ドライブ全体暗号化のコラボラティブ プロテクションプロファイルー暗号エンジン

バージョン 2.0

2016 年 9 月 9 日

バージョン 2.0

平成 29 年 3 月 15 日　翻訳第 1.0 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

謝辞

本コラボラティブプロテクションプロファイル(cPP) は、産業界、政府機関、コモンクライテリア評価機関、及び学術会員メンバーからの代表者の参加する、Full Drive Encryption international Technical Community (FDE iTC) によって開発された。

0. 序文

0.1 本書の目的

本書は、コモンクライテリア (CC) コラボラティブプロテクションプロファイル(cPP) としてドライブ全体暗号化 - 暗号エンジン (訳注：原文は Encryption Engine, EE) に関するセキュリティ機能要件 (SFR) 及びセキュリティ保証要件 (SAR) を記す。ある製品が本 cPP において取り込まれた SFR を満たすかどうかを決定するために評価者が実行するアクションを特定する評価アクティビティは、*サポート文書 (必須技術文書) ドライブ全体暗号化：暗号エンジン 2016 年 9 月*に記述されている。

完全な FDE ソリューションは、許可取得 (訳注：原文は Authorization Acquisition, AA) コンポーネントと暗号エンジンコンポーネントの両方を要求する。製品は全体のソリューションを提供し、及び本 cPP 及び FDE-AA cPP へ適合主張してもよい。

しかし、AA/EE プロテクションプロファイルスイートは初期段階にあり、すべての依存製品が cPP へ適合することを必須とすることはまだできない。認証されていない依存製品 (例えば、EE) が、関連する国のスキームによる決定に基づき、ケースバイケースで、AA TOE／製品に関して運用環境の一部として受け入れ可能と考えてもよい。

FDE iTC は、FDE cPP の両方に適合主張できるようなセキュリティターゲット (ST) の開発において助けとなる両方のコンポーネント (すなわち、AA と EE) を提供する製品の開発者がガイダンスを開発することを意図している。注意すべき一つの重要な観点は以下のとおりである：

ST 作成者への注釈： ASE_TSS において、選択が完成されなければならない。本 cPP において SAR を単に参照できないものがある。

0.2 本書の適用範囲

開発及び評価プロセスにおける cPP の適用範囲は、IT セキュリティ評価のためのコモンクライテリア[CC] に記述されている。特に、cPP は、TOE の特定の技術分野の IT セキュリティ要件を定義し、適合 TOE によって満たされるべきセキュリティ機能要件と保証要件を特定する。

0.3 想定される読者層

本 cPP の対象読者は、開発者、CC 消費者、システムインテグレータ、評価者及びスキームである。

0.4 関連する文書

プロテクションプロファイル

[FDE – AA] ドライブ全体暗号化のコラボラティブプロテクションプロファイル– 許可取得、バージョン 2.0、2016 年 9 月 9 日

コモンクライテリア [1]

[CC1] 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、
パート 1：概説と一般モデル、
CCMB-2012-09-001、 バージョン 3.1 改訂第 4 版、2012 年 9 月。

[CC2] 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、
パート 2：セキュリティ機能コンポーネント、
CCMB-2012-09-002、バージョン 3.1 改訂第 4 版、2012 年 9 月。

[CC3] 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、
パート 3：セキュリティ保証コンポーネント、
CCMB-2012-09-003、バージョン 3.1 改訂第 4 版、2012 年 9 月。

[CEM] 情報技術セキュリティ評価のための共通方法、
評価方法
CCMB-2012-09-004、バージョン 3.1 改訂第 4 版、2012 年 9 月。

[SD] サポート文書 (必須技術文書)、ドライブ全体暗号化：暗号エンジン、
2016 年 9 月

[1] For details see http://www.commoncriteriaportal.org/

0.5 改訂履歴

バージョン	日付	説明
0.1	2014 年 8 月 26 日	iTC レビュー用初期リリース
0.2	2014 年 9 月 5 日	公開レビュー用ドラフト発行
0.13	2014 年 10 月 17 日	公開レビューからのコメントを取り込む
1.0	2015 年 1 月 26 日	CCDB レビューからのコメントを取り込む
1.5	2015 年 9 月 2 日	iTC により開発された追加の適用例に基づく改訂
2.0	2016 年 9 月 9 日	公開レビューからのコメントの取り込み、及び鍵破棄セクションと AVA_VAN の更新

目次

図／表

1. PP 序説

1.1 PP 参照識別

PP 参照： collaborative Protection Profile for Full Drive Encryption - Encryption Engine (ドライブ全体暗号化のコラボラティブプロテクションプロファイルー暗号エンジン)

PP バージョン: 2.0

PP 日付: 2016 年 9 月 9 日

1.2 FDE コラボラティブ PP (cPPs) の取組みへの序説

ドライブ全体暗号化(FDE)：許可取得 (AA) 及び暗号エンジン (EE) のためのコラボラティブプロテクションプロファイルの初版の目的は、ストレージを内蔵するデバイスを紛失した際の保存データ保護のための要件を提供することである。これらの cPP は、要件を満たすためにソフトウェア及び／またはハードウェアでの FDE ソリューションを許容している。ストレージデバイスのフォームファクタは、変わるかもしれないが、以下を含むと考えられる：サーバ、ワークステーション、ラップトップ、モバイルデバイス、タブレット、外部メディアにおけるシステムハードドライブ／ソリッドステートドライブ。ハードウェアソリューションは、自己暗号化ドライブまたはほかのハードウェアベースのソリューション：ホストマシンにストレージデバイスを接続するために使用されるインタフェース (USB、SATA 等) は、本 PP の適用範囲外である。

ドライブ全体暗号化は、ストレージデバイス上のすべてのデータ (一定の例外あり) を暗号化し、FDE ソリューションへの許可取得に成功した後にのみデータへのアクセスが許可される。例外として、マスターブートレコード (MBR) またはその他の AA/EE 事前認証ソフトウェアのようなものについて、ストレージデバイスの一部を暗号化しないままにする必要性がある。これらの FDE cPP は、用語「ドライブ全体暗号化」の解釈として、利用者データまたは認証データを含まない場合に限り、ストレージデバイスの一部分を暗号化しないままにすることを FDE ソリューションに許容する。

FDE cPP は、さまざまなソリューションをサポートするので、２つの cPP は、図 1 に示される FDE コンポーネントについての要件を記述している。

図 1：FDE コンポーネント

FDE cPP – 許可取得(AA) は、許可取得部分の要件、及び利用者との対話や結果的に暗号エンジンへ境界暗号化値 (BEV：Border Encryption Value) を送信可能となるために必要なセキュリティ要件と保証アクティビティの詳細を記述している。

FDE cPP - 暗号エンジン (EE) は、暗号エンジン部分の要件、及び DEK (Data Encryption Key) によるデータの実際の暗号化／復号のために必要なセキュリティ要件及び保証アクティビティの詳細を記述している。それぞれの cPP は、管理機能、暗号鍵の適切な取扱い、高信頼な方法で実行されるアップデート、監査及び自己テストのための中核となる要件についても記述している。

本 TOE 記述は、暗号エンジンの適用範囲と機能を定義し、セキュリティ課題定義は、cPP 要件が対処する EE に対する運用環境と脅威についてなされた前提条件を記述する。

1.3 実装

ドライブ全体暗号化ソリューションは、実装やベンダの組み合わせにより変わる。

したがって、ベンダは、ドライブ全体暗号化ソリューション(AA と EE) の両方のコンポーネントを提供する製品について両方の cPP に適合した評価を行うーこれは、ひとつの ST を使って 1 回の評価において実行可能である。FDE ソリューションの単一のコンポーネントを提供するベンダは、適用可能な cPP に適合した評価のみを行う。FDE cPP は、評価機関が一つの cPP または他に合わせたソリューションを個別に評価できるように 2 つの文書に分かれている。ある顧客が FDE ソリューションを調達するとき、彼らは AA+EE cPP を満たす単一のベンダ製品または 2 つの製品、ひとつは AA を満たし、他は EE cPP を満たすようなものを得ることができる。

以下の表に、認証のためのいくつかの例を示す。

表 1：cPP 実装の例

実装	cPP	説明
ホスト	AA	自己暗号化ドライブへのインタフェースを提供する ホストソフトウェア
自己暗号化ドライブ (SED)	EE	別のホストソフトウェアとの組み合わせで使用された自己暗号化ドライブ
ソフトウェア FDE	AA + EE	ソフトウェアによるドライブ全体暗号化ソリューション
ハイブリッド	AA + EE	単一ベンダのハードウェア(例、ハードウェア暗号エンジン、暗号コプロセッサ)とソフトウェアの組合せ

1.4 評価対象 (TOE) の概要

本 cPP の評価対象は、暗号エンジン単体、または FDE の一連の cPP (許可取得と暗号エンジン)を組み合わせのいずれかである。

以下のセクションは、FDE EE cPP の機能概要をセキュリティ機能と同様に提供する。

1.4.1 暗号エンジンの序説

暗号エンジン cPP の目的は、データ暗号化、ポリシー実施、及び鍵管理にフォーカスしている。EE は、管理下の DEK 及びその他の中間鍵の生成、更新、アーカイブ、リカバリー、保護及び破棄に責任がある。EE は、AA より BEV を受け取る。EE は、DEK の復号用の BEV を利用するが、２つの点の間に内在するかもしれないその他の

中間鍵が存在してもよい。鍵暗号化鍵 (KEK) はその他の鍵、とりわけ DEK または DEK へ chain するその他の中間鍵ををラッピングする。鍵解放鍵(KRK)は、EE が DEK か、DEK へ chain するその他の中間鍵 のいずれかを出力する権限を付与する。これらの鍵は機能的な用途においてのみ異なる。

EE は、AA により提供された KEK または KRK に基づく要求されたアクションを許可するか、または拒否するかを決定する。要求される可能性のあるアクションは、暗号鍵の変更、データの復号、暗号鍵(DEK を含む)のサニタイズ(Sanitization)等を含むが、これらに限らない。EE は、ストレージデバイスの暗号文または暗号化されない部分へのアクセスを防止するための追加ポリシーの実施を提供してもよい。さらに、EE は、個人ベースで複数利用者向けの暗号サポートを提供してもよい。

図 2 は、EE 内部の構成要素と AA との関連性について説明している。

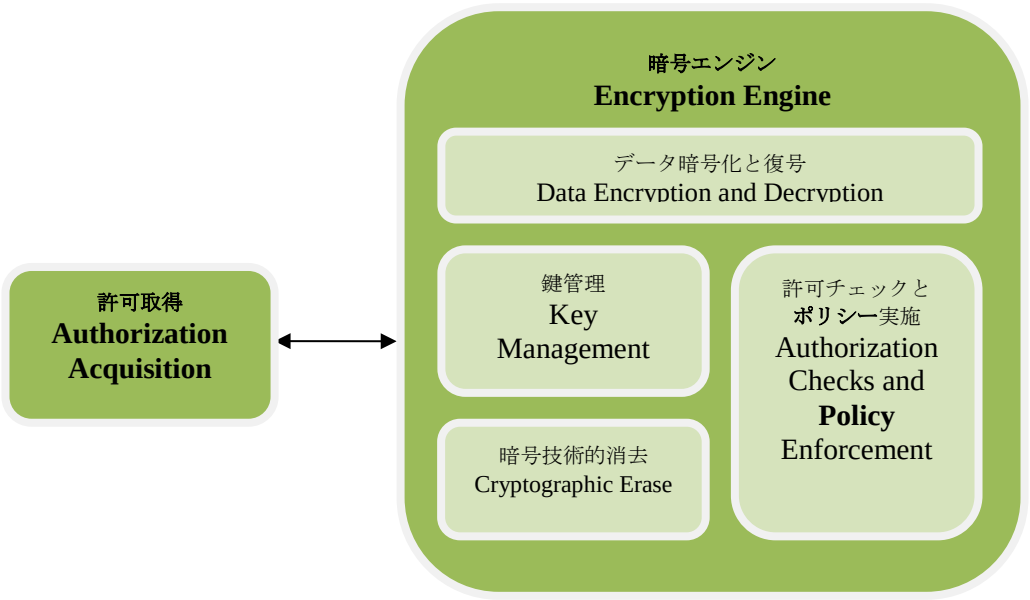


図 2：暗号エンジンの詳細

1.4.2 暗号エンジンのセキュリティ機能

暗号エンジンは、所定のアルゴリズムのセットを用いてデータが暗号化されることを保証する究極の責任がある。EE は、AA によって提供された BEV の有効性に基づく DEK の復号を通してストレージデバイス上のデータの復号を管理する。それは、DEK の変更、DEK の復号または出力のために要求される BEV の管理、その制御下にある中間的なラッピング鍵の管理、及び鍵サニタイズの実行等の管理者機能を管理する。

EE は、鍵のアーカイブ及び回復機能を提供してもよい。EE は、それ自身のアーカイブまたは回復、または本機能を実行するための AA とのインタフェースを管理し

てもよい。また、鍵材料の移動を制限したり、回復機能を無効化したりするような設定可能な機能を提供してもよい。

ストレージデバイス暗号化の最大のセキュリティ対策方針は、DEK またはその他の中間鍵の回復のために極めて大きな鍵空間に対して敵対者が総当たり検索を実行せざるを得なくすることである。EE は、承認された暗号を使用して、鍵を生成、取扱い、及び保護することによって、紛失または盗難にあって電源の入っていないプラットフォームを取得したが、許可要素または中間鍵の知識を持たない攻撃者には、データを取得するために中間鍵または DEK の暗号鍵空間を総当たり攻撃せざるを得なくする。EE は、DEK を、またある場合には中間鍵もランダムに生成する。EE は、ストレージデバイス上のストレージユニット (例えば、セクタまたはブロック) を暗号化するためのモードとして適切な初期化ベクタを持った適切なモードで対称鍵暗号アルゴリズムにおいて DEK を使用する。EE は、DEK を KEK または中間鍵のいずれかで暗号化する。

本バージョンの cPP には、高度な省電力要件とファームウェア署名要件を含む、追加のセキュリティ上の機能が含まれている。

1.4.3 TOE 及び運用／Pre-Boot 環境

EE 機能が置かれる環境は、運用におけるプラットフォームのブート段階に依存して異なるかもしれない、図 3 を参照。初期化、及びおそらく許可の観点は、Pre-Boot 環境、プロビジョニング、暗号化、復号、及び管理機能がオペレーティングシステム環境で実行されている間で、実行されるかもしれない。これらの観点のいくつかは、両方の環境で発生するかもしれない。

オペレーティングシステム環境は、ハードウェアドライバ、暗号ライブラリ、及びおそらくその他の TOE 外部のサービスを含めて、暗号エンジンに対してあらゆるタイプのサービスを利用可能にさせている。

プリブート環境は、機能が制限されているという意味で、はるかに制限されている。本環境は、最小限の周辺機器を起動し、プラットフォームをコールドスタートから、アプリケーションの動作を含めて完全に機能するオペレーティングシステムを実行させるのに必要なドライバのみをロードする。

EE TOE は、運用環境内の機能を含めるかまたは利用してもよい。

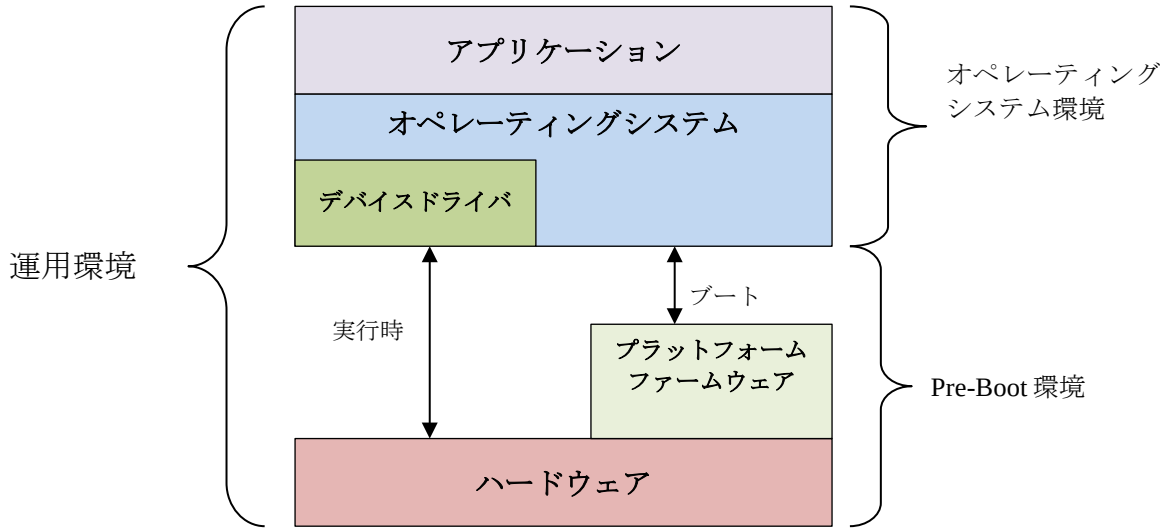


図3：運用環境

1.5 次の cPP まで猶予された機能

時間的な制約のため、本 cPP では、いくつかの重要な機能についての要件を次期バージョンの cPP まで見送った。これらは、パーティション／ボリューム管理に関する要件が含まれる。

1.6 TOE 適用例

FDE cPP に適合する製品の適用例は、敵対者からの事前アクセスなしに電源オフの間に紛失または盗難にあったデバイス上の保存データを保護することである。敵対者が電源オンの状態でデバイスを取得し、環境または TOE そのものに改変を加えること(例、悪意のメイド攻撃)ができるような適用例は、これらの cPP(すなわち、FDE-AA 及び FDE-EE)によって対処されない。

2. CC 適合主張

参照文書 [CC1], [CC2] 及び [CC3] により定義されるとおり、本 cPP は、コモンクライテリア v3.1、改訂第 4 版の要件に適合する。本 cPP は、CCv3.1r4、CC パート 2 拡張及び CC パート 3 適合である。 拡張コンポーネント定義は、附属書 C にある。

cPP 評価に適用される方法は、[CEM] に定義されている。

本 cPP は、以下の保証ファミリを満たしている： APE_CCL.1, APE_ECD.1, APE_INT.1, APE_OBJ.1, APE_REQ.1 及び APE_SPD.1。

本 cPP は、別の PP への適合を主張しない。

本 cPP に適合するためには、TOE は*完全適合(Exact Compliance)*を論証しなければならない。*完全適合*は、本 cPP のセクション 5 のすべての要件を含み、本 cPP の附属書 A または附属書 B の要件を含む可能性のある ST として定義される。繰り返しは許容されているが、いかなる追加の要件 (CC パート 2 または 3 からのもの) も ST に含めることは許容されない。さらに、本 cPP のセクション 5 のいかなる要件も、省略は許されない。

3. セキュリティ課題定義

3.1 脅威

本セクションは要件が対応する脅威をどのように軽減するかを記述する物語を提供する。ある要件は、複数の脅威の側面を軽減するかもしれない。ある要件は、限定された方法で脅威を軽減するのみかもしれない。いくつかの要件は、TSF が主張される追加の要件なしに脅威を十分に軽減するか、または TSF がオプション要件に記述される機能を提供する運用環境を信頼するかのいずれかのため、オプションである。

脅威は 1 つの脅威エージェント、資産及びその資産におけるその脅威エージェントの有害なアクションからなる。脅威エージェントは、敵対者が紛失または盗難にあったストレージドライブを取得した場合に資産に対してリスクを負わせるエンティティのことである。脅威は、評価対象 (TOE) の機能要件を導く。例えば、以下のある脅威は T.UNAUTHORIZED_DATA_ACCESS である。脅威エージェントは、紛失または盗難にあったストレージデバイスの所持者(許可されない利用者)である。資産はストレージデバイス上のデータであるが、有害なアクションはストレージデバイスからそれらのデータを得ようと試行することである。この脅威は、ストレージデバイス暗号化 (TOE) のための機能要件が、ハードディスクのアクセスとデータの暗号化／復号のために TOE を使用できる人を許可するように方向付ける。KEK、DEK 中間鍵、許可要素、サブマスク、及び乱数またはその他のあらゆる鍵生成または許可要素の作成に寄与する値の知識を有することは、不正な利用者が暗号を破ることができてしまうので、本 SPD は、鍵材料が重要なデータと同等であると考え、それらは以下で対処されるその他の資産の中にある。

ここで、本コラボラティブプロテクションプロファイルでは、悪意のあるコードまたは悪用できるハードウェアコンポーネントを評価対象 (TOE) または運用環境に持ち込むことができるような、紛失または盗難にあったハードディスクの所持者に対して保護することを評価対象 (TOE) に対して期待していないという、この点について再度強調することは重要である。利用者が物理的に TOE を保護し、運用環境が論理的攻撃に対して十分な保護を提供することが想定されている。適合 TOE が何らかの保護を提供するようなある特定の分野は、TOE へのアップデートの提供にある；この分野以外には、本 cPP はその他の対策を強制していない。同様に、本要件は、一度紛失した後に発見されたハードディスクの問題には対処しない、敵対者はハードディスクを取得し、ブートデバイスの暗号化されない部分 (例、MBR、ブートパーティション) を危殆化した上で、危殆化したコードを実行することを目的として、元の利用者に回収させる。

(T.UNAUTHORIZED_DATA_ACCESS) 本 cPP は、ストレージデバイス上に格納される保護データの不正な暴露の主たる脅威に対処する。相手が紛失または盗難にあったストレージデバイス(例、ラップトップに内蔵のストレージデバイスまたはポータブルな外部ストレージデバイス) を取得する場合、彼らは標的となったストレージデバイスを完全に制御下におくホストへ接続し、ストレージデバイスへの生(raw)アク

セス(例、特定のディスク上のセクタへ、特定のブロックへ)を得ようとするだろう。

[FMT_SMF.1, FPT_PWR_EXT.1, FPT_PWR_EXT.2, FCS_SNI_EXT.1, FCS_VAL_EXT.1, FDP_DSK_EXT.1, FPT_TST_EXT.1, FCS_COP.1(f)]

根拠：FDP_DSK_EXT.1は、TOEが、すべての保護データを含めて、ドライブ全体暗号化を実行することを保証する。附属書Fで定義された「ドライブ全体暗号化」は、MBR(訳注：マスターブートレコード)及びその他のAA/EE事前認証ソフトウェアを除き、「利用者がアクセス可能なデータの論理ブロックからなるパーティションであって、インデックスを作成したり、パーティション分割をしたりするファイルシステム、並びにこれらのパーティションの中のブロックのデータの読み出し及び書き込みのための許可を対応付けるようなオペレーティングシステムによって定義されるもの」を参照している。これは、たとえデバイスを紛失した場合でも、保護データが暴露されないことを保証する。

FPT_PWR_EXT.1 は、どのような電力状態が本 TOE に適合するかを定義する。FPT_PWR_EXT.2 は、どの条件で TOE が適合電力状態に入るかを定義する。これらの要件は、適合電力状態で紛失した場合、そのデバイスがセキュアであることを保証する。

FMT_SMF.1 は、TSF が DEK を変更及び消去する要求を含めて、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。すべての暗号機能の正しいふるまいは、自己テストの利用を通して検証される[FPT_TST_EXT.1]。FCS_VAL_EXT.1 は、正しい認証を検証し、かつデータを復号するため試行を制限する。FCS_SNI_EXT.1 は、適切なノンスと IV がデータの暗号化に使用されることを保証する。FCS_COP.1(f)は、適切な AES 暗号化を定義する。

(T.KEYING_MATERIAL_ COMPROMISE) 鍵、許可要素、サブマスク、及び乱数またはその他の鍵生成または許可要素の生成に寄与するような値のいずれかを知っていることは、許可されない利用者が暗号を破ることを可能にし得る。cPP は、鍵材料の知ることがデータそのものと同じ重要性を持つと考えている。脅威エージェントは、ストレージデバイスの暗号化されないセクタ内、及び運用環境内の他の周辺機器、例、BIOS 設定、SPI フラッシュ、または TPM における鍵材料を探すかもしれない。

[FCS_CKM.4(a),FCS_CKM.4(b),FCS_CKM_EXT.4(a),FCS_CKM_EXT.4(b), FCS_KYC_EXT.2,FMT_SMF.1,FCS_KYP_EXT.1,FPT_PWR_EXT.1, FPT_PWR_EXT.2,FCS_CKM.1(c),FCS_SNI_EXT.1,FCS_VAL_EXT.1, FPT_TST_EXT.1,FCS_CKM.1(a),FCS_CKM.1(b),FCS_COP.1(b),FCS_COP.1(c), FCS_COP.1(d),FCS_COP.1(e),FCS_COP.1(f),FCS_COP.1(g),FCS_KDF_EXT.1, FCS_RBG_EXT.1, FCS_SMC_EXT.1]

根拠：脅威エージェントがセキュリティ侵害を試行するかもしれないような鍵材料は、FCS_CKM.1(a)、(b)、及び FCS_CKM.1(c)により規定されるとおり生成され、これらのすべては FCS_RBG_EXT.1 経由で適切に生成される。 1 つ以上のサブマスクが、DEK を保護するために、コンバイニングされてもよい [FCS_SMC_EXT.1] し、 及び／またはチェインされてもよい [FCS_KYC_EXT.2]。鍵チェインは、以下を含む、いくつかの方法によって維持され得る：

- 鍵導出[FCS_KDF_EXT.1]
- 鍵ラッピング[FCS_COP.1(d)]
- 鍵コンバイニング[FCS_SMC_EXT.1]
- 鍵配送[FCS_COP.1(e)]
- 鍵暗号化[FCS_COP.1(g)]

これらの要件は、BEV が適切に保護されることを保証する。ソルト、ノンス、及び IV の適切な生成[FCS_SNI_EXT.1]は、それらの (対称鍵生成及びガロア／カウンターモード[GCM]を用いる AES 暗号化及び復号のような) 利用を要求している暗号機能をサポートするために実行される。これには、乱数ビット生成器の利用が含まれてもよい[FCS_RBG_EXT.1]。FCS_VAL_EXT.1 は、ハッシュ[FCS_COP.1(b)]。鍵付きハッシュメッセージ認証[FCS_COP.1(c)]、及び鍵材料を用いた既知の値の復号[FCS_COP.1(f)]のような BEV の検証方法を定義する。鍵データは、ハッシュ関数を利用して実施可能なサブマスクコンバイニング[FCS_SMC_EXT.1]を用いて保護することも可能である。すべての暗号機能の正しいふるまいは、自己テストの利用を通じて検証される[FPT_TST_EXT.1]。

FPT_KYP_EXT.1 は、ラッピング解除された鍵材料が不揮発性メモリに格納されないことを保証し、また FCS_CKM_EXT.4(a) が FCS_CKM.4(a)とともに、鍵材料を適切に破棄することを保証する；平文の鍵及び鍵材料の暴露を最小限にする。

セキュアな電力管理は、省電力状態が攻撃者によって平文の鍵材料をアクセスするために使用できないことを保証するために欠かせないものである。TSF は、適合省電力状態 [FPT_PWR_EXT.1] を定義し、様々な条件 [FPT_PWR_EXT.2]によって、その省電力状態に遷移するときにすべての鍵材料を暗号化または破棄[FCS_CKM.4(b), FCS_CKM_EXT.4(b)]する。この材料は、BEV が検証されるまで[FCS_VAL_EXT.1]、復号されない。

FMT_SMF.1 は、TSF が暗号学的データの改変及び消去を含めて、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。

(T.AUTHORIZATION_GUESSING) 脅威エージェントは、パスワードや PIN のような許可要素を繰り返し推測するため、ホストソフトウェアを動作させるかもしれない。許可要素の推測の成功は、TOE に DEK を出力させるかもしれない、さもなければ許可されない利用者へ保護データを開示するような状態に TOE を陥れるかもしれない。

[FCS_SNI_EXT.1, FCS_VAL_EXT.1]

根拠： [FCS_VAL_EXT.1] は、DEK の鍵サニタイズ、または設定可能な検証試行の失敗回数が 24 時間以内に規定回数に到達した場合のような、検証を実施するためのいくつかのオプションを要求する。これは、パスワードや PIN 等の許可要素に対する総当たり攻撃を防止する。[FCS_SNI_EXT.1]に従って、ソルトは、事前計算済み攻撃を防止するものとして利用されてもよい。

(T.KEYSPACE_EXHAUST) 脅威エージェントは、鍵空間に対する暗号技術的な総当たり攻撃を実行するかもしれない。暗号アルゴリズム及び／またはパラメタの不完全な選択は、鍵空間の総当たり攻撃やデータへの不正なアクセスを攻撃者に許してしまう。

[FCS_KYC_EXT.2, FCS_CKM.1(a), FCS_CKM.1(b), FCS_CKM.1(c), FCS_RBG_EXT.1]

根拠：[FCS_CKM.1(a), (b), 及び(c)]、及び [FCS_RBG_EXT.1] は、総当たり攻撃試行が暗号技術的に困難でコスト的に割に合わないようにするため、暗号鍵がランダムで適切な強度／長さであることを保証する。 [FCS_KYC_EXT.2] は、DEK を保護しているすべての鍵が同じ鍵強度であることを保証する。

(T.KNOWN_PLAINTEXT) 脅威エージェントは、特にオペレーティングシステムのような既知のソフトウェアが含まれる領域と同様に初期化(すべてゼロ)されない領域において、ストレージデバイスの領域における平文を知っている。暗号アルゴリズム、暗号モード、及び初期化ベクタの不完全な選択は、既知の平文とともに、攻撃者が有効な DEK を回復するのを許してしまうことがある、したがってストレージデバイス上の既知の平文への不正なアクセスを提供してしまう結果となる。

[FCS_COP.1(f)(オプション), FCS_SNI_EXT.1]

根拠：FCS_COP.1(f) は、暗号アルゴリズムとモードの適切な選択を保証する。FCS_SNI_EXT.1 は、ソルト、ノンス、及び初期化ベクタの適切な取り扱いを保証する。

(T.CHOSEN_PLAINTEXT) 脅威エージェントは、許可された利用者を騙して、画像、文書、またはその他のファイルの形式でストレージデバイス上に選択された平文を格納させようとするかもしれない。暗号アルゴリズム、暗号モード、及び初期化ベクタの不完全な選択は、選択された平文とともに、有効な DEK を攻撃者が回復するのを許してしまうことがある、したがってストレージデバイス上の既知の平文への不正なアクセスを提供してしまう結果となる。

[FCS_COP.1(f) (オプション), FCS_SNI_EXT.1]

根拠： FCS_COP.1(f) は、暗号アルゴリズムとモードの適切な選択を保証する。FCS_SNI_EXT.1 は、ソルト、ノンス、及び初期化ベクタの適切な取り扱いを保証する。

(T.UNAUTHORIZED_UPDATE) 脅威エージェントは、TOE のセキュリティ機能を侵害するような製品のアップデートを実行しようするかもしれない。アップデートプロトコル、署名生成アルゴリズム及び署名検証アルゴリズム、並びにパラメタの不完全な選択は、攻撃者が意図したセキュリティ機能を迂回し、データへの不正なアクセスを提供するようなソフトウェアをインストールできるようにするかもしれない。

[FCS_COP.1(a) (オプション), FMT_SMF.1, FPT_TUD_EXT.1]

根拠：FPT_TUD_EXT.1は、TOE ソフトウェアの現在のバージョンを問い合わせ、アップデートを開始し、そして製造事業者のディジタル署名を用いてインストールの前にアップデートを検証する能力を許可された利用者に提供する。

FMT_SMF.1 は、TSF がシステムソフトウェアアップデートの開始を含む TOE の重要なふるまい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。

(T.UNAUTHORIZED_FIRMWARE_UPDATE) ある攻撃者が、AA またはホストプラットフォームからのコマンド経由で、SED 上のファームウェアを TOE のセキュリティ機能を危殆化するかもしれないような悪意のあるファームウェアアップデートで置き換えようと試行する。

[FCS_COP.1(a) (オプション), FCS_COP.1(b) (オプション), FMT_SMF.1, FPT_FUA_EXT.1(オプション), FPT_TUD_EXT.1, FPT_FAC_EXT.1(オプション), FPT_RBP_EXT.1 (オプション)]

根拠：FPT_TUD_EXT.1 は、FMT_SMF.1 によって提供される管理機能によって開始された TOE ファームウェアをアップデートするためのセキュアなメカニズムを定義する。FCS_COP.1(a)及び FCS_COP.1(b)は、FPT_FUA_EXT.1 により定義されるとおり、ファームウェアアップデートの真正性と完全性を検証するために利用可能であるような暗号機能を定義する。FPT_FAC_EXT.1 は、信頼される管理者だけに知られているような情報をイニシエータが提供できる場合にのみ、アップデートを開始することを許可するような追加のセキュリティを提供する。FPT_RBP_EXT.1 は、より最近のバージョンでは存在しないような、セキュリティ欠陥を持っているかもしれない古いバージョンのファームウェアに、悪意をもって、またはうっかりしてダウングレードすることから保護する。

(T.UNAUTHORIZED_FIRMWARE_MODIFY) 攻撃者が、TOE のセキュリティ機能を危殆化するかもしれないような AA またはホストプラットフォームからのコマンド経由で、SED 上のファームウェアの改変を試行する。

[FPT_FUA_EXT.1 (オプション), FPT_TUD_EXT.1]

根拠：FPT_FUA_EXT.1 は、既存のファームウェアが FPT_TUD_EXT.1 の一部として開始された、有効なアップデートに置き換え得ることなしに改変され得ないことを保証する。

3.2 前提条件

脅威を低減するために忠実でなければならない前提条件を以下に示す：

(A.TRUSTED_CHANNEL) 製品コンポーネント (例、AA と EE) の間の通信は、情報暴露を防止するために十分に保護される。両方の cPP を満たす単独の製品の場合、コンポーネント間の通信は TOE の境界 (例、通信経路は TOE 境界内にある) を越えて拡がることはない。AA 及び EE の要件を満たす独立した複数の製品の場合、運用中の 2 つの製品が物理的に近接して配置されることによって、脅威エージェントが、利用者に気付かれることなく、または適切なアクションを取られることなく、2つの間のチャネルに割り込む機会はほとんどないことを意味している。

[OE.TRUSTED_CHANNEL]

(A. INITIAL_DRIVE_STATE) 利用者は、暗号化対象でない領域に保護データが存在しないような、新規に設定されたまたは初期化されたストレージデバイス上のドライブ全体暗号化を有効化する。設定が完了するまで、保護することを意図したデータが、対象となるストレージメディア上に存在すべきでないということも想定されている。cPP は、保護データが含まれる可能性のあるストレージデバイスのすべての領域を調べるための要件を含むことは意図していない。場合によっては、例えばデータが「不良」セクタに含まれていた場合、可能ではないかもしれない。不良セクタまたは非パーティション化空間に含まれるデータが不注意で暴露されることは起こりそうもないが、ある人はストレージデバイスのこのような領域からデータを回復するためのフォレンジックツールを使用するかもしれない。結果的に、cPP は、不良セクタ、非パーティション化空間、及び暗号化されないコードを含んでいるに違いない領域 (例、MBR 及び AA/EE 事前認証ソフトウェア) は何ら保護データを含まないと想定する。

[OE.INITIAL_DRIVE_STATE]

(A.TRAINED_USER) 利用者は、TOE 及び許可要素をセキュアにするために提供されたガイダンスに従う。これには、その目的専用の外部トークン許可要素を用いて、ストレージデバイス及び／またはプラットフォームから別個にセキュアに格納された外部トークンを保証するような、許可要素強度への適合を含む。利用者は、それらのシステムの電源をオフする方法についても訓練を受けるべきである。

[OE.PASSPHRASE_STRENGTH, OE. POWER_DOWN, OE.SINGLE_USE_ET, OE.TRAINED_USERS]

(A.PLATFORM_STATE) ストレージデバイスが依存する(または外部ストレージデバイスが接続された)プラットフォームは、製品の正しい運用を妨げるようなマルウェアに感染していない。

[OE.PLATFORM_STATE]

(A.POWER_DOWN) 利用者は、デバイスが適合省電力状態または完全に電源オフとなるまで、プラットフォーム及び／またはストレージデバイスから離れない。これは、メモリを適切に消去し、デバイスをロックダウンする。許可された利用者は、機微な情報が不揮発性ストレージに残存するようなモードの状態のまま、プラットフォーム及び／またはストレージデバイスから離れない (例、ロックスクリーンまたはスリープ状態)。 利用者は、プラットフォーム及び／またはストレージデバイスの電源を落とす、または電源管理された状態、例えば「ハイバーネーションモード」へ移行させる。

[OE.POWER_DOWN]

(A.STRONG_CRYPTO) 運用環境において実装され、製品により使用されるすべての暗号技術は、cPP に列挙された要件を満たす。これは、RBG による外部トークン許可要素の生成を含む。

[OE.STRONG_ENVIRONMENT_CRYPTO]

(A.PHYSICAL) プラットフォームが運用環境において物理的に保護されており、セキュリティを侵害したり、及び／またはプラットフォームの正常な動作を妨害したりするような物理的攻撃を受けないと仮定される。

[OE.PHYSICAL]

3.3 組織のセキュリティ方針

本 cPP による組織のセキュリティ方針はない。

4. セキュリティ対策方針

4.1 運用環境のセキュリティ対策方針

TOE の運用環境は、TOE がセキュリティ機能を正しく提供することを支援するための技術的及び手続的な対策を実装する。この部分の賢いソリューションは、運用環境のためのセキュリティ対策方針を作ることであり、運用環境が達成するべき目標を記述しているステートメントのセットからなる。

(OE.TRUSTED_CHANNEL) 製品のコンポーネントの間 (即ち、AA と EE) の通信は、情報の暴露を防ぐために十分保護されている。

> 根拠：敵対者が AA と EE の間のチャネルに割り込むような機会がある場合、悪用を防ぐために高信頼チャネルが確立されなければならない。[A.TRUSTED_CHANNEL] は、AA と EE の間で高信頼チャネルが存在することを想定しており、TOE の境界が製品の内部にあって TOE を侵害しないか、または検知なしに侵害できないように双方が近接している場合を除く。

(OE.INITIAL_DRIVE_STATE) OE(運用環境)は、新たに設定された、または初期化されたストレージデバイスで、暗号化の対象外の領域に保護データのないようなものを提供する。

> 根拠： cPP は、すべての保護データが暗号化されることを要求するので、 A.INITIAL_DRIVE_STATE は、FDE の対象となるデバイスの初期状態が、暗号化の実行されないドライブ領域(例、MBR や AA/EE 事前認証ソフトウェア)に保護データがないことを想定している。この既知の開始状態を前提として、製品(一度インストールされて運用中の)は利用者アクセス可能データの論理ブロックのパーティションが保護されていることを保証する。

(OE.PASSPHRASE_STRENGTH) 許可された管理者は、パスフレーズ許可要素が TOE を使用する企業からのガイダンスに適合していることを保証する責任を持つこと。

> 根拠：利用者は、管理者ガイダンスに適合する許可要素を生成するために、適切に訓練される[A.TRAINED_USER] 。

(OE.POWER_DOWN) 揮発性メモリは、適合省電力状態または電源オフ後に消去されるので、メモリ残存攻撃は不可能である。

> 根拠：利用者は、デバイスが適合省電力状態または完全に電源オフとなるまでストレージデバイスを放置したまま離れないように、適切に訓練される[A.TRAINED_USER] 。

(OE.SINGLE_USE_ET) 許可要素を含む外部トークンは、外部トークン許可要素を格納する以外の目的で使用されない。

根拠：利用者は、外部トークン許可要素を意図されたとおりに使用し、それ以外の目的で使用しないよう、適切に訓練される[A.TRAINED_USER]。

(OE.STRONG_ENVIRONMENT_CRYPTO) 運用環境は、要件及び TOE の能力、附属書 A と整合する暗号機能に関する能力を提供する。

根拠：運用環境に実装され、製品が使用するすべての暗号は、本 cPP に列挙された要件を満たす[A.STRONG_CRYPTO]。

(OE.TRAINED_USERS) 許可された利用者は、適切に訓練され、TOE 及び許可要素をセキュアにするためのすべてのガイダンスに従う。

根拠：利用者は、ガイダンスに適合する許可要素を作成し、外部トークン許可要素をそのデバイスに保存せず、要求された時に TOE を電源オフにする (OE.PLATFORM_STATE) ように、適切に訓練される[A.TRAINED_USER]。ストレージデバイスが存在する (または外部ストレージデバイスが接続される) プラットフォームは、製品の正しい動作を妨げることのあるマルウェアには感染しない。

マルウェアに感染していないプラットフォーム[A.PLATFORM_STATE] は、製品の正しい運用を潜在的に妨げる可能性のある攻撃ベクタを防止する。

(OE.PHYSICAL) 運用環境は、敵対者がその環境または TOE 自体に改変させることができないようにセキュアな物理計算空間を提供すること。

根拠：セクション 1.6 に記述したとおり、本 cPP の適用例は、敵対者が電源オフ状態のデバイスを受け取り、そのデバイスに事前にアクセスしたことがないような状況で、デバイス上の保存データを保護することである。

5. セキュリティ機能要件

個別のセキュリティ機能要件は、以下のセクションにおいて規定される。 これらの SFR でなされた選択に基づき、附属書 B の選択ベースの SFR のいくつかを含める必要がある。追加のオプション SFR についても、運用環境の代わりに TOE によって提供されるような機能について附属書 A に列挙されたものから適用することもできる。

[SD]で定義される評価アクティビティは、評価者がその SFR を持つ特定の TOE の適合性を決定するために取るようなアクションを記述する。これらの評価アクティビティの内容は、ゆえに TOE 開発者から要求される証拠資料へのより詳細な確認を提供する。

5.1 表記法

SFR の記述で使用される表記法は、以下の通りである：

- 割付：*イタリックテキストで示される*；
  - PP 作成者による詳細化：オリジナルの SFR への追加またはからの削除されたテキストについて、**太字**または~~取り消し線~~で示される；
  - 選択：<u>下線</u>で示される；
  - 選択内の割付：<u>*イタリックと下線*</u>で示される；
  - 繰り返し：SFR に、それぞれの繰り返しについて一意の文字を含むような括弧を追加することで示される、例、(a)、(b)、(c) 及び／またはスラッシュ(/) と後に続く SFR の目的についての記述文字列、例、/Server；

太字、イタリック、及び下線の SFR テキストは、オリジナル SFR が割付操作を定義したことを示すが、PP 作成者はオリジナル SFR の詳細化であると見なされるような、選択操作としてそれを詳細化することによってその割付を完成したことを示す。

選択または割付が ST 作成者によって完成されるべきである場合、「選択：」または「割付：」で開始される。選択または割付が PP 作成者によって完成され、ST 作成者はそれを改変する能力を持たない場合、適切なフォーマットの表記法が適用されるが、開始される用語は含まれない。これに対する例外は、SFR 定義が選択または割付に複数の選択肢を含み、PP が特定の選択肢を除外しているが、少なくとも 2 つは残っている場合である。この場合、本 PP によって許されないような選択または割付操作が追加のフォーマットを適用することなく削除され、「選択：」または「割付：」テキストは、ST 作成者がまだ選択肢の減らされたセットから選択できることを示すために残される。

拡張 SFR (即ち、CC パート 2 で定義されていないような SFR) は、SFR 名称の末尾に「_EXT」ラベルを持つことにより特定される。

5.2 SFR アーキテクチャ

以下の表は、本 cPP で必須の SFR を列挙する。

表 2：TOE セキュリティ機能要件

機能クラス	機能コンポーネント
暗号サポート (FCS)	FCS_CKM.1(c) 暗号鍵生成(データ暗号化鍵)
	FCS_CKM.4(a) 暗号鍵破棄 (電力管理)
	FCS_CKM_EXT.4(a) 暗号鍵及び鍵材料破棄 (破棄のタイミング)
	FCS_CKM_EXT.4(b) 暗号鍵及び鍵材料破棄 (電力管理)
	FCS_CKM_EXT.6 暗号鍵破棄種別
	FCS_KYC_EXT.2 鍵 チェイニング (受領者)
	FCS_SNI_EXT.1 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成)
	FCS_VAL_EXT.1 検証
利用者データ保護(FDP)	FDP_DSK_EXT.1 ディスク上のデータの保護
セキュリティ管理(FMT)	FMT_SMF.1 管理機能の特定
TSF の保護 (FPT)	FPT_KYP_EXT.1 鍵及び鍵材料の保護
	FPT_PWR_EXT.1 省電力状態
	FPT_PWR_EXT.2 省電力状態のタイミング
	FPT_TST_EXT.1 TSF テスト
	FPT_TUD_EXT.1 高信頼アップデート

5.3 クラス：暗号サポート (FCS)

FCS_CKM.1(c) 暗号鍵生成 (データ暗号化鍵)

FCS_CKM.1.1(c) **詳細化：** TSFは、 ~~以下に合致する、~~規定された鍵生成~~アルゴリズム~~**方法[選択：**

- **FCS_RBG_EXT.1で規定されるとおりRBGを用いてDEKを生成する、**
- **ホストプラットフォームにより提供されるRBGによって生成されたDEKを 受け入れる、**
- **FCS_COP.1(d)で規定されるとおりラッピングされたDEKを受け入れる]**

及び規定された鍵長[***選択：128 ビット、256 ビット***] に従って暗号鍵を生成しなければならない(shall) ~~：[割付：規格のリスト]~~。

適用上の注釈： *本 SFR は、追加の繰り返しが附属書 A のオプション要件として定義されるため、繰り返しされる。繰り返しの(c)は、２つの FDE cPP 間での一貫性を保証するため、特に選ばれた。*

本要件の目的は、プロビジョニング(プロビジョニング)中の DEK 生成を説明することである。

TOE が一つ以上の方法で DEK を取得するよう設定可能な場合、ST 作成者は、選択における適用可能なオプションを選択すること。例えば、環境からの DEK を受け入れるためのインタフェースを提供するのと同様に、TOE が DEK を生成するために承認された RBG を用いて乱数生成してもよい。

ST 作成者が、選択の中の最初及び／または三番目の選択肢を選んだ場合、関連する要件が附属書 A から引用され、ST の本文に含まれること。

FCS_CKM.4(a) 暗号鍵破棄(電力管理)

FCS_CKM.4.1(a) TSF は、以下に合致する、FPT_PWR_EXT.1 により定義されるとおりに適合省電力状態へ遷移しようとするとき、暗号鍵及び鍵材料を[***選択：運用環境に対してクリア(clear)するよう指示、運用環境に対して消去(erase)するよう指示***]しなければならない(shall)：[*FCS_CKM_EXT.6 で規定される暗号鍵破棄方法*]。

適用上の注釈： *いくつかの場合に、不揮発性メモリからの鍵の消去は、運用環境によってサポートされるのみである、この場合に運用環境は良く文書化されたメカニズムまたはメモリクリア操作を起動するインタフェースを開示しなければならない(shall)。*

自己暗号化ドライブは、運用環境の鍵を格納しないし、運用環境にその機能を実行するよう指示することができないので、それらは、「運用環境に対してクリアするよう指示」を選択すると予測されない。

FCS_CKM_EXT.4(a) 暗号鍵及び鍵材料破棄(破棄のタイミング)

FCS_CKM_EXT.4.1(a) TSF は、鍵及び鍵材料がもはや不要となったとき、それらすべてを破棄しなければならない(shall)。

適用上の注釈： *もはや不要となった中間鍵及び鍵材料を含め、鍵は、承認された方法、FCS_CKM_EXT.6 を用いて破棄される必要がある。鍵の例としては、中間鍵、サブマスク、及び BEV がある。永続的なストレージに格納されている鍵または鍵材料が、もはや不要となり破棄が必要な例があるかもしれない。それらの実装に基づいて、ベンダは、いつ特定の鍵が不要となるかについて説明すること。鍵材料が不要となる複数の状況がある、例えば、ラッピングされた鍵は、パスワード変更時に破棄される必要があるかもしれない。しかし、例えば、デバイス識別鍵のように、鍵がメモリ上に残存することが許容される場合がある。*

FCS_CKM_EXT.4(b) 暗号鍵及び鍵材料破棄(電力管理)

FCS_CKM_EXT.4.1(b) TSF は、FPT_PWR_EXT.1 により定義されるとおりの適合省電力状態へ遷移しようとするとき、平文で格納された、すべての鍵及び鍵材料、BEV、及び認証要素を破棄しなければならない(shall)。

適用上の注釈： *TOE は、適合電力状態から区別できない非適合の省電力状態で終了するかもしれない(例、突然及び／または想定外の電力喪失の結果として)。ガイダンス証拠資料は、揮発性メモリに平文の鍵または鍵材料が残るような結果をもたらすかもしれない条件について記述しなければならない(must)、また揮発性メモリのクリアをもたらすような軽減対策を特定しなければならない(must)。*

FCS_CKM_EXT.6 暗号鍵破棄の種別

FCS_CKM_EXT.6.1 TSF は、[***選択：FCS_CKM.4(b)、FCS_CKM.4(c)、FCS_CKM.4(d)***]の鍵破棄方法を利用しなければならない(shall)。

適用上の注釈： *複数の選択肢が選択される場合、TSS は、どの鍵がどの選択肢に従って、破棄されるかを特定しなければならない(shall)。*

FCS_KYC_EXT.2 鍵チェイニング(受領者)

FCS_KYC_EXT.2.1 TSF は、 少なくとも[選択：128 ビット、256 ビット]の BEV を[*AA*]から受け入れなければならない。

FCS_KYC_EXT.2.2 TSF は、以下の方法を用いて BEV から DEK へ向けて生成する中間鍵のチェインを維持しなければならない(shall)：[選択：

- FCS_CKM.1(a)で規定される非対称鍵生成、
- FCS_CKM.1(b)で規定される対称鍵生成、
- FCS_KDF_EXT.1 で規定される鍵導出、
- FCS_COP.1(d) で規定される鍵ラッピング、
- FCS_SMC_EXT.1 で規定される鍵コンバイニング、
- FCS_COP.1(e) で規定される鍵配送、
- FCS_COP.1(g) で規定される鍵暗号化]

ここで、対称鍵については[選択：128 ビット、256 ビット]の有効な強度及び非対称鍵については[選択：該当なし、112 ビット、128 ビット、192 ビット、256 ビット]の有効な強度を維持すること。

適用上の注釈： *鍵チェイニングは、ドライブ上の暗号化された保護データを最終的にセキュアにするために多階層暗号鍵を用いる方法である。中間鍵の数は、２つから(例えば、中間鍵として BEV を用いて DEK をラッピングする場合)数多くまでさまざまである。これが最終的なラッピング、または DEK の導出に寄与するすべての鍵に適用される；保護されたストレージの領域におけるそれら(例えば、TPM 保存の鍵、比較用の値)を含めて適用される。*

BEV は、鍵材料と等価であると見なされ、ゆえに追加のチェックサムまたは同様な値が BEV と共に送信されたとしても、それらは BEV ではない。

一度、ST 作成者が(鍵を導出するか、アンラッピングのいずれかによって)チェインを作成する方法を選択したなら、彼らは、附属書 B から適切な要件を取り込む。両方の方法を使用するような実装が許容されている。

鍵をチェインさせたり、それらを管理／保護するために TOE が使用する方法は、鍵管理記述に記述される；詳細は、附属書 E を参照のこと。

FCS_SNI_EXT.1 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成)

FCS_SNI_EXT.1.1 TSF は、[選択：ソルトを利用しない、[選択： FCS_RBG_EXT.1 で規定される DRBG、 ホストプラットフォームによって提供される DRBG]によって生成されるソルトの利用する]ようにしなければならない(shall)。

FCS_SNI_EXT.1.2 TSF は、[選択：ノンスを利用しない、最小 [*64*]ビット長の一意のノンスを利用する]ようにしなければならない(shall)。

FCS_SNI_EXT.1.3 TSF は、以下のやり方で IV(初期化ベクタ) を生成しなければならない (shall)：[選択：

- CBC: IV は、繰り返し無し、かつ予測不可能でなければならない(shall)；
- CCM: ノンスは、繰り返し無し、かつ予測不可能でなければならない(shall)；
- XTS: IV 無し。 Tweak 値は、非負の整数であり、連続に割り当てられ、かつ任意の非負の整数から始まらなければならない(shall)；
- GCM: IV は、繰り返し無し。所与の秘密鍵について GCM の呼び出し回数は 2^32 回を超えてはならない(shall not)]。

適用上の注釈： *本 SFR は、ソルト、ノンス、及び IV がいつ使用されなければならないかについては規定しない、ただ、それらが使用されるときにそれらが生成されなければないやり方について規定する。ST 作成者は、ソルト、ノンス、及び／または IV の利用を要求するようなそれぞれの主張された SFR (FCS_CKM.1(b) により定義された対称鍵生成、及び FCS_COP.1(f)により定義された AES 暗号化／復号等) について記述することが期待されている。TSF がソルト、ノンス、または IV を何らの機能にも利用しない場合、本 SFR は、満たされたと見なされて不要となる。*

本要件は、いくつかの重要な要素ーソルトはランダムでなければならないが、ノンスは単に一意でなければならない。FCS_SNI_EXT.1.3 は、各暗号モードでIV がどのように取り扱われるべきかを規定する。連続的な割付は 1 ずつ繰り上がるカウンタの利用を意味する。さらに、ノンスは、ISO/IEC 19772 では Starting Variable (SV) と呼ばれている。

Tweak 値は、任意の非負の数から始まる非負の数でなければならず、かつ、すべての後続の tweak 値は、初期値からインクリメント (1 つずつ単純増加) されなければならない。

FCS_VAL_EXT.1 検証

FCS_VAL_EXT.1.1 TSF は、以下の方法を用いて［BEV]の検証を実行しなければならない (shall)：［選択：

- FCS_COP.1(d) で規定された鍵ラッピングする、
- [選択： FCS_COP.1(b), FCS_COP.1(c)] で規定される［BEV]をハッシュし、保存されているハッシュされた［**値**］と比較する、
- FCS_COP.1(f)で規定される［選択：中間鍵, BEV］を用いて既知の値を復号し、保存された既知の値と比較する]。

FCS_VAL_EXT.1.2 TSF は、[BEV] の検証を [*適合省電力状態でなくなった後、TSF データへのアクセスを許容する*]の前に要求しなければならない(shall)。

FCS_VAL_EXT.1.3 TSF は、[選択：

- 設定可能な連続する検証試行失敗回数に達したときに[*DEK の鍵サニタイズを実行する*]、
- 24 時間以内に [*割付: ST 作成者が規定した試行回数*] までしか実行できないように遅延を設定する、
- 連続する検証試行失敗回数が[*割付: ST 作成者が規定した試行回数*]に達した後に検証をブロックする、

- 連続する検証試行失敗回数が[*割付：ST 作成者が規定した試行回数*] に達した後に TOE の再起動／リセットを要求する]

ようにしなければならない(shall)。

適用上の注釈：*DEK が復号されるときを含め、BEV の「検証」は鍵チェインにおけるいずれのポイントでも発生しうる。本要件の目的として、BEV から導出される鍵の検証は、BEV の「検証」と同一である。セキュアな検証を実行する目的は、サブマスクを侵害するかもしれないあらゆる材料を暴露しないようにするためである。*

TOE は、ドライブ上に格納されたデータへのアクセスを利用者に許可する前に、BEV を検証する。FCS_COP.1(d)の鍵ラッピングが使用される時、検証が本質的に実行される。

遅延が TOE によって実施されなければならない(must)が、本要件は製品を迂回するような攻撃(例、攻撃者がハッシュ値または「既知の」暗号値を入手し、第三者パスワードクラッカーのような、TOE 外部から攻撃を組み込む)に対処することを意図していない。実行される暗号機能(即ち、ハッシュ、復号)は、FCS_COP.1(b)及びFCS_COP.1(f)で規定されたものである。

5.4 クラス：利用者データ保護 (FDP)

本ファミリは、ドライブに書き込まれるすべての保護データの暗号化を義務付けるために使用される。

FDP_DSK_EXT.1 ディスク上のデータの保護

FDP_DSK_EXT.1.1 TSF は、ドライブに平文の保護データが一切含まれないように、FCS_COP.1(f)に従ってドライブ全体暗号化を実行しなければならない(shall)。

FDP_DSK_EXT.1.2 TSF は、利用者の介在なしにすべての保護データを暗号化しなければならない(shall)。

適用上の注釈： *本要件の意図は、あらゆる保護データの暗号化がそのデータを保護するために利用者の選択に依存しないよう特定することである。FDP_DSK_EXT.1 で規定されるドライブ暗号化は、利用者に対して透過的に発生し、データを保護するための決定は利用者の裁量の範囲外であり、それがファイル暗号化とそれを区別する特徴である。保護データの定義は、用語集で見つけることができる。*

データの暗号化／復号を実行する暗号機能は、環境によって提供されてもよい。この場合、FCS_COP.1(f)で記述されるふるまいと環境が提供する AES の実装とが一貫していることが想定されていることに注意されたい。データを暗号化／復号する暗号機能を TOE が提供する場合、ST 作成者は附属書 A から FCS_COP.1(f)を引用し、ST の本文にそれを含めること。

5.5 クラス：セキュリティ管理 (FMT)

FMT_SMF.1 管理機能の特定

FMT_SMF.1.1 詳細化：TSF は、以下の管理機能を実行可能でなければならない(shall)： [

a) 再プロビジョニング時またはコマンドを受けた時、FCS_CKM.1 で規定されたとおり、DEK を変更する、
b) FCS_CKM.4(a) で規定されるとおり、DEK を消去する、
c) TOE ファームウェア／ソフトウェアのアップデートを開始する、
*d) [**選択：その他の機能なし、ファームウェアアップデート用のパスワードを設定する、ラッピングされた DEK をインポートする、暗号機能を設定する、鍵回復機能を無効化する、高信頼アップデートで必要とされる公開鍵をセキュアにアップデートする、是正のふるまいを起動するために要求される検証試行失敗回数を設定する、検証試行失敗回数の超過事象に生じる是正のふるまいを設定する、[割付：TSF によって提供されるその他の管理機能]***]。

適用上の注釈： *本要件の意図は、TOE が持っている管理機能を表現することである。これは、TOE がリストアップされた機能を実行できなければならないことを意味する。項目(d)は、TOE に含まれてもよい機能を特定するために使用されるが、cPP へ適合するために必須のものではない。「暗号機能を設定する」は、鍵管理機能を含む可能性がある、例えば、BEV はラッピングされるか、または暗号化され、EE は BEV をラッピング解除または復号する必要がある。項目(d)でその他の管理機能が一切提供されない(または主張されない)場合、「その他の機能なし」が選択されるべきである。デフォルト許可要素は、ドライブを操作するために使用される初期値である。*

本書の目的のため、鍵のサニタイズは、承認された破棄方法の一つを用いて、DEK を破棄することを意味する。これは、不揮発性ストレージに存在するような保護された鍵のインスタンスに適用される。

5.6 クラス：TSF の保護(FPT)

FPT_KYP_EXT.1 鍵及び鍵材料の保護

FPT_KYP_EXT.1.1 TSF は、鍵が以下の基準の任意の 1 つを満たさない限り、[選択：不揮鍵メモリ内に鍵を格納しない、FCS_COP.1(d)で規定されるとおりラッピングされるまたは FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化されるときのみ不揮発性メモリ内に鍵を格納する]ようにしなければならない(shall)： [選択：

- 平文の鍵は、[FCS_KYC_EXT.2]で規定されるとおり鍵チェインの一部ではない。
- 平文の鍵は、初期プロビジョニングの後、暗号化されたデータへのアクセスをもはや提供しない。
- 平文の鍵は、FCS_SMC_EXT.1 で規定されるとおりコンバイニングされるような鍵分散であり、鍵分散の他の半分は[選択：FCS_COP.1(d)で規定されるとおりラッピングされる、FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化される、導出されて不揮発性メモリに格納されない]。
- 平文の鍵は、許可要素として利用するための外部ストレージデバイス上に格納される。
- 平文の鍵は、[選択：FCS_COP.1(d)で規定されるとおり鍵をラッピングするために利用される、FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化される]、ここで、それ(鍵)はすでに [選択：FCS_COP.1(d)で規定されるとおりラッピングされている、FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化されている]。

適用上の注釈： *不揮発性メモリでの平文の鍵の格納は、いくつかの理由で許容される。TOE または OE 上で利用者がアクセスできない保護メモリ内に鍵が存在する場合、BEV また*

は DEK を保護するというセキュリティに重要な役割を担うことを許容する唯一の方法は、それが鍵分散であるか、既に保護されている鍵をさらにラッピングまたは暗号化の層を追加で提供する場合である。

不揮発性メモリに保存されるとき(保護されたストレージにおいても)、DEK は、データを暗号化または復号するために使用されるときには、常に暗号化され (ラッピングされ)、揮発性メモリにおいてのみ平文形式で存在する。プロビジョニング鍵は、ドライブの所有者によるプロビジョニングの前に不揮発性メモリにおいて平文形式で存在してもよい。

TOE が不揮発性メモリに鍵を格納しない場合、不揮発性メモリには鍵を決して格納しないという TSS でのステートメントが要求されるすべてであり、いかなる評価アクティビティも実行される必要はない。

本要件は、利用者データの暗号化に関連する鍵 － 特に鍵チェイン内からの鍵 に対処している。

FPT_PWR_EXT.1 省電力状態

FPT_PWR_EXT.1.1 TSF は、以下の適合省電力状態を定義しなければならない(shall)：[選択：以下から少なくとも 1 つ選択：S3、S4、G2(S5) 、G3、D0、D1、D2、D3 [*割付：その他の省電力状態*]]。

適用上の注釈：*省電力状態 S3、S4、G2(S5) 、G3、D0、D1、D2、D3 は、アドバンスト・コンフィギュレーション・アンド・パワー・インタフェース(ACPI)規格によって定義される。*

FPT_PWR_EXT.2 省電力状態のタイミング

FPT_PWR_EXT.2.1 FPT_PWR_EXT.1.1 で定義された各省電力状態について、TSF は、以下の条件が発生したときに適合省電力状態へ入らなければならない(shall)：利用者起動の要求、[選択：以下から少なくとも 1 つ選択：システムシャットダウン、利用者の非活動状態、リモート管理システムにより起動された要求、[*割付：その他の条件*]、その他の条件なし]。

適用上の注釈：*予期されない電源シャットダウンシーケンスの一部として揮発性メモリがクリアされない場合、ガイダンス証拠資料は、軽減アクティビティを定義しなければならない (must) (例、予期されない電源切断後、揮発性メモリがクリアされたと見なすことができるまで、利用者がどのくらいの時間を待つべきか)。*

FPT_TST_EXT.1 TSF テスト

FPT_TST_EXT.1.1 TSF は、TSF の正常動作を実証するため、[選択：初期立ち上げ中 (電源投入時)、条件[*機能が最初に呼び出される前*]において]、以下の自己テストのスイートを実行しなければならない(shall)：[*割付：TSF によって実行される自己テストのリスト*]。

適用上の注釈： *TOE に実装された暗号機能に関するテストは、機能が呼び出される前にテストが実行される限り、延期することができる。*

FCS_RBG_EXT.1がTOEによって実装され、NIST SP800-90に従っている場合、評価者は、NIST SP 800-90のセクション11.3と一貫するようなヘルステストについてTSSに記述されていることを検証しなければならない(shall)。

FCS_COP機能のいずれかがTOEによって実装されている場合、TSSにはそれらの機能の既知解自己テストについて記述されなければならない(shall)。

評価者は、TSFの正しい動作に影響を与える非暗号機能について、それらの機能がテストされる方法を、TSSが記述していることを検証しなければならない(shall)。

TSSは、それらの各機能について機能・構成要素の正しい動作の検証方法について記述すること。評価者は、識別された機能／構成要素のすべて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。

FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1.1 詳細化：TSF は、TOE [**選択：ソフトウェア、ファームウェア**]の現在のバージョンを問い合わせる能力を[*許可された利用者*] に提供しなければならない(shall)。

FPT_TUD_EXT.1.2 詳細化：TSF は、TOE [**選択：ソフトウェア、ファームウェア**] のアップデートを開始する能力を[*許可された利用者*] に提供しなければならない(shall)。

FPT_TUD_EXT.1.3 詳細化：TSF は、TOE[**選択：ソフトウェア、ファームウェア**]へのアップデートを製造者による[選択：**FCS_COP.1(a)で規定されるとおりの**ディジタル署名、**FPT_FUA_EXT.1 で記述されるような署名検証されたファームウェアアップデートメカニズム**]を用いて、それらのアップデートをインストール前に検証しなければならない(shall)。

適用上の注釈：*「許可された利用者」は、デバイスの正当で物理的な所持者である個人を指している。*

3 番目のエレメントで参照されるディジタル署名メカニズムは、附属書A のFCS_COP.1(a) で規定されたものである。本コンポーネントは TOE に対してアップデート機能自身を実装することを要求しているが、運用環境において利用可能な機能を用いて暗号学的なチェックを実行することは受け入れ可能である。

TOE がソフトウェア製品である場合、ST 作成者は「ディジタル署名」を選択する。TOE がハードウェア製品である場合、ST 作成者は「FPT_FUA_EXT.1 で記述されるとおりの署名検証されたファームウェアアップデートメカニズム」を選択する。

新しいアップデートパッケージの真正性と完全性を検証するため、及びセキュアアップデート処理の外からの改変から保護されることを保証するため、セキュアファームウェアアップデートメカニズムが利用される。署名検証されたファームウェアアップデートメカニズムは、RTU 及びファームウェアを保護しているものと少なくとも同じ強度であるようなメカニズムによる意図しないまたは悪意のある改変から保護されなければならない(shall)。

本要件の意図は、署名検証されたファームウェアアップデートメカニズムが提供されることを保証することである。署名検証は、ファームウェアパッケージが真正な情報源により生成されたこと、及び変更されていないことを検証する。既存のファームウェアへのすべてのアップデートは、FPT_FUA_EXT.1 に記述されるとおり、署名検証されたアップデートメカニズムを通して行われなければならない(shall)。

6. セキュリティ保証要件

本 cPP は、評価者が評価に提供可能な文書を評定し、独立テストを実施するための拡張を構成するセキュリティ保証要件(SAR)を特定する。

ST 作成者への注釈：ASE_TSS には、完成されなければならない選択がある。本 cPP における SAR を単に参照することはできない。

本セクションは、本 cPP に対する評価において要求される CC パート 3 からの SAR のセットを列挙する。実施されるべき個別の評価アクティビティはサポート文書*(必須技術文書) ドライブ全体暗号化：暗号エンジン　2016 年 9 月)* にて特定されている。

本 cPP に適合するために書かれた ST に対する TOE の評価の一般モデルは、以下のとおりである：ST が評価用として承認された後、評価機関は TOE、サポートする IT 環境(必要があれば)、及び TOE の管理者／利用者ガイドを取得する。評価機関は ASE 及び ALC の SAR について共通評価方法 (CEM) によって必須とされているアクションを実行することが期待されている。評価機関は、また TOE において例示された特定の技術へ適用するものとしてその他の CEM 保証要件の解釈とすることを意図されている、SD に含まれる評価アクティビティを実行する。SD において取り込まれた評価アクティビティは、TOE が cPP に適合していることを実証するために開発者が提供する必要のあるものとして、明確化もまた提供している。

表 3：セキュリティ保証要件

保証クラス	保証コンポーネント
セキュリティターゲット評価 (ASE)	適合主張 (ASE_CCL.1)
	拡張機能要件定義 (ASE_ECD.1)
	ST 概説 (ASE_INT.1)
	運用環境のセキュリティ対策方針(ASE_OBJ.1)
	主張されたセキュリティ要件 (ASE_REQ.1)
	セキュリティ課題定義(ASE_SPD.1)
	TOE 要約仕様(ASE_TSS.1)
開発 (ADV)	基本機能仕様 (ADV_FSP.1)
ガイダンス文書(AGD)	利用者操作ガイダンス(AGD_OPE.1)
	準備手続き (AGD_PRE.1)
ライフサイクルサポート (ALC)	TOE のラベル付け (ALC_CMC.1)
	TOE の CM 範囲 (ALC_CMS.1)
テスト (ATE)	独立テスト – ~~サンプル~~適合 (ATE_IND.1)
脆弱性評定 (AVA)	脆弱性調査 (AVA_VAN.1)

6.1　ASE: セキュリティターゲット評価

ST は、CEM で定義された ASE アクティビティ毎に評価される。さらに、TOE 技術種別に特有の TSS に含まれる必須の記述について記述された SD 内に特定される評価アクティビティがあるかもしれない。

本 cPP における SFR は、基本原則を満たしている限り、適合する実装として幅広く受け入れ可能な鍵管理のアプローチを含めることを許容している。鍵管理スキームの重要性を考慮し、本 cPP は、開発者が鍵管理の実装についての詳細記述を提供することを要求している。本情報は、ST への専有権対象と表示された附属書として提出可能なものであり、このレベルの

詳細な情報は公開されることは想定されていない。開発者の鍵管理記述についての想定される詳細は、附属書 E を参照されたい。

さらに TOE が乱数ビット生成器を含む場合、附属書 D は、エントロピーの品質に関して提供されると期待されている情報についての記述を提供している。

ASE_TSS.1.1C 詳細化： TOE 要約仕様は、**保護対象の情報である鍵管理記述 (附属書 E)、及び [選択：エントロピー解説、サードパーティのソフトウェアライブラリのすべてのリスト(バージョン番号を含めて)、サードパーティのハードウェア部品(モデル／バージョン番号を含めて)、その他の cPP が規定する保護対象の証拠資料なし]**を含めて、TOE が各 SFR をどのように満たすかを記述しなければならない。

6.2 ADV: 開発

TOE についての開発情報は、ST の TSS 部分や非公開の本 cPP に要求される追加情報(例、エントロピー解説) と同様に、最終利用者が利用可能なガイダンス文書にも含まれている。

6.2.1 基本機能仕様 (ADV_FSP.1)

機能仕様は、TOE セキュリティ機能インタフェース(TSFI)を記述する。これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 cPP に適合する TOE は必然的に TOE 利用者によって直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、このようなインタフェースは間接的なテストしかできないことから、そのようなインタフェース自体の記述を特定することはあまり意味がない。本 cPP では、本ファミリの評価アクティビティは、TSS に存在する機能要件に対応したインタフェース及び AGD に存在するインタフェースを理解することにフォーカスしている。SD において特定された評価アクティビティを満たすために、追加の「機能仕様」文書は、必要とされない。

SD の評価アクティビティは、該当する SFR と関連付けられている；これらは SFR に直接関連しているため、ADV_FSP.1.2D エレメントにおけるトレースは、すでに暗黙的になされており、追加の文書は必要とされない。

6.3 AGD: ガイダンス文書

ガイダンス文書は、ST と共に提供される。ガイダンスには、運用環境がセキュリティ機能に対する役割を果たすことができることを IT 要員が検証する方法の記述が含まれなければならない。この文書は、非形式的なスタイル (口語体) で IT 要員が読みやすい形であるべきである。

ガイダンスは、ST で主張されたとおり製品がサポートしているあらゆる運用環境に関して提供されなければならない。ハードウェア製品に関して、開発者は製品を配付するためにインテグレータが使用を選択するプラットフォームのすべてを知っていないかもしれない。インテグレータが TOE を適切に設定する(即ち、ST の SFR を満たす) ために発行する必要があるコマンドの記述は「製品がサポートするすべての運用環境」の意図を満たすだろう。本ガイダンスには、以下が含まれる：

- その環境において TSF を正常にインストールするための指示；及び

- 製品として、またより大規模な運用環境のコンポーネントとして TSF のセキュリティを管理するための指示；及び
- 保護された管理者機能を提供するための指示。

特定のセキュリティ機能に関するガイダンスも提供されなければならない；このようなガイダンスの要件は SD において特定される評価アクティビティに含まれている。

6.3.1 利用者操作ガイダンス (AGD_OPE.1)

利用者操作ガイダンスは、必ずしも単一の文書に含まれている必要はない。利用者、管理者、アプリケーション開発者及びインテグレータ向けのガイダンスが文書またはウェブページに分散されていてもよい。

開発者は、評価者がチェックするだろうガイダンスの部分を確認するために、SD に含まれる評価アクティビティをレビューするべきである。これによって、受け入れ可能なガイダンスの作成に必要な情報が提供されることになる。

6.3.2 準備手続き (AGD_PRE.1)

操作ガイダンスと同様に、開発者は、準備手続きについて必要とされる内容を決定するために評価アクティビティを確認するべきである。

6.4 クラス ALC: ライフサイクルサポート

本 cPP に適合する TOE に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの検査よりもむしろ、ライフサイクルの最終利用者から見えるような側面に限定されている。これは、製品の全般的な信頼性の向上に開発者の実践が果たす重要な役割を軽減することを意味していない；むしろ、本保証レベルでの評価で利用可能な情報を反映したものである。

6.4.1 TOE のラベル付け (ALC_CMC.1)

本コンポーネントは、TOE を同一ベンダから他の製品またはバージョンから区別でき、また最終利用者によって調達される際に容易に指定できるように、TOE を識別することを目標としている。ラベルには、「ハードラベル」(例、金属への刻印、紙ラベル等)または「ソフトラベル」(例、問い合わせ時に電子的に提示されるもの等)からなる。評価者は、ALC_CMC.1 に関連する CEM ワークユニットを実行する。

6.4.2 TOE の CM 範囲 (ALC_CMS.1)

TOE の適用範囲及び関連する評価証拠の要件を考慮して、評価者は ALC_CMS.1 に関連する CEM ワークユニットを実行する。

6.5 クラス ATE: テスト

テストは、システムの機能的な観点、及び設計または実装の弱点の利用するような観点について特定される。前者は、ATE_IND ファミリよって行われるが、後者は AVA_VAN ファミリによって行われる。本 cPP では、テストは公表された機能及びインタフェースに基づき、

設計情報の利用可能性に依存して行われる。評価プロセスの主要なアウトプットの一つは、以下の要件で特定されるテスト報告書である。

6.5.1 独立テスト – 適合 (ATE_IND.1)

テストは、TSS と操作ガイダンス(「評価された構成」指示を含む)に記述された機能を確認するために実施される。テストで重視されるのは、セクション 5 で規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。SD における評価アクティビティは、SFR への適合を検証するために必要な具体的なテストアクティビティを識別している。評価者は、本 cPP への適合を主張するプラットフォーム／TOE の組合せに焦点を絞ったカバレージ論拠とともに、テストの計画と結果を文書化したテスト報告書を作成する。

6.6 クラス AVA: 脆弱性評定

本 cPP の現在の世代として、iTC は、このタイプの製品においてどのような脆弱性が発見されているかを見つけるために公開情報源を調査することが期待され、その内容を AVA_VAN の議論へ提供することが期待される。 ほとんどの場合、これらの脆弱性には、基本的な攻撃能力を持つ攻撃者を超える高度な知識が要求される。本情報は、将来のプロテクションプロファイルの開発において活用されるだろう。

6.6.1 脆弱性調査 (AVA_VAN.1)

別文書であるサポート文書の附属書 A では、脆弱性分析を実施するための評価者へのガイドが提供されている。

附属書 A: オプション要件

本 cPP への序説で示すとおり、ベースライン要件(TOE によって実施されなければならないもの)は、本 cPP の本文に含まれている。さらに、附属書 A と B で特定される、他の 2 つのタイプの要件がある。

最初のセット (本附属書) は、ST に含めることが可能な要件であるが、TOE が本 cPP への適合を主張するために必ずしもなくてはならないものではない。2 番目のセット (附属書 B) は、cPP の本文の選択に基づく要件である：もし特定の選択が為されるならば、その附属書にある追加の要件が ST の本文に含まれる必要がある (例、高信頼チャネル要件で選択された暗号プロトコル等)。

A.1 内部の暗号実装

本 cPP の本文に示されるとおり、TOE がドライブ暗号化／復号処理をサポートする暗号機能を直接実装するか、または運用環境の暗号機能を使用するか (例えば、OS の暗号提供インタフェース；サードパーティの暗号ライブラリ；またはハードウェア暗号アクセラレータを呼び出す) のいずれかが許容される。しかし、運用環境によってオプションとして実装可能であるような、これらの SFR のそれぞれのひとつは、「選択ベース」の SFR であるとも見なされる。これは、それらの機能はその他の SFR について ST 作成者が何らかの選択をすることに付随するためである。このため、これらの SFR は附属書 B に配置された。運用環境がこれらの機能のセキュアな用途を可能とするような暗号インタフェースを TSF に含み、その機能が[SD]に記述されたとおりの同じレベルの厳格さで検証された証拠を ST 作成者が提供可能な限り、求められる SFR を省くことが受け入れ可能である場合において、これらの機能いくつかは運用環境によって提供されるかもしれないという期待がまだある。

暗号機能のすべてが TSF によって実装され、かつ TOE があらゆる暗号サービスを提供することをその運用環境に頼らない場合、運用環境がこの場合に対策方針を満たすために必要ではないため、OE.STRONG_ENVIRONMENT_CRYPTO 及びその関連する前提条件を ST 作成者は省略しなければならない(shall)。

A.2 ファームウェアアップデート検証

TOE がソフトウェアまたはハードウェア製品のいずれかである。ST 作成者は、FPT_TUD_EXT.1 の完成を通じてこれを選択する。TOE がハードウェア製品(即ち、SED)である場合、本 cPP は、ファームウェアアップデートの真正性と完全性の保証を提供することを意図するようないくつかの選択ベース要件を定義する。しかし、これらのメカニズムの他に、いくつかの追加のセキュリティ対策が適合する TOE によって提供されてもよい。TSF がこれらのセキュリティ対策を提供する場合、ST 作成者は、以下に記述された 1 つ以上の SFR をオプションで含めてもよい。

FPT_FAC_EXT.1 ファームウェアアクセス制御

FPT_FAC_EXT.1.1 TSF は、ファームウェアアップデートが開始される前に、[選択：パスワード、デバイス上に印刷された既知の一意な値、特権利用者アクション]を要求しなければならない(shall)。

適用上の注釈：アップデートが実行される前に、ドライブ所有者は、ドライブ上に印刷されたような既知の一意な値(例えば、シリアル番号)、パスワード(FMT_SMF.1で定義されるとおりに管理上設定可能であるべきもの)、または特権利用者としての操作を実行する、のいずれかを提供することによりアップデートを許可すること。ドライブに対する物理的提示は許可された要員に限定されると想定される。正しい値が提供されない場合、アップデートは実行されない。その値は、容易に総当たり攻撃されないように、ドライブ毎に一意であるよう意図される。

パスワードを消去するための同様の要件は、同様に適用される。

FPT_RBP_EXT.1 ロールバック保護

FPT_RBP_EXT.1.1 TSF は、新しいファームウェアパッケージが[*割付：セキュリティバージョン番号が現在インストールされているバージョンと同じか、より高いものであることを検証する方法*]により、より低いセキュリティバージョン番号へダウングレードしていないことを検証しなければならない(shall)。

FPT_RBP_EXT.1.2 TSF は、試行されたファームウェアアップデートパッケージが無効なバージョンとして検出される場合、エラーコードを生成し、応答しなければならない(shall)。

適用上の注釈： *本要件は、より以前の真正なバージョンへのファームウェアの許可されないロールバックを防止する。これは、セキュリティ上の弱点を持つかもしれないような以前の真正なファームウェアバージョンを気付かずにインストールすることを軽減する。ベンダは、それぞれの新しいアップデートパッケージのセキュリティバージョン番号を増加させることが想定されている。*

FPT_RBP_EXT.1.1 について、目的は、現在インストールされているファームウェアパッケージのセキュリティバージョン番号と等しいか、より大きいようなセキュリティバージョン番号を新しいパッケージが持っていることを検証することである。

管理者ガイダンスには、可能であれば、ロールバック防止メカニズムを管理者が設定するための指示が含まれるであろう。

A.3 暗号鍵破棄

TOE は、オプションとして、鍵破棄要件を通して、親の鍵を破棄することによって鍵を破棄することを選択することができる。破棄方法は、完全消去として通常呼ばれるデータ破棄方法を反映する。ST 作成者は、伝統的な鍵破棄要件を依然として行わなければならないか、これは、鍵破棄方法を拡張するような追加のオプションである。

FCS_CKM.4(e) 暗号鍵破棄 (鍵の暗号学的消去)

FCS_CKM.4.1(e) TSF は、以下に合致する、規定された暗号学的鍵破棄方法[*破棄されるはずの鍵を暗号化しているすべての暗号鍵を破棄するための適切な方法を用いることによる*]に従って、暗号鍵を破棄しなければならない(shall)：[*規格なし*]。

適用上の注釈：*鍵は、その鍵を保護するような鍵を破棄することによって破棄されると見なされることが可能である。鍵がラッピングまたは暗号化される場合、必ずしもその鍵(訳注：データを暗号化／復号する鍵)を「上書き」する必要はない。そのメモリタイプ用の適*

切な方法を用いて、データを暗号化／復号するために使用される鍵をラッピングまたは暗号化するために使用される鍵があって、その鍵を上書きすることで、十分である。例えば、ある製品がデータ暗号化鍵(DEK)を暗号化するために鍵暗号化鍵(KEK)を使用する場合、FCS_CKM_EXT.6.1 の方法のうちの 1 つを用いて KEK を破棄することで十分である、なぜなら DEK は、もはや利用可能でないであろうから(もちろん、DEK がまだ暗号化されていることを想定している)。

附属書 B: 選択ベース要件

本 cPP の概説で示されるとおり、ベースライン要件(TOE または下位のプラットフォームにより実行されなければならないもの)が本 cPP の本文に含まれている。cPP の本文における選択に基づいた追加の要件がある：特定の選択が為された場合、以下の追加の要件が含まれる必要があるかもしれない。

これらの選択ベースの SFR の多くは、TOE の運用環境における暗号サービスによって実装されることも可能である。この場合、同等な機能を運用環境が提供可能だと示されるならば、求められる SFR を含む必要はない。

B.1 クラス: 暗号サポート (FCS)

FCS_CKM.1(a) 暗号鍵生成 (非対称鍵)

FCS_CKM.1.1(a) 詳細化：TSF は、~~以下を満たす、~~規定された暗号鍵生成アルゴリズム：[***選択：***

- ***RSA 方式のうち、[選択：2048 ビット、3072 ビット、4096 ビット]の暗号鍵長を使用するもので、以下を満たすもの： FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;***
- ***ECC 方式のうち、[選択：P-256、P-384 、P-521]の「NIST 曲線」を使用するもので、以下を満たすもの： FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;***
- ***FFC 方式のうち、[選択：2048 ビット、3072 ビット、4096 ビット]の暗号鍵長を使用するもので、以下を満たすもの：FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1***

] ~~及び規定された~~暗号鍵長[*~~割付：暗号鍵長~~*] に従って、**非対称**暗号鍵を生成しなければならない(shall) ~~：[*割付：規格のリスト*]~~。

適用上の注釈： *非対称鍵は、鍵またはサブマスクを「ラッピング」するために使用されてもよい。本 SFR は、FCS_COP にて適切な選択がなされるとき、ST 作成者によって含められるべきである。*

非対称鍵は、鍵チェインのために使用されることもある。ゆえに、ST 作成者は、非対称鍵生成が使用される場合、FCS_CKM.1(a)を選択するべきである。

TOE が RSA 鍵確立方式における受信者としてふるまう場合、TOE は、RSA 鍵生成を実装する必要はない。

すべての方式 (RSA 方式, ECC 方式, FFC 方式)について、RBG は、a)RSA 用にシード値を生成する必要があり、かつ b)ECC 及び FFC 用のプライベート鍵を直接生成する必要がある。そのため FCS_RBG_EXT.1 は、本 SFR と共に使用される。FIPS 186-4 の附属書 B.3.2 または B.3.5 のいずれかに基づく鍵ペア生成アルゴリズムが選択される場合、ハッシュアルゴリズムもまた要求される。このような場合、FCS_COP.1(d)が本 SFR と共に使用される。

FCS_CKM.1(b) 暗号鍵生成 (対称鍵)

FCS_CKM.1.1(c) 詳細化： TSF は、以下を満たす、**FCS_RBG_EXT.1 で規定されたとおりの乱数ビット生成器**及び規定された暗号鍵長[*選択： 128 ビット、 256 ビット*]**を用いて対称**暗号鍵を生成しなければならない：[*規格なし*]。

適用上の注釈：*対称鍵生成機能は、鍵チェインに沿った鍵または DEK の生成に使用されてもよい。また、鍵コンバイニング、鍵暗号化、または鍵ラッピングのための入力を提供するために使用されてもよい。したがって、ST 作成者は、対称鍵生成が使用される場合、FCS_CKM.1(b)を選択するべきである。*

FCS_CKM.4(b) 暗号鍵破棄 (TOE 管理のハードウェア)

FCS_CKM.4.1 (b) 詳細化：TSF は、以下を満たす、規定された暗号鍵破棄方法：[***選択：***

- ***揮発性メモリについて、破棄は以下によって実行されなければならない(shall)：[選択：***
  - ***以下からなる 1 回上書き：[選択：***
    - ***TSF の RBG を用いる疑似ランダムパタン、***
    - ***すべてゼロ、***
    - ***すべて 1、***
    - ***鍵の新しい値、***
    - ***[割付： CSP を何ら含まないような何らかの値]]、***
  - ***メモリへの電力の遮断、***
  - ***その鍵への直接の参照の破棄、その後にガーベージコレクションの要求]；***
- ***不揮発性メモリについて、[選択：***
  - ***ウェアレベリングアルゴリズムを採用する場合、破棄は、以下によって実行されなければならない(shall)：[選択：***
    - ***すべてゼロからなる 1 回の上書き、***
    - ***すべて 1 からなる 1 回の上書き、***
    - ***同じ長さの鍵の新しい値で上書き、***
    - ***[割付： CSP を何ら含まないような何らかの値]からなる 1 回の上書き、***
    - ***ブロック消去]；***
  - ***ウェアレベリングアルゴリズムを採用しない場合、破棄は、以下によって実行されなければならない(shall)：[選択：***
    - ***[選択：1 回、[割付：ST 作成者が定義した複数回]]のすべてゼロからなる上書き、その後読み出し検証を行う、***
    - ***[選択：1 回、[割付：ST 作成者が定義した複数回]]のすべて 1 からなる上書き、その後読み出し検証を行う、***
    - ***同じ長さの鍵の新しい値で上書き、その後読み出し検証を行う、***
    - ***[選択：1 回、[割付：ST 作成者が定義した複数回]]の[割付： CSP を何ら含まないような何らかの値]からなる上書き、その後読み出し検証を行う、***
    - ***ブロック消去]***

    かつ、上書きデータの読み出し検証が失敗する場合、処理は[割付：上書きを試行する回数]回まで繰り返されなければならない(shall)、その場合はエラーが返される。

  ]

]に従って、暗号学的鍵を破棄しなければならない(shall)：[*規格なし*]。

適用上の注釈：*最初の選択において、ST 作成者は、TOE 内に鍵が格納されるようなメモリまたはストレージの技術に基づく鍵の破棄のための選択肢を提示されている。*

不揮発性メモリが鍵を格納するために利用される場合、ST 作成者は、メモリストレージアルゴリズムがウェアレベリングを利用するかしないかを選択する。ウェアレベリングを利用するようなストレージ技術またはメモリ種別は、読み出し検証の実行は要求されない。破棄の選択にはオプションとしてブロック消去が含まれる、このオプションは、フラッシュメモリに対してのみ適用される。ブロック消去は、読み出し検証を要求しない、なぜなら消去されたメモリのロケーションへの論理アドレスのマッピングは、データ自体と同様に消去されるからである。

選択の中には、鍵の新しい値で使用されなくなった鍵を上書きする選択肢がある。その意図は、新しい鍵の値(本 PP の別の SFR で規定される通り)が既存の鍵を「置き換える」ために利用されることを可能としている。

読み出し検証についての選択肢が選択される場合、失敗に際して監査記録が生成されるべきである。

いくつかの選択は、「CSP を何ら含まないような値」の割付を許容している。これは、TOE がその他の選択肢として列挙された特定の値でないような、FCS_RBG_EXT 要件を満たす RBG から導かれない何らかの規定されたデータを利用することを意味する。「CSP を何ら含まない」というフレーズのポイントは、上書きデータが注意深く選択され、それ自身が機密性保護を要求するような現在のデータまたは残存データを含むかもしれないような一般的な「プール」から取り出されたものではないことを保証することである。

鍵破棄は、非対称鍵ペアの公開鍵部分には適用されない。

FCS_CKM.4(c) 暗号鍵破棄(汎用ハードウェア)

FCS_CKM.4.1 (c)　詳細化：TSF は、以下を満たす、規定された暗号鍵破棄方法：[***選択：***

- ***揮発性メモリについて、破棄は以下によって実行されなければならない(shall)：[選択：***
  - ***以下からなる 1 回上書き：[選択：***
    - ***TSF の RBG を用いる疑似ランダムパタン、***
    - ***すべてゼロ、***
    - ***すべて 1、***
    - ***鍵の新しい値、***
    - ***[割付：CSP を何ら含まないような何らかの値]、***
  - ***メモリへの電力の遮断、***
  - ***その鍵への直接の参照の破棄、その後にガーベージコレクションの要求]；***
- ***不揮発性メモリについて、以下からなる[選択：1 回、[割付：ST 作成者が定義する複数回]] の上書きを実行する：[選択：***
  - ***TSF の RBG を用いる疑似ランダムパタン、***
  - ***すべてゼロ、***
  - ***すべて 1、***
  - ***同じ長さの鍵の新しい値、***

- ***[割付：CSP を何ら含まないような何らかの値]、ブロック消去]***

]
]に従って、暗号学的鍵を破棄しなければならない(shall)：[*規格なし*]。

適用上の注釈：*最初の選択において、ST 作成者は、TOE 内の揮発性メモリまたは不揮発性ストレージ内に鍵があるかどうかに基づいて利用されない暗号鍵の破棄についての選択肢を提示されている。不揮発性ストレージのブロック消去の選択は、フラッシュメモリへのみ適用される。ブロック消去は、メモリロケーションへの参照は、データ自体と同様に消去されるので、読み出し検証を要求しない。*

選択内に鍵の新しい値を用いてメモリロケーションを上書きする選択肢がある。意図は、鍵の新しい値が(本 PP 内の別の SFR で規定されるとおり)既存の鍵を「置き換える」ために使用可能であることである。

いくつかの選択が「CSP を何ら含まないような何らかの値」の割付を可能にする。これは、TOE が FCS_RBG_EXT 要件を満たす RBG から引き出されない何らかの他の規定されたデータを利用することを意味し、他の選択肢のように列挙された特定の値のいずれかでないことを意味する。「CSP を何ら含まない」という部分は、上書きされるデータが注意深く選択され、かつそれ自身が機密性保護を要求するような現在のまたは残存のデータを含むかもしれない一般的な「プール(貯めておくところ)」から取り出されないことを保証することである。

鍵破棄は、非対称鍵ペアの公開鍵コンポーネントへは適用されない。

FCS_CKM.4(d) 暗号鍵破棄(ソフトウェア TOE、サードパーティ製ストレージ)

FCS_CKM.4.1 (d)　詳細化：TSF は、以下を満たす、規定された暗号鍵破棄方法：[***選択：***

- ***揮発性メモリについて、破棄は以下によって実行されなければならない(shall)：[選択：***
  - ***以下からなる 1 回上書き：[選択：***
    - ***TSF の RBG を用いた疑似ランダムパタン、***
    - ***すべてゼロ、***
    - ***すべて 1、***
    - ***鍵の新しい値、***
    - ***[割付：CSP を何ら含まないような何らかの値]]、***
  - ***メモリへの電力供給停止、***
  - ***その鍵への直接の参照の破棄、その後でガーベージコレクションの要求]；***
- ***不揮発性ストレージで、以下のような下位プラットフォームによって提供されるインタフェースの呼び出しからなるようなものについて：[選択：***
  - ***鍵のストレージロケーションを論理的にアドレス指定し、以下からなる [選択：1 回、[割付：ST 作成者が定義する複数回]] の上書きを実行する：[選択：***
    - ***TSF の RBG を用いた疑似ランダムパタン、***
    - ***すべてゼロ、***
    - ***すべて 1、***
    - ***鍵の新しい値、***
    - ***[割付：CSP を何ら含まないような何らかの値]、ブロック消去]；***
  - ***鍵を表現するような抽象化を破棄するよう下位プラットフォームに指示する]***

]
]に従って、暗号学的鍵を破棄しなければならない(shall)：[*規格なし*]。

適用上の注釈：*本要件で参照されるインタフェースは、異なる形状を取る可能性があり、OS カーネルへのアプリケーションプログラムインタフェース(API)のようなものである可能性が最も高い。さまざまなレベルの目に見える抽象化があるかもしれない。例えば、所与の実装において、アップリケーションは、ファイルシステムの詳細へのアクセスを有するかもしれないし、具体的なメモリロケーションに論理的にアドレス指定が可能かもしれない。別の実装では、アプリケーションは、単に資源へのハンドルを有しているかもしれないし、そのプラットフォームに資源の削除を依頼することだけが可能かもしれない。TOE がアクセスを有する詳細レベルは、ST の TSS セクションで反映されるだろう。*

いくつかの選択が「CSP を何ら含まないような何らかの値」の割付を可能にする。これは、TOE が FCS_RBG_EXT 要件を満たす RBG から引き出されない何らかの他の規定されたデータを利用することを意味し、他の選択肢のように列挙された特定の値のいずれかでないことを意味する。「CSP を何ら含まない」という部分は、上書きされるデータが注意深く選択され、かつそれ自身が機密性保護を要求するような現在のまたは残存のデータを含むかもしれない一般的な「プール(貯めておくところ)」から取り出されないことを保証することである。

鍵破棄は、非対称鍵ペアの公開鍵コンポーネントへは適用されない。

FCS_COP.1(a) 暗号操作 (署名検証)

FCS_COP.1.1(a) 詳細化：TSF は、以下を満たす、 [*暗号署名サービス(検証)*] を [***選択：***

- ***RSA ディジタル署名アルゴリズムで、鍵長 (modulus) が 2048 ビット以上のもの、***
- ***楕円曲線ディジタル署名アルゴリズムで、鍵長が 256 ビット以上のもの***

]に従い、実行しなければならない(shall)： [*選択：*

- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1-v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3, for RSA schemes***
- ***FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [selection: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4, for ECDSA schemes***

]。

適用上の注釈： *ST 作成者は、ディジタル署名を実行するために実装されたアルゴリズムを選択するべきである。選択されたアルゴリズムについて、ST 作成者は、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ために、適切な割付／選択を行うべきである。*

FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム)

FCS_COP.1.1(b) 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：SHA-256、SHA-384、SHA-512***]に従って[*暗号ハッシュサービス*]を実行しなければならない(shall)：[*ISO/IEC 10118-3:2004*] 。

適用上の注釈：*ハッシュ選択は、FCS_COP.1(a)に使用されるアルゴリズムの総合的な強度と一貫しているべきである。例えば、SHA256 は 、2048 ビット RSA または P-256 を用いた*

ECC 用に選択されるべきであり、SHA-384 は 3072 ビット RSA、4096 ビット RSA、または P-384 を用いた ECC 用に選択されるべきであり、SHA 512 は P-521 を用いた ECC 用に選択されるべきである。規格の選択は、選択されたアルゴリズムに基づいてなされる。

FCS_COP.1(c) 暗号操作 (メッセージ認証)

FCS_COP.1.1(c) **詳細化：**TSF は、以下を満たす、[*メッセージ認証*]を規定された暗号アルゴリズム[**選択： HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512、CMAC-AES-128、CMAC-AES-256**]及び暗号鍵長[***割付: [選択：HMAC、AES] で使用される鍵長(ビット)***] に従って実行しなければならない(shall)：[***選択：ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"、 NIST SP 800-38B***]。

適用上の注釈： *1 つ以上の HMAC アルゴリズムが選択される場合、ST 作成者は、2 番目の選択で「HMAC」を選択し、3 番目の選択で「ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"」を選択する。割付において、鍵長 [k] は、L1 と L2 の間の範囲に入る。(適切なハッシュ関数について、ISO/IEC 10118 で定義されている)。例えば、SHA-256 については、L1=512 かつ L2 =256 となる、ここで、 $L2 \leq k \leq L1$ となる。*

1 つ以上の CMAC アルゴリズムが選択される場合、ST 作成者は、2 番目の選択肢で「AES」及び 3 番目の選択で「NIST SP 800-38B」を選択する。割付については、鍵長は、128 と 256 の間の範囲に入る。

FCS_COP.1(d) 暗号操作(鍵ラッピング)

FCS_COP.1.1(d) **詳細化：**TSF は、以下を満たす、[*鍵ラッピング*]を規定された暗号アルゴリズム[*AES*] を**以下のモード**[**選択：KW, KWP, GCM, CCM**]及び暗号鍵長[***選択：128 ビット、256 ビット***]に従って、実行しなければならない(shall)：[*ISO/IEC 18033-3 (AES) で規定される AES、*[***選択：NIST SP 800-38F、ISO/IEC 19772、その他の規格なし***]]。

適用上の注釈： *ST 作成者が FCS_KYC_EXT.1 で規定される鍵チェイニング アプローチで、鍵ラッピングの利用を選択する場合、本要件は ST の本文で使用されること。*

FCS_COP.1(e) 暗号操作 (鍵配送)

FCS_COP.1.1(e) **詳細化：** TSF は、以下を満たす、[*鍵配送*]を規定された暗号アルゴリズム[*以下のモード*[***選択：KTS-OAEP、 KTS-KEM-KWS***] *での RSA*]及び暗号鍵長[***選択：2048 ビット、 3072 ビット***]に従い、実行しなければならない(shall)：[*NIST SP 800-56B, Revision 1*]。

適用上の注釈：*ST 作成者が FCS_KYC_EXT.1 で規定された鍵チェイニング アプローチで、鍵配送の利用を選択する場合、本要件は ST の本文にて使用されること。*

FCS_COP.1(f) 暗号操作 (AES データ暗号化／復号)

FCS_COP.1.1(f) **詳細化：**TSF は、以下を満たす、[*データ暗号化及び復号*]を規定された暗号アルゴリズム[[***選択：CBC、GCM、XTS***] *モードで使用される AES*]及び暗号鍵長 [***選択：128 ビット、256 ビット***]に従って、実行しなければならない(shall)：[*ISO/IEC 18033-3 で規定される AES、*[***選択：ISO/IEC 10116 で規定される CBC、ISO/IEC 19772 で規定される GCM、IEEE 1619 で規定される XTS***]]。

適用上の注釈：*本 cPP は、ソフトウェア暗号化またはハードウェア暗号化を許容している。ソフトウェア暗号化では、TOE はデータ暗号化／復号を提供できる、またはホストプラットフォームが暗号化／復号を提供するかもしれない。反対に、ハードウェア暗号化については、暗号化／復号は、汎用コントローラ内の専用ハードウェア、ストレージデバイスの SOC、または専用(コ)プロセッサのようにさまざまなメカニズムによって提供されることがある。*

XTS モードが選択される場合、256 ビットまたは 512 ビットの暗号鍵長が IEEE1619 で規定されるとおり許可される。XTS-AES 鍵は、２つの等しい鍵長に分割される - 例えば、256 ビット鍵と XTS モードが選択されるとき、AES-128 が基礎となるアルゴリズムとして使用される。512 ビット鍵と XTS モードが選択されるとき、AES-256 が使用される。

本要件の意図は、ハードディスク上の適切な情報の AES 暗号化のために ST 作成者が選択して良い承認された AES モードを特定することである。最初の選択について、ST 作成者は TOE 実装によりサポートされるモード(ひとつまたは複数)を示すべきである。2 番目選択は、使用される鍵長を示し、FCS_CKM.1(1)で特定されるものと同一である。3 番目の選択は、最初の選択で特定されたモード(ひとつまたは複数)と一致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、ST の中で本コンポーネントを繰り返し使用した方がより明確であろう。

FCS_COP.1(g) 暗号操作 (鍵暗号化)

FCS_COP.1.1(g) **詳細化：** TSF は、以下を満たす、[*鍵暗号化及び復号*]を規定された暗号アルゴリズム[*[**選択：CBC、GCM**]モードで使用される AES*]及び暗号鍵長 [選択：128 ビット、256 ビット] に従って、実行しなければならない(shall)：[*ISO/IEC 18033-3 で規定される AES、[**選択：ISO/IEC 10116 で規定される CBC、ISO/IEC 19772 で規定される GCM**]*]。

適用上の注釈：*ST 作成者が FCS_KYC_EXT.2 で規定される鍵チェイニングアプローチの一部として鍵を保護するために AES 暗号化／復号の使用を選択する場合、本要件は ST の本文において使用されること。*

FCS_KDF_EXT.1 暗号鍵導出

FCS_KDF_EXT.1.1 TSF は、出力が少なくとも BEV と等しいセキュリティ強度(ビット数で) となるように、FCS_COP.1(c)で規定される鍵付ハッシュ関数を用いて、中間鍵を導出するため、 [選択：FCS_RBG_EXT.1 で規定される RNG 生成されたサブマスク、調整されたパスワードサブマスク、インポートされたサブマスク]を以下で定義されるとおり受け入れなければならない(shall) [選択：

- NIST SP 800-108 [選択：カウンターモードを用いた KDF、フィードバックモードを用いた KDF、ダブルパイプライン繰り返しモードを用いた KDF]、
- NIST SP 800-132]。

適用上の注釈：*ST 作成者が、FCS_KYC_EXT.2 で規定される鍵チェイニング アプローチにおいて鍵導出の利用を選択する場合、本要件は ST の本文において使用されること。*

FCS_RBG_EXT.1 乱数ビット生成

FCS_RBG_EXT.1.1 TSF は、[選択：ISO/IEC 18031:2011、NIST SP 800-90A]に従い、[選択：Hash_DRBG (任意)、HMAC_DRBG (任意)、CTR_DRBG (AES)]を用いて、すべての決定論的乱数ビット生成サービスを実行しなければならない(shall)。

FCS_RBG_EXT.1.2 決定論的 RBG は、[選択：

- [*割付：ソフトウェアベースのノイズ源の数*]個のソフトウェアベースのノイズ源、
- [*割付：ハードウェアベースのノイズ源の数*]個のハードウェアベースのノイズ源]

からエントロピーを蓄積するような、少なくとも 1 つのエントロピー源によってシード値を与えられなければならない(shall)。ここで、ノイズ源については、ISO/IEC 18031:2011 Table C.1 「Security Strength Table for Hash Functions」に従い、生成する鍵やハッシュの最大セキュリティ強度と少なくとも等しく、かつ最小でも[選択：128 ビット、256 ビット]のエントロピーを持つようなものでなければならない(shall)。

適用上の注釈： *ISO/IEC 18031:2011 には、乱数を生成する異なる複数の方法が含まれている；これらは、それぞれ、言い換えれば、下位の暗号プリミティブ (ハッシュ関数／暗号) に依存している。ST 作成者は、使用される関数を選択し、その要件で使用される具体的な下位の暗号プリミティブを含めること。識別されたハッシュ関数(SHA-256, SHA-512)のいずれも Hash_DRBG または HMAC_DRBG 用として許容されるが、CTR_DRBG には AES ベースの実装のみが許容される。ISO/IEC 18031:2011 の表 C.2 は、AES-128 及び 256 ブロック暗号用のセキュリティ強度の識別、エントロピー及びシード長の要件を提供している。*

ISO/IEC 18031:2011 の CTR_DRBG は導出関数の使用を要求するが、NIST SP 800-90A では要求されない。いずれのモデルも受け入れ可能である。FCS_RBG_EXT.1.1 の最初の選択において、ST 作成者は適合する規格を選択すること。

FCS_RBG_EXT.1.2 の最初の選択では、ST 作成者は、採用されるエントロピー源のタイプごとにいくつのエントロピー源が使用されるかを記入する。ハードウェア及びソフトウェアベースのノイズ源の組合せが受け入れ可能であることに注目するべきである。

*エントロピー源は、DRBG の一部と考えられ、DRBG が TOE に含まれている場合、開発者は附属書D に概説されるエントロピー記述を提供することが要求されることに注目するべきである。本エレメントの評価アクティビティで要求される 文書化 *及びテスト* が FCS_RBG_EXT.1.2 で示された各エントロピー源を必ず網羅すること。エントロピー文書が個別のエントロピー源からのエントロピーが独立に生成されることを実証するならば、最小限必要なエントロピーの量を、エントロピープールへの個別の寄与を組み合わせることで提供するとしてもよい。*

FCS_SMC_EXT.1 サブマスクコンバイニング

FCS_SMC_EXT.1.1 TSFは、以下の方法 [選択：排他的論理和 (XOR)、SHA-256、SHA-512] を用いて、[*中間鍵またはDEK*]を生成するために、サブマスクをコンバイニングしなければならない(shall)。

適用上の注釈： *本要件は、製品が XOR または承認された SHA-hash のいずれかを用いてさまざまなサブマスクをコンバイニングする方法を規定する。承認されたハッシュ関数は、FCS_COP.1(b)において取り込まれている。*

B.2　クラス: TSF の保護 (FPT)

FPT_FUA_EXT.1 ファームウェアアップデート検証

FPT_FUA_EXT.1.1 TSFは、[選択：公開鍵、FCS_COP.1(b)で規定される公開鍵のハッシュ値] を含むようなRTUを用いるような、FCS_COP.1(a)で規定されるディジタル署名アルゴリズムを用いて、ファームウェアアップデートの情報源を認証しなければならない(shall)。

FPT_FUA_EXT.1.2 TSFは、ディジタル署名がFCS_COP.1(a)で規定されるとおり検証が成功した場合にのみ、アップデートのインストールを許可しなければならない(shall)。

FPT_FUA_EXT.1.3 TSFは、FPT_TUD_EXT.1.2で記述されるメカニズムを用いて、ディジタル署名の検証が成功した後にのみ、既存のファームウェアの改変を許可しなければならない(shall)。

適用上の注釈： *TSF のファームウェア部分(例、RTU(鍵ストア及び署名検証アルゴリズム))は、TOE 上の書込み保護された領域に格納されなければならない。ファームウェアは、FPT_FUA_EXT.1 で記述された認証されたアップデートメカニズムを用いてのみ、製造後の状態において改変可能でなければならない。TSF は、FPT_TUD_EXT で規定されたメカニズムを用いてのみ改変可能である。*

FPT_FUA_EXT.1.4 TSF は、ファームウェアアップデート処理の任意の一部が失敗する場合、エラーコードが返されなければならない(shall)。

適用上の注釈： *これらの要件は、製造中のドライブではなく－動作状態にある SED についてのものである。*

認証されたファームウェアアップデートメカニズムは、ファームウェアアップデートイメージの真正性を保証するため、ディジタル署名を採用する。TSF は、アップデートイメージの署名を検証するために必要とされる公開鍵を含むような、署名検証アルゴリズムと鍵ストアを含むような RTU を提供する。RTU 内の鍵ストアには、公開鍵の複製がアップデートイメージと共に提供される場合、アップデートイメージまたはその公開鍵のハッシュに対する署名を検証するために使用される公開鍵が含まれる。後者の場合、アップデートメカニズムは、アップデートイメージと共に提供された公開鍵をハッシュしなければならない、またアップデートイメージの署名を検証するために提供された公開鍵を使用する前に鍵ストア内に現れるようなハッシュ値と一致することを保証しなければならない。公開鍵のハッシュ値が選択される場合、ST 作成者は、使用されるハッシュ関数を特定するため－FCS_COP.1(b)要件を繰り返しすることができる。

本要件の意図は、認証されたアップデートメカニズムは、新しいイメージがディジタル署名されていること；及びアップデートが実施される前にディジタル署名が公開鍵を用いて検証可能であることを、保証すると規定することである。本要件は、ディジタル署名が TSF によって検証成功したときにのみアップデートのインストレーションを認証されたアップデートメカニズムが許可することも規定する。

附属書 C: 拡張コンポーネント定義

本附属書は、附属書 A 及び B で使用されるものを含め、cPP で使用される拡張要件の定義を含んでいる。

本 cPP に使用される拡張要件のいくつかは、本 cPP の中で繰り返される SFR への依存性がある(例えば、FCS_COP.1(d))。これらの依存性のために SFR の名称が、他のプロテクションプロファイルで使用される同じ拡張コンポーネントと異なるかもしれないことを読者に忠告する。

C.1 背景と適用範囲

本書は、この cPP で使用されるすべての拡張コンポーネントの定義を提供する。これらのコンポーネントは以下の表において識別される：

表 4：拡張コンポーネント

Functional Class	Functional Components
暗号サポート(FCS)	FCS_CKM_EXT 暗号鍵管理
	FCS_KDF_EXT 暗号鍵導出
	FCS_KYC_EXT 鍵チェイン
	FCS_RBG_EXT 暗号操作(乱数ビット生成)
	FCS_SMC_EXT サブマスクコンバイニング
	FCS_SNI_EXT 暗号操作(ソルト、ノンス、初期化ベクタ)
	FCS_VAL_EXT 暗号による要素検証
利用者データ保護(FDP)	FDP_DSK_EXT データ上のデータ保護
TSF 保護(FPT)	FPT_FAC_EXT ファームウェアアクセス制御
	FPT_FUA_EXT ファームウェアアップデート検証
	FPT_KYP_EXT 鍵及び鍵材料の保護
	FPT_RBP_EXT ロールバック保護
	FPT_TST_EXT TSF のテスト
	FPT_TUD_EXT 高信頼アップデート

いくつかの拡張コンポーネントは、本 cPP で定義された、繰り返される Part 2 の SFR の依存性を定義していることに留意されたい。本定義は、これらの依存性がその SFR を主張する PP に含まれることを義務付けるが、その依存する SFR が同じ繰り返し識別子を用いて定義されることを義務付けてはいない (例、FCS_KDF_EXT.1 の包含は、FCS_COP.1(c)として特に識別されるべき鍵付きハッシュメッセージ認証の依存する SFR を要求せず、FCS_COP.1 繰り返しが存在すること、及び本 cPP が FCS_COP.1(c)として定義するものと同じふるまいを定義することのみを義務付けている)。

C.2 拡張コンポーネント定義

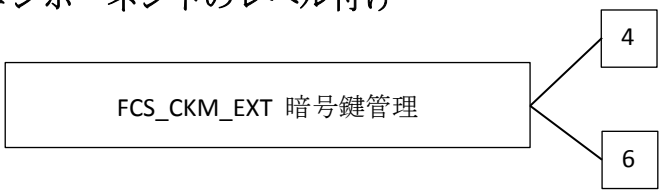
FCS_CKM_EXT 暗号鍵管理

ファミリのふるまい

暗号鍵は、そのライフサイクルにわたって管理されなければならない(must)。本ファミリは、ライフサイクルをサポートし、その結果として以下のアクティビティについての要件を定めることを意図している：暗号鍵生成、暗号鍵配付、暗号鍵アクセス及び暗号鍵破棄。本ファミリは、暗号鍵の管理のための機能要件がある限り含まれるべきである。

本ファミリの作成は、CC Part 2 が鍵破棄の方法を規定する能力を提供するが、鍵破棄のタイミングまたは複数の鍵破棄方法を実装する能力についての SFR を定義していないため、必要である

コンポーネントのレベル付け



FCS_CKM_EXT.4 鍵及び鍵材料の破棄は、(CC Part 2 で、FCS_CKM.4 として定義されるような、実際の破棄方法とは対照的に) TSF に、鍵が破棄されるときの状況を規定することを要求する。番号 4 は、2 つの SFR 間の類似性を反映するために選択された。

FCS_CKM_EXT.6 暗号鍵破棄の種別は、TOE に、複数の鍵破棄方法の間で選択する能力を提供する。

管理： FCS_CKM_EXT.4

特定の管理機能は識別されない。

監査： FCS_CKM_EXT.4

予見される監査対象事象はない。

管理： FCS_CKM_EXT.6 (訳注：原文は 4 だが、6 が正しい)

特定の管理機能は識別されない。

監査： FCS_CKM_EXT.6 (訳注：原文は 4 だが、6 が正しい)

予見される監査対象事象はない。

FCS_CKM_EXT.4　暗号鍵及び鍵材料の破棄

下位階層：　なし

依存性：　　なし

FCS_CKM_EXT.4.1　TSF は、すべての鍵及び鍵材料がもはや不要となったとき、それらを破棄しなければならない(shall)。

FCS_CKM_EXT.6　暗号鍵破棄の種別

下位階層：　なし

依存性：　　FCS_CKM.4 暗号鍵破棄

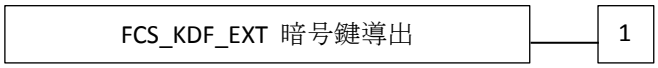
FCS_CKM_EXT.6.1　TSF は、[*割付：セキュリティターゲットのどこかで定義されたFCS_CKM.4 の2 つ以上の繰り返し*] の鍵破棄方法を使用しなければならない(shall)。

FCS_KDF_EXT 暗号鍵導出

ファミリのふるまい

本ファミリは、中間鍵が規定されたセットのサブマスクから導出される手段を規定する。

コンポーネントのレベル付け



FCS_KDF_EXT.1　暗号鍵導出は、TSF に、規定されたハッシュ関数を用いてサブマスクから中間鍵を導出することを要求する。

管理：FCS_KDF_EXT.1

特定の管理機能は識別されていない。

監査：FCS_KDF_EXT.1

予見される監査対象事象はない。

FCS_KDF_EXT.1　暗号鍵導出

下位階層：　なし

依存性；　　FCS_COP.1(c) 暗号操作 (鍵付ハッシュアルゴリズム)

FCS_KDF_EXT.1.1 TSF は、出力が少なくとも BEV と等しいセキュリティ強度(ビット数で) となるように、FCS_COP.1(c)で規定される鍵付ハッシュ関数を用いて、中間鍵を導出するため、[選択：FCS_RBG_EXT.1 で規定される RNG 生成されたサブマスク、調整されたパスワードサブマスク、インポートされたサブマスク]を以下で定義されるとおり受け入れなければならない(shall) [選択：

- NIST SP 800-108 [選択：カウンターモードを用いた KDF、フィードバックモードを用いた KDF、ダブルパイプライン繰り返しモードを用いた KDF]、
- NIST SP 800-132]。

FCS_KYC_EXT 鍵チェイニング

ファミリのふるまい

本ファミリは、ドライブ上の暗号化された保護データを最終的にセキュアにするための多層の暗号鍵を用いるために使用される仕様を提供する。

コンポーネントのレベル付け

FCS_KYC_EXT.1 鍵チェイニング(イニシエータ)は、TSF に、TOE 外部のコンポーネントへ提供される BEV の鍵チェインの維持を要求する。

FCS_KYC_EXT.2 鍵チェイニング(受信者)は、TSF に、何らかの方法を介して TSF によって利用される DEK へチェインされる BEV を受け入れ可能であることを要求する。

本 cPP は、FCS_KYC_EXT.2 を含まないことに留意されたい；ここでは、FCS_KYC_EXT ファミリの完全な定義を提供するために含まれている。

管理：FCS_KYC_EXT.1

特定の管理機能は識別されていない

監査： FCS_KYC_EXT.1

予見される監査対象事象はない。

管理：FCS_KYC_EXT.2

特定の管理機能は識別されていない

監査： FCS_KYC_EXT.2

予見される監査対象事象はない。

FCS_KYC_EXT.1 鍵チェイニング（イニシエータ）

下位階層：なし

依存性： FCS_CKM.1(a) 暗号鍵生成 (非対称鍵),
FCS_CKM.1(b) 暗号操作(対称鍵),
FCS_COP.1(d) 暗号操作(鍵ラッピング),
FCS_COP.1(e) 暗号操作(鍵配送),
FCS_COP.1(g) 暗号操作 (鍵暗号化),
FCS_SMC_EXT.1 サブマスクコンバイニング,
FCS_VAL_EXT.1 検証
FCS_VAL_EXT.2 利用者検証

FCS_KYC_EXT.1.1 TSF は、以下の鍵チェインを維持しなければならない(shall)：
[選択：

- BEV としてサブマスクを使用するもの；
- 以下の方法を用いて TSF によって生成される中間鍵：[選択：
  - FCS_CKM.1(a)で規定される非対称鍵生成、
  - FCS_CKM.1(b)で規定される対称鍵生成]；
- 以下の方法を用いて BEV への一つ以上のサブマスクから由来の中間鍵：[選択：
  - FCS_KDF_EXT.1 で規定される鍵導出(key derivation)、
  - FCS_COP.1(d)で規定される鍵ラッピング(key wrapping)、
  - FCS_SMC_EXT.1 で規定される鍵コンバイニング(key combining)、
  - FCS_COP.1(e)で規定される鍵配送(key transport)、
  - FCS_COP.1(g)で規定される鍵暗号化(key encryption)]]

ここで、対称鍵については[選択：128 ビット、256 ビット]の有効な強度、及び非対称鍵については[選択：該当なし、112 ビット、128 ビット、192 ビット、256 ビット]の有効な強度を維持すること。

FCS_KYC_EXT.1.2 TSF は、[選択：128 ビット、256 ビット]の BEV を[*割付：1 つ以上の外部エンティティ*]へ以下のように提供しなければならない(shall)：[選択：

- FCS_VAL_EXT.1 で規定されるとおり TSF が検証プロセスの実行に成功した後に、
- 検証を実行することなしに**]。**

適用上の注釈：*鍵チェイニングは、BEV (境界暗号化値) を最終的にセキュアにするために多階層の暗号鍵を用いる方法である。 中間鍵の数は、1 つ(例、調整されたパスワード認証要素を用いたり、直接それを BEV として用いたりするように)から数多くまでさまざまである。これは、BEV の最終的なラッピング、または BEV の導出に*

寄与するすべての鍵に適用される；保護されたストレージの領域におけるもの（例、TPM 保存の鍵、比較用の値）を含めて適用される。

FCS_KYC_EXT.2 鍵チェイニング（受信者）

下位階層： なし

依存性： なし

FCS_KYC_EXT.2.1 TSF は、[選択：128 ビット、256 ビット] の BEV を[*割付：1 つ以上の外部エンティティ*] から受け入れなければならない(shall)。

FCS_KYC_EXT.2.2 TSF は、以下の方法を用いて BEV から DEK へ向けて生成する中間鍵のチェインを維持しなければならない(shall)：[選択：

- FCS_CKM.1(a)で規定される非対称鍵生成、
- FCS_CKM.1(b)で規定される対称鍵生成、
- FCS_KDF_EXT.1 で規定される鍵導出、
- FCS_COP.1(d)で規定される鍵ラッピング、
- FCS_SMC_EXT.1 で規定される鍵コンバイニング、
- FCS_COP.1(e)で規定される鍵配送、
- FCS_COP.1(g)で規定される鍵暗号化]

ここで、対称鍵については[選択：128 ビット、256 ビット]の有効な強度及び非対称鍵については[選択：該当なし、112 ビット、128 ビット、192 ビット、256 ビット]の有効な強度を維持すること。

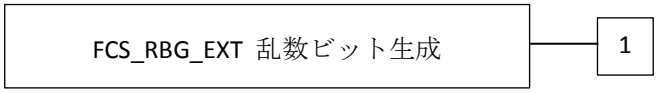
適用上の注釈： *鍵チェイニングは、ドライブ上の暗号化された保護データを究極的にセキュアにするために多階層暗号鍵を用いる方法である。中間鍵の数は、1 つから(例えば、鍵暗号化鍵(KEK)として BEV を用いるように)数多くまでさまざまである。これが最終的なラッピング、または DEK の導出に寄与するすべての鍵に適用される；保護されたストレージの領域におけるそれら(例えば、TPM 保存の鍵、比較用の値)を含めて適用される。*

FCS_RBG_EXT 乱数ビット生成

ファミリのふるまい

本ファミリのコンポーネントは、乱数ビット／乱数の生成についての要件に対処する。これは FCS クラスとして定義された新しいファミリである。

コンポーネントのラベル付け



FCS_RBG_EXT.1 乱数ビット生成は、乱数ビット生成に、選択された規格に従って実行され、エントロピー源によってシード値を供給されることを要求する。

管理： FCS_RBG_EXT.1

特定の管理機能は識別されていない。

監査： FCS_RBG_EXT.1

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである：

- 攪拌プロセスの失敗

FCS_RBG_EXT.1　暗号操作 (乱数ビット生成)

下位階層：なし

依存性：　FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム) 、
FCS_COP.1(c) 暗号操作 (鍵付ハッシュアルゴリズム)

FCS_RBG_EXT.1.1　TSF は、ISO/IEC 18031:2011 に従い、[選択： Hash_DRBG (any)、 HMAC_DRBG (any)、CTR_DRBG (AES)] を用いて、すべての決定論的乱数ビット生成サービスを実行しなければならない。

FCS_RBG_EXT.1.2　決定論的 RBG は、 [選択：

- [*割付：ソフトウェアベースのノイズ源の数*]個のソフトウェアベースのノイズ源、
- [*割付：ハードウェアベースのノイズ源の数*]個のハードウェアベースのノイズ源]

からエントロピーを蓄積するような、少なくとも 1 つのエントロピー源によってシード値を与えられなければならない(shall)。ここで、ノイズ源については、ISO/IEC 18031:2011 Table C.1 「Security Strength Table for Hash Functions」に従い、生成する鍵やハッシュの最大セキュリティ強度と少なくとも等しく、かつ最小でも[選択：128 ビット、256 ビット]のエントロピーを持つようなものでなければならない(shall)。

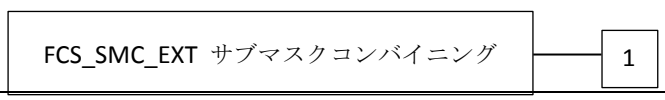
適用上の注釈： *ISO/IEC 18031:2011 には、乱数を生成する異なる複数の方法が含まれている；これらは、それぞれ、言い換えれば、下位の暗号プリミティブ (ハッシュ関数／暗号) に依存している。ST 作成者は、使用される関数を選択し、その要件で使用される具体的な下位の暗号プリミティブを含めること。識別されたハッシュ関数(SHA-256, SHA-512)のいずれも Hash_DRBG または HMAC_DRBG 用として許容されるが、CTR_DRBG には AES ベースの実装のみが許容される。*

FCS_SMC_EXT サブマスクコンバイニング

ファミリのふるまい

本ファミリは、TOE が BEV を導出または保護するために使用されるひとつ以上のサブマスクをサポートする場合、それらのサブマスクがコンバイニングされる手段を手奥呈する。

コンポーネントのレベル付け



FCS_SMC_EXT.1 サブマスクコンバイニングは、TSF に、予測可能な方法でサブマスクをコンバイニングすることを要求する。

管理： FCS_SMC_EXT.1

特定の管理機能は識別されていない。

監査： FCS_SMC_EXT.1

予見される監査対象事象はない。

FCS_SMC_EXT.1 サブマスクコンバイニング

下位階層： なし

依存性： FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム)

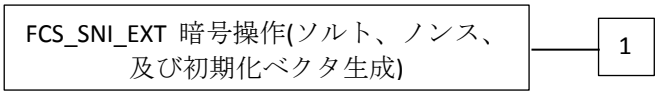
FCS_SMC_EXT.1.1 TSFは、以下の方法 [選択：排他的論理和(XOR)、SHA-256、SHA-512] を用いて、[*割付：鍵の種別*]を生成するために、サブマスクをコンバイニングしなければならない。

FCS_SNI_EXT 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成)

ファミリのふるまい

本ファミリは、ソルト、ノンス、及び IV が適格であることを保証する。

コンポーネントのレベル付け



FCS_SNI_EXT.1 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成) は、ソルト、ノンス、及び IV の生成に、規定されたやり方で実行されるべき、TOE の暗号コンポーネントによって使用されることを要求する。

管理： FCS_SNI_EXT.1

特定の管理機能は識別されていない

監査： FCS_SNI_EXT.1

予見される監査対象事象はない。

FCS_SNI_EXT.1 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成)

下位階層： なし

依存性： FCS_RBG_EXT.1 暗号操作(乱数ビット生成)

FCS_SNI_EXT.1.1 TSF は、[選択：ソルトを利用しない、[選択：FCS_RBG_EXT.1 で規定される DRBG、ホストプラットフォームによって提供される DRBG] によって生成されるソルトを使用する]ようにしなければならない(shall)。

FCS_SNI_EXT.1.2 TSF は、[選択：ノンス利用しない、最小 64 ビット長の一意のノンスを使用する]ようにしなければならない(shall)。

FCS_SNI_EXT.1.3 TSF は、以下のやり方で IV (初期化ベクタ) を生成しなければならない(shall) [選択：

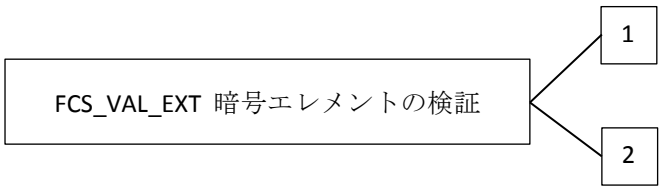
- CBC: IV は、繰り返してはならない(shall not)、
- CCM: ノンスは、繰り返してはならない(shall not)、
- XTS: IV はなし。 Tweak 値は、非負の整数であり、連続に割り当てられ、かつ任意の非負の整数から始まらなければならない(shall)、
- GCM: IV は、繰り返してはならない(shall not)。所与の秘密鍵について GCM の呼び出し回数は 2^32 回を超えてはならない(shall not)]。

FCS_VAL_EXT 暗号エレメントの検証

ファミリのふるまい

本ファミリは、サブマスク及び／または BEV が有効であることを、その利用に前に決定する手段を規定する。

コンポーネントのレベル付け



FCS_VAL_EXT.1、検証は、TSF に、1 つ以上の規定された方法によって、サブマスク及び BEV を検証することを要求する。

FCS_VAL_EXT.2、利用者検証は、TSF に、利用者に暗号データを提供する前に、利用者の要求の正当性を検証することを要求する。

管理：FCS_VAL_EXT.1

特定の管理機能は識別されていない。

監査：FCS_VAL_EXT.1

予見される監査対象事象はない。

管理：FCS_VAL_EXT.2

以下のアクションは FMT における管理機能と考えられる：

- 利用される検証方法の特定
- TSF によって受け入れられる検証試行失敗回数の設定
- 受け入れ不可能な検証試行失敗回数となるような事象における TSF によって取られるアクション

監査：FCS_VAL_EXT.2

予見される監査対象事象はない。

FCS_VAL_EXT.1 検証

下位階層： なし

依存性： FCS_COP.1(b) 暗号操作(ハッシュアルゴリズム)、
FCS_COP.1(c) 暗号操作(鍵付きハッシュアルゴリズム)、
FCS_COP.1(d) 暗号操作(鍵ラッピング)、
FCS_COP.1(f) 暗号操作(AES データ暗号化／復号)

FCS_VAL_EXT.1.1 TSF は、以下の方法を用いて[選択：サブマスク、中間鍵、BEV]の検証を実行しなければならない(shall)：[選択：

- FCS_COP.1(d) で規定される鍵ラッピング、
- [選択： FCS_COP.1(b), FCS_COP.1(c)] で規定される[選択：サブマスク、中間鍵、BEV]をハッシュし、保存されているハッシュされた[選択：サブマスク、中間鍵、BEV]と比較する、
- FCS_COP.1(f)で規定された[選択：サブマスク、中間鍵、BEV]を用いて既知の値を復号し、保存された既知の値と比較する]

FCS_VAL_EXT.1.2 TSF は、[選択：サブマスク、中間鍵、BEV] の検証を [*割付：検証を要求するアクティビティ*]の前に要求しなければならない(shall)。

FCS_VAL_EXT.1.3 TSF は、[選択：

- 設定可能な連続する検証試行失敗回数に達したときに[*DEK の鍵サニタイズを実行する*]、

- 24 時間以内に [*割付: ST 作成者が規定した試行回数*] までしか実行できないように遅延を設定する、
- 連続する検証試行失敗回数が[*割付: ST 作成者が規定した試行回数*]に達した後に検証をブロックする、
- 連続する検証試行失敗回数が[*割付：ST 作成者が規定した試行回数*] に達した後に TOE の再起動／リセットを要求する]

ようにしなければならない(shall)。

FCS_VAL_EXT.2 利用者検証

FCS_VAL_EXT.2.1 TSF は、[*割付：利用者認証の責任を負う運用環境コンポーネント*]から利用者有効性主張を受信することによって[利用者]の検証を実行しなければならない(shall)。

FCS_VAL_EXT.2.2 TSF は、[*割付：暗号操作または暗号データの送信*]の前に利用者の検証を要求しなければならない(shall)。

FCS_VAL_EXT.2.3 TSF は、[選択：

- 運用環境からの設定可能な連続失敗回数の検証試行の受信時の [*割付：鍵サニタイズアクティビティ*] 、
- 24 時間以内に[*割付：ST 作成者が規定した試行回数*]までしか実行できないように遅延を設定、
- 検証試行の連続失敗回数が[*割付: ST 作成者が規定した試行回数*]に達した後に検証をブロック、
- 検証試行の連続失敗回数が[*割付：ST 作成者が規定した試行回数*] に達した後に TOE の再起動／リセットを要求]

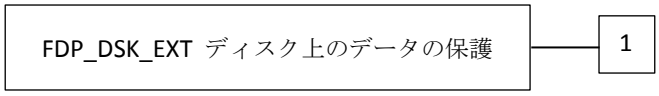
するようにしなければならない(shall)。

FDP_DSK_EXT ディスク上のデータの保護

ファミリのふるまい

本ファミリは、ディスク上で永続的なストレージに存在しているデータが不正な暴露の対象でないことを保証するための方法を規定する。

コンポーネントのレベル付け



FDP_DSK_EXT.1　検証は、1 つ以上の規定された方法によって、サブマスク及び BEV を検証することを TSF に要求する。(訳注：原文の誤り。正しくは、「ディスク上のデータの保護は、TSF が許可要素の一定の構成を受け入れ、それらを適切に条件付けすることを要求する。」)

管理： FDP_DSK_EXT.1

特定の管理機能は識別されていない

監査： FDP_DSK_EXT.1

予見される監査対象事象はない。

FDP_DSK_EXT.1 拡張：ディスク上のデータの保護

下位階層：　なし

依存性：　FCS_COP.1(f) 暗号操作 (AES データ暗号化／復号)

FDP_DSK_EXT.1.1　TSF は、ドライブに平文の保護データが一切含まれないように、FCS_COP.1(f)に従ってドライブ全体暗号化を実行しなければならない(shall)。

FDP_DSK_EXT.1.2　TSF は、利用者の介在なしにすべての保護データを暗号化しなければならない(shall)。

適用上の注釈： *本要件の意図は、あらゆる保護データの暗号化がそのデータを保護するために利用者の選択に依存しないよう特定することである。FDP_DSK_EXT.1 で規定されるドライブ暗号化は、利用者に対して透過的に発生し、データを保護するための決定は利用者の裁量の範囲外であり、それがファイル暗号化とそれを区別する特徴である。保護データの定義は、用語集で見つけることができる。*

データの暗号化／復号を実行する暗号機能は、環境によって提供されてもよい。この場合、FCS_COP.1(f) で記述されるふるまいと環境が提供する AES の実装とが一貫していることが想定されていることに注意されたい。データを暗号化／復号する暗号機能を TOE が提供する場合、ST 作成者は附属書 A から FCS_COP.1(f) を引用し、ST の本文にそれを含めること。

FPT_FAC_EXT ファームウェアアクセス制御

ファミリのふるまい

本ファミリは、そのファームウェアのアップデートを TSF が許可する前に有効な認証要素が提供されることを要求する。

コンポーネントのレベル付け

FPT_FAC_EXT.1、ファームウェアアクセス制御は、TSF に、ファームウェアアップデートを許可する前に、認証要素を要求することを要求する。

管理： FPT_FAC_EXT.1

以下のアクションは FMT における管理機能と考えられる：

a) ファームウェアアップデートを許可するために利用されるパスワードの管理

監査： FPT_FAC_EXT.1

予見される監査対象事象はない。

FPT_FAC_EXT.1 ファームウェアアクセス制御

下位階層： なし

依存性： なし

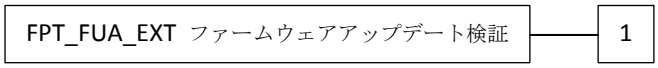
FPT_FAC_EXT.1.1 TSF は、ファームウェアアップデートが開始される前に、[選択：パスワード、デバイス上に印刷された既知の一意な値、特権利用者アクション]を要求しなければならない(shall)。

FPT_FUA_EXT ファームウェアアップデート検証

ファミリのふるまい

本ファミリは、適用される前に TSF によってファームウェアアップデートが検証されることを要求する。

コンポーネントのレベル付け



FPT_FUA_EXT.1、ファームウェアアップデート検証は、TSF に、規定された方法を用いてファームウェアアップデートを検証することを要求する。

管理： FPT_FUA_EXT.1

特定の管理機能は識別されていない。

監査：FPT_FUA_EXT.1

予見される監査対象事象はない。

FPT_FUA_EXT.1 ファームウェアアップデート検証

下位階層： なし

依存性： FCS_COP.1(a) 暗号操作 (署名検証)、
FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム)

FPT_FUA_EXT.1.1 TSFは、[選択：公開鍵、FCS_COP.1(b)で規定される公開鍵のハッシュ値] を含むようなRTUを用いるような、FCS_COP.1(a)で規定されるディジタル署名アルゴリズムを用いて、ファームウェアアップデートの情報源を認証しなければならない(shall)。

FPT_FUA_EXT.1.2 TSFは、ディジタル署名がFCS_COP.1(a)で規定されるとおり検証に成功した場合にのみ、ファームウェアアップデートのインストールを許可しなければならない(shall)。

FPT_FUA_EXT.1.3 TSFは、FPT_TUD_EXT.1.2で記述されるメカニズムを用いて、ディジタル署名の検証が成功した後にのみ、既存のファームウェアの改変を許可しなければならない(shall)。

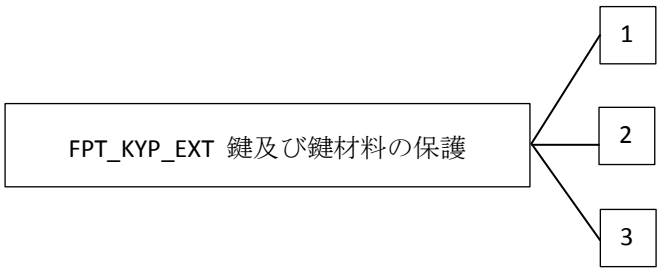
FPT_FUA_EXT.1.4 TSF は、ファームウェアアップデート処理の任意の一部が失敗する場合、エラーコードを返さなければならない(shall)。

FPT_KYP_EXT 鍵及び鍵材料保護

ファミリのふるまい

本ファミリは、鍵及び鍵材料が不揮発性ストレージへ書き込まれる場合、鍵及び鍵材料が保護されることを要求する。

コンポーネントのレベル付け



FPT_KYP_EXT.1 鍵及び鍵材料の保護は、TSF に、平文の鍵または鍵材料が不揮発性ストレージに書き込まれないことを保証することを要求する。

FPT_KYP_EXT.2 保護された鍵及び鍵材料の格納は、TSF に、暗号化された鍵または鍵材料が格納される不揮発性ストレージのロケーションを規定することを要求する。

FPT_KYP_EXT.1 保護された鍵及び鍵材料の属性は、TSF に、暗号化された鍵または鍵材料と、そのデータを復号及び／または利用することを許可されたサブジェクトの間の関係を、維持することを要求する。

管理： FPT_KYP_EXT.1

特定の管理機能は識別されていない

監査： FPT_KYP_EXT.1

予見される監査対象事象はない。

管理： FPT_KYP_EXT.2

特定の管理機能は識別されていない

監査： FPT_KYP_EXT.2

予見される監査対象事象はない。

管理： FPT_KYP_EXT.3

特定の管理機能は識別されていない

監査： FPT_KYP_EXT.3

予見される監査対象事象はない。

FPT_KYP_EXT.1 鍵及び鍵材料の保護

下位階層： なし

依存性： FCS_COP.1(d) 暗号操作 (鍵ラッピング)、
FCS_COP.1(e) 暗号操作 (鍵配送)、
FCS_COP.1(g) 暗号操作 (鍵暗号化)、
FCS_KYC_EXT.1 鍵チェイニング (イニシエータ)、
FCS_KYC_EXT.2 鍵チェイニング (受信者)、
FCS_SMC_EXT.1 サブマスクコンバイニング

FPT_KYP_EXT.1.1 TSF は、鍵が以下の基準の任意の 1 つを満たさない限り、[選択：不揮鍵メモリ内に鍵を格納しない、FCS_COP.1(d)で規定されるとおりにラッピングされるまたは FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化されるときのみ不揮発性メモリ内に鍵を格納する]ようにしなければならない：［選択：

- 平文の鍵は、以下で規定されるとおりの鍵チェインの一部ではない：[選択：
  - FCS_KYC_EXT.1、
  - FCS_KYC_EXT.2]。
- 平文の鍵は、初期プロビジョニングの後、暗号化されたデータへのアクセスをもはや提供しない。
- 平文の鍵は、FCS_SMC_EXT.1 で規定されるとおりコンバイニングされるような鍵分散であり、鍵分散の他の半分は[選択：FCS_COP.1(d)で規定されると

おりラッピングされる、FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化される、導出されて不揮発性メモリに格納されない]。

- 平文の鍵は、許可要素として利用するための外部ストレージデバイス上に格納される。
- 平文の鍵は、[選択：FCS_COP.1(d)で規定されるとおり鍵をラッピングするために利用される、FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化される]、ここで、それはすでに [選択：FCS_COP.1(d)で規定されるとおりラッピングされている、FCS_COP.1(g)または FCS_COP.1(e)で規定されるとおり暗号化されている]。

FPT_KYP_EXT.2 保護された鍵及び鍵材料の格納

下位階層： なし

依存性： FPT_KYP_EXT.1 鍵及び鍵材料の保護

FPT_KYP_EXT.2.1 TSF は、[選択：TSF 内に、運用環境の SQL データベース内に、[*割付：他の鍵ストレージ場所*]] のみに鍵及び鍵材料を格納しなければならない (shall)。

FPT_KYP_EXT.3 保護された鍵及び鍵材料の属性

下位階層： なし

依存性： FPT_KYP_EXT.1 鍵及び鍵材料の保護

FPT_KYP_EXT.3.1 TSF は、[*割付：鍵及び鍵材料のリスト*] と[*割付：識別された鍵及び鍵材料を利用することを許可されるサブジェクト*]の間の関係を維持しなければならない(shall)。

FPT_PWR_EXT 電力管理

ファミリのふるまい

本ファミリは、TOE が複数省電力状態をサポートするときの TSF のセキュアなふるまいを定義する。適合省電力状態の利用(即ち、エントリ時にセキュリティ関連データをパージするような省電力状態) が TOE 自己保護メカニズムを迂回するための攻撃ベクタとして状態遷移が利用可能でないことを保証するためには基本的なことである。

コンポーネントのレベル付け

FPT_PWR_EXT.1、省電力状態は、TSFによって実装される適合省電力状態を定義する。

FPT_PWR_EXT.2、省電力状態のタイミングは、入るべき適合省電力状態を引き起こす状況を記述する。

管理：FPT_PWR_EXT.1

以下のアクションは FMT における管理機能と考えられる：

- 個別の省電力状態の利用の有効化または無効化
- 1 つ以上の省電力状態の構成を規定する

監査：FPT_PWR_EXT.1

予見される監査対象事象はない。

管理：FPT_PWR_EXT.2

予見される管理アクティビティはない。

監査：FPT_PWR_EXT.2
FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである：

- 異なる省電力状態への TSF の遷移

FPT_PWR_EXT.1 省電力状態 (訳注：原本の「認証要素取得」は誤り。)

下位階層： なし

依存性： なし

FPT_PWR_EXT.1.1 TSF は、以下の適合省電力状態を定義しなければならない(shall)：[選択：少なくとも 1 つ選択： S3, S4, G2(S5), G3, D0, D1, D2, D3 [*割付：ほかの省電力状態*]]。

FPT_PWR_EXT.2 省電力状態のタイミング(訳注：原本の「認証要素取得」は誤り。)

下位階層： なし

依存性： FPT_PWR_EXT.1 省電力状態

FPT_PWR_EXT.2.1 FPT_PWR_EXT.1.1 で定義された各省電力状態について、TSF は、以下の条件が発生したときに適合省電力状態へ入らなければならない(shall)：利用者起動の要求、[選択：以下から少なくとも 1 つ選択：システムシャットダウン、

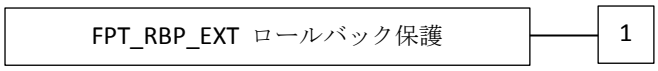
利用者の非活動状態、リモート管理システムにより起動された要求、[*割付：その他の条件*]、その他の条件なし]。

FPT_RBP_EXT ロールバック保護

ファミリのふるまい

本ファミリは、TSF がファームウェアのロールバックまたはダウングレードに対して保護することを要求する。

コンポーネントのレベル付け



FPT_RBP_EXT.1、ロールバック保護は、TSF が許可されないロールバックを検知し防止することを要求する。

管理： FPT_RBP_EXT.1 (訳注：原本の FPT_KYP_EXT.1 は誤り)

特定の管理機能は識別されていない。

監査： FPT_ RBP_EXT.1 (訳注：原本の FPT_KYP_EXT.1 は誤り)

予見される監査対象事象はない。

FPT_RBP_EXT.1 ロールバック保護

下位階層： なし

依存性： なし

FPT_RBP_EXT.1.1 TSF は、新しいファームウェアパッケージが[*割付：セキュリティバージョン番号が現在インストールされているバージョンと同じか、より高いものであることを検証する方法*]により、より低いセキュリティバージョン番号へダウングレードしていないことを検証しなければならない(shall)。

FPT_RBP_EXT.1.2 TSF は、試行されたファームウェアアップデートパッケージが無効なバージョンとして検出される場合、エラーコードを生成し、応答しなければならない(shall)。

FPT_TST_EXT TSF 自己テスト

ファミリのふるまい

本ファミリのコンポーネントは、選択された正しい動作のために TSF の自己テストについての要件に対処する。

コンポーネントのレベル付け

FPT_TST_EXT.1 拡張： TSF テストは、TSF の正しい動作を実証するため、初期起動中に一連の自己テストを要求する。

管理： FPT_TST_EXT.1

特定の管理機能は識別されていない。

監査： FPT_TST_EXT.1

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである：

- TSF 自己テストが完了したことの表示

FPT_TST_EXT.1 拡張：TSF テスト

下位階層：なし。

依存性：なし。

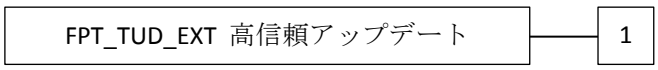
FPT_TST_EXT.1.1 TSF は、TSF の正常動作を実証するために、[選択：初期立ち上げ中 (電源オン時)、通常運用中定期的に、許可利用者の要求時に、条件[*割付：自己テストが作動すべき条件*]において] 以下の自己テストのスイートを実行しなければならない：[*割付：TSF によって実行される自己テストのリスト*]。

FPT_TUD_EXT 高信頼アップデート

ファミリのふるまい

本ファミリのコンポーネントは、TOE ファームウェア及び／またはソフトウェアをアップデートするための要件に対処する。

コンポーネントのレベル付け



FPT_TUD_EXT.1　高信頼アップデートは、インストール前にアップデートウィ検証する機能を含め TOE ファームウェア及びソフトウェアをアップデートするために提供される機能を要求する。

管理： FPT_TUD_EXT.1

以下のアクションは FMT における管理機能と考えられる：

a) TOE をアップデートする能力及びアップデートを検証する能力

監査： FPT_TUD_EXT.1

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである：

a) アップデートプロセスの開始
b) アップデートの完全性検証の失敗

FPT_TUD_EXT.1 高信頼アップデート

下位階層：　なし

依存性：　FCS_COP.1(a) 暗号操作 (署名検証)、
FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム)

FPT_TUD_EXT.1.1　TSF は、TOE ソフトウェア／ファームウェアの現在のバージョンを問い合わせる能力を[*割付：サブジェクトのリスト*]に提供しなければならない(shall)。

FPT_TUD_EXT.1.2　TSF は、TOE ソフトウェア／ファームウェアへのアップデートを開始する能力を[*割付：サブジェクトのリスト*]に提供しなければならない(shall)。

FPT_TUD_EXT.1.3　TSF は、TOE ソフトウェア／ファームウェアへのアップデートを製造者による[選択：ディジタル署名、公開ハッシュ]を用いて、それらのアップデートをインストールする前に検証しなければならない(shall)。

附属書 D: エントロピーに関する証拠資料及び評定

これは、cPP におけるオプションの附属書であり、TOE が乱数ビット生成器を提供する場合にのみ適用される。

本附属書では、TOE によって利用される各エントロピー源に関して要求される補足情報について記述している。

エントロピー源に関する証拠資料は、それを読んだ後で、評価者が完全にエントロピー源を理解し、それが十分にエントロピーを供給すると信頼できる理由を完全に理解できるように、十分に詳細であるべきである。本証拠資料には、設計記述、エントロピーの正当化、運用条件及びヘルステストという、複数の詳細なセクションが含まれるべきである。本証拠資料は、公開が予定される ST の TSS の一部である必要はない。

D.1 設計記述

証拠資料には、すべてのエントロピー源コンポーネントの相互作用を含め、各エントロピー源の全体的な設計が含まれなければならない。製品に含まれるサードパーティのエントロピー源についても、設計に関して共有可能なあらゆる情報が含まれなければならない。

証拠資料には、どのようにエントロピーが作り出されるのか、及びテスト目的で未処理(生の)データをエントロピー源の内部からどのように取り出せるかを含め、エントロピー源の運用が記述されること。その証拠資料では、エントロピー源の設計の概略説明(ウォークスルー)が行われ、エントロピーがどこに由来し、次にどこへエントロピー出力が渡されるのか、生の出力に対するあらゆる後処理(ハッシュ、XOR 等)、それが保存される場合／どこに保存されるのか、そして最後に、どのようにしてエントロピー源から出力されるのかを示すべきである。処理に課されるあらゆる条件(例えば、ブロッキング等)があれば、それについてもエントロピー源の設計の中で記述されるべきである。図や例を利用することが推奨される。

この設計には、エントロピー源のセキュリティ境界の内容の記述、及び境界外部の敵対者がエントロピー量に影響を与えることができないことをセキュリティ境界がどのように保証するかについての記述が、含まれなければならない。

サードパーティのアプリケーションが RBG へエントロピーを追加できる方法が実装されている場合、設計記述にはその記述が含まれなければならない。電源オフから電源オンまでの間に保存される RBG 状態があれば、その記述が含まれなければならない。

D.2 エントロピー正当化

エントロピー源の予測不可能性がどこに由来し、(この特定の TOE による)RBG 出力の作成に使用するのに十分なエントロピーをエントロピー源が供給できることを確信できる理由についての技術的な論証が存在すべきである。この論証には、期待さ

れる最小エントロピー率(即ち、情報源データの 1 ビットまたは 1 バイト当たりの最小エントロピー(ビット単位))の記述、及び十分なエントロピーが TOE の攪拌シード生成プロセスへ投入されることを説明する記述を含むこと。この説明は、エントロピー源がエントロピーを含むビットを生成すると確信できる理由の正当化の一部となる。

期待される最小エントロピー率を正当化するために必要な情報量は、製品に含まれるエントロピー源の種別に依存する。

開発者が提供するエントロピー源について、最小エントロピー率を正当化するため、大量の生の情報源ビットが収集され、統計学的なテストが実行され、統計学的なテストから最小エントロピー率が決定されることが期待される。現時点では、特定の統計学的なテストは要求されないが、各出力における最小エントロピーの量を決定するために何らかのテストが必要であることが想定される。

サードパーティによって提供されるエントロピー源について、TOE ベンダは、エントロピー源の設計及び生のエントロピーデータへのアクセスが制限されるため、証拠資料にはこのサードパーティから取得された最小エントロピー率の見積りが示されること。ベンダが最小エントロピー率を「想定」することは受け入れ可能だが、この想定は提供される証拠資料に明確に記述されなければならない。特に最小エントロピーの見積りは特定されなければならず、その前提条件は ST に含まれなければならない。

エントロピー源の種別にかかわらず、正当化は、ST に記述されるエントロピーを用いて DRBG が初期化される方法が含まれること。例えば、最小エントロピー率が DRBG へシード値を供給するために使用される情報源のデータ量に乗算されること、または情報源のデータ量に基づき期待されるエントロピー率が明示的に記述され、統計学的な率と比較されることを検証することによって行われる。DRBG へシード値を供給するために使用される情報源のデータ量が明確でない場合、または計算された率が明示的にシード値と関連付けられていない場合、証拠資料は完結したとは考えられない。

エントロピー正当化には、サードパーティのアプリケーションからの追加データも、再起動までの間に保存している任意の状態からの追加データも一切含まれてはならない。

D.3 運用条件

エントロピー率は、エントロピー源それ自体が制御できない条件によって影響を受けることがある。例えば、電源電圧、周波数、温度、及び電源投入後の経過時間等は、エントロピー源の運用に影響し得る要因のほんの数例である。このように、証拠資料には、エントロピー源が乱数データを生成すると期待される動作条件の範囲も含まれることになる。同様に、証拠資料には、エントロピー源がもはや十分なエントロピーを供給すると保証できないようになる条件についても記述されなければ

ならない。エントロピー源の故障または機能低下を検出するための方法が含まれなければならない。

D.4 ヘルステスト

さらに具体的には、すべてのエントロピー源ヘルステスト及びそれらの根拠が、文書化されること。これには、ヘルステストの記述、各ヘルステストが実行される頻度や条件(例えば、起動時、連続的、または要求に応じて)、各ヘルステストでの期待される結果、エントロピー源の故障時におけるTOEのふるまい、及び各テストがエントロピー源において1つ以上の故障を検知するために適切であると信じられる理由を示す根拠が含まれること。

B. 附属書 E: 鍵管理記述

製品の暗号鍵管理の証拠資料は十分詳細であるべきで、読んだ後で評価者が十分に製品の鍵管理について、鍵が適切に保護されていることを保証するための要件をどのように満たすかを理解できるようにするべきである。本文書には、解説と図を含むべきである。本証拠資料は、TSS の一部とすることは要求されず ー 別文書として提出され、開発者の保護情報として表示することができる。

以下のトピックは、すべてに製品に適用される訳ではなく、なぜ詳細が適用されないかの注釈が含まれる。

解説（エッセイ）：

解説は、鍵チェインにおけるすべての鍵について、以下の情報を提供する：

- 鍵の目的
- 鍵が不揮発性メモリに保存されるかどうか
- いつ、どのように鍵が保護されるか
- いつ、どのように鍵が導出されるか
- 鍵の強度
- いつ鍵がもはや不要とされるか、鍵が不要とされるかどうか、正当化と共に

解説は、以下のトピックについても記述する：

- どのような値が検証で使用されるか、検証を実行するために使用されるプロセスに注目して、検証プロセスが記述されなければならない。鍵チェインにおける鍵がこのプロセスにより弱体化または暴露されないことをこのプロセスがどのように保証するかについて記述しなければならない。連続する許可試行の失敗回数を制限するための方法について記述しなければならない。
- DEK の最終出力へ導く許可プロセス。このセクションは、製品によって使用される鍵チェインについての詳述しなければならない。どの鍵が DEK の保護に使用されるか、それらが導出または鍵ラッピングをどのように満たすかについて、記述しなければならない。その鍵チェインへ追加される値または鍵チェインと相互作用する値、及びそれらの値が鍵チェインの全体的な強度を弱体化または暴露させないことを保証するような保護についても含まれなければならない。
- 図や解説は、暗号技術的な総当り攻撃または BEV の知識なしにチェインが破られることがないこと、及び DEK の有効強度が鍵チェインの全般にわたり維持されていることを保証するために、鍵階層を明確に図示し、説明すること。
- データ暗号化エンジンの記述、そのコンポーネント、及びその実装の詳細（例、ハードウェアについて：デバイスの主たる SOC または別チップのコプロセッサに集積されたもの、ソフトウェアについて：製品の初期化、ドライバ、ライブラリ（適用可能な場合）、暗号化／復号のための論理インタフェ

ース、及び暗号化されない領域（例、ブートローダ、マスターブートレコード（MBR）と関連する部分、パーティションテーブル等））。記述は、デバイスのホストインタフェースから、データを保存しているデバイスの永続的なメディアへのデータフロー、データ暗号化エンジンを迂回するようなデータについての条件に関する情報（例、暗号化されていないマスターブートレコード(MBR)領域への読み出し-書き込み動作）についても含めるべきである。記述には、利用者が暗号化を有効化するときに製品がすべてのハードストレージデバイスを暗号化することを保証するため、すべてのプラットフォームを検証するために十分に詳細であるべきである。また、プラットフォームのブート初期化、暗号化の初期化プロセス、及びどの時期に製品が暗号化を有効化するかについても記述するべきである。

- すべての鍵の格納場所の種別及びそのストレージ用の破棄方法を含めて、鍵がもはや不要となったときに鍵を破棄するためのプロセス。

図：

- 図は、BEV から DEK までのすべての鍵、及びチェインへ寄与する任意の鍵または値を含めること。各鍵の暗号強度を列挙し、チェインに沿って各鍵が鍵導出または鍵ラッピング（許容されるオプションから）のいずれかで、どのように保護されるかについても図示しなければならない。図は、チェインにおいてそれぞれの鍵を導出またはラッピングを解くために使用される入力を示すべきである。
- 主なコンポーネント(メモリやプロセッサのような)及びそれらの間のデータ経路を示すような機能（ブロック）図、ハードウェアについては、デバイスのホストインタフェース及びデバイスのデータ保存用の永続的メディア、またはソフトウェアについては、利用者または管理者が最初に製品を設定する際にストレージデバイス全体を暗号化することを保証するために TOE が実行するアクティビティが必要とする初期ステップ。ハードウェア暗号化の説明図は、データ経路の中にデータ暗号化エンジンの場所を示さなければならない。
- ハードウェア暗号化の説明図は、データ経路の中にデータ暗号化エンジンの場所を示さなければならない。評価者は、ハードウェア暗号化の説明図にデータ経路の主なコンポーネントが十分詳細に示されていること、それがデータ暗号化エンジンを明確に識別していることを検証しなければならない。

C. 附属書 F: 用語集

用語	意味
Authorization Factor(許可要素)	利用者が知っている値(例、パスワード、トークン等)で、ハードディスクを使用するために許可されたコミュニティの中の利用者がいて、BEV の導出または復号、そして最終的には DEK の復号において使用されることを確立するために TOE へ送信されるもの。これらの値は、利用者固有の識別を確立するために使用されてもよいし、または使用されなくてもよいことに注意すること。
Assurance(保証)	TOE が SFR を満たしていることを信頼する根拠 [CC1].
Border Encryption Value(境界暗号化値：BEV)	AA から EE へ渡される値で、２つのコンポーネントの鍵チェインを繋ぐことを意図したもの。
Key Sanitization(鍵サニタイズ)	データを暗号化した鍵をセキュアに上書きすることで暗号化データをサニタイズする方法。
Data Encryption Key (DEK)	保存データを暗号化するために使用された鍵。
Full Drive Encryption(ドライブ全体暗号化)	利用者がアクセスできるデータの論理ブロックのパーティションへの参照で、これらのパーティションのブロックへデータの読み出しまたは書き込みのための権限を写像するオペレーティングシステムのようなホストシステムによって インデックス、パーティションが管理されたもの。 本 SPD 及び cPP のために、FDE はひとつのパーティションの暗号化と権限管理を実行する。OS 及びファイルシステムによる定義及びサポートについては検討中である。 FDE 製品はストレージデバイスのパーティション上のすべてのデータ(特定の例外はある)を暗号化し、FDE ソリューションへの権限付与が成功した後にデータへのアクセスを許可する。例外として、マスターブートレコード(MBR)またはその他の AA/EE 事前認証ソフトウェアとして暗号化されないようなストレージデバイスの一部(サイズは実装に依存して変わるかもしれない)が含まれる。これらの FDE cPP は「ドライブ全体暗号化」という用語を、保護されないデータが含まれていないとして暗号化されていないストレージデバイスの部分を残してはいるが FDE ソリューションを許容するように解釈する。
Intermediate Key(中間鍵)	初期の利用者権限付与と DEK の間で使用される鍵。
Host Platform(ホストプラットフォーム)	TOE が実行しているローカルのハードウェア及びソフトウェアで、ローカルのハードウェア及びソフトウェアに接続されうる周辺のデバイス(USB デバイス等)を含まないもの。
Key Chaining (鍵チェイン)	データを保護するために複数階層の暗号鍵を使用する方法。最上位層の鍵はデータを暗号化する下位の鍵を暗号化する；この方法は何階層でもよい。
Key Encryption Key (鍵暗号化鍵：KEK)	DEK または鍵を含むストレージのような、その他の暗号鍵を暗号化するために使用された鍵。
Key Material(鍵材料)	鍵材料は、重要セキュリティパラメタ(CSP)として知られ、認証データ、ノンス、メタデータも含まれる。

用語	意味
Key Release Key (KRK) (鍵解放鍵)	ストレージから別の鍵をリリースするために使用される鍵で、別の鍵の直接導出または復号には使用されない。
Operating System (OS) (オペレーティングシステム、基本システム)	最高の特権レベルで動作するソフトウェアで、直接ハードウェア資源を制御できるもの。
Non-Volatile Memory (不揮発性メモリ)	電源なしで情報を保持するコンピュータメモリの一種。
Powered-Off State (電源オフ状態)	デバイスがシャットダウンしている状態。
Protected Data (保護されたデータ)	これはストレージデバイス上のすべてのデータへの参照で。TOE として正常に機能することが要求される小さな部分を除いたもの。OS,アプリケーション、利用者データを含め、利用者がデータを書き込みできるディスク上のすべての空間。保護されたデータは、暗号化されない必要のあるマスターブートレコードまたはドライブの事前認証領域を含まない。
Submask（サブマスク）	サブマスクは、いくつかの方法で生成され、保存されるビット列である。
Target of Evaluation (評価対象)	ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び／またはハードウェアのセット。[CC1]

その他のコモンクライテリア略語や用語については、 [CC1]を参照されたい。

D.附属書 G: 頭字語

頭字語	意味
AA	Authorization Acquisition (許可取得)
AES	Advanced Encryption Standard(高度暗号規格)
BEV	Border Encryption Value(境界暗号化値)
BIOS	Basic Input Output System(基本入出力システム：バイオス)
CBC	Cipher Block Chaining(暗号ブロックチェイニング)
CC	Common Criteria(コモンクライテリア)
CCM	Counter with CBC-Message Authentication Code(CBC メッセージ認証コード付きカウンタ)
CEM	Common Evaluation Methodology (共通評価方法)
CPP	Collaborative Protection Profile(コラボラティブプロテクションプロファイル)
DEK	Data Encryption Key(データ暗号化鍵)
DRBG	Deterministic Random Bit Generator(決定論的乱数ビット生成器)
DSS	Digital Signature Standard (ディジタル署名規格)
ECC	Elliptic Curve Cryptography (楕円曲線暗号)
ECDSA	Elliptic Curve Digital Signature Algorithm(楕円曲線ディジタル署名アルゴリズム)
EE	Encryption Engine(暗号エンジン)
EEPROM	Electrically Erasable Programmable Read-Only Memory (電気的消去可能プログラマブル ROM)
FIPS	Federal Information Processing Standards(連邦情報処理規格)
FDE	Full Drive Encryption(ドライブ全体暗号化)
FFC	Finite Field Cryptography(有限体暗号)
GCM	Galois Counter Mode(ガロアカウンターモード)
HMAC	Keyed-Hash Message Authentication Code(鍵付ハッシュメッセージ認証コード)
IEEE	Institute of Electrical and Electronics Engineers(アメリカ電気電子通信学会)
IT	Information Technology(情報技術)
ITSEF	IT Security Evaluation Facility(IT セキュリティ評価機関)
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission (国際標準化機構／国際電気標準会議)
IV	Initialization Vector(初期化ベクタ)
KEK	Key Encryption Key(鍵暗号化鍵)
KMD	Key Management Description(鍵管理記述)
KRK	Key Release Key(鍵解放鍵)
MBR	Master Boot Record(マスターブートレコード)
NIST	National Institute of Standards and Technology(アメリカ国立標準技術研究所)
OS	Operating System(オペレーティングシステム、基本システム)
RBG	Random Bit Generator(乱数ビット生成器)
RNG	Random Number Generator(乱数生成器)
RSA	Rivest Shamir Adleman Algorithm(リベスト・シャミア・エーデルマン(RSA)アルゴリズム)
SAR	Security Assurance Requirement(セキュリティ保証要件)
SED	Self Encrypting Drive(自己暗号化ドライブ)
SHA	Secure Hash Algorithm(セキュアハッシュアルゴリズム)
SFR	Security Functional Requirement(セキュリティ機能要件)
SPD	Security Problem Definition(セキュリティ課題定義)

SPI	Serial Peripheral Interface(シリアルペリフェラルインタフェース)
ST	Security Target(セキュリティターゲット)
TOE	Target of Evaluation(評価対象)
TPM	Trusted Platform Module(高信頼プラットフォームモジュール)
TSF	TOE Security Functionality(TOE セキュリティ機能)
TSS	TOE Summary Specification(TOE 要約仕様)
USB	Universal Serial Bus(ユニバーサルシリアルバス)
XOR	Exclusive or(排他的論理和)
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

E. 附属書 H: 参照文書

National Institute of Standards and Technology (NIST) Special Publication 800-38F, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, National Institute of Standards and Technology, December 2012.

National Institute of Standards and Technology (NIST) Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, National Institute of Standards and Technology, August 2009.

National Institute of Standards and Technology (NIST) Special Publication 800-88 Revision 1, Guidelines for Media Sanitization, National Institute of Standards and Technology, December 2014.

National Institute of Standards and Technology (NIST) Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, National Institute of Standards and Technology, January 2012.

National Institute of Standards and Technology (NIST) Special Publication 800-132, Recommendation for Password-Based Key Derivation Part 1: Storage Applications, National Institute of Standards and Technology, December 2010.

Federal Information Processing Standard Publication (FIPS-PUB) 186-4, Digital Signature Standard (DSS), National Institute of Standards and Technology, July 2013.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 9796-2:2010 (3rd edition), Information technology — Security techniques — Digital signature schemes giving message recovery, International Organization for Standardization/International Electrotechnical Commission, 2010.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 9797-2:2011 (2nd edition), Information technology — Security techniques — Message Authentication Codes (MACs) – Part 2: Mechanisms using a dedicated hash-function, International Organization for Standardization/International Electrotechnical Commission, 2011.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 10116:2006 (3rd edition), Information technology — Security techniques — Modes of operation for an n-bit block cipher, International Organization for Standardization/International Electrotechnical Commission, 2006.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 10118-3:2004 (3rd edition), Information technology — Security techniques — Hash-functions – Part 3: Dedicated hash-functions, International Organization for Standardization/International Electrotechnical Commission, 2004.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 14888-3:2006 (2nd edition), Information technology — Security techniques —Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms,

International Organization for Standardization/International Electrotechnical Commission, 2006.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18031:2011 (2nd edition), Information technology — Security techniques — Random bit generation, International Organization for Standardization/International Electrotechnical Commission, 2011.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 18033-3:2011 (3rd edition), Information technology — Security techniques — Encryption algorithms – Part 3: Block ciphers, International Organization for Standardization/International Electrotechnical Commission, 2011.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19772:2009, Information technology — Security techniques Authenticated encryption, International Organization for Standardization/International Electrotechnical Commission, 2009.