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許可取得

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 - 許可取得 (訳注：原文は Authorization Acquisition, AA)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施するアクションを規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：許可取得 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) 構成要素と暗号エンジン (訳注：原文は Encryption Engine, EE) 構成要素の両方を要求する。製品は全体のソリューション及び本 cPP 及び FDE-EE 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 (評価認証制度) 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構成要素 (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、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] 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 (評価認証制度関係者) 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 – EE] 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– 暗号エンジン、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：許可取得、2016 年 9 月

[1] 詳細については、http://www.commoncriteriaportal.org/ を参照。

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 22 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を取り込む、また鍵破棄セクションと AVA_VAN を更新

目次

謝辞 2
0. 序文 3
0.1 本書の目的 3
0.2 本書の適用範囲 3
0.3 想定される読者層 3
0.4 関連する文書 4
プロテクションプロファイル 4
コモンクライテリア 4
0.5 改訂履歴 5
1. PP 序説 10
1.1 PP 参照識別 10
1.2 FDE コラボラティブ PP (cPPs) の取組みへの序説 10
1.3 実装 11
1.4 評価対象 (TOE)の概要 11
1.4.1 許可取得への序説 12
1.4.2 許可取得のセキュリティ機能 13
1.4.3 インタフェース／境界 13
1.5 TOE 及び運用／Pre-Boot 環境 13
1.6 TOE 適用例 14
2. CC 適合主張 15
3. セキュリティ課題定義 16
3.1 脅威 16
3.2 前提条件 19
3.3 組織のセキュリティ方針 21
4. セキュリティ対策方針 22
4.1 運用環境のセキュリティ対策方針 22
5. セキュリティ機能要件 24
5.1 表記法 24
5.2 SFR アーキテクチャ 25
5.3 クラス：暗号サポート (FCS) 25
FCS_AFA_EXT.1 許可要素取得 25
FCS_AFA_EXT.2 許可要素取得のタイミング 26
FCS_CKM.4(a) 暗号鍵破棄（電力管理） 26
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) 26
FCS_CKM_EXT.4(a) 暗号鍵及び鍵材料破棄 (破棄のタイミング) 27
FCS_CKM_EXT.4(b) 暗号鍵及び鍵材料破棄（電力管理） 27
FCS_KYC_EXT.1 鍵チェイニング(イニシエータ) 28
FCS_SNI_EXT.1 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成) 29
5.4 クラス：セキュリティ管理(FMT) 30
FMT_MOF.1 セキュリティ機能のふるまいの管理 30
FMT_SMF.1 管理機能の特定 30
5.5 クラス： TSF の保護 (FPT) 31
FPT_KYP_EXT.1 鍵及び鍵材料の保護 31
FPT_PWR_EXT.1 省電力状態 31
FPT_PWR_EXT.2 省電力状態のタイミング 31
FPT_TUD_EXT.1 高信頼アップデート 32
6. セキュリティ保証要件 33
6.1 ASE：セキュリティターゲット評価 33

6.2 ADV：開発 34
6.2.1 基本機能仕様 (ADV_FSP.1) 34
6.3 AGD：ガイダンス証拠資料 34
6.3.1 利用者操作ガイダンス (AGD_OPE.1) 35
6.3.2 準備手続 (AGD_PRE.1) 35
6.4 クラス ALC：ライフサイクルサポート 35
6.4.1 TOE のラベル付け (ALC_CMC.1) 35
6.4.2 TOE の CM 範囲 (ALC_CMS.1) 35
6.5 クラス ATE：テスト 35
6.5.1 独立テスト– 適合 (ATE_IND.1) 36
6.6 クラス AVA：脆弱性評定 36
6.6.1 脆弱性調査 (AVA_VAN.1) 36
附属書 A：オプション要件 37
A.1 内部の暗号実装 37
A.2 TSF 自己テスト 37
FPT_TST_EXT.1 TSF テスト 38
附属書 B：選択ベース要件 39
B.1 クラス：暗号操作 (FCS) 39
FCS_CKM.1(a) 暗号鍵生成 (非対称鍵) 39
FCS_CKM.1(b) 暗号鍵生成 (対称鍵) 40
FCS_COP.1(a) 暗号操作 (署名検証) 40
FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム) 40
FCS_COP.1(c) 暗号操作 (鍵付ハッシュアルゴリズム) 41
FCS_COP.1(d) 暗号操作 (鍵ラッピング) 41
FCS_COP.1(e) 暗号操作 (鍵配送) 41
FCS_COP.1(f) 暗号操作 (AES データ暗号化／復号) 41
FCS_COP.1(g) 暗号操作 (鍵暗号化) 42
FCS_KDF_EXT.1 暗号鍵の導出 42
FCS_PCC_EXT.1 暗号パスワードの生成と調整 42
FCS_RBG_EXT.1 暗号操作 (乱数ビット生成) 43
FCS_SMC_EXT.1 サブマスクコンバイニング 43
FCS_VAL_EXT.1 検証 44
附属書 C：拡張コンポーネント定義 45
C.1 背景と適用範囲 45
C.2 拡張コンポーネント定義 45
FCS_AFA_EXT 許可要素取得 45
FCS_CKM_EXT 暗号鍵管理 47
FCS_KDF_EXT 暗号鍵導出 48
FCS_KYC_EXT 鍵チェイニング 49
FCS_PCC_EXT 暗号パスワードの生成と調整 51
FCS_RBG_EXT 乱数ビット生成 52
FCS_SMC_EXT サブマスクコンバイニング 53
FCS_SNI_EXT 暗号操作 (ソルト、ノンス、及び初期化ベクタの生成 54
FCS_VAL_EXT 暗号エレメントの検証 55
FPT_KYP_EXT 鍵及び鍵材料の保護 56
FPT_PWR_EXT 電力管理 59
FPT_TST_EXT TSF テスト 60
FPT_TUD_EXT 高信頼アップデート 61
附属書 D：エントロピー証拠資料及び評定 62
D.1 設計記述 62
D.2 エントロピーの正当化 62

D.3 動作条件 63
D.4 ヘルステスト 64
附属書 E：鍵管理記述 65
附属書 F：用語集 67
附属書 G：頭字語 69
附属書 H：参照文書 71

図 / 表

表 1：cPP 実装の例 11
表 2：TOE セキュリティ機能要件 25
表 3：TOE セキュリティ保証要件 33
表 4：拡張コンポーネント 45

図 1：FDE 構成要素の詳細 10
図 2：許可取得の詳細 12
図 3：運用環境 14

1. PP 序説

1.1 PP 参照識別

PP 参照：collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition (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)

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最初のセットの目的は、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形状要素は、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、外部媒体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 認証前のソフトウェアのようなものについて、非暗号化のストレージデバイスの部分を残す必要性がある。これらの FDE cPP は、用語「ドライブ全体暗号化」について、ストレージデバイスの暗号化されない部分、平文の利用者データまたは認証用データを含むような部分が残る FDE ソリューションを許容すると解釈する。

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 構成要素についての要件を記述している。

図 1：FDE 構成要素の詳細

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コアな要件についても記述している。

本 TOE 記述は、許可取得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 AA 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。

従って、ベンダは、ドライブ全体暗号化ソリューション(AA と EE) の両方の構成要素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 (訳注：ベンダは、「評価を行う」のではなく「評価を受ける」が正しい) ーこれは、1 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構成要素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、1 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 (許可取得：AA) の評価対象は、HW 暗号エンジン(SED 等) を管理するホストソフトウェア、または両方の構成要素を含むソリューションを提供するようなベンダのための本 cPP と暗号エンジン cPP を組み合わせた評価の一部として、のいずれかであるだろう。

以下のセクションは、セキュリティ機能と同様に FDE AA の機能の概要を提供する。

1.4.1 許可取得への序説

許可取得は、鍵暗号化鍵(KEK：Key Encryption Key)、鍵出力鍵(KRK：Key Releasing Key)、暗号エンジンのその他の種類の鍵であるような境界暗号化値(BEV)を送信する。EE は、これらの値を DEK を復号または出力するための鍵として直接使用してはならない。DEK を最終的に保護するためのその他の中間鍵を使用する方式の一部としてこれを使用してもよい。KEK は、他の鍵、とりわけ DEK または DEK にチェインするようなその他の中間鍵をラップする。鍵出力鍵(KRK) は、EE が DEK または DEK にチェインするようなその他の中間鍵を出力することを許可する。図２では、AA に含まれる構成要素及び EE との関係について説明する。

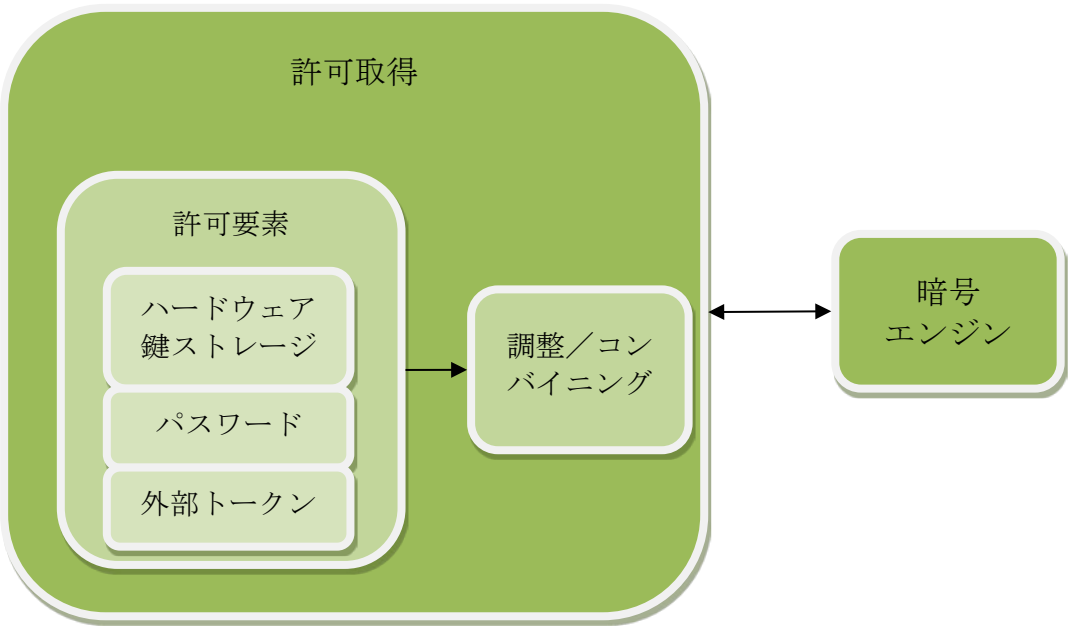


図２：許可取得の詳細

許可要素(Authorization factor) は、個別の利用者に対して一意であり、個別のグループによって使用されてもよい。言い換えれば、EE は、許可要素の所有者がストレージデバイス上に格納された情報をアクセスするために許可された利用者のコミュニティに属していることを確立するために AA からの許可要素を要求する(また、特定の利用者許可を要求しない)。 許可要素の例として、パスワード、パスフレーズ、または USB トークンに格納されたランダムに生成された値 またはトラステッドプラットフォームモジュール(TPM) 等のハードウェアストレージ媒体上の鍵を出力するための PIN が含まれるが、これらに限定されない。

1.4.2 許可取得のセキュリティ機能

AA は、ストレージデバイス上のデータをアクセスするために EE が利用する許可要素を収集し、さまざまな管理機能を実行する。許可要素の種別に依存して AA は、それらをさらに調整することができる。例えば、パスワードに関しては、承認されたパスワードベースの鍵導出関数（例、PBKDF2）が適用できる。十分な強度をを持つランダムに生成された値を持つ外部トークンは許可要素に関してさらなる調整を要求しないだろう。AA は、その際、一つ以上の許可要素を、双方の要素の強度を維持するような方法で結合するだろう。

AA は、EE への主たる管理インタフェースとして機能する。しかし、EE は管理機能を提供してもよい。EE cPP における要件は EE がこれらの機能をどのように取り扱うべきかについて対処する。管理機能は、例えば、DEK の変更、新規利用者の設定、KEK 及びその他の中間鍵の管理、及び鍵の廃棄処理の実行(例、DEK の上書き)のような EE へのコマンドを送信する能力を含んでもよい。また、複数の利用者によって使用するためにドライブを分割するコマンドを送信してもよい。しかし、本文書は、分割の管理については、保留とし、管理者及び利用者のみは全ドライブ上のデータを設定し管理することを前提とする。

1.4.3 インタフェース／境界

AA と EE の間のインタフェースと境界は、実装に基づき変化する。あるベンダが FDE 全体のソリューションを提供する場合、AA と EE 構成要素の間のインタフェースを実装しないように選択してもよい。あるベンダが構成要素の一つについてのソリューションを提供する場合、以下の前提条件は、２つの構成要素の間チャネルが十分セキュアな状態であると記述している。AA と EE 構成要素の間のインタフェースに関して規格と使用が存在するが、cPP は本バージョンにおいてベンダが規格に従うことを要求しない。

1.5 TOE 及び運用／Pre-Boot 環境

AA 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ステージに依存して異なるかもしれない、図 3 を参照。ソリューションのアーキテクチャに依存して、設定、初期化、許可の観点は、Pre-Boot 環境で実行されるかもしれないが、暗号化、復号、管理機能がオペレーティングシステム環境で実行されるかもしれない。非ソフトウェアソリューションにおいて、暗号／復号は Pre-OS 環境で開始し、OS の提供する環境へと続く。

オペレーティングシステム環境において、許可取得は、ハードウェアドライバ、暗号ライブラリ、及びおそらく TOE 以外のその他のサービスを含めて、オペレーティングシステム(OS) から利用可能なサービスのすべてが適用範囲となっている。

Pre-Boot 環境は、限定された機能にさらに一層制約されている。本環境は、最低限の周辺を起動させ、プラットフォームをコールドスタートから実行中のアプリケーションとともに十分に機能的なオペレーティングシステムの実行へと導くために必要なドライバのみをロードする。

AA の TOE は、運用環境の中の機能を含むか、または利用するかもしれない。

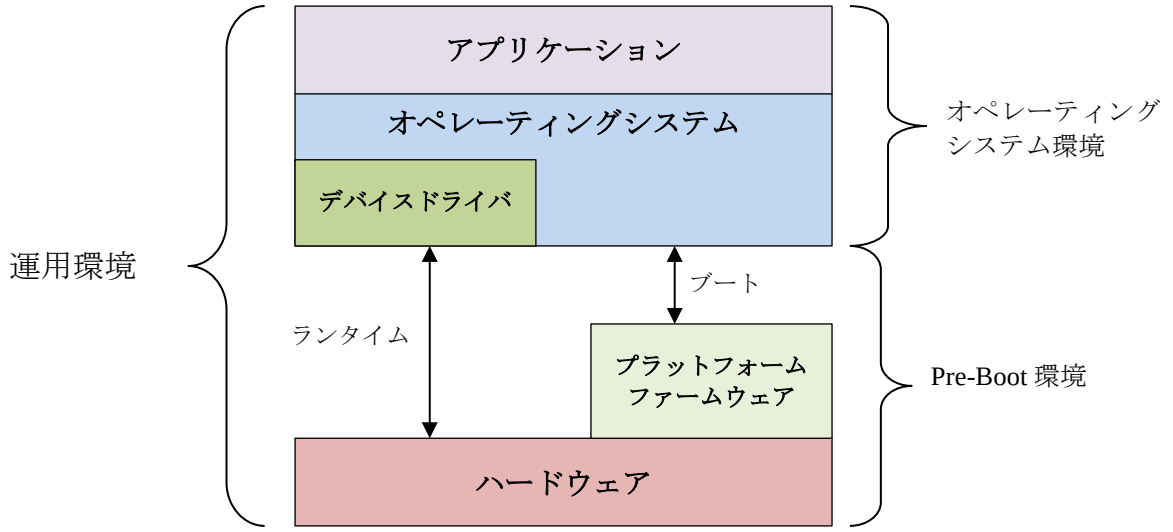


図3：運用環境

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切断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。敵対者が電源投入の状態でデバイスを取得し、環境または TOE 自体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、リリース 4 の要件に適合する。本 cPP は、CC v3.1 R4、CC パート 2 及び CC パート 3 に適合。拡張コンポーネント定義は、**拡張コンポーネント定義**に書かれている。

cPP 評価のため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す： 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 の要件すべてを含み、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 として定義されている。繰り返しは許容されているが、追加の要件 (CC パート 2 または 3 からのもの) を 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 の要件は、省略が許容されない。

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。要件は複数の脅威の側面を軽減するかもしれない。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。

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有者 (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有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。

[FCS_AFA_EXT.2, FMT_MOF.1, FMT_SMF.1, FPT_PWR_EXT.1, FPT_PWR_EXT.2, FCS_VAL_EXT.1, FPT_TST_EXT.1]

根拠：[FCS_AFA_EXT.2]は、適合する電力状態からの復帰に際して認証が再度入力されることを要求する。[FMT_MOF.1]は、適合する電力状態を改変する能力を管理者に制限する。[FPT_PWR_EXT.1]は、どの電力状態が TOE に適合するかを定義する。[FPT_PWR_EXT.2]は、TOE が適合する電力状態に入る条件を定義する。これらの要件は、適合する電力状態で紛失した場合に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 の変更及び消去の要求を含め、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[FPT_TST_EXT.1]の利用を通して検証される。[FCS_VAL_EXT.1]は、正しい認証を検証し、データを復号するための試行を制限する。

(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所有することは、不正な利用者が暗号を破ることを可能にし得る。cPP では、鍵材料の所有がデータそのものと同じ重要性を持つとみなす。脅威エージェントは、ストレージデバイスの非暗号化セクタ内、及び運用環境(OE)内の他の周辺機器、例、BIOS 設定、SPI フラッシュにおける鍵材料を探すかもしれない。

[FCS_AFA_EXT.1, FCS_AFA_EXT.2, FCS_CKM.4(a), FCS_CKM.4(b) , FCS_CKM_EXT.4(a), FCS_CKM_EXT.4(b), FCS_KYC_EXT.1, FMT_MOF.1, FMT_SMF.1, FPT_KYP_EXT.1, FCS_PWR_EXT.1, FCS_PWR_EXT.2, 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_PCC_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鍵材料は、両方ともが [FCS_RBG_EXT.1] を介して適切に生成されるような、[FCS_CKM.1(a) 及び (b)] によって生成される。一つ以上のサブマスク [FCS_AFA_EXT.1]が結合され[FCS_SMC_EXT.1]、及び／またはチェインされ[FCS_KYC_EXT.1]、BEV を生成する。鍵チェインは、以下を含めて、数種類の方法によって維持可能である：

- 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 が適切に生成され、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、認証要素の調整及び暗号機能がそれらの利用を要求することをサポートすること(対称鍵生成及びガロア／カウンターモード[GCM])を用いた AES 暗号化と復号、等)を保証する。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)]、及び鍵材料を伴う既知の値の復号[FCS_COP.1(f)]のような鍵材料の検証方法を定義する。鍵データは、ハッシュ関数を用いて実行することも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[FPT_TST_EXT.1]の利用を通して検証される。

FPT_KYP_EXT.1 は、ラップされていない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、適切な鍵材料破棄；平文の鍵及び鍵材料の暴露を最小限にすることを保証する。

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利用されることが可能ではないことの保証の基本的なものである。TSF は、さまざまな条件[FPT_PWR_EXT.1]によって入ったときすべての鍵材料を暗号化または破棄[FCS_CKM.4(b)、FCS_CKM_EXT.4]するような、適合省電力状態[FPT_PWR_EXT.2]を定義する。この材料は、有効な許可要素が提供される[FCS_AFA_EXT.2]まで、復号されない。FMT_MOF.1 は、適合する電力状態を改変する能力を管理者に制限する。

FMT_SMF.1 は、許可要素及び TSF が使用する省電力状態の生成と設定を含め TOE の重要な側面を管理するために必要な機能を TSF が提供することを保証する。

(T.AUTHORIZATION_GUESSING) 脅威エージェントは、パスワード及び PIN のような、許可要素を繰り返し推測するためのホストソフトウェアを試行するかもしれない。許可要素の推測に成功すると、TOE が BEV をリリースするか、さもなければ保護されたデータを許可されない利用者に開示するような状態にしてしまう事態が発生するかもしれない。

[FCS_AFA_EXT.1,FCS_SNI_EXT.1,FCS_PCC_EXT.1,FCS_SMC_EXT.1, FCS_VAL_EXT.1]

根拠：[FCS_VAL_EXT.1] は、DEK の鍵のサニタイズまたは設定可能な検証試行失敗回数が 24 時間以内に到達されたときのような、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。これにより、パスワード及び PIN のような許可要素に対する総当たり攻撃を軽減される。

[FCS_AFA_EXT.1] は、推測が困難であるような許可要素のセット、利用者提供の値を繰り返し推測するコストを増加させるために調整される[FCS_PCC_EXT.1]要素を利用者が提供することを要求する。[FCS_SNI_EXT.1]は、事前に計算された攻撃を防止するような適切なソルトを要求するFCS_SMC_EXT.1 は、さらに認証要素を推測の困難性を増加するような、複数要素の認証オプションを許容する。

(T.KEYSPACE_EXHAUST) 脅威エージェントは、鍵空間に対して暗号学的総当たりを実行するかもしれない。不適切に選択された暗号アルゴリズム及び／またはパラメタは、攻撃者が総当たりを通して鍵空間を調べ尽くし、データへのアクセスを得ることを許してしまう。

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

根拠：[FCS_CKM.1(a) 及び (b)] 及び [FCS_RBG_EXT.1] は、暗号鍵がランダムであり、総当たり試行が暗号学的に困難であり、コスト的な禁止となるような適切な強度／長さであることを保証する。[FCS_KYC_EXT.1] は、BEV を保護しているすべての鍵が、同じ強度であることを保証する。

(T.UNAUTHORIZED_UPDATE) 脅威エージェントは、TOEのセキュリティ機能を危殆化させ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、署名生成と検証アルゴリズム、及び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及び／またはファーム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、許可された利用者に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、アップデートを起動し、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提供する。 FCS_COP.1(a)は、アップデートを検証するために使用される署名機能を定義する。

FMT_SMF.1 は、TSFがシステムファームウェア／ソフトウェアアップデートの起動を含む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。

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(must)前提条件を以下に示す：

(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。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された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、ストレージデバイスのこのような領域からデータを復元するためのフォレンジックツールを使用する人がいるかもしれない。結果的に、cPP は、不良セクタ、非パーティション化された空間、及び暗号化されないコードを含むに違いない領域 (例、MBR 及び AA/EE 事前認証ソフトウェア) には、何ら保護データを含まないと想定する。

[OE.INITIAL_DRIVE_STATE]

(A.SECURE_STATE) 適切な設定の完了において、ドライブは電源切断状態において電源投入となってから初期の許可を受けるまでの間、セキュアであるとのみ想定される。

[OE.POWER_DOWN]

(A.TRUSTED_CHANNEL) 製品構成要素 (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、構成要素間の通信は 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.TRAINED_USER) 許可された利用者は、パスワード／パスフレーズ及びストレージデバイス及び／またはプラットフォームとは別にセキュアに格納された外部トークンを守ることを含め、利用者ガイダンスに従う。

[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、製品の正しい動作を妨げるようなマルウェアに感染していない。

[OE.PLATFORM_STATE]

(A.SINGLE_USE_ET) 許可要素を含んでいる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。

[OE.SINGLE_USE_ET]

(A.POWER_DOWN) 利用者は、電源切断の後にすべての揮発性メモリが消去されるまで、プラットフォーム及び／またはストレージデバイスから操作者がいない状態にせず、メモリ残存攻撃が実行不可能となるようにする。

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を放置しない (例、

ロックスクリーン)。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.PASSWORD_STRENGTH) 許可された管理者は、機微なデータが保護されていることを反映するため、パスワード／パスフレーズ許可要素が十分な強度とエントロピーを持っていることを保証する。

[OE.PASSPHRASE_STRENGTH]

(A.PLATFORM_I&A) 製品は、オペレーティングシステムログインのような通常のプラットフォーム識別と認証機能を妨げたり、または変更したりしない。オペレーティングシステムのログインインタフェースへ許可要素を提供してもよいが、実際のインタフェースの機能を変更したり、低下させたりしないこと。

[OE. PLATFORM_I&A]

(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と。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) プラットフォームは、その運用環境において物理的に保護されていると仮定され、セキュリティを侵害し、及び／またはそのプラットフォームの正しい運用を妨害するような物理的攻撃の対象ではないと仮定される。

[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) 製品の構成要素の間(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るべきである。[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 を危殆化しないか、または検知なしに危殆化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、電源切断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、電源を落とすまでストレージデバイスを放置したまま離れない、または「ハイバーネーションモード」のような管理された電源の状態に置くように、適切に訓練される[A.TRAINED_USER] 。A.POWER_DOWN は、デバイスが電源切断または「ハイバーネーションモード」状態ではこのようなメモリ残存攻撃が不可能であることを要求する。

(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ないようマルウェアには感染しない。

マルウェアに感染しないプラットフォーム[A.PLATFORM_STATE] は、製品の正しい動作を潜在的に妨げるような攻撃ベクトルを防止する。

(OE.PLATFORM_STATE) 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せつぞくされる) プラットフォームは、製品の正しい動作を妨げないようマルウェアには感染しない。

根拠：マルウェアに感染しないプラットフォーム[A.PLATFORM_STATE] は、製品の正しい動作を潜在的に妨げるような攻撃ベクトルを防止する。

(OE.PLATFORM_I&A) 運用環境は、TOE が使用する許可要素とは独立に動作する利用者識別と認証メカニズムを提供する。

根拠：製品が許可要素をオペレーティングシステムのログインインタフェースへ提供するかもしれないが、実際のインタフェースの機能を変更または低下させてはならない。A.PLATFORM_I&A は、製品が通常のプラットフォームの I&A 機能を妨げたり、変更したりしないことを要求する。

(OE.PHYSICAL) 運用環境は、敵対者がその環境または TOE 自身に対して改変が可能でないような、セキュアな物理的計算空間を提供する

根拠：セクション 1.6 で記述されるとおり、本 cPP の適用例は、敵対者が電源切断状態でそれを受け取って事前にアクセスできないような、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特定される。これらの SFR における選択に基づき、附属書 B の選択ベースの SFR のいくつかが含まれる必要もある。追加のオプション SFR についても、その運用環境の代わりに TOE により提供されるそれらの機能について、附属書 A に列挙されたものから適用されるかもしれない。

[SD] で定義された評価アクティビティは、評価者が特定の TOE の SFR への適合を決定するために取られるアクションについて記述している。これらの評価アクティビティの内容は、ゆえに、TOE 開発者からの必須の評価用提供物件へのより多くの洞察を提供する。

5.1 表記法

SFR の記述で使用される表記法は、以下のとおりである：

- 割付：*イタリック体*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_AFA_EXT.1 許可要素取得
	FCS_AFA_EXT.2 許可要素取得のタイミング
	FCS_CKM.4(a) 暗号鍵破棄 (電力管理)
	FCS_CKM.4(d) 暗号鍵破棄 (ソフトウェア TOE、サードパーティのストレージ)
	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) 暗号鍵破棄 (電力管理)
	FCS_KYC_EXT.1 鍵 チェイニング (イニシエータ)
	FCS_SNI_EXT.1 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成)
セキュリティ管理 (FMT)	FMT_MOF.1 機能のふるまいの管理
	FMT_SMF.1 管理機能の特定
TSF の保護 (FPT)	FPT_KYP_EXT.1 拡張：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_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_AFA_EXT.1 許可要素取得

FCS_AFA.EXT.1.1 TSF は、以下の許可要素を受け入れなければならない：[選択：

- FCS_PCC_EXT.1 で定義されたとおりに調整されたパスワード許可要素から導出されたサブマスク、
- スマートカード及び [選択：なし、運用環境が定義した PIN、設定可能な PIN] の提示によって証明された利用者の存在と共に、鍵長 [選択：2048 ビット、3072 ビット、4096 ビット] の RSA を用いて保護された、[選択：TOE により生成された(FCS_RBG_EXT.1 で規定された RBG を用いて)、ホストプラットフォームにより生成された] サブマスクを保護し、少なくとも DEK と同じビット長であるような、外部のスマートカードの要素、
- FCS_RBG_EXT.1 で特定されたとおり RBG を用いて、TOE により生成されるサブマスクを提供している、少なくとも BEV と同じセキュリティ強度である、外部の USB トークンの要素、
- ホストプラットフォームにより生成されるサブマスクを提供している、 少なくとも BEV と同じセキュリティ強度である、外部の USB トークンの要素

] 。

適用上の注釈：*本要件は、利用者からのどのような許可要素が TOE に受け入れられるかを規定している。利用者により入力されるパスワードは、FCS_PCC_EXT.1 で規定されるとおり、TOE が調整できなければならない許可要素の 1 つである。別の選択肢は、スマートカー*

ド許可要素であり、TOE の RBG またはプラットフォームの RBG のいずれかによって、値をどのように生成するかという点において差別化の特徴を持つものである。外部 USB トークンも、TOE またはプラットフォームの RBG のいずれかによって生成されるサブマスクの値を持つものとして使用してよい。

TOE は、許可要素をいくつでも受け入れることができ、「サブマスク」として分類される。ST 作成者は、サポートする許可要素を選択するが、複数の方法を選択してもよい。

複数の許可要素を使用するほうが望ましい；一つ以上の許可要素が使用される場合、生成されるサブマスクは附属書 A で規定された FCS_SMC_EXT.1 を用いてコンバイニング（combined）されなければならない。

FCS_AFA_EXT.2 許可要素取得のタイミング

FCS_AFA.EXT.2.1 TSF は、平文データへのアクセスを許可する前に、FPT_PWR_EXT.1 で規定される任意の適合省電力状態における FCS_AFA_EXT.1 で規定された許可要素を再取得しなければならない(shall)。

適用上の注釈：*これは、鍵が再度導出または復号されなければならない(must) ように、もはや不要である鍵を消去することによって達成されるべきである(should)。*

FCS_CKM.4(a) 暗号鍵破棄（電力管理）

FCS_CKM.4.1(a) TSF は、以下：[*FCS_CKM.4(d) で規定された鍵破棄方法*]を満たすような FPT_PWR_EXT.1 により定義された適合省電力状態へ遷移するとき、揮発性メモリから暗号鍵及び鍵材料を[選択：運用環境に消去 (Clear) するよう指示、消去 (erase)]しなければならない(shall)。

適用上の注釈：*この場合、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場合のみであり、この場合、うまく文書化された、メモリ消去操作を呼び出すためのメカニズムとインタフェースを開示しなければならない(must)。*

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 回の上書き：[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：任意の CSP を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：***
  - ***鍵の格納場所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：任意のCSPを含まないような何らかの値]；***

o ***鍵を表すような抽象化の破棄を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SFRは、FDE EE cPPでの番号付けに合わせるため、FCS_CKM.4(d)となった。*

本要件で参照されるインタフェースは、最も可能性が高いOSカーネルへのアプリケーション プログラミングインタフェースのような、異なる形態を取る可能性がある。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、アプリケーションはファイルシステムの詳細へアクセスできるかもしれないし、特定のメモリロケーションに論理的にアドレス指定できるかもしれない。別の実装において、アプリケーションは、単に資源を取り扱うだけかもしれないし、その資源を削除するようプラットフォームに依頼のみが可能かもしれない。TOEがアクセスする詳細のレベルはSTのTSSセクションに反映されるだろう。

いくつかの選択は、「任意のCSPを含まないような値」の割付を許容する。これは、TOEが、その他の選択しとして列挙された特定の値のいずれでもないような、FCS_RBG_EXT要件を満たすRBGから引き出されないその他の何らかの特定されたデータを使用することを意味する。「任意のCSPを含まない」というフレーズの観点は、上書きされたデータが注意深く選択されること、及び現在含まれるに違いない一般的な「プール」または機密性保護をそれ自身要求するような残存データから取られないことを保証することである。

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、すべての鍵と鍵材料について、もはや不要となった場合、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.4(d)を用いて破棄される。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ような複数の状況がある、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よう場合がある。PINがスマートカード用に使用された場合、PINが適切に破棄されたことの保証が対処されなければならない(shall)。*

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) 詳細化：TSFは、**FPT_PWR_EXT.1によって定義されたとおり、適合省電力状態へ移行しようとする**とき、**平文で格納された**すべての**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)。それらのシナリオについて、TOEまたは運用環境ガイダンス証拠資料は、鍵材料の破棄をサポートするための手順を提供*

しなければならない (must) (例、システムの電源投入時シーケンスの初期段階でメモリ消去を伴う自動化再ブート)。

FCS_KYC_EXT.1 鍵チェイニング(イニシエータ)

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 としてのサブマスクを利用する、もの；
- 以下の方法を利用する BEV への 1 つまたはそれ以上のサブマスクから作られた中間鍵：[選択：
  - FCS_KDF_EXT.1 で規定された鍵導出、
  - FCS_COP.1(d)で規定された鍵ラッピング、
  - FCS_SMC_EXT.1 で規定された鍵コンバイニング、
  - FCS_COP.1(e)で規定された鍵配送、
  - FCS_COP.1(g)で規定された鍵暗号化]]

ここで、対称鍵について[選択：128 ビット、256 ビット]の有効強度及び非対称鍵について[選択：適用されない、112 ビット、128 ビット、192 ビット、256 ビット]の有効強度を維持すること。

FCS_KYC_EXT.1.2 TSF は、少なくとも [選択：128 ビット、256 ビット]の BEV を[*割付：1 つまたはそれ以上の外部エンティティ*]へ、[選択：

- TSF が、FCS_VAL_EXT.1 で規定された検証プロセスを成功裏に実行した後に
- 検証を実行することなしに]

提供しなければならない。

適用上の注釈： *鍵チェイニングは、BEV (訳注：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許可要素を用いたり、それを直接 BEV として用いたりするように) から多数のまで、さまざまである。これが最終的な BEV のラッピングまたは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、TPM に格納された鍵、比較用の値) を含めて適用される。*

BEV への複数の鍵チェインは、すべての鍵チェインがその鍵チェイニング要件を満たす限り、許容される。

BEV は、鍵材料と等価であると考えられ、ゆえに追加のチェックサムまたは同様な値は、例えそれらが BEV と共に送信されたとしても、BEV ではない。

一度、ST 作成者が (鍵導出または鍵アンラッピングまたは暗号化鍵または RSA 鍵配送の使用、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、ST 作成者は、附属書 B から適切な要件を取り込む。いずれかの方法またはすべてを使用する実装が許容される。

FCS_KYC_EXT.1.2 について、評価プロセスは、附属書 B、FCS_VAL_EXT.1 で定義される。その選択が ST 作成者により行われる場合、FCS_VAL_EXT.1 は ST 本文に含まれる。

TOE が鍵をチェインするために、それらを管理／保護するために使用する方法は、鍵管理記述に記述される；さらなる情報については、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：一切のソルトを利用しない、[選択： FCS_RBG_EXT.1 で規定された 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：一切のノンス無し、最小ビット長[*64*] ビットの一意なノンス]を利用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。ひとつの秘密鍵での GCM の呼び出し回数は 2^32 回を超えてはならない(shall)。]

適用上の注釈：*本要件は、いくつかの重要な要素―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。CBC、 XTS、及び GCM が、データの AES 暗号化用として許可される。AES-CCM は、鍵ラッピング用に許可されたモードである。*

5.4　クラス：セキュリティ管理(FMT)

FMT_MOF.1 セキュリティ機能のふるまいの管理

FMT_MOF.1.1 TSF は、機能 [*適合省電力状態の利用*] の [ふるまいを改変する] 能力を[*許可された管理者*] に限定しなければならない(shall)。

適用上の注釈：*「ふるまいを改変する」は、適合する電力状態がいつ、どのように発生するかについての任意の変更を指す。特権利用者のみが「適合省電力状態の利用」機能の改変を介して、適合省電力状態の有効化または無効化を許可される。*

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できなければならない(shall)：[

a) DEK を変更する要求を EE に送る、
b) DEK を暗号学的に消去する要求を EE に送る、
c) 使用される許可要素または複数の許可要素を許可された利用者による変更に従う、
d) 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、
e) *[選択：その他の機能なし、TSF RBG を用いて許可要素を生成する、許可要素を設定する、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、是正のためのふるまいを起動するための検証試行失敗回数を設定する、検証試行失敗回数超過の事象で発行する是正のため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 が持つ管理機能を表現することである。これは、TOE が列挙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 (e)は、TOE に含まれている機能を特定するために使用されるが、cPP に適合するために要求されるわけではない。鍵管理機能を含んでいるような暗号機能を設定しなさい、例えば BEV がラップまたは暗号化されていれば、EE は BEV のラップを解くまたは復号する必要がある。項目(e) において、その他の管理機能が提供されない (または主張されない)場合、「その他の機能なし」が選択されるべきである。*

DEK を変更することは、新しい DEK によってデータが再度暗号化されることを要求することになるが、利用者が新しい DEK を生成する能力を認める。

本文書の目的について、鍵の廃棄処理は、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。ある実装において、DEK を変更することは DEK を暗号技術的に消去することと同じ機能であるかもしれない。

5.5 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、鍵が以下の基準のいずれか 1 つを満たすことなしに、[選択：不揮発性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た状態または 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た状態で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.1 で規定される鍵チェインの一部ではない。
- 平文の鍵は、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た鍵分散であり、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は格納されない]。
- 平文の鍵は、許可要素として使用するため、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使用される、
    - 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]、すでに[選択：
        - FCS_COP.1(d)で規定されるとおりラップされている、
        - 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 または運用環境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 を保護するためのセキュリティ関連の役割を担うことを許容する唯一の方法は、それが分散鍵であるか、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。*

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、[*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 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、利用者の非アクティブ状態、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、利用者はどのくらいの時間を待つべきか)。*

FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1.1 詳細化：TSF は、[*許可された利用者*] に、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提供しなければならない(shall)。

FPT_TUD_EXT.1.2 詳細化：TSF は、[*許可された利用者*] に、 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提供しなければならない(shall)。

FPT_TUD_EXT.1.3 詳細化：TSF は、アップデートをインストール前に、TOE ソフトウェアへのアップデートを製造者による[**FCS_COP.1(a)で規定されるとおりの**ディジタル署名]を用いて検証しなければならない(shall)。

適用上の注釈：*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。*

6. セキュリティ保証要件

本 cPP は、評価者が評価に適用可能な証拠資料を評定し、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) を識別する。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：許可取得 2016 年 9 月*で規定される。

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 cPP に適合するために書かれた ST に対する TOE の評価用の一般モデルは、以下のとおりである：ST が評価用として承認された後、ITSEF は TOE、サポートしている 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こと。ITSEF は ASE 及び ALC の SAR について共通評価方法(CEM)によって義務付けられたアクションを実行することが期待される。ITSEF 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 保証要件の解釈となることを意図された、SD に含まれる評価アクティビティを実行する。SD に取り込まれた評価アクティビティは、TOE が cPP に適合することを実証するため開発者が提供する必要のあるものとして、明確化も提供している。

表 3：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
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 アクティビティに従って評価される。さらに、TOE 技術種別に特有で、かつ TSS に含めることが必須である記述についてそれを求める評価アクティビティが SD 内にあるかもしれない。

本 cPP における SFR は、適合する実装が、基本原則を満たした上で、受け入れ可能な鍵管理のやり方を幅広く取り込むことを許容している。鍵管理方式の重要性を考慮し、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。この情報は、所有権表示され、ST への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を想定されていない。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 を参照すること。

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が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、**専有権対象の情報(Proprietary)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む)、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む)、その他の cPP が規定する専有権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 についての設計情報は、ST の TSS 部分や本 cPP が要求する追加情報であって非公開のもの(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証拠資料にも含まれている。

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」証拠資料は、必要とされない。

SD の評価アクティビティは、該当する SFR に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、追加の証拠資料は必要とされない。

6.3 AGD：ガイダンス証拠資料

ガイダンス文書は ST と共に提供される。ガイダンスは、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。この証拠資料は、非公式なスタイル（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す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。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構成要素として 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係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、管理者及びアプリケーション開発者向けのガイダンスが文書またはウェブページに分散して存在していてもよい。

開発者は、評価者がチェックする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 (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証よりむしろ、ライフサイクルの最終利用者から見えるような側面に制限されている。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 を同一のベンダからの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特定できるように、TOE を識別することを目標としている。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こと。

6.4.2 TOE の CM 範囲 (ALC_CMS.1)

TOE の適用範囲及びそれに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こと。

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 ファミリによって行われるが、後者は

AVA_VAN ファミリによって行われる。本 cPP では、テストは公表された機能や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。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こと。

6.6 クラス AVA：脆弱性評定

本 cPP の第一世代として、iTC は、この種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)

付属サポート文書の附属書 A は、脆弱性分析を実施するための評価者へのガイドを提供する。

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 つの要件集がある。

最初の要件集 (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 番目の要件集 (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)。

本セクションにあるいくつかの要件は繰り返しが可能だが、ST 作成者は ST の本文に附属書からの適切な要件を含めることに責任を持ち、正確な繰り返しの番号付けは ST 作成者にゆだねられる。

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、それらの機能はその他の SFR における選択を ST 作成者が確定することを条件とするため、「選択ベース」の SFR であるとも見なされる。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ために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 TSF 自己テスト

TOE によって提供されるあらゆる暗闘プリミティブが適切に機能していることを保証するため、TSF がそれらの完全性を検証するために使用される自己テスト機能を提供することは必要である。TSF が FCS_RBG_EXT.1 または FCS_COP.1 の任意の繰り返しを含む場合、ST 作成者は、以下の SFR を含まなければならない(shall)：

FPT_TST_EXT.1 TSF テスト

FPT_TST_EXT.1.1 TSF は、TSF の正しい動作を実証するために、[選択：*初期起動中に（電源投入時）*、条件 [*機能が最初に呼び出される前*] において]、以下の一連の自己テス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その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 に実装され、 NIST SP 800-90 に従っている場合、評価者は、NIST SP800-90 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化機能について、それらの機能をテストするための方法が、TSS に記述されていることを検証しなければならない(shall)。 TSS は、それらの各機能について、機能／部品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／部品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(shall)。

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 または下層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 の本文には、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、運用環境が同等な機能を提供することを示すことが可能な限り、求められる SFR を含む必要はない。

B.1 クラス：暗号操作 (FCS)

FCS_VAL_EXT.1 が ST に含まれる場合、評価者は、以下の脅威を ST に含めなければならない：

> (T.AUTHORIZATION_GUESSING) 脅威エージェントは、パスワードやPIN (訳注：暗証番号) のような許可要素を推定するために繰り返しホストソフトウェアを実行するかもしれない。許可要素の推定の成功は、TOEにDEKのリリースを生じさせるかもしれない、または許可されない利用者に保護データを暴露するような状態にTOEを置くかもしれない。
>
> [FCS_VAL_EXT.1]
>
> 根拠：有効なBEV [FCS_VAL_EXT.1] のみが EE [FCS_VAL_EXT.1] へ送られる。検証試行の失敗の応答 [FCS_VAL_EXT.1] は、許可要素の推測が成功する脅威を低減する。

FCS_CKM.1(a) 暗号鍵生成 (非対称鍵)

FCS_CKM.1.1(a) 詳細化：TSF は、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、~~以下を満たす、~~**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、非対称鍵生成が使用される場合、ST 作成者は 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 と一緒に使用される。鍵ペア生成アルゴリズムが FIPS 186-4 の附属書 B.3.2 または B.3.5 のいずれかに基づいて選択される場合、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(b**) 詳細化：** TSF は、以下を満たす規定された暗号鍵長[***選択： 128 bits、256 bits***]で、**FCS_RBG_EXT.1 で規定されたとおりの乱数ビット生成器を使用して対称**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： *対称鍵は、鍵チェインに沿って鍵生成のために使用されることがある。ゆえに、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_COP.1(a) 暗号操作 (署名検証)

FCS_COP.1.1(a) 詳細化： TSF は、以下に従い、[*暗号署名サービス(検証)*]を実行しなければならない[***選択：***

- ***RSA ディジタル署名アルゴリズムで、鍵長 (modulus)が 2048 bits 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 bits 以上のもの***

]

ここで、以下を満たすものとする：[***選択：***

- ***RSA 方式について、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***
- ***ECDSA 方式について、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***

].

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指定するために、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***] ~~及び暗号鍵長[*割付：暗号鍵長*]~~ に従い、[*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)用に使用されるアルゴリズムの全体の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 の ECC 用に選択されるべきであり、SHA 512 は P-521 の 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ている。*

FCS_COP.1(c) 暗号操作 (鍵付ハッシュアルゴリズム)

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

適用上の注釈： *割付の鍵長 [k] は、L1 と L2 (適切なハッシュ関数は ISO/IEC 10118 で定義されている。例えば、 SHA-256 については、 L1 = 512, L2 =256)の間の範囲に入る。 ここで、L2 ≤ k ≤ L1 とする。*

FCS_COP.1(d) 暗号操作 (鍵ラッピング)

FCS_COP.1.1(d) 詳細化：TSF は、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、以下を満たす、[*鍵ラッピング*] を実行しなければならない(shall)：[*ISO/IEC 18033-3 で規定されたとおりの 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ンアプローチにおける鍵ラッピングの使用を選択する場合、本要件は ST の本文にて使用される。*

FCS_COP.1(e) 暗号操作 (鍵配送)

FCS_COP.1.1(e) 詳細化：TSF は、規定された暗号アルゴリズム[*RSA を以下のモードで* ***[選択：KTS-OAEP, KTS-KEM-KWS]***]及び暗号鍵長[***選択：2048 ビット、3072 ビット***] に従って、以下を満たす、[*鍵配送*]を実行しなければならない：[*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のやり方での鍵配送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_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、規定される暗号アルゴリズム[*以下のモードで使用される AES：****[選択：CBC、GCM、XTS]モード***]及び暗号鍵長[***選択：128 ビット、256 ビット***] に従って、以下を満たす、[*データ暗号化及び復号*]を実行しなければならない：[*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 における本要件の意図は、TOE で使用するために適した適切な対称鍵暗号化／復号アルゴリズムを表現する SFR を提供することである。ST 作成者が検証要件 (FCS_VAL_EXT.1)を含め、かつ既知の値を復号して比較を行うようなオプションを選択することを選ぶ場合、これは、ST 作成者が選択可能なアルゴリズム、モード、及び鍵長を規定するために使用される要件である。あるいは、ST 作成者が、FCS_KYC_EXT.1 で規定される鍵チェイニングのやり方の一部として鍵を保護するために AES 暗号化／復号を使用する場合、本要件が ST の本文において使用されること。*

XTS モードが選択される場合、256-bit または 512-bit の暗号鍵が IEEE 1619 に規定されるとおり許容される。XTS-AES 鍵は、２つの等しい鍵長の AES 鍵に分割される － 例えば、256-bit 鍵と XTS モードが選択されるとき、AES-128 が下位のアルゴリズムとして使用される。512-bit 鍵と XTS モードが選択されるとき、AES-256 が使用されること。

FCS_COP.1(g) 暗号操作 (鍵暗号化)

FCS_COP.1.1(g) 詳細化： TSF は、規定される暗号アルゴリズム[*以下で使用される AES [**選択：CBC、GCM]**モード*] 及び暗号鍵長 [***選択：128 ビット、256 ビット***]に従って、以下を満たす、[*鍵暗号化と復号*]を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： *FCS_KYC_EXT.1 で規定される鍵チェイニングのやり方の一部として、鍵を保護するために AES 暗号化／復号の利用を ST 作成者が選択する場合、本要件は ST の本文で使用されること。*

FCS_KDF_EXT.1 暗号鍵の導出

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、 [選択：FCS_RBG_EXT.1 で規定されるように RNG が生成したサブマスク、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 [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]

の定義に従って、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に、受け入れなければならない(shall)。

適用上の注釈： *FCS_KYC_EXT.1 で規定される鍵チェイニングのやり方において鍵導出 (KDF) の利用を ST 作成者が選択する場合、本要件は ST の本文で使用されること。*

本要件は、鍵チェインに沿った新しい鍵を生成するため、新しいランダムな鍵の生成、または既存のサブマスクについての受け入れ可能な方法を確立する。

FCS_PCC_EXT.1 暗号パスワードの生成と調整

FCS_PCC_EXT.1.1 パスワード許可要素を生成するために TSF によって使用されるパスワードは、[***割付：64 ケタ以上の正の整数***] 文字までの{大文字、小文字、数字及び[***割付：その他のサポートされる特殊文字***]}の文字セットを有効化しなければならない(shall)、また以下を満たす、規定された暗号アルゴリズム HMAC-[選択： SHA-256、SHA-512]に従って、[*割付：1000 以上の正の整数*]回繰り返し、出力暗号鍵長[選択： 128、256]を用いて、パスワードベースの鍵導出関数を実行しなければならない(shall)：[*NIST SP 800-132*]。

適用上の注釈： *パスワードは、ホストマシンにおいて TOE 及び下位の OS に依存するコード化された文字列として表現される。このシーケンスは、鍵チェインへの入力として使用されるべきサブマスクを形成するようなビット列へ調整されて与えられなければならない (must)。調整は、識別されたハッシュ関数の一つまたは NIST SP800-132 で定義されるプロセスを用いて実行され得る；使用される方法は、ST 作成者により選択される。 800-132 による調整が規定される場合、ST 作成者は実行される繰り返し回数を記入すること。800-132 は、承認されたハッシュ関数を用いた HMAC から構成される疑似乱数関数（PRF）の使用につい*

ても要求している。ST 作成者は、使用するハッシュ関数を選択し、HMAC の適切な要件についても含めること。

FCS_RBG_EXT.1 暗号操作 (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 (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(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、乱数を生成する複数の異なる方法が含まれている；これらのそれぞれは、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下位の具体的な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)のいずれでも Hash_DRBG または HMAC_DRBG 用として許容されるが、CTR_DRBG 用としては 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 のブロック暗号用のセキュリティ強度、エントロピー及びシード長の要件の識別を提供する。*

ISO/IEC 18031:2011 での CTR_DRBG は、導出関数の利用を要求するが、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種別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、RBG の一部と考えられ、RBG が TOE に含まれている場合、開発者は附属書D で概説されたエントロピー記述を提供することが要求されることに留意されるべきである。本エレメントの評価アクティビティで要求される証拠資料 *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。エントロピープールへの個別の寄与は、エントロピー証拠資料がこれらの個別の情報源のそれぞれ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限り、エントロピーの最小量を提供するためにコンバイニングされることができる。*

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-384、SHA-512] を用いて、[*中間鍵またはBEV*]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 ハッシュ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ことができるような方法を規定する。承認されたハッシュ関数は、FCS_COP.1(b) で取り込まれている。*

FCS_VAL_EXT.1 検証

FCS_VAL_EXT.1.1 TSF は、[選択： サブマスク、中間鍵、BEV]の検証を以下の方法を用いて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、
- 以下で規定される[選択：サブマスク、中間鍵、 BEV] をハッシュし、保存されたハッシュされた[選択：サブマスク、中間鍵、 BEV]と比較する：[選択： FCS_COP.1(b), FCS_COP.1(c)]、
- FCS_COP.1(f)で規定される[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、[BEV]の検証を、[*BEV を EE へ転送*]する前に要求しなければならない(shall)。

FCS_VAL_EXT.1.3 TSF は、[選択：

- 設定可能な回数の連続する検証試行失敗に際して、[*DEK の鍵のサニタイズ処理を実行*]、
- 24 時間以内で発生しうる[*割付：ST 作成者が規定した試行回数*] 回しかできないように遅延を設定、
- [*割付: ST 作成者が規定した試行回数*] 回の連続する検証試行失敗の後、検証を阻止、
- [*割付：ST 作成者が規定した試行回数*] 回の連続する検証試行失敗の後、TOE の電源再起動／リセットを要求]

しなければならない(shall)。

適用上の注釈：*セキュアな検証を実行する目的は、サブマスクを危殆化するかもしれないような任意の材料を暴露させないようにすることである。FCS_VAL_EXT.1.1 での選択について、ある種別のエンティティが複数存在する場合、具体的にどのエンティティが本SFR において参照されるかを、ST 作成者は KMD において明確にしなければならない(must)。*

TOE は、BEV を EE へ提示する前に、サブマスク(例、許可要素)を検証すること。あるパスワードが許可要素として使用されるとき、それが検証の試行前に調整されること。許可要素の検証が失敗するような場合において、製品は BEV を EE へ送信しないこと。

FCS_COP.1(d)の鍵ラップが使用されるとき、検証が本質的に実行される。

遅延は TOE によって強制されなければならないが、本要件は製品を迂回するような攻撃（例、第三者パスワードクラッカーのように、攻撃者がハッシュ値または「既知の」暗号値を取得し、TOE の外部で攻撃を開始する）に対処することは意図していない。実行される暗号機能（即ち、ハッシュ、復号）は、 FCS_COP.1(b)、 FCS_COP.1(c)、及びFCS_COP.1(f) で規定されている。

ST 作成者は、複数の許可要素が使用される場合、異なる方法が検証で用いられる場合、または一つ以上の許可要素が検証される場合、かつ一つ以上が検証されない場合、本要件を繰り返す必要があるかもしれない。

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 で使用される拡張要件のいくつかは、cPP で繰り返しされる SFR (例、FCS_COP.1(d)) の依存性を有していることに留意されたい。読者は、これらの依存性について、同じ拡張コンポーネントがほかのプロテクションプロファイルで使用される場合、SFR 名が異なるかもしれないと説明されている。

C.1 背景と適用範囲

本書は、本 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特定される：

表 4：拡張コンポーネント

機能クラス	機能コンポーネント
暗号サポート(FCS)	FCS_AFA_EXT 許可要素取得
	FCS_CKM_EXT 暗号鍵管理
	FCS_KDF_EXT 暗号鍵の導出
	FCS_KYC_EXT 鍵チェイニング
	FCS_PCC_EXT 暗号パスワードの生成と調整
	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、及び初期化ベクタ)
	FCS_VAL_EXT 暗号エレメントの検証
TSF の保護(FPT)	FPT_KYP_EXT 鍵及び鍵材料の保護
	FPT_TST_EXT TSF テスト
	FPT_TUD_EXT 高信頼アップデート

拡張コンポーネントのいくつかは、本 cPP で定義されるような、繰り返しされたパート 2 の SFR における依存性を定義することに留意されたい。この定義は、これらの依存性が SFR を主張する PP に含まれることを義務付けているが、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は義務付けていない(例、FCS_KDF_EXT.1 の包含は、FCS_COP.1(c)として特別に識別されるべき鍵付きハッシュメッセージ認証のために依存する SFR を要求せず、ただ FCS_COP.1 の繰り返しが存在し、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のみである)。

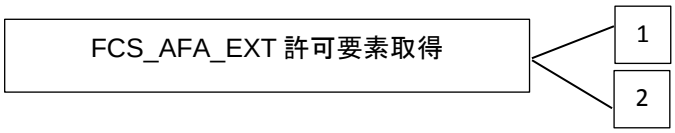
C.2 拡張コンポーネント定義

FCS_AFA_EXT 許可要素取得

ファミリのふるまい

本ファミリのコンポーネントは、さまざまな許可要素を受け付けるための TOE の能力に対処する。

コンポーネントのレベル付け



FCS_AFA_EXT.1、許可要素取得は、TOEによって受け入れられる許可要素を要求する。

FCS_AFA_EXT.2、許可要素取得のタイミングは、TOEが許可要素を受け入れるべき状況を定義する。

管理： FCS_AFA_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：

- 使用される許可要素の改変
- TSF RNG を用いて外部の許可要素を生成する

監査： FCS_AFA_EXT.1

予見される監査対象事象はない。

管理： FCS_AFA_EXT.2

予見される管理アクティビティはない。

監査： FCS_AFA_EXT.2

予見される監査対象事象はない。

FCS_AFA_EXT.1　許可要素取得

下位階層：　なし

依存性：　なし

FCS_AFA.EXT.1.1 TSF は以下の許可要素を受け入れなければならない(shall)： [選択：

- FCS_PCC_EXT.1 で定義されたとおりに調整されたパスワード許可要素から導出されたサブマスク、

- 外部スマートカード要素で、少なくとも DEK と同じビット長であり、鍵長[選択：2048 ビット、3072 ビット、4096 ビット]の RSA を用いて保護された[選択：TOE によって生成された(FCS_RBG_EXT.1 で特定されたとおり RBG を用いて)、ホストプラットフォームによって生成された] もので、スマートカード及び[選択：なし、運用環境が定義する PIN、設定可能な PIN]の提示によって証明された利用者の存在を有するもの、

- 外部の USB トークンの要素で、少なくとも BEV と同じセキュリティ強度であり、FCS_RBG_EXT.1 で規定されたとおり RBG を用いて、TOE により生成されたサブマスクを提供しているもの、

- ホストプラットフォームにより生成されるサブマスクを提供している、少なくともBEV と同じセキュリティ強度である、外部の USB トークンの要素

]。

FCS_AFA_EXT.2 許可要素取得

下位階層： なし

依存性： FCS_AFA_EXT.1 許可要素取得
FPT_PWR_EXT.1 省電力状態

FCS_AFA_EXT.2.1 TSF は、FPT\PWR_EXT.1 で規定される任意の適合する電力状態からの遷移に関して、平文データへのアクセスを許可する前に、FCS_AFA_EXT.1 で規定された許可要素を再度要求しなければならない(shall) 。

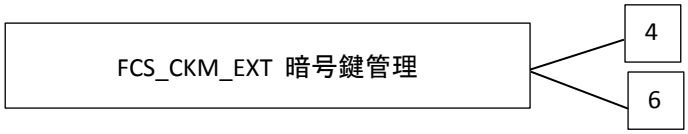
FCS_CKM_EXT 暗号鍵管理

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、その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 パート 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、鍵及び鍵材料破棄は、(CC パート 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

特定の管理アクションは識別されていない

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)

特定の管理アクションは識別されていない

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

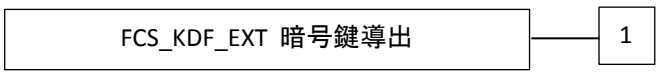
FCS_CKM_EXT.6.1 TSF は、[*割付：セキュリティターゲットのどこかで定義された FCS_CKM.4 の２つ以上の繰り返し*] の鍵破棄方法を使用しなければならない(shall)。

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

特定の管理アクション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

特定の管理アクション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

特定の管理アクション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) 暗号鍵生成(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 1 つ以上のサブマスク由来の中間鍵：[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、少なくとも [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許可要素を用いたり、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、少なくとも [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 から由来し DEK までの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)で規定されるとおりの非対称鍵生成
- FCS_CKM.1(b)で規定されるとおりの対称鍵生成
- FCS_KDF_EXT.1 で特定された鍵導出(key derivation)、
- FCS_COP.1(d)で特定された鍵ラッピング(key wrapping)、
- FCS_COP.1(e)で特定された鍵配送 (key transport)、
- FCS_COP.1(g)で特定された鍵暗号化]]

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：適用されない、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。

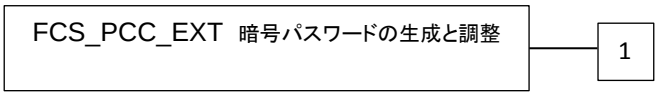
適用上の注釈：*鍵チェイニングは、ドライブ上で保護されたデータを採取的にセキュアにするための複数階層の暗号鍵を用いる方法である。中間鍵の数は、さまざまである―一つ(例、鍵暗号化鍵(KEK)としてBEVを用いる)から多数まで。これは、DEKの最終的なラッピングまたは導出に貢献するようなすべての鍵に適用する；保護されたストレージの領域にあるようなものを含めて(例、TPM保存された鍵、比較値)。*

FCS_PCC_EXT 暗号パスワードの生成と調整

ファミリのふるまい

本ファミリは、BEV を生成するためのパスワードが堅牢(それらの生成に関して)であり、適切な長さのビット列が提供されるよう調整されていることを保証する。

コンポーネントのレベル付け



FCS_PCC_EXT.1、 暗号パスワード生成と調整は、TSF が特定のパスワードを受け付け、それらを適切に調整することを要求する。

管理： FCS_PCC_EXT.1

特定の管理アクションは識別されていない

監査： FCS_PCC_EXT.1

予見される監査対象事象はない。

FCS_PCC_EXT.1　暗号パスワードの生成と調整

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)

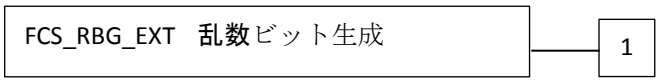
FCS_PCC_EXT.1.1 パスワード許可要素を生成するために TSF によって使用されるパスワードは、[***割付：64 ケタ以上の正の整数***] 文字までの{大文字、小文字、数字及び[***割付：その他のサポートされる特殊文字***]}の文字セットを有効化しなければならない(shall)、また以下を満たす、規定された暗号アルゴリズム HMAC-[選択： SHA-256、SHA-512]に従って、[***割付：1000 以上の正の整数***]回繰り返し、出力暗号鍵長[選択：128、256]を用いて、パスワードベースの鍵導出関数を実行しなければならない(shall)：[*PBKDF 推奨または仕様*]。

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／乱数生成のための要件に対処する。これは FCS クラスのために定義されたファミリである。

コンポーネントのレベル付け



FCS_RBG_EXT.1 拡張：乱数ビット生成は、選択された規格に従い、エントロピー源によってシードされて実行される乱数ビット生成を要求する。

管理： FCS_RBG_EXT.1

予見される管理アクティビティはない

監査： FCS_RBG_EXT.1

以下のアクションは PP/ST において FAU_GEN セキュリティ監査データ生成が含まれる場合監査可能であるべきである：

- ランダム化プロセスの失敗

FCS_RBG_EXT.1　拡張: 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 (ハッシュ関数) または
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（訳注：本拡張コンポーネント定義は、セクション B.1 と同様に[選択：ISO/IEC 18031:2011、NIST SP 800-90A]とすべき）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(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)。

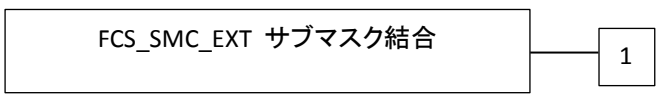
適用上の注釈： *ISO/IEC 18031:2011 には、乱数を生成する 3 つの異なる方法が含まれている；これらは、それぞれ、言い換えれば、下位の暗号プリミティブ（ハッシュ関数／暗号）に依存している。ST 作成者は、使用される関数を選択し、その要件で使用される具体的な下位の暗号プリミティブを含めること。識別されたハッシュ関数（SHA-1, SHA-224, SHA-256, SHA-384, SHA-512）のいずれも Hash_DRBG または HMAC_DRBG 用に許容されるが、CTR_DRBG には AES ベースの実装のみが許容される。*

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 1 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特定する。

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 が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

特定の管理アクション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)

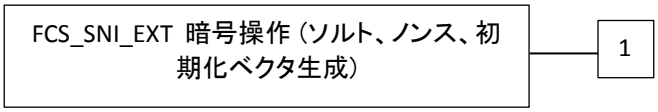
FCS_SMC_EXT.1.1 TSFは、以下の方法 [選択：排他的論理和 (XOR)、SHA-256、SHA-512] を用いて、[*割付：鍵の種別*]を生成するため、サブマスクをコンバイニングしなければならない(shall)。

FCS_SNI_EXT 暗号操作 (ソルト、ノンス、及び初期化ベクタの生成

ファミリのふるまい

本ファミリは、ソルト、ノンス、及び IV がうまく形成されることを保証する。

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、初期化ベクタ生成)は、TOE の暗号コンポーネントによって利用されるソルト、ノンス及び IV の生成が特定された方法で実行されることを要求する。

管理： FCS_SNI_EXT.1

特定の管理アクション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： なし

FCS_SNI_EXT.1.1 TSF は、[選択： FCS_RBG_EXT.1 において特定される RNG、 ホストプラットフォームによって提供される RNG]によって生成されるソルトのみを使用しなければならない(shall)。

FCS_SNI_EXT.1.2 TSF は、[選択：ノンスなし、最小 [64]ビットのユニークなノンス]を使用しなければならない(shall)。

FCS_SNI_EXT.1.3 TSF は、以下の方法で 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)；
- CCM：ノンスは、繰り返してはならない(shall)；
- XTS：IV 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)；

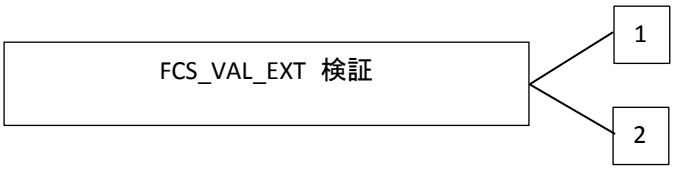
- GCM：IV は、繰り返してはならない(shall)。1 つの所与の秘密鍵について GCM の呼出し回数は 2^32 を超えてはならない(shall)]。

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、使用前に有効性が決定されるための手段を特定する。

コンポーネントのレベル付け



FCS_VAL_EXT.1　検証は、TSF が 1 つ以上の特定された方法によりサブマスク及び BEV を検証することを要求する。

FCS_VAL_EXT.2　利用者検証は、TSF が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

特定の管理アクション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：

- 使用される検証方法の仕様
- TSF によって受け入れられる検証試行失敗回数の設定
- 検証試行失敗回数が受け入れ可能でなくなった事象において 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 (ハッシュ関数)、
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、[選択： サブマスク、中間鍵、BEV]の検証を以下の方法を用いて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プ；
- [選択： FCS_COP.1(b), FCS_COP.1(c)]で規定されるとおり[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]とそれを比較；
- FCS_COP.1(f)で規定されるとおり[選択：サブマスク、中間鍵、BEV] を用いて既知の値を復号して、それを保存された既知の値と比較]

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*]する前に要求しなければならない(shall)。

FCS_VAL_EXT.1.3 TSF は、[選択：

- 設定可能な回数の連続する検証試行の失敗に際して、[*DEK の鍵のサニタイズ処理を実行*]、
- 24 時間以内で発生しうる[*割付：ST 作成者が規定した試行回数*] 回しかできないように遅延を設定、
- [*割付: ST 作成者が規定した試行回数*]回の連続する検証失敗の試行の後、検証を阻止、
- [*割付：ST 作成者が規定した試行回数*]回の連続する検証失敗の試行の後、TOE の電源再起動／リセットを要求]

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、[利用者]の検証を以下からの利用の有効性の主張を受領することにより実行しなければならない(shall)：[*割付：利用者認証に責任のある運用環境コンポーネント*]。

FCS_VAL_EXT.2.2 TSF は、 利用者の検証を[*割付：暗号操作または暗号学的データの送信*]の前に、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回数の連続する検証試行の失敗を受けて、[*割付：鍵のサニタイゼーション アクティビティ*]；
- 24 時間以内に発生しうる[*割付: ST 作成者が規定した試行回数*] 回しかできないように遅延を設定；
- 連続する検証失敗の試行が[*割付：ST 作成者が規定した試行回数*]回に達した後に検証を阻止；
- [*割付：ST 作成者が規定した試行回数*]回の連続した検証試行失敗の後に、TOE の電源再起動／リセットを要求]

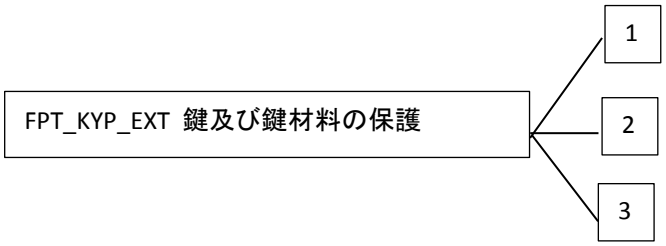
しなければならない(shall)。

FPT_KYP_EXT 鍵及び鍵材料の保護

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 が平文の鍵または鍵材料が不揮発性ストレージへ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、保護される鍵及び鍵材料の格納は、TSF が暗号化された鍵及び鍵材料が格納される不揮発性ストレージの場所を規定することを要求する。

FPT_KYP_EXT.1、保護される鍵及び鍵材料の属性は、TSF が暗号化された鍵及び鍵材料とそのデータを復号及び／または利用する許可を得たサブジェクトの間の関係付けを維持することを要求する。

管理： FPT_KYP_EXT.1

特定の管理アクション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

特定の管理アクション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

特定の管理アクション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(受領者)、
FCS_SMC_EXT.1 サブマスクコンバイニング

FPT_ KYP _EXT.1.1 TSF は、鍵が以下の基準のいずれか 1 つを満たさない場合、[選択：不揮発性メモリに鍵を格納しない、FCS_COP.1(d)で規定されたとおりラップされるとき、または FCS_COP.1(g) または FCS_COP.1(e) で規定されたとおり暗号化されるときにのみ不揮発性メモリに鍵を格納する] ようにしなければならない(shall) [選択：

- 平文の鍵が、以下で規定された鍵チェインの一部ではない：[選択：
  - FCS_KYC_EXT.1、
  - FCS_KYC_EXT.2]。
- 平文の鍵が、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。
- 平文の鍵が FCS_SMC_EXT.1 で規定されたとおりコンバイニングされた分散鍵であり、分散鍵の他の半分は[選択：
  - FCS_COP.1(d)で規定されたとおりラップされる、
  - FCS_COP.1(g)または FCS_COP.1(e) で規定されたとおり暗号化される、
  - 導出されるが不揮発性メモリには格納されない]。
- 平文の鍵は、許可要素として使用するため、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) で規定されたとおり鍵をラップするために使用される、
  - FCS_COP.1(g) または FCS_COP.1(e) で規定されたとおり暗号化され]、すでに[選択：
    - FCS_COP.1(d)で規定されたとおりラップされている、
    - FCS_COP.1(g) または FCS_COP.1(e)で規定されたとおり暗号化されている]]。

FPT_KYP_EXT.2　保護される鍵及び鍵材料の格納

下位階層：　なし

依存性：　FCS_KYP_EXT.1 鍵及び鍵材料の保護

FPT_ KYP _EXT.2.1 TSF は、[選択：TSF 内の、運用環境内の SQL データベース内の、[*割付：その他の鍵格納場所の*]] 保護される鍵及び鍵材料のみを格納しなければならない(shall)。

FPT_KYP_EXT.3　保護される鍵及び鍵材料の属性

下位階層：　なし

依存性：　FCS_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：特定された鍵及び鍵材料を利用することが許可されたサブジェクト*] の間の関係付け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 が複数の省電力状態をサポートするとき、TSF のセキュアなふるまいを定義する。適合省電力状態(即ち、セキュリティ関連データを入力に際して抹消するような省電力状態) の利用は、状態遷移が TOE 自己保護メカニズムを迂回するような攻撃ベクター―として使用できないことを保証するための基本である。

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起動する状況を定義する。

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を有効化または無効化
- １つ以上の省電力状態設定の特定

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

特定の管理アクションは識別されていない

監査： FPT_PWR_EXT.2

以下のアクションは PP/ST において FAU_GEN セキュリティ監査データ生成が含まれる場合監査可能であるべきである：

- 異なる省電力状態への TSF の遷移

FPT_PWR_EXT.1 省電力状態

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：以下の少なくとも 1 つは選択：S3、S4、G2(S5)、G3、[*割付：その他の省電力状態*]]。

FPT_PWR_EXT.2 省電力状態のタイミング

下位階層： なし

依存性： FPT_PWR_EXT.1 省電力状態

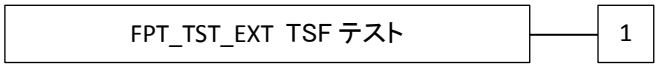
FPT_PWR_EXT.2.1 FPT_PWR_EXT.1 で定義されたそれぞれの省電力状態について、TSF は、以下の条件が起きたときに適合省電力状態へ入らなければならない(shall)：[選択：以下の少なくとも 1 つは選択：利用者起動の要求、システムシャットダウン、利用者の活動なし、リモート管理システムにより起動される要求、[*割付：その他の条件*]、その他の条件なし]。

FPT_TST_EXT TSF 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について TSF を自己テス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_TST_EXT.1 TSF テストは、TSF の正しい動作を実証するために初期起動中に実行される自己テスト一式を要求する。

管理:**FPT_TST_EXT.1**

特定の管理アクションは識別されていない

監査:**FPT_TST_EXT.1**

以下のアクションは PP/ST において FAU_GEN セキュリティ監査データ生成が含まれる場合監査可能であるべきである：

- TSF 自己テストが完了したことの表示

FPT_TST_EXT.1 TSF テスト

下位階層： なし.

依存性： なし.

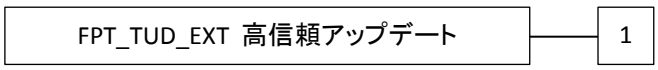
FPT_TST_EXT.1.1 TSF は、TSF の正しい動作を実証するため、以下の自己テスト一式を [選択：初期起動中（電源投入時）に、正常動作中に定期的に、許可された利用者の要求時に、[*割付：自己テストが発生するべき条件*] の条件のときに]、実行しなければならない(shall)：[*割付：TSF により実行される自己テストのリスト*]。

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更新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を検証する能力を含めて、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：

- 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の生成が 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：

- アップデートプロセスの起動。
- 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、[*割付：サブジェクトのリスト*] に 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提供しなければならない。

FPT_TUD_EXT.1.2 TSF は、[*割付：サブジェクトのリスト*] に TOE 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提供しなければならない。

FPT_TUD_EXT.1.3 TSF は、アップデートをインストール前に製造者による[選択：ディジタル署名、公開ハッシュ]を用いて TOE ファームウェアへのアップデートを検証しなければならない。

附属書 D：エントロピー証拠資料及び評定

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 によって使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する。

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。その証拠資料には、設計記述、エントロピーの正当化、動作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。その証拠資料は、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の構成要素の相互作用を含め、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るべきである。

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、及びテストの目的で未処理(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、エントロピー源の動作を記述すること。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)、もし保存される場合にはどこに保存されるのか、そして最後に、どのように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割合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も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。電源切断から電源投入までの間で保存される 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 エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、(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列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 動作条件

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、エントロピー源の動作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の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つ以上の故障を検出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。

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。本証拠資料には、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。

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
- 鍵がいつ、どのように保護されるか
- 鍵がいつ、どのように導出されるか
- 鍵の強度
- いつ鍵がもはや不要とされるか、または鍵が不要とされるかどうか、正当化と共に。

解説には、以下のトピックについても記述すること：

- 製品がサポートするすべての許可要素の記述、及び各要素が実行されるあらゆる調整 (conditioning) やコンバイニング (combining) を含めてどのように取り扱われるか。
- 検証がサポートされる場合、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も記述しなければならない。
- BEV 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詳述しなければならない。どの鍵が BEV の保護に使用されるのか、それらが導出、鍵ラッピング、または 2 つの要件の組み合わせをどのように満たすのかについて、最初の許可から BEV への直接のチェインを含めて、記述しなければならない。また、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。
- 図と解説は、暗号技術的な総当り攻撃または最初の許可要素のすべての値なしにチェインが破られることがないこと、及び BEV 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：デバイスの主な 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）に関連する部分、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、データを格納す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及び不揮発性メモリに格納されるすべての鍵の保護を記述して、鍵がもはや不要となった時に鍵を破棄するためのプロセス。

図：

- 図は、最初の許可要素から BEV へのすべての鍵、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もの）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のための永続的なメディア、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。

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つの構成要素の鍵チェインを繋ぐことを意図したもの。
Key Sanitization（鍵サニタイゼ―ション）	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ホスト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にデータを読み出しまたは書き込みに許可を対応付けるオペレーティングシステムによって管理されたものを指す。 本 SPD 及び cPP のために、FDE は 1 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などのために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）を暗号化されないままにする必要がある。これらの FDE cPP は保護データが含まれていない限りにおいて、FDE ソリューションがストレージデバイスの一部を暗号化しないままにすることを許容する、という意味で「ドライブ全体暗号化」という用語を解釈する。
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 （鍵チェイニング）	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、クリティカル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) （鍵出力鍵）	ストレージから別の鍵を出力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 （電源切断状態）	デバイスがシャットダウンしている状態。
Protected Data （保護データ）	これは TOE が正しく機能するために必要なごく一部を除いたストレージデバイス上のすべてのデータを指す。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]

他のコモンクライテリア略語と用語については [CC1]を参照されたい。

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）
HW	Hardware（ハードウェア）
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（鍵出力鍵）
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）
PBKDF	Password-Based Key Derivation Function（パスワードベース鍵導出関数）
PRF	Pseudo Random Function（疑似ランダム関数）
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 Requirements（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）

頭字語	意味
SFR	Security Functional Requirements（セキュリティ機能要件）
ST	Security Target（セキュリティターゲット）
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）
TOE	Target of Evaluation（評価対象）
TPM	Trusted Platform Module（トラステッド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

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.