、評価者は、このアクティビティが実行されるときにホスト及び USB フラッシュドライブで実行されるアクティビティのシーケンスが TSS に記載されていること、及び KEK と DEK がこの変更中に開示されないことを確認するために、TSS を検査しなければならない。評価者は、次のテストも実行しな

ければならない。

- テスト 2：評価者は、USB デバイス用のパスワード認証要素を確立しなければならない。次に、評価者は、ホストからデバイスに利用者データを転送しなければならない。次に、「認証要素を変更する」機能を使用して、デバイス上のパスワードを変更し、現在の認証要素の入力を要求されることを確認しなければならない。現在の認証要素について間違った値を入力し、認証要素の変更が行われないことを確認しなければならない。現在の認証要素について正しい値を入力したときには、デバイス上の利用者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、（正常に認証要素を変更した後で）古い認証要素を使用して、デバイス上の利用者データにアクセスできなくなっていることを示さなければならない。

148 **条件付きアクティビティ**

149 上記の要件における項目 d には、TOE によって提供できるが、本 PP への適合には必須でない機能を指定するいくつかの選択が含まれている。ただし、機能が提供される場合、TOE は、附属書 C から該当する要件を含め、対応する上記の選択を行って、適合を主張することができる。適用上の注意に記載されているように、割付を行う場合は、PP への適合を主張できるかを決定するために、評価を監督する国の認証機関（スキーム）に相談する必要がある。

150 USB フラッシュドライブに既定の認証要素が設定されている場合がある。その場合は、これらの認証要素を変更するメカニズムが存在することを示すために、項目 d の選択を行わなければならない。運用ガイダンスには、利用者がデバイスの所有権を取得するときに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 には、存在する既定の認証要素を記述しなければならない。

- テスト 3 [条件付き]：TOE が既定の認証要素を提供する場合、評価者は、運用ガイダンスに記述されるようにデバイスの所有権を取得す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）認証要素がもはやデータアクセスに有効でないことを確認しなければならない。

151 ホスト分割認証要素と PIN 保護方式のサブマスクという選択の 1 つは認証要素の生成に関係している。いずれの場合も、附属書 C からの追加要件を ST に含める。これらの要件には、認証要素/サブマスクを生成する方法の詳細を取り扱う保証アクティビティが関連付けられている。管理者が特定のデバイスに対してどの認証要素の組合せが有効であるかを決定するオプションを持っている場合は、選択も行うべきである。これらの機能の管理に関連する FMT_SMF アクティビティについては、評価者は、認証要素メカニズムを呼び出す手順が詳述され、必須の特性を持つ認証要素を生成できるように十分明確であることを確認するために、AGD 情報をレビューしなければならない。認証要素を保存または操作するために要求されるアクティビティについても、確認しなければならない。使用するために（TOE によってサポートされる認証要素のうち）どの認証要素が設定されるかを決定する観点から管理者によって行われる設定アクティビティについても、評価チームによって記述され、確認されなければならない。これらのメカニズムに関連するテストは、特定のメカニズムの保証アクティビティの一環として規定される。

152 一部の TOE では、使用される基礎となる暗号に関する選択がある場合がある。例えば、DEK のビット長、または AES に使用される暗号化モードなど。この場合も、TOE が PP への適合を主張するために、この機能を提供する必要はない。ただし、機能が提供される場合は、それを ST に規定し、上記の要件で「暗号機能を設定する」を選択する。

153 この選択について、評価者は、暗号機能のどの部分が設定可能かを ST から決定しなければならない。これには、FCS 要件及び TSS の関連記述の参照が伴う。評価者は、この情報を利用して、主張されるすべてのメカニズムを操作するための手順が存在することを決定するために、AGD 文書をレビューしなければならない。

154 TOE が鍵エスクローをサポートする場合、このことを TSS に記載しなければならない。また、TSS はエスクロー関連情報をエスクロー所有者に提供する方法を含めて、この機能を無効にする方法を記述しなければならない。その意図は、評価者がテストでこの記述を使用して、エスクロー機能が実際に無効になっているかどうかを決定できることである（例えば、新しい KEK/DEK が生成されるときに関連情報がネットワーク接続を通じて第三者に送信されることが TSS に記載されている場合、評価者は、機能を無効にし、ネットワークモニターを接続し、新しい KEK/DEK が生成されるときにネットワーク接続が行われるかどうかを確認できる）。この機能を無効にするためのガイダンスは、AGD 文書に記述されなければならない。

- テスト 4 [条件付き]：TOE が効果を TOE インタフェースで確認できるエスクロー機能を提供する場合、評価者は、ベンダから提供されるガイダンスに従ってエスクロー機能が無効になっている、または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考案しなければならない。

4.1.5 クラス：TSF の保護（FPT）

拡張：TSFシステムファイル保護（FPT_SFP_EXT.1）

FPT_SFP_EXT.1	**拡張：TSFシステムファイル保護**
FPT_SFP_EXT.1.1	TSFは、署名付きの検証済みシステムファイルのみがUSBフラッシュドライブにインストールされ、使用されることを確認しなければならない。

適用上の注意：

155 この要件は、運用ガイダンス及び FPT_TUD_EXT.1 に規定されているように TOE の更新を実行できる一方で、利用者（または多くの場合、利用者の代わりに機能する悪意のあるプログラム）が USB フラッシュドライブの操作に使用される合法のファイルを悪意のあるバージョンで置換するのを防止する。悪意のあるファイルの配付のベクターは、デバイスが挿入されるときに自動的に実行されるファイル（例えば ini ファイル）または USB デバイスがブートデバイスとして使用されるときに実行されるファイルから組み込むことができる。

保証アクティビティ：

156 署名付き更新機能は、FPT_TUD_EXT.1 要件に関して実行される保証アクティビティを通じて検証される。この要件の他の側面は、更新手順の外でシステムファイルを置換する機能である（例えば、デバイスにファイルを直接コピーする、または更新機能のために提供されているインタフェースを使用して、デバイスにシステムファイルを直接コピーすることを試みる）。評価者は、FPT_TUD_EXT.1 から、更新機能が動作する方法に関する情報を取得する。また、評価者は、TSS に USB フラッシュドライブ上のすべての暗号化されていないファイルの一覧が提供され、機能の説明があり、どれが USB フラッシュドライブ上のシステムファイルであるか、また（実行可能な場合）各ファイルがどこで実行されるかが示されていることを決定するために、TSS を検査する。また、評価者は、ファイルごとにファイルを更新/変更できるかどうかが TSS に記述されていることを決定しなければならない。ファイルを更新/変更できる場合、評価者は、更新/変更を実行する方法が TSS に記述されていることを決定する。評価者は、システムファイルとして識別されないファイルが正し

く分類されていることを決定しなければならない。評価者は、次のテストも実行しなければならない。

- テスト1：評価者は、TSSに含まれる情報を使用して、USBフラッシュドライブのセキュリティ特性に影響するように、またはUSBフラッシュドライブを悪意のあるソフトウェアの自動的な実行のベクターにするような方法（例えば、悪意のあるバージョンを持つデバイスに含まれているWindowsのautorun.infファイル置換する機能）でシステムファイルの上書きまたは変更を試みなければならない。
- テスト2：デバイスがブート可能である場合（すなわち、製造者から提供されるシステムファイルによってデバイスをブートデバイスとして使用できる場合）、評価者は、ブートすると利用者データにアクセスできる、他のシステムファイルを上書きできる、または任意のコードでホストを感染させることができるカスタムブートファイルで、この領域の上書きを試みなければならない。評価済み設定で配付されるとブート可能な適切なシステムファイルがデバイスに含まれない場合、評価者は、ホスト上で任意のコード（すなわち評価者の設計及び選択によるコード）を実行できるブートデバイスとして使用できるように、デバイスへのファイルの配置を試みなければならない。

拡張：USBフラッシュデバイス高信頼更新（FPT_TUD_EXT.1）

FPT_TUD_EXT.1	**拡張：USBフラッシュデバイス高信頼更新**
FPT_TUD_EXT.1.1	TSFは、許可された利用者に、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機能を提供しなければならない。
FPT_TUD_EXT.1.2	TSFは、許可された利用者に、TOEファームウェア/ソフトウェアの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/ソフトウェア更新をインストールする前に、USBフラッシュドライブ上に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：

157 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）で規定されるメカニズムである。

保証アクティビティ：

158 USB フラッシュドライブの更新は、許可された配付元によって署名される。許可された配付元の定義は、更新検証メカニズムによって使用される証明書がデバイスに含まれる方法の記述と共に 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、候補更新を取得する方法、更新のデジタル署名の検証に関連する処理、及び成功（署名は検証された）及び失敗（署名は検証できなかった）の場合に行われるアクションが TSS（または運用ガイダンス）に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/ファームウェアの位置も TSS に記述され、評価者によって検証されなければならない。評価者は、以下のテストを実行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決定するために、バージョン検証アクティビティを実行する。以下のテストに記述されている更新テストの後で、評価者は、バージョンが更新のバージョンに正確に一致することを確認するために、再びこのアクティビティを実行する。

- テスト2：評価者は、運用ガイダンスに記述されている手順を使用して合法の更新を入手し、正常にTOEにインストールされることを検証する。他の保証アクティビティの部分集合を実行して、更新が期待通りに機能することを実証する。
- 評価者は、違法の更新を入手または生成し、TOEへのインストールを試みる。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が正しく動作することを実証するために、初回の起動時（電源を入れるとき）に自己テストスイートを実行しなければならない。

保証アクティビティ：

159 NIST SP 800-90 に従って FCS_RBG_EXT.1 が実装されている場合、評価者は、NIST SP 800-90 の Section 11.3 と一貫しているヘルステストが TSS に記述されていることを検証しなければならない。

160 TSS は、すべての FCS_COP 機能について、答えがわかっている自己テストを記述しなければならない。

161 評価者は、TSF の正しい動作に影響する暗号以外の一部の機能について、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 は、これらの機能のそれぞれについて、機能/コンポーネントが正しく動作することを検証する方法を記述しなければならない。評価者は、識別されるすべての機能/コンポーネントが起動時に適切にテストされることを決定しなければならない。

4.2 セキュリティ機能要件の根拠

162 本節では、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。表 7 に、要件によって対策方針が達成される対応する根拠と共にセキュリティ機能要件とセキュリティ対策方針の対応関係を示す。この表は、4.1 節における要件に関する選択と割付を行う際に ST 執筆者/ベンダによって追加されるべきである。また、（潜在的に）附属書 C からの要件を持つ基底要件を追加するべきである。

表 7：TOE セキュリティ機能要件に関する根拠

対策方針	対策方針を達成する要件	根拠
O.AUTHORIZED_USER TOEは、USBフラッシュドライブ上のデータを暗号化及び復号できるように、利用者から認証要素を取得しなければならない。	FIA_AUT_EXT.1 FCS_CKM.1(2)	FIA_AUT_EXT.1では、USBフラッシュドライブから暗号化されていないデータへのアクセスを許される前に、利用者がFCS_CKM.1(2)に規定されているメカニズムによって許可されなければならないことが要求される。
O.CORRECT_TSF_OPERATION TOEは、TSFが運用環境で正しく動作することを検証する機能を提供しなければならない。	FPT_TST_EXT.1	FPT_TST_EXT.1では、対策方針が満たされるように、TOEを運用する前にTOEで（暗号機能及び他のコンポーネントに関する）自己テストを実行することが要求される。
O.ENCRYPT_ALL TOEは、USBフラッシュドライブに保存されるすべての利用者データを暗号化する。	FDP_DSK_EXT.1 FCS_CKM.1(1) FCS_COP.1(1)	FDP_DSK_EXT.1は、TOEUSBフラッシュドライブの暗号化を実行することを確認する。これには、すべての利用者データ及び適切な鍵関連情報が含まれる。 すべてのデータが暗号化されるという要件があることに加えて、FCS_CKM.1(1)は、暗号化を実行するために使用される鍵の品質、及び暗号操作に使用されるアルゴリズム及び鍵の長さを規定する。
O.DEK_SECURITY TOEは、認証要素を持たない脅威エージェントがDEKを取得して利用者データにアクセスできないように、(認証要素から導出した）1つまたは複数のサブマスクから作成された鍵暗号鍵（KEK）を使用してDEKをマスクする。	FCS_CKM.1(2) FCS_CKM.1(3) FCS_RBG_EXT.1 FMT_MTD.1 FMT_SMF.1	FCS_CKM.1(2)は、KEKが導出される方法を規定し、KEKの鍵の長さを規定する要件である。この要件は、各認証要素の実効強度が維持されることを必須とする。 FCS_CKM.1(3)は、パスワードに内在するエントロピーが維持されるようにパスワードが条件付けされ、パスワードがDEKを保護する際に使用するのに適したサブマスクに変換されるように、パスワード認証要素に関する要件を課す。

		FCS_RBG_EXT.1は、鍵関連情報が堅牢に生成されることを保証する。 FMT_MTD.1は、あらゆる形のDEKにデバイスの外部からアクセスできることを防止し、鍵に対するオフライン攻撃を防止する。 FMT_SMF.1は、TSFがTOEの重要な側面を管理するために必要な機能を提供することを保証する。これには、DEKの生成、保護、及び削除、認証要素の生成及び設定、及び暗号機能の設定が含まれる。ST執筆者は、そのように選択するなら、他の管理機能を組み込むこともできる。
O.OWNERSHIP TOEは、利用者データをTOEに保存する前に、所有権が取得された（すなわち、DEKが作成され、認証要素が確立され、既定の認証要素が変更され、KEKが導出したサブマスクから生成され、DEKがKEKに関連付けられている）ことを保証しなければならない。	FMT_SMF.1	FMT_SMF.1は、デバイスが使用に供されるときにDEKが生成されること、及びDEKが選択した認証要素から生成されるサブマスクから導出されるKEKで保護されることを要求する。さらに、既定の認証要素が存在する場合は、許可された利用者がこれらの値を変更する許可を与えるメカニズムが存在することが要求される。 これらの要件全体で対策方針を達成する。
O.KEY_MATERIAL_COMPROMISE TOEは、暗号化/マスクされていない鍵または鍵関連情報がUSBフラッシュドライブ上の永続メモリに書き込まれないことを保証しなければならない。	FDP_DSK_EXT.1 FMT_MTD.1	FDP_DSK_EXT.1は、利用者データが暗号化され、平文の鍵関連情報がUSBフラッシュドライブの永続メモリに書き込まれないことを要求する。 FMT_MTD.1は、あらゆる形の鍵関連情報にデバイスの外部からアクセスできることを防止し、鍵に対するオフライン攻撃を防止する。
O.PROPAGATION_PREVENTION TOEは、USBフラッシュドライブが悪意のあるソフトウェアを自動的に拡散するメカニズムとして使用されることを防止するメカニズムを実装しなければならない。	FPT_SFP_EXT.1	FPT_SFP_EXT.1は、TOEが、許可されていない利用者（またはその代わりに動作するプログラム）が、システムファイルが自らをホスト間で自動的に転送し、そこに含まれているかもしれない悪意のあるペイロードのコピーを拡散するようにそれらのシステムファ

		イルを変更する許可を与えることができないことを要求する。
O.SAFE_AUTHFACTOR_VERIFICATION TOEは、KEK、DEK、または利用者データが意図せず開示されないように、認証要素の検証を実行しなければならない。	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を要求する。また、攻撃者がDEKまたはKEKを推測する際に有利な方法を提供しないようにこれを実行することが要求される。
O.TRUSTED_UPDATE TOEは、TOEファームウェア/ソフトウェアを更新し、製品の更新が意図した配付元から受信されることを検証する機能を利用者に提供しなければならない。	FCS_CKM.2 FCS_COP.1(2) FCS_COP.1(3) FPT_TUD_EXT.1	FPT_TUD_EXT.1は、利用者がバージョンをチェックし（これによって利用者は更新が必要なことがわかる）、更新プロセスを開始し、更新が改ざんされていないこと、及び信頼される配付元から来ていることを、暗号を用いて検証できることによって、要求される機能を提供する（FCS_CKM.2, FCS_COP.1(2), FCS_COP.1(3)）。

4.3 セキュリティ保証要件

163 3.1 節の TOE に関するセキュリティ対策方針は、第 2 章に識別されている脅威に対応するために作成された。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の形式的な具体化である。

164 4.1 節の序説に示されているように、本節には CC からの完全な SAR セットが含まれているが、評価者によって実行される保証アクティビティについては 4.1 節と本節の両方で詳述されている。

165 ファミリごとに、開発者によって提供される必要がある追加の文書/アクティビティ（存在する場合）を明確にするために、開発者アクションエレメントに「開発者向け注意事項」が提供されている。内容/プレゼンテーション及び評価者アクティビティエレメントについては、追加の保証アクティビティ（既に 5.1 節に含まれている保証アクティビティ）が、エレメントごとではなく、ファミリ全体として記述されている。さらに、本節に記述されている保証アクティビティは、4.1 節に規定されている保証アクティビティに対する補足である。

166 表 8 に示す TOE セキュリティ保証要件は、本 PP の第 2 章に識別されている脅威に対応するために要求される管理アクティビティと評価アクティビティを識別する。4.4 節は、本節にセキュリティ保証要件を選択するための簡潔な正当化を提供する。

表 8：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説明
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
テスト	ATE_IND.1	独立テスト－適合
脆弱性評価	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 CMカバレージ

4.3.1 ADV クラス：開発

167 この PP に適合する TOE については、TOE に関する情報は、最終利用者が使用できるガイダンス文書及び ST の TOE 要約仕様（TSS）部分に含まれる。TOE 開発者が TSS を執筆することは要求されないが、TOE 開発者は、機能要件に関連しているため、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 節に含まれる保証アクティビティは、TSS 節に適した内容を決定するために十分な情報を ST 執筆者に提供するはずである。

4.3.1.1 ADV_FSP.1 基本機能仕様

168 機能仕様は、TSFI を記述する。必ずしもこれらのインタフェースの形式的または完全な仕様である必要はない。さらに、本 PP に適合する TOE は、TOE 利用者によって直接起動されない運用環境とのインタフェースを必ず備えているはずであるから、このようなインタフェースでは間接的なテストしか可能でないため、このようなインタフェースを記述することを規定する意味はほとんどない。本 PP では、このファミリに関するアクティビティは、機能要件に対応して TSS で規定されるインタフェース及び AGD 文書に規定されるインタフェースの理解に集中するべきである。規定されている保証アクティビティを満たすために、追加の「機能仕様」書は必要でないはずである。

169 TOE へのインタフェースの理解では、対応するべき主な脅威は、攻撃者が USB フラッシュドライブを発見し、ドライブのデータを復号するために TOE へのインタフェースを探ろうと試みることであることを考慮することが重要である。攻撃者はただ USB フラッシュドライブを操作するだけであるから、信頼できない主な利用者インタフェースは、USB フラッシュドライブがホストに挿入されるときに利用者に提供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、運用インタフェース（TOE を設定する方法）についても記述する必要がある。他の主なインタフェースは、ファームウェア及び USB ミドルウェア更新インタフェースである。前述のように、置換されるコードまたはデータが正しく署名され、署名が検証されることが非常に重要である。

170 評価する必要があるインタフェースの特徴は、独立した抽象的なリストでなく、リストに記載されている保証アクティビティを実行するために必要な情報を通じて表現される。

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への追跡を提供しなければならない。

開発者向け注意事項：本節の序説で示したように、機能仕様は、STのTSSに提供されている情報と共に、AGD_OPR及びAGD_PRE文書に含まれている情報から構成される。機能要件内の保証アクティビティは、文書及びTSS節に存在するべきである証拠を指し示す。これらはSFRに直接関連付けられるため、エレメントADV_FSP.1.2Dでの追跡は既に明示的に行われており、追加文書は必要でない。

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が強制し、SFRがサポートする各TSFIを使用する目的と方法を記述しなければならない。

ADV_FSP.1.2C 機能仕様は、SFRが強制し、SFRがサポートする各TSFIに関連付けられた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非干渉としてのインタフェースの暗黙的な分類に関する根拠を提供しなければならない。

ADV_FSP.1.4C 追跡は、機能仕様におけるSFRのTSFIへの追跡を実証しなければならない。

評価者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の内容とプレゼンテーションに対する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：

171 この SAR に関連する保証アクティビティは特にない。機能仕様は、4.2 節に述べられた評価アクティビティや AGD、ATE、AVA SAR に述べられた他のアクティビティをサポートするために提供されている。機能要件に関する情報の内容についての要件は、実行された他の保証アクティビティを通じて暗黙的に評価されている。インタフェース情報が不十分なために評価者がアクティビティを実行できなければ、適切な機能仕様が提供されていないのである。例えば、TOE が AES 暗号化アルゴリズム用の鍵の長さを設定する機能を提供しながら、この機能を実行するインタフェースを指定しない場合、FMT_SMF に関連付けられた保証アクティビティは失敗することになる。

4.3.2 AGD クラス：ガイダンス文書

172 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。序説で述べたように、実際の「管理者」の責務は非常に制限されているため、ガイダンス文書は TOE のすべての利用者によって要求され、使用される情報を含むことになる。この目的に沿って、下記では多くの場合に「許可された利用者」を使用する。「管理者」が使用されるときは（CC からの逐語的要件を除き）、（オプションで）強力なパスワード認証要素を作成する責任を持つ利用者の部分集合を示している。

173 ガイダンスは、許可された利用者が、運用環境（USB フラッシュドライブを搭載する製品）がセキュリティ機能に関する役割を果たすことができることを検証する方法の記述を含まなければならない。文書は、形式的にならず、許可された利用者にとって読みやすいものであるべきである。

174 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を正常に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。

175 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に関する要件は、4.1 節に指定されている保証アクティビティに含まれている。

4.3.2.1 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： ここで情報を繰り返すよりも、評価者がチェックするガイダンスの詳細を確定するために、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するべきである。それによって、許容可能なガイダンスの準備に関する必要な情報が提供されるだろう。

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により提供された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かを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を、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セキュリティ関連事象の各タイプについて、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。

評価者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の内容とプレゼンテーションに対する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：

176 操作ガイダンスの内容の一部は、4.1 節の保証アクティビティによって検証される。ただし、ガイダンスでは 2 つの追加警告を利用者に提供しなければならない。ガイダンスは、USB フラッシュドライブがホストに接続され、ホストの電源が入っているときは、USB フラッシュドライブを放置してはならないことを許可された利用者に警告しなければならない。さらに、許可された利用者は、パスワード及び/またはホスト分割認証要素及び/または PIN 認証要素を USB フラッシュドライブに、または複数要素を使用する場合は相互に、残し/保存してはならないことを記載しなければならない。

177 以下の追加情報も要求される。

178 文書には、TOE の更新が意図した配付元（多くの場合 TOE ベンダ）から来ることを検証するための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、USB フラッシュドライブ上の TSF によって実行される。評価者は、このプロセスに以下の手順が含まれていることを検証しなければならない。

1. 証明書所有者から署名付き更新を受け取ったことを確認するためにFCS_COP.1(2)メカニズムによって使用される証明書を取得するための指示。これは、製品に同梱してもよいし、または他の手段で取得し、初期設定の一環としてUSBフラッシュドライブにインストールしてもよい。USBフラッシュドライブに同梱されない場合は、取得した証明書を最終利用者が信頼できることを決定する方法に関する指

示をガイダンスに提供しなければならない。

2. 更新を取得するための指示自体。これには、USBフラッシュドライブから更新にアクセスできるようにするための指示（特定のディレクトリに配置するなど）も含めるべきである。

3. 更新プロセスを開始するための指示、及びプロセスの成功または失敗を区別するための指示。

4.3.2.2 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関心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。

評価者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の内容とプレゼンテーションに対する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が操作のためにセキュアに準備されることを確認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：

179 上記の序説で説明した通り、特に、TOE 機能要件をサポートするために運用環境を設定する時、文書に関して大きな期待がある。評価者は、TOE 用に提供されたガイダンスが適切に ST で TOE について主張された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合せ）に対処していることを確認しなければならない。

180 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。

- 製品のセットアップ時にUSBフラッシュドライブ上の利用者データが暗号化され、適合するTOEに対して唯一許される設定であるように、製品を設定する方法を詳述する指示及び情報が許可された利用者に提供される。
- TOEがホスト分割認証要素をサポートする場合は、対象ホストに常駐する分割をTOEのセキュリティを維持する方法でインストールする手段を文書に記述しなければならない。評価者は、これらの手続きが健全であることを決定するために、これらの手続きを評価しなければならない。

- 附属書C、C.1節に記載されている暗号機能について運用環境に関する要件がある場合、評価者は、TOEに対する許容可能な実装が識別され、テストがガイダンスに識別されている許可された設定で実行されることを確認しなければならない。

4.3.3 ATE クラス：テスト

181 テストは、機能の観点と共に、設計や実装の弱さを利用する観点について指定される。前者は、ATE_IND ファミリを通して行われ、後者は、AVA_VAN ファミリを通して行われる。本 PP で指定される保証レベルでは、テストは設計情報が利用可能かに依存して、公開されている機能性及び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、以下の要件に規定されたテスト報告書である。

4.3.3.1 ATE_IND.1 独立テスト ー 適合

182 テストは、TSS（TOE 要約仕様）に記載されている機能性や提供される管理文書（設定や運用も含む）を確認するために実行される。テストの焦点は、一部の追加テストは 4.3 節で SAR として特定されているが、5.1 節に特定された要件が満たされていることを確認することである。保証アクティビティは、これらのコンポーネントに関する最小テストアクティビティを識別する。評価者は、テスト計画や結果を記載するテスト報告書と、本 PP に適合を主張するプラットフォーム/TOE コンビネーションに焦点をあてるカバレージ論証を作成する。

開発者アクションエレメント：

ATE_IND.1.1D 開発者は、テストのために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。

評価者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の内容とプレゼンテーションに対する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、指定された通りにTSF操作を確認するために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：

183 評価者は、システムのテスト面を記載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体に含まれるテストアクションすべてをカバーする。保証アクティビティに載っているテスト毎にテストケースが必要ではないが、評価者は*該当する各*テスト要件が *ST* でカバーされていることをテスト計画に記載しなければならない。

184 テスト計画はテストされるプラットフォームを特定し、テスト計画にはなく ST に含まれるプラットフォームについては、テスト計画はプラットフォームのテストのためではない正当化の理由を提供する。この正当性は、テストされたプラットフォームとテストされていないプラットフォームの違いを述べなければならず、その違いが実行されるテストに影響しないことを議論しなければならない。その違いによる影響がないと単に断言するのは不十分であり、根拠が提供されなければならない。もし ST に主張された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。

185 テスト計画は、テストされる各プラットフォームの構成を記述し、AGD 文書に含まれるもの以外にも必要となるセットアップについても記述する。注意すべきことは、評価者は各プラットフォームの実装とセットアップについて、テストの一部か標準プレテスト条件として、AGD 文書に従うことが期待されている。これは、特別なテストドライバやツールを含むかもしれない。各ドライバやツールに関して、ドライバやツールが *TOE* やプラットフォームの機能のパフォーマンスに悪影響を与えないよう論証（単なる主張ではなく）が提供されるべきである。

186 テスト計画は、ハイレベルのテスト目標とこの目標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、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のアクティビティを詳述し、テストの実際の結果を含む。これは累積的計算であるべきであり、テストの実行が不合格に終わった場合は、修正をインストールし、テストを正しく再実行し、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（論点を補強する例証）を示さなければならない。

4.3.4 AVA クラス：脆弱性評定

187 本 PP の第一世代（初版）のために、評価機関は、これらの製品のタイプに見つかった脆弱性を見つけるため、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、基本的な攻撃以上の複雑さを必要とする。侵入ツールが作られ評価機関に一様に配付されるまで、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載っ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ている。この情報は、侵入テストツールの開発や将来の PP の開発のために使われるだろう。

4.3.4.1 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、テストのために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。

評価者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の内容とプレゼンテーションに対する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の潜在的な脆弱性を特定するために公開情報の探索を実施しなければならない。

AVA_VAN.1.3E 評価者は、特定された潜在的な脆弱性に基づいて、TOEが基本的な攻撃能力を持つ攻撃者による攻撃に抵抗することを決定するために、侵入テストを実施しなければならない。

保証アクティビティ：

188 ATE_IND と同様に、評価者はこの要件に関して、所見を記載するために報告書を作らなけ

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の一部でも別文書でもよい。評価者は、USB フラッシュドライブ暗号化製品全般で見つかった脆弱性や特定の TOE に関連する脆弱性を決定するために公開情報を検索しなければならない。評価者は、参考にした情報源と見つかった脆弱性を報告書に記載する。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、不適用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って）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のベクトルを査定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合せを押すことによって検知されたら、本 PP の保証レベルのテストが適しているであろう。脆弱性の悪用に、例えば、電子顕微鏡と液体ニトロジェンが必要となるならば、テストは適しておらず、適切な正当化が策定されるべきである。

4.3.5 ALC クラス：ライフサイクルサポート

189 本 PP に適合する TOE に提供される保証レベルに関して、ライフサイクルサポートは、TOE ベンダの開発、構成管理プロセスの調査よりも、最終利用者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実践する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される情報の反映である。

4.3.5.1 ALC_CMC.1 TOE のラベル付け

190 このコンポーネントは、TOE を特定することを対象としており、これを使うことによって、最終利用者が購入した際に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、容易に特定できる。

開発者アクションエレメント：

ALC_CMC.1.1D 開発者は、TOEとTOEの参照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、その一意の参照でラベル付けされなければならない。

評価者アクションエレメント：

ALC_CMC.2.1E 評価者は、提供された情報が証拠の内容とプレゼンテーションに対する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：

191 評価者は、ST の要件を満たすバージョンを明確に特定する識別子（製品の名前、バージョン番号等）を ST が含んでいることを確認するために、ST をチェックしなければならない。さらに、評価者は、ST に載っているバージョン番号と一致していることを確認するために、AGD ガイダンスとテスト用に受け取った TOE サンプルをチェックしなければならない。ベンダが TOE を宣伝する Web サイトを維持している場合は、ST の情報が製品を区別するために十分であることを確認するために、評価者は Web サイトの情報を調査しなければならない。

4.3.5.2 ALC_CMS.1 TOE CM カバレージ

192 TOE の範囲と関連する評価証拠要件をもってすると、このコンポーネントの保証アクティビティは、ALC_CMC.1 に載っ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。

評価者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の内容とプレゼンテーションに対する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：

193 本 PP の「SAR が要求する評価証拠」とは、AGD 要件のもとで管理者や利用者に提供されるガイダンスに加え、ST の情報に限定される。TOE が明確に識別され、この識別が ST や AGD ガイダンス（ALC_CMC.1 の保証アクティビティになされているように）と一致していることを確認することによって、評価者は暗黙的にこのコンポーネントが必要とする情報を確認する。

4.4 セキュリティ機能要件の根拠

194 これらのセキュリティ保証要件を選択するための根拠は、これがこの技術に関する米国政府の最初のプロテクションプロファイルであることである。これらの製品タイプで脆弱性が見つかった場合は、実際のベンダプラクティスに基づいて、より厳格なセキュリティ保証要件が義務付けられるだろう。

5 適合主張

195 適合主張は、PP またはその評価に合格するセキュリティターゲット（ST）によって満たされる要件の集合の情報源を示す。満たさなければならない具体的な要件をさらに明確にするために、セキュリティ機能要件（SFR）及びセキュリティ保証要件（SAR）の節に適用上の注意が提供されている。

5.1 PP 適合主張

196 本 PP は、CC 3.1r3、CC パート 2 拡張、及び CC パート 3 適合に適合する。

197 本 PP への適合を主張する ST は、CC パート 1（CCMB-2006-09-001）の Section D3 に定義されているように、厳格な PP 適合の最小規格を満たさなければならない。

198 厳格な PP 適合とは、PP 内の要件が満たされ、ST が PP の具体化であることを意味する。ST は、PP より広範であることができる。ST は、TOE が最低でも PP と同じことを実行し、運用環境が最大でも PP と同じことを実行することを規定する。本 PP では、規定された要件の意図及びベンダが要件を満たす方法についての期待をさらに明確にし、説明するために、適用上の注意が提供されている。ST の評価者は、ST 及びそこに記述されている TOE に本 PP のすべての文（あるいはそれ以上）が含まれるだけでなく、適用上の注意に記載されている期待も満たしていることを決定することで、厳格な PP 適合を確認することが期待される。

5.2 PP 適合主張の根拠

199 本 PP は、他の PP への適合を主張しない。

200

附属書 A：サポート表と参考文献

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

[11] Universal Serial Bus Mass Storage Class Specification Overview, Version 1.2, June 23, 2003

略語

AES	Advanced Encryption Standard（高度暗号規格）
AF	Authorization factor（認証要素）
AS	Authorization subsystem（許可サブシステム）
CAC	Common Access Card（共通アクセスカード）
CAVS	Cryptographic Algorithm Validation System（暗号アルゴリズム検証システム）
CC	Common Criteria（共通基準）
CM	Configuration management（構成管理）
COTS	Commercial Off-The-Shelf（民生品）
CS	Configuration subsystem（設定サブシステム）
DAR	Data-at-Rest（保存データ）
DEK	Data Encryption Key（データ暗号鍵）
DRBG	Deterministic Random Bit Generator（決定性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）
ES	Encryption Subsystem（暗号化サブシステム）
FDE	Full Disk Encryption（ディスク全体暗号化）
FIPS	Federal Information Processing Standards（連邦情報処理規格）
ISSE	Information System Security Engineers（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（鍵暗号鍵）
MBR	Master Boot Record（マスターブートレコード）
OSP	Organization Security Policy（組織セキュリティ方針）
PIN	Personnel Identification Number（個人識別番号）
PP	Protection Profile（プロテクションプロファイル）
PUB	Publication（出版）
RBG	Random Bit Generator（ランダムビット生成器）
SAR	Security Assurance Requirement（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	TSF Interface（TSFインタフェース）
TSS	TOE Summary Specification（TOE要約仕様）
TOE	Target of Evaluation（評価対象）
USB	Universal Serial Bus（ユニバーサルシリアルバス）

附属書 B：NIST SP 800-53/CNSS 1253 マッピング

NIST SP 800-53/CNSS 1253の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る。本節は、取り上げられた要件を概説しており、TOEが運用構成に組み込まれるときに要求される追加テスト（存在する場合）を認定担当者が決定するために利用できる。

適用上の注意：このバージョンは、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、認定チームのために更なる情報を提供する追加説明が追加される予定である。この追加情報は、TOEによって提供される適合の程度（例えば、完全に管理策を満たす、部分的に管理策を満たす）について議論している管理策マッピングに対するSFRについての詳細を含むだろう。さらに、適合が決定された方法に関する情報（文書レビュー、ベンダ主張、テスト/検証の程度）を認定チームに提供するために、規定された保証アクティビティ及びSARを満たす一環として行われる評価アクティビティの総合的なレビューが要約されるだろう。この情報は、規定された管理策の適合の程度を決定するために、実行する必要がある追加アクティビティ（存在する場合）を認定チームに示すだろう。

STは選択の範囲までは選択できるので、割付を埋めて、STが完成し評価されるまでは必ずしも最終的なストーリーは出来上がらない。したがって、この情報はPPに対する追加としてSTに含まれるべきである。さらに、特定の実装に基づいて評価者によって実行されるアクティビティに対するいくつかの必要な解釈（例えば、「修正」等）があるかもしれない。スキームは監督担当（例えば検証者）がこの種の情報を与えることができるか、または保証アクティビティの一部として評価者によって実施されるかもしれない。検証アクティビティは提供されなければならない重要な部分の情報であり、評価チームの作業に追加して行う必要があることがある場合、認定チームがそれを決定できるように提供されなければならない。

識別子	名称	適用可能なSFR
CM-2	基底構成	FPT_SFP_EXT.1
CM-5	変更のためのアクセス制限	FPT_TUD_EXT.1
IA-5	認証者管理	FCS_CKM.1(3), FIA_AUT_EXT.1, FMT_SMF.1
IA-7	暗号化モジュール認証	FIA_AUT_EXT.1
MP-4	保存媒体	FDP_DSK_EXT.1
MP-5	伝送媒体	FDP_DSK_EXT.1
SA-7	利用者がインストールするソフトウェア	FPT_SFP_EXT.1
SC-12	暗号鍵の確立と管理	FCS_CKM.1(1), FCS_CKM.1(2), FCS_CKM.2、 FMT_SMF.1
SC-13	暗号の使用	FCS_CKM.1(3), FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RBG_EXT.1, FMT_SMF.1
SC-28	保存情報の保護	FDP_DSK_EXT.1
SI-6	セキュリティ機能検証	FPT_TST_EXT.1
SI-7	ソフトウェアと情報の完全性	FPT_SFP_EXT.1

附属書 C：追加要件

201 PP の本草案について、この附属書は、サポートする脅威、対策方針、根拠、または保証アクティビティはなく、追加コンポーネントのみを含んでいる（ただし、一部のエレメントについてはガイダンスが提供されている）。このサポート情報は、現在のレビューサイクルに沿って、開発され、次回の PP の公開に組み込まれる予定である。本節に含まれる情報（含まれる要件が潜在的な適合 TOE に適用可能かどうか、またこの附属書に含まれていないが USB フラッシュドライブ暗号化製品に広く適用可能な要件）に関するコメントを歓迎すると共に、ぜひお願いしたい。

202 本 PP の序説に示したように、本 PP に適合し、TOE が実装できるいくつかの機能がある。これらの機能は、運用環境に依存することになるため必須ではない（例えば TOE の管理者の識別及び認証）。ただし、TOE がこのような機能を実装する場合、ST 執筆者は次の情報を取得して ST に記載する。この附属書に含まれない要件を ST に含めることはできるが、本 PP への適合を主張する前に、評価を監督する国の認証機関（スキーム）によるレビューと容認に支配される。

C.1 FCS_RBG_EXTサポート要件

203 FCS_RBG_EXT 参照規格に関する基底要件にあるいくつかの選択では、TOE は PP の本体で規定されている以上の追加の暗号機能を実装することが要求される。ST を作成する際、ST 執筆者がこのような規格を参照する選択を選ぶ場合、本節には ST の本体に必要になる追加の SFR 及び関連する保証アクティビティが含まれるだろう。

C.1.1 ブロックサイファ機能

204 ブロックサイファ機能は、NIST SP 800-90 CTR_DRBG 機能を実装するために使用される。USB フラッシュドライブには RBG 機能を実装することが要求されるため、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。

暗号操作（FCS_COP）

FCS_COP.1(1)	**暗号操作（データ暗号化）**
FCS_COP.1.1(1)	**詳細化**：TSFは、以下を満たす**CTR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、規定された暗号アルゴリズム**AES**に従って、**データ暗号化**を実行しなければならない。**FIPS PUB 197、「Advanced Encryption Standard (AES)」及び NIST SP 800-38A**。

適用上の注意

205 選択について、使用される鍵サイズは、NIST SP 800-90 の勧告と一貫するように選択される。

保証アクティビティ：

206 ECB モードテストの参照文献は The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) [AESAVS]であり、これは http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf から入手できる。

207 評価者は、このモード用のカウンタ値が導出/取得される方法が TSS に記述されていること

を確認するために TSS を検査し、記述されている実装が、各カウンタ値が所定の鍵で暗号化されるただ 1 つの平文ブロックに関連付けられるという必須特性を満たすことを確認する。

208 評価者は、TSF によってサポートされる鍵サイズごとに、1 組の答えがわかっているテストを実行しなければならない。入力は、鍵、IV、及び暗号化される平文または復号される暗号文のいずれかである。
http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip からサポートされる鍵の長さにある CTR モード用のすべてのテストベクター（暗号化及び復号の両方）を使用して、これらのテストを実行しなければならない。

209 評価者は、サポートされる鍵の長さごとにマルチブロックメッセージテストを実行しなければならない。このテストを実行するために、評価者は、暗号化用に 10 のデータセットと復号用に 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（暗号化用）または暗号文（復号用）から構成される。ブロックの長さは、128 ビットでなければならない。平文/暗号文の長さは、ブロックの長さ*i でなければならない。ここで、i はデータセット番号を表し、1〜10 の範囲にある（したがって、メッセージは 128 ビットから 1280 ビットの範囲にある）。

210 評価者は、モンテカルロテストを実行しなければならない。評価者は、暗号化用に 10 組の開始値（鍵、IV、及び平文の値）を生成し、復号用に 10 組の開始値（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。各組の開始値を使用して 100 個のテストが生成され、実行される。（開始値の組ごとに）100 個のテスト値を生成するためのアルゴリズムは[AESAVS]の 6.4.1 節に記載されている。[1]

C.1.2 ハッシュ関数

211 ハッシュ関数は、NIST SP 800-132 で Hash_DRBG、HMAC_DRBG、及び Dual_EC_DRBG のほか、PRF にも要求される。USB フラッシュドライブには RBG 機能を実装することが要求されるため、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も実装しなければならないことに注意するべきである。

FCS_COP.1(X2)	**暗号操作（暗号ハッシュ）**
FCS_COP.1.1(X2)	**詳細化**：TSFは、以下に合致する［**選択**：**SHA-1、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、256、384、512］ビット**に従って、**暗号ハッシュサービス**を実施しなければならない：**FIPS Pub 180-2、「Secure Hash Standard」**

適用上の注意：

212 この要件の意図は、ハッシュ関数を特定することである。ハッシュ選択は、メッセージダイジェストサイズ選択をサポートしなければならない。ハッシュ選択は、FCS_COP1(1)及び FCS_COP.1(2)用に使用されるアルゴリズム（128 ビット鍵の場合は SHA 256、256 ビット鍵の場合は SHA 512）の全体的強度と一貫しているべきである。おそらく、この PP の今後の刊行では、SHA-1 は暗号ハッシュに承認されるアルゴリズムではなくなるだろう。

保証アクティビティ：

213 評価者は、必要なハッシュサイズ用の機能を設定するために行う必要がある設定が存在す

[1] CTR モードは、ECB モンテカルロアルゴリズムを使用する。

ることを決定するために、AGD 文書をチェックしなければならない。

214 評価者は、以下のテストを実行しなければならない。これらの暗号ハッシュテストの参考文献は *The Secure Hash Algorithm Validation System (SHAVS) [SHAVS]*であり、これは http://csrc.nist.gov/groups/STM/cavp/documents/shs/SHAVS.pdf から入手できる。

215 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。最初のモードは、バイト指向モードである。このモードでは、TSF は、長さが整数バイトであるメッセージのみをハッシュする。すなわち、ハッシュ対象メッセージの長さ（ビット単位）は 8 で割り切れる。2 番目のモードは、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。モードごとに異なるテストがあるため、以下の節ではビット指向テストとバイト指向テストの区別を明記する。

216 評価者は、TSF によって実装され、この 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、以下のすべてのテストを実行しなければならない。

短いメッセージテスト　－　ビット指向モード

217 評価者は、*m+1* 個のメッセージ（m はハッシュアルゴリズムのブロック長）から構成される入力セットを考案する。メッセージの長さは、順番に 0～*m* ビットの範囲にある。メッセージ文は、擬似ランダム的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計算し、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。

短いメッセージテスト　－　バイト指向モード

218 評価者は、*m/8*+1 個のメッセージ（*m* はハッシュアルゴリズムのブロック長）から構成される入力セットを考案する。メッセージの長さは順番に 0～m/8 バイトの範囲にあり、各メッセージは整数バイトである。メッセージ文は、擬似ランダム的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計算し、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。

選択された長いメッセージテスト　－　ビット指向モード

219 評価者は、*m* 個のメッセージ（*m* はハッシュアルゴリズムのブロック長）から構成される入力セットを考案する。*i* 番目のメッセージの長さは、512 + 99**i*（ただし $1 \le i \le m$）である。メッセージ文は、擬似ランダム的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計算し、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。

選択された長いメッセージテスト　－　バイト指向モード

220 評価者は、*m/8* 個のメッセージ（*m* はハッシュアルゴリズムのブロック長）から構成される入力セットを考案する。*i* 番目のメッセージの長さは、512 + 8*99**i*（ただし $1 \le i \le m/8$）である。メッセージ文は、擬似ランダム的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計算し、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。

擬似ランダム的に生成されるメッセージテスト

221 このテストはバイト指向実装専用である。評価者は、*n* ビット長のシードをランダムに生成する（*n* は、テストされる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）。評価者は、次に[SHAVS]の図 1 に提供されているアルゴリズムに従って、1 組の 100 個のメッセージ及び関連ダイジェストを作成する。評価者は、次にメッセージが 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。

C.10.3 HMAC関数

222 HMAC 関数は、NIST SP 800-90 HMAC_DRBG 機能及び NIST SP 800-132 の PRF を実装するために使用される。なお、SHA 関数の使用も要求される。そのため、ST でこの要件を使用する場合は、適切な選択と共に C.1.2 のハッシュ要件も記載しなければならない。USB フラッシュドライブには RBG 機能を実装することが要求されるため、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。ただ 1 つの鍵の長さ/ハッシュ関数/ブロックサイズ/出力 MAC 長が使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を設定できる場合は、このことを反映するためにこの要件を ST に繰り返すべきである。

FCS_COP.1	**暗号操作（有鍵暗号ハッシュ）**
FCS_COP.1.1	**詳細化**：TSFは、以下を満たす**[有鍵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]**に従って、**有鍵暗号ハッシュサービス**を実行しなければならない。**FIPS 198-1**。

適用上の注意：

223 この要件内の選択は、DEK のサイズに指定されている鍵サイズと一貫していなければならない。

保証アクティビティ：

224 評価者は、HMAC 関数によって使用される次の値が TSS に指定されていることを確認するために、TSS を検査しなければならない。鍵の長さ、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 MAC 長。

225 また、評価者は、ランダムメッセージテストを実行しなければならない。このテストの参考文献は *The Keyed-Hash Message Authentication Code Validation System (HMACVS)* [HMACVS]であり、
http://csrc.nist.gov/groups/STM/cavp/documents/mac/HMACVS.pdf から入手できる。

226 評価者は、テスト用に 15 組のテストデータを作成しなければならない。各組は、鍵とメッセージデータから構成される。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.2 パスフレーズ許可

227 最低要件として、TOE は、長さが 32 文字以上のパスワード認証要素をサポートすることが要求される。これらの要素はそれが保護する鍵よりエントロピーが低いので、これらの鍵を保護するためにより長い要素を使用することが望ましい。ベンダは、大幅に強力な認証要素をサポートしてもよい。そのより複雑な性質を反映するために、これを「パスフレーズ」と呼ぶ。パスフレーズがサポートされる場合、ST 執筆者は以下のアクションを取るべきである。

228 1) 対策方針の記述で「パスワード」が現れるすべての箇所を「パスフレーズ」に変更する。

229 2) FCS_CKM.1(3)及び関連する適用上の注意と保証アクティビティを以下で置換する。

FCS_CKM.1(3) **暗号鍵生成（パスフレーズの条件付け）**

FCS_CKM.1.1(3) **詳細化：サブマスクを生成するために使用されるパスフレーズは、{大文字、小文字、及び[割付：サポートされる他の文字]}の集合の中から最大[割付：8以上の正整数個の]長さの最大[割付：9以上の正整数個の]単語を含み、以下のように条件付けされなければならない。[選択：**

- **128ビットDEK用に[選択：SHA-1、SHA-256、SHA-512]を使用する、**
- **256ビットDEK用に[選択：SHA-256、SHA-512]を使用する、**
- **FCS_RBG_EXT.1で規定されているようにランダムビット生成器を使用して生成されるソルトでNIST SP 800-132、[割付：*1000以上*の数]の繰返しカウント、及び[選択：SHA-1、SHA-256、SHA-512]を使用するHMACを使用する、**

] これは、条件付け機能の出力がDEKのサイズ（ビット数）に等しくなるようにするものである。

適用上の注意： パスフレーズとは、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に、単語の辞書からランダムに取り出される単語の並びである。この要件はパスフレーズの組成に要件を課すが、辞書から単語を選択する特定の方法は要求されない（ただし、通常、これは暗号論的にランダムに行われる）。生成される文字列は、基礎となるOSによって決定されるスキームで符号化された文字の並びから構成される。この並びは、KEKの入力として使用されるサブマスクを形成するビット列に条件付けされなければならない。条件付けは、識別されるハッシュ関数のいずれか、またはNIST SP 800-132に記載されているプロセスを使用して実行できる。使用する方法は、ST執筆者によって選択される。800-132条件付けを指定する場合、ST執筆者は実行される繰返しの数（C）を入力する。この値は、10000以上でなければならない。また、800-132では、承認されたハッシュ関数を持つHMACから構成される擬似ハッシュ関数（PRF）の使用が要求される。ST執筆者は、附属書CからのHMAC及びハッシュ関数に関する該当する要件も含めて、使用されるハッシュ関数を選択する。

USBフラッシュドライブは、鍵導出機能（または800-132に規定された条件付けによって要求される暗号操作）によって要求されるハッシュ関数を実装しなければならないことに注意するべきである。

おそらく、本PPの今後の刊行では、SHA-1は暗号ハッシュに承認されるアルゴリズムではなくなり、SP 800-132を使用した条件付けが要求されるだろう。

保証アクティビティ： このコンポーネントには、評価が必要な2つの側面がある。1～8文字の単語の辞書から選択された9個以上の単語を持つパスフ

レーズがサポートされ、入力される文字は選択した条件付け機能に支配される。これらのアクティビティについては、以下で個別に取り扱う。

最大8文字以上の9個以上の単語の長さを持つパスフレーズのサポート

評価者は、この割付文の中のSTに指定されている長さの最大単語数のパスフレーズを受け付ける機能が存在することがTSS節に指定されており、指定されている値が要件に規定されている個数以上であることを決定するために、TSS節をチェックしなければならない。また、評価者は、このようなパスフレーズを生成する管理者用の指示が存在し、パスフレーズをTOEに入力する方法がガイダンスに記載されていることを決定するために、運用ガイダンスもチェックしなければならない。

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で以下のテストも実行しなければならない。

- テスト1：TOEが、9個（または最初の割付に関してSTに規定された値のいずれか大きい方）以上の単語を持つパスフレーズをサポートすることを確認する。2番目の割付で規定された個数（または8のいずれか大きい方）以上の単語がサポートされることも検証するべきである。
- テスト2：TOEが、ベンダから提供される運用ガイダンスに規定されている内容と一致する短い長さのパスフレーズをサポートすることを確認する（例えば、ガイダンスにパスフレーズの長さが5単語以上と規定されている場合、このテストではTOEが最低でも5単語のパスフレーズを受け付けることを決定する）。
- テスト3[条件付き]：もしST執筆者が3番目の割付に追加のサポート文字を入れる場合は、TOEが、指定された特殊文字に関してAGD_OPRまたはAGD_PREガイダンスに含まれるガイダンスに規定されているように構成されたパスフレーズのサポートを備えていることを確認する。例えばパスフレーズが特殊文字を含まなければならないとガイダンスに規定されている場合、このテストはTOEが英数字しかサポートしていない場合に失敗する。

  パスフレーズ条件付け

  SHAベースのパスフレーズ条件付けについては、評価者は以下のアクティビティを実行する。評価者は、最初にパスフレーズを符号化し、それからSHAアルゴリズムに渡す方法がTSSに記載されていることをチェックしなければならない。

  アルゴリズムの設定値（パディング、ブロッキングなど）が記述されなければならず、評価者は、これらが

このコンポーネントでの選択及びハッシュ関数自体に関するFCS_COP.1(3)での選択によってサポートされることを検証しなければならない。評価者は、ハッシュ関数の出力を使用してFCS_CKM.1(2)に記載されている関数に入力されるサブマスクを形成する方法の記述がTSSに含まれており、FCS_CKM.1(1)に規定されているようにDEKと同じ長さであ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ついては、必要な保証アクティビティは、該当する附属書C要件の保証アクティビティを実行するときに実行される。KEKを形成するために使用されるサブマスクを形成するときにマスター鍵の操作が実行される場合は、そのプロセスをTSSに記載しなければならない。

入力されるパスフレーズからのサブマスクの形成を明示的にテストする必要はない。

C.3 認証要素/サブマスク生成

230 TOE は、ホスト分割認証要素または PIN 保護方式のサブマスクを生成する必要はない。ただし、TOE がこのサービスを提供する場合は、TOE がこの機能に関するクレジットを主張するために、以下のコンポーネントを ST に含める必要がある。この附属書に含まれない他のタイプの認証要素/サブマスクに関する要件は、本 PP への適合を主張する前に、評価を監督する国の認証機関（スキーム）によるレビューと容認に支配される。

231 TOE は、それ自体または他の認証要素と組合せて使用されるパスワード認証要素をサポートしなければならない。TOE によってサポートされる認証要素は、FCS_CKM.1(2)に規定される。また、FCS_CKM.1(2)は、認証要素から導出される様々なサブマスクを組み合わせて KEK を形成する方法も規定する。ホスト分割認証要素または PIN 保護方式のサブマスクが使用される場合は、本 PP に適合するために、下記の適切な要件を ST に含めなければならない。ホスト分割認証要素及び PIN 保護方式のサブマスクは、TOE によって生成されなければならない。なお、ホスト分割認証要素の性質は、最終的にホストに保存される分割を（ホスト分割が生成されるときに TOE をサポートするホスト以外の）外部の手段を通じてホストに保存しなければならないことである。

C.3.1 ホスト分割認証要素生成

232 ホスト分割認証要素は、ホスト分割サブマスクと同一である。それはホストプラットフォームに保存されるランダムビット列である。下記のコンポーネントには、このような認証要素/サブマスクの生成と保存に関する要件が含まれる。

FCS_CKM_EXT.1(X1) **暗号鍵生成（ホスト分割認証要素）**

FCS_CKM_EXT.1.1(X1) TSFは、FCS_CKM.1(1)で規定されるように、DEKのサイズ以上のエントロピーでシードされた[選択：128ビット、256ビット]の認証要素を生成する、FCS_RBG_EXT.1で規定されるランダムビット生成器を使用して、ホスト分割認証要素を生成しなければならない。

FCS_CKM_EXT.1.2(X1) TSFは、生成されるホスト分割認証要素を、生成するホストに保存できなければならない。

FCS_CKM_EXT.1.3(X1) TSFは、ホスト分割認証要素が生成するホストに保存されたら、USBフラッシュドライブ上のホスト分割認証要素を消去しなければならない。

適用上の注意：

233 選択は、FCS_CKM.1(1)で DEK 用に規定されたものと同じビット数を示すべきである。「生成するホスト」とは、ホスト分割認証要素が生成されるときに USB フラッシュドライブに接続されているホストである。ランダムビット生成器は、TOE 上のランダムビット生成器である（FCS_RBG_EXT）。

保証アクティビティ：

234 評価者は、管理者がホスト分割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ために、ガイダンス文書をレビューする。評価者は、生成機能が RBG を使用する方法、及び RBG 機能がシードされる方法（これが RBG の他の使用と異なる場合）など、認証要素生成プロセスが記述されていることを確認するために、ST の TSS 部分をレビューする。評価者は、生成するホストで RBG によって生成される値が確立される方法を決定するために、TSS 節（または管理ガイダンス文書）をレビューする（他のホストでそれを確立するための手順は、AGD_PRE 保証アクティビティで取り扱われる）。最後に、評価者は、生成するホストに分割が保存された後、どの時点でどの手段によってどのように USB デバイス上のホスト分割が消去されるかが TSS に記述されていることを確認する。

235 評価者は、以下のテストを実行しなければならない。

- テスト 1：管理ガイダンスに従って、ホスト分割認証要素を作成する。可能な場合は、認証要素に含まれるビット数を確認する。この認証要素を使用して、暗号化された TOE にアクセスできることを確認する。

C.3.2 PIN保護方式のサブマスク

236 PIN 保護方式のサブマスクとは、TOE の永続メモリの保護された部分に保存され、PIN 認証要素によってアクセスされるランダムビット列のサブマスクである。下記のコンポーネントには、このようなサブマスクの生成と保存に関する要件が含まれる。PIN が最初に確立された後で PIN の変更を TOE が許可する場合、ST 執筆者は、この機能を FMT_SMF.1(d)に指定しなければならない。さらに、パスワード/パスフレーズ認証要素を検証する（FIA_AUT_EXT.1.3 でパスワード認証要素の変更が行われるように）または既存の PIN を検証することで、変更の許可を確立するための要件を指定する必要がある。

FCS_CKM_EXT.1(X2) 暗号鍵生成（TOEに保存されるサブマスク）

FCS_CKM_EXT.1.1(X2) TSFは、FCS_CKM.1(1)で規定されるように、DEKのサイズ以上のエントロピーでシードされた[選択：128ビット、256ビット]のサブマスクを生成する、FCS_RBG_EXT.1で規定されるランダムビット生成器によって生成されるPIN保護方式のサブマスクを導出しなければならない。

FCS_CKM_EXT.1.2(X2) TSFは、[割付：最小桁数]から[割付：最大桁数,20以上でなければならない]の範囲のPINを入力することで保護され[割付：サブマスクが保護される手段]、アクセスされる、生成されたサブマスクをUSBフラッシュドライブに保存できなければならない。

適用上の注意：

237 最初のエレメントに関する選択は、FCS_CKM.1(1)で DEK 用に規定されたものと同じビット数を示すべきである。2 番目のエレメントで、最初の割付は、PIN で行われる操作を含めて認証要素を保護する方法で埋めるべきである。PIN 保護方式のサブマスクは（暗号化されていない鍵関連情報を永続メモリに書き込んではならないとする）FDP_DSK_EXT.1.4 の例外であるが、サブマスクが USB フラッシュドライブ上の保護されているメモリに書き込まれるまで他の永続メモリに書き込むことができないという事例でなければならない。2 番目と 3 番目の割付は、（それぞれ）PIN の最小サイズと最大サイズを指定する。適合する TOE は、20 桁以上の PIN をサポートできなければならない。ランダムビット生成器は、USB フラッシュドライブ上のランダムビット生成器である（FCS_RBG_EXT）。

保証アクティビティ：

238 評価者は、管理者が PIN 保護方式のサブマスク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ために、ガイダンス文書をレビューする。評価者は、生成機能が RBG を使用する方法、及び RBG 機能がシードされる方法（これが RBG の他の使用と異なる場合）など、認証要素生成プロセスが記述されていることを確認するために、ST の TSS 部分をレビューする。評価者は、生成する TOE で RBG によって生成される値が確立される方法を決定するために、TSS 節（または管理ガイダンス文書)をレビューする。これには、PIN が確立される方法、サブマスクが USB フラッシュドライブの保護された部分に書き込まれる前に永続メモリに書き込まれない方法の詳細、及び（書き込まれた)サブマスクが USB フラッシュドライブ上で保護される方法が含まれる。なお、該当する FCS_COP 要件を使用して、使用される暗号が ST に指定される（まだ指定されていない場合)。PIN を収集するためのインタフェースが記述されなければならない。

239 評価者は、以下のテストを実行しなければならない。

- テスト1：運用ガイダンスに従って、PIN保護方式のサブマスクを作成する。可能な場合は、サブマスクに含まれるビット数を確認する。PINを確立し、このPINが暗号化されるTOEにアクセスするために使用できるサブマスクへのアクセスを提供することを確認する。間違ったPINがデータへのアクセスを提供しないことを確認する。
- テスト2：要件に規定された最小のPIN長より短いPIN（そのPIN長が1より大きい場合)及び最大長より長いPINの確立を試みる。PINが確立されず、暗号化されたデータへのアクセスが許可されないことを確認する。
- テスト3：割付に指定されている最小値と最大値のPINを確立する。これらのPINが正常に確立され、暗号化されたデータへのアクセスが許可されることを確認する。

C.5　PIN認証要素入力失敗処理

240　TSF に PIN 保護方式のサブマスクが含まれる場合、一般に PIN 認証要素は、（ビット数/桁数の観点から）それが保護するサブマスクより大幅に強度が低い。PIN 推測攻撃を防止するために、USB デバイスを攻撃者からロックする連続推測回数に制限を課すことができる。ST のこの機能が要求される箇所に、次の要件を記載するべきである。

241 このコンポーネントが含まれる場合は、以下の対策方針と根拠を ST に追加するべきである。

O.ANTI_HAMMER	TSFは、PIN保護方式のサブマスクに対するブルートフォースPIN推測試行を軽減するためのメカニズムを実装する。

T.KEYSPACE_EXHAUST 許可されていない利用者は、データまたはTOE資源への無許可アクセスの取得を目指して暗号鍵または認証要素を決定するためにブルートフォース攻撃を試みることがある。	O.ANTI_HAMMER TSFは、PIN保護方式のサブマスクに対するブルートフォースPIN推測試行を軽減するためのメカニズムを実装する。	O.ANTI_HAMMERに規定されているPIN保護方式のサブマスクに対するブルートフォース攻撃の実効性を制限するメカニズムの実装により、鍵空間総当り攻撃が成功する可能性が低いことが保証される。

O.ANTI_HAMMER TOEは、TSFが運用環境で正しく動作することを検証する機能を提供しなければならない。	FIA_AFL_EXT.1	FIA_AFL_EXT.1は、USBデバイスをロックする前の連続PIN認証要素入力失敗回数の制限を要求する。制限が十分小さいなら、推測回数を効果的に制限し、ブルートフォース攻撃の効果を低減する。

拡張：許可失敗処理（FIA_AFL）

FIA_AFL_EXT.1	**許可失敗処理**
FIA_AFL_EXT.1	TSFは、[割付：間違ったPIN入力回数]連続失敗PIN入力試行が行われたとき、DEKをゼロ化しなければならない。

適用上の注意：

242　（サブマスクのサイズに対し）比較的短い PIN がブルートフォース攻撃にさらされる脅威を低減するために、このコンポーネントは、指定回数の許可失敗の後で DEK をゼロ化する（その結果、デバイス上のすべてのデータが消失する）ことを要求する。この回数は ST 執筆者によって指定される。

保証アクティビティ：

243　評価者は、許可失敗試行を検出する方法及び連続した失敗を追跡する方法が記述されていることを決定するために、TSS を検査しなければならない。これには、デバイスがホストから切断されてから再接続された後の失敗が含まれる。評価者は、次のテストも実行しなければならない。

- テスト 1：評価者は、指定回数の連続許可失敗が行われたとき、その後正しい PIN が入力されても、デバイス上のデータにアクセスできなくなることを検証しなければならない。評価者は、USB フラッシュドライブが継続的にホストに接続されているときに 1 回以上のテストが実行され、デバイスが取り外されてから再接続されたときに 1 回以上のテストが実行されることを確認しなければならない。

附属書 D：本書の表記規則

244 英国綴りを米国綴りで置き換えたことを除き、本 PP に使用される表記、書式、及び表記規則は、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。ここでは、PP 読者の役に立つように一部を抜粋して示す。

245 本 PP で使用される表記、書式、及び表記規則は、コモンクライテリア（CC）のバージョン 3.1 と概ね一貫している。ここでは、PP 読者の役に立つように一部を抜粋して示す。CC は、機能要件と保証要件に対していくつかの操作を実行することを許可する。詳細化、選択、割付、及び繰返しは、CC 3.1 パート 1 の附属書 C4 に定義されている。これらの各操作は本 PP で使用される。

詳細化表記規則

246 **詳細化**操作は、要件に詳細を追加し、さらに要件を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、太字の要件内のエレメント番号と追加テキストの後の**太字**の「詳細化」という語句によって示される。

選択表記規則

247 **選択**操作は、要件の記載中の CC によって提供される 1 つまたは複数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 執筆者によって行われた選択は、**太字**で選択を示し、括弧及び「選択」という語句は削除される。ST 執筆者によって埋められるべき選択は、[選択：]として角括弧内に示され、選択が行われるべきことを示す。

割付表記規則

248 **割付**操作は、パスワードの長さのように指定されていないパラメタに特定の値を割り付け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）。**太字**で示される値は PP 執筆者によって行われた割付を示し、括弧及び「割付」という語句は削除される。ST 執筆者によって埋められるべき割付は、[割付：]として角括弧内に示され、割付が行われるべきことを示す。

繰返し表記規則

249 **繰返し**操作は、コンポーネントが様々な操作で置換されるときに使用される（CC 3.1 パート 1 附属書 C.4.1 を参照）。繰返し回数（iteration_number）は、コンポーネント識別子の後に括弧内に示される。

250 繰返し操作は、すべてのコンポーネントに対して実行できる。PP/ST 執筆者は、同じコンポーネントに基づいて複数の要件を含めることで繰返し操作を実行する。コンポーネントの繰返しは、それぞれそのコンポーネントの他のすべての繰返しと異なっていなければならない。それには、別の方法で割付と選択を行うか、別の方法で詳細化を適用する。

拡張要件表記規則

251 執筆者のニーズを満たすのに適した要件が CC にない場合、拡張要件を使用できる。**拡張要件**は識別されなければならず、要件を明確にする上で CC クラス/ファミリ/コンポーネントモデルを使用することが要求される。拡張要件は、コンポーネント内の「EXT」の挿入で示される。

適用上の注意

252 適用上の注意には、適合する TOE 用のセキュリティターゲットの構築に関連するまたは役に立つと見なされる追加の補足情報及び開発者、評価者、及び ISSE に対する一般的な情報が含まれる。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助言も含まれる。

保証アクティビティ：

253 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関する共通評価方法として機能する。アクティビティには、評価者が TSS の記載に従って TOE の特定の側面を分析するための指示が含まれる。したがって ST 執筆者には、この情報を TSS 節に記載する暗黙的要件が課される。これらのアクティビティは、本バージョンの PP では機能コンポーネントと保証コンポーネントに直接関連しているが、将来のバージョンではこれらの要件が別の附属書または文書に移動される可能性がある。

附属書 E：用語

管理者（administrator）ー TOEを設定または更新する管理者権限を持つ利用者。

認証要素（AF：authorization factor）ー 利用者（及び潜在的にホスト）がUSBフラッシュドライブの使用を許可されたコミュニティに属することを確立するために利用者によって提供される値またはホスト上に存在する値。認証要素は、KEKを形成するために使用されるサブマスクを生成する。認証要素がサブマスクと同一の場合もある。なお、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。

許可された利用者（authorized user）ー TOEを使用するための認証要素を管理者から提供された利用者。

データ暗号化（data encryption）ー USBフラッシュドライブに書き込まれるすべての利用者データを暗号化するプロセス。

データ暗号鍵（DEK：data encryption key）ー USBフラッシュドライブ上のデータを暗号化するために暗号化アルゴリズムによって使用される鍵。

決定性ランダムビット生成器（DRBG：deterministic random bit generator）ー 秘密の最初のシード値からビット列を生成する暗号アルゴリズム。シード値の知識がない場合、出力シーケンスはDRBGのセキュリティレベルまで予測不能であるべきである。

エントロピー源（entropy source）ー この暗号機能は、1つまたは複数のノイズ源からの出力を蓄積して、ランダムビット生成器用のシードを提供する。機能には、与えられた出力を推測するために必要な最小作業の指標及びノイズ源が正常に動作することを確認するためのテストが含まれる。

ホスト分割認証要素（**host split** authorization factor）**ー** サブマスクでもある認証要素。（オプションでUSBフラッシュドライブ上に）RNGによって作成され、ソースホストとターゲットホストに配付され、保存される。

鍵暗号鍵（KEK：key encryption key）ー DEKをマスクするために使用される鍵。1つ以上の認証要素から導出されるサブマスクから構成される。

鍵関連情報（keying material）ー KEK、DEK、サブマスク、認証要素及び乱数または鍵が導出されるその他の値。

ノイズ源（noise source）ー 非決定性エントロピー生成アクティビティを含んでいるRBGのコンポーネント。

運用環境（operational environment）ー TOE境界の外部にあってTOE機能及びセキュリティ方針をサポートするハードウェア及びソフトウェア。これには、ホストプラットフォーム、そのファームウェア、及びオペレーティングシステムが含まれる。

パスワード（password）ー ある程度までデバイス上のデータに対する許可に使用される短い文字列。

パスフレーズ（passphrase）ー ある程度までデバイス上のデータに対する許可に使用できる長い文字列。

永続メモリ（persistent memory）ー 電源を切っても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：random bit generator）ー 鍵関連情報を生成するために必要なランダムビットのために呼び出されるエントロピー源とDRBGから構成される暗号機能。

SAR（security assurance requirements：セキュリティ保証要件）ー 開発者と評価機関がセキュリティ機能要件適合を実証するための開発方法と評価方法を記述する。

SFR（security functional requirement：セキュリティ機能要件）ー TOEによって満たされなければならないセキュリティ機能を記述する。

ST（security target：セキュリティターゲット）ー TOEのセキュリティ特性を記述し、識別する。

シャットダウン（Shutdown）ー USBフラッシュドライブの抽出またはソフトウェア抽出、または電源を切ること、またはホストプラットフォームの意図しない電源喪失。

ソフトウェア抽出（software extraction）ー 運用環境を使用してUSBフラッシュドライブの電源を切る、またはUSBフラッシュドライブを取り外すプロセス。

サブマスク（submask）ー KEKを形成するために使用される認証要素から導出される値。

システムファイル（system file）ー デバイスの操作に使用されるUSBフラッシュドライブ上に常駐するファイル。これには、デバイスがホストに挿入されるとき、最初にホスト環境に読み込まれるソフトウェアが含まれる。デバイスを使用する準備のために異なる媒体から運用環境にインストールされるソフトウェア（付属CD-ROMからのドライバなど）は含まれない。

TOE（target of evaluation：評価対象）ー USBフラッシュドライブ上のデータを暗号化するという要件を満たす製品または製品の集合を指す。これには、USBハードウェア自体、USBに常駐するデバイスのセキュリティ機能を実装するすべてのファームウェア、及びデバイスを操作するために使用されるソフトウェア（システムファイル）が含まれる。

TOEセキュリティ機能（TSF：TOE security functionality）ー TSPの正しい実施に依存しなければならないすべてのハードウェア、ソフトウェア、及びTOEのファームウェアから構成されるセット。

TOEセキュリティ方針（TSP：TOE security policy） ー TOE内の資産を管理、保護、配付する方法を規定する1組のルール。

TOE要約仕様（TSS：TOE summary specification）ー TOEの操作とセキュリティ機能要件の実装を理解できるように、TOEがSFRを満たす方法を十分な詳しさで記述する説明。

高信頼ホスト（trusted host）ー USBフラッシュドライブによって保護される利用者データの価値に応じて、USBフラッシュドライブに適切なセキュリティを提供するために設定され、保守されるソース/ターゲットホスト。

許可されていない利用者（unauthorized user）ー （正しい認証要素の所有による）TOEの使用を許可されていない利用者。

利用者データ（user data）ー　ホストに元々存在するすべてのデータ、またはホストに元々存在するデータから導出されるすべてのデータ。TOE製造者からのシステムファイルや署名付きファームウェア更新を除く。

揮発性メモリ（volatile memory）ー　電源を切ると内容が消えるメモリ。

ゼロ化する（zeroize）ー　この用語は、メモリ位置を逆参照することと積極的に定数でメモリ位置を上書きすることを区別するために使用される。 鍵関連情報は、もはや不要になったとき、上書きされる必要がある。

附属書 F：PP の識別

タイトル：	USBフラッシュドライブのためのセキュリティ要件
バージョン：	1.0
スポンサー：	国家安全保障局（NSA）
CC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
キーワード：	認証要素、許可サブシステム、DEK、データ暗号化、 暗号化サブシステム、エントロピー、KEK、ノイズ源