Supporting Document
必須技術文書

ドライブ全体暗号化: 暗号エンジン

2016 年 9 月

バージョン 2.0

CCDB-2016

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

序文

本書は、IT セキュリティ評価のための共通基準バージョン 3 及び関連の共通評価方法を補足することを意図したサポート文書である。

サポート文書は、サポート文書の適用が相互承認上必須でない分野に対する具体的なアプローチと規格の適用に注目した、それ自体が規格としての性質を持たない「ガイダンス文書」であってもよいし、またはサポート文書の適用範囲によりカバーされる評価において、その適用が必須とされるような「必須技術文書」であってもよい。後者の使用法は必須であるだけでなく、それらの適用の結果として発行される認証書は CCRA の下で承認される。

本サポート文書は、*Full Drive Encryption iTC（ドライブ全体暗号化 iTC）* により開発されたものであり、セクション 1.1 で識別される cPP に適合する製品の評価をサポートするために使用されるよう設計されている。

テクニカルエディタ：

FDE iTC

文書履歴：

V0.7, 2014 年 9 月 (公開レビューのための初期リリース)

V0.11, 2014 年 10 月 (公開レビューからのコメントへ対応、CCDB へ送付)

V1.0 2015 年 1 月 (CCDB からのコメントへ対応)

V1.5 2015 年 9 月 (cPP の最新改訂版を反映するためのアップデート)

V2.0 2016 年 9 月 (受け付けたコメントを反映するためのアップデート)

目的：

FDE 技術分野は、その物理的範囲及び限定された外部インタフェースに起因して特殊である。これにより、TOE の提供するセキュリティ機能の実装の正確さの評価において、いくつかの困難に直面している。暗号エンジンの場合、TSF が利用者データを適切に暗号化していることを実証するためのインタフェースを刺激することは困難かもしれない。したがって、評価方法は、どのようにしてこのチャレンジに打ち勝つかについて（その他と同じように）、本書では、比較可能で、透明性があり、再現可能な方法で、記述されなければならない。

さらに、FDE の主たる機能は、ドライブ上の暗号化された形式で利用者データを保存することである。実装された暗号メカニズムの比較可能、透明で再現可能な評価を保証するため、評価方法は合意された評価アプローチから構成されるように記述されなければならない、例えば、主張された利用者データの暗号化が TOE によって本当に実行されたかを証明する方法、または利用者データが暗号化された形でのみ保存されていることを証明する方法（及びさらに平文では保存されない）、しかし必要となるかもしれない特殊なテストツール及びそのマニュアルの定義も含む。

特殊用途分野：

ドライブ全体暗号化デバイス、特に暗号エンジンコンポーネントに関連するセキュリティ機能要件集。

謝辞：

本サポート文書は、産業界、政府機関、コモンクライテリア評価機関、及び学術会員からの代表者の参加するドライブ全体暗号化国際的技術部会（iTC）により開発された。

目次

1 序説 5

1.1 技術分野、及びサポート文書の適用範囲 5

1.2 本書の構成 6

1.3 用語 6
1.3.1 用語集 6
1.3.2 頭字語 8

2 SFR に関する評価アクティビティ 10

2.1 暗号サポート (FCS) 11
2.1.1 暗号鍵管理 (FCS_CKM) 11
2.1.2 暗号鍵管理 (FCS_CKM_EXT) 12
2.1.3 鍵チェイニング (FCS_KYC_EXT) 13
2.1.4 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成) 14
2.1.5 暗号エレメントの検証 (FCS_VAL_EXT) 15

2.2 利用者データ保護 (FDP) 16
2.2.1 ディスク上のデータ保護 (FDP_DSK_EXT.1) 16

2.3 セキュリティ管理 (FMT) 18
2.3.1 管理機能の特定 (FMT_SMF) 18

2.4 TSF の保護 (FPT) 19
2.4.1 鍵及び鍵材料の保護（FPT_KYP_EXT) 19
2.4.2 電力管理 (FPT_PWR_EXT) 20
2.4.3 TSF テスト (FPT_TST_EXT) 21
2.4.4 高信頼アップデート (FPT_TUD_EXT) 22

3 オプション要件の評価アクティビティ 23

3.1 暗号サポート (FCS) 23
3.1.1 暗号鍵管理 (FCS_CKM) 23

3.2 TSF の保護 (FPT) 23
3.2.1 ファームウェアアクセス制御 (FPT_FAC_EXT) 23
3.2.2 ロールバック保護 (FPT_RBP_EXT) 24

4 選択ベース要件の評価アクティビティ 25

4.1 暗号サポート(FCS) 25
4.1.1 暗号鍵管理 (FCS_CKM) 25
4.1.2 暗号操作 (FCS_COP) 37
4.1.3 暗号鍵導出 (FCS_KDF_EXT) 48
4.1.4 乱数ビット生成 (FCS_RBG_EXT) 49
4.1.5 サブマスクコンバイニング (FCS_SMC_EXT) 50

4.2 TSF の保護 (FPT) **51**
4.2.1 ファームウェアアップデート検証 (FPT_FUA_EXT) 51

5 SAR の評価アクティビティ **52**

5.1 ASE: セキュリティターゲット評価 **52**
5.1.1 適合主張 (ASE_CCL.1) 52

5.2 ADV: 開発 **52**
5.2.1 基本機能仕様 (ADV_FSP.1) 52

5.3 ガイダンス文書 (AGD) **55**
5.3.1 利用者操作ガイダンス (AGD_OPE.1) 55
5.3.2 準備手続き (AGD_PRE.1) 56

5.4 ALC: ライフサイクルサポート **57**
5.4.1 TOE のラベル付け (ALC_CMC.1) 57
5.4.2 TOE の CM 範囲 (ALC_CMS.1) 57

5.5 テスト (ATE) **57**
5.5.1 独立テスト – 適合 (ATE_IND.1) 57

5.6 脆弱性評定 (AVA) **59**
5.6.1 脆弱性調査 (AVA_VAN.1) 59

6 必須の補足情報 **63**

7 参考文献 **64**

A 脆弱性分析 **66**

A.1 脆弱性情報源 **66**
A.1.1 タイプ 1 仮説—公開脆弱性ベース 66
A.1.2 タイプ 2 仮説—iTC 出典のもの 67
A.1.3 タイプ 3 仮説—評価チームによって生成されたもの 68
A.1.4 タイプ 4 仮説—ツールによって生成されたもの 68

A.2 評価者脆弱性分析のプロセス **68**

A.3 報告 **70**

B. FDE 同等性検討 **72**

1 序説

1.1 技術分野、及びサポート文書の適用範囲

1 *ドライブ全体暗号化 (FDE：Full Drive Encryption)：許可取得 (AA：Authorization Acquisition) 及び暗号エンジン (EE：Encryption Engine)* のコラボラティブプロテクションプロファイル(cPP)の初版の目的は、紛失したドライブ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、ソフトウェア及び／またはハードウェアに基づく FDE ソリューションが要件を満たすことを可能にする。ストレージデバイスについての形式ファクタは、多様かも知れないが、以下のようなものを含めることができる：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、及び外部メディアに搭載されたシステムハードドライブ／ソリッドステートドライブ（SSD）。ハードウェアソリューションは Self-Encrypting Drive（SED：自己暗号化ドライブ）またはその他のハードウェアベースのソリューション；ストレージデバイスをホストマシンへ接続するために使用されるインタフェース（USB、SATA 等）は、適用範囲外である。

2 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（特定の例外はあるが）を暗号化し、FDE ソリューションへの許可（Authorization）が成功した後のみ、データへのアクセスを許可する。その例外には、マスターブートレコード（MBR）やその他の AA/EE 事前認証ソフトウェアのようなものについては暗号化されないストレージデバイスの部分（サイズは実装により変わるかもしれない）として残す必要があるものが含まれる。これらの FDE cPP は、「ドライブ全体暗号化」という用語を平文の利用者データや平文の許可データを一切含まない限り、ストレージデバイスの一部分が暗号化されないまま残すことを FDE ソリューションに許容すると解釈する。

3 The *FDE cPP - Encryption Engine （FDE cPP - 暗号エンジン）* は、暗号エンジン部分のための要件及び DEK による実際のデータ暗号化／復号についての必要な保証アクティビティを詳述する。各 cPP には、管理機能、暗号鍵の適切な取り扱い、信頼されるやり方で行われるアップデート、セキュリティ監査及び自己テストのための一連の中核的な要件も含まれる。

4 本サポート文書は以下の cPP への適合を主張する TOE 評価に必須なものである：

5 a) 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。

6 評価アクティビティは、主に評価者が従うものとして定義されるが、一般的に開発者が、その TOE の具体的な要件を識別することにより、評価の準備に役立てることにもなるだろう。評価アクティビティの具体的な要件では、SFR の意味を明確化し、またセキュリティターゲット（特に TOE 要約仕様）、利用者ガイダンス証拠資料、及びおそらく補足情報（例、エントロピー分析、または暗号鍵管理アーキテクチャ等）の内容についての具体的な要件を特定するかもしれない。

1.2 本書の構成

1 評価アクティビティは、セキュリティ機能要件とセキュリティ保証要件の両方について定義することができる。これらは、本サポート文書の別々のセクションで定義されている。

2 いずれかの評価アクティビティが評価中に成功裏に完了できなかった場合、その評価の総合判定は、「不合格」となる。まれな場合、評価アクティビティが修正され、または特定の TOE には適用できないと考えられるような、受け入れ可能な理由があるかもしれないが、このような場合には、その評価に関して認証機関との合意がなされなければならない。

3 一般的には、すべての評価アクティビティ（SFR 及び SAR の両方に関して）が評価で成功裏に完了した場合、評価の総合判定は「合格」となる。評価が成功裏に完了した時に「不合格」判定となるためには、その TOE について、評価アクティビティがなぜ不十分であるかの理由について評価者からの具体的な正当化が必要とされる。

4 同様に、より粒度の細かい保証コンポーネントのレベルにおいて、ある保証コンポーネントについての評価アクティビティ及びそれに関連する SFR の評価アクティビティのすべてが評価中に成功裏に完了した場合、その保証コンポーネントについての判定は「合格」となると期待される。これらの評価アクティビティが成功裏に完了した時にその保証コンポーネントについて「不合格」の判定となるためには、その TOE について、評価アクティビティがなぜ不十分であるかの理由について評価者からの具体的な正当化が必要とされる。

1.3 用語

1.3.1 用語集

5 標準の CC 用語の定義については 、[CC] パート 1 を参照すること。

6 **補足情報** —セキュリティターゲットまたは操作ガイダンスに必ずしも含める必要のない情報で、公開される必要がないかもしれないもの。このような情報の例としては、エントロピー分析、または TOE で (またはそのサポートにおいて) 使用される暗号鍵管理アーキテクチャについての記述であろう。そのような補足情報に関する要件は、関連の cPP で識別される（セクション 4 を参照されたい）。

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ための根拠 [CC1].

用語	意味
Border Encryption Value （境界暗号化値、BEV と略す）	AA から EE へ渡される値で、２つのコンポーネントの鍵チェインを繋ぐことを意図したもの。
Key Sanitization （鍵のサニタイゼーション）	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) （データ暗号化鍵）	保存データを暗号化するために使用された鍵。
Full Drive Encryption （ドライブ全体暗号化）	利用者がアクセスできるデータの論理ブロックのパーティションへの参照で、これらのパーティションのブロックへデータの読み出しまたは書き込みのための権限を写像するオペレーティングシステムのようなホストシステムによって インデックス、パーティションが管理されたもの。 本 SPD 及び cPP のために、FDE はひとつのパーティションの暗号化と権限管理を実行する。OS 及びファイルシステムによる定義及びサポートについては検討中である。 FDE 製品はストレージデバイスのパーティション上のすべてのデータ（特定の例外はある）を暗号化し、FDE ソリューションへの権限付与が成功した後にデータへのアクセスを許可する。例外として、マスターブートレコード（MBR）またはその他の AA/EE 事前認証ソフトウェアとして暗号化されないようなストレージデバイスの一部（サイズは実装に依存して変わるかもしれない）が含まれる。これらの FDE cPP は「ドライブ全体暗号化」という用語を、保護されないデータが含まれていないとして暗号化されていないストレージデバイスの部分を残してはいるが FDE ソリューションを許容するように解釈する。
Intermediate Key （中間鍵）	初期の利用者権限付与と DEK の間で使用される鍵。
Host Platform（ホストプラットフォーム）	TOE が実行しているローカルのハードウェア及びソフトウェアで、ローカルのハードウェア及びソフトウェアに接続されうる周辺のデバイス（USB デバイス等）を含まないもの。
Key Chaining （鍵チェイン）	データを保護するための複数階層の暗号鍵を用いる方法；この方法は任意の階層を持つことができる。
Key Encryption Key (KEK) （鍵暗号化鍵）	DEK または鍵を含むストレージのような、その他の暗号鍵を暗号化するために使用された鍵。
Key Material （鍵材料）	鍵材料は、重要セキュリティパラメタ（CSP）として知られ、認証データ、ノンス、メタデータも含まれる。
Key Release Key (KRK) （鍵解放鍵）	ストレージから別の鍵をリリースするために使用される鍵で、別の鍵の直接導出または復号には使用されない。
Operating System (OS) （オペレーティングシステム、基本システム）	最高の特権レベルで動作するソフトウェアで、直接ハードウェア資源を制御できるもの。
Non-Volatile Memory （不揮発性メモリ）	電源なしで情報を保持するコンピュータメモリーの一種。
Powered-Off State （電源オフ状態）	デバイスがシャットダウンしている状態。

用語	意味
Protected Data （保護されたデータ）	これはストレージデバイス上のすべてのデータへの参照で。TOE として正常に機能することが要求される小さな部分を除いたもの。OS,アプリケーション、利用者データを含め、利用者がデータを書き込みできるディスク上のすべての空間。保護されたデータは、暗号化されない必要のあるマスターブートレコードまたはドライブの事前認証領域を含まない。
Submask （サブマスク）	サブマスクは、いくつかの方法で生成され、保存されるビット列である。
Target of Evaluation （評価対象）	ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び／またはハードウェアのセット。[CC1]

1.3.2 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（暗号ブロック連鎖）
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（決定論的ランダムビット生成器）
DSS	Digital Signature Standard （デジタル署名規格）
ECC	Elliptic Curve Cryptography （楕円曲線暗号）
ECDSA	Elliptic Curve Digital Signature Algorithm（楕円曲線デジタル署名アルゴリズム）
EE	Encryption Engine（暗号エンジン）
EEPROM	Electrically Erasable Programmable Read-Only Memory （電気的消去可能プログラマブル ROM）
FIPS	Federal Information Processing Standards（連邦情報処理規格）
FDE	Full Drive Encryption(ドライブ全体暗号化)
FFC	Finite Field Cryptography（有限体暗号）
GCM	Galois Counter Mode（ガロアカウンターモード）
HMAC	Keyed-Hash Message Authentication Code（鍵付ハッシュメッセージ認証コード）
IEEE	Institute of Electrical and Electronics Engineers（アメリカ電気電子通信学会）
IT	Information Technology（情報技術）
ITSEF	IT Security Evaluation Facility（IT セキュリティ評価機関）
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission（国際標準化機構／国際電気標準会議）
IV	Initialization Vector（初期化ベクタ）
KEK	Key Encryption Key（鍵暗号化鍵）
KMD	Key Management Description（鍵管理記述）
KRK	Key Release Key（鍵解放鍵）
MBR	Master Boot Record（マスターブートレコード）

NIST	National Institute of Standards and Technology（アメリカ国立標準技術研究所）
OS	Operating System（オペレーティングシステム、基本システム）
RBG	Random Bit Generator（ランダムビット生成器）
RNG	Random Number Generator（乱数生成器）
RSA	Rivest Shamir Adleman Algorithm（リベスト・シャミア・エーデルマン（RSA）アルゴリズム）
SAR	Security Assurance Requirement（セキュリティ保証要件）
SED	Self Encrypting Drive（自己暗号化ドライブ）
SHA	Secure Hash Algorithm（セキュアハッシュアルゴリズム）
SFR	Security Functional Requirement（セキュリティ機能要件）
SPD	Security Problem Definition（セキュリティ課題定義）
SPI	Serial Peripheral Interface（シリアルペリフェラルインタフェース）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TPM	Trusted Platform Module（高信頼プラットフォームモジュール）
TSF	TOE Security Functionality（TOE セキュリティ機能）
TSS	TOE Summary Specification（TOE 要約仕様）
USB	Universal Serial Bus（ユニバーサルシリアルバス）
XOR	Exclusive or（排他的論理和）
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing

2 SFR の評価アクティビティ

7 本セクションで提示される EA は、特定の SAR (例、ASE_TSS.1、ADV_FSP.1、AGD_OPE.1 及び ATE_IND.1)をカバーする技術特有の側面に対処するために評価者が実行するアクションを集めたものであるーこれは、セクション 5 で実行されるような CEM ワークユニットへの追加である。

8 設計記述 (保護情報として取り扱われるかもしれない必須の補足資料と同様に、TSS という表題のサブセクションによって割り当てられている) に関して、評価者は、EA を満たすような具体的な情報があることを保証しなければならない(must)。TSS セクションに関する所見として、評価者の判定は、CEM ワークユニット ASE_TSS.1-1 に対応する。補足証拠に対応する評価者判定についても、この証拠を提供するための要件が cPP の ASE において規定されるので、ASE_TSS.1-1 に対応する。

9 ガイダンス証拠資料が SFR に関連するものとして、管理者／利用者に十分な情報を提供することを保証するため、評価者の判定は、CEM ワークユニット ADV_FSP.1-7、AGD_OPE.1-4、及び AGD_OPE.1-5 に対応する。

10 最後に、テストという表題のサブセクションは、iTC が対応する SFR の文章にて製品のテストが必要であることを決定するような場所である。評価者は、テストを開発することが期待されるが、開発者がテストを構築するためにより実際的であるような例であるかもしれないし、開発者が既存のテストを所持しているかもしれないような場所である。ゆえに、評価者が、そのテストを実行する代わりに開発者が生成したテストを目撃(立ち合い)することは受け入れ可能である。この場合、評価者は、開発者のテストがその開発者によって宣言されたやり方及び EA によって義務付けられたやり方の両方で実行していることを保証しなければならない(must)。本セクションで規定される EA に対応する CEM ワークユニットは、ATE_IND.1-3、ATE_IND.1-4、ATE_IND.1-5、ATE_IND.1-6、及び ATE_IND.1-7 である。

2.1 暗号サポート (FCS)

2.1.1 暗号鍵管理 (FCS_CKM)

2.1.1.1 FCS_CKM.1(c) 暗号鍵生成 (データ暗号化鍵)

2.1.1.1.1 TSS

11 評価者は、TOE が DEK を取得する方法 (DEK の生成、または環境から受領のいずれか) が TSS に記述されていることを決定するため、TSS を検査しなければならない(shall)。

12 TOE が DEK を生成する場合、評価者は FCS_RBG_EXT.1 に記述された機能が起動される方法について TSS に記述されていることを決定するため、TSS をレビューしなければならない(shall)。DEK が TOE の外部で生成される場合、評価者は TOE で識別された各プラットフォームについて、TSS にこの機能を起動するために TOE 画が使用するインタフェースについて記述されていることを保証するためにチェックすること。評価者は、要求された鍵長と等しいまたはそれ以上の長さの鍵を要求していることを決定するため、RBG と TOE の間のインタフェースの記述を使用すること。

13 TOE がホストプラットフォームの外から DEK を受け取る場合、評価者は、適切な暗号アルゴリズムを用いてラッピングされて DEK が送信されることを決定するため、TSS を検査しなければならない(shall)。

2.1.1.1.2 操作ガイダンス

14 本 SFR についての AGD 評価アクティビティは一切ない。

2.1.1.1.3 KMD

15 TOE がホストプラットフォームの外部から DEK を受け取る場合、評価者は、TOE が DEK をアンラッピングする方法が KMD に記述されていることを検証しなければならない(shall)。

2.1.1.1.4 テスト

16 評価者は、以下のテストを実行しなければならない(shall)：

17 テスト 1：評価者は、すべての選択の機能を保証するため、TOE を構成しなければならない(shall)。

2.1.1.2 FCS_CKM.4(a) 暗号鍵破棄 (電力管理)

2.1.1.2.1 TSS

18 評価者は、TSS が鍵及び鍵材料がもはや不要となることが何を意味するのか、及びいつ破棄されることが期待されるべきかについての上位レベルの記述を提供していることを検証しなければならない(shall)。

2.1.1.2.2 操作ガイダンス

19 評価者は、メモリ消去とその達成方法について TOE が運用環境に依存するかどうか、ガイダンス証拠資料をチェックしなければならない(shall)。

2.1.1.2.3 KMD

20 評価者は、KMD にそれぞれの鍵の種別、その起源、不揮発性メモリにおけるメモリ上の考えられる場所について列挙していることを保証するため、チェックしなければならない(shall)。

2.1.1.2.4 テスト

21 本 SFR のテスト評価アクティビティは、一切ない。

2.1.2 暗号鍵管理 (FCS_CKM_EXT)

2.1.2.1 FCS_CKM_EXT.4(a) 暗号鍵及び鍵材料破棄 (破棄タイミング)

2.1.2.1.1 TSS

22 評価者は、TSS が鍵及び鍵材料がもはや不要となることが何を意味するのか、及びいつ破棄されると期待されるべきかについての上位レベルの記述を提供していることを検証しなければならない(shall)。

2.1.2.1.2 操作ガイダンス

23 本 SFR についての AGD 評価アクティビティは、一切ない。

2.1.2.1.3 KMD

24 評価者は、KMD に、鍵及び鍵材料が存在する領域、及び鍵及び鍵材料が不要となる時期についての記述がふくまれていることを検証しなければならない(shall)。

25 評価者は、鍵材料がどこに存在しているか、鍵材料がどのように使用されるか、鍵及び鍵材料不要であることをどのようにして決定するか、及び必要でない材料がどのように一度に破棄されるかどうか、及び KMD での証拠資料が破棄に関して FCS_CKM.4(a) に従っていることについての記述を含むような鍵ライフサイクルが KMD に含まれていることを検証しなければならない(shall)。

2.1.2.1.4 テスト

26 本 SFR についてのテスト評価アクティビティは、一切ない。

2.1.2.2 FCS_CKM_EXT.4(b) 暗号鍵及び鍵材料破棄 (電力管理)

2.1.2.2.1 TSS

27 評価者は、適合省電力状態に入るとき、どの鍵及び鍵材料が破棄されるかについての記述を TSS が提供していることを検証しなければならない(shall)。

2.1.2.2.2 操作ガイダンス

28 評価者は、ガイダンス証拠資料に明確な警告及び TOE が適合省電力状態とは区別できるような非適合の省電力状態で終了するかもしれない条件についての情報を含んでいることを検証しなければならない(shall)。その場合、

このようなシナリオにおいてリスク低減のために何をすべきかについての指示を含まなければならない(must)。

2.1.2.2.3 KMD

29 評価者は、KMD に鍵及び鍵材料がどの領域に存在するかについての記述がふくまれていることを検証しなければならない(shall)。

30 評価者は、鍵材料がどこに存在しているか、鍵材料がどのように使用されるか、及び必要でない材料がどのように一度に破棄されるかどうか、及び KMD での証拠資料が破棄に関して FCS_CKM.4(b) に従っているかを含むような鍵ライフサイクルが KMD に含まれることを検証しなければならない(shall)。

2.1.2.2.4 テスト

31 本 SFR についてのテスト評価アクティビティは、一切ない。

2.1.2.3 FCS_CKM_EXT.6 暗号鍵破棄種別

2.1.2.3.1 TSS/KMD (鍵管理記述は、必要な詳細事項が保護情報を記述する場合に利用されるかもしれない)

32 評価者は、TSS/KMD における TOE の鍵チェインを検査、及び破棄対象のすべての鍵が規定された方法の一つに従って破棄されることを検証しなければならない(shall)。

2.1.2.3.2 操作ガイダンス

33 本 SFR のための AGD 評価アクティビティは、一切ない。

2.1.2.3.3 テスト

34 本 SFR のテスト評価アクティビティは、一切ない。

2.1.3 鍵チェイニング (FCS_KYC_EXT)

2.1.3.1 FCS_KYC_EXT.2 鍵チェイニング(受信側)

2.1.3.1.1 TSS

35 本 SFR の TSS 評価アクティビティは、一切ない。

2.1.3.1.2 操作ガイダンス

36 本 SFR の AGD 評価アクティビティは、一切ない。

2.1.3.1.3 KMD

37 評価者は、上位レベルの鍵階層及び鍵チェインの詳細が KMD に記述されていることを保証するため、KMD を検査しなければならない(shall)。鍵チェインの記述は、それが FCS_KDF_EXT.1, FCS_COP.1(d), FCS_COP.1(e), 及び／または FCS_COP.1(g)を満たす鍵ラッピングまたは鍵導出の方法を用いて、

鍵のチェインを維持していることを保証するため、レビューされなければならない(shall)。

38 評価者は、鍵チェインプロセスがどのように機能するか、例えば、任意の材料が暴露されないこと、鍵チェインにおいて任意の鍵が侵害されないことについて、KMD に記述されていることを保証するため、KMD を検証しなければならない(shall)。（例えば、TPM に対する比較値のように鍵を直接使用する等）本記述は、実装された鍵階層を説明する図やすべての鍵や鍵材料が保存される場所またはどこから導出されるかについての詳細を含まなければならない(must)。評価者は、チェインは暗号総当たりまたは初期許可の値なしでチェインが壊されることがないという点で、BEV の有効強度が鍵チェインの全体にわたって維持されていることを保証するため、鍵階層を検査しなければならない(shall)。

39 評価者は、鍵チェインの全体にわたる鍵の強度についての記述が KMD に含まれていることを検証しなければならない(shall)。

2.1.3.1.4 テスト

40 本 SFR のテスト評価アクティビティは、一切ない。

2.1.4 暗号操作 (ソルト、ノンス、及び初期化ベクタ生成)

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

2.1.4.1.1 TSS

41 評価者は、ソルトが生成される方法について TSS に記述されていることを保証しなければならない(shall)。評価者は、FCS_RBG_EXT.1 に記述されている RBG を用いて、または運用環境によって、ソルトが生成されていることを確認しなければならない(shall)。外部の機能が本目的のために使用される場合、入力を伴って呼び出される具体的な API が TSS に含まれるべきである(should)。

42 評価者は、ノンスが一意に生成される方法、及び IV と tweak が（AES モードに基づいて）取り扱われる方法について、TSS に記述されていることを保証しなければならない(shall)。評価者は、ノンスが一意であること、IV と tweak が記述された要件を満たすことを確認しなければならない(shall)。

2.1.4.1.2 操作ガイダンス

43 本 SFR の AGD 評価アクティビティは、一切ない。

2.1.4.1.3 KMD

44 本 SFR の KMD 評価アクティビティは、一切ない。

2.1.4.1.4 テスト

45 本 SFR のテスト評価アクティビティは、一切ない。

2.1.5 暗号エレメントの検証 (FCS_VAL_EXT)

2.1.5.1 FCS_VAL_EXT.1 検証

2.1.5.1.1 TSS

46 評価者は、どの許可要素が検証をサポートするかを決定するために TSS を検査しなければならない(shall)。

47 評価者は、複数のサブマスクが TOE 内で利用される場合、サブマスクが検証される方法 (例、各サブマスクはコンバイニングの前に検証される、一度コンバイニングされたときに検証が行われる) について、上位レベル記述をレビューするため、TSS を検査しなければならない(shall)。

48 評価者は、SFR で特定された許可要素のサブセットまたはすべてが適合省電力状態から抜け出るために利用可能であることを決定するために TSS についても検査しなければならない(shall)。

2.1.5.1.2 操作ガイダンス

49 [条件] 検証機能が設定可能である場合、評価者は、検証試行に関する制限が確立可能であることを保証するように TOE を設定する方法について記述されていることを保証するため、操作ガイダンスを検査しなければならない(shall)。

50 評価者は、ガイダンス証拠資料にどの許可要素が適合省電力状態から抜け出るために許可されるかについて記述していることを検証しなければならない(shall)。

2.1.5.1.3 KMD

51 評価者は、連続する失敗した権限付与試行回数を制限するために TOE が採用する方法について記述されていることを検証するため、KMD を検査しなければならない(shall)。

52 評価者は、検証が実行される方法について記述されていることを検証するため、ベンダの KMD を検査しなければならない(shall)。KMD における検証プロセスの記述は、TOE が BEV をどのように検証するかについての詳細な情報を提供すること。

53 KMD には、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しないように、そのプロセスが動作する方法について記述すること。

2.1.5.1.4 テスト

54 評価者は、以下のテストを実行しなければならない(shall) :

55 テスト 1 : 評価者は、連続する失敗した権限付与試行回数の平均率についての制限を決定しなければならない(shall)。評価者は、保護されたデータをアクセスするために連続する試行において不正な許可要素をその回数入力することによって TOE をテストすること。制限メカニズムに「ロックアウト」機関を含む場合、テストされる期間が少なくともこのような一つの期間を含むべきである。そして、評価者は、TSS に記述される通りに TOE がふるまうことを検証すること。

56 テスト 2：評価者は、適合省電力状態に TOE が入り、この状態からレジュームするよう試行し、ガイダンス証拠資料によって定義される通りの有効な許可要素のみが適合省電力状態を抜け出ることを TOE に許可するために十分でことを検証しなければならない(shall)。

2.2 利用者データ保護 (FDP)

2.2.1 ディスク上のデータ保護 (FDP_DSK_EXT.1)

2.2.1.1 FDP_DSK_EXT.1 ディスク上のデータ保護

2.2.1.1.1 TSS

57 評価者は、データがディスクへ書き込まれる方法及び暗号機能が適用される点において、記述が包括的であることを保証するために TSS を検査しなければならない(shall)。TSS は、ホストプラットフォームのオペレーティングシステム経由でディスクドライブをアクセスする標準的な方法 がこれらの機能を通して受け渡されるようにさせなければならない(shall)。

58 運用環境により提供される暗号機能について、評価者は、ST において識別された各インタフェースについて、この機能を起動するために TOE によって使用されるインタフェースについて TSS に記述されていることを保証するため、TSS をチェックしなければならない(shall)。

59 評価者は、本要件の評価アクティビティの実行に際して、TSS を検証しなければならない(shall)。評価者は、TOE がディスクドライブにデータを書き込む方法の確認、及び暗号機能が適用される点についての、記述の包括性を保証しなければならない(shall)。

60 評価者は、利用者または管理者が TOE を最初に設定するときに TOE の初期化及び TOE がストレージ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)。評価者は、暗号化されないディスクの領域（例、マスターブートレコード（MBR）、ブートローダ、パーティションテーブル等に関連する部分）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)。TOE が複数のディスク暗号化をサポートする場合、評価者は、初期化手続きがプラットフォーム上のすべてのストレージデバイスを暗号化することを保証するため、管理者ガイダンスを検査しなければならない(shall)。

2.2.1.1.2 操作ガイダンス

61 評価者は、任意の必要な準備ステップを含めて、FDE 関数を有効化するために必要な初期ステップについて AGD ガイダンスに記述されていることを決定するため、AGD ガイダンスをレビューしなければならない(shall)。ガイダンスは、暗号化が有効化されるときに、すべてのハードドライブデバイスが暗号化されることを保証するため、十分な指示を提供しなければならない(shall)。

2.2.1.1.3 KMD

62 評価者は、データ暗号化エンジン、そのコンポーネント、及びその実装 (例、ハードウェアについて：デバイスの主たる SOC（訳注：ASIC）または別の

コプロセッサ、ソフトウェアについて：デバイスの初期化、ドライバ、ライブラリ（適用可能であれば）、暗号化／復号のための論理インタフェース、暗号化されない領域（例、ブートローダ、秘密データを含まない部分、パーティションテーブル等）) についての詳細の記述が KMD に含まれることを検証しなければならない(shall)。評価者は、主たるコンポーネント（メモリやプロセッサ等）及びデータパスを示す機能的（ブロック）図、ハードウェアについてはデバイスのインタフェースやデバイスの永続的なデータ保存用のメディア、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の製品をセットアップする時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単に TOE が実行するアクティビティに必要な初期手順について、KMD が提供していることを検証しなければならない(shall)。ハードウェア暗号化の図は、データパス内のデータ暗号化エンジンの位置を示していなければならない(shall)。評価者は、ハードウェア暗号化の説明図にデータパス内の主たるコンポーネントを示す十分な詳細情報を含んでいること、及びデータ暗号化エンジンを明確に特定していることを検証しなければならない(shall)。

63 評価者は、暗号化が有効化される時、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についての十分な指示を KMD が提供していることを検証しなければならない(shall)。評価者は、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について KMD に記述されていることを検証しなければならない(shall)。評価者は、データがデータ暗号化エンジンを迂回（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出し−書き込み操作）するような条件に関する情報を KMD が提供していることを検証しなければならない(shall)。

64 評価者は、ブート初期化、暗号化の初期化プロセス、及び製品が暗号化を有効化する時についての記述を KMD が提供していることを検証しなければならない(shall)。評価者は、暗号化の初期化が完全に行われる前に、製品が秘密データの転送を許可しないことを検証しなければならない(shall)。評価者は、In-Band 方式（訳注：データフローと制御フローを同じ経路で流す方式）、Out-of-Band 方式（訳注：データフローと制御フローを別の経路で流す方式）のいずれかで、暗号化されたドライブの検査を可能とするような特殊なツール、及び既知の鍵で初期設定できてもよい特殊なツールをソフトウェア開発者が提供することを保証しなければならない(shall)。

2.2.1.1.4 テスト

65 評価者は、以下のテストを実行しなければならない(shall)：

66 テスト１：ランダムな場所にデータを書き込み、要求されたアクションを実行し比較する：

- TOE が初期化され、ハードウェアの場合、暗号エンジンが待機状態となることを保証する；
- ストレージデバイスを暗号化するように TOE を設定する。ソフトウェア暗号化製品、またはハイブリッド製品について、既知の鍵及び開発者のツールを使用する。
- 少なくとも64KBのランダムな文字パタンを決定する；
- 暗号化が有効になっているデバイス上の TOE の最下位及び最上位の論理アドレスにある情報を取り出す；

67 テスト２：ストレージデバイスの複数の場所にパタンを書き込む：

- ハードウェア暗号化について、デバイスの最下位から最上位までのアドレス範囲内のいくつかの場所をランダムに選択し、それらのアドレスにパタンを書き込む；
- ソフトウェア暗号化について、複数の論理アドレスに複数のファイルを用いてパタンを書き込む。

68 テスト３：データが暗号化されていることを検証する：

- ハードウェア暗号化について：
  - 新しい暗号化鍵の生成にデバイスの機能を用いる、ゆえに FCS_CKM.4(a) によって鍵の消去を実行する；
  - データが書き込まれたところと同じ場所から読み出す；
  - 取出したデータを書き込んだデータと比較し、一致しないことを保証する
- SW 暗号化について、開発者ツールを用いて；
  - ファイルが書き込まれたそれぞれの場所で平文のパタンについて暗号化されたストレージデバイスをレビューし、平文のパタンが見つからないことを確認する。
  - 既知の鍵を用いて、ファイルが書き込まれたそれぞれの場所を検証し、平文のパタンが鍵を用いて正しく復号できる。
  - 開発者ツールが利用可能な場合、暗号化領域に平文のファイルが人も存在しないことを検証する。

2.3 セキュリティ管理 (FMT)

2.3.1 管理機能の特定 (FMT_SMF)

2.3.1.1 FMT_SMF.1 管理機能の特定

2.3.1.1.1 TSS

69 オプション A: 評価者は、TOE が DEK を変更する方法について TSS に記述されていることを保証しなければならない(shall)。

70 オプション B: 評価者は、TOE が暗号技術的に DEK を消去する方法について TSS に記述されていることを保証しなければならない(shall)。

71 オプション C: 評価者は、TOE ファームウェア／ソフトウェアアップデートを開始するプロセスが TSS に記述されていることを保証しなければならない(shall)。

72 オプション D: 追加の管理機能が ST で主張されている場合は、評価者はそれらの機能が TSS に記述されていることを検証しなければならない(shall)。

2.3.1.1.2 操作ガイダンス

73 オプション A: 評価者は、AGD ガイダンスをレビューしなければならず、存在する DEK を変更する指示（命令）を決定しなければならない(shall)。指示は、適合主張している TOE のすべての運用環境を網羅し、DEK を成功裏に生成または再生成するために存在しなければなければならない任意の前提条件を含めなければならない(shall)。

74 オプション C: 評価者は、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方法について操作ガイダンスに記述されていることを保証するため、操作ガイダンスを検査しなければならない(shall)。

75 オプション D: デフォルト許可要素：TOE がデフォルト許可要素を設定した形で届く場合があるかもしれない。その場合、項目 D での選択は、これらの許可要素を変更するメカニズムがあるような選択でなければならない(shall)。操作ガイダンスは、利用者がデバイスの所有権を取得する時にこれらの要素を変更する方法について記述していなければならない(shall)。TSS は、存在するデフォルトの許可要素を記述しなければならない(shall)。

76 鍵リカバリーの無効化：この機能の無効化についてのガイダンスは、AGD 証拠資料に記述されていなければならない(shall)。

2.3.1.1.3 KMD

77 オプション D: TOE が暗号化された DEK をインポートする機能を提供する場合、評価者は TOE がラッピングされた DEK をインポートし、ラッピングされた DEK の復号を実行する方法について KMD に記述されていることを保証しなければならない(shall)。

2.3.1.1.4 テスト

78 オプション A + B: 評価者は、TOE が DEK を変更したり、暗号技術的に消去したり（以前の利用者データを取り出すための能力を有効に除去する）する機能を有していることを検証しなければならない(shall)。

79 オプション C: 評価者は、TOE ファームウェア／ソフトウェアアップデートを開始する機能を TOE が持っていることを検証しなければならない(shall)。

80 オプション D: 追加の管理機能が主張されている場合、評価者は記述された通りの追加の機能が機能していることを検証しなければならない(shall)。

2.4 TSF の保護 (FPT)

2.4.1 鍵及び鍵材料の保護（FPT_KYP_EXT)

2.4.1.1 FPT_KYP_EXT.1 鍵及び鍵材料の保護

2.4.1.1.1 TSS

81 評価者は、中間鍵がサブマスクコンバイニングを用いて生成される方法が記述されていることを検証するため、TSS を検査しなければならない(shall)。

2.4.1.1.2 操作ガイダンス

82 本 SFR のための AGD 評価アクティビティは、一切ない。

2.4.1.1.3 KMD

83 評価者は、不揮発性メモリに格納される鍵を保護するために使用される方法の記述について KMD を検査しなければならない(shall)。

84 評価者は、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検証しなければならない(shall)。不揮発性メモリにおけるラッ

ピングされたまたは暗号化された鍵、及びストレージに関する基準の一つを満たすような不揮発性メモリにおける平文の鍵のストレージに関して、FCS_COP.1(d) または FCS_COP.1(g) に従っていることを保証するため、鍵チェインの記述はレビューされなければならない(shall)。

2.4.1.1.4 テスト

85 本 SFR のためのテスト評価アクティビティは、一切ない。

2.4.2 電力管理 (FPT_PWR_EXT)

2.4.2.1 FPT_PWR_EXT.1 省電力状態

2.4.2.1.1 TSS

86 評価者は、適合省電力状態のリストが TSS に含まれることを検証しなければならない(shall)。

2.4.2.1.2 操作ガイダンス

87 評価者は、適合省電力状態のリストがガイダンス証拠資料に含まれていることを保証しなければならない(shall)。もし、追加の省電力状態がサポートされる場合、評価者は、非適合の省電力状態の利用がどのように回避できるかについて、ガイダンス証拠資料に記述されていることを検証しなければならない(shall)。

2.4.2.1.3 KMD

88 本 SFR のための KMD 評価アクティビティは、一切ない。

2.4.2.1.4 テスト

89 評価者は、列挙された各適合状態についてすべての鍵／鍵材料が揮発性メモリから FCS_CKM.4(b)で定義されたテストを用いて削除されることを確認しなければならない(shall)。

2.4.2.2 FPT_PWR_EXT.2 省電力状態のタイミング

2.4.2.2.1 TSS

90 評価者は、TOE が適合省電力状態へ入るような条件のリストが TSS に含まれていることを検証しなければならない(shall)。

2.4.2.2.2 操作ガイダンス

91 評価者は、TOE が適合省電力状態に入るような条件のリストがガイダンスに含まれていることをチェックしなければならない(shall)。さらに、評価者は、TOE が適合省電力状態へ完全に遷移するために取ると期待される時間(例、揮発性メモリが完全にクリアされるまでに何秒かかるか) についての情報をガイダンス証拠資料が提供することを検証しなければならない(shall)。

2.4.2.2.3 KMD

92 本 SFR のための KMD 評価アクティビティは、一切ない。

2.4.2.2.4 テスト

93 評価者は、特定された条件のリストにおけるそれぞれの条件をトリガーとして、FCS_CKM.4(b)で特定されたテストを実行することによって TOE が適合省電力状態になることを保証しなければならない(shall)。

2.4.3 TSF テスト (FPT_TST_EXT)

2.4.3.1 FPT_TST_EXT.1 TSF テスト

2.4.3.1.1 TSS

94 評価者は、暗号機能の既知解セルフテストについて TSS に記述されていることを検証しなければならない(shall)。

95 評価者は、TOE の正しい動作に影響を与えるようないくつかの非暗号機能、及び TOE がそれらの機能をテストするための手法について TSS に記述されていることを検証しなければならない(shall)。評価者は、これらの機能のそれぞれについて、TOE がその機能の正しい動作を検証するための手法のそれぞれについて、TSS に含まれていることを検証しなければならない(shall)。評価者、TSF データが TSF テスト用として適切であることを検証しなければならない(shall)。例えば、より多くのブロックが AES の CBC モードについてテストされ、AES の GCM モードの出力がトランケーションなしにテストされ、または 512 ビット鍵が HMAC-SHA512 のテストで使用される。

96 FCS_RBG_EXT.1 が NIST SP 800-90 に従って TOE により実装される場合、評価者は、NIST SP 800-90 のセクション 11.3 と一貫性のある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)。

97 任意の FCS_COP 機能が TOE により実装される場合、それらの機能の既知解セルフテストについて TSS に記述されなければならない(shall)。

98 評価者は、TSF の正しい動作に影響を与えるようないくつかの非暗号機能、それらの機能がテストされる手法について、TSS に記述されていることを検証しなければならない(shall)。TSS は、これらの各機能、機能／コンポーネントの正しい動作が検証される手法について記述していること。評価者は、識別された機能／コンポーネント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)。

2.4.3.1.2 操作ガイダンス

99 本 SFR のための AGD 評価アクティビティは、一切ない。

2.4.3.1.3 KMD

100 本 SFR のための KMD 評価アクティビティは、一切ない。

2.4.3.1.4 テスト

101 本 SFR のためのテスト評価アクティビティは、一切ない。

2.4.4 高信頼アップデート (FPT_TUD_EXT)

2.4.4.1 FPT_TUD_EXT.1 高信頼アップデート

2.4.4.1.1 TSS

102 評価者は、権限のある提供元が TOE のアップデートに対して署名を行い、デジタル署名されていることを表明する情報が記述されていることを保証するため TSS を検査しなければならない(shall)。評価者は、運用環境におけるアップデートの検証メカニズム用に TOE がどのように公開鍵を使用するかの記述とともに権限のある提供元の定義が TSS に含まれていることを検査しなければならない(shall)。評価者は、TOE のアップデートのクレデンシャルの保護及び維持に関する詳細が TSS に含まれていることを保証すること。

103 運用環境が署名検証を実行する場合、評価者は、ST において識別されたそれぞれのプラットフォームについて、この暗号機能を起動するために TOE が使用するインタフェースが記述されていることを保証するために TSS を検査しなければならない(shall)。

2.4.4.1.2 操作ガイダンス

104 評価者は、TOE の更新をベンダが提供する方法；更新のデジタル署名の検証に関連する処理（FCS_COP.1(a)に定義されるとおり）；及び成功と不成功の場合に取られるアクションが運用ガイダンスに記述されていることを保証すること。

2.4.4.1.3 KMD

105 本 SFR のための KMD 評価アクティビティは、一切ない。

2.4.4.1.4 テスト

106 評価者は、以下のテストを実行しなければならない(shall)（TOE が複数の署名がサポートする場合、それぞれについて異なるハッシュアルゴリズムを用いて、評価者は、デジタル署名単体と同様に、算術的及び非算術的なデジタル署名とハッシュの異なる組み合わせについてテスト２と３を実行すること）：

107 テスト 1: 評価者は、TOE の現在のバージョンを決定するため、バージョン検証アクティビティを実行すること。以下のテストで記述されているテストの後、評価者は、アップデートのバージョンに相当する正しいバージョンであることを検証するため、このアクティビティを再度実行すること。

108 テスト 2: 評価者は、運用ガイダンスに記述された手続きを用いて正当なアップデートを取得し、TOE にアップデートのインストールが成功することを検証すること。評価者は、アップデートが期待通りに機能することを論証するため、その他の保証アクティビティテストの一部を実行しなければならない(shall)。

3 オプション要件の評価アクティビティ

3.1 暗号サポート (FCS)

3.1.1 暗号鍵管理 (FCS_CKM)

3.1.1.1 FCS_CKM.4(e) 暗号鍵破棄 (鍵暗号学的消去)

3.1.1.1.1 TSS

109 本 SFR のための TSS 評価アクティビティは、一切ない。

3.1.1.1.2 操作ガイダンス

110 本 SFR のための AGD 評価アクティビティは、一切ない。

3.1.1.1.3 KMD

111 評価者は、TSS/KMD における TOE の鍵チェインを検査し、この方法によって鍵が破壊されるそれぞれの例を特定しなければならない(shall)。それぞれの例において、評価者は、対象となる鍵を復号できるすべての鍵が規定された鍵破棄方法に従って破壊されることを検証しなければならない(shall)。

3.1.1.1.4 テスト

112 本 SFR のためのテスト評価アクティビティは、一切ない。

3.2 TSF の保護 (FPT)

3.2.1 ファームウェアアクセス制御 (FPT_FAC_EXT)

3.2.1.1 FPT_FAC_EXT.1 ファームウェアアクセス制御

3.2.1.1.1 TSS

113 評価者は、使用される値の記述に沿ってアクセス制御プロセスがどのように実行されるかについての情報が TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。

3.2.1.1.2 操作ガイダンス

114 評価者は、利用者が許可プロセスとどのように対話すると期待されるかについて、操作ガイダンスに記述されていることを保証すること。

3.2.1.1.3 KMD

115 本 SFR のための KMD 評価アクティビティは、一切ない。

3.2.1.1.4 テスト

116 評価者は、以下のテストを実行しなければならない(shall)。

117 テスト１：評価者は、ファームウェアアップデートのインストールを試行し、要求されるプロンプトと適切な値がアップデートを継続するために必要であることを検証しなければならない(shall)。

3.2.2 ロールバック保護 (FPT_RBP_EXT)

3.2.2.1 FPT_RBP_EXT.1 ロールバック保護

3.2.2.1.1 TSS

118 評価者は、アップグレードがインストールされる前にセキュリティバージョンチェックが実行されることを検証するためのプロセスが上位レベルで TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。評価者は、エラーコードの種別の上位レベル記述が提供され、いつエラーがトリガーされるかについて検証しなければならない(shall)。

3.2.2.1.2 操作ガイダンス

119 評価者は、エラーコードを利用者がどのように解釈するべきかについての記述が提供されることを保証すること。

3.2.2.1.3 KMD

120 本 SFR のための KMD 評価アクティビティは、一切ない。

3.2.2.1.4 テスト

121 評価者は、以下のテストを実行しなければならない(shall)：

122 テスト１：評価者は、より低いセキュリティバージョン番号のアップグレード (単にバージョン番号を改変することによって、またはベンダによって提供されたアップグレードを利用することによって、のいずれか) のインストールを試行しなければならない(shall)、そして、より低いバージョンがインストールできないこと及びエラーが利用者に提示されることを検証すること。

4 選択ベース要件の評価アクティビティ

4.1 暗号サポート(FCS)

4.1.1 暗号鍵管理 (FCS_CKM)

4.1.1.1 FCS_CKM.1(a) 暗号鍵生成 (非対称鍵)

4.1.1.1.1 TSS

123 評価者は、TOE がサポートする鍵長を TSS が識別していることを保証しなければならない。ST が一つ以上のスキームを特定している場合、評価者は、それぞれのスキームの用途を識別していることを検証するため、TSS を検査しなければならない(shall)。

4.1.1.1.2 操作ガイダンス

124 評価者は、AGD 証拠資料によって規定され、本 cPP において定義されたすべての用途のために選択された鍵生成スキームと鍵長を利用するための TOE の設定方法を AGD ガイダンスが管理者に指示していることを検証しなければならない(shall)。

4.1.1.1.3 KMD

125 TOE が鍵チェインの一部として非対称鍵を利用する場合、KMD には、鍵チェインの一部としてどのように非対称鍵が利用されるかについて詳述されるべきである。

4.1.1.1.4 テスト

126 以下のテストは、工場製品では通常見つからないようなツールを評価者に提供するテストプラットフォームへのアクセスを提供することを開発者に要求する。

127 ***FIPS PUB 186-4 RSA スキームの鍵生成***

128 評価者は、鍵生成テストを用いて TOE による RSA 鍵生成の実装を検証しなければならない(shall)。本テストは、公開鍵検証指数（public verification exponent）e、プライベート素因数（private prime factor） p 及び q、公開鍵の法（public modulus）n 及び プライベート署名指数（private signature exponent）d の計算を含めた鍵コンポーネントの値を正しく生成するような TSF の能力を検証する。

129 鍵ペア生成では、素数 p と q を生成するために 5 通りの方法（または手法）を特定している。これらには、以下のものが含まれる：

130 1. ランダムな素数：

- 証明可能素数（Provable primes）
- 確率的素数（Probable primes）

131 2. 以下の条件付きの素数：

- 素数 p1, p2, q1,q2, p 及び q は、すべて証明可能素数でなければならない

- 素数 p1, p2, q1, 及び q2 は、証明可能素数で、 p 及び q は確率的素数でなければならない
- 素数 p1, p2, q1,q2, p 及び q は、すべて確率的素数でなければならない

132 ランダムな証明可能素数手法とすべての条件付き素数手法についての鍵生成手法をテストするため、評価者は決定論的に RSA 鍵ペアを生成するために十分なデータをシード値として TSF 鍵生成ルーチンに与えなければならない(shall)。これには、1 つまたは複数の乱数シード値、RSA 鍵の公開鍵指数、及び望ましい鍵長が含まれる。公開鍵指数は、範囲（2^16, 2^256）内の奇数の整数でなければならない。サポートされている鍵の長さのそれぞれについて、評価者は 25 個の鍵ペアを TSF に生成させなければならない(shall)。評価者は、TSF により生成された値を、既知の良好な実装から生成された値と比較することによって、TSF の実装の正確さを検証しなければならない(shall)。

133 ***楕円曲線暗号 (ECC) の鍵生成***

134 *FIPS 186-4 ECC 鍵生成テスト*

135 サポートされている NIST 曲線、すなわち P-256、P-384 及び P-521 のそれぞれについて、評価者は 10 個のプライベート鍵／公開鍵ペアの生成を試験対象実装(IUT：Implementation under test) に対して要求しなければならない(shall)。プライベート鍵は、承認済みランダムビット生成器 (RBG) を用いて生成されなければならない(shall)。正確であることを決定するため、評価者は、既知の良好な実装の公開鍵検証 (PKV) 機能へ、生成された鍵ペアを送出しなければならない(shall)。

136 *FIPS 186-4 公開鍵検証 (PKV) テスト*

サポートされている NIST 曲線、すなわち P-256、P-384 及び P-521 のそれぞれについて、評価者は既知の良好な実装の鍵生成機能を用いて 10 個のプライペート鍵／公開鍵ペアを生成し、うち 5 個の公開鍵を不正な値となるよう改変し、残り 5 個を未改変の（すなわち、正しい）値のままにしなければならない(shall)。評価者は、これに応じた 10 個の合格／不合格の値を取得しなければならない(shall)。

137 ***有限体暗号 (FFC) の鍵生成***

138 評価者は、パラメタ生成及び鍵生成テストを用いて TOE による FFC のためのパラメタ生成及び鍵生成の実装を検証しなければならない(shall)。このテストは、フィールド素数 p、暗号素数 q (p-1 を割り切れる)、暗号群生成元 g、並びにプライベート鍵 x 及び公開鍵 y の計算の値を正しく生成するような TSF の能力を検証する。

139 パラメタ生成では、暗号学的素数 q 及びフィールド素数 p を生成するための 2 通りの方法（または手法）を規定する：

140 暗号学的素数及びフィールド素数：

- 素数 q 及び p は、両方とも証明可能素数（Provable primes）でなければならない
- 素数 q 及びフィールド素数 p は、両方とも確率的素数（Probable primes）でなければならない

及び、暗号学的群生成元 g を生成するための 2 通りの方法を規定する：

141

142 暗号学的群生成元：

- 検証可能プロセスによって構築された生成元 g
- 検証不可能プロセスによって構築された生成元 g。

143 鍵生成は、プライベート鍵 x を生成するための 2 通りの方法を規定する：

144 プライベート鍵：

- RBG の len(q) ビットの出力、ここで 1 <=x <= q-1
- RBG の len(q) + 64 ビットの出力に、q-1 を Modulus（法）とする剰余演算を行ったもの、ここで 1<= x<=q-1 とする。

145 RBG のセキュリティ強度は、少なくとも FFC パラメタセットによって提供されるセキュリティ強度と同じでなければならない。

146 証明可能素数の手法については、暗号素数及びフィールド素数生成手法をテストするために、及び／または検証可能プロセスについては、群生成元 g をテストするために、評価者は決定論的にパラメタセットを生成するのに十分なデータを TSF パラメタ生成ルーチンにシード値として与えなければならない(shall)。

147 サポートされている鍵長のそれぞれについて、評価者は 25 個のパラメタセットと鍵ペアを TSF に生成させなければならない(shall)。評価者は、TSF により生成された値を、既知の良好な実装から生成された値と比較することによって、TSF の実装の正確さを検証しなければならない(shall)。検証では、FFC パラメタと鍵ペアのそれぞれについて、以下についても確認しなければならない(shall)

- g != 0,1
- q が p-1 を割り切れること
- g^q mod p = 1
- g^x mod p = y 。

4.1.1.2 FCS_CKM.1(b) 暗号鍵生成 (対称鍵)

4.1.1.2.1 TSS

148 評価者は、対称鍵が製品によりサポートされること、TSS に個の鍵に対して製品によって提供される保護についての記述が含まれることを決定するため、TSS をレビューしなければならない(shall)。評価者は、TSS に TOE によってサポートされる鍵長を特定されていることを保証しなければならない(shall)。

4.1.1.2.2 操作ガイダンス

149 評価者は、AGD ガイダンスが管理者に対して、AGD 証拠資料によって規定され、また本 cPP で定義された、すべての利用者のために選択された鍵長を利用するために、TOE を設定する方法について指示していることを検証しなければならない(shall)。

4.1.1.2.3 KMD

150 TOE が鍵チェインの一部として対称鍵を利用する場合、KMD には、鍵チェインの一部として対称鍵がどのように利用されるかについて詳述されるべきである(should)。

4.1.1.2.4 テスト

151 本 SFR のためのテスト評価アクティビティは、一切ない。

4.1.1.3 FCS_CKM.4(b) 暗号鍵破棄 (TOE 管理ハードウェア)

4.1.1.3.1 TSS + KMD (必要な詳細情報が保護情報を記述する場合、鍵管理記述が利用されるかもしれない)

152 評価者は、TSS に揮発性メモリでその鍵がどのように管理されるかについて記述されていることを検証するため、TSS を検査しなければならない(shall)。この記述は、揮発性メモリへそれぞれの特定された鍵がどのように導入されるかについての詳細 (例、利用者入力からの導出によって、または不揮発性メモリに格納されているラッピングされた鍵をラッピング解除することによって)及びそれらがどのように上書きされるかを含むこと。

153 評価者は、TSS に格納されるそれぞれの鍵の種別が列挙され、鍵材料が格納されるメモリ種別を特定していることを保証するため、チェックしなければならない(shall)。列挙しているメモリ種別が採用されるとき、TSS には、異なるメモリコントローラまたは格納アルゴリズムを採用するようなあらゆるメモリ種別と同様に、FCS_CKM.4.1 の SFR で選択されたそれぞれのメモリ種別が列挙されること。例えば、TOE が NOR フラッシュと NAND フラッシュを利用する場合、両方の種別が列挙されるべきである(should)。

154 評価者は、列挙されたそれぞれの種別のメモリからメモリ書き込み及び読み出しするためにメモリコントローラによって資料される手法について TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。ここでの目的は、誰でも鍵がメモリに書き込まれる方法を完全に決定できるように、メモリコントローラがどのように動作するかについての記述を提供することである。記述には、データがメモリへ書き込まれ、読み出される方法 (例、ブロックレベル、セルレベル)、存在する可能性のある鍵の複製についてのメカニズム (例、パリティビットを持つ複製、パリティビットを持たない複製、冗長性のために利用される任意のメカニズム)が含まれること。

155 評価者は、特定されたそれぞれの鍵についての破壊手順について TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。異なる種別のメモリが鍵の格納に利用される場合、評価者は、鍵が格納される(例、フラッシュメモリに格納される鍵 X は、ゼロで 1 回の上書きによって破壊される、EEPROM に格納される鍵 X'は、疑似ランダムパタンからなる上書きによって破壊されるーTOE で利用される EEPROM は記述されるとおりウェアレベリング手法を利用する) それぞれのメモリ種別についての破壊手順を TSS に特定していることを保証するため、チェックしなければならない(shall)。

156 ST がオープンな割付を利用し、利用される種別のパタンを記入する場合、評価者は、そのパタンの取得方法と利用方法について TSS に記述されていることを保証するため、TSS を検査すること。評価者は、そのパタンにあらゆる CSP が含まれないことを検証しなければならない(shall)。

157 評価者は、鍵破棄要件に厳密に適合しないかもしれないような設定または状況について、TSS において特定していることをチェックしなければならない(shall)。

158 TSS 検査の完了に際して、評価者は、すべての鍵(及び潜在的な複製) が破壊される方法について理解すること。

4.1.1.3.2 操作ガイダンス

159 ある場合において、鍵破壊を妨げる、または遅延させるかもしれないような様々な懸念がある。評価者は、鍵破棄要件に厳密に適合しないかもしれないような設定または状況についてガイダンス証拠資料に特定されていること、及びこの記述が TSS の関連部分及びあらゆるその他の関連する「必須補足情報」と一貫していることをチェックしなければならない(shall)。評価者は、鍵破棄が物理層で遅延されるかもしれないような状況についてのガイダンスをガイダンス証拠資料が提供していることをチェックしなければならない(shall)。

160 例えば、TOE が物理メモリへのフルアクセスをできないとき、ストレージがウェアレベリングやガーベージコレクションを実装しているかもしれない可能性がある。これは、論理的にアクセスできないが物理的に永続するような鍵の追加の複製を作成するかもしれない。この場合、その他のタスクで積極的に使用されないとき、ドライブがこれらの永続的な複製を破壊するため、TRIM コマンドをサポートし、ガーベージコレクションを実装していると想定される。

161 ドライブベンダは、データがこれらのソリューションから本当に削除されるまでのさまざまな時間など、異なるさまざまな方法でガーベージコレクションを実装する。削除できないその他のデータと共に 1 つのブロックにデータが含まれる場合、データがより長い時間永続するというリスクがある。それらの削除に際してガーベージコレクションを介して複製を消去するよう不揮発性メモリに指示するような、TRIM をサポートする運用環境のオペレーティングシステム及びファイルシステムと想定されること。

162 RAID アレイが利用されている場合、TRIM をサポートするセットアップのみが活用されることが想定されること。ドライブが PCI-Express を介して接続される場合、オペレーティングシステムは、そのチャネルを介して TRIM をサポートすることが想定されること。ドライブがヘルシーであり、最小限の破損したデータを含み、ドライブの健全性に対する重大な損傷が発生する前に寿命を迎えることが想定され、潜在的に回復可能なデータがドライブの損傷を受けた領域に残存するかもしれないようなリスクがあると想定すること。

163 最後に、マスターファイルテーブルに完全に含まれるであろう 982 バイトよりも少ないファイルに含まれているなど、鍵は TRIM にアクセスできないような方法を用いて格納されないことを想定すること。

164 ウェアレベリングされたメモリ上での破壊について、ST 作成者が見積もられた範囲を抵抗しなければならない (shall) ような破壊を処理する前に、一定の時間が要求される。

4.1.1.3.3 テスト

~~165 本 SFR のためのテスト評価アクティビティは、一切ない。~~
(訳注：以下にテストについての記述があるので、削除する)

166 これらのテストについて、評価者は、その鍵を用いた正常な暗号処理中に TOE によって内部的に生成されるかもしれないようなすべての鍵の複製を含めて、鍵がクリアされることをテストするため、適切な開発環境(例、仮想マシン)及び開発ツール(デバッガ、シミュレータ、等)を活用しなければならない(shall)。

167 ウェアレベリングされたメモリ上での破壊について、一定の時間が事前に要求される場合、評価者は、テスト 2 と 3 で鍵のクリア後にその時間待たなければならない(shall)。

168 テスト 1：揮発性メモリにおける平文及び TOE による上書きによって破壊の対象として保持されるそれぞれの鍵に適用される(平文の値が揮発性または不揮発性メモリに格納のためにその後暗号化されるかどうかにかかわらず)。鍵が電源の切断により削除されるような破壊方法のみが選択されるような場合、このテストは必要ない。評価者は、以下を実行しなければならない(shall)：

1. クリア対象の TOE にある鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵をクリアさせる。
4. TOE に対して、実行を停止させるが、終了しない。
5. TOE に対して、TOE の全メモリをバイナリ―ファイルへダンプさせる。
6. ステップ #1 からの既知の鍵の値の例について、ステップ #5 で作成されたバイナリファイルの内容を検索する。
7. ステップ#1 からの鍵の値を 3 つの同様なサイズの断片に分割し、それぞれの断片を用いて検索を実行する。

ステップ 1-6 は、完全な鍵が揮発性メモリのどこにも存在しないことを保証する。もし、複製が見つかる場合、テストは不合格となる。

ステップ 7 は、部分的な鍵の断片がメモリに残存しないことを保証する。断片が見つかる場合、鍵に関係のないような極小な機械である(例、何らかのランダムなビットが一致してしまう)。このような場合、テストはステップ #1 で異なる鍵を用いて繰り返されるべきである(should)。断片が見つかる場合、テストは不合格となる。

169 テスト 2：不揮発性メモリに保持されるそれぞれの鍵で TOE による上書きによって破壊の対象となるそれぞれの鍵に適用される。評価者は、必要な場合に TOE 開発者によって提供されるような、特別なツール(必要に応じて)を、鍵格納場所を閲覧するために、利用しなければならない(shall)：

1. クリア対象の TOE にある鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵をクリアさせる。

4. ステップ #1 からの既知の鍵の値の例について、ステップ #5 で作成されたバイナリファイルの内容を検索する。複製が見つかる場合、テストは不合格となる。
5. ステップ#1 からの鍵の値を 3 つの同様なサイズの断片に分割し、それぞれの断片を用いて検索を実行する。断片が見つかる場合、テストは繰り返される(上記テスト 1 の記述のとおり)、また断片が繰り返し見つかる場合、テストは不合格となる。

170 テスト 3：不揮発性メモリに保持されるそれぞれの鍵で TOE による上書きによって破壊の対象となるそれぞれの鍵に適用される。評価者は、必要な場合に TOE 開発者によって提供されるような、特別なツール(必要に応じて)を、鍵格納場所を閲覧するために、利用しなければならない(shall)：

1. クリア対象の TOE にある鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵をクリアさせる。
4. 適切なパタンが活用されることを保証するため、不揮発性メモリのステップ #1 の格納場所を読み出す。

そのメモリの場所にある鍵を上書きするために正しいパタンが利用される場合、テストは合格となる。そのパタンが見つからない場合、テストは不合格となる。

4.1.1.4 FCS_CKM.4(c) 暗号鍵破棄 (汎用ハードウェア)

4.1.1.4.1 TSS + KMD (必要な詳細情報が保護情報を記述する場合、鍵管理記述が利用されるかもしれない)

171 評価者は、鍵が揮発性メモリ内でどのように管理されるかについて、TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。この記述には、それぞれの特定された鍵が揮発性メモリへどのように導入されるか(例、利用者入力からの導出によって、または不揮発性メモリに格納されたラッピングされた鍵をラッピング解除することによって)、及びそれらが上書きされる方法についての詳細を含まれること。

172 評価者は、格納されるそれぞれの種別の鍵が TSS に列挙され、鍵材料が格納されるメモリ種別(揮発性または不揮発性)を特定していることを保証するため、チェックしなければならない(shall)。

173 TSS はメモリを読み出し／書き込みするためのコマンドをサービスするために利用されるインタフェースについて特定し、記述すること。評価者は、そのインタフェースが ST 作成者によってなされた選択をサポートすることを保証するため、それぞれの異なるメディア種別についてのインタフェース記述を検査すること。

174 ST がオープンな割付を利用し、利用される種別のパタンを記入する場合、評価者は、そのパタンの取得方法と利用方法について TSS に記述されていることを保証するため、TSS を検査すること。評価者は、そのパタンにあらゆる CSP が含まれないことを検証しなければならない(shall)。

175 評価者は、鍵破棄要件に厳密に適合しないかもしれないような設定または状況について、TSS において特定していることをチェックしなければならない(shall)。

4.1.1.4.2 操作ガイダンス

176 ある場合において、鍵破壊を妨げる、または遅延させるかもしれないような様々な懸念がある。評価者は、鍵破棄要件に厳密に適合しないかもしれないような設定または状況についてガイダンス証拠資料に特定されていること、及びこの記述が TSS の関連部分及びあらゆるその他の関連する「必須補足情報」と一貫していることをチェックしなければならない(shall)。評価者は、鍵破棄が物理層で遅延されるかもしれないような状況についてのガイダンスをガイダンス証拠資料が提供していることをチェックしなければならない(shall)。

177 例えば、TOE が物理メモリへのフルアクセスをできないとき、ストレージがウェアレベリングやガーベージコレクションを実装しているかもしれない可能性がある。これは、論理的にアクセスできないが物理的に永続するような鍵の追加の複製を作成するかもしれない。この場合、その他のタスクで積極的に使用されないとき、ドライブがこれらの永続的な複製を破壊するため、TRIM コマンドをサポートし、ガーベージコレクションを実装していると想定される。

178 ドライブベンダは、データがこれらのソリューションから本当に削除されるまでのさまざまな時間など、異なるさまざまな方法でガーベージコレクションを実装する。削除できないその他のデータと共に１つのブロックにデータが含まれる場合、データがより長い時間永続するというリスクがある。それらの削除に際してガーベージコレクションを介して複製を消去するよう不揮発性メモリに指示するような、TRIM をサポートする運用環境のオペレーティングシステム及びファイルシステムと想定されること。

179 RAID アレイが利用されている場合、TRIM をサポートするセットアップのみが活用されることが想定されること。ドライブが PCI-Express を介して接続される場合、オペレーティングシステムは、そのチャネルを介して TRIM をサポートすることが想定されること。ドライブがヘルシーであり、最小限の破損したデータを含み、ドライブの健全性に対する重大な損傷が発生する前に寿命を迎えることが想定され、潜在的に回復可能なデータがドライブの損傷を受けた領域に残存するかもしれないようなリスクがあると想定すること。

180 最後に、マスターファイルテーブルに完全に含まれるであろう 982 バイトよりも少ないファイルに含まれているなど、鍵は TRIM にアクセスできないような方法を用いて格納されないことを想定すること。

4.1.1.4.3 テスト

181 これらのテストについて、評価者は、その鍵を用いた正常な暗号処理中に TOE によって内部的に生成されるかもしれないようなすべての鍵の複製を含めて、鍵がクリアされることをテストするため、適切な開発環境(例、仮想マシン)及び開発ツール(デバッガ、シミュレータ、等)を活用しなければならない(shall)。

182 テスト 1：揮発性メモリにおける平文及び TOE による上書きによって破壊の対象として保持されるそれぞれの鍵に適用される(平文の値が揮発性または不揮発性メモリに格納のためにその後暗号化されるかどうかにかかわらず)。鍵が電源の切断により削除されるような破壊方法のみが選択されるような場合、このテストは必要ない。評価者は、以下を実行しなければならない(shall)：

1. クリア対象の TOE にある鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵をクリアさせる。
4. TOE に対して、実行を停止させるが、終了しない。
5. TOE に対して、TOE の全メモリをバイナリ―ファイルへダンプさせる。
6. ステップ #1 からの既知の鍵の値の例について、ステップ #5 で作成されたバイナリファイルの内容を検索する。
7. ステップ#1 からの鍵の値を 3 つの同様なサイズの断片に分割し、それぞれの断片を用いて検索を実行する。

ステップ 1-6 は、完全な鍵が揮発性メモリのどこにも存在しないことを保証する。もし、複製が見つかる場合、テストは不合格となる。

ステップ 7 は、部分的な鍵の断片がメモリに残存しないことを保証する。断片が見つかる場合、鍵に関係のないような極小な機械である(例、何らかのランダムなビットが一致してしまう)。このような場合、テストはステップ #1 で異なる鍵を用いて繰り返されるべきである(should)。断片が見つかる場合、テストは不合格となる。

183 テスト 2：不揮発性メモリに保持されるそれぞれの鍵で TOE による上書きによって破壊の対象となるそれぞれの鍵に適用される。評価者は、必要な場合に TOE 開発者によって提供されるような、特別なツール(必要に応じて)を、鍵格納場所を閲覧するために、利用しなければならない(shall)：

1. クリア対象の TOE にある鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵をクリアさせる。
4. ステップ #1 からの既知の鍵の値の例について、ステップ #5 で作成されたバイナリファイルの内容を検索する。複製が見つかる場合、テストは不合格となる。
5. ステップ#1 からの鍵の値を 3 つの同様なサイズの断片に分割し、それぞれの断片を用いて検索を実行する。断片が見つかる場合、テストは繰り返される(上記テスト 1 の記述のとおり)、また断片が繰り返し見つかる場合、テストは不合格となる。

184 テスト 3：不揮発性メモリに保持されるそれぞれの鍵で TOE による上書きによって破壊の対象となるそれぞれの鍵に適用される。評価者は、必要な

場合に TOE 開発者によって提供されるような、特別なツール(必要に応じて)を、鍵格納場所を閲覧するために、利用しなければならない(shall)：

1. クリア対象の TOE にある鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵をクリアさせる。
4. 適切なパタンが活用されることを保証するため、不揮発性メモリのステップ #1 の格納場所を読み出す。

185 そのメモリの場所にある鍵を上書きするために正しいパタンが利用される場合、テストは合格となる。そのパタンが見つからない場合、テストは不合格となる。

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

4.1.1.5.1 TSS + KMD (必要な詳細情報が保護情報を記述する場合、鍵管理記述が利用されるかもしれない)

186 評価者は、鍵が揮発性メモリ内でどのように管理されるかについて、TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。この記述には、それぞれの特定された鍵が揮発性メモリへどのように導入されるか(例、利用者入力からの導出によって、または不揮発性メモリに格納されたラッピングされた鍵をラッピング解除することによって)、及びそれらが上書きされる方法についての詳細を含まれること。

187 評価者は、不揮発性メモリ内に格納されるそれぞれの種別の鍵が TSS に列挙され、鍵を管理(例、格納、検索、破壊)するための基礎となるプラットフォームと TOE がどのように対話するかについて特定することを保証するためチェックしなければならない(shall)。その記述には、TOE が鍵を管理するために利用するインタフェース(例、ファイルシステム API、プラットフォーム鍵ストア API)の特定と記述を含め、TOE がそのプラットフォームとどのように対話する方法についての詳細が含まれること。

188 評価者は、そのインタフェースが TSS における選択と記述をサポートすることを保証するため、それぞれの異なるメディア種別についてのインタフェース記述を検査すること。

189 評価者は、鍵破棄要件に厳密に適合しないかもしれないようなあらゆる設定または状況について TSS が特定することをチェックしなければならない(shall)。もし、ST がオープンな割付を利用し、利用される種別のパタンを記入する場合、評価者は、そのパタンの取得方法と利用方法について TSS に記述されていることを保証するため、TSS を検査すること。評価者は、そのパタンにあらゆる CSP が含まれないことを検証しなければならない(shall)

4.1.1.5.2 操作ガイダンス

190 ある場合において、鍵破壊を妨げる、または遅延させるかもしれないような様々な懸念がある。評価者は、鍵破棄要件に厳密に適合しないかもしれないような設定または状況についてガイダンス証拠資料に特定されている

こと、及びこの記述が TSS の関連部分及びあらゆるその他の関連する「必須補足情報」と一貫していることをチェックしなければならない(shall)。評価者は、鍵破棄が物理層で遅延されるかもしれないような状況についてのガイダンスをガイダンス証拠資料が提供していることをチェックしなければならない(shall)。

191 例えば、TOE が物理メモリへのフルアクセスをできないとき、ストレージがウェアレベリングやガーベージコレクションを実装しているかもしれない可能性がある。これは、論理的にアクセスできないが物理的に永続するような鍵の追加の複製を作成するかもしれない。この場合、その他のタスクで積極的に使用されないとき、ドライブがこれらの永続的な複製を破壊するため、TRIM コマンドをサポートし、ガーベージコレクションを実装していると想定される。

192 ドライブベンダは、データがこれらのソリューションから本当に削除されるまでのさまざまな時間など、異なるさまざまな方法でガーベージコレクションを実装する。削除できないその他のデータと共に 1 つのブロックにデータが含まれる場合、データがより長い時間永続するというリスクがある。それらの削除に際してガーベージコレクションを介して複製を消去するよう不揮発性メモリに指示するような、TRIM をサポートする運用環境のオペレーティングシステム及びファイルシステムと想定されること。

193 RAID アレイが利用されている場合、TRIM をサポートするセットアップのみが活用されることが想定されること。ドライブが PCI-Express を介して接続される場合、オペレーティングシステムは、そのチャネルを介して TRIM をサポートすることが想定されること。ドライブがヘルシーであり、最小限の破損したデータを含み、ドライブの健全性に対する重大な損傷が発生する前に寿命を迎えることが想定され、潜在的に回復可能なデータがドライブの損傷を受けた領域に残存するかもしれないようなリスクがあると想定すること。

194 最後に、マスターファイルテーブルに完全に含まれるであろう 982 バイトよりも少ないファイルに含まれているなど、鍵は TRIM にアクセスできないような方法を用いて格納されないことを想定すること。

4.1.1.5.3 テスト

195 テスト 1：揮発性メモリにおける平文及び TOE による上書きによって破壊の対象として保持されるそれぞれの鍵に適用される(平文の値が揮発性または不揮発性メモリに格納のためにその後暗号化されるかどうかにかかわらず)。鍵が電源の切断により削除されるような破壊方法のみが選択されるような場合、このテストは必要ない。評価者は、以下を実行しなければならない(shall)：

1. 消去対象の TOE 内の鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵をクリアさせる。
4. TOE に対して、実行を停止させるが、終了しない。

5. TOE に対して、TOE の全メモリをバイナリ―ファイルへダンプさせる。
6. ステップ #1 からの既知の鍵の値の例について、ステップ #5 で作成されたバイナリファイルの内容を検索する。
7. ステップ#1 からの鍵の値を 3 つの同様なサイズの断片に分割し、それぞれの断片を用いて検索を実行する。

ステップ 1-6 は、完全な鍵が揮発性メモリのどこにも存在しないことを保証する。もし、複製が見つかる場合、テストは不合格となる。

ステップ 7 は、部分的な鍵の断片がメモリに残存しないことを保証する。断片が見つかる場合、鍵に関係のないような極小な機械である(例、何らかのランダムなビットが一致してしまう)。このような場合、テストはステップ #1 で異なる鍵を用いて繰り返されるべきである(should)。断片が見つかる場合、テストは不合格となる。

196 *以下のテストは、選択 a)にのみ適用する、なぜならこの例における TOE は下位プラットフォーム内で発生していることをより多く観測できるからである(例、メディアの論理的な閲覧)。選択 b)において、TOE は、内部の動作について全く観測できない、また下位のプラットフォームに完全に依存しているので、テスト 1 を超えて TOE をテストする理由がない。*

197 *選択 a)について、以下のテストは TOE がプラットフォームに TOE 供給のパタンでの鍵の上書きを要求できることを決定するために使用される。*

198 テスト 2：不揮発性メモリに保持されるそれぞれの鍵であり、TOE による上書きによって破棄の対象となるような、それぞれの鍵に適用される。評価者は、メディア(例、MBR ファイルシステム)の論理的な閲覧を提供するようなツールを利用しなければならない(shall)：

1. 消去対象の TOE 内の鍵の値を記録する。
2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵を消去させる。
4. ステップ #1 からの既知の鍵の値の例について、ステップ #5 で作成されたバイナリファイルの内容を検索する。複製が見つかる場合、テストは不合格となる。
5. ステップ#1 からの鍵の値を 3 つの同様なサイズの断片に分割し、それぞれの断片を用いて検索を実行する。断片が見つかる場合、テストは繰り返される(上記テスト 1 の記述のとおり)、また断片が繰り返し見つかる場合、テストは不合格となる。

199 テスト 3：不揮発性メモリに保持されるそれぞれの鍵であり、TOE による上書きによって破壊の対象となるような、それぞれの鍵に適用される。評価者は、メディアの論理的な閲覧を提供するようなツールを利用しなければならない(shall)：

1. 消去対象の TOE 内の鍵の値を記録する。

2. TOE に対して、ステップ #1 からの鍵を用いて通常の暗号処理を実行させる。
3. TOE に対して、その鍵を消去させる。
4. 適切なパタンが活用されることを保証するため、不揮発性メモリのステップ #1 の格納場所を読み出す。

200 そのメモリの場所にある鍵を上書きするために正しいパタンが利用される場合、テストは合格となる。そのパタンが見つからない場合、テストは不合格となる。

4.1.2 暗号操作 (FCS_COP)

4.1.2.1 FCS_COP.1(a) 暗号操作 (署名検証)

201 本要件は、TOE に関する更新をインストールする前に TOE 製造事業者からの更新に添付されたデジタル署名を検証するために使用される。なぜならこのコンポーネントは更新機能において使用されるべきもので、以下に列挙されたものへの追加の評価アクティビティが本文書のその他の保証アクティビティにおいて網羅されている。以下のアクティビティはデジタル署名アルゴリズムの実装のみに対応する；評価者コンポーネントにおいて選択されたアルゴリズムにとって適切なテストを実行すること。

202 これらのアルゴリズムによって要求されるハッシュ関数及び／または乱数生成は ST において特定されなければならない(shall)；したがってそれらの関数に関連する評価アクティビティは、関連する暗号ハッシュ及びランダムビット生成セクションに含まれている。さらに TOE によって要求される機能のみがデジタル署名の検証である。本 cPP で要求される機能の実装をサポートするために TOE がデジタル署名を生成する場合、要求された保証アクティビティを決定するために認識された評価と検証スキームが調べられなければならない(shall)。

4.1.2.1.1 TSS

203 評価者は、署名検証の全体フローが記述されていることを保証するために TSS をチェックしなければならない(shall)。これは、少なくとも、デジタル署名の検証で使用されるデータのフォーマットの識別と一般的なロケーション（例えば、「ハードドライブデバイス上のファームウェア」のかわりに「メモリーロケーション 0x00007A4B」のように）；運用環境から受信したデータがどのようにデバイスへ持ってこられるか；デジタル署名アルゴリズム（すなわち、証明書廃棄リストのチェック）の一部ではない実行されるあらゆる処理を含むべきである(should)。

4.1.2.1.2 操作ガイダンス

204 本 SFR のための AGD 評価アクティビティは、一切ない。

4.1.2.1.3 KMD

205 本 SFR のための KMD 評価アクティビティは、一切ない。

4.1.2.1.4 テスト

206 以下の各セクションは、評価者がデジタル署名スキームのそれぞれのタイプについて実行しなければならないテストを含んでいる。要件における割付と選択に基づき、評価者は、それらの選択に関連する具体的なアクティビティを選ぶこと。

207 以下で与えられるスキームに関して、鍵生成／ドメインパラメタ生成のテスト要件が無いことに注意するべきである(should)。これは、本機能がエンドデバイスで必要とされていることを想定していないからであり、その機能が配付されたアップデートのデジタル署名をチェックすることに限定されているからである。これは、ハードドライブファームウェアまたはオンボードの不揮発性ストレージ上に、ドメインパラメタがすでに生成されカプセル化されているべきあることを意味している。鍵生成／ドメインパラメタ生成が要求される場合、要求される保証アクティビティと任意の追加コンポーネントの正確な特定を保証するため、評価及び検証スキームが調べられなければならない(shall)。

208 以下のテストは、SFR 内の選択に基づく条件付きのものである。

209 以下のテストは、工場製品では通常見つからないようなツールを評価者に提供するようなテストプラットフォームへのアクセスを提供することが開発者に対して求められるかもしれない。

210 ECDSA アルゴリズムテスト

211 **ECDSA FIPS 186-4 署名検証テスト**

サポートされている NIST 曲線 (すなわち、P-256、P-384 及び P-521) と SHA 関数のペアのそれぞれについて、評価者は 10 個の 1024 ビットのメッセージ、公開鍵及び署名の組 (tuples) のセットを生成し、10 組のうち 5 組で値のいずれか (メッセージ、公開鍵または署名) を改変しなければならない。評価者は、これに応じた 10 個の合格/不合格の値のセットを取得しなければならない(shall)。

212 RSA 署名アルゴリズムテスト

213 **署名検証テスト**

214 評価者は、署名検証テストを行って、相手方の有効及び無効な署名を認識する TOE の能力を検証しなければならない(shall)。評価者は、公開鍵 e、メッセージ、IR フォーマット、及び／または署名、またはこれらのうち 2 つ以上にエラーを起こすことによって、署名検証テスト中に作成されたテストベクタへエラーを注入しなければならない(shall)。TOE は署名の検証を試行し、成功または失敗を返す。

215 評価者は、対応するパラメタを用いた署名検証テストをエミュレートするため、これらのテストベクタを利用し、TOE がこれらのエラーを検出することを検証しなければならない(shall)。

4.1.2.2 FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム)

4.1.2.2.1 TSS

216 評価者は、ハッシュ関数と他の TSF 暗号機能（例えば、デジタル署名検証機能）の関係が TSS に文書化されていることをチェックしなければならない(shall)。

4.1.2.2.2 操作ガイダンス

217 評価者は、必須のハッシュ長についての機能を設定するために行う必要があるあらゆる設定が存在していることを決定するために操作ガイダンス文書をチェックすること。

4.1.2.2.3 KMD

218 本 SFR ための KMD 評価アクティビティは、一切ない。

4.1.2.2.4 テスト

219 TSF ハッシュ関数は、2 つのモードのいずれかで実装できる。第 1 のモードは、バイト指向モードである。このモードでは、TSF は長さがバイトの整数倍であるメッセージのみをハッシュする。すなわち、ハッシュされるべきメッセージのビット長が 8 で割り切れる必要がある。第 2 のモードは、ビット指向モードである。このモードでは、TSF は任意の長さのメッセージをハッシュする。各モードについて異なるテストが存在するため、ビット指向とバイト指向のテストについて、以下のセクションで指示を与える。

220 評価者は、TSF によって実装され、本 cPP の要件を満たすために用いられるハッシュアルゴリズムのそれぞれについて、以下のテストをすべて行わなければならない(shall)。

221 Short Messages Test - Bit-oriented Mode

222 評価者は、m+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは、0 から m ビットまでシーケンシャルに変化する。メッセージの本文は、疑似ランダム的に生成されなければならない(shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証すること。

223 Short Messages Test - Byte-oriented Mode

224 評価者は m/8+1 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。メッセージの長さは 0 から m/8 バイトまでシーケンシャルに変化し、各メッセージは整数個のバイトとなる。メッセージの本文は、疑似ランダム的に生成されなければならない(shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証すること。

225 Selected Long Messages Test - Bit-oriented Mode

226 評価者は m 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。SHA-256 について、i 番目のメッセージの長さは 512 + 99*i となる (ここで $1 \le i \le m$)。SHA-512 について、i 番目のメッセージの長さは 1024 + 99*i となる (ここで $1 \le i \le m$)。メッセージの本文は、疑似ランダム的に生成されなければならない(shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証すること。

227 Selected Long Messages Test - Byte-oriented Mode

228 評価者は m/8 個のメッセージからなる入力セットを作り上げる。ここで m はハッシュアルゴリズムのブロック長である。SHA-256 について、i 番目のメッセージの長さは 512 + 8*99*i となる (ここで $1 \le i \le m/8$)。SHA-512 について、i 番目のメッセージの長さは 1024 + 8*99*i となる (ここで $1 \le i \le m/8$)。

メッセージの本文は、疑似ランダム的に生成されなければならない(shall)。評価者は、それぞれのメッセージについてメッセージダイジェストを計算し、メッセージが TSF へ提供された際に正しい結果が得られることを保証すること。

229 Pseudorandomly Generated Messages Test

230 このテストは、バイト指向の実装にのみ行われる。評価者は、n ビットの長さのシード値をランダムに生成する。ここで n はテストされるハッシュ関数によって作成されるメッセージダイジェストの長さである。次に評価者は、[SHAVS] の図 1 に示されるアルゴリズムに従って 100 個のメッセージと関連するダイジェストのセットを作成する。次に評価者は、メッセージが TSF へ提供された際に正しい結果が得られることを保証する。

4.1.2.3 FCS_COP.1(c) 暗号操作 (鍵付きハッシュアルゴリズム)

4.1.2.3.1 TSS

231 HMAC が選択された場合：

232 評価者は、HMAC 関数により使用される以下の値を特定していることを保証するために TSS を検査しなければならない(shall)：鍵長、使用されるハッシュ関数、ブロック長、及び使用される出力 MAC 長。

233 CMAC が選択された場合：

234 評価者は、CMAC 関数により使用される以下の値を特定していることを保証するために TSS を検査しなければならない(shall)：鍵長、使用されるハッシュ関数、(暗号の)ブロック長、及び使用される出力 MAC 長。

4.1.2.3.2 操作ガイダンス

235 本 SFR ための AGD 評価アクティビティは、一切ない。

4.1.2.3.3 KMD

236 本 SFR ための KMD 評価アクティビティは、一切ない。

4.1.2.3.4 テスト

237 HMAC が選択された場合：

238 サポートされるパラメタセットのそれぞれについて、評価者は 15 セットのテストデータを作成しなければならない(shall)。それぞれのセットは、1 つの鍵とメッセージデータから構成されなければならない(shall)。評価者は、これらのテストデータについての HMAC タグを TSF に生成させなければならない(shall)。結果として生じる MAC タグは、同様の鍵とともに既知の良好な実装を用いて HMAC タグを生成した結果と比較されなければならない(shall)。

239 CMAC が選択された場合：

240 サポートされるパラメタセットのそれぞれについて、評価者は少なくとも 15 セットのテストデータを作成しなければならない(shall)。それぞれのセットは、1 つの鍵とメッセージデータから構成されなければならない(shall)。テストデータは、あるものは最終ブロックとして不完全ブロック、あるものは最終ブロックとして完全ブロックを持つような、異なる長さのメッセ

ージを含まなければならない(shall)。テストデータ鍵には、既約多項式 R_b を用いて、及び用いないでの両方により、サブ鍵 K1 が生成される場合を、既約多項式 R_b を用いて、及び用いないでの両方により、サブ鍵 K2 が K1 から生成される場合と同様に含まなければならない(shall)。(サブ鍵生成及び多項式 R_b については、SP800-38E で定義されるとおりである。) 評価者は、これらのテストデータについての CMAC タグを TSF に生成させなければならない (shall)。結果として生じる MAC タグは、既知の良好な実装を用いた同様の鍵とともに CMAC タグを生成した結果と比較されなければならない(shall)。

4.1.2.4 FCS_COP.1(d) 暗号操作 (鍵ラッピング)

4.1.2.4.1 TSS

241 評価者は、鍵ラッピング機能の記述について TSS に含まれていることを検証しなければならない、また鍵ラッピングが適切な特定に従って承認された鍵ラッピングアルゴリズムを使用することを検証しなければならない(shall)。

4.1.2.4.2 操作ガイダンス

242 本 SFR のための AGD 評価アクティビティは、一切ない。

4.1.2.4.3 KMD

243 評価者は、すべての鍵が承認された方法を用いてラッピングされること、及び鍵ラッピングがいつ発生するかについての記述を保証するため、KMD をレビューしなければならない(shall)。

4.1.2.4.4 テスト

244 本 SFR のためのテスト評価アクティビティは、一切ない。

4.1.2.5 FCS_COP.1(e) 暗号操作 (鍵配送)

4.1.2.5.1 TSS

245 評価者は、RSA 方式の上位レベル記述及び使用されている暗号鍵長、及び鍵配送のために利用されている非対称アルゴリズムが RSA であることを TSS が提供することを検証しなければならない(shall)。1 つ以上の方式／鍵長が許可される場合、評価者は、方式と鍵長のすべての組み合わせを確認し、テストしなければならない(shall)。1 つ以上の規定された鍵長があるかもしれないーRSA モジュラス長(及び／または暗号化指数サイズ)、AES 鍵長、ハッシュ長、MAC 鍵／MAC タグ長。

246 もし KTS-OAEP 方式が選択された場合、評価者は、ハッシュ関数、マスク生成関数、乱数ビット生成器、暗号化プリミティブ及び復号プリミティブについて、TSS が特定していることを検証しなければならない(shall)。

247 もし KTS-KEM-KWS 方式が選択された場合、評価者は、鍵導出方法、AES ベースの鍵ラッピング方法、秘密値カプセル化手法、及び乱数生成器について、TSS が特定していることを検証しなければならない(shall)。

4.1.2.5.2 操作ガイダンス

248 本 SFR のための AGD 評価アクティビティは、一切ない。

4.1.2.5.3 KMD

249 本 SFR のための KMD 評価アクティビティは、一切ない。

4.1.2.5.4 テスト

250 それぞれのサポートされる鍵配送方式について、評価者は、独立に作られた鍵配送エンティティのリモートインスタンスと共に鍵配送を、既知の RSA 鍵ペアを用いて要求するような、少なくとも 25 セションを開始しなければならない(shall)。評価者は、TOE の送信側から、及び受信側へと通過するトラフィクを観測しなければならない(shall)、また採用された鍵配送方式に特有の、以下のテストを実行しなければならない(shall)。

251 KTS-OAEP 方式が選択された場合、評価者は、以下のテストを実行しなければならない(shall)：

1. 評価者は、TOE の RSA-OAEP 暗号化操作によって生成された、それぞれの暗号文、C について検査しなければならない(shall)、また RSA 鍵長により 256 バイトまたは 384 バイトのいずれかの正しい長さであることを確認しなければならない(shall)。評価者は、TOE の RSA-OAEP 復号操作へ間違った長さの何らかの暗号文の供給も行わなければならない(shall)、そして間違った入力が検出され、復号操作がエラーコードと共に終了することを検証しなければならない(shall)。
2. 評価者は、TOE の RSA-OAEP 暗号化操作によって生成された、それぞれの暗号文、C について、正しい暗号文の整数 C へ変換しなければならない(shall)、また em = RSADP((n,d),c) を計算するため、復号プリミティブを用いて、em をエンコードされたメッセージ EM へ変換しなければならない(shall)。評価者は、次に EM の最初のバイトが 0x00 であることをチェックしなければならない(shall)。評価者は、TOE の RSA-OAEP 復号操作へ、EM の最初のバイトが 0x00 以外の値にセットされたような何らかの暗号文の供給も行わなければならない(shall)、そして、間違った入力が検出され、復号操作がエラーコードと共に終了することを検証しなければならない(shall)。
3. 評価者は、TOE の RSA-OAEP 暗号化操作によって生成された、RSADP を用いてそれぞれの暗号文を復号しなければならない(shall)、また HA' || X を復元するため、OAEP でコード操作(NIST SP 800-56B section 7.2.2.4 で定義される) を実行しなければならない(shall)。それぞれの HA'について、評価者は、対応する A と規定されたハッシュアルゴリズムを取り、HA' = Hash(a)であることを検証しなければならない(shall)。評価者は、A 値が不正に合格するような何らかの RSA-OAEP 復号を実行するよう TOE に強制も行わなうべきである(should) [行わなければならない(shall) ?] 、そして評価者は、エラーが検出されることを検証するべきである(should) [しなければならない(shall)?]。
4. 評価者は、フォーマットが PS || 01 || K の形式、ここで PS はゼロまたはより連続した 0x00 のバイトからなり、K は配送された鍵材料であ

るようなものであることを保証するため、OAEP.テスト.3 で復元された文字列 'X' のフォーマットをチェックしなければならない(shall)。評価者は、TOE の RSA-OAEP 復号操作へ、結果として文字列 'X' が正しいフォーマットを持たないような (例、左端の non-zero バイトが 0x01 でない) 何らかの暗号文の供給も行うべきである(should)[しなければならない(shall)?]、そして評価者は、エラーが検知されることを検証するべきである(should) [しなければならない(shall)?]。

5. 評価者は、すべての検出可能な復号エラーにトリガーをかけて、返されるエラーコードが同じであり、発生したエラーの種別について送信者に何の情報も与えられないことを検証しなければならない(shall)。評価者は、TOE の受信者側の操作からの一切の中間結果が送信者へ明らかにされないことについても検証しなければならない(shall)。

252 KTS-KEM-KWS 方式が選択された場合、評価者は、以下のテストを実行しなければならない(shall) :

1. 評価者は、TOE の RSA-KEM-KWS 暗号化操作によって生成された、それぞれの暗号文、C について検査しなければならない(shall)、また暗号文の長さ(バイト)、cLen が nLen (RSA 公開鍵のモジュラスの長さ(バイト)) よりも大きいこと、及び cLen – nLen が鍵ラッピングアルゴリズムによってサポートされるバイト長と一貫していることを確認しなければならない(shall)。評価者は、RSA-KEM-KWS 復号操作へサポートされない長さの何らかの暗号文の供給も行わなければならない(shall)、そしてエラーが検出され、復号処理が停止することを検証しなければならない(shall)。

2. 評価者は、TOE の送信側によって生成された暗号文 C を、その C0 と C1 コンポーネントへ分割し C0 から秘密値 Z を復元するために RSA 復号プリミティブを使用しなければならない(shall)。評価者は、Z により表現される符号なし整数が 1 よりも大きく、n-1 よりも小さいこと、ここで、n は RSA 公開鍵のモジュラスとする、をチェックしなければならない(shall)。評価者は、暗号文が秘密値 Z を用いて生成されるような例を構築し、RSA-KEM-KWS 復号処理がエラーを検出することを確認しなければならない(shall)。同様に、評価者は、暗号文が秘密値 Z = n – 1 を用いて生成されるような例を構築し、RSA-KEM-KWS 復号処理がエラーを検出することを確認しなければならない(shall)。

3. 評価者は、NIST SP 800-56B section 7.2.3.4 で与えられる RSA-KEM-KWS 復号処理に従って、秘密値 Z の復元、鍵ラッピング鍵 KWK の導出、KWA-暗号文のラッピング解除に成功するよう試行しなければならない(shall)。鍵ラッピングアルゴリズムが AES-CCM である場合、評価者は、ラッピングされた鍵材料を用いて合格したような、任意の（ラッピング解除された）対応するデータの値 A が正しいことを検証しなければならない(shall)。評価者は、TOE の RSA-KEM-KWS 復号操作へ間違った暗号文の例を供給しなければならない(shall)、そして復号エラーが検出されることを検証しなければならない(shall)。同様に鍵ラッピングアルゴリズムが AES-CCM である場合、評価者は、間違ったノンスが RSA-KEM-KWS 復号操作へ与えられる

ような、少なくとも 1 回の復号を試行しなければならない(shall)、そして復号エラーが検出されることを検証しなければならない(shall)。

4. 評価者は、すべての検出可能な復号エラーにトリガーをかけて、返されるエラーコードが同じであり、発生したエラーの種別について送信者に何の情報も与えられないことを検証しなければならない(shall)。評価者は、TOE の受信者側の操作からの一切の中間結果が送信者へ明らかにされないことについても検証しなければならない(shall)。

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

4.1.2.6.1 TSS

253 評価者は、暗号で利用される鍵長と暗号で使用されるモードについての記述が TSS に含まれていることを検証しなければならない(shall)。

4.1.2.6.2 操作ガイダンス

254 複数の暗号モードがサポートされている場合、評価者は、具体的なモード／鍵長がエンドユーザにより選択される方法を決定するため、ガイダンス文書を検査すること。

4.1.2.6.3 KMD

255 本 SFR のための KMD 評価アクティビティは、一切ない。

4.1.2.6.4 テスト

256 以下のテストは、SFR における選択に基づく条件付きのものである。

257 **AES-CBC テスト**

258 下記の AES-CBC テストについて、平文、暗号文、及び IV 値は、128 ビットブロックから構成されなければならない(shall)。正確性を決定するため、評価者は、その結果得られた値を同じ入力を既知の良好な実装へ入力することによって得られたものと比較しなければならない(shall)。

259 これらのテストは、NIST の AES アルゴリズム検証スイート(AESAVS)(http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf)で記述されたものと等価であることを意図している。AES-CBC 実装を検査するために特別に用意された既知解の値は、NIST の CAVS アルゴリズム検証ツールを用いて、または利用可能であれば NIST の自動化されたアルゴリズムテストのための ACPV サービス(acvp.nist.gov)から得ることができる。AESAVS 文書から得られた NIST の AES 既知解テスト値の例のようなスタティックなソースから得られる値を評価者が利用したり、明示的に AES-CBC 実装の検査用に生成されたものでない値を利用することは、推奨されない。

260 **AES-CBC 既知解テスト**

261 KAT-1 (GFSBox):

262 AES-CBC の暗号化機能をテストするため、評価者は 5 個の異なる平文の値を選択されたそれぞれの鍵長について供給し、すべてゼロの鍵の値とすべ

てゼロの IV を用いて所与の平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない(shall)。

263 AES-CBC の復号機能をテストするため、評価者は 5 個の異なる暗号文の値を選択されたそれぞれの鍵長について供給し、すべてゼロの鍵の値とすべてゼロの IV を用いて所与の暗号文の AES-CBC 復号から得られる平文の値を取得しなければならない(shall)。

264 KAT-2 (KeySBox):

265 AES-CBC の暗号化機能をテストするため、評価者は 5 個の異なる鍵の値を選択されたそれぞれの鍵長について供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの平文の AES-CBC 暗号化から得られる暗号文の値を取得しなければならない(shall)。

266 AES-CBC の復号機能をテストするため、評価者は 5 個の異なる鍵の値を選択されたそれぞれの鍵長について供給し、所与の鍵の値とすべてゼロの IV を用いてすべてゼロの暗号文の AES-CBC 復号から得られる平文の値を取得しなければならない(shall)。

267 KAT-3 (Variable Key) :

268 AES-CBC の暗号化機能をテストするため、評価者は選択されたそれぞれの鍵長(下記のとおり)について 1 セットの鍵を供給し、それぞれの鍵とすべてゼロの IV を用いてすべてゼロの平文の AES 暗号化から得られる暗号文の値を取得しなければならない(shall)。

269 それぞれのセットにおける鍵 i は、左端の i ビット目までが 1 にセットされ、残りのビットがゼロにセットされるようにしなければならない(shall)、ここで i の値は、1 から鍵長とする。鍵と対応する暗号文は、AESAVS、Appendix E に列挙されている。

270 AES-CBC の復号機能をテストするため、評価者は、上記から得られた暗号文を復号するため、上記と同じ鍵を使用しなければならない(shall)。それぞれの復号は、すべてゼロの平文が得られるべきである(should)。

271 KAT-4 (Variable Text):

272 AES-CBC の暗号化機能をテストするため、選択されたそれぞれの鍵長について、評価者は、1 セットの 128 ビットの平文の値(下記のとおり)を供給し、それぞれの長さの 1 つの鍵とすべてゼロからなる IV を用いてそれぞれの平文の AES-CBC 暗号化から得られる暗号文をを取得しなければならない(shall)。

273 平文の値 i は、左端 i ビット目までが 1 にセットされ、残りのビットはゼロにセットされるようにしなければならない(shall)、ここで i の値は、1 から 128 とする。平文の値は、AESAVS、Appendix D に列挙されている。

274 AES-CBC の復号機能をテストするため、選択されたそれぞれの鍵長について、上記からの平文の値を使用し、AES-CBC は、すべてゼロからそれぞれの長さの 1 つの鍵とすべてゼロからなる IV を用いてそれぞれの暗号文の値を復号すること。

275 **AES-CBC Multi-Block Message Test**

276 評価者は、選択されたそれぞれの鍵長について、*i* ブロックからなる 9 個のメッセージ (ここで 2 < *i* <=10) を暗号化することによって、暗号化機能をテ

ストしなければならない(shall)。それぞれのテストのため、評価者は、鍵、IV 及び長さ *i* ブロックの平文メッセージを供給し、AES-CBC を用いてメッセージを暗号化しなければならない(shall)。得られる暗号文の値は、既知の良好な実装を用いて平文メッセージを暗号化した結果と比較されなければならない(shall)。

277 評価者は、選択されたそれぞれの鍵長について、*i* ブロックからなる 9 個のメッセージ (ここで 2 < *i* <=10) を復号することによって、復号機能をテストしなければならない(shall)。それぞれのテストのため、評価者は、鍵、IV 及び長さ *i* ブロックの暗号文メッセージを供給し、AES-CBC を用いてメッセージを復号しなければならない(shall)。得られる平文の値は、既知の良好な実装を用いて暗号文メッセージを復号した結果と比較されなければならない(shall)。

278 **AES-CBC モンテカルロテスト**

279 評価者は、選択されたそれぞれの鍵長について、100 個の平文、IV、及び鍵についての 3 つ組のセットを用いて、暗号化機能をテストしなければならない(shall)。

280 評価者は、選択されたそれぞれの鍵長について疑似ランダムな値の 3 つ組を 1 つ供給しなければならない(shall)。この平文、IV、及び鍵の 3 つ組は、残りの 99 個の 3 つ組を生成するため、及びそれぞれの 3 つ組について AES-CBC 暗号化の 1000 回の反復を通して実行するため、以下のアルゴリズムへの入力として提供されること。

281
```
# Input: PT, IV, Key
Key[0] = Key
IV[0] = IV
PT[0] = PT

for i = 1 to 100 {
        Output Key[i], IV[i], PT[0]
        for j = 1 to 1000 {
        if j == 1 {
                CT[1] = AES-CBC-Encrypt(Key[i], IV[i], PT[1])
                PT[2] = IV[i]
        } else {
                CT[j] = AES-CBC-Encrypt(Key[i], PT[j])
                PT[j+1] = CT[j-1]
        }
    }
      Output CT[1000]

      If KeySize == 128 { Key[i+1] = Key[i] xor CT[1000] }
      If KeySize == 256 { Key[i+1] = Key[i] xor ((CT[999] << 128) | CT[1000]) }

      IV[i+1] = CT[1000]
      PT[0] = CT[999]
 }
```

282 1000 回目の反復処理 (すなわち、CT[1000]) において計算された暗号文が、選択されたそれぞれの鍵長について 100 個の 3 つ組のそれぞれの結果とな

る。この結果は、既知の良好な実装を用いて同一の値により 1000 回反復処理を実行した結果と比較されなければならない(shall)。

283 評価者は、暗号化と同一のテストを用い、CT と PT とを入れ替え、AES-CBC 暗号化を AES-CBC 復号で置き換えて、復号機能をテストしなければならない(shall)。

284 **AES-GCM テスト**

285 評価者は、以下の入力パラメタ長のそれぞれの組み合わせについて、AES-GCM の認証付き暗号化機能をテストしなければならない(shall)：

128 ビット及び 256 ビットの鍵

2 通りの平文の長さ。 1 つの平文の長さは、サポートされる場合、128 ビットのゼロ以外の整数倍としなければならない(shall)。他の平文の長さは、サポートされる場合、128 ビットの整数倍であってはならない(shall not)。

3 通りの AAD（訳注：Additional Authenticated Data）の長さ。 1 つの AAD 長は、サポートされる場合、0 としなければならない(shall)。1 つの別の AAD 長は、サポートされる場合、128 ビットのゼロ以外の整数倍としなければならない(shall)。残りの 1 つの AAD 長は、サポートされる場合、128 ビットの整数倍であってはならない(shall not)。

2 通りの IV の長さ。 96 ビットの IV がサポートされる場合、テストされる 2 通りの IV 長の一方を 96 ビットとしなければならない(shall)。

286 評価者は、上記のパラメタ長の組み合わせのそれぞれについて、10 個の鍵、平文、AAD、及び IV の組を 1 セット用いて暗号化機能をテストし、AES-GCM 認証付き暗号化から得られた暗号文の値とタグを取得しなければならない(shall)。サポートされているタグ長はそれぞれ、10 個のセットにつき少なくとも 1 度はテストされなければならない(shall)。IV の値は、それが既知である限り、評価者によって供給されても、テストされている実装によって供給されてもよい。

287 評価者は、上記のパラメタ長の組み合わせのそれぞれについて、10 個の鍵、平文、暗号文、タグ、AAD、及び IV の 5 つ組を 1 セット用いて復号機能をテストし、認証に関する合格／不合格結果、及び合格の場合には復号した平文を取得しなければならない(shall)。セットには、合格となる 5 組と不合格となる 5 組が含まれなければならない(shall)。

288 各テストの結果は、評価者により直接取得されるか、または実装者へ入力を供給してその結果を受領することによって取得するかのいずれかでよい。正確性を決定するため、評価者は、結果の値を既知の良好な実装へ同一の入力を与えることによって得られた値と比較しなければならない(shall)。

289 **XTS-AES Test**

290 評価者は、以下の入力パラメタ長の組み合わせのそれぞれについて、XTS-AES の暗号化機能をテストしなければならない(shall)：

256 ビット (AES-128 用) 及び 512 ビット (AES-256 用) の鍵

3 通りのデータユニット(すなわち、平文) の長さ。 データユニット長の 1 つは、サポートされる場合、128 ビットのゼロ以外の整数倍としなけ

ればならない(shall)。データユニット長の別の 1 つは、サポートされる場合、128 ビットの整数倍としなければならない(shall)。3 番目のデータユニット長は、サポートされる最も長いデータユニット長、または 216 ビットのいずれか小さいほうとしなければならない(shall)。

291 100 個の（鍵、平文及び 128 ビットのランダムな tweak 値）の 3 つ組を 1 セット用いて、XTS-AES 暗号化から得られた暗号文を取得すること。

292 評価者は、実装がサポートする場合、tweak 値の代わりにデータユニットシーケンス番号を供給してもよい。データユニットシーケンス番号は、実装により内部的に tweak 値へ変換されるような、0 から 255 までの範囲の 10 進数である。

293 評価者は、平文の値を暗号文の値に置き換え、また XTS-AES 暗号化を XTS-AES 復号に置き換えて、暗号化と同一のテストを用いて XTS-AES の復号機能をテストしなければならない(shall)。

4.1.2.7 FCS_COP.1(g) 暗号操作 (鍵暗号化)

4.1.2.7.1 TSS

294 評価者は、TSS に暗号化のために使用される鍵長及び鍵暗号化のために使用されるモードの記述が含まれていることを検証しなければならない(shall)。

4.1.2.7.2 操作ガイダンス

295 複数の鍵暗号化モードがサポートされる場合、評価者は、エンドユーザによる具体的なモード／鍵長を選択する方法が記述されていることを決定するため、ガイダンス証拠資料を検査すること。

4.1.2.7.3 KMD

296 評価者は、KMD に鍵暗号化が鍵チェインの一部として使用される方法の記述が含まれていることを検証するため、ベンダの KMD を検査しなければならない(shall)。

4.1.2.7.4 テスト

297 AES テストは、FCS_COP.1(f)暗号操作(AES データ暗号化／復号)に従うべきである(should)。

4.1.3 暗号鍵導出 (FCS_KDF_EXT)

4.1.3.1 FCS_KDF_EXT.1 暗号鍵導出

4.1.3.1.1 TSS

298 評価者は、TSS が鍵導出関数の記述を含んでいることを検証しなければならない、また鍵導出が SP 800-108 及び SP 800-132 に従った承認された導出モード及び鍵拡張アルゴリズムを使用していることを検証しなければならない(shall)。

4.1.3.1.2 操作ガイダンス

299 本 SFR のための AGD 評価アクティビティは、一切ない。

4.1.3.1.3 KMD

300 評価者は、すべての使用される鍵が承認された手法を用いて導出されること、及びどのように、いつ、鍵が導出されるかについての記述を保証するため、ベンダの KMD を検査しなければならない(shall)。

4.1.3.1.4 テスト

301 本 SFR のためのテスト評価アクティビティは、一切ない。

4.1.4 乱数ビット生成 (FCS_RBG_EXT)

4.1.4.1 FCS_RBG_EXT.1 乱数ビット生成

4.1.4.1.1 TSS

302 サードパーティにより提供される RBG サービスについて、評価者は、TSS にこのような情報源から受け取る期待されるエントロピー量についての記述、及びサードパーティの情報源の出力の処理に関する完全な記述が含まれていることを保証しなければならない(shall)。評価者は、この記述が DRBG にシード値として与えるための FCS_RBG_EXT.1.2 における選択と一貫していることを検証しなければならない(shall)。ST が複数の DRBG を特定する場合、評価者は、それぞれの DRBG メカニズムの使用が識別されていることを検証するため、TSS を検査しなければならない(shall)。

4.1.4.1.2 操作ガイダンス

303 評価者は、選択された DRBG メカニズムを使用するために TOE をどのように設定するかについて、必要な場合、AGD ガイダンスが管理者に指示していることを検証しなければならない(shall)。また、本 cPP で必要とされる RBG サービス用の DRBG をインスタンス作成（Instantiate）／コールする方法についての情報を提供することを検証しなければならない(shall)。

4.1.4.1.3 KMD

304 本 SFR のための KMD 評価アクティビティは、一切ない。

4.1.4.1.4 テスト

305 評価者は、RNG 実装について 15 回の試行を実行しなければならない(shall)。RNG が TOE によって設定で変更可能であれば、評価者はそれぞれの設定について 15 回の試行を実施しなければならない(shall)。評価者は、RNG の設定についての操作ガイダンスにおける指示が有効であることを検証しなければならない(shall)。

306 RNG が予測に対する対抗が可能な場合、各試行は、(1) DRBG を Instantiate する、(2) ランダムビットの最初のブロックを Generate する、(3)ランダムビットの 2 番目のブロックを Generate する、(4) Uninstantiate する、より構成される。評価者は、各試行について８つの入力値を生成しなければならない。最初は、カウント (0-14) となる。次の３つは、Instantiate 操作のため、エントロピー入力、ノンス、及び Personalization String である。次の２つは、最初の Generate コールのための、追加の入力と最初の Generate コールのた

めのエントロピー入力である。最後の２つは、2 回目の Generate コールのための、追加の入力とエントロピー入力である。これらの値はランダムに生成される。「ランダムビットの１ブロックを生成する」とは、（NIST SP800-90A に定義されるとおり）出力ブロック長と等しい戻り値ビットの数でランダムビットが生成されることを意味している。

307 RNG が予測に対する対抗を持たない場合、各試行は、(1) DRBG を Instantiate する、(2) ランダムビットの最初のブロックを Generate する、(3) Reseed する、(4) ランダムビットの 2 番目のブロックを Generate する、(5) Uninstantiate する、より構成される。評価者は、ランダムビットの 2 番目のブロックが予測された値であることを検証する。評価者は、各試行について８つの入力値を生成しなければならない。最初は、カウント (0-14) となる。次の３つは、Instantiate 操作のため、エントロピー入力、ノンス、及び Personalization String である。5 番目の値は、最初の Generate コールのための、追加の入力である。6 番目と 7 番目は、Reseed コールのための追加の入力とエントロピー入力である。最後の値は、2 回目の Generate コールのための、追加の入力である。

308 以下のパラグラフは、評価者によって生成／選択される入力値のいくつかについてのさらなる情報が含まれている。

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

Nonce (ノンス) : ノンスがサポートされている場合（導出関数を持たない CTR_DRBG は、ノンスを使用しない）、ノンスビット長は、シード長の半分となる。

Personalization string: personalization string の長さは、シード長以下でなければならない。実装が単一の personalization string 長をサポートする場合、同一の長さが両方の値として使用することができる。複数のストリング長がサポートされる場合、評価者は、２つの異なる長さの personalization string を用いなければならない。実装が personalization string を使用しない場合、値が供給される必要はない。

Additional input（追加の入力）: 追加の入力ビット長は、personalization string 長と同様のデフォルト及び制限を持つ。

4.1.5 サブマスクコンバイニング (FCS_SMC_EXT)

4.1.5.1 FCS_SMC_EXT.1 サブマスクコンバイニング

4.1.5.1.1 TSS

309 複数の許可要素から生成される複数サブマスクが BEV または中間の鍵を形成するために一緒に XOR される場合、TSS セクションにはこれが実行される方法を特定されなければならない(shall) (例、順序の要件がある場合、チェックが実行される、等)。評価者は、どのように生成される出力の長さが少なくとも BEV のものと同じであるかについて。TSS に記述されていることも確認しなければならない(shall)。

4.1.5.1.2 操作ガイダンス

310 本 SFR のための AGD 評価アクティビティは、一切ない。

4.1.5.1.3 KMD

311 評価者は、承認されたコンバイニングが使用されること及びそれが弱体化されないことまたは鍵材料の暴露招かないことを保証するため、KMD をレビューしなければならない(shall)。

4.1.5.1.4 テスト

312 評価者は、以下のテストを実行しなければならない(shall)：

313 テスト 1 [条件付き]：1 つ以上の許可要素がある場合、要求される許可要素の供給失敗は、暗号化されたデータのアクセスを招かないことを保証しなさい。

4.2 TSF の保護 (FPT)

4.2.1 ファームウェアアップデート検証 (FPT_FUA_EXT)

4.2.1.1 FPT_FUA_EXT.1 ファームウェアアップデート検証

4.2.1.1.1 TSS

314 評価者は、TOE がどのように RTU を利用するか、鍵のタイプまたはハッシュ値はどのようなものか、及び RTU 上にどこにその値は格納されるかについて、TSS に記述されていることを保証するため、TSS を検査しなければならない(shall)。評価者は、TSS にオリジナルのファームウェアがどこに存在するか(格納場所について)の記述が含まれていることも検証しなければならない(shall)。

4.2.1.1.2 操作ガイダンス

315 本 SFR のための AGD 評価アクティビティは、一切ない。

4.2.1.1.3 KMD

316 本 SFR のための KMD 評価アクティビティは、一切ない。

4.2.1.1.4 テスト

317 本 SFR のためのテスト評価アクティビティは、一切ない。

5 SAR の評価アクティビティ

318 以下のセクションは、関連する cPP（上記のセクション 1.1 を参照）に含まれるセキュリティ保証要件のための評価アクティビティを特定する。評価アクティビティは、TOE の特定の技術分野に適用するために、より一般的な CEM 保証要件の解釈である。

319 要件が技術依存でない場合、評価者は CEM ワークユニット（例、ASE、ALC_CMC.1、ALC_CMS.1）を実行することが期待されており、それらのアクティビティは cPP の一部として表現するよりも、むしろ、ここでは再掲しない。

5.1 ASE: セキュリティターゲット評価

320 ここでは、セキュリティターゲットにおいて cPP への完全適合を主張する評価のための評価アクティビティが定義される。ASE のその他の観点は CEM に定義されているとおりである。

5.1.1 適合主張 (ASE_CCL.1)

321 以下の表は、cPP への完全適合を決定するための特定の ASE_CCL.1 エレメントに対して取られるべきアクションを示している。

ASE_CCL.1 エレメント	*評価者アクション*
ASE_CCL.1.8C	評価者は、PP と ST におけるセキュリティ課題定義の文章が同一であることをチェックしなければならない。
ASE_CCL.1.9C	評価者は、PP と ST におけるセキュリティ対策方針の文章が同一であることをチェックしなければならない。
ASE_CCL.1.10C	評価者は、ST のセキュリティ要件の文章が cPP におけるすべての必須の SFR、及び他の SFR（ST において追加された繰り返しを含む）でなされた選択によって必要とされるすべての選択ベースの SFR を含んでいることをチェックしなければならない。評価者は、その他の SFR が（cPP における SFR の繰り返しは別として）ST に存在する場合、それらは cPP において指定されたオプションの SFR のリストからのみ取られたものである(cPP は、オプショナル SFR を含むことは必要ではないが、そうしてもよい)。cPP からのオプション SFR が ST に含まれる場合、評価者は、適用されたオプション SFR によって必要とされる選択ベースの SFR が ST にも含まれていることチェックしなければならない。

5.2 ADV: 開発

5.2.1 基本機能仕様 (ADV_FSP.1)

322 本保証コンポーネントの評価アクティビティ(EA)は、AGD 文書に記述されたインタフェース(例、アプリケーションプログラムインタフェース、コマンドラインインタフェース、グラフィカルユーザインタフェース、ネットワークインタフェース)、及び機能要件(SFR) に応えて TOE 要約仕様(TSS)で

おそらく特定されたインタフェースを理解することに焦点を当てている。この証拠資料に対して実行されるべき具体的な評価者アクションは、セクション 2 *(SFR の評価アクティビティ)* において、またセクション 5 のその他の部分で AGD、ATE、及び AVA の SAR に関する EA において、それぞれの SFR について(関連する場所で)特定されている。

323 本セクションで表現される EA は、CEM ワークユニット ADV_FSP.1-1、ADV_FSP.1-2、ADV_FSP.1-3、及び ADV_FSP.1-5 に対処する。

324 EA は、評価者によるより客観的で再現可能なアクションとなるように、CEM ワークユニットを明確化のための言い換え、解釈を行っている。本 SD における EA は、評価者が等価なアクションの一貫した実行を保証することを意図している。

325 したがって、評価における本保証コンポーネントのために検査されるべき文書は、セキュリティターゲット、AGD 証拠資料、及び cPP によって要求される必須の補足情報である：追加の「機能仕様書」証拠資料は、EA を満たすためにはまったく必要ない。評価のために必要なインタフェースは、各 SFR の列挙された EA への参照により特定され、セキュリティターゲット、AGD 証拠資料、及び CC 評価の目的のための別リストというよりはむしろ cPP で定義された必須の補足情報の文脈の中で特定されることが期待されている。証拠資料の要件を直接特定すること、及び各 SFR の EA の一部としてのそれらの評価は、ADV_FSP.1.2D (ワークユニット AADV_FSP.1-4、ADV_FSP.1-6 及び ADV_FSP.1-7)で求められるトレースは暗黙に取り扱われ、本エレメントに関した別のマッピング情報は要求されないことを意味する。

CEM ADV_FSP.1 ワークユニット	評価アクティビティ
ADV_FSP.1-1　評価者は、機能仕様が SFR 支援及びSFR 実施の各TSFI の目的を記述していることを決定するために、その仕様を***検査しなければならない(shall)。***	5.2.1.1 評価アクティビティ：*評価者は、セキュリティ関連であると特定されるような、それぞれの TSFI の目的と使用方法が記述されていることを保証するため、インタフェース証拠資料を検査しなければならない(shall)。*
ADV_FSP.1-2　評価者は、SFR 支援及びSFR 実施の各TSFI の使用方法が記述されていることを決定するために、機能仕様を***検査しなければならない(shall)。***	5.2.1.1 評価アクティビティ：*評価者は、セキュリティ関連であると特定されるような、それぞれの TSFI の目的と使用方法が記述されていることを保証するため、インタフェース証拠資料を検査しなければならない(shall)。*
ADV_FSP.1-3　評価者は、TSFI の提示がSFR 実施及びSFR 支援の各TSFI に関連するすべてのパラメタを識別していることを決定するために、その提示を***検査しなければならない(shall)。***	5.2.1.2 評価アクティビティ：*評価者は、セキュリティ関連であると特定されるような、それぞれの TSFI のパラメタが特定され、記述されていることを保証するため、インタフェース証拠資料をチェックしなければならない(shall)。*
ADV_FSP.1-4　評価者は、暗黙的にSFR 非干渉として分類されているインタフェースについて、その分類が正しいことを決定するために、開発者によって提供される根拠	CEMのパラグラフ561：「このコンポーネントの残りのワークユニットで要求される分析を行うのに十分な証拠資料が開発者によって提供されていて、SFR 実施及びSFR 支援のインタ

を***検査しなければならない(shall)。***	フェースは明示的に識別されていない場合、このワークユニットは満たされているものとみなされるべきである。」 ADV_FSP.1の残りのワークユニットがEAの完了に際して満たされるので、本ワークユニットは同様に満たされるという結果となる。
ADV_FSP.1-5　評価者は、追跡によってSFR が対応するTSFI にリンクされることを***チェックしなければならない(shall)。***	5.2.1.3 評価アクティビティ：*評価者は、インタフェースから SFR へのマッピングを作るために、インタフェース証拠資料を検査しなければならない(shall)。*
ADV_FSP.1-6　評価者は、機能仕様がSFR の完全な具体化であることを決定するために、その仕様を***検査しなければならない(shall)。***	セクション 2、及び適用可能な場合、セクション 3、4 の SFR に対応する EA は、セキュリティ機能が外部から見えるような(即ち、TSFI において) すべての SFR が網羅されることを保証するために実行される。ゆえに、本ワークユニットの意図は網羅される。
ADV_FSP.1-7　評価者は、機能仕様がSFR の正確な具体化であることを決定するために、その仕様を***検査しなければならない(shall)。***	セクション 2、及び適用可能な場合、セクション 3、4 の SFR に対応する EA は、セキュリティ機能が外部から見えるような(即ち、TSFI において) すべての SFR が対処されること、及びそのインタフェースの記述が SFR で取り込まれた使用に関して正確であることを保証するために実行される。ゆえに、本ワークユニットの意図は網羅される。

表 1：ADV_FSP.1 CEM ワークユニットの評価アクティビティへのマッピング

5.2.1.1 評価アクティビティ：

326 *評価者は、セキュリティ関連であると特定されるような、それぞれの TSFI の目的と使用方法が記述されていることを保証するため、インタフェース証拠資料を検査しなければならない(shall)。*

327 この文脈において、TOE の設定またはその他の管理者機能を実行する（例、監査レビューまたはアップデートの実行）ため、管理者が TSFI を使用する場合、TSFI はセキュリティ関連であるとみなされる。さらに、ST やガイダンス証拠資料で特定されるそれらのインタフェースも、セキュリティ方針を守るものとして (SFR で提示されたとおり)、セキュリティ関連と考えられる。その意図は、適切なテスト網羅性が適用されることを保証するために必要であるような、TOE でのこれらのインタフェースの使用方法の理解をしつつ、これらのインタフェースが適切にテストされることである。

328 評価証拠として提供される一連の TSFI は、管理者ガイダンスと利用者ガイダンスに含まれる。

5.2.1.2 評価アクティビティ：

329 *評価者は、セキュリティ関連であると特定されるような、それぞれの TSFI のパラメタが特定され、記述されていることを保証するため、インタフェース証拠資料をチェックしなければならない(shall)。*

5.2.1.3 評価アクティビティ

330 *評価者は、インタフェースから SFR へのマッピングを作るために、インタフェース証拠資料を検査しなければならない(shall)。*

331 評価者は、提供された証拠資料を用いて、最初に特定を行い、次にセクション 2 で提示された EA を実行するため、インタフェースのテストに関レスる EA を含めて、インタフェースの代表的なものを検査する。

332 それらが、求められる機能を呼び出すために明示的に「マッピング」されているインタフェースを持たないような、何らかの SFR であるかもしれことについて留意されるべきである。例えば、ランダムなビット列の生成、もはや不要となった暗号鍵の破壊、またはセキュアな状態にならないような TSF は、SFR で規定されているかもしれない機能であるが、インタフェースによって呼び出されない。

333 しかし、不十分な設計情報及びインタフェース情報のため、評価者が何らかのその他の必須の EA を実行できない場合、評価者は、適切な機能仕様書が提供されていないという結論を下す権限がある、またそれゆえに、ADV_FSP.1 保証コンポーネントの判定は、「不合格」となる。

5.3 ガイダンス文書 (AGD)

334 TOE について、AGD_OPE と AGD_PRE の個別の要件を満たすため、必ずしも別々の証拠資料を提供する必要はない。本セクションの評価アクティビティは、伝統的な別々の AGD ファミリの下で記述されているが、現実の TOE 文書と AGD_OPE 及び AGD_PRE 要件の間のマッピングが、TOE の一部として (適切なものとして)、管理者と利用者へ配付される証拠資料ですべての要件が満たされる限り、多対多であってもよい。

5.3.1 利用者操作ガイダンス (AGD_OPE.1)

335 利用者ガイダンス証拠資料における具体的な要件及びチェックは各 SFR、及び他のいくつかの SAR（例えば、ALC_CMC.1）に関する個別の評価アクティビティにおける（関連した場所で）識別される。

336 *評価アクティビティ:*

337 評価者は、操作ガイダンスによって満たされる以下の要件をチェックしなければならない(shall)。操作ガイダンスは、TOE 開発者がインタフェースの記述 (例、ホストプラットフォームが SED を設定するため呼び出すかも知れないような複数のコマンド) を提供するような「インテグレータ向けガイド」の形式を取っているかもしれないことについて留意されるべきである。

338 評価された構成の確立と維持で、管理者と利用者が証拠資料の存在と役割を知っているという合理的な保証が得られるようにするため、操作ガイダンス証拠資料は、TOE の一部として (適切なものとして) 管理者と利用者に配付されなければならない(shall)。

339 操作ガイダンスは、セキュリティターゲットで主張されるとおり TOE がサポートするすべての運用環境に対して提供されなければならない(shall)、また、セキュリティターゲットで TOE について主張されたすべてのプラットフォームに適切に対処しなければならない(shall)。これは、一つの文書にすべてが含まれていてもよい。

340 操作ガイダンスの内容は、以下で定義される評価アクティビティにより、上記セクション 2 のすべての個別の SFR について適切なものとして検証されること。

341 SFR 関連の評価アクティビティに追加して、以下の情報も要求される。

- 操作ガイダンスは、TOE の評価された構成に対応するあらゆる暗号エンジンの設定に関する指示を含まなければならない。TOE の CC 評価の間に、他の暗号エンジンの用途について評価もテストもされていないという警告を管理者に提供しなければならない。

- 操作ガイダンスは、管理者的に定義された非アクティブ期間の後、シャットダウンすることをサポートするような IT 環境の設定方法を記述しなければならない。

- 操作ガイダンスは、すべてのサポートされる運用環境及びそれぞれの環境のためのシステム「スリープ」状態を特定し、スリープ状態を無効化する方法についての管理者ガイダンスを提供しなければならない(shall)。上記のとおり、TOE 開発者は、インテグレータ向けガイドを提供してもよく、また「電力状態」はさまざまなレベルで SED が提供する抽象化であってもよい ー 例、デバイスの状態を管理するためにホストプラットフォームが発行するコマンドを単に提供してもよいし、ホストプラットフォームがより洗練された電力管理方法の提供に責任を持ってもよい。

- TOE は、本 cPP の基づく評価の適用範囲に該当しないセキュリティ機能を含むこともありうる。操作ガイダンスは評価アクティビティによってカバーされるセキュリティ機能がどれなのかを管理者に明確に示さなければならない(shall)。

5.3.2 準備手続き (AGD_PRE.1)

342 操作ガイダンスに関しては、準備手続きにおける特定の要件やチェックは各 SFR に関する個別に評価アクティビティにおいて（関連する場所で）識別される。

343 *評価アクティビティ：*

344 評価者は、準備手続きによって満たされる以下の要件をチェックしなければならない(shall)。

345 準備手続きの内容は、上記セクション 2 のすべての個別の SFR について適切であるよう、以下に定義された評価アクティビティによって検証されること。

346 準備手続きは、評価された構成を確立と維持における証拠資料の存在と役割を管理者と利用者が知っていることを合理的に保証するために、TOE の

一部として (適切なものとして) 管理者と利用者に配付されなければならない(shall)。

347 準備手続きの内容は、以下で定義される評価アクティビティによって、上記セクション 2 のすべての個別 SFR について適切なものとして検証される。

348 SFR 関連の評価アクティビティに追加して、以下の情報も要求される。

349 準備手続きには、(セキュリティターゲットで規定される運用環境のセキュリティ対策方針の要件を含め)、セキュリティ機能をサポートする運用環境がその役割を満たせることを管理者が検証する方法についての記述を含まなければならない(shall)。証拠資料は、形式的でない形であるべき(should)で、(一般的な IT 経験を持つが TOE そのものの経験は必ずしも必要ないような IT 担当者を通常含むような) 対象読者により理解と利用が可能なように十分な詳細度で書かれるべきである(should)。

350 準備手続きは、セキュリティターゲットで主張されたとおり TOE がサポートするすべてのプラットフォームに対して提供されなければならない(must)、また、セキュリティターゲットで TOE について主張されたすべてのプラットフォームに適切に対処しなければならない(must)。これは一つの文書にすべてが含まれてもよい。

351 準備手続きには、以下が含まれなければならない

- 各運用環境で TSF のインストールに成功するための指示；及び
- 製品として、及びより大きな運用環境のコンポーネントとして、TSF のセキュリティを管理するための指示；及び
- 保護される管理者機能を提供するための指示。

5.4 ALC: ライフサイクルサポート

5.4.1 TOE のラベル付け (ALC_CMC.1)

352 TOE が提供されたこと、一意な参照でラベル付けされていることを評価しているとき、評価者は、CEM で提示されるとおりのワークユニットを実行すること。

5.4.2 TOE の CM 範囲 (ALC_CMS.1)

353 開発者の CM システムにおいて、開発者の TOE 範囲を評価しているとき、評価者は、CEM で提示されるとおりのワークユニットを実行すること。

5.5 テスト (ATE)

5.5.1 独立テスト – 適合 (ATE_IND.1)

354 操作ガイダンス証拠資料と同様に TSS に記述される機能を確認するため、テストが実行される。テストの焦点は、SFR にて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。

355 評価者は、評価中かもしれない TOE の複数のバリエーションやモデルのテストについての適切な戦略を決定する時に、附属書 B の FDE 同等性検討を調べるべきである。

356 SD (訳注：本書のようなサポート文書) における SFR 関連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特定のテストアクティビティを識別する。このような他の評価アクティビティで識別されるテストは、ATE_IND.1.2E を満たす目的で十分なテストのセットを構成する。評価アクティビティは実行される必要があるテストを識別するが、評価者は各 SFR で指定されるセキュリティ機能についてインタフェースが適切にテストされることを保証することに責任があることに注意することは重要である。

357 *評価アクティビティ：*

358 評価者はテスト構成が ST で指定されたとおり、評価における構成と一貫していることを決定するために TOE を検査しなければならない(shall)。

359 *評価アクティビティ：*

360 評価者は、TOE が適切にインストールされ、既知の状態にあることを保証するため、TOE を検査しなければならない(shall)。

361 *評価アクティビティ：*

362 評価者は、CEM 及び SFR 関連評価アクティビティにおける ATE_IND.1 のテストアクションのすべてをカバーするテスト計画を準備しなければならない。評価アクティビティに列挙されたテストごとにテストケースを用意する必要はないが、評価者は、SFR 関連評価アクティビティにおけるすべての適用可能なテスト要件がテスト計画においてカバーされていることを示さなければならない(shall)。

363 テスト計画はテストされる運用環境を識別し、テスト計画に含まれないが ST に含まれるすべてのプラットフォームについてテスト計画がテストされないプラットフォームに関して正当化を提供すること。この正当化はテストされたプラットフォームとテストされないプラットフォームの間の相違について対処し、その相違が実行されたテストに影響しないことについて議論しなければならない。その相違が影響ないことを単に断言するだけでは不十分で、根拠が提供されなければならない。ST で主張されたすべてのプラットフォームがテストされる場合、根拠は必要ない。

364 テスト計画は、テストされるすべての運用環境の構成や設定、また AGD 証拠資料に含まれるものを超えて必要とされるあらゆる設定アクションについて記述する。評価者は、テストの一部としてまたは標準的なテスト事前調整として、各プラットフォームのインストレーションやセットアップに関して AGD 証拠資料に従うことが期待されていることに注意するべきである。これは、特定のテストドライバまたはツールを含んでもよい。それぞれのドライバまたはツールに関して、ドライバまたはツールが TOE 及びそのプラットフォームによる機能のパフォーマンスに対して不利に働かないように議論（単に断言ではなく）が提供されるべきである。これは、使用されるすべての暗号エンジン（例えば、評価される暗号プロトコルに関して）の設定も含まれる。

365 テスト計画は、それらの目的や期待される結果を達成するために従うべきテスト手続きと同様にハイレベルのテスト目的を識別する。

366 テスト報告書（単にテスト計画の更新されたバージョンであってもよい）は、テストの実際の結果を含み、テスト手続きが実行されるときに実施されるアクティビティについての詳細を記述する。これは、累積的な報告で

なければならない、もしテスト実行が不合格の結果であった場合、修正版がインストールされ、その結果再テストがうまく実行され、報告書は「不合格」結果の後、「合格」結果（詳細についてサポートしつつ）示し、単に「合格」結果 [1]だけではいけない。

5.6 脆弱性評定 (AVA)

5.6.1 脆弱性調査 (AVA_VAN.1)

367 脆弱性分析は、本質的に主観的な活動であるが、最小限のレベルの分析は、定義可能であり、何らかの尺度での客観性と再現性(または少なくとも互換性)を脆弱性分析プロセスにおいて課すことが可能である。このような客観性と再現性を達成するために、評価者がよく定義された活動のセットに従い、他の人がその議論にしたぐことができ評価者として同じ結論を導き出すことができるような書面を文書することが重要である。これによって、異なる評価機関が全く同じ種別の脆弱性を識別すること、または全く同じ結論を導き出すことを保証しないが、そのアプローチは最小レベルの分析及びその分析の適用範囲を定義し、最小レベルの分析が評価機関によって実行されているというある尺度の保証を認証機関へ提供する。

368 これらの目標を満たすため、AVA_VAN.1 の CEM ワークユニットの何らかの詳細化が必要とされる。以下の表は AVA_VAN.1 におけるそれぞれのワークユニットについて、CEM ワークユニットが記述されるとおり実行されるべきであるか、または評価アクティビティによって明確化されているかを示す。明確化が提供されている場合、本明確化への参照が表において提供される。

369

CEM AVA_VAN.1 ワークユニット	評価アクティビティ
AVA_VAN.1-1　評価者は、テスト構成が ST に特定されたとおりに評価における構成と一貫していることを決定するために、TOE を***検査しなければならない。***	評価者は、規定されるとおり CEM ワークユニットを実行しなければならない(shall)。 *iTC がセクション A.3.4 の本分析の実行において利用されるべき任意のツールを規定する場合、以下の文章も本セルに含まれること：「CEM のパラグラフ 1418 で規定されるテスト資源の校正が、附属書 A, セクション A.1.4 に列挙されたツールに対して適用される。」*
AVA_VAN.1-2　評価者は、TOE が適切に設置され、定義された状態にあることを決定するために、そのTOE を***検査しなければならない。***	評価者は、規定されるとおり CEM ワークユニットを実行しなければならない(shall)。

[1] テスターまたはテスト環境の部分に関するエラーに起因する失敗を記録にとどめる必要は無い。ここでの意図は、計画したテストがいつ、当初のテスト計画における具体的なテスト構成、ST 及び操作ガイダンス、または TOE 自体で識別された評価構成に対する変更を必要となる結果となったかについて、完全に明確にすることである。

AVA_VAN.1-3　評価者は、TOE の潜在的脆弱性を識別するために、公開の場で利用できる情報源を***検査しなければならない。***	CEM ワークユニットを附属書 A、セクション A.1 で概説されるアクティビティに置き換える。
AVA_VAN.1-4　評価者は、ETR 内で、テストの候補となり、運用環境のTOE に適用できる識別された潜在的な脆弱性を***記録しなければならない。***	CEM ワークユニットを附属書 A、セクション A.1 の潜在的な脆弱性のリストについての分析アクティビティ、及び附属書 A、セクション A.3 で規定される証拠資料に置き換える。
AVA_VAN.1-5　評価者は、潜在的な脆弱性に対する独立探索に基づいて、侵入テストを***考え出さなければならない。***	CEM ワークユニットを附属書 A、セクション A.2 で規定されるアクティビティに置き換える。
AVA_VAN.1-6　評価者は、潜在的な脆弱性のリストに基づき、テストを再現可能にするために十分に詳細に侵入テスト証拠資料を***作成しなければならない。***テスト証拠資料には、次のものを含めなければならない: a) TOE はどの潜在的な脆弱性の調査のためにテストされるか、その脆弱性の識別; b) 侵入テストを実施するために必要となるすべての必要なテスト装置を接続し、セットアップするための指示; c) すべての侵入テスト前提初期条件を確立するための指示; d) TSF を刺激するための指示; e) TSF のふるまいを観察するための指示; f) すべての期待される結果と、期待される結果と比較するために観察されたふるまいに実施する必要がある分析の記述; g) TOE のテストを終了し、終了後の必要な状態を確立するための指示。	CEM ワークユニットは、附属書 A、セクション A.3 で取り込まれている；実質的な違いは全くない。
AVA_VAN.1-7　評価者は、侵入テストを***実施しなければならない。***	評価者は、規定されるとおり CEM アクティビティを実行しなければならない(shall)。確認された欠陥についての攻撃能力に関するガイダンスについては附属書 A、セクション A.3、パラグラフ 409 を参照すること。
AVA_VAN.1-8　評価者は、侵入テストの実際の結果を***記録しなければならない。***	評価者は、規定されるとおり CEM ワークユニットを実行しなければならない(shall)。
AVA_VAN.1-9　評価者は、ETR に、テスト手法、構成、深さ、及び結果を概説して評価者の侵入テストの成果を***報告しなければならない。***	CEM ワークユニットを附属書 A、セクション A.3 で求められる報告に置き換える。
AVA_VAN.1-10　評価者は、TOE が、運用環境において、基本的な攻撃能力を持つ攻撃者に耐えられることを決定するため	本ワークユニットは、iTC による本サポート文書への包含は基本攻撃能力を持つ攻撃者を対象とするこれらの欠陥から生

に、すべての侵入テストの結果を***検査しなければならない。***	じる脆弱性をを確認させるので、タイプ 1、及びタイプ 2 の欠陥 (附属書 A、セクション A.1 で定義されるとおり) には適用されない。本ワークユニットは、タイプ 3 及びタイプ 4 欠陥のために、附属書 A、セクション A.3 パラグラフ 409 で定義されるアクティビティに置き換えられる。
AVA_VAN.1-11　評価者は、ETR に、すべての悪用され得る脆弱性と残存脆弱性を、次のそれぞれを詳細に述べて***報告しなければならない*****:** a) 出所(例えば、脆弱性が予想されたとき実行していたCEM アクティビティ、評価者に既知である、公表されたものを読んで知った、など); b) 満たされていないSFR(1 つまたは複数); c) 記述; d) 運用環境で悪用されるか否か(つまり、悪用される可能性があるか残存か); e) 識別された脆弱性を実行するために必要な時間量、専門知識のレベル、TOE に関する知識のレベル、機会のレベル、及び装置。及び附属書B.4 の表3 及び4 を使用した対応する値。	CEM ワークユニットを附属書 A、セクション A.3 で求められる報告に置き換えられる。

370 **表 2. AVA_VAN.1 CEM ワークユニットの評価アクティビティへのマッピング**

371 評価アクティビティに要求される詳細レベルのため、指示の大部分は附属書 A に含まれるが、保証アクティビティの「概要」は、以下で提供される。

5.6.1.1 評価アクティビティ(証拠資料):

372 開発者は、TOE を構成するソフトウェア及びハードウェアコンポネントのリストを特定するような証拠資料を提供しなければならない(shall)。ハードウェアコンポネントは、ST で主張されるすべてのシステムに適用され、また少なくとも TOE により使用されるプロセッサを特定するべきである(should)。ソフトウェアコンポーネントは、暗号ライブラリなど、TOE により使用されるわらゆるライブラリを含む。この追加の証拠資料は、単にコンポーネントの名称とバージョン番号のリストであり、分析中に仮説を考案するに評価者により活用される。

373 評価者は、すべての要求される情報が含まれていることを確認するため、ベンダにより提供される以下で概説される証拠資料を検査しなければならない(shall)。この証拠資料は、前に列挙された EA への回答において供給されるように、すでに要求された証拠資料への追加されたものである。

374 上記表 2 に従って CEM により規定されるアクティビティに追加して、評価者は、以下のアクティビティを実行しなければならない(shall)。

5.6.1.2 評価アクティビティ

375 評価者は、附属書 A.1 で定義されるプロセスに従って仮説を考案すること。評価者は、附属書 A.3 のガイドラインに従う報告書で、TOE について生成された欠陥仮説について文書化すること。評価者は、附属書 A.2 に従って、脆弱性分析を実行しなければならない(shall)。分析の結果は、附属書 A.3 に従って報告書に文書化されなければならない(shall)。

376

6 必須の補足情報

377 本サポート文書は、評価用提供物件の一部として供給されることを求めている「補足情報」が様々な場所で参照されている。この用語は、セキュリティターゲットまたは操作ガイダンスに必ずしも含まれる必要のない、公開される必要のない情報を記述することを意図している。このような情報の例は、エントロピー分析、または TOE（またはそのサポート）において用いられる暗号鍵管理アーキテクチャの記述である。このような補足情報に関する要件は関連する cPP において識別される。

378 暗号エンジンのための FDE cPP は、TOE が RNG を提供する場合、鍵管理記述及びエントロピー分析を要求する。 それらの文書を用いて評価者が実施する EA（訳注：評価アクティビティ）は、セクション 2 における適切な SFR の下に書かれている。

7 参考文献

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model CCMB-2012-09-001, Version 3.1 Revision 4, September 2012

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, CCMB-2012-09-002, Version 3.1 Revision 4, September 2012

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 4, September 2012

[CEM] Common Methodology for Information Technology Security Evaluation, CCMB-2012-09-004, Version 3.1 Revision 4, September 2012

[FDE-EE] collaborative Protection Profile for Full Drive Encryption − Encryption Engine, Version 1.5, 22 September 2016

附属書

A 脆弱性分析

A.1 脆弱性情報源

379 CEM ワークユニット AVA_VAN.1-3 は、調査用により良い定義された一連の欠陥、及びこの特定技術に基づいてフォローするための手順を提供するため、本サポート文書で補足されている。利用される用語は、評価チームが欠陥を仮設し、次にそれらの欠陥(欠陥は、CEM で利用されるとおり「潜在的な脆弱性」と等価である)を証明または反証のいずれかを行うような、欠陥仮説法に基づいている。欠陥は、それらが考案される方法に依存する４つの「タイプ」へ分類される。

1. 本 cPP により記述されるその技術に適用可能な欠陥仮説のリストは、セクション A.1.1 で文書かれるとおり公開情報源から導出されるーこの固定セットは、iTC により合意された。さらに、(以下のセクション A.1.1 のプロセスにより定義されるとおり) TOE またはその特定されたコンポーネントに直接適用可能であるような、一連の公開情報源(以下に示されるとおり)についてのエントリと共に補足されている；これは、評価者は、cPP が公開されたので発見されたようなエントリに適用可能なそれらの評価に含めていることをほしょうするためのものである；

2. セクション A.1.2 に記述されるとおり、その技術及び(例えば、その他の公開情報源と脆弱性データベースから導出されるに違いないような)その他の iTC からの入力に特有の学んだことから導出された本書に含まれた欠陥仮説のリスト；

3. 評価者に利用可能な情報から導出された欠陥仮説のリスト；これには、セクション A.1.3 で文書化されたとおりのその他の情報(公開及び／または評価経験に基づく)と同様に、サポート文書(EA に対応する証拠資料、セクション 3.5.11 で記述された証拠資料)に記述されたベンダより提供されたベースライン証拠を含む；及び

4. セクション A.1.4 で規定された iTC 定義のツール(例、nmap、protocol tester)とそれらのアプリケーションの活用を通して生成された欠陥仮説のリスト。

A.1.1 タイプ１仮説―公開脆弱性ベース

380 脆弱性情報の公開情報源についての以下のリストが iTC により選択された：

a. Common Vulnerabilities and Exposures を検索：http://cve.mitre.org/cve/
b. National Vulnerability Database を検索：https://nvd.nist.gov/
c. US-CERT を検索：http://www.kb.cert.org/vuls/html/search

381 上記情報源のリストは、以下の検索用語を用いて検索される：

○一般

- Product name
- underlying components (e.g. OS, Software Libraries (crypto libraries), chipsets)
- drive encryption, disk encryption
- key destruction/sanitization

○EE：

- Underlying components (e.g. chipsets, firmware)

○SED (EE)：

- Self Encrypting Drive (SED), OPAL

○ソフトウェア FDE (AA または EE)：

- Key caching

382 本アクティビティを成功裏に完了するため、評価者は、開発者が提供した彼らの製品の一部として利用されているサードパーティのライブラリ情報のすべてのリストを、バージョン及びその他の特定するための情報と共に利用すること(これは、ASE_TSS.1.1C の一部として本 cPP で要求されている)。これは、TOE の一部としてベンダが活用するハードウェア(チップセット等を含め) に適用する。この TOE 固有の情報は、評価者が上記リストに追加して利用する用語の検索で活用されること。

383 評価者は、選択された要件及びそれぞれの要件に結びつけられた適切なガイダンスについても検討すること。

384 本リストを補足するため、評価者は、cPP の公開日よりもより最近の潜在的な欠陥仮説のリスト、及び上記追加の証拠資料により規定されるとおり TOE とそのコンポーネントに特有のものを決定するため、上記の列挙された情報源について検索を実行しなければならない(shall)。任意の重複－同一または異なる情報源からのエントリから生成されるような具体的なエントリ、または欠陥仮説のいずれかでーは、留意され、評価チームによる検討から除去されることが可能である。

385 TOE の具体的なコンポーネントのタイプ 1 の欠陥仮説生成の一部として、評価者は、欠陥仮説がこの方法(例えば、評価されたコンポーネントのバージョンに対してセキュリティパッチがリリースされている場合、それらのパッチの対象が欠陥仮説の根拠となるかもしれない)で生成されることが可能であるかどうかを決定するため、コンポーネントの製造者のウェブサイトについても検索しなければならない(shall)。

A.1.2 タイプ 2 仮説—iTC 出典のもの

386 この技術についての iTC により生成された欠陥仮説の以下のリストは、脆弱性評定の実行における欠陥仮説として評価チームにより検討されなければならない(shall)：

387 *一般：*

388 EE：

- ソフトウェア FDE：
    - ソフトウェア暗号化インストールプロセスの間、暗号化が中断される可能性がある(例、電源の喪失等)。評価者は、ソフトウェア暗号化がいつレジュームされ、完了するか、すべての利用者データが暗号化されることを検証するべきである(should)。

389 評価者が、本 cPP の将来のバージョンでタイプ 2 と見なされるべきであると彼らが信じるような、タイプ 3、またはタイプ 4 欠陥を発見する場合、かれらは、iTC による検討のためにその欠陥を提出する適切な手段を決定するため、認証機関と共に作業を行うべきである(should)。

A.1.3 タイプ 3 仮説—評価チームによって生成されたもの

390 iTC は、適切な検索用語と脆弱性データベースを熱心に開発するために、開発者と評価機関の知見を活用している。彼らは、評価者が適用可能な使用事例や SFR によって軽減される脅威に基づいて活用するべきである、iTC 出典の仮説についても思慮深く検討した。ゆえに、タイプ 1 とタイプ 2 仮説におけるすべてのとりくみに焦点をあてるような評価のため、iTC の意図は、タイプ 3 仮説は必要ないと決定した。

391 しかし、評価者が考慮すべきと信じるようなタイプ 3 仮説を発見する場合、彼らは仮説の追跡の実現可能性について決定するため、認証機関と共に作業するべきである(should)。認証機関は、潜在的な欠陥仮説が cPP/SD の将来のドラフトにおけるタイプ 2 仮説としての検討のために iTC へ提出するに十分であるかどうかを決定することができる。

A.1.4 タイプ 4 仮説—ツールによって生成されたもの

392 iTC は、タイプ 2 仮説プロセスの間に利用されるべきいくつかのツールを求めている。ゆえに、任意のツールの利用は、タイプ 2 構築内で網羅され、iTC は必要とされる追加のツールがわからない。本 cPP のバージョン 2 の使用事例は、むしろ簡単であるーデバイスは電源切断状態で見つかり、見直し／悪意のメイド攻撃の対象とならない。それが使用事例であるので、iTC は、AA と EE の間の高信頼チェネルがあるという仮定もしている。使用事例が狭いので、新にゅうてすつやふぁじんぐテストの典型で来なモデルではなく、テストの通常のタイプは、適用されない。ゆえに、関連するタイプのツールは、タイプ 2 で参照される。

A.2 評価者脆弱性分析のプロセス

393 欠陥仮説が上記のアクティビティから作成されると、評価チームはこれらを処置する；すなわち、その仮説の証明、反証、または適用不可能の決定を試行する。このプロセスは、以下のようになる。

394 評価者は、TOE の各欠陥仮説を詳細化し、開発者より提供される情報を用いて、または侵入テストによって、反証しようと試みることになる。このプロセス中、評価者は、欠陥が存在するかどうかを決定するため、自由に開発者と対話することができる。これには、開発者に追加の証拠資料 (例、詳細な設計情報、技術スタッフへの相談等) を要求することが含まれる；しかし、これらの議論のすべてに、CB は含まれるべきである。開発者が、評価アクティビティ／cPP の全体的なレベルに適合していないとして情報が要求されることを拒んだり、提出されていれば欠陥が反証できたはずの証拠資料を提供できなかったりした場合、評価者は、一連の適切な資料を以下のように準備する：

- 仮説の策定に使用された情報源の文書、及びそれが特定の TOE 機能に対するセキュリティ侵害の可能性を示す理由；
- それまで提供された証拠資料によって欠陥仮説が証明も反証もできなかった理由；
- 欠陥仮説をさらに調査するために要求される情報の種別。

395 次に認証機関 (CB) が、追加の情報についての要求を承認または却下のいずれかをする。承認された場合、開発者は、欠陥仮説を反証するために、要求された証拠資料を提供する (または、もちろん欠陥を認めてもよい)。

396 各仮説について、評価者は、その欠陥仮説の反証が成功したか、識別された欠陥があることの証明に成功したか、またはさらなる調査を要求するかについて、記録することになる。重要なのは、以下のセクション A.3 に概説されるとおり、結果が文書化されることである。

397 評価者が欠陥を見つける場合、評価者は、これらの欠陥を開発者へ報告することになる。報告されたすべての欠陥は、以下のとおり対処されなければならない(must)。

398 開発者がその欠陥が存在すること及びそれが基本的攻撃能力で悪用可能であることを確認した場合、開発者によって変更がなされ、もたらされる解決策は、評価者によって合意され、評価報告書の一部として記録される。

399 開発者、評価者、及び CB が、その欠陥が基本的攻撃能力を超えてのみ悪用可能であることに合意しその他の理由で解決が要求されない場合、一切の変更は行われず、欠陥は、CB 内部の報告書 (ETR) に残存脆弱性として記録される。

400 開発者、評価者が、その欠陥が基本的攻撃能力を超えてのみ悪用可能であることに合意したが、通常の使用事例または運用環境のような技術特有または cPP 特有の観点から解決することが重要であると見なされる場合、変更が開発者によって行われ、もたらされる解決が評価者によって合意され、評価報告書の一部として記録される。

401 ある欠陥の存在、その攻撃能力、またはそれが重要と見なされるべきかについての疑義に関する、評価者とベンダの間での意見の相違は、CB によって解決される。

402 評価者により実行されるあらゆるテストは、以下のセクション A.3 で概説されるとおりテスト報告書に文書化されなければならない(shall)。

403 セクション A.3 に示されるように、cPP に適合する TOE について実施された脆弱性分析に関する公開ステートメントは、タイプ 1 及び 2 (セクション A.1 に定義される) 欠陥仮説のみに関連付けられた欠陥のカバレージに限定される。iTC がこれらの仮説の候補を作成したという事実は、対処されなければならない(must)ことを示している。

A.3 報告

404 評価者は、テストの取り組みに関して 2 つの報告書を作成しなければならない； ひとつは公開向けの (すなわち、評価報告書(ETR)のサブセットであるような、機密情報を含まない評価報告書、)、もうひとつは監督している CB へ配付される完全な ETR である。

405 公開向けの報告書には、以下が含まれる：

406 * 公開情報源の検索のための手順がサポート文書のセクション A.1.1 の指示に従って行われたときに返った欠陥識別子；

407 * 評価者が本サポート文書のセクションの A.1.1 で規定されたタイプ 1 の欠陥仮説及び本サポート文書のセクション A.1.2 で規定されたタイプ 2 の欠陥仮説を検査したことを示すステートメント。

408 その他の一切の情報は、公開向けの報告には提供されない。

409 内部の CB 報告書には、公開向け報告における情報に追加して以下を含む：

- 生成されたすべての欠陥仮説のリスト(参照、AVA_VAN.1-4)；
- 評価者侵入テスト作業、テストアプローチの概説、設定、深さと結果(参照、AVA_VAN.1-9)；
- 欠陥仮説を作成するために使用されたすべての証拠資料 (欠陥仮説を思い付くときに使用された証拠資料の特定において、評価チームは、読者が本サポート文書によって厳密に要求されるかどうかを決定できるように、その証拠資料を特徴付けなければならない(must)、また証拠資料の性質(設計情報、開発者の技術ノート、等))；
- 評価者は、すべての悪用可能な脆弱性、及び残存脆弱性を、以下のそれぞれについて詳述して、報告しなければならない(shall)：
    a) その情報源 (例、それについて、思い付き、評価者に知られて、公開情報で読まれたときに着手されている CEM アクティビティ)；
    b) 満たされない SFR；
    c) 記述；
    d) その運用環境において悪用可能か否か(即ち、悪用可能か残存か)。

e) 特定された脆弱性を実行するために要求される、時間の量、知見のレベル、TOE の知識レベル、機会のレベル及び装置(参照、AVA_VAN.1-11)；

f) 各欠陥仮説がどのように解決されたか (これには、元の欠陥仮説が確認されたか反証されたか、及び残存脆弱性が基本的な攻撃能力を有する攻撃者によって悪用可能かどうかに関する任意の分析が含まれる)(参照、AVA_VAN.1-10)；及び

g) 調査において実際のテストが実行されような場合に(セクション A.1.4 で iTC)によって規定されたツールを用いた欠陥仮説生成の一部として、または特定の結果の証明／反証において、のいずれか)、TOE のセットアップで従うステップ(及びあらゆる必須のテスト装置)；テストの実行；post-テスト手順；及び実際の結果(以下を含めて、テストの再現を許すような詳細レベルまで：

- TOE がテストされている潜在的な脆弱性の特定；
- 侵入テストを実行する必要があるものとしてのすべての必須のテスト装置に接続し、セットアップするための指示；
- すべての侵入テスト必要条件初期条件を確立するための指示；
- TSF をシミュレートするための指示；
- TSF のふるまいを観測するための指示；
- すべての期待される結果と観測された結果について期待される結果との比較のために実行されるべき必要な分析；
- テストを完了し、必要な TOE のためのテスト後の状態を確立するための指示(参照、AVA_VAN.1-6,AVA_VAN.1-8)。

B. FDE 同等性検討

410 **序論**

411 本附属書は、異なる OS／プラットフォームの製品の透過性について、FDE コラボラティブプロテクションプロファイルへ適合主張しようと望むようなベンダの要求に関して評価者が決定するための根拠を提供する。

412 本評価の目的について、透過性は 2 つのカテゴリーに分けられる：

- **モデルにおけるバリエーション：** 別々の TOE モデル／バリエーションがそれぞれのモデルにわたって必要とされるような相違が含まれるかもしれない。以下にリストアップされるカテゴリーのいずれかにバリエーションが無い場合、モデルは等価であると考えられる。
- **テストされる製品の OS／プラットフォームにおけるバリエーション（例、テスト環境）：**TOE が機能を提供する方法（または機能そのもの）がインストールされる OS に依存して変わるかもしれない。TOE が提供する機能または TOE が機能を提供する方法において相違がない場合、モデルは等価であると考えられる。

413 上記の具体的なカテゴリーのそれぞれの間での透過性の決定は、いくつかの異なるテスト結果をもたらし得る。

414 いくつかの TOE が等価であると決定される場合、テストは TOE のひとつのバリエーションで実行されればよい。しかし、TOE バリエーションがセキュリティに関連する機能上の相違がある場合、機能的または構造的な相違を持つ TOE モデルのそれぞれについて別々にテストされなければならない。一般的に、TOE 各バリエーション間での相違のみがテストされなければならない。その他の等価な機能については、代表的なモデルについてテストされればよく、複数のプラットフォームに割る必要はない。

415 TOE がインストールされるプラットフォーム／OS に同じくかかわりなく動作すると決定される場合、テストはすべての等価な構成について単一の OS／プラットフォーム組合せにおいて実行されればよい。しかし、TOE が環境依存の機能を提供すると決定される場合、テストは機能において相違存在するそれぞれの環境について行われなければならない。上記のシナリオと同様に、環境の相違により影響を受ける機能のみについて再テストされなければならない。

416 ベンダが同等性についての評価者の調査に合意しない場合、認証者は同等性が存在するかどうかについて、2 者間の調停を行う。

417 **同等性を決定するための評価者ガイド**

418 以下の表は、評価者が TOE モデルのバリエーション間及び運用環境にわたる同等性に影響する要素のそれぞれについて考慮するべき記述を提供する。さらに、表には、モデル／プラットフォームにわたる追加の別々のテストに至るシナリオも識別している。

要素	同じ／同じでない	評価者ガイダンス
プラットフォーム／ハードウェア依存性	独立性	プラットフォーム／ハードウェアの依存性が識別されない場合、評価者は、等価であるために複数のハードウェアプラットフォームでのテストを考慮しなければならない。
	依存性	プラットフォーム／ハードウェアの間で具体的な相違がある場合、評価者は cPP 特有のセキュリティ機能に影響を与える相違あるか、またはそれらが非 PP 特有の機能に提起用されるか、について識別しなければならない。cPP で特定された機能がプラットフォーム／ハードウェアが提供するサービスに依存する場合、特定のファー度ウェアの組合せで認証されたと考えられるために、TOE は異なるプラットフォームのそれぞれにおいてテストされなければならない。このような場合、評価者は、プラットフォーム／ハードウェアが提供する機能に依存する機能の再テストのみのオプションを持つ。相違が非 PP 特有の機能のみに影響する場合、バリエーションは依然等価であると考えられる。各相違について評価者は、なぜ相違が cPP 特有の機能に影響するか、または影響しないかの説明を提供しなければならない。
ソフトウェア／OS 依存性	独立性	ソフトウェア／OS 依存性がない場合、等価であるために、評価者は複数の OS におけるテストを考慮しなければならない。
	依存性	OS 間の具体的な相違がある場合、評価者は、相違が cPP 特有のセキュリティ機能に影響するか、またはそれらが非 PP 特有の機能に適用されるかについて識別しなければならない。cPP で特定された機能が OS 提供のサービスに依存する場合、TOE は異なる OS のそれぞれでテストされなければならない。この場合、評価者は、OS 提供の機能に依存する機能を再テストのみ行うオプションを持っている。相違が非 PP 特有の機能にのみ影響する場合、モデルバリエーションは、以前等価であると考えられる。各相違について評価者は、なぜ相違が cPP 特有の機能に影響するか、または影響しないかの説明を提供しなければならない。
TOE ソフトウェアバイナリにおける相違	同一	モデルバイナリが同一である場合、モデルバリエーションは等価と考えなければならない。
	相違	モデルソフトウェアバイナリに相違がある場合、相違が cPP 特有のセキュリティ機能に影響を与えるかどうか決定がなされなければならない。cPP 特有の機能が影響を受ける場合、モデルは等価でないと考えられ、別々にテストされなければならない。評価者は、ソフトウェア相違により影響される機能を再テストのみ行うオプションを持つ。相違が非 PP 特有の機能にのみ

要素	同じ／同じでない	評価者ガイダンス
		影響する場合、モデルは依然等価であると考えられる。各相違について評価者は、なぜ相違が cPP 特有の機能に影響するか、または影響しないかの説明を提供しなければならない。
TOE 機能を提供するために使用されるライブラリにおける相違	同じ	さまざまな TOE モデルでしようされるライブラリ間で相違がない場合、モデルバリエーションは等価であると考えなければならない。
	相違	モデルバリエーション間で別々のライブラリが使用される場合、cPP 特有の機能に影響を与えるライブラリによって機能が提供されるかどうかの決定がなされなければならない。cPP 特有の機能が影響を受ける場合、モデルは等価であるとは考えられず、別々にテストされなければならない。評価者は、含まれるライブラリにおける相違によって影響を受けた機能を再テストするのみのオプションを持つ。異なるライブラリが非 PP 特有の機能のみに影響する場合、モデルは依然等価であると考えられる。それぞれの異なるライブラリについて評価者は、なぜ異なるライブラリが cPP 特有の機能に影響を与えるのか、または与えないのかについての説明を提供しなければならない。
TOE 管理インタフェースの相違	一貫性あり	さまざまな TOE モデル間で管理インタフェースに相違がない場合、モデルバリエーションは等価であると考えなければならない。
	相違	TOE がインストールされた OS,またはモデルバリエーションに基づく別々のインタフェースを提供する場合、cPP 特有の機能が異なるインタフェースにより設定可能かどうかについて決定がなされなければならない。インタフェースの相違が cPP 特有の機能に影響する場合、バリエーション／OS インストレーションは等価であるとは考えられず、別々のテストを行わなければならない。評価者は、異なるインタフェース(及びいわゆる機能の設定)によって設定され得る機能の再テストのみ行うオプションを持つ。異なる管理インタフェースのみが非 PP 特有の機能のみに影響する場合、モデルは依然等価であると考えられる。各管理インタフェースの相違について、評価者は、なぜ異なる管理インタフェースが cPP 特有の機能に影響を与えるのか、または与えないのかについての説明を提供しなければならない。
TOE 機能の相違	同一	異なる TOE モデルバリエーションにより提供される機能が同一の場合、モデルバリエーションは、等価と考えられなければならない。
	相違	異なる TOE モデルバリエーションにより提供される

要素	同じ／同じでない	評価者ガイダンス
		機能が異なる場合、機能的な相違が cPP 特有の機能に影響を与えるかどうかの決定がなされなければならない。cPP 特有の機能がモデル間で相違する場合、モデルは等価であるとは考えられず、別々にテストされなければならない。これらの場合、評価者は、モデル間で相違する機能を再テストするのみのオプションを持つ。機能的相違が非 PP 特有の機能のみに影響を与える場合、モデルバリエーションは依然等価と考えられる。それぞれの相違について、評価者は、なぜ相違が cPP 特有の機能影響を与えるのか、または与えないのかについての説明を提供しなければならない。

419 **戦略**

420 同等性分析を実行する時、評価者は、それぞれの要素を独立に検討するべきである。独立した要素のそれぞれの分析は、２つの結果の一つを生み出す、

- 個別の要素について、すべてのサポートされるプラットフォーム上の TOE のすべてのバリエーションは、等価である。この場合、テストは単一のモデルで単一のテスト環境で行われてもよく、すべてのサポートされるモデルや環境で行われてもよい。
- 個別の要素について、その他すべての等価な TOE にて同一の動作をすることを保証するための別々のテストを要求するために、TOE のサブセットが識別される。分析は、テストされる必要があるモデル／テスト環境の具体的な組み合わせを識別することになる。

421 TOE の完全な CC テストは識別された要素のそれぞれについて実行される個別の分析それぞれの全体を包含することになる。

422 **テストプレゼンテーション／告知における真実**

423 何をテストしたかに加えて、評価結果及びその結果となる認証報告書は、テストされた実際のモデル及びテスト環境の組合せを識別しなければならない。テストするサブセットを決定するために使用された分析は、機密であると考えられ、オプションとしてのみ、公開情報に含められること。