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

バージョン 1.0

CCDB-2015-01-003

平成 28 年 1 月 15 日　翻訳 暫定第 0.2 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、その適用の相互承認が要求されないような分野への規格の適合と具体的なアプローチについてハイライトを当てて、それ自体が基準としての性質を持たない「ガイダンス文書」の位置付けとしてもよいし、あるいはサポート文書の適用範囲により網羅される評価において、適用が強制されるような「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、セクション 1.1 に識別される 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, September 2014 (公開レビューのための初期リリース)

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

V1.0 January 2015 (CCDB からのコメントへ対応)

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。許可取得(AA：Authorization Acquisition)の場合、TSF がパスワードを適切に調整していること、または複数のサブマスクを結合していることを実証するために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、AA の主たる機能は、利用者の入力を集め、暗号エンジンに暗号化／復号機能で利用可能なデータ暗号化鍵を作成するために使用可能な値を提供することである。実装された暗号メカニズムの比較可能で、透明性があり、再現可能な評価を保証するため、評価方法は、合意された評価のやり方、例えば、主張された機能が TOE によって本当に実行されたかを証明する方法、から構成されるように記述されなければならない。

特別な用途としての分野： *ドライブ全体暗号化デバイス、特に許可取得構成要素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

目次

表一覧

1 序説

1.1 技術分野、及びサポート文書の適用範囲

*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)*のため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フォームファクタは、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。

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を(特定の例外はあるが)暗号化し、FDE ソリューションへの許可(Authorization)が成功した後、データへのアクセスが許可される。例外には、マスターブートレコード(MBR)またはその他の AA/EE 事前認証ソフトウェアのようなものについては暗号化されずストレージデバイスの一部(サイズは実装に基づいて変わるかもしれない)として残す必要があるものを含む。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含んでいない限りは、ストレージデバイスの一部分が暗号化されないことを FDE ソリューションに対して許容すると解釈する。

*FDE cPP – Authorization Acquisition (FDE cPP - 許可取得)*は、許可取得部分のための要件を記述し、利用者との対話に必要かつデータ暗号化鍵(DEK)を利用可能とするためのセキュリティ機能要件と保証アクティビティについて詳述する。

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

a) *collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition, January 26, 2015.*

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における具体的な要件は、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)、利用者ガイダンス文書、及び想定される補足情報(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)の内容の具体的な要件を識別するかもしれない。

1.2 本書の構成

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。

任意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。

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機関からの具体的な正当化が必要とされる。

同様に、保証コンポーネントのより粒度の細かいレベルにおいて、ある保証コンポーネントの保証アクティビティ及びそれに関連する SFR 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要求される。

1.3 用語

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

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。このような補足情報に対する要件は、関連の cPP で識別される(セクション 4 を参照されたい)。

2 SFR に関する評価アクティビティ

2.1 クラス：暗号サポート (FCS)

2.1.1 FCS_AFA_EXT.1 許可要素取得

TSS

評価者は、STの中で規定された許可要素がTSSのセクションに記述されていることを保証するため、初めにTSSのセクションを検査しなければならない。パスワードベースの要素に関してTSSのセクションの検査がFCS_PCC_EXT.1評価アクティビティの一部として実行される。さらにこの場合、評価者はTOEが使用可能である外部の許可要素の特性(例えば、許可要素がどのように生成されなければならないか；許可要素が満たさなければならないフォーマットまたは規格等)について述べている操作ガイダンスを検証しなければならない。

その他の許可要素が特定されている場合、それぞれの要素に関して、TSSはTOEへどのように入力されるかを規定すること。

操作ガイダンス

評価者は、AGD ガイダンスがすべての許可要素に関する指示を含んでいることを検証しなければならない。AGD では、TOE が使用可能である外部の許可要素の特性(例えば、許可要素がどのように生成されなければならないか；許可要素が満たさなければならないフォーマットまたは規格、使用される TPM デバイスの構成等)について説明すること。

KMD

評価者は、初期許可要素(サブマスク)がBEVのラップを解くために直接的に寄与することを確認するため、鍵管理記述(KMD: Key Management Description)を検査しなければならない。

評価者は、サブマスクが許可要素からどのように生成されるか(この処理に適合しなければならないあらゆる関連規格を含む)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。また検証はサブマスクの長さが要求された長さ(本要件において規定されるとおり)を満たすことを保証するために実行される。

テスト

パスワード許可要素は、FCS_PCC_EXT.1においてテストされる。

評価者は以下のテストについても実行しなければならない。：

- テスト 1 [条件付き]：一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に失敗した場合、復号された平文データへのアクセスに帰結しないことを保証せよ。

2.1.2 FCS_KYC_EXT.1（鍵チェイニング）

TSS

評価者は、AES-128 のみをサポートする製品に関して BEV 出力が 128 ビット以上であり、かつ AES-256 をサポートする製品に関して 256 ビット以上であるようなー BEV 長の上位レベルの記述を TSS が含んでいることを検証しなければならない。

KMD

評価者は、すべての受け入れられる BEV に関する鍵階層の上位レベルの記述を KMD に記述されていることを検査しなければならない。評価者は、KMD に鍵チェインが詳細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。鍵チェインの記述は、FCS_COP.1(d)、FCS_COP.1(e)、FCS_COP.1(g)、FCS_KDF_EXT.1 を満たす鍵ラップ、鍵配送、鍵暗号化、鍵導出方法を用いて鍵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。

評価者は、鍵チェイン処理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危殆化されないことを、KMD が記述し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。 (例えば、TPM に対する比較値のように直接鍵を使用する等) 本記述は、実装された鍵階層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。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。

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。

2.1.3 FCS_PCC_EXT.1 暗号パスワード生成及び調整

TSS

評価者は、TOE がパスワードの生成を実行する方法について、文字の長さや要件(文字数や文字種)を含めて TSS に記述されていることを保証しなければならない。また、TSS はパスワードがどのように調整されるかについて記述を提供するとともに、評価者はそれが要件を満たすことを保証すること。

KMD

評価者は、BEV 及び中間鍵の形成が記述されていること、及び ST 作成者によって選択された鍵長と一致する鍵長であることを保証するため、KMD を検査しなければならない。

評価者は、パスワード／パスフレーズが最初にエンコードされ、その後 SHA アルゴリズムにフィードされるという方法が KMD に記述されていることをチェックしなければならない。アルゴリズムの設定(パディング、ブロッキング等)は、記述さ

れなければならない、また評価者は、ハッシュ関数に関係する選択と同様に、これらが本コンポーネントにおける選択によってサポートされることを検証しなければならない。評価者は、ハッシュ関数の出力がどのようにして、上記のように BEV と同じ長さであり、関数への入力される、サブマスクを形成するために使用されるかについての記述が KMD に含まれていることを検証しなければならない。

テスト

評価者は、以下のテストについても実行する：

- テスト 1：TOE が 64 文字の最小長のパスワード／パスフレーズをサポートしていることを保証すること。
- テスト 2：TOE が最大文字数、n(64 を超えるような)までのパスワード／パスフレーズ長をサポートしている場合、TOE が n 文字を超えて受け入れないことを保証すること。
- テスト 3：ST 作成者によって割り付けられ、サポートされたすべての文字から構成されるパスワードを TOE がサポートしていることを保証すること。

2.1.4 FCS_CKM_EXT.4 暗号鍵及び鍵材料の破棄

TSS

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。

KMD

評価者は、KMD に鍵及び鍵材料がどの領域に存在するか、及びいつ鍵及び鍵材料が不要となるかについての記述が含まれていることを検証しなければならない。

評価者は、鍵のライフサイクルがKMDに含まれていることを検証しなければならない、それは、KMD に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、鍵及び鍵材料がもはや不要であることをどのようにして決定するか、及び必要でなくなった材料がどのように破棄されるか、についての記述を含まれる、さらに、KMD における記述が、破棄に関して FCS_CKM.4 に従っていることを検証しなければならない。

2.1.5 FCS_CKM.4 暗号鍵破棄

TSS

評価者は、TSS が鍵及び鍵材料がどのように破壊される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。

KMD

評価者は、KMD が鍵材料のそれぞれの種別、その起源、一時的に存在する可能性のある場所(例えば、鍵レジスタ、キャッシュメモリ、スタック、FIFO)及び保存場

所を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。

評価者は、KMD にそれぞれの種別の鍵材料(ソフトウェアベース鍵ストレージ、BEV、パスワード等)がいつ消去されるか(例えば、システムの電源切断時、ワイプ機能実行時、高信頼チャネルの切断時、プロトコル毎の高信頼チャネルによって不要となった時等)について記述されていることを検証しなければならない。

評価者は、それぞれの種別の鍵とストレージについて、実施される消去手続きの種別（暗号技術的な消去、ゼロによる上書き、ランダムパタンによる上書き、またはブロック消去）が列挙されていることも検証しなければならない。異なる種別のメモリが保護されるべき材料を保存するために使用されている場合、評価者は、TSS にデータが保存されたメモリについての消去手続き(例えば、「フラッシュに保存された秘密鍵はゼロで 1 回だけ上書きされるが、内部の永続的なストレージデバイスに保存された秘密鍵は書き込みの前にランダムパタンが 3 回上書きされる」)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しなければならない。

評価者は、KMD が鍵材料のそれぞれの種別(ソフトウェアベースの鍵ストレージ、BEV、パスワード等)及びその起源、保存場所、及びそれぞれの鍵の破棄方法について列挙していることを保証するためにチェックしなければならない。

テスト

それぞれのソフトウェア及びファームウェアによる鍵消去状況について、評価者は揮発性メモリについて以下のテストを繰り返さなければならない。以下のテストにおいて「鍵」とは、鍵及び鍵材料を指す。

- *テスト 1：*評価者は、その鍵で通常の暗号処理中に TOE によって内部で生成される可能性のあるすべての複製された鍵を含めて、鍵が正しく消去されることをテストするために特化した運用環境(例えば、仮想マシン)及び開発ツール(デバッガ、シミュレータ等)の適切な組み合わせを活用しなければならない。

  消去対象のそれぞれの鍵について、TOE によって暗号化され、保持される鍵の中間的な複製を含めて、評価者は、以下を実行しなければならない：

  1. TOE ソフトウェア／ファームウェアとデバッガを接続する。
  2. TOE の消去対象の鍵の値を記録する。
  3. #1 からの鍵を用いて通常の暗号化処理を TOE に実行させる。
  4. TOE に対し、鍵消去を実行させる。
  5. TOE に対し、実行を停止させるが、終了しない。
  6. TOE に対し、バイナリーファイルへ TOE の全メモリ情報をダンプさせる。
  7. #2 からの既知の鍵の値について、#6 で作成されたバイナリーファイルの内容を検索する。

  #2 からの鍵の複製が上記のステップ#7 で一切見つからなければテストは成功であり、それ以外であれば失敗となる。

評価者は、すべての鍵について、暗号化された形で残存しているものを含めて、中間的な複製が消去されていることを保証するため、このテストを実行しなければならない。

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

TSS

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。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り、ソルトが生成されることを確認しなければならない。外部の機能が本目的のために使用される場合、TSS は入力を伴って呼び出される具体的な API を含むべきである。

評価者は、ノンスがユニークに生成される方法、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。評価者は、ノンスがユニークであること、IVとtweakが記述された要件を満たしていることを確認しなければならない。

2.1.7 FMT_SMF.1 管理機能の特定

TSS

オプション A：評価者は、TOE が DEK を変更するために EE に対して要求を送信する方法について TSS に記述されていることを保証しなければならない。

オプション B：評価者は、TOE が DEK を暗号技術的に消去するために EE に対して要求を送信する方法について TSS に記述されていることを保証しなければならない。

オプション C：評価者は、利用者がサポートされるすべての許可要素を変更可能な方式について TSS に記述されていることを保証しなければならない。

オプション D：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ための処理について TSS に記述されていることを保証しなければならない。

オプション E：追加の管理機能が ST において主張されている場合、評価者は、追加機能について TSS に記述されていることを保証しなければならない。

操作ガイダンス

オプション A + B：評価者は、利用者が A 及び B の機能を開始でき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。

オプション C：評価者は、選択された許可要素の値を変更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。

オプション D：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。

オプション E：デフォルトの許可要素：TOE がデフォルトの許可要素を設定した形で届く場合があるかもしれない。そのような場合、それらの許可要素を変更するためのメカニズムが存在するので、セクション E における選択が実施されなければならない。操作ガイダンスは、デバイスの所有権を取得する時にこれらの許可要素を利用者が変更する方法について記述していなければならない。TSS は、存在するデフォルトの許可要素について記述していなければならない。

鍵回復の無効化：この機能の無効化についてのガイダンスは AGD 文書において記述されていなければならない。

テスト

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するために EE に対してコマンドを送るような機能を持っていることを検証しなければならない。暗号技術的な消去の実際のテストは、EE において実行すること。

オプション C：評価者は、TOE が暗号化データへアクセスするために許可要素の入力を利用者に要求するように、TOE を初期化しなければならない。

> テスト 1：評価者は、まず利用者許可要素を使用できるよう設定し、その後すべてのサポートされている許可の値が利用者に暗号データへのアクセスを許可することを検証しなければならない。そして評価者は、利用者許可要素の値を新しい値に変更するために管理機能を動作させなければならない。そして、評価者は、アクセスを得るために古いまたはオリジナルの許可要素の値を使用するときに、TOE が利用者の暗号化されたデータへのアクセスを拒否することを検証すること。

オプション D：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機能を TOE が持っていることを検証しなければならない。

オプション E：追加の管理機能が主張されている場合、評価者は、記述された追加機能について検証しなければならない。

> テスト 2：[条件付き] TOE がデフォルト許可要素を提供する場合、評価者は、操作ガイダンスに記述されているとおり、デバイスの所有権を得る過程でこれらの要素を変更しなければならない。評価者は、(古い)許可要素がデータアクセスのために、もはや有効でないことを確認しなければならない。
> テスト 3：[条件付き] TOE が鍵回復機能を提供し、その影響が TOE インタフェースにおいて観測可能な場合、評価者は、鍵回復機能がベンダ提供のガイダンスに従って無効化されていること、または無効化することが可能であることを保証するためのテストを考案しなければならない。

2.1.8 FPT_KYP_EXT.1 拡張：鍵及び鍵材料の保護

KMD

評価者は、不揮発性メモリに保存される鍵を保護するために使用される方式についての記述に関して KMD を検査しなければならない。

評価者は、すべての鍵の保存場所及び不揮発性メモリに保存されるすべての鍵の保護を検証しなければならない。鍵チェインの記述は、ストレージについての基準の一つを満たすような、不揮発性メモリにおけるラップまたは暗号化された鍵、及び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(c) または FCS_COP.1(xx) (訳注：正しくは、FCS_KYC_EXT.1に記述されたとおり、FCS_COP.1(d)、FCS_COP.1(g)、またはFCS_COP.1(e)) に従っていることを保証するためにレビューされなければならない。

2.1.9 FPT_TUD_EXT.1 高信頼アップデート

TSS

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、*ディ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。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について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。評価者は、TOE のアップデート用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。

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。

操作ガイダンス

評価者は、TOE に対するベンダのアップデートを TOE が取得する方法；アップデートのディ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。

テスト

評価者は、以下のテストを実行しなければならない(TOE が異なるハッシュアルゴリズムを用いて、複数の署名をサポートする場合、評価者は、ディジタル署名だけのテストと同様に、本物及び偽物のディジタル署名の異なる組み合わせについてもテストを実行する)：

- 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にバージョン検証アクティビティを実行する。以下のテストで記述されるテストの後、評価者は、このアクティビティを再度実行し、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。

- 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更新を取得し、TOE にインストールが成功することを検証する。評価者は更新が期待どおりに機能することを論証するために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。

オプション要件

2.1.10 FCS_CKM.1 暗号鍵生成（非対称鍵）

TSS

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 が一つ以上の方式を規定する場合、評価者は、それぞれの方式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。

操作ガイダンス

評価者は、本 cPP において定義され、AGD 文書によって特定されたすべての利用者について、選択された鍵生成方式及び鍵長を用いて TOE の設定を行う方法を管理者に対し、AGD ガイダンスが指示していることを検証しなければならない。

テスト

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。

FIPS PUB 186-4 RSA 方式の鍵生成

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。本テストは、public verification exponent（公開鍵検証指数）*e*、private prime factor（プライベート素因数）*p* 及び *q*、public modulus（公開鍵の法）*n* 及び private signature exponent (プライベート署名指数) *d* の計算を含めた鍵要素の値を正しく生成する TSF の能力を検証する。
鍵ペア生成では、素数 *p* と *q* を生成するために 5 とおりの方法(または手法)を規定している。これらには、以下のものが含まれる：

1. ランダム素数：
   - 証明可能素数
   - 確率的素数
2. 条件付き素数：
   - 素数 *p1, p2, q1,q2, p* 及び *q* を、すべて証明可能素数としなければならない。
   - 素数 *p1, p2, q1,* 及び *q2* を証明可能素数とし、 *p* 及び *q* を確率的素数としなければならない。
   - 素数 *p1, p2, q1,q2, p* 及び *q* を、すべて確率的素数としなければならない。

ランダム証明可能素数手法とすべての条件付き素数手法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。これには、1 つ以上の乱数シード値、RSA 鍵の公開鍵指数、及び望ましい鍵長が含まれる。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。評価者は、TSF によって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 の実装の正しさを検証しなければならない。

楕円曲線暗号(ECC)の鍵生成

FIPS 186-4 ECC 鍵生成 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 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。プライベート鍵は、承認された乱数ビット生成器(RBG)を用いて生成されなければならない。正しさを判断するため、評価者は生成された鍵ペアを既知の良好な実装の公開鍵検証 (PKV) 機能へ送出しなければならない。

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 個のプライベート鍵／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。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。

有限体暗号 (FFC)の鍵生成

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。このテストは、体を定義する素数 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。

パラメタ生成では、暗号素数 q 及び体を定義する素数 p を生成するための 2 とおりの方法(または手法)が規定され、

暗号素数及び体を定義する素数：

- 素数 q 及び p を両方とも証明可能(Provable)素数としなければならない。
- 素数 q 及び体を定義する素数 p を両方とも確率的(Probable)素数としなければならない

そして、暗号群生成元 g を生成するための 2 とおりの方法を規定している。

暗号群生成元：

- 検証可能処理によって構築された生成元 g
- 検証不可能処理によって構築された生成元 g

鍵生成は、プライベート鍵 x を生成するための 2 とおりの方法を規定している。

プライベート鍵：

- RBG の len(q) ビットの出力、ここで 1 <=x <= q-1 とする
- RBG の len(q) + 64 ビット出力に、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。

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。

証明可能素数の手法については、暗号素数及び体を定義する素数生成手法をテストするために、及び／または検証可能処理については、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として与えなければならない。

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。評価者は、TSF によって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 の実装の正しさを検証しなければならない。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。

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

2.1.11 FCS_SMC_EXT.1 サブマスク結合

TSS

許可要素から生成されたサブマスクがBEVまたは中間鍵を形成するためにXORされる場合、TSSのセクションはこれがどのように実行されるかをしきべつしなければならない(例えば、順序の要求事項がある場合、チェックが実行される、等)。また、評価者は、生成された出力の長さがBEVの長さと少なくとも同じであるようにTSSに記述されていることを確認しなければならない。

KMD

評価者は、承認された組み合わせが使用され、鍵材料を弱めたり、暴露を引き起こしたりし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。

テスト

- テスト 1 [条件付き]：複数許可要素がある場合、要求された許可要素の供給の失敗が暗号化データへのアクセスに結びつかないことを保証すること。

2.1.12 FCS_VAL_EXT.1 検証

TSS

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

評価者は、複数のサブマスクがTOEで使用されているかどうか、サブマスクがどのように検証されるか(例えば、それぞれのサブマスクが結合の前に検証され、一度結合された検証が実行される)についての上位レベルの記述をレビューするため TSSを検査しなければならない。

KMD

評価者は、TOEが連続して失敗した許可の試行の数の制限を用いる手法について KMDに記述されていることを検証するためにKMDを検査しなければならない。

評価者は、どのように検証が実行されるかについてKMDに記述されていることを保証するため、ベンダのKMDを検査しなければならない。KMDでの検証処理の記述は、TOEがサブマスクをどのように検証するかについての詳細な情報を提供していること。

KMDでは処理がどのように動作するか、例えば、サブマスクを危殆化するかもしれないあらゆる材料を暴露させない等について記述していること。

操作ガイダンス

[条件付き] 評価者は、検証の試行に関する制限が確立できることを保証するために TOE をどのように設定するか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。

テスト

評価者は、以下のテストを実行しなければならない。：

- テスト 1：評価者は、連続して失敗した許可の試行回数の平均率における制限を決定しなければならない。評価者は、保護データへのアクセスの連続した試行において不正な許可要素の数を入力することにより TOE をテストすること。制限のメカニズムが「ロックアウト」期間を含む場合、テストされる期間は少なくともひとつの期間を含むべきである。その時評価者は TOE が TSS に記述されたとおりの振る舞いをすることを検証すること。
- テスト 2：それぞれの検証された許可要素について、利用者が不正な許可要素を提供した時に、TOE が BEV を TOE の外(例えば、EE へ)に送ることを防止したことを保証すること。

2.1.13 FCS_COP.1(a) 暗号操作 (署名検証)

本要件は、TOE のアップデートをインストールする前に TOE 製造事業者からのアップデートに添付されたディ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アップデート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ィジタル署名アルゴリズムの実装のみに対応する；評価者は、そのコンポーネントにおいて選択されたアルゴリズムについて適切なテストを実行すること。

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；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乱数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ィ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 がディ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方式が調べられなければならない。

TSS

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。これは、少なくとも、ディ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；ディ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。

テスト

以下の各セクションは評価者ディジタル署名スキームのそれぞれの種別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択すること。

以下で与えられる方式に関して、鍵生成／ドメインパラメタ生成テスト要件が無いことに注意するべきである。これは、本機能がエンドデバイスにおいて必要とされていることを予測していないからで、機能が供給された更新におけるディ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。こらは、ドメインパラメタがすでに生成され、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に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使用を保証するため、評価及び検証方式が調べられなければならない。

以下のテストは、SFR 内の選択に基づく条件付のものである。

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。

ECDSA アルゴリズムテスト

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) を変更しなければならない。評価者は、これに応じた 10 個の合格／不合格値のセットを取得しなければならない。

RSA 署名アルゴリズムテスト

署名検証テスト

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。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。TOE は署名の検証を試行し、成功または失敗を返す。

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。

2.1.14 FCS_COP.1(b) 暗号操作 (ハッシュアルゴリズム)

TSS

評価者は、他のTSF暗号機能のハッシュ関数の関連性 (例えば、ディジタル署名検証関数) がTSSに記録されていることをチェックしなければならない。

操作ガイダンス

評価者は、要求された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。

テスト

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。

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。

Short Messages Test - Bit-oriented Mode

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、疑似乱数的に生成されなければならない。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。

Short Messages Test - Byte-oriented Mode

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。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。

Selected Long Messages Test - Bit-oriented Mode

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。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。

Selected Long Messages Test - Byte-oriented Mode

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、疑似乱数的に生成されなければならない。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。

Pseudorandomly Generated Messages Test

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。

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

TSS

評価者は、HMAC 関数によって使用される以下の値を規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：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。

テスト

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。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。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 HMAC タグを生成した結果と比較されなければならない。

2.1.16 FPT_TST_EXT.1 拡張：TSF テスト

TSS

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。

評価者は、TOE の正しい運用に影響を与える非暗号機能のいくつかのセット及び TOE がそれらの機能をテストするための手法について、TSS が記述していることを検証しなければならない。評価者は、これらの機能のそれぞれ、機能のただし操作を TOE が検証する手法について TSS に含んでいることを検証しなければならない。評価者、TSF データが TSF テストに適切であることを検証しなければならない。例えば、AES の CBC モードについてブロックより多くについてテストされたり、AES の GCM モードの出力が切り捨てなしにテストされたり、または 512 ビット鍵が HMAC-SHA512 のテストで使用される。

FCS_RBG_EXT.1 が NIST SP 800-90 にしたがって TOE によって実装される場合、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 が記述していることを検証しなければならない。

FCS_COP 機能が TOE によって実装される場合、TSS はそれらの機能についての既知解セルフテストについて記述しなければならない。

評価者は、TSF の正しい操作に影響を与える非暗号機能のいくつかのセット、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。TSS はこれらの各機能、機能／コンポーネントの正しい操作が検証さ

れる手法について記述すること。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。

選択ベース要件

2.1.17 FCS_COP.1(d) 暗号操作 (鍵ラッピング)

TSS

評価者は、TSS が鍵ラップ機能の記述を含むことを検証しなければならない、また適切な仕様に従って承認された鍵ラップアルゴリズムを鍵ラップが使用していることを検証しなければならない。

KMD

評価者は、承認された手法を用いてすべての鍵ラップされることと鍵ラップが発生する時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。

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

TSS

評価者は、TSS が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を含んでいることを検証しなければならない。

ガイダンス

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。

テスト

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。

AES-CBC テスト

AES-CBC 既知解テスト

既知解テスト (KAT) には、以下に記述される 4 つがある。すべての KAT において、平文、暗号文、及び IV の値は 128 ビットのブロックとしなければならない。各テストの結果は、直接評価者によって得られてもよいし、または実装者へ入力を供給しその結果を受領することによって取得されてもよい。正しいことを決定するため、評価者は、結果の値を、既知の良好な実装へ同一の入力することによって得られた値と比較しなければならない。

> **KAT-1.** AES-CBC の暗号化機能をテストするため、評価者は 10 個の平文の値を供給し、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。うち 5 個の平文の値は 128 ビットのすべてゼロの鍵で暗号化されなければならず、

それ以外の 5 個は 256 ビットのすべてゼロの鍵で暗号化されなければならない。

AES-CBC の復号機能をテストするため、評価者は 10 個の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを実行しなければならない。

KAT-2. AES-CBC の暗号化機能をテストするため、評価者は 10 個の鍵の値を供給し、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。うち5個の鍵は 128 ビットの鍵とし、それ以外の 5 個は 256 ビットの鍵としなければならない。

AES-CBC の復号機能をテストするため、評価者はすべてゼロの暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない。

KAT-3. AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 2 セットの鍵の値を供給し、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 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。第 1 の鍵のセットは 128 個の 128 ビットの鍵からなるものとし、第 2 のセットは 256 個の 256 ビットの鍵からなるものとする。[1,N] の範囲の *i* について、各セットの鍵 *i* の左端の *i* ビットは 1、右端の *N-i* ビットは 0 としなければならない。

AES-CBC の復号機能をテストするため、評価者は以下に記述する 2 セットの鍵と暗号文の値のペアを供給し、所与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。第 1 の鍵／暗号文のペアのセットは 128 個の 128 ビットの鍵／暗号文のペアからなるものとしなければならず、第 2 のセットは 256 個の 256 ビットの鍵／暗号文のペアからなるものとしなければならない。[1,N] の範囲の i について、各セットの鍵 i の左端の i ビットは 1、右端の N-i ビットは 0 としなければならない。各ペアの暗号文の値は、それに対応する鍵で復号された際にすべてゼロの平文が得られるような値としなければならない。

KAT-4. AES-CBC の暗号化機能をテストするため、評価者は以下に記述する 128 個の平文の値のセットを供給し、2 種類の暗号文の値 (それぞれ、すべてゼロの 128 ビットの鍵の値とすべてゼロの IV、及びすべてゼロの 256 ビット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) を取得しなければならない。[1,128] の範囲の i について、各セットの平文の値 i の左端の i ビットは 1、右端の N-i ビットは 0 としなければならない。

AES-CBC の復号機能をテストするため、評価者は暗号化テストにおける平文と同一の形式の暗号文の値を入力として AES-CBC 復号を用いて、暗号化と同一のテストを行わなければならない。

AES-CBC 複数ブロックメッセージテスト

評価者は、*i* 個のブロックからなるメッセージ (ここで 1 < *i* <=10) を暗号化することにより、暗号化機能をテストしなければならない。評価者は鍵、IV 及び長さ *i* ブロックの平文メッセージを選択し、試験すべきモードを用いて選択した鍵と IV によりメッセージを暗号化しなければならない。暗号文は、既知の良好な実装を用いて同一の鍵と IV により同一の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。

また評価者は、*i* 個のブロックからなるメッセージ (ここで 1< *i* <=10) を復号することにより、各モードについて復号機能をテストしなければならない。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選択し、試験すべきモードを用いて選択した鍵と IV によりメッセージを復号しなければならない。平文は、既知の良好な実装を用いて同一の鍵と IV により同一の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。

AES-CBC モンテカルロテスト

評価者は、200 個の平文、IV、及び鍵の 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。これらのうち 100 個は 128 ビットの鍵を用いるものとし、それ以外の 100 個は 256 ビットの鍵を用いなければならない。平文と IV の値は、128 ビットのブロックとしなければならない。3 つ組のそれぞれについて、以下のように 1000 回の反復処理が実行されなければならない。:

```
# 入力： PT, IV, Key
for i = 1 to 1000:
        if i == 1:
                CT[1] = AES-CBC-Encrypt(Key, IV, PT)
                PT = IV
        else:
                CT[i] = AES-CBC-Encrypt(Key, PT)
                PT = CT[i-1]
```

1000 回目の反復処理において計算された暗号文 (すなわち、CT[1000]) が、その試行の結果となる。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。

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-Encrypt を AES-CBC-Decrypt で置き換えて、復号機能をテストしなければならない。

AES-GCM テスト

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、AES-GCM の認証付き暗号機能をテストしなければならない：

128 ビット及び 256 ビットの鍵

2 とおりの平文の長さ。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。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。

3 とおりの 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。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 。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。

2 とおりの 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 とおりの IV 長の一方を 96 ビットとしなければならない。

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 の組のセットを用いて暗号化機能をテストし、AES-GCM 認証付き暗号から得られた暗号文とタグを取得しなければならない。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。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。

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 つ組のセットを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。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。

各テストの結果は、直接評価者によって、または入力を実装者へ供給しその結果を受領することによって、取得することができる。正しさを判断するため、評価者は結果の値を、同一の入力を既知の良好な実装へ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。

XTS-AES テスト

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 。 :

256 ビット (AES-128 について) 及び 512 ビット (AES-256 について) の鍵

3 とお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、128 ビットのゼロ以外の整数倍としなければならない 。 (サポートされる場合)。データユニット長の 1 つは、128 ビットの整数倍としなければなら

ない。 (サポートされる場合)。データユニット長の 3 番目は、サポートされる最も長いデータユニット長か 2^{16} ビットの、いずれか小さいほうとしなければならない。

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

評価者は、実装によってサポートされている場合、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 0 から 255 の間の 10 進数である。

評価者は、平文の値を暗号文の値に置き換え、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 復号機能をテストしなければならない。

2.1.19 FCS_KDF_EXT.1 暗号鍵導出

TSS

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。

KMD

評価者は、すべての鍵が承認された手法を用いて導出されていること及び鍵がどのようにいつ導出されるかの記述を保証するためにベンダの KMD を検査しなければならない。

2.1.20 FCS_RBG_EXT.1 拡張：暗号操作 (乱数ビット生成)

TSS

第三者が提供する 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、及び第三者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。評価者は、この記述が DRBG にシード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。ST が複数の DRBG を規定する場合、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。

エントロピーエッセイ

評価者は、cPP の附属書 D に記述されるとおりすべての要求される情報をエントロピーエッセイが提供していることを保証しなければならない。評価者は、提供された情報を評価し、ランダムビット列を生成する時に TOE が十分なエントロピーを提供していることを保証すること。

操作ガイダンス

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。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／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。

テスト

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。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。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。

RNG が予測困難性をサポートする場合、各試行は、(1) DRBG を Instantiate する、(2) 乱数ビットの最初のブロックを Generate する、(3)乱数ビットの 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。「乱数ビットの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乱数ビットが生成されることを意味している。

RNG が予測困難性をサポートしない場合、各試行は、(1) DRBG を Instantiate する、(2) 乱数ビットの最初のブロックを Generate する、(3) Reseed する、(4) 乱数ビットの 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、乱数ビットの 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。

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。

3 SAR に関する評価アクティビティ

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。

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。

3.1 ASE：セキュリティターゲット評価

1 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。

3.1.1 適合主張 (ASE_CCL.1)

2 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

ASE_CCL.1 エレメント	評価者アクション
	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。

3.2 ADV：開発

3.2.1 基本機能仕様 (ADV_FSP.1)

本保証コンポーネントの評価アクティビティは、機能要件に応えて TOE 要約仕様 (TSS) に表されたインタフェース、及び AGD 文書に表されたインタフェースを理解することに焦点をあてている。本文書の技術特有の要件が、上記セクション 2 及び本サポート文書のセクション 3 の他の部分において AGD、ATE、及び AVA の SAR に関する評価アクティビティにおいて、各 SFR として (関連して) 識別されている。さらに評価者が本 SAR コンポーネントを満たすために実行する評価アクティビティは以下のとおりである。

評価アクティビティ：

評価者は、セキュリティに関連するとして識別された各 TSFI の使用目的や使用方法についてインタフェース文書に記述されていることを保証するため、インタフェース文書をチェックしなければならない。

この文脈において、TOE を構成するため、またはその他の管理者機能を実行する (例、アップデートを実行する)ために、管理者により TSFI が使用される場合、TSFI はセキュリティに関連するとみなされる。さらに、ST またはガイダンス文書においてセキュリティ方針を忠実に実行するものとして(SFR に書かれるとおり)、識別されるそれらのインタフェースについてもセキュリティ関連と考えられる。意図は、これらのインタフェースが適切にテストされ、TOE においてどのように使用されるかを理解することが、適切なテストの網羅性が適用されることを保証するために必要である。

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識別される各 TSFI のパラメタについてインタフェース文書が識別し記述していることを保証するため、インタフェース文書をチェックしなければならない。

評価における本保証コンポーネントに関して検証されるべき文書はセキュリティターゲット、AGD 文書、及びエントロピー分析または暗号鍵管理アーキテクチャ [1]のような観点から cPP によって必須の補足情報：追加の「機能仕様」文書は、評価アクティビティを満たすためにまったく必要ない。評価されるべきインタフェースは、各 SFR についてリストアップされた保証アクティビティを参照することによって識別され、セキュリティターゲット、AGD 文書、及び特別に CC 評価の目的のための別のリストではなく、cPP によって必須の補足情報の文脈の中で識別されることが期待されている。ADV_FSP.1.2D で要求されているトレースをも意味する、各 SFR についての評価アクティビティの一部分として文書化要件の直接の識別とそれらの分析は、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。

しかし、評価者が不十分な設計及びインタフェース情報のためにその他の要求された評価アクティビティを実行できない場合、評価者は、適切な機能仕様が提供されないことを理由に評価を終了する権限を与えられ、その結果 ADV_FSP.1 の保証コンポーネントの判定は「不合格」となる。

3.3 AGD：ガイダンス文書

AGD_OPE 及び AGD_PRE の個別の要件に適合するために TOE として別々の文書を提供する必要はない。本セクションにおける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 の要件の間のマッピングが、TOE の(適切な)一部として、管理者と利用者へ配付される文書においてすべての要件が満たされる限り、多対多であってもよい。

3.3.1 利用者操作ガイダンス（AGD_OPE.1)

利用者ガイダンス文書における特定の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。

評価アクティビティ：

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。

操作ガイダンス文書は、評価された構成を確立し維持するために文書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。

[1] セキュリティターゲット及び AGD 文書は公開文書である。補足情報は、公開文書または機密情報であるかもしれない：cPP 及び／または評価アクティビティ記述はこのような補足情報が機密情報であり非公開であることを許容していることを識別している。

操作ガイダンスは、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運用環境に対して提供されなければならない、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。これは、一つの文書にすべてが含まれていてもよい。

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って、上記セクション２ですべての個別の SFR について適切であるように、検証されるだろう。

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。

a) 操作ガイダンスは TOE の評価された構成に関係する任意の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。

b) 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。

3.3.2 準備手続き (AGD_PRE.1)

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。

評価アクティビティ：

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。

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だろう。

準備手続きは、評価された構成を確立し維持するために文書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。

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 ですべての個別の SFR について適切であるように、検証されるだろう。

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。

準備手続きは、(セキュリティターゲットで規定される運用環境に関する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すことができることを管理者がどのように検証するかについての記述を含まなければならない。文書化は、情報提供の形であるべきで、(一般的な IT 経験を持

つが TOE そのものの経験が必ずしも必要でないような IT 担当を通常は含むような) 対象読者によって理解され利用できるよう十分な詳細度で説明が書かれているべきである。

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提供しなければならない、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。これは一つの文書にすべてが含まれていてもよい。

準備手続きは以下を含まなければならない

a) すべての運用環境で TSF をうまくインストールするために指示する；及び

b) 製品として、及び大きな運用環境の構成要素としての TSF のセキュリティを監視するために指示する；及び

c) 保護される管理機能を提供するために指示する。

3.4 ATE：テスト

3.4.1 独立テスト - 適合 (ATE_IND.1)

操作ガイダンス文書と同様に 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 にて規定された要件が満たされていることを確認することである。

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に対する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 等価性検討を調べるべきである。

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。

評価アクティビティ：

評価者はテスト構成が ST で規定されたとおり、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。

評価アクティビティ：

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。

評価アクティビティ：

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網羅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網羅されていることを示さなければならない。

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。

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 文書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の事前調整のいずれかとして、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 文書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。

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順と同様に上位レベルのテスト目的を識別する。

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[2]だけではいけない。

[2] 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。

3.5 AVA：脆弱性評定

3.5.1 脆弱性調査 (AVA_VAN.1)

評価アクティビティ：

3 評価者は、本要件に関する潜在的な脆弱性の分析とテストについて文書化しなければならない。本報告書は、ATE_IND のテスト報告書の一部として含まれるか、または別文書となる。

4 評価者は、具体的な TOE に関連するものと同様に、製品が象徴する関連の TOE 種別(TOE で使用される構成要素や使用される通信プロトコルのような観点に関連する脆弱性を含む)において発見された脆弱性を決定するため、公開情報の検索を実施する。評価者は調べた情報源や見つけた脆弱性を報告書に文書化する。発見したそれぞれの脆弱性について、その脆弱性を確認するため、適切であれば、評価者はテストを(ATE_IND のために提供されるガイドラインを用いて)考案する。

5 脆弱性評価についてのさらなる情報は、附属書 A を参照のこと。

4 必須の補足情報

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」がさまざま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。

許可取得のための FDE cPP は、エントロピー分析、及び鍵管理の記述を要求する、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。

5 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

附属書 A：脆弱性分析

本文書は、許可取得 (AA) 及び暗号エンジン (EE) cPP の AVA アクティビティのための補足的なガイダンスを提供する。本ガイダンスは SPD のバージョン 0.10 及び ESR のバージョン 0.10、及びドラフト cPP 脆弱性分析ホワイトペーパ[VAWP]に基づいている。

はじめに

このような客観性と再現性を達成するために、評価者が良く定義されたアクティビティ集に従い、所見を文書化し、他の人々がその議論を追うことができ、評価者の報告書における評価者として同じ結論へたどり着くことができる。その結果、保証アクティビティは脅威モデル及び評価されるべき製品種別についての既知の脆弱性に基づく cPP のために作成された。

特定の TOE を評価することによって達成される付加的な理解に基づく cPP へ含められる必要があるような iTC へ追加の保証アクティビティを提案するため、本補足的ガイダンス処理が評価者により使用される。本処理は、発見されたその他の脆弱性及び公知の脆弱性として付加的なアクティビティを提案するためにも使用することが可能である。

脆弱性の情報源

FDE AA 及び EE バージョン 1 のための使用事例が甚だ単刀直入であることを覚えていることが重要であるーデバイスは電源切断の状態で見つかり、再検討／悪意のメイド攻撃の対象外であった。使用事例があまりにも狭いため、使用事例は、侵入テストまたはファジングテストの典型的モデルではなく、通常のテストが適用できない。したがって、基本的攻撃の定義は、非常に狭い脅威ウィンドウに限定されている。例えば、脆弱性がブートアップ時のキー押下の組み合わせによって検出できる場合、テストは本 cPP の保証レベルに適しているだろう。

新たなアクティビティの提案処理

評価機関は、認証者に提案を行い、認証機関がある種の脆弱性に基づき新しい保証アクティビティを提案するよう促す。この脆弱性は、評価者が以下のステップにより適切な対処することができないと信じるようなものである：

1. 評価者は、脆弱性の種別、及び cPP での脅威モデルへの適用方法について記述する。
2. 評価者は、認証者により承認を得た場合その製品についてのアクティビティを実行する。(評価者は、もちろん常にベンダ、評価者、及び認証者が合意するアクティビティを実行できることは有用である。)
3. 評価者と認証者は、cPP へ含めるべきと決定する脆弱性の種別に基づき提案される保証アクティビティ(または保証アクティビティへの改訂)について文書化する。

iTC は、文書を読み、スキーム(評価認証制度)から提供された何らかの文書または証拠に基づき、cPP への回答をするかどうかの決定を行う。

脅威モデルに適用される脆弱性がある製品で発見され、認証者の満足するまで軽減されない場合、スキーム(評価認証制度)はその製品を不合格としなければならず、CVE において脆弱性が報告される。

附属書 B：FDE 等価性検討

序説

本附属書は、FDE コラボラティブプロテクションプロファイルへ適合を主張しようと望むさまざまな OS／プラットフォームの製品の等価性についての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。

本評価の目的について、等価性は 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 に依存してさまざまであるかもしれない。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。

上記の具体的なカテゴリーのそれぞれの間での等価性の決定は、いくつかの異なるテスト結果をもたらす可能性がある。

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 の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 の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わたる必要はない。

TOE がインストールされるプラットフォーム／OS にかかわりなく同じように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 1 つの 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が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。

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

等価性を決定するための評価者ガイド

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等価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、この表には、モデル／プラットフォームにわたる追加的な別個のテストに至るシナリオも識別している。

要素	同一/同一でない	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、等価であるべき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があるか、またはそれらが PP 特有でない機能に該当するか、について識別しなければならない。cPP で規定された機能がプラットフォーム／ハードウェアの提供するサービスに依存する場合、TOE が特定のファームウェアの組合せで検証されたとみなされるためには、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／ハードウェアの提供する機能に依存する機能のみを再テストするという選択肢を有する。相違が PP 特有でない機能のみに影響する場合、それらのバリエーションは依然として等価であると考えられる。相違のそれぞれについて、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、評価者は等価であるべき複数の OS においてテストを考慮しなければならない。
	依存性	OS 間に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 PP 特有でない機能に該当するかについて識別しなければならない。cPP で規定された機能が 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のみを再テストするという選択肢を有する。相違が PP 特有でない機

要素	同一/同一でない	評価者ガイダンス
		能にのみ影響する場合、それらのモデルバリエーションは、依然として等価であると考えられる。相違のそれぞれについて評価者は、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	モデルの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	モデルのソフトウェアバイナリ間に相違がある場合、その相違が cPP 特有のセキュリティ機能に影響を与えるかどうかの決定が行わ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、ソフトウェアの相違により影響される機能のみを再テストするという選択肢を有する。相違が PP 特有でない機能のみに影響する場合、モデルは依然として等価であると考えられる。相違のそれぞれについて評価者は、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	同一	さまざまな TOE モデルで使用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 に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 に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のみを再テストするという選択肢を有する。異なるライブラリが PP 特有でない機能のみに影響する場合、モデルは依然として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、なぜその異なるライブラリについて、評価者は 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。

要素	同一/同一でない	評価者ガイダンス
TOE 管理インタフェースの相違	一貫性あり	さまざまな TOE の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 特有の機能がその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、それらのバリエーション／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によって設定可能な機能(及びいわゆる機能の設定)のみを再テストするという選択肢を有する。異なる管理インタフェースのみが PP に特有でない機能に影響する場合、それらのモデルは依然として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 に特有の機能に影響を与えるのか、または与えないのか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 のモデルバリエーションによって提供される機能が同一の場合、それらのモデルバリエーションは、等価であるとみなさ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って提供される機能が異なる場合、その機能の相違が cPP に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 に特有の機能がモデル間で相違する場合、それらの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のみを再テストするという選択肢を有する。機能の相違が PP に特有でない機能のみに影響を与える場合、それらのモデルバリエーションは依然として等価であると考えられる。それぞれの相違について、評価者はなぜその相違が cPP に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。

表 1 - 評価の等価性分析

戦略

等価性分析を行うにあたって、評価者は、各要因を独立に検討するべきである。個別の要因分析によって、以下の 2 つの結果の 1 つがもたらされる。

- 個別の要因について、サポートされるすべての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 1 つのモデルで 1 つのテスト環境で行われてもよく、サポートされるすべてのモデルや環境で行われてもよい。
- 個別の要因について、その他のすべての等価な TOE と同一の動作をすることが保証され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。分析によって、テストが必要なモデル／テスト環境の具体的な組み合わせを識別されることになる。

TOE の完全な CC テストは、識別された要因のそれぞれについて行なわれる個別の分析それぞれの全体を包含することになる。

テストプレゼンテーション／告知における真実

何をテストするべきかを決定することに加えて、評価結果及びそれによって得られる認証報告書は、テストされた実際のモジュール及びテスト環境の組み合わ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用いら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。

附属書 C：用語集

用語	意味
Authorization Factor (許可要素)	利用者がハードディスクを利用するための許可を受けるコミュニティに属していることを確立するために TOE へ送信されるような、及び BEV の導出または復号及び場合によっては DEK の復号で使用されるような、利用者の知っている値（例、パスワード、トークン等）。これらの値は、利用者の特殊な識別を確立するために使用されてもよいし、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].
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 (鍵の廃棄処理)	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されたデータを廃棄処理する方法。
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る鍵。
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及び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るものを指す。本セキュリティ課題定義(SPD)及び cPP のために、FDE は 1 つのパーティション上の暗号化と権限管理を実行する、OS とファイルシステムの連携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のみ、データへのアクセスを許可する。例外には、マスターブートレコード(MBR)またはその他の AA/EE の事前認証ソフトウェアのようなストレージデバイスの部分(サイズは実装によって変わる)を暗号化されないままに残す必要がある。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)	初期の利用者許可と DEK の間の地点において使用される鍵。
Host Platform (ホストプラットフォーム)	TOE が動作しているローカルのハードウェア及びソフトウェア、これはローカルハードウェア及びソフトウェアへ接続されるかもしれない周辺デバイス(例、USB デバイス)を含まない。
Key Chaining (鍵チェイニング)	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。

用語	意味
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)データとして一般に知られ、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、別の鍵の直接導出または復号用には使用されないもの。
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)	電源の供給なしに情報を保持しているある種のコンピュータメモリ。
Powered-Off State (電源切断状態)	デバイスがシャットダウンされている状態。
Protected Data (保護されたデータ)	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。オペレーティングシステム、アプリケーション、及び利用者データを書き込むことのできるディスク上のすべての空間を含む。保護データは、必ずしも暗号化されない領域で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)	サブマスクは多くの方法で生成でき、保存できるような、ビット列である。
Target of Evaluation (評価対象)	ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び／またはハードウェアのセット。[CC1]

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

附属書 D：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 (決定論的乱数ビット生成器)
DSS	Digital Signature Standard (ディジタル署名規格)
ECC	Elliptic Curve Cryptography (楕円曲線暗号)
ECDSA	Elliptic Curve Digital Signature Algorithm (楕円曲線ディジタル署名アルゴリズム)
EE	Encryption Engine (暗号エンジン)
EEPROM	Electrically Erasable Programmable Read-Only Memory (電気的消去可能プログラマブル ROM)
FIPS	Federal Information Processing Standards (連邦情報処理規格)
FDE	Full Drive Encryption (ドライブ全体暗号化)
FFC	Finite Field Cryptography (有限体暗号)
GCM	Galois Counter Mode (ガロアカウンターモード)
HMAC	Keyed-Hash Message Authentication Code (鍵付ハッシュメッセージ認証コード)
IEEE	Institute of Electrical and Electronics Engineers (アメリカ電気電子通信学会)
IT	Information Technology (情報技術)
ITSEF	IT Security Evaluation Facility (IT セキュリティ評価機関)
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission (国際標準化機構／国際電気標準会議)
IV	Initialization Vector (初期化ベクタ)
KEK	Key Encryption Key (鍵暗号化鍵)
KMD	Key Management Description (鍵管理記述)
KRK	Key Release Key (鍵出力鍵)
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)
RBG	Random Bit Generator (乱数ビット生成器)
RNG	Random Number Generator (乱数生成器)
RSA	Rivest Shamir Adleman Algorithm (リベスト・シャミア・エーデルマン(RSA)アルゴリズム)
SAR	Security Assurance Requirement (セキュリティ保証要件)
SED	Self Encrypting Drive (自己暗号化ドライブ)
SHA	Secure Hash Algorithm (セキュアハッシュアルゴリズム)
SFR	Security Functional Requirement (セキュリティ機能要件)
SPD	Security Problem Definition (セキュリティ課題定義)
SPI	Serial Peripheral Interface (シリアルペリフェラルインタフェース)
ST	Security Target (セキュリティターゲット)
TOE	Target of Evaluation (評価対象)

頭字語	意味
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