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

2015 年 1 月 26 日

バージョン 1.0

平成 28 年 1 月 15 日　翻訳 暫定第 0.4 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 文書の目的

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：許可取得 2015 年 1 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 文書の適用範囲

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。

cPP 及び SD には、編集上の軽微な誤りが含まれているかもしれないが、cPP は常に更新される生きた文書として認識されており、iTC は継続的に更新及び改訂を行っていく。何か問題があれば、FDE iTC へご報告ください。

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 1.0、2015 年 1 月 26 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、2015 年 1 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

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 – Authorization Acquisition (ドライブ全体暗号化用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：1.0

PP 日付：January 26,2015 (2015 年 1 月 26 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。

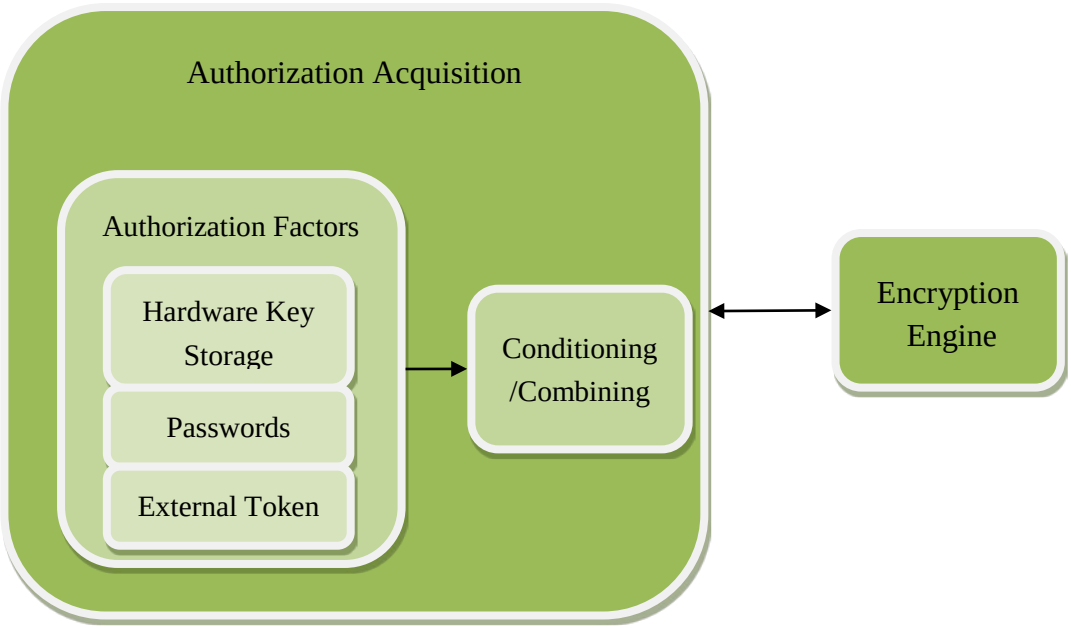


図2：許可要素の詳細

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 に 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。

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。

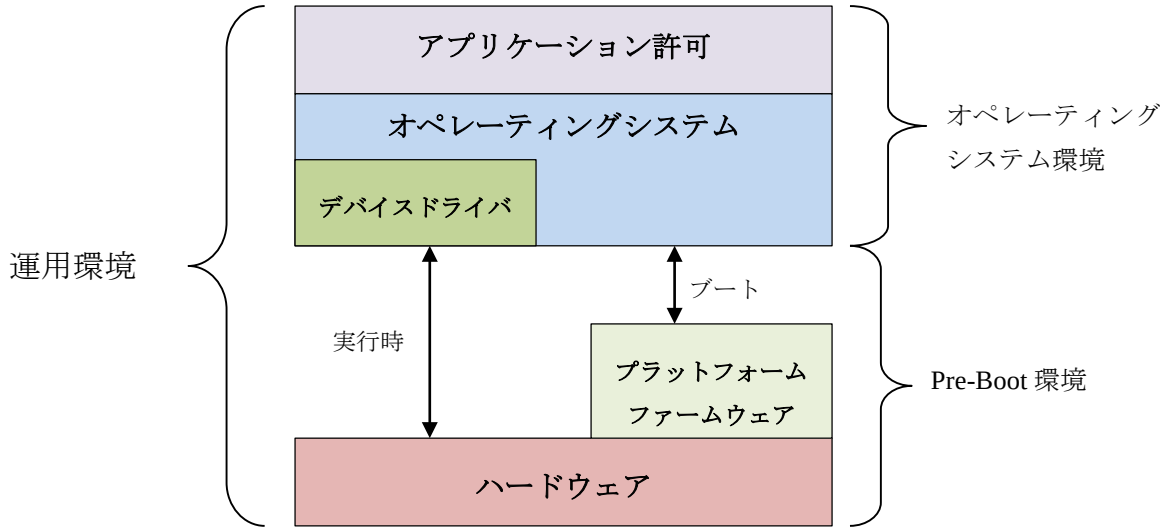


図3：運用環境

1.6 cPP の次のバージョンまで猶予された機能

時間的な制約により、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。パーティション／ボリューム管理、リモート管理、及び電力管理（電力状態保護の要件）に関する要件が含まれる。

1.7 TOE 使用事例

FDE cPP に適合する製品の使用事例は、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 そのものに改変を加えること (例、悪意のメイド攻撃) ができるような使用事例は、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 に適合主張する ST は、CC パート 1 (CCMB-2012-09-001) の附属書 D.2 に定義されるとおり、正確 PP 適合の最低限の規格を満たさなければならない。

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、CC に定義されている*正確適合 (Strict Compliance)* のサブセットとして、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を所有することは、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等価であり、それらは以下で対処されるその他の資産の中にある。

本コラボラティブプロテクションプロファイルが、悪意のあるコードまたは悪用できるハードウェア構成要素を評価対象 (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製品(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、しかし本 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て見つかったハードディスク問題に対処していない、相手はハードディスクを取得し、ブートデバイスの非暗号化部分 (例、MBR、ブートパーティション) を危殆化させた上で、危殆化されたコードを実行することを目的として、オリジナル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される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彼らが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.1.1, FCS_KYC_EXT.1.1, FCS_KYC_EXT.1.2, FCS_PCC_EXT.1, FMT_SMF.1.1]

根拠：FCS_KYC_EXT.1.2 は、BEV が暗号化されたドライブ上の保護データへのアクセスを EE に提供することを要求する。1 つ以上のサブマスク[FCS_AFA_EXT.1.1]は、結合 (Combined) され[FCS_SMC_EXT.1.1]、そして／またはチェイン (Chained) され[FCS_KYC_EXT.1.1] 、BEV を生成する。これらの要件は、BEV が適切に生成され、保護され、暗号化された保護データの不正な暴露を防止することを保証する。FMT_SMF.1.1 は、TSF が DEK の変更及び消去要求を含めて 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。

(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_PCC_EXT.1, FCS_KYC_EXT.1.1, FCS_AFA_EXT.1.1, FPT_KYP_EXT.1.1, FCS_CKM_EXT.4, FCS_CKM.4.1, FCS_CKM.1.1, FCS_VAL_EXT.1.1, FMT_SMF.1.1]

根拠：BEV は、 1 つ以上のサブマスク[FCS_AFA_EXT.1.1] とチェインされる[FCS_KYC_EXT.1.1]される。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。FPT_KYP_EXT.1.1 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 が FCS_CKM.4.1 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。

FMT_SMF.1.1 は、TSF が許可要素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提供することを保証する。

(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。

[FPT_TUD_EXT.1.1, FPT_TUD_EXT.1.2, FPT_TUD_EXT.1.3, FMT_SMF.1.1]

根拠：FPT_TUD_EXT.1.1, FPT_TUD_EXT.1.2 及び FPT_TUD_EXT.1.3 は、許可された利用者が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。

FMT_SMF.1.1 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。

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. 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復元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.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り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]

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。

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。

表2：セキュリティ機能要件

機能クラス	機能コンポーネント
Cryptographic support Class (FCS)	FCS_AFA_EXT.1 許可要素取得
Cryptographic support Class (FCS)	FCS_KYC_EXT.1 (鍵 チェイニング)
Cryptographic support Class (FCS)	FCS_CKM_EXT.4 暗号鍵及び鍵材料破棄
Cryptographic support Class (FCS)	FCS_CKM.4 暗号鍵破棄
Cryptographic support Class (FCS)	FCS_SNI_EXT.1 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成)
Security management Class (FMT)	FMT_SMF.1 管理機能の特定
Protection of the TSF Class (FPT)	FPT_KYP_EXT.1 拡張：鍵及び鍵材料の保護
Protection of the TSF Class (FPT)	FPT_TUD_EXT.1 高信頼アップデート

5.1 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、

- RSA (鍵長 2048 以上) を用いて保護された、(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保護している、少なくとも DEK と同じビット長である、外部のスマートカードの要素、

- RSA (鍵長 2048 以上) を用いて保護された、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保護している、少なくとも DEK と同じビット長である、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 を用いて結合（combined）されなければならない。

FCS_KYC_EXT.1 (鍵チェイニング)

FCS_KYC_EXT.1.1 TSF は、[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 BEV へ 1 つ以上のサブマスクから生成する中間鍵：[選択：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_SMC_EXT.1 で特定された鍵結合 (key combining)、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]]の鍵チェインを維持しなければならない。ここで、[選択：128bits、256bits] の有効な強度を維持すること。

FCS_KYC_EXT.1.2 TSF は、EE への［選択：128bits、256 bits］の BEV を[選択：FCS_VAL_EXT.1 で特定されたように TSF が検証プロセスを実行して成功した後に限り、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 (境界暗号化値) 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、ー 1 つ (例えば、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) から多数の場合まで、さまざまである。これが最終的なラッピングまたは BEV を導出するために寄与するすべて

の鍵に適用され、；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 への複数の鍵チェインは、鍵チェイニング要件を満たす限り、許容される。

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 では、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 本文へ引用される。

*TOE が鍵をチェインさせたり、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；詳細は、**鍵管理記述**を参照のこと。*

FCS_CKM_EXT.4 暗号鍵及び鍵材料破棄

FCS_CKM_EXT.4.1 TSF は、すべての鍵及び鍵材料について、もはや不要となった場合、破棄しなければならない。

***適用上の注釈**：中間鍵及び鍵材料を含め、もはや不要となった鍵は、FCS_CKM.4.1 の承認された方法を用いて破棄されること。鍵の例としては、中間鍵、サブマスクや BEV がある。永続的なストレージ上の鍵または鍵材料がもはや不要となり破棄が要求される場合があるかもしれない。ベンダは、実装に基づいて、いつ鍵が不要となるかを説明すること。鍵材料が不要となる複数の状況がある、例えば、ラップされた鍵は、パスワードが変更された時に破棄される必要があるかもしれない。しかし、例えば、デバイス識別用の鍵のように、メモリ上に残存することが許容される場合がある。*

FCS_CKM.4 暗号鍵破棄

FCS_CKM.4.1 TSF は、以下の特定された暗号鍵消去方法［選択：

- 揮発性メモリでは、消去は 1 回の直接上書き[選択：TSF の RBG を用いて疑似ランダムパタンによる、ホストプラットフォームの RBG を用いた疑似ランダムパタンによる、ゼロによる]とその後の読み出し−検証によって実行されなければならない。
- 不揮発性ストレージでは、消去は以下により実行されなければならない：
    - [選択：1 回、3 回以上]の鍵データ保存場所の上書きを[選択：TSF の RBG (FCS_RBG_EXT.1 にて特定されるとおり) を用いた疑似ランダムパタン、ホストプラットフォームの RBG を用いた疑似ランダムパタン、固定のパタン]によって行い、その後に[選択：読み出し-検証、なし]を行う。上書きデータの読み出し-検証が失敗した場合、処理が再度繰り返されなければならない；

] に従い暗号鍵を消去しなければならない。ただし、この方法が以下を満たすこと：［選択：NIST SP800-88、規格なし]。

***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む鍵は、承認された方法の 1 つを用いて揮発性メモリ内で破棄されること。これらの場合において、破棄方法は、本要件において規定された方法の 1 つに適合すること。本要件は、暗号技術的消去を実行するための方法を呼び出し、これは鍵情報の破棄のためのよく定義された用語と考えられる。いくつかのソリューションは、鍵が格納される媒体のロケーションへの書き込みアクセスをサポートしており、これによって鍵及び鍵材料データへの直接上書きによる暗号鍵の破棄を可能としている。それ以外の場合には、システム及び／またはデバイスレベルにおけるストレージ仮想化技術は、鍵データを複数複製する結果となったり、かつ／または、基盤となる媒体技術は、鍵データの保存されているロケーションに直接上書きすることをサポートしていない。ワンタイムのプログラマブルメモリが除外されることに注意すること。*

5.2 管理機能の特定 (FMT_SMF)

FMT_SMF.1 管理機能の特定

FMT_SMF.1.1 TSF は、以下の管理機能を実行できなければならない：[

a) DEK を変更する要求を EE に送る、
b) DEK を暗号技術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、[選択：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安全にアップデートする、[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。

5.3 クラス： TSF の保護 (FPT)

FPT_KYP_EXT.1 拡張：鍵及び鍵材料の保護

FPT_KYP_EXT.1.1 TSF は、FCS_COP.1(d)で特定されたとおりラップされるか、または FCS_COP.1(g) または FCS_COP.1(e) で特定されたとおり暗号化されるときは、不揮発性メモリに鍵を格納するのは、鍵が以下の基準を満たさない場合にのみに限定しなければならない：[選択：

- 平文の鍵が FCS_KYC_EXT.1 で特定された鍵チェインの一部ではない。
- 初期設定の後、暗号化データへのアクセスをもはや提供しない平文の鍵。
- 平文の鍵が FCS_SMC_EXT.1 で特定されたとおり結合された分散鍵であり、他の分散鍵の半分は[選択：FCS_COP.1(d)で特定されたとおりラップされるか、FCS_COP.1(g)または FCS_COP.1(e) で特定されたとおり暗号化される、または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、外部ストレージ上に格納される。
- 平文の鍵は、[選択：FCS_COP.1(d)で特定されたとおり鍵をラップされている、FCS_COP.1(g) または FCS_COP.1(e) で特定されたとおり暗号化されている］鍵を、[選択：FCS_COP.1(d)で特定されたとおりラップする、FCS_COP.1(g) または FCS_COP.1(e)で特定されたとおり暗号化する]ために使用される。

適用上の注釈：不揮発性メモリでの平文の鍵ストレージは、いくつかの理由により許容される。鍵が TOE 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、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する鍵であれば、BEV または DEK を保護するためのセキュリティに関連する役割を担う方法として許容される。

FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1.1 TSF 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る能力を提供しなければならない。

FPT_TUD_EXT.1.2 TSF は、[許可された利用者に] TOE 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[ディジタル署名]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。

適用上の注釈：3 番目のエレメントにおけるディジタル署名メカニズムは、附属書 A の FCS_COP.1(a) に規定されるものである。本コンポーネントは TOE 自身にアップデート機能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技術的なチェックを実行することも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*(Mandatory Technical Document) Full Drive Encryption: Authorization Acquisition January 2015)* にて特定されている。

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。ITSEF 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。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。

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 –適合 (ATE_IND.1) (訳注：CCPart3 より「適合」とした)
脆弱性評定(AVA)	脆弱性調査 (AVA_VAN.1)

表3：セキュリティ保証要件

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、**所有権表示された鍵管理記述 (附属書 E) 、及び [選択：エントロピー解説、その他の cPP が特定する所有権表示された文書なし]**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 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 クラス：暗号サポート (FCS)

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を呼び出す；第三者の暗号ライブラリ；またはハードウェア暗号アクセラレータ) のいずれかが許容される。本セクションの要件は、TOE がセキュリティ対策方針を満たすため、TOE または運用環境のいずれかに存在していなければならない暗号機能を特定する。TOE にその機能が存在する場合、ST 作成者によってこれらの要件が ST の本文に移されるだろう。

機能が単に TOE によって使用され、運用環境によって提供される場合、開発者は、ST で列挙された各運用環境におけるそれらの機能を識別することになる。この識別は、評価者が、本セクションの要件を満たすような TOE について列挙された各運用環境を検証するためのアクティビティを実行するために運用環境における機能についての情報とともに、TSS (各操作を呼び出す方法が識別されることを要求している) における情報が利用可能であるべきである。評価者は、運用環境がそれらの機能を提供すること、インタフェースが運用環境の付随資料に存在することを確認するため、運用環境をチェックすること。

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： 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。

FCS_SNI_EXT.1.2　TSF は、最小 [64] **bits** のユニークなノンスのみを使用しなければならない。

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：[

- CBC：IV は、繰り返してはならない。
- CCM：ノンスは、繰り返してはならない。
- XTS：IV なし。 Tweak 値は、非負の整数であり、連続に割り振られ、かつ任意の非負の整数から始まらなければならない。
- GCM：IV は、繰り返してはならない。1 つの秘密鍵での GCM 演算回数は 2^32 を超えてはならない。

]。

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、ノンスはユニークであればよい。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特定する。CBC、 XTS、及び GCM は、データの AES 暗号化用として許可される。AES-CCM は、鍵ラッピング用のモードとして許可される。

FCS_CKM.1　暗号鍵生成 (非対称鍵)

FCS_CKM.1.1 詳細化：TSF は、以下に特定された暗号鍵生成アルゴリズムに従って**非対称**暗号鍵を生成しなければならない： [選択：

- ***RSA 方式*** *のうち* ***2048 bits 以上*** *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、* ***「NIST 曲線」 P-256, P-384 及び [選択: P-521, その他の曲線なし]*** *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* ***2048 bits 以上*** *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*

]。

適用上の注釈： ST 作成者は、鍵確立で使用されるすべての鍵生成方式を選択しなければならない。 鍵生成が鍵確立で使用される場合、FCS_CKM.2.1 における方式及び選択された暗号プロトコルは選択と一致しなければならない。
TOE が RSA 鍵確立方式においてレシーバとして動作する場合、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、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。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(c)　暗号鍵生成 (対称鍵)

FCS_CKM.1.1(c)　**詳細化：** TSF は、以下を満たす特定された暗号鍵長[選択： 128 bits、 256 bits]で、FCS_RBG_EXT.1 で特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に使用されることがある。*

FCS_SMC_EXT.1　サブマスク結合

FCS_SMC_EXT.1.1 TSFは、中間鍵またはBEVを生成するために以下の方法 [選択： 排他的論理和 (XOR)、 SHA-256、 SHA-512] を用いてサブマスクを結合しなければならない。

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結合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) 及び FCS_COP.1(c) に取り込まれている。*

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：[選択： FCS_COP.1(d)にて特定された鍵ラップ、[選択： FCS_COP.1(b), FCS_COP.1(c)]で特定されるとおり[選択：サブマスク、中間鍵、 BEV] をハッシュして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)で特定されるとおり[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] を用いて実行しなければならない。

FCS_VAL_EXT.1.2 TSF は、検証が発生した後にのみ、BEV を EE へ送信しなければならない。

FCS_VAL_EXT.1.3 TSF は、[選択：設定可能な連続する検証失敗の試行回数によって DEK の鍵の廃棄処理を EE へ発行、24 時間で発生しうる[割付：ST 作成者が規定した回数の試行] 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 作成者が特定した試行回数]に達した後に検証を阻止]しなければならない。

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材料を暴露しないようにすることである。FCS_VAL_EXT.1.1 における選択について、ST 作成者はある種の複数のエンティティが存在する場合、KMD においてどのようなエンティティが本 SFR において参照されているかを明確にしなければならない。*

TOE は、EE へ BEV を送る前に、サブマスク(例、許可要素)を検証する。パスワードが許可要素として使用される場合、検証の実行前に調整される。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。

遅延が 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 外部に攻撃を開始する）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)、 FCS_COP.1(c)、及び FCS_COP.1(f) で特定されている。

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、本要件を繰り返す必要があるかもしれないし、一つ以上が検証されない。

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：

- 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” P-256, P-384, and [selection: P-521, no other curves]; 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、 [選択：SHA-256、SHA-512]に従い、[ISO/IEC 10118-3:2004] を満たすような[暗号ハッシュサービス**]**を実行しなければならない。

適用上の注釈：*ハッシュ選択は、FCS_KYC_EXT.1.2 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。(SHA256 は AES 128 bit 鍵用に選択されるべきであり、SHA 512 は AES 256 bit 鍵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、以下を満たす、[鍵付ハッシュメッセージ認証] を[選択： HMAC-SHA-256, HMAC-SHA-512] 及び暗号鍵長[割付: HMAC で使用される鍵長(bits)] に従って実行しなければならない：[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 に定義されている。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。*

A.2　Class：TSF の保護 (FPT)

FPT_TST_EXT.1　拡張： TSF テスト

FPT_TST_EXT.1.1 TSF は、TSF の正しい動作を実証するために、[選択：*初期起動中（電源投入時）に、機能が最初に呼び出される前に*] 、一連の自己テストを実行しなければならない。

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場合に限って、延期することができる。*

FCS_RBG_EXT.1 が、 NIST SP 800-90 に従って TOE に実装されている場合、評価者は、NIST SP800-90 の section 11.3 と一貫するヘルステストについて TSS が記述していることを検証しなければならない。

FCS_COP 機能のいずれかが TOE に実装されている場合、TSS はそれらの機能の既知解自己テストについて記述しなければならない。

評価者は、TSF の正しい動作に影響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。 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。

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 または基礎となる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。

附属書 A に特定されるそれらの要件と同様に、ST 作成者は、ST 本文へ引用されたオプション及び選択ベースの要件に依存して、それらが正しく繰り返し番号を整合していることを保証しなければならない。

(T.AUTHORIZATION_GUESSING) 脅威エージェントは、パスワードやPIN (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.1.1, FCS_VAL_EXT.1.2, FCS_VAL_EXT.1.3]

根拠：有効なBEV [FCS_VAL_EXT.1.1]のみがEE [FCS_VAL_EXT.1.2]へ送られる。検証試行の失敗の対応 [FCS_VAL_EXT.1.3] は、許可要素推定の成功の脅威を低減する。

B.1 クラス：暗号操作 (FCS)

FCS_COP.1(d)　暗号操作 (鍵ラッピング)

FCS_COP.1.1(d) 詳細化：TSF は、[鍵ラッピング]を、特定された暗号アルゴリズム [AES] に従い、[選択：KW, KWP, GCM, CCM]のモード及び暗号鍵長[選択：128 bits、256 bits]で[ISO/IEC 18033-3 (AES)、[選択：NIST SP 800-38F、ISO/IEC 19772]]を満たすように、実行しなければならない。

適用上の注釈：*ST 作成者が FCS_KYC_EXT.1 で規定する鍵チェインにおける鍵ラッピングを使用するよう選択する場合、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、以下を満たす、以下のモード[選択：KTS-OAEP, KTS-KEM-KWS]及び暗号鍵長[選択：2048, 3072] で特定された暗号アルゴリズム [RSA] に従って、[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中で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)　TSF は、以下を満たす、[選択：CBC, GCM, XTS]モード及び暗号鍵長[選択：128 bits、256 bits]を用いて、特定された暗号アルゴリズム AES に従って、[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、[選択： ISO/IEC 10116 で特定される CBC、ISO/IEC 19772 で特定される GCM、IEEE 1619 で特定される XTS]　で特定される AES]。

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 ー 例えば、256-bit 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-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(d)　**詳細化**： TSF は、以下を満たす、以下のモード [選択：CBC、GCM]]及び暗号鍵長　[選択：128 bits, 256 bits]を用いて、特定された暗号アルゴリズム AES に従って、[鍵暗号化と復号]を実行しなければならない：[ISO /IEC 18033-3、[選択： ISO/IEC 10116 で特定される CBC、ISO/IEC 19772 で特定される GCM]　で特定される AES]。

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の一部として、鍵を保護するために AES 暗号化／復号を選択する場合、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 で特定されたとおり 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)で特定された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。

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鍵導出（KDF）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。*

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

FCS_RBG_EXT.1　拡張：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。
FCS_RBG_EXT.1.2　決定論的 RBG 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：*128bits*、*256bits*]のエントロピーを、[選択：*[割付：ソフトウェアベースのノイズ源の数]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]のハードウェアベースのノイズ源*]から収集するような、少なくとも１つのエントロピー源によってシード値が与えられなければならない。

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、基礎となる暗号プリミティブ(ハッシュ関数／暗号)に依存している。ST 作成者は、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基礎となる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-224, SHA-256, SHA-384, 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 での 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 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。*

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のパスワードは、**[割付：64 ケタ以上の正の整数]**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]**}からなる文字が有効でなければならない、かつ**[NIST SP 800-132]**を満たす、特定された暗号アルゴリズム**[HMAC-[選択： SHA-256, SHA-384, SHA-512]]**に従って、[**割付：1000 以上の正の整数**]回繰り返し、暗号鍵長[**選択： *128, 256***]を出力するように**[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。

適用上の注釈： *パスワードは、ホストマシンにおいてTOE 及び基礎となる OS に依存するコード化された文字のシーケンスとして表される。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ビット列へ調整されて与えられなければならない。調整は、識別されたハッシュ関数または NIST SP800-132 で定義されるプロセスの一つ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 による調整が特定される場合、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。*

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。

C.1 背景と適用範囲

本書は、*ドライブ全体暗号化のため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*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：

FCS_AFA_EXT.1	許可要素取得
FCS_KYC_EXT.1	鍵チェイニング
FCS_PCC_EXT.1	暗号パスワードの生成と調整
FCS_CKM_EXT.4	暗号鍵及び鍵材料の破棄
FCS_SNI_EXT.1	暗号操作（ソルト、ノンス、及び初期化ベクタ）
FPT_KYP_EXT.1	拡張：鍵及び鍵材料の保護
FPT_TUD_EXT.1	高信頼アップデート
FCS_SMC_EXT.1	サブマスク結合
FCS_VAL_EXT.1	検証
FPT_TST_EXT.1	拡張：TSF テスト
FCS_KDF_EXT.1	暗号鍵の導出
FCS_RBG_EXT.1	拡張：暗号操作（乱数ビット生成）

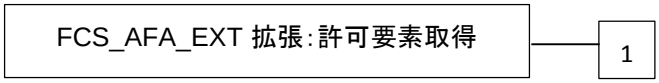
C.2 拡張コンポーネント定義

許可要素取得 (FCS_AFA_EXT)

ファミリのふるまい

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

コンポーネントのレベル付け



FCS_AFA_EXT.1 拡張：許可要素取得は、TOEによって受けるけられる許可要素を要求する。

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。

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： [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、**
- **RSA (鍵長 2048 以上) を用いて保護された、(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保護している、少なくとも DEK と同じビット長である、外部のスマートカードの要素、**
- **RSA (鍵長 2048 以上) を用いて保護された、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保護している、少なくとも DEK と同じビット長である、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 を用いている、TOE により生成されるサブマスクを提供しており、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**

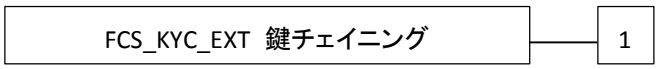
]。

鍵チェイニング (FCS_KYC_EXT)

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 鍵チェイニングは、TSF が鍵チェインを維持し、そのチェインの特性を特定することを要求する。

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。

FCS_KYC_EXT.1　鍵チェイニング

下位階層：なし

依存性：なし

FCS_KYC_EXT.1.1 TSF は、[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 BEV へ 1 つ以上のサブマスクから生成する中間鍵：[選択： 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_SMC_EXT.1 で特定された鍵結合 (key combining)、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]]の鍵チェインを維持しなければならない。ここで、[選択： 128bits、256bits]の有効な強度を維持すること。

FCS_KYC_EXT.1.2 TSF は、EE へ[選択：128bits、256bits]の BEV を [選択：FCS_VAL_EXT.1 で特定されたように TSF が検証プロセスを実行して成功した後に限り、検証を実行することなしに] 提供しなければならない。

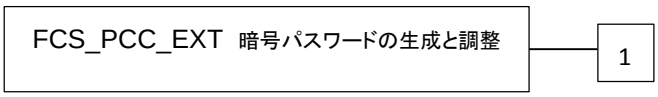
適用上の注釈:鍵チェイニングは、BEV（境界暗号化値）を最終的にセキュアにするために多階層の暗号鍵を用いる方法である。中間鍵の数は、一 1つ（例えば、調整されたパスワード許可要素を用いたり、それを直接BEVとして用いたりするように）から数多くまでさまざまである。これは、最終的なラッピング、またはBEVの導出に寄与するすべての鍵に適用される;保護されたストレージの領域におけるそれらを含めて（例えば、TPM保存の鍵、比較用の値）を含めて適用される。

暗号パスワードの生成と調整 (FCS_PCC_EXT)

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のパスワードは、[割付: 64 ケタ以上の正の整数]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]}からなる文字が有効でなければならない、かつ[PBKDF 勧告または仕様（訳注：PP で使用されている SFR では、「NIST SP 800-132」となっている）] を満た

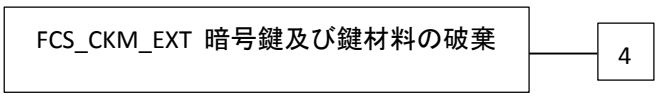
す、特定された暗号アルゴリズム[HMAC-[選択： SHA-256、 SHA-384、 SHA-512]]に従って、[割付：1000 以上の正の整数]回の繰り返し、暗号鍵長[選択： *128, 256*]を出力するように[パスワードベースの鍵導出関数]を実行しなければならない。

暗号鍵管理 (FCS_CKM)

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。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。本ファイミリは、暗号鍵の管理のための機能要件がある限り含まれなければならない。

コンポーネントのレベル付け



FCS_CKM_EXT.4 暗号鍵及び鍵材料破棄は、FCS_CKM.4 配下の拡張コンポーネントであり、鍵破棄のタイミングについての要件を含んでいる。

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。

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

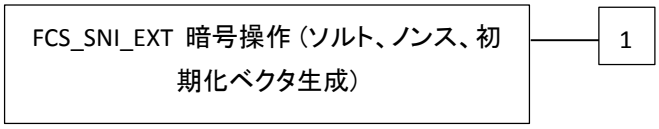
FCS_CKM_EXT.4 TSF は、すべての鍵及び鍵材料がもはや不要となったとき、それらを破棄しなければならない。

暗号操作（ソルト、ノンス、及び初期化ベクタの生成 (FCS_SNI_EXT)

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。

FCS_SNI_EXT.1.2 TSF は、最小 [64]bits のユニークなノンスのみを使用しなければならない。

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：[

- **CBC：IV は、繰り返してはならない。**
- **CCM：ノンスは、繰り返してはならない。**
- **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。**
- **GCM：IV は、繰り返してはならない。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。**

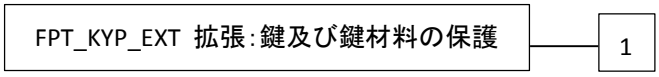
]

鍵及び鍵材料の保護 (FPT_KYP_EXT)

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 拡張：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。

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。

FPT_KYP_EXT.1　拡張：鍵及び鍵材料の保護

下位階層：なし

依存性：なし

FPT_ KYP _EXT.1.1 TSF は、鍵が以下の基準：[選択：

- **FCS_KYC_EXT.2 で特定されたとおり鍵 チェイン の一部でない平文の鍵。**
- **初期設定の後、もはや暗号データへアクセスが提供されない平文の鍵。**
- **平文の鍵が FCS_SMC_EXT.1 で特定されたとおり結合された分散鍵であり、もう半分の分散鍵は[選択：FCS_COP.1(d)で特定されたとおりラップされるか、FCS_COP.1(g) または FCS_COP.1(e) で特定されたとおり暗号化される、または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上に格納される。**
- **平文の鍵は、既に[選択：FCS_COP.1(d)で特定されたとおり鍵ラップされている、FCS_COP.1(g) または FCS_COP.1(e) で特定されたとおり暗号化されている］鍵を、[選択：FCS_COP.1(d)で特定されたとおり鍵をラップする、FCS_COP.1(g) または FCS_COP.1(e) で特定されたとおり暗号化する］ために使用される。**

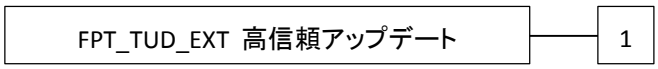
］のいずれかを満たさない限り、FCS_COP.1(d)で特定されたとおりラップされるか、または FCS_COP.1(g)で特定されたとおり暗号化されるときのみ、不揮発性メモリに鍵を格納しなければならない。

高信頼アップデート (FPT_TUD_EXT)

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、[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る能力を提供しなければならない。

FPT_TUD_EXT.1.2 TSF は、[許可された利用者に] TOE 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。

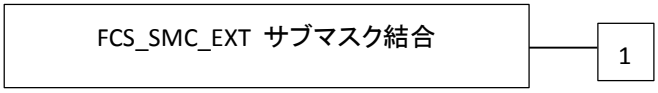
FPT_TUD_EXT.1.3 TSF は、アップデートをインストール前に製造者による[ディジタル署名]を用いて TOE ファームウェアへのアップデートを検証しなければならない。

サブマスク結合 (FCS_SMC_EXT)

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結合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 サブマスク結合は、TSF が予測可能な方法でサブマスクを結合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　サブマスク結合

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、中間鍵またはBEVを生成するため、以下の方法 [選択：排他的論理和 (XOR)、 SHA-256、 SHA-512] を用いて、サブマスクを結合しなければならない。

暗号エレメントの検証 (FCS_VAL_EXT)

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。

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。

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(d) 暗号操作 (鍵ラッピング)

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：[選択： FCS_COP.1(d)にて特定された鍵ラップ、[選択： FCS_COP.1(b), FCS_COP.1(c)]で特定されるとおり[選択：サブマスク、中間鍵、 BEV] をハッシュして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)で特定されるとおり[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] を用いて実行しなければならない。

FCS_VAL_EXT.1.2 TSF は、検証が発生した後にのみ、BEV を EE へ送信しなければならない。

FCS_VAL_EXT.1.3 TSF は、[選択：設定可能な連続する検証失敗の試行回数によって DEK の鍵廃棄処理を EE へ発行、24 時間で発生しうる[割付: ST 作成者が特定した回数の試行] 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 作成者が特定した試行回数]に達した後に検証を阻止]しなければならない。

TSF 自己テスト (FPT_TST_EXT)

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 拡張：TSF 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

以下のアクションは、FMT における管理機能と考えられる：

管理機能なし。

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　拡張：TSF テスト

下位階層：　なし.

依存性：　　なし.

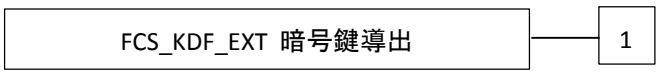
FPT_TST_EXT.1.1 TSF は、TSF の正しい動作を実証するために、以下の自己テスト一式を[選択：初期起動中（電源投入時）に、機能が最初に起動される前に] 実行させなければならない。

鍵導出 (FCS_KDF_EXT)

ファミリのふるまい

本ファミリは、特定されたサブマスク一式から中間鍵が導出されるような手段を特定する。

コンポーネントのレベル付け



FCS_KDF_EXT.1 暗号鍵導出は、特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 TSF に要求する。

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)

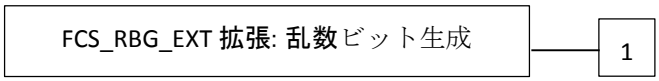
FCS_KDF_EXT.1.1 TSF は、出力が少なくとも BEV と等しいセキュリティ強度（ビット数で）となるように、 [選択：FCS_RBG_EXT.1 で特定されたとおり RNG が生成したサブマスク, 調整されたパスワードサブマスク、インポートされたサブマスク]を [選択：NIST SP 800-108 [選択：カウンターモードを用いた KDF、フィードバックモードを用いた KDF、ダブルパイプライン繰り返しモードを用いた KDF]、NIST SP 800-132] の定義に従って、FCS_COP.1(c)で特定された鍵付ハッシュ関数を用いて中間鍵を導出するために受け入れなければならない。

乱数ビット生成 (FCS_RBG_EXT)

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

以下のアクションは、FMT における管理機能と考えられる：

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：

最小：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。

FCS_RBG_EXT.1.2　決定論的 **RBG** 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：***128bits***、***192bits, 256bits***］のエントロピーを、**[選択：*ソフトウェアベースのノイズ源、ハードウェアベースのノイズ源*]**（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：*[割付：ソフトウェアベースのノイズ源の数]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]のハードウェアベースのノイズ源*］とすべき）から収集するような、少なくとも１つのエントロピー源によってシード値が与えられなければならない。

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、基礎となる暗号プリミティブ（ハッシュ関数／暗号）に依存している。ST 作成者は、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基礎となる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。

附属書 D：エントロピーに関する文書及び評定

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。

本附属書は、TOE によって使用される各エントロピー源に要求される補足情報を記述する。

エントロピー源に関する文書は、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。その文書には、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。その文書は、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

文書には、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。

文書には、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。その文書では、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 出力を使う複数の用途に対して、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なぜ確信できるのかについての技術的な議論が存在すべきである。この議論には、期待される最小エントロピー割合(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))の記述と、十分なエントロピーが TOE の攪拌シード生成処理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、なぜ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割合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、最小エントロピー割合を正当化するため、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割合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。

サードパーティが提供す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、文書にはこのサードパーティ情報源から取得される最小エントロピー割合の見積りが示されること。ベンダが最小エントロピー割合を「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文書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、その想定が 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 に示されるエントロピーで DRBG が初期化される方法が含まれること。例えば、最小エントロピー割合に 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割合が明示的に示され、統計学的な量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く、または計算された量が明示的にシードと関連付けられていない場合、文書化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、再起動の間で保存される状態からの追加データも、一切含めてはならない。

D.3 動作条件

エントロピー割合は、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、文書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記述されることになる。同様に、文書にはエントロピー源が十分なエントロピーを供給するとは、もはや保証されない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、またはオンデマンド)、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いう確信を示す根拠を含むこと。

附属書 E：鍵管理記述

製品の暗号鍵管理の文書化は十分詳細であるべきで、読んだ後、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。その文書には、解説と図を含むべきである。その文書は、TSS の一部とすることを要求されず 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のかどうかについて、その正当化と共に。

解説文には、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) や結合 (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処理に注目して、検証処理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処理において弱体化または暴露されないことをこの処理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処理。このセクションは、製品によって使用される鍵チェインの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、鍵ラップ、または 2 つの要件の結合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対話する値、及びそれらの値が鍵チェインの全体の強度を危殆化または暴露しないことを保証する保護についても含まなければならない。
- 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。
- データ暗号エンジンの記述、その構成要素、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 (訳注：ASIC) または別チップのコ

プロセッサ内に集積されたもの、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媒体へのデータフロー、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領域への読み書き動作)についても含めるべきである。記述は、いつ利用者が暗号化を有効化するか、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かを保証するために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、暗号初期化処理、及びどのようなとき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。

- すべての鍵の保存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することにより、鍵がもはや不要となった時に鍵を破棄するための処理。

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プを解くために使用される入力を示すべきである。
- 主な構成要素（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媒体、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構成要素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（鍵廃棄処理）	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廃棄処理する方法。
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）
SFR	Security Functional Requirements（セキュリティ機能要件）

頭字語	意味
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（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.