ハードコピーデバイスのプロテクションプロファイル

IPA、NIAP と MFP テクニカルコミュニティ

2015 年 9 月 10 日

バージョン 1.0

令和３年３月３日　和訳 第 j1.3 版

独立行政法人情報処理推進機構 JISEC

IPA まえがき

はじめに

本書は、ハードコピーデバイスのプロテクションプロファイルである「Protection Profile for Hardcopy Device」を翻訳した文書です。本書は、製品の開発や評価の際の参考資料として「IT セキュリティ評価及び認証制度」で作成したものです。翻訳にあたっては注意を払っていますが、正確を期する場合は原文を参照してください。

原文

Protection Profile for Hardcopy Device
Version 1.0
IPA, NIAP, and the MFP Technical Community
September 10, 2015

改訂履歴

版	日付	コメント
1.0	2015 年 9 月 10 日	初版発行

謝辞

本プロテクションプロファイルは、産業界、日米政府機関、コモンクライテリア評価機関、及び国際的なコモンクライテリアスキームからの代表者の参加する Multifunction Printers Technical Community により開発された。独立行政法人情報処理推進機構（IPA）と米国国家情報保証パートナーシップ（NIAP）は、発行に際して多大な貢献と献身的な取り組みをされた本グループのメンバーの皆様に感謝の意を表します。

目次

List of Tables

1 プロテクションプロファイル序説 (APE_INT, APE_CCL)

1.1 目的

¶1 本プロテクションプロファイル（PP）の目的は、情報技術セキュリティ評価のためのコモンクライテリア（CC）評価方法を用いて、市販（COTS）のハードコピーデバイス（HCD）の効率のよい調達を促進することである。

¶2 本書は、その目的を達成するための米国と日本の政府調達要件に基づく 2 か国の PP である。

¶3 顧客や一般的なセキュリティ専門家のため、本 PP の本序説は、自然言語を用いて、HCD の主な用途、運用環境についての前提条件、セキュリティ関連の使用事例、それらの使用事例を支援する主なセキュリティ機能について説明する。セクション 2 では、本 PP に適合する製品によって保護される資産、対抗される脅威、実施される方針について説明する。これらのセクションの意図は、潜在的な利用者に対して、本 PP が HCD についてのそれらのセキュリティ要件を満していることを決定するために十分な情報を提供することである。

¶4 また、HCD 開発者、CC 評価者、その他の CC 専門家のため、本 PP は評価対象（TOE）のセキュリティ課題を定義し、そのセキュリティ課題に対処するセキュリティ対策方針、セキュリティ機能要件（SFR）、セキュリティ保証要件（SAR）を特定するための標準的な CC の構造や言語も提供する。自然言語のセクションは、標準的な CC の定義と仕様に関する状況的背景を提供することを意図している。これらのセクションの意図は、開発者が評価に適合した製品を実装するための簡潔な情報を提供すると共に、評価者が客観的で再現可能な方法で製品の適合性をテストするための簡潔な情報を提供することである。

1.2 PP 識別と適合主張

¶5 **タイトル：** Protection Profile for Hardcopy Devices

¶6 **PP バージョン：** 1.0 dated September 10, 2015

¶7 **スポンサー：** IPA JISEC (Japan), NIAP CCEVS (US)

¶8 **著者：** MFP Technical Community

¶9 **編集者：** Brian Smithson, Ricoh Americas

¶ 10 **キーワード：** Multifunction Printer, Multifunction Peripheral, MFP, Multifunction Device, MFD, All-in-one, Hardcopy Device, HCD. Printer, Copier, Photocopier, Scanner, Fax

¶ 11 **CC 適合：** Common Criteria version: Version 3.1, Release 4, Part 2 (CCMB-2012-09-002) Extended, and Part 3 (CCMB-2012-09-003) Conformant.

¶ 12 **パッケージ適合：** 本プロテクションプロファイルはパッケージ[1]への適合を主張しない。

¶ 13 ***他のプロテクションプロファイルへの適合：*** 本プロテクションプロファイルは別のプロテクションプロファイルへの適合を主張しない。

¶ 14 **本プロテクションプロファイルへの適合：** 本プロテクションプロファイルへの適合を主張するためには、適合するセキュリティターゲットが以下のすべての規則に適合しなければならない：

¶ 15 1. TOE は、セクション 1.3.1.1 に記述されたスキャン、プリント、またはコピーの必須用途の少なくとも一つ、及びネットワーク通信と管理の必須用途をサポートしなければならない。

¶ 16 2. TOE によってサポートされるそれら必須用途のすべてのセキュリティについて、本プロテクションプロファイルの要件への適合性について評価されなければならない。

¶ 17 3. TOE が、セクション 1.3.1.2 に記述された条件付き必須用途のいずれかをサポートする場合、そのサポートは、附属書 B において記述された対応する条件付き必須の要件に適合していることを評価されなければならない。

¶ 18 4. 選択された通信プロトコルは、附属書 D.2 における対応する選択ベースのプロトコル要件への適合性について評価されなければならない。

¶ 19 5. セキュリティターゲット作成者は、セクション 1.3.1.3 に記述されたオプション用途のいずれかを評価のために含むために選択することができる。ベンダは、附属書 C に記述されたそれらのオプション機能を

[1] 本プロテクションプロファイルは、セキュリティターゲットが EAL1 及び追加の保証コンポーネント ASE_SPD.1 への適合を主張するために要求されるセキュリティ保証コンポーネントを含んでいる。プロテクションプロファイル自体は CC パート 3 で定義されるとおりの標準の PP 評価パッケージに適合している。

評価することが選択できる。

¶ 20 6. TOE は、*完全適合（Exact Conformance）*[2]を論証しなければならない。*完全適合*は、CC パート 1（CCMB-2012-09-001）の Annex D.2 に定義される*正確適合（Strict Conformance）*のサブセットとして、上記適合規則のすべてを満たす ST として定義されている。繰り返しは許容されているが、追加の要件（CC パート 2 または 3 からのもの）を ST に含めることは許容されない。

1.3 ハードコピーデバイス(HCD)の概要

1.3.1 用途

¶ 21 本 PP の評価対象は、HCD である。HCD は、ハードコピー文書をデジタル形式へ変換（スキャン）、デジタル文書をハードコピー形式へ変換（プリント）、ハードコピー文書を複写（コピー）、または PSTN 接続を介して文書を送信（PSTN ファクス）、等を実行するジョブ機能をサポートする。ハードコピー文書は、通常紙の形式をとるが、その他の形式（例えばスライド）のこともある。

¶ 22 本 PP の目的上、適合する HCD は、プリント、スキャン、またはコピーのうち少なくとも一つのジョブ機能をサポートしなければならない、かつネットワーク通信機能及び管理機能（セクション 1.3.1.1 に記述されるとおり）をサポートしなければならない。

¶ 23 HCD によりサポートされるジョブ機能及びネットワーク通信と管理機能は、適合する HCD の「必須用途」であり、必須の機能である。適合する HCD は、「条件付き必須用途」をサポートしてもよい。条件付き必須用途はオプション機能であり、HCD においては存在することは必須ではないが、HCD にそれらが存在する場合は条件付き必須要件を満たさなければならない。

1.3.1.1 必須用途

¶ 24 適合 HCD に存在しなければならない必須用途は以下のとおりである：

¶ 25 以下の一つ以上：

[2] 完全適合 (Exact Conformance) がコモンクライテリアに追加されるまでは、完全適合の要件はスキーム特有の要件である。CCRA での要求は正確適合（*Strict Conformance*）となる。

i. **プリント**：電子文書をハードコピー形式へ変換、または

ii. **スキャン**：ハードコピー文書を電子形式へ変換、

iii. **コピー**： ハードコピー文書を複製する

—かつ—

¶ 26 **ネットワーク通信**：ローカルエリアネットワーク（LAN）上で文書を送受信、

—かつ—

¶ 27 **管理**： HCD のセキュリティを設定、監査及び検証

¶ 28 言い換えれば、適合する HCD が少なくとも必須用途、スキャン、プリントまたはコピーのうちの一つをサポートし、必須用途、ネットワーク通信及び管理をサポートしなければならない。

1.3.1.2 条件付き必須用途

¶ 29 適合する HCD に存在するかもしれない条件付き必須用途は以下のとおり：

¶ 30 **PSTN ファクス**： 標準ファクシミリプロトコルを用いて、公衆電話回線交換網（PSTN）を介して文書を送受信する

¶ 31 **保存と取出し**：電子文書を保存し、後に、それらを取り出す

¶ 32 **現地交換可能な不揮発性ストレージ**：現地交換可能な不揮発性デバイスに文書または秘密のシステム情報を保存する

¶ 33 適合するためには、HCD は、TOE に存在する機能については、その機能に関係する要件を満たさなければならない。

1.3.1.3 オプション用途

¶ 34 適合する HCD に存在してもよいオプション用途は以下のとおりである：

¶ 35 **内部監査ログ格納**：監査証跡を HCD 内部に格納する

¶ 36 **画像上書き**：画像処理ジョブの終了時に残存画像を能動的に上書きする

¶ 37 **データ完全削除**：再配置、廃棄、またはその他の環境の変更のため HCD から顧客が提供したデータすべてを完全削除する

1.3.2　TOE の境界

¶ 38　TOE の物理的な境界は、HCD 製品全体である。フィニシャ等のセキュリティには無関係のオプションやアドオンは、TOE に含める必要はない。利用者が、HCD に個人的なストレージデバイス（ポータブルフラッシュメモリデバイス等）を接続可能な場合、それらのデバイスや中に含まれるデータは、TOE の適用範囲外であり、このようなデバイスに接続するインタフェースは無効化されるべきである。

¶ 39　TOE の論理的な境界は、セクション 1.3.1.1 に記述されたとおり、HCD の必須用途に関連するすべてのセキュリティ機能を含むと共に、セクション 1.3.1.2 に記述されたとおり、HCD に存在するすべての条件付き必須用途、及びセクション 1.3.1.3 に記述されるとおり、評価に含まれるべきすべてのオプション用途を含む。

1.3.3　運用環境

¶ 40　本 PP においては、HCD は、民間企業、政府、その他の組織によって、オフィス環境で使用され、有線ローカルエリアネットワーク（LAN）へ接続される。PSTN ファクス機能がある場合、HCD は PSTN ファクスを送受信するため、PSTN へも接続することが可能である。

¶ 41　利用者は、様々なインタフェースを通じて HCD と対話する：

- ローカル利用者は、物理的なオペレータコンソールを用いて HCD と対話する
- ネットワーク利用者は、LAN を介して HCD と通信する、HCD 外部のその他の IT デバイスやパソコンにインストールしたプログラムを用いて HCD と通信する。これには、ウェブブラウザのような一般的なクライアントプログラム及びプリントまたはスキャンドライバのような特定のプログラムの使用を含む。

¶ 42　HCD や外部 IT エンティティもまた、利用者本人の入力とは無関係に対話できる。

¶ 43　運用環境は、物理的にも論理的にも、その環境の外部で発生する脅威から保護されており、一般的に HCD への物理的なアクセスを制限し、公衆インターネットより保護された LAN に接続されることを想定している。

1.4 HCD のセキュリティ使用事例

¶ 44 セキュリティ使用事例は、利用者が HCD を使用する際に利用者のセキュリティに対する期待について説明する。

1.4.1 必須使用事例

¶ 45 適合する HCD の必須用途に関するセキュリティ関連の使用事例は以下のとおりである：

¶ 46 **1. 以下の一つ以上：**

a) **プリント**：ネットワーク利用者は、外部 IT エンティティから LAN 上の HCD へプリント指示と共に文書を送る。HCD には、利用者文書の HCD へのデータ送信中や、HCD 内での一時的保存中、及びプリント結果が利用者に出力される前に、利用者文書を不正な暴露や改ざんより保護する機能がある。

b) **スキャン**：ローカル利用者は、HCD 上で文書のスキャンを起動し、HCD はそのデジタル画像を外部 IT エンティティへ送る。HCD には、利用者文書の一時保存中や外部 IT エンティティへのデータ送信中に、利用者文書を不正な暴露や改ざんより保護する機能がある。

c) **コピー**：ローカル利用者は、HCD 上で文書をスキャンし、HCD は文書をプリントする。HCD には、HCD 内に一時保存中の利用者文書を不正な暴露や改ざんから保護する機能がある。

¶ 47 **2. 設定**：管理者特権を持つローカルまたはネットワーク利用者は、HCD のセキュリティ設定情報を設定する。HCD は、管理機能を実行可能な利用者と利用者機能を実行可能な利用者を区別するような、役割を利用者に対して割り当てる機能を持っている。HCD には、HCD への保存、外部 IT エンティティへの送信や受信に際して、セキュリティ設定情報を不正な暴露や改ざんから保護する機能も持っている。

¶ 48 **3. 監査**：許可された要員は、監査ログにおけるセキュリティ関連事象をモニターする。HCD は、セキュリティ関連事象が発生した時、監査ログ記録を生成する。HCD は、格納のため外部 IT エンティティへ監査ログをセキュアに送信できることが必須であり、HCD には外部 IT エンティティへの転送の間、不正な暴露または改ざんより監査ログを保護する機能を有する。

¶ 49 4. **ソフトウェアアップデートの検証：**許可された者が更新されたソフトウェアを HCD にインストールする。HCD は、許可された者のみがソフトウェアのインストールを許可されるということを保証し、インストールする人に対して、ソフトウェアアップデートの真正性の検証を支援する機能を持つ。

¶ 50 **5. HCD 機能の検証：**HCD は、電源起動時に毎回自己テストを実施することで、誤作動について自己チェックする。

1.4.2 条件付き必須使用事例

¶ 51 適合する HCD の条件付き必須用途（存在する場合）に関するセキュリティ関連の使用事例として以下を含むことができる：

¶ 52 **PSTN ファクス送信：** ローカル利用者が HCD で文書をスキャンするか、またはネットワーク利用者が文書を外部 IT エンティティから HCD へ送信して、利用者がそれを離れた PSTN ファクスの宛先へ送信する指示を行う；HCD は、標準 PSTN ファクスプロトコルを用いて PSTN 経由で PSTN ファクスの宛先へファクシミリ文書を送信する。HCD は、LAN 上での転送中にネットワーク利用者の文書を不正な暴露や改ざんより保護する機能を持つ。HCD は、また HCD 内で一時保存中に利用者の文書を不正な暴露や改ざんから保護する機能を持つ。

¶ 53 **PSTN ファクス受信**：リモートの PSTN ファクス送信者が、標準 PSTN ファクスプロトコルを用いて PSTN 経由で HCD にファクシミリ文書を送信する。HCD は受信した PSTN ファクスが HCD 内に存在する間、受信した PSTN ファクスを不正な暴露や改ざんより保護する機能を持つ。更に、HCD は PSTN ファクスモデムが LAN へのアクセスに使用されないことを確実にする機能を持つ。

¶ 54 **文書の保存と取り出し：**ローカルまたはネットワーク利用者は、HCD に指示を行い、HCD 内の電子文書を保存したり取り出したりする。このような文書の情報源と出力先は、スキャン、プリント、または PSTN ファクスのように他の操作のいずれかであってもよい。HCD は、転送中や保存中に、それらの文書を不正な暴露や改ざんより保護する機能を持つ

¶ 55 **現地交換可能な不揮発性ストレージデバイス：**許可された要員は、予防的なメンテナンス、修理、またはその他のサービス関連の操作を実施するために、HCD を運用環境におけるサービスから除去する。HCD は、

現地交換可能な不揮発性ストレージデバイスに存在するかもしれない文書または秘密のシステム情報を、このようなデバイスが HCD から除去される場合に、暴露から保護する能力を持つ。

1.4.3　オプション使用事例

¶ 56　適合する HCD のオプションの用途（存在する場合）に関するセキュリティ関連の使用事例として以下を含むことができる：

¶ 57　**内部監査ログ格納：**監査証跡が HCD にも格納可能な場合、HCD は監査証跡を許可されない暴露や改変から保護する能力を持つ。

¶ 58　**画像上書き：**画像処理ジョブの完了時、残存画像データが HCD に存在するかもしれない。HCD はこのような画像データを能動的に上書きする能力を持つ。

¶ 59　**HCD の再配置または廃棄：**許可された要員は、HCD を運用環境におけるサービスから除去して、異なる運用環境に移動したり、永久に運用が除去したり、さもなければ所有権を変更したりする。HCD が運用環境から除去される場合、HCD は、HCD に存在するかもしれないすべての顧客データが復元に利用できないようにする機能を持っている。

1.5　HCD の主なセキュリティ機能

¶ 60　セクション 1.4 の使用事例を支援するため、適合する HCD は、以下のセキュリティ機能を提供する：

1. 識別、認証、及び HCD 機能を使用するための権限付与
2. アクセス制御
3. 暗号化
4. 高信頼な通信
5. 管理者の役割
6. 監査
7. 高信頼な運用
8. PSTN ファクス-ネットワーク間の分離（PSTN ファクス機能がある場合）
9. データ消去及び完全削除（オプション）

¶ 61　これらの各機能は、次のサブセクションに記述されている。

1.5.1　識別、認証、及び権限付与

¶ 62　利用者の識別、認証、及び権限付与は、HCD の機能が、管理者によって権限付与された利用者のみにアクセス可能であることを保証する。利用者の識別と認証は、アクセス制御と管理者役割の根拠としても利用され、セキュリティ関連事象と HCD の使用を特定の利用者に関連付ける上での支援にもなる。識別と認証は、HCD または外部サーバによって実行されてもよい。

1.5.2　アクセス制御

¶ 63　アクセス制御は、文書や文書処理に関連する情報、セキュリティ関連データが、適切なアクセス権限を持つ利用者のみにアクセス可能であることを保証する。

1.5.3　データ暗号化

¶ 64　データ暗号化は、データ資産が、LAN 上での通信中にアクセスできないことを保証する。

¶ 65　- ポリシーにより、データ暗号化が現地交換可能な不揮発性ストレージデバイス上の文書及び秘密のシステム情報を保護したり、このようなデバイスが HCD から除去される場合にこのようなデータを保護するために使用される。

¶ 66　- データ暗号化の有効性は、国際的に承認された暗号アルゴリズムの使用により保証される。

1.5.4　高信頼な通信

¶ 67　高信頼な通信パスは、HCD との通信が既知の終端との間で行われることを保証するために確立される。

1.5.5　管理者の役割

¶ 68　役割によるアクセス制御は、HCD のセキュリティ設定を構成する能力が、管理者役割の権限が付与された利用者のみに利用可能であることを保証する。

1.5.6　監査

¶ 69　セキュリティ関連の事象と HCD の利用が許可された要員によりモニターできることを保証するため、監査ログは HCD により生成される。HCD は、監査ログを生成なければならず、保存のため外部 IT エンティティへそのログデータ

をセキュアに送信しなければならない。オプションとして、監査ログは管理者によりレビューできるような HCD にも保存されてもよい。

1.5.7　高信頼な運用

¶ 70　HCD へのソフトウェアのアップデートは、アップデートの適用前にソフトウェアの真正性を保証するために検証される。HCD は、その運用が検出可能な故障等により中断されないことを保証するため、自己テストを実行する。

1.5.8　PSTN ファクス-ネットワーク間の分離

¶ 71　適合する HCD が PSTN ファクス機能を備えている場合、PSTN ファクス-ネットワーク間の分離は、PSTN ファクスモデムが PSTN と LAN 間のデータ・ブリッジを生成するために使えないことを保証する。

1.5.9　データ消去及び完全削除

¶ 72　オプションとして、HCD は、画像データを能動的に上書きする機能、またはすべての顧客が提供した情報を許可された管理者の要求する時に完全消去する機能を提供してもよい。これらは附属書 C において議論される。

2 セキュリティ課題定義 (APE_SPD)

¶ 73 セキュリティ課題定義（SPD）は、２つの部分に分かれている。初めの部分は、資産、脅威、組織のセキュリティ方針について説話形式で記述する。[括弧] は、２番目の部分、利用者、資産、脅威、組織のセキュリティ方針、及び前提条件の正式な定義への参照を附属書 A に示す。

¶ 74 注意：本書のこの点から、評価対象は、製品分類の「HCD」（Hardcopy Device）の代わりに接頭辞「TOE」（Target of Evaluation：評価対象）によって参照される。

2.1 利用者

¶ 75 適合する TOE は、少なくとも次の 2 つの利用者役割を定義しなければならない：

1. 管理者役割を持たない、識別及び認証される一般利用者 [U.NORMAL]。
2. 管理者役割を持つ、識別及び認証される管理者 [U.ADMIN]。

¶ 76 適合する TOE は、追加の役割や副次的な役割、またはグループを許可してもよい。特に、TOE のさまざまな側面を管理する権限を持つ管理者役割を適合する TOE は、いくつか許可してもよい。

¶ 77 利用者は、人間または外部 IT エンティティであることに注意すること。

¶ 78 利用者に関するさらなる詳細な記述は、附属書 A.1 に書かれている。

2.2 資産

¶ 79 利用者の観点から、TOE における一次保護資産は、利用者文書データ [D.USER.DOC] である。利用者ジョブ命令、利用者ジョブデータ [D.USER.JOB]（利用者文書または文書処理ジョブに関連する情報）に対するセキュリティ侵害が利用者文書データの保護に影響する場合、それらについても保護してもよい。利用者文書データと利用者ジョブデータは合わせて利用者データと考えられる。

¶ 80 説明に役立つ事例として、プリント用にネットワーク利用者によって送信されたデータは、他の誰かにアクセスされてはならないような利用者の文書 [D.USER.DOC]、及び他の誰かに改ざんされてはならないようなスキャンされた文書の送信宛先等のジョブ命令 [D.USER.JOB]を含んでいる。

¶ 81 管理者の観点から、TOE における一次保護資産は、TOE のセキュアな運用を設定及びモニターするために使うデータである。この種のデータは、TOE セキュリティ機能 (TSF)データであると考えられる。

¶ 82 この種のデータは、大きく２つに分類される：

1. 保護された TSF データで、あらゆる利用者に閲覧されてもよいが、不正な改変や削除から保護されなければならないもの[D.TSF.PROT]；及び、
2. 秘密の TSF データで、権限のある利用者以外は、閲覧も改変も削除もできないもの[D.TSF.CONF]。

¶ 83 説明に役立つ事例として、権限のある利用者を識別及び認証するために TOE が使用するデータである。一般に、識別のために使用する利用者名は誰でも閲覧できるが、不正な改変や削除から保護しなければならない [D.TSF.PROT]。一方、認証のために使用する利用者パスワードは、権限のないあらゆるアクセスを禁止し、秘密に保たなければならない [D.TSF.CONF]。

¶ 84 TSF データが侵害を受けた場合、特権の昇格、格納文書へのアクセス、処理された文書の宛先変更、権限のある利用者または管理者へのなりすまし、TOE の運用中のソフトウェアの改ざん、外部 IT エンティティへの攻撃を含む、悪意のある目的に使用される可能性がある。

¶ 85 適合する TOE において、TSF データは、保護された TSF データ、または秘密の TSF データのいずれかに明確に識別され、分類される。

¶ 86 ネットワークセキュリティの観点から、運用環境において TOE と他の IT エンティティのセキュアな運用を保証することが重要である。運用環境は TOE の適用範囲外なので、組織のセキュリティ方針が運用環境の保護に対処するために使用される。

¶ 87 資産についてさらに詳細な記述は、附属書 A.2 に書かれている。

2.3 脅威

¶ 88 適合製品が対抗する TOE に対する脅威は、以下のとおりである。脅威についてさらに詳細な記述は、附属書 A.3 に書かれている。

2.3.1 利用者データへの不正なアクセス

¶ 89 攻撃者は、TOE 内の利用者文書データに対するアクセス（閲覧、改変、または削除）、または利用者ジョブデータに対する変更(改変、または削除)を TOE

のインタフェースの一つを通して行うかもしれない [T.UNAUTHORIZED_ACCESS]。例えば、TOE の設計により、攻撃者は、ネットワーク利用者のプリントジョブのプリント出力へアクセスしたり、プリント待ちのジョブ命令を改変したり、利用者個人またはグループの保存領域の利用者文書データを閲覧しようと試みるかもしれない。

2.3.2 TSF データへの不正アクセス

¶ 90 攻撃者は、TOE 内の TSF データへ TOE のインタフェースの一つを通して不正アクセスを得るかもしれない [T.TSF_COMPROMISE]。例えば、TOE の設計により、攻撃者は、自身の特権を昇格させるために TSF データに不正アクセスしたり、さまざまな宛先に出力を変更するためアドレス帳を改ざんしたり、外部サーバへのアクセスを得るために TOE のクレデンシャル情報を使用するかもしれない。

¶ 91 攻撃者は、TOE に不正なソフトウェアをインストールしようとするかもしれない [T.UNAUTHORIZED_UPDATE]。例えば、TOE が処理する情報へのアクセスを得るため、または LAN 上でその他のシステムを攻撃するために不正なソフトウェアが使用されるかもしれない。

2.3.3 ネットワーク通信への攻撃

¶ 92 攻撃者は、通信中のデータにアクセスするか、またはネットワーク通信をモニターしたり、操作したりして TOE のセキュリティを侵害するかもしれない [T.NET_COMRPOMISE]。例えば、ネットワーク通信を侵害できるかもしれない方法がいくつかある：有線 LAN 上の平文通信を傍受することにより、攻撃者は、利用者文書データ、利用者クレデンシャル情報、またはシステムクレデンシャル情報を入手したり、または対話型セションをハイジャックしたりするかもしれない。攻撃者は、文書にアクセスする権限を付与された利用者として、またはセキュリティ設定を変更する権限を付与された管理者として、TOE にログインするためネットワーク通信セションを記録しリプレイするかもしれない。攻撃者は、発出するスキャンジョブを受信したり、システムクレデンシャル情報の送信を記録したり、または TOE へ悪意のあるデータを送ったりするため、LAN 上の信頼されるシステムになりすましするかもしれない。

2.3.4 故障

¶ 93 劣化した状態で TOE が運用を許可された場合、TSF の故障によりセキュリティの喪失を起こすかもしれない [T.TSF_FAILURE]。ハードウェアまたはソフ

トウェアの故障は、セキュリティ機能が正しく動作しない可能性のある、予測不能な結果をもたらすことがある。

2.4 組織のセキュリティ方針

¶ 94 以下は、適合する製品が掲げる組織のセキュリティ方針[3]（OSP）である。OSP についてのさらなる詳細情報は、附属書 A.4 に述べる。

2.4.1 利用者への権限付与

¶ 95 文書処理や管理者機能を実行する前に、利用者は、権限付与されなければならない [P.AUTHORIZATION]。TOE 所有者は、誰が TOE の資源を使用でき、誰が管理者機能の実行を許可されているかについての管理を権限付与によって許可する。

2.4.2 監査

¶ 96 セキュリティ関連のアクティビティは、監査されなければならず、そのようなアクションのログは保護され、外部 IT エンティティへ送信されなければならない [P.AUDIT]。外部 IT エンティティ上に保存され（または、オプションで TOE にも保存され）、監査証跡は、許可された要員がレビュー可能であり、不審なアクティビティの識別を行い、サイト方針や法令で義務付けられるような TOE 利用の説明責任を果たすことを可能とする。

2.4.3 保護された通信

¶ 97 TOE は、LAN 上の他のデバイスに対し自身を識別できなければならない [P.COMMS_PROTECTION]。識別を保証することは、着信するプリントジョブを受信したり、利用者クレデンシャル情報の送信を記録したり、または外部 IT エンティティに悪意のあるデータを送信したりするために、攻撃者が TOE になりすますことの防止に役立つ。

2.4.4 ストレージ暗号化（条件付き必須）

¶ 98 TOE が利用者文書データまたは秘密の TSF データを現地交換可能な不揮発性

[3] 組織のセキュリティ方針は、TOE により支持／強制されるセキュリティ方針を包含する用語である。すなわち、TOE は識別された方針を強制する必要がある組織の要件を援用する。サイト方針は PP において特定し得ない顧客のセキュリティ方針として参照する一般的な用語である。

ストレージデバイス[4]上に格納する場合、TOE はそれらのデバイス上のこのようなデータを暗号化する[P.STORAGE_ENCRYPTION]。データは、その運用環境において TOE が動作している時、TSF によって保護されると想定される。しかし、現地交換可能な不揮発性ストレージデバイスが、保守サービス、他の環境への再配置、または廃棄のために、TOE から除去される場合、攻撃者は、利用者文書データまたは秘密の TSF データを暴露または改変できるかもしれない。このようなデータの暗号化は、攻撃者が暗号鍵や鍵材料へのアクセスなしに、そのようなことを実行するのを防止する。

¶ 99 利用者文書データまたは秘密の TSF データの現地交換可能な不揮発性ストレージのための暗号鍵の生成に寄与する平文の鍵、サブマスク、乱数、またはその他の値は、不正なアクセスから保護されなければならない、かつそのストレージデバイス上に保存してはならない[P.KEY_MATERIAL]。平文の鍵材料の許可されていない保有は、攻撃者が利用者文書データまたは秘密の TSF データを復号することを許してしまうかもしれない。

2.4.5 PSTN ファクス-ネットワーク間の分離（条件付き必須）

¶ 100 TOE に PSTN ファクス機能がある場合、TOE は PSTN ファクス回線と LAN の間の分離を保証する [P.FAX_FLOW]。TOE は、外部のファイアウォール等によって、保護された運用環境にあると想定される。しかし、PSTN ファクスモデムは、公衆交換電話網へ接続される。PSTN ファクスとネットワークの分離を保証することは、攻撃者が保護された環境へアクセスするためにファイアウォールまたはその他の外部保護を迂回するために PSTN ファクスモデムを使用することを防止する。

2.4.6 画像上書き（オプション）

¶ 101 文書処理ジョブの完了または中止の際に、その TOE は現地交換可能な不揮発性ストレージデバイスから残存画像データを上書き消去しなければならない[P.IMAGE_OVERWRITE]。 顧客は、文書処理ジョブが完了又は中止した後、TOE で動作しているソフトウェアにより参照されなくなった画像データが TOE 内の現地交換可能な不揮発性ストレージデバイス上に残存しているかもしれないという懸念を持つかもしれない。このような顧客は、画像データが

[4] 「現地交換可能な不揮発性ストレージデバイス」は、主たる目的が不揮発性ストレージを提供することであるようなあらゆる現地交換可能なユニット（FRU:Field-Replaceable Unit）である。OSP (組織のセキュリティ方針) は、主としてストレージ用に使用されない大規模な FRU の非現地交換部品であるストレージデバイスには適用されない。

その他のデータで上書き消去することによって利用不可能になることを望んでいる。

2.4.7　データ完全削除（オプション）

¶ 102　TOE は、許可された管理者が、すべての顧客が提供した利用者データ及び TSF データが不揮発性ストレージデバイスから永久に取り出せないようにするために起動できる機能を提供しなければならない [P.PURGE_DATA]。顧客は運用環境において保護されているデータが、サービスを終了するかまたは異なる運用環境へ再配置されるため、TOE がその運用環境から永久に除去された後、不揮発性ストレージデバイスに残存するかもしれないことを懸念するかもしれない。このような顧客は、すべての顧客が提供した利用者データ及び TSF データが運用環境の外で取り出せないように、TOE から完全削除されることを望んでいる。

2.5　前提条件

¶ 103　以下の前提条件について、本 PP で記述する脅威に、対策方針及び要件が効果的に対抗するため、満たされなければならない。前提条件についてのさらなる詳細情報は附属書 A.5 に記述する。

2.5.1　物理的セキュリティ

¶ 104　物理的セキュリティについては、TOE、及び TOE に格納され処理されるデータの価値に見合ったものが環境により提供されると想定する [A.PHYSICAL]。TOE は物理的攻撃が防止または検知されるように管理され、監視されるような物理的環境に設置されると想定する。

2.5.2　ネットワークセキュリティ

¶ 105　運用環境は、TOE をその LAN インタフェースへ直接の、外部からのアクセスから保護すると想定する [A.NETWORK] 。TOE は、管理されていないネットワーク環境からのネットワークによる攻撃に対抗することを意図していない。

2.5.3　管理者の信頼

¶ 106　TOE 管理者は、サイトセキュリティ方針に従い TOE を管理すると信頼されている[A.TRUSTED_ADMIN]。サイト方針に従い TOE を設定し、運用し、悪意のある目的で特権を使用しないと信頼されている管理者のみに権限付与することは TOE 所有者の責任である。

2.5.4　利用者の訓練

¶ 107　権限のある利用者は、サイトセキュリティ方針に従い TOE を利用するよう訓練を受けている [A.TRAINED_USERS]。サイト方針に従い TOE を利用するよう訓練された利用者に対してのみ権限付与を行うことは TOE 所有者の責任である。

3 セキュリティ対策方針 (APE_OBJ)

3.1 TOE のセキュリティ対策方針

¶ 108 以下のセキュリティ対策方針は、TOE によって満たされなければならない。TOE の対策方針についてのさらなる詳細情報は、附属書 A.6 及び A.7 に記述する。

3.1.1 利用者の権限付与

¶ 109 TOE は、セキュリティ方針に従い利用者の権限付与を実行しなければならない [O.USER_AUTHORIZATION]。

¶ 110 本対策方針は、TOE を管理するか、または TOE 資源を消費する文書処理機能を実行するために、利用者に権限を付与するという方針を支援する。利用者は、TOE に存在する文書処理機能のいずれかを実行するためには、権限を付与されなければならない。

¶ 111 権限付与のメカニズムは、TOE 内に実装され、さらに信頼された外部 IT エンティティに依存してもよい。適合する TOE が 2 つ以上のメカニズムをサポートする場合、それぞれについて別の運用モードとして評価されるべきである。

¶ 112 プリントの場合（TOE にその機能が存在する場合）、利用者への権限付与は、ジョブ投入後に実行されてもよいが、利用者がプリント出力を入手する前に実行されなければならない。

¶ 113 利用者は、適合する TOE が PSTN ファクス送信機能と文書の保存と取り出し機能を提供する場合、それらの機能を実行するために権限が付与されなければならない。

¶ 114 TOE は、利用者への権限付与なしでも PSTN ファクスを受信することができるが、受信文書はアクセス制御の対象になるという点に注意すること。

3.1.2 利用者の識別と認証

¶ 115 TOE は、アクセス制御、利用者の権限付与、または管理者役割が要求される操作のため、利用者の識別及び認証を実行しなければならない[O.USER_I&A]。

¶ 116 識別及び認証（I&A）のメカニズムは、TOE 内に実装され、さらに信頼された外部 IT エンティティ（例えば、LDAP、Kerberos、または Active Directory）に依存してもよい。適合する TOE が 2 つ以上のメカニズムをサポートする場合、それぞれについて別々の運用モードとして評価するべきである。

3.1.3　アクセス制御

¶ 117　TOE は、セキュリティ方針に従って、利用者データ及び TSF データを保護するアクセス制御を実施しなければならない [O.ACCESS_CONTROL]。

¶ 118　本 PP におけるアクセス制御セキュリティ方針についての指針は以下のとおりである：

- 利用者文書データ[D.USER.DOC]は、文書所有者または管理者のみがアクセスできる。
- 利用者ジョブデータ[D.USER.JOB]は、あらゆる利用者が閲覧できるが、ジョブ所有者または管理者のみが改変できる。
- 保護された TSF データ[D.TSF.PROT]は、あらゆる利用者が閲覧できるが、管理者または（特定の場合）そのデータの所有者である一般利用者またはそのデータに関係する一般利用者のみが改変できるデータである。
- 秘密の TSF データ[D.TSF.CONF]は、管理者または（特定の場合）所有者である一般利用者か、またはそのデータに関係する一般利用者のみによってアクセスが可能なデータである。

¶ 119　適合する TOE のセキュリティターゲットは、利用者データ及び TSF データのアクセス制御方針を明確に特定しなければならない。

3.1.4　管理者の役割

¶ 120　TOE は、権限付与された管理者のみが管理者機能の実行を許可されていることを保証しなければならない[O.ADMIN_ROLES]。

¶ 121　この対策方針は、一般利用者と区別される管理者役割が少なくとも一つは持つという必要性に対処する。適合する TOE は、例えばデバイス管理、ネットワーク管理、または監査マネジメント等、特別な管理者のサブ役割を持ってもよい。

3.1.5　ソフトウェアアップデート検証

¶ 122　TOE は、ソフトウェアアップデートの真正性を検証するメカニズムを提供しなければならない[O.UPDATE_VERIFICATION]。

¶ 123　本対策方針は、悪意のあるソフトウェアがソフトウェアアップデートとして TOE に導入されるかもしれないという懸念に対処する。例えばデジタル署名または公開ハッシュを用いた真正性検証が要求される。アクセス制御自体では本対策方針を満たさない。

3.1.6　自己テスト

¶ 124　TOE は、セキュリティ機能のサブセットをテストしなければならず、これによりサブセットが正常に動作していることの保証を支援する[O.TSF_SELF_TEST]。

¶ 125　故障が検知されず TOE の運用が許可された場合、TOE の故障はセキュリティを危殆化するかもしれない。自己テストは、このような故障を検知することを意図している。電源投入時の処理中に自己テストが実行される。

3.1.7　通信の保護

¶ 126　TOE は、不正なアクセス、リプレイ、送信元／宛先のなりすましからの利用者データ及び TSF データの LAN 通信を保護する機能を有していなければければならない[O.COMMS_PROTECTION]。

¶ 127　本対策方針は、ネットワーク通信に共通の懸念に対処している：

- 機微なデータまたはクレデンシャル情報は、TOE 外の LAN データを傍受することにより入手される。
- 認証が成功したセションが LAN 上でキャプチャされ、リプレイされることで、攻撃者が認証された利用者になりすますことを可能にする。
- 機微なデータまたはクレデンシャル情報は、TOE からの通信または外部 IT エンティティからの通信を悪意のある宛先にリダイレクトすることで入手される。

3.1.8　監査

¶ 128　TOE は、監査データを生成し、信頼される外部 IT エンティティへ送信可能でなければならない。オプションとして、TOE は監査データを TOE 内に格納してもよい [O.AUDIT]。

¶ 129　TOE は、監査データを信頼される外部 IT エンティティ（例えば、syslog サーバ等の監査サーバ）へ送信できなければならない。監査データは、機密性と完全性を保証するため、適切なアクセス制御を用いて TOE 内に保存してもよい。適合する TOE が両方のメカニズムをサポートする場合、それぞれについて別々の運用モードとして評価されるべきである。

3.1.9　ストレージ暗号化(条件付き必須)

¶ 130　TOE が利用者文書データまたは秘密の TSF データを現地交換可能な不揮発性ストレージデバイスに格納する場合、TOE はそれらのデバイス上にあるこの

ようなデータを暗号化しなければならない[O.STORAGE_ENCRYPTION]。

¶ 131 本対策方針は、現地交換可能な不揮発性ストレージデバイスが保守サービス、別の環境への再配置または廃棄等により TOE から除去される場合、デバイス上の利用者文書データまたは秘密の TSF データが暴露されるかもしれないという懸念に対処する。

3.1.10 鍵材料の保護（条件付き必須）

¶ 132 TOE は、現地交換可能な不揮発性ストレージデバイスの利用者文書データ又は秘密の TSF データを格納するための暗号鍵の生成に寄与するあらゆる平文の鍵、サブマスク、乱数又はその他の値を、不正アクセスから保護しなければならない；TOE は、そのような鍵材料が、その材料を使用するデバイス上に平文で格納されないことを保証しなければならない[O.KEY_MATERIAL]。

¶ 133 本対策方針は、利用者文書データまたは秘密の TSF データを復号するために使用されるかもしれない鍵または鍵材料の不正な保有に対処する。

3.1.11 PSTN ファクス-ネットワーク間の分離(条件付き必須)

¶ 134 TOE が PSTN ファクス機能を提供する場合、TOE は PSTN ファクス電話回線と LAN の間の分離をシステム設計または動作中のセキュリティ機能によって保証しなければならない[O.FAX_NET_SEPARATION]。

¶ 135 本対策方針は、ファイアウォール内にあるデバイスに接続された電話回線があることに対する顧客の懸念に対処するものである。実装に依存して、異なる方法で本対策方針を満たすことができる。例えば、システムアーキテクチャ（PSTN ファクスインタフェースからネットワークインタフェースへのデータ経路がないこと）、システム設計（ファクスチップセットは PSTN ファクスプロトコルのみを認識すること）、動作中のセキュリティ機能（フロー制御）。

3.1.12 画像上書き(オプション)

¶ 136 文書処理ジョブの完了または中止の際に、TOE は現地交換可能な不揮発性ストレージデバイス内の残存画像データを上書き消去しなければならない[O.IMAGE_OVERWRITE]。 本対策方針は、文書処理ジョブが完了または中止した後、画像データが TOE 内の現地交換可能な不揮発性ストレージデバイス上に残存するかもしれないという顧客の懸念に対処する。

3.1.13 データ完全削除(オプション)

¶ 137 TOE は、許可された管理者が、すべての顧客が供給した利用者データ及び TSF データが不揮発性ストレージデバイスから永久に取り出せないようにするために起動できる機能を提供する [O.PURGE_DATA]。 本対策方針は、顧客が、運用環境において保護されているデータが、サービスを終了するかまたは異なる運用環境へ再配置されるため、TOE がその運用環境から永久に除去された後、不揮発性ストレージデバイスに残存するかもしれないという懸念に対処する。

3.2 運用環境のセキュリティ対策方針

¶ 138 以下のセキュリティ対策方針は、運用環境によって提供されなければならない。運用環境の対策方針についてのさらなる詳細情報は附属書 A.7 に記述する。

3.2.1 物理的保護

¶ 139 運用環境は、TOE の価値、及び TOE にて格納または処理するデータの価値に相応しい、物理的な保護を提供しなければならない [OE.PHYSICAL_PROTECTION]。

¶ 140 その意図する機能のため、この種の TOE は、権限の付与された利用者が物理的アクセス可能でなければならないが、物理的な攻撃に対して耐えうるよう堅牢であるとは想定されていない。従って、その環境は、適切なレベルの物理的な保護または物理的攻撃を防止するためのモニタリングを提供しなければならない。

3.2.2 ネットワーク保護

¶ 141 運用環境は、外部からの直接の LAN インタフェースへのアクセスから TOE を保護するため、ネットワークセキュリティを提供しなければならない [OE.NETWORK_PROTECTION]。

¶ 142 この種の TOE は、敵意のあるネットワークに直接接続することを意図していない。従って、その環境は、適切なレベルのネットワーク隔離を提供しなければならない。

3.2.3 信頼された管理者

¶ 143 TOE 所有者は、管理者がその権限を悪意のある目的で使用しないという信頼を確立しなければならない[OE.ADMIN_TRUST]。

¶ 144 管理者は、悪意のある目的で悪用でき得る権限を持っている。TOE 所有者が信頼できる個人にのみ管理者権限を与えるということは、TOE 所有者の責任である。

3.2.4 訓練された利用者

¶ 145 TOE 所有者は、利用者がサイトセキュリティ方針を自覚し、それに従う力量を持っていることを保証しなければならない[OE.USER_TRAINING]。

¶ 146 サイトセキュリティは、TOE セキュリティ機能とそれら機能の一般利用者による適切な使用の組み合わせに依存している。製造事業者は、一般利用者に適用する TOE セキュリティ機能に関して TOE 所有者向けガイダンスを提供してもよい。

3.2.5 訓練された管理者

¶ 147 TOE 所有者は、管理者がサイトセキュリティ方針を理解し、TOE を正しく設定し、かつパスワードと鍵をそれぞれ保護するために製造事業者のガイダンスを使用する力量を持っていることを保証しなければならない[OE.ADMIN_TRAINING]。

¶ 148 この種の TOE は、セキュリティ機能を有効化及び無効化する多くのオプションを持っているかもしれない。管理者は、サイトセキュリティ方針を実施するために、TOE セキュリティ機能を理解し、設定することができなければならない。

4 セキュリティ機能要件(APE_REQ, APE_ECD)

4.1 表記法

¶ 149 **ボールド**書体は、本プロテクションプロファイルで完成または詳細化された SFR の部分を示し、コモンクライテリア パート 2 の本来の SFR 定義または拡張コンポーネント定義に関連している。

¶ 150 *イタリック*書体は、適合するセキュリティターゲットにおいて ST 作成者によって選択され、かつ／または完成されなければならない SFR 内のテキストを示す。

¶ 151 ***ボールドイタリック***書体は、本プロテクションプロファイルで完成または詳細化された SFR の部分を示し、コモンクライテリア パート 2 の本来の SFR 定義または拡張コンポーネント定義に関連している SFR の部分を示している。これらは、また、適合するセキュリティターゲットにおいて ST 作成者によって選択され、かつ／または完成されなければならない。

¶ 152 括弧内に文字、例えば、(a)、(b)、・・・、が続くような SFR コンポーネントは、必須の繰返しを示す。

¶ 153 拡張コンポーネントは、SFR 識別に「_EXT」を追加して識別される。

4.2 拡張コンポーネント

¶ 154 拡張コンポーネント定義は、附属書 A.9 に列挙される。

4.3 クラス FAU：セキュリティ監査

4.3.1 FAU_GEN.1 監査データ生成

(O.AUDIT)
下位階層： なし
依存性： FPT_STM.1 高信頼タイムスタンプ

¶ 155 **FAU_GEN.1.1** TSF は、以下の監査対象事象の監査記録を生成できなければならない：

¶ 156 a) 監査機能の起動と終了；

¶ 157 b) 監査の**指定なし**レベルのすべての監査対象事象；及び

¶ 158 c) 表 1 監査対象事象に掲載されたすべての監査対象事象、［割付：*その他の特別に定義された監査対象事象*］。

¶ 159 **FAU_GEN.1.2** TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

¶ 160 a) 事象の日付・時刻、事象の種別、サブジェクト識別情報(該当する場合)、事象の結果(成功または失敗)；及び

¶ 161 b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、**表 1 に示す追加情報**、［割付：*その他の監査関連情報*］。

表 1 監査対象事象

監査対象事象	関連の SFR	追加情報
ジョブの終了	FDP_ACF.1	ジョブ種別
利用者認証失敗	FIA_UAU.1	なし
利用者識別失敗	FIA_UID.1	なし
管理機能の利用	FMT_SMF.1	なし
役割の一部である利用者グループの改変	FMT_SMR.1	なし
時刻の変更	FPT_STM.1	なし
セション確立の失敗	FTP_ITC.1, FTP_TRP.1(a), FTP_TRP.1(b)	失敗の理由

¶ 162 ***適用上の注釈：***

¶ 163 *利用者識別事象が利用者認証事象から分離できない場合、それらは監査目的として一つの事象とみなしてもよい。*

¶164 *FMT_SMR.1 に関して、利用者と役割の関係が変更可能でない場合、その監査対象事象は生成されることができないため、監査記録を生成する要件は無視することができる。*

¶165 *ST 作成者は、表のその他の監査対象事象を直接含めることができる；それらは、提示されたリストに限定されない。*

¶166 **保証アクティビティ：**

¶167 ***TSS：***

¶168 評価者は、監査対象事象及び記録された情報が SFR の定義と一貫していることを保証するため、TOE 要約仕様（TSS）をチェックしなければならない。

¶169 ***操作ガイダンス：***

¶170 評価者は、監査対象事象と記録された情報が SFR 定義と一貫していることを保証するため、ガイダンス文書をチェックしなければならない。

¶171 ***テスト：***

¶172 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：

¶173 評価者は、表 1 に記述されたそれぞれの監査対象事象の監査記録が適切に生成されることを保証するため、チェックしなければならない。

¶174 評価者は、監査対象事象の生成方法が複数ある場合、それらの方法の代表的なサンプルをチェックしなければならない。

¶175 評価者は、いくつかの異なる I&A メカニズムがある場合、それぞれのメカニズムについて、FIA_UAU.1 事象が生成されていることをチェックしなければならない。

4.3.2 FAU_GEN.2　利用者識別情報の関連付け

(O.AUDIT)

下位階層：　なし

依存性：　FAU_GEN.1 監査データ生成

FIA_UID.1 識別のタイミング

¶176 **FAU_GEN.2.1** 識別された利用者のアクションがもたらした監査事象に対し、

TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

¶ 177 **保証アクティビティ：**

¶ 178 FAU_GEN.1 の保証アクティビティは本 SFR に対処している。

4.3.3 FAU_STG_EXT.1　拡張：外部監査証跡格納

(O.AUDIT)

下位階層：　なし

依存性：　FAU_GEN.1 監査データ生成、

FTP_ITC.1 TSF 間高信頼チャネル

¶ 179 **FAU_STG_EXT.1.1** TSF は、FTP_ITC.1 に従い、高信頼チャネルを用いて、外部 IT エンティティへ生成した監査データを送信できなければならない。

¶ 180 **保証アクティビティ：**

¶ 181 ***TSS：***

¶ 182 評価者は、監査データが外部監査サーバに送信される手段、及び高信頼チャネルがどのように提供されるのかについて TSS に記載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。高信頼チャネルメカニズムのテストは、特定の高信頼チャネルメカニズムに関する一連の保証アクティビティとして指定されるとおりに実行されるだろう。

¶ 183 評価者は、ローカル保存される監査データの容量；ローカル監査データの保存領域が満杯になった時に何が起きるか；これらの記録を不正なアクセスからどのように保護しているかについて、TSS に記載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、ローカル監査データと監査ログサーバへ送信される監査データの関係について、操作ガイダンスに記載されていることを決定するために操作ガイダンスを検査しなければならない。例えば、ある監査事象が生成されたとき、外部サーバとローカル保存領域へ同時に送信されるのか、またはローカル保存領域はバッファとして使用され、監査サーバへのデータ送信により定期的に「消去」されるのか。

¶ 184 ***操作ガイダンス：***

¶ 185 評価者は、監査サーバへの高信頼チャネルをどのように確立するかについて、監査サーバのあらゆる要件（特定の監査サーバプロトコル、要求されるプロトコルのバージョン等）についての記載や監査サーバと通信するために必要な TOE の設定と同様に、操作ガイダンスに記載されていることを保証するため、操作ガイダンスについても検査しなければならない。評価者は、本要件について以下のテストを実行しなければならない：

¶ 186 ***テスト：***

¶ 187 テスト 1：評価者は、提供された設定ガイダンスに従い、TOE と監査サーバ間にセションを確立しなければならない。次に、評価者は、監査サーバへ送信される監査データを生成するために、評価者が選択し考案するいくつかのアクティビティの間に、監査サーバと TOE の間を通過するトラフィックを検査しなければならない。評価者は、転送中にこれらのデータが平文で見ることができないこと、及び監査サーバがデータを正常に受信していることを確認しなければならない。評価者は、テスト中、監査サーバ上で使用される特定のソフトウェア（名称、バージョン）を記録しなければならない。

4.4 クラス FCO：通信

¶ 188 FCO クラスの要件は、なし。

4.5 クラス FCS：暗号サポート

4.5.1 FCS_CKM.1(a)　暗号鍵生成 (非対称鍵用)

(O.COMMS_PROTECTION)
下位階層：　なし
依存性：　[~~FCS_CKM.2 暗号鍵配付、または~~
FCS_COP.1(b) 暗号操作（署名生成／検証）]
FCS_CKM_EXT.4 拡張：暗号鍵材料廃棄

¶ 189 **FCS_CKM.1.1(a) 詳細化：** TSF は、以下に従って、**鍵確立で使用される非対称**暗号鍵を生成しなければならない［選択：

- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite***

field-based key establishment schemes;

- ***NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [選択: P-521, no other curves] (as defined in FIPS PUB 186-4, "Digital Signature Standard")***
- ***NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes***

¶ 190 **] 及び 112 ビット相当の対称鍵強度、またはそれ以上の指定された暗号鍵サイズ。**

¶ 191 ***適用上の注釈：***

¶ 192 *ST 作成者は、鍵確立及びデバイス認証のために使用する鍵生成スキームを選択する。 複数のスキームがサポートされている場合、ST 作成者は本機能を取り込むため、本コンポーネントを繰り返すべきである。鍵生成がデバイス認証のために使用されるとき、公開鍵は X.509v3 証明書と関連付けされると想定される。TOE が RSA 鍵確立において受信側として動作する場合、TOE は RSA 鍵生成を実装する必要はない。*

¶ 193 *使用するドメインパラメタは、本 PP のプロトコルの要件により指定されるので、TOE がドメインパラメタを生成すると想定されていないので、本 PP で指定されたプロトコルに TOE が適合する場合、追加のドメインパラメタ検証は一切ない。*

¶ 194 *FIPS SP 800-56B は、FIPS 186-3 に従った鍵生成を参照している（が必須ではない）。HCD PP の本バージョンにおける適合の目的として、TOE が SP 800-56B への適合を主張するために、FIPS186-4 に従った RSA 鍵ペア生成が許されている。*

¶ 195 *生成された 2048 ビットの DSA 鍵と rDSA 鍵の鍵強度は、112 ビットの対称鍵強度と同等かそれ以上である必要がある。同等な鍵強度についての情報は、NIST Special Publication 800-57、「Recommendation for Key Management」を参照。*

¶ 196 **保証アクティビティ：**

¶ 197 ***TSS：***

¶198 評価者は、選択に応じて、TSF が 800-56A 及び／または 800-56B にどのように適合するかについての記載が TSS に含まれていることを保証しなければならない。本記述には、TSF によって実装される 800-56A 及び／または 800-56B のセクションを示さなければならない、また、評価者は、TSF が実装を主張しているそれらのセクション中に鍵確立があることを保証しなければならない。

¶199 TOE 特有のあらゆる拡張、本書に含まれていない処理、または TOE が実施すべきセキュリティ要件に影響を与えうるような、本書によって許可された別の実装については、TSS に記載しなければならない。

¶200 TSS は、評価者に鍵管理記述（KMD）を参照させることができる、KMD は附属書 F に記述されており、公表しなくてよいものである。

¶201 *テスト：*

¶202 評価者は、ST 作成者が行った選択によって、上記要件のテストでのガイドとして、「The FIPS 186-4 Digital Signature Algorithm Validation System （DSA2VS）」、「The FIPS 186-4 Elliptic Curve Digital Signature Algorithm Validation System（ECDSA2VS）」、及び「The 186-4 RSA Validation System （RSA2VS）」の鍵ペア生成部分を利用しなければならない。評価者テストにおいて検証可能なテストベクタを生成できるように、アルゴリズムの信頼できる参照実装を持っていることが要求されている。

4.5.2 FCS_CKM.1(b)　暗号鍵生成(対称鍵)

（O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION）

下位階層：　なし

依存性：　[~~FCS_CKM.2 暗号鍵配付、または~~
FCS_COP.1(f) 暗号操作(鍵暗号化)]
FCS_CKM_EXT.4 拡張：暗号鍵材料の破棄
FCS_RBG_EXT.1 拡張：暗号操作（乱数ビット生成）

¶203 **FCS_CKM.1.1(b) 詳細化：** TSF は、以下の：**標準なし**に合致する、**FCS_RBG_EXT.1 で指定された乱数ビット生成器**と指定された暗号鍵長［**選択：128 ビット、256 ビット**］**に従って**対称暗号鍵を生成しなければならない。

¶204 *適用上の注釈：*

¶205 *対称鍵は鍵チェインに沿って鍵を生成するために使用されるかもしれない。*

¶ 206 保証アクティビティ：

¶ 207 ***TSS：***

¶ 208 評価者は、FCS_RBG_EXT.1 に記述された機能がどのように起動されるかについて、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。

¶ 209 ***KMD***

¶ 210 TOE がサードパーティの供給元からの乱数生成に依存している場合、KMD は、サードパーティの DRBG 関数をコールする時に使用される関数コールとパラメタが記述されている必要がある。KMD はまた、サードパーティの DRBG にシードとして与えるエントロピー量に関するベンダの前提条件についての簡潔な記述を含む必要があること。評価者は、要求される鍵長が、利用者データの暗号化／復号（FCS_COP.1(d)）に用いられる鍵長及びモードと同一であることを決定するため、FCS_RBG_EXT における RBG 機能の記述または KMD を用いること。

¶ 211 KMD は、附属書 F に記述されている。

4.5.3 FCS_CKM_EXT.4　拡張：暗号鍵材料の破棄

(O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
下位階層：　なし
依存性：　[FCS_CKM.1(a) 暗号鍵生成（非対称鍵）、または
FCS_CKM.1(b) 暗号鍵生成（対称鍵）]、
FCS_CKM.4 暗号鍵破棄

¶ 212 **FCS_CKM_EXT.4.1**　TSF は、**すべての平文の秘密鍵及びプライベート暗号鍵及び暗号クリティカルセキュリティパラメタ**がもはや不要となったとき、**それらを**破棄しなければならない。

¶ 213 ***適用上の注釈：***

¶ 214 *「暗号クリティカルセキュリティパラメタ」は FIPS 140-2 において、「暴露または改変によって、暗号モジュールのセキュリティが危殆化され得るようなセキュリティ関連情報（例、秘密鍵及びプライベート暗号鍵、及びパスワードや PIN 等の認証データ）」として定義されている。*

¶215 *もはや不要となった中間鍵及び鍵材料を含む、鍵については、承認された方法、FCS_CKM.4.1 を用いて破棄されること。鍵の例としては、中間鍵、サブマスクや BEV（訳注：Boarder Encryption Value：境界暗号化値）がある。永続的なストレージに含まれる鍵または鍵材料で、もはや不要となり破棄が求められるような場合があるかもしれない。それらの実装に基づき、ベンダはいつ鍵が不要となるかを説明すること。不要となる鍵材料において複数の状況があり、例えばラップされた鍵はパスワードが変更された時に破棄することができる。しかし、デバイス識別鍵のように、鍵がメモリに残存可能な場合がある。*

¶216 **保証アクティビティ：**

¶217 ***TSS：***

¶218 評価者は、鍵及び鍵材料がもはや不要となり、その時に破棄されると期待されるべきであることの意味についてのハイレベルな記載を TSS が提供することを検証しなければならない。

¶219 ***KMD：***

¶220 評価者は、鍵及び鍵材料の常駐する領域や、いつ鍵及び鍵材料が不要となるかについての記載が鍵管理記述（KMD）に含まれていることを検証しなければならない。

¶221 評価者は、鍵ライフサイクルが KMD に含まれていること、鍵ライフサイクルに鍵材料がどこに存在するか、鍵材料がどのように使われるか、鍵材料が不要となった時にどのように破棄されるかが含まれること、KMD における文書化は破棄に関して FCS_CKM.4 に従っていることを検証しなければならない。

4.5.4 FCS_CKM.4　暗号鍵破棄

(O.COMMS_PROTECTION, O.STORAGE_ENCRYPTION, O.PURGE_DATA)
下位階層：　なし
依存性：　[FCS_CKM.1(a) 暗号鍵生成（非対称鍵）、または FCS_CKM.1(b)暗号鍵生成（対称鍵）]

¶222 **FCS_CKM.4.1 詳細化：** TSF は、以下の［選択：***NIST SP800-88***、***規格なし***］に合致する、指定された暗号鍵破棄方法［選択：

¶ 223 **揮発性メモリについては、破棄は、[選択：*デバイスの電源断*、*[割付：鍵を破棄されたことを保証するその他のメカニズム]*]。**

¶ 224 **不揮発性ストレージについては、破棄は、[選択：*1 回*、*3 回以上*]の [選択：*TSF の RBG（FCS_RBG_EXT.1 で指定されたとおりの）疑似ランダムパターン*、*固定パターン*]で鍵データ格納場所の上書きを行い、その後[選択：*読み出し検証*、*なし*]を行う方法により実行されなければならない。上書きデータの読み出し検証が失敗する場合、処理は再度繰り返されなければならない；**

¶ 225] に従って、暗号鍵を破棄しなければならない。

¶ 226 ***適用上の注釈：***

¶ 227 *もはや不要となった中間鍵及び鍵材料を含む鍵については、承認された方法の一つを用いて揮発性メモリ内で破棄されること。これらの場合において、破棄方法は、本要件において指定される方式の一つに適合すること。本要件は、暗号消去の実行のための方法を呼び出し、鍵情報の破棄のためのよく定義された用語について考慮している。いくつかの解決策がメディアの場所へ書き込みアクセスをサポートしており、これによって鍵及び鍵材料データの直接上書きによって暗号鍵の破棄を可能とする。保存されている場所に直接上書きすることをサポートしていないストレージ技術を用いて保存された鍵材料とワンタイムのプログラマブルメモリが本 SFR を満たすための要件から除外されることに注意すること。*

¶ 228 **保証アクティビティ：**

¶ 229 ***TSS：***

¶ 230 評価者は、鍵や鍵材料がどのように破棄されるかについてのハイレベルな記載を TSS が提供することを検証しなければならない。

¶ 231 ***KMD：***

¶ 232 評価者は、鍵材料、その起源、一時保存の可能性のある場所（例えば、鍵レジスタ、キャッシュメモリ、スタック、FIFO）、及び保存場所のそれぞれのタイプを KMD がリストアップ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。

¶ 233 評価者は、鍵材料のそれぞれのタイプがいつ破棄されるか（例えば、システム電源断時に、ワイプ機能時に、高信頼チャネルの切断時に、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）を KMD が記載

していることを検証しなければならない。

¶ 234 評価者は、鍵及びストレージの各タイプについて、実行される破棄手続きのタイプ（暗号技術的な消去、ゼロで上書き、ランダムパターンで上書き、またはブロック消去）がリストアップされていることも検証しなければならない。材料の保存に使用するためにいくつかの異なるタイプのメモリが保護される場合、評価者は、データが保存されるメモリの観点から消去手続き（例えば、「フラッシュ上に保存された秘密鍵はゼロで一回上書きすることにより破棄し、一方内部の永続的ストレージデバイス上に保存される秘密鍵は 3 回ランダムパターンで上書きによる破棄を行い、それぞれの上書きの前にパターンを変更する」）が TSS に記載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。

¶ 235 評価者は、それぞれのタイプの鍵材料（ソフトウェアによる鍵ストレージ、BEV、パスワード、等）とその起源、保存場所、各鍵の破棄方法を KMD がリストアップされ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。

¶ 236 *テスト：*

¶ 237 各ソフトウェア及びファームウェアによる鍵破棄の状況について、評価者は不揮発性メモリに関して以下のテストを繰り返さなければならない。揮発性メモリ内の鍵は、TOE を電源切断により破棄されるので、揮発性メモリ内の鍵についてのテストはない。以下のテストについて、「鍵」は鍵及び鍵材料を指している。

¶ 238 テスト 1 ： 評価者は、鍵を用いた通常の暗号処理の間、TOE によって内部的に生成されているかもしれない鍵のすべてのコピーを含めて、鍵が破棄されることをテストするため、特別な運用環境（例、仮想マシン）と開発ツール（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。

¶ 239 TOE によって暗号化され永続的に残る鍵の中間コピーを含めて破棄対象の各鍵について、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／ファームウェアにデバッガを取り付ける、または開発者が提供する、特殊なテスト構成においてデバイスのメモリを検査できるような特殊なツールの使用を含めテストを実行するための別の方法を使用する。
2. 破棄対象の TOE 内の鍵の値を記録する。

3. #1 より鍵を用いて通常の暗号化処理を TOE に実行させる。
4. 鍵の消去を TOE に実行させる。
5. TOE に実行を停止させるが終了させない。
6. TOE に TOE の使用する全メモリ領域をバイナリーファイルへダンプさせる。
7. #6 で作成したバイナリーファイルの中身を#2 から既知の鍵の値で検索する。

¶ 240 ステップ#7 で#2 からの鍵のコピーが見つからない場合、テストは成功し、それ以外の場合は失敗となる。

¶ 241 評価者は、暗号化された形で永続的に保存されているものを含め、中間コピーが消去されていることを保証するため、破棄対象のすべての鍵について本テストを実行しなければならない。

4.5.5 FCS_COP.1(a)　暗号操作 (対称鍵暗号化／復号)

(O.COMMS_PROTECTION)
下位階層：　なし
依存性：　[~~FDP_ITC.1 セキュリティ属性なし利用者データのインポート、または~~
FDP_ITC.2 ~~セキュリティ属性を伴う利用者データのインポート、または~~
FCS_CKM.1(b) 暗号鍵生成（対称鍵）]
FCS_CKM_EXT.4　拡張：暗号鍵材料の破棄

¶ 242 **FCS_COP.1.1(a) 詳細化：** TSF は、以下に合致する、特定された暗号アルゴリズム[[**割付：一つまたは複数のモード]での AES 操作**] と **128 ビット及び 256 ビット**の暗号鍵長に従って、**暗号化及び復号**を実行しなければならない：

- **FIPS PUB 197, “Advanced Encryption Standard (AES)”**
- **[選択：*NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D*]**

¶ 243 ***適用上の注釈：***

¶ 244 *割付について、ST 作成者は、FTP_ITC と FTP_TRP のために選択した暗号プロトコルをサポートするための AES が操作するモードを選択するべきである。*

¶ 245 *選択について、ST 作成者は、割付におけるモードについて記載する規格を選択するべきである。*

¶ 246 **保証アクティビティ：**

¶ 247 ***テスト：***

¶ 248 評価者は、上記要件をテストする際のガイドとして、"The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)"（これらの文書は http://csrc.nist.gov/groups/STM/cavp/index.htm から入手可能である）から上記要件において割付したモードに適切なテストを使用しなければならない。これにより、評価者は、テスト中に検証可能なテストベクトルを生成できるような良好なものとして知られたアルゴリズムの参照実装を持っていることを要求される。

4.5.6 FCS_COP.1(b)　暗号操作（署名生成／検証）

(O.UPDATE_VERIFICATION、O.COMMS_PROTECTION)

下位階層：　なし

依存性：　~~[FDP_ITC.1 セキュリティ属性なしの利用者データのインポート、または~~
~~FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~
~~FCS_CKM.1 (b)暗号鍵生成~~]、
FCS_CKM_EXT.4　拡張：暗号鍵材料破棄

¶ 249 **FCS_COP.1.1(b) 詳細化：** TSF は、以下に従って、**暗号署名サービス**を実行しなければならない：[**選択：**

- ***デジタル署名アルゴリズム(DSA) で鍵長 (modulus) が***
  [割付：*2048 ビットまたはそれ以上*] のもの、
- ***RSA デジタル署名アルゴリズム(rDSA) で鍵長 (modulus) が***

[割付：*2048 ビットまたはそれ以上*] のもの、または

- ***楕円曲線デジタル署名アルゴリズム(ECDSA) で鍵長が***
  [割付：*256 ビットまたはそれ以上*] のもの]

¶ 250 であり、以下に合致するものに従って、：**[選択：**

¶ 251 *ケース：デジタル署名アルゴリズム*

- *FIPSPUB 186-4, "Digital Signature Standard"*

¶ 252 *ケース：RSA デジタル署名アルゴリズム*

- *FIPS PUB 186-4, "Digital Signature Standard"*

¶ 253 *ケース：楕円曲線デジタル署名アルゴリズム*

- *FIPS PUB 186-4, 「Digital Signature Standard」*
- *TSF は、「NIST 曲線」P-256、P-384 及び*[選択：*P-521、その他の曲線なし*] *(FIPS PUB 186-4,「Digital Signature Standard」で定義されるとおり)実装しなければならない。*

¶ 254]。

¶ 255 ***適用上の注釈：***

¶ 256 *ST 作成者は、デジタル署名を実行するために実装されたアルゴリズムを選択するべきである；一つ以上のアルゴリズムが利用可能な場合、その機能を指定するために本要件(及び関連する FCS_CKM.1 要件)を繰り返しするべきである。選択したアルゴリズムについて、ST 作成者はそのアルゴリズムに実装されたパラメタを指定するための適切な割付／選択を行うべきである。*

¶ 257 *楕円曲線ベースのスキームについて、鍵長はベースポイントの位数の log2 を参照する。*

¶ 258 **保証アクティビティ：**

¶ 259 ***テスト：***

¶ 260 評価者は、上記の要件をテストする際にガイドとして、「The Digital Signature Algorithm Validation System」 (DSA2VS)、「The Elliptic Curve Digital Signature Algorithm Validation System」(ECDSA2VS)、及び「The RSA Validation System」RSA2VS の署名検証部分を使用しなければなら

ない。使用する検証システムは、ST において識別された適合規格 (FIPS PUB 186-4) に適合しなければならない。これは、評価者がテストにおいて検証可能なテストベクタの生成が可能な、既知の良いアルゴリズム実装を持っていることを要求している。

4.5.7　FCS_RBG_EXT.1　拡張：暗号操作（乱数ビット生成）

(O.STORAGE_ENCRYPTION 及び O.COMMS_PROTECTION)
下位階層：　　なし
依存性：　　なし

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

¶ 262 **FCS_RBG_EXT.1.2** 決定論的 RBG は、[選択：[割付：*ソフトウェアベースのノイズ源の数*]のソフトウェアによるノイズ源、[割付：*ハードウェアベースのノイズ源の数*]のハードウェアによるノイズ源]から、ISO/IEC 18031:2011 表 C.1 「Security strength table for hash functions」に従って、いくつか生成する鍵とハッシュの中で最も大きいセキュリティ強度のものと少なくとも等しいような、[選択：128 ビット、256 ビット]のエントロピーを最小限持つようにエントロピーを蓄積する少なくとも一つのエントロピー源によってシード値を供給されなければならない。

¶ 263 ***適用上の注釈：***

¶ 264 *ISO/IEC 18031:2011 は、乱数を生成する異なる方法を含んでいる；それぞれが同様に基礎となる暗号プリミティブに依存している(ハッシュ関数／暗号)。ST 作成者は、使用する機能を選択し、要件で使用される特定の基礎となる暗号プリミティブを含めること。識別されたハッシュ関数（SHA-1、SHA-224、SHA-256、SHA-384、SHA-512）のいずれかが Hash_DRBG または HMAC_DRBG 用として許可されているが、CTR_DRBG 用の AES ベースの 実装のみが許可される。ISO/IEC 18031:2011 の表 C.2 が、セキュリティ強度の識別、AES-128 及び 256 ブロック暗号用エントロピー及びシード長の要件を提供している。*

¶ 265 *ISO/IEC 18031:2011 にて CTR_DRBG は、導出関数を使用することを要求しているのに対して NIST SP 800-90A では要求していない。いずれのモデ*

ルも受け入れ可能である。FCS_RBG_EXT.1.1 での最初の選択では、ST 作成者は、適合する規格を選択すること。

¶ 266 *FCS_RBG_EXT.1.2 での最初の選択は、採用したそれぞれのノイズ源のタイプにいくつのエントロピー源を用いたかを ST 作成者は記入する。ハードウェアによるノイズ源とソフトウェアによるノイズ源の組み合わせが使用可能であることに注意するべきである。*

¶ 267 *エントロピー源が RBG の一部であると考えられ、TOE に RBG が含まれる場合開発者は附属書 E に概説するエントロピー記述を提供する必要があることに注意するべきである。本エレメントの評価アクティビティで要求される、その文書 *及びテスト* は、FCS_RBG__EXT.1.2 で示される各ノイズ源を必ず網羅すること。*

¶ 268 **保証アクティビティ：**

¶ 269 ***TSS：***

¶ 270 第三者から提供されるあらゆる RBG サービスについて、評価者は、提供元から受け取る予測されたエントロピー量についてのステートメント、及び第三者の提供元からの出力処理に関する十分な記述が TSS に含まれていることを保証しなければならない。評価者は、本ステートメントが DRBG のシード供給について FCS_RBG_EXT.1.2 にて行われた選択と整合性が取れていることを検証しなければならない。ST が複数の DRBG を指定している場合、評価者は各 DRBG メカニズムの使用法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。

¶ 271 ***エントロピー記述：***

¶ 272 評価者は、エントロピー記述が本 PP の附属書 E に記述されるとおり必要な情報のすべてを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、乱数ビット列を生成する際に十分なエントロピーを TOE が提供していることを確認し保証する。

¶ 273 ***操作ガイダンス：***

¶ 274 評価者は、AGD ガイダンスが管理者に対して選択した 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の指示を与えていることを検証しなければならない、必要な場合。

¶ 275 ***テスト：***

¶ 276 評価者は、RBG 実装について 15 回の試行を実行しなければならない。

RBG が TOE によって設定可能な場合、評価者は、各設定について 15 回の試行を実行しなければならない。評価者は、RBG の設定に関する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。

¶ 277 RBG が予測困難性を有効にしている場合、各試行は(1)DRBG をインスタンス化し、(2)乱数ビットの最初のブロックを生成し、(3)乱数ビットの第 2 ブロックを生成し、(4)非インスタンス化する、という手順からなる。評価者は、乱数ビットの第 2 ブロックが期待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)である。次の 3 つは、インスタンス化操作のためのエントロピー入力、ノンス、及び Personalization String である。次の 2 つは、生成のための最初の呼出しのための Additional Input とエントロピー入力である。最後の 2 つは、生成のための 2 番目の呼出しのための Additional Input 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」とは出力ブロック長（NIST SP800-90A に定義されるとおり）と等しい数の戻り値ビットを持つ乱数ビットを生成することを意味する。

¶ 278 RBG が予測困難性を持たない場合、各試行は(1)DRBG をインスタンス化し、(2)乱数ビットの最初のブロックを生成し、(3)再度シードを供給し、(4)乱数ビットの第 2 ブロックを生成し、(5)非インスタンス化する、という手順からなる。評価者は、乱数ビットの第 2 ブロックが期待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)である。次の 3 つは、インスタンス化操作のためのエントロピー入力、ノンス、及び Personalization String である。5 番目の値は、生成のための最初の呼出しのための Additional Input である。6 番目と 7 番目は、再度シードを供給するための呼出しへの Additional Input とエントロピー入力である。最後の値は、生成のための 2 番目の呼出しのための Additional Input である。

¶ 279 以下のパラグラフには、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、より多くの情報が含まれている。

¶ 280 エントロピー入力：エントロピー入力値の長さは、シード長と等しくなければならない。

¶ 281 ノンス：ノンスがサポートされている場合（導出関数を用いない CTR_DRBG は、ノンスを使用しない）、ノンスのビット長はシード長の半分となる。

¶ 282 Personalization string：Personalization String の長さは、シード長以下でなければならない。実装において一つの Personalization String 長のみがサポートされている場合には、それと同じ長さが両方の値として用いることができる。複数の string 長がサポートされている場合、評価者は２つの異なる長さの Personalization String を使用しなければならない。実装において Personalization String を使用しない場合、値を供給する必要はない。

¶ 283 Additional input：Additional Input のビット長は、Personalization String 長と同一のデフォルト値と制約条件を持つ。

4.6 クラス FDP：利用者データ保護

¶ 284 *適用上の注釈：*

¶ 285 *利用者データアクセス制御 SFP は、表２、表３、FDP_ACC.1、FDP_ACF.1、FMT_MSA.1、及び FMT_MSA.3 からなる。*

4.6.1 FDP_ACC.1　サブセットアクセス制御

(O.ACCESS_CONTROL 及び O.USER_AUTHORIZATION)
下位階層：　なし
依存性：　FDP_ACF.1 セキュリティ属性によるアクセス制御

¶ 286 **FDP_ACC.1.1　詳細化：**TSF は、**サブジェクト、オブジェクト、及び表 2 及び表 3 で特定されるサブジェクトとオブジェクトの間の操作に対して、利用者データアクセス制御 SFP を**実施しなければならない。

¶ 287 **保証アクティビティ：**

¶ 288 FDP_ACF.1 に関する保証アクティビティによって対応されている。

4.6.2 FDP_ACF.1　セキュリティ属性によるアクセス制御

(O.ACCESS_CONTROL 及び O.USER_AUTHORIZATION)
下位階層：　なし
依存性：　FDP_ACC.1 サブセットアクセス制御
　　FMT_MSA.3 静的属性初期化

¶ 289 **FDP_ACF.1.1　詳細化：**TSF は、以下に基づいて、オブジェクトに対して、**利**

用者データアクセス制御 SFP を実施しなければならない：**サブジェクト、オブジェクト、及び表 2 及び表 3 で特定される属性。**

¶ 290 **FDP_ACF.1.2　詳細化：**TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない：***制御されたサブジェクトと制御されたオブジェクト間で、表 2 及び表 3 で特定された制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則。***

¶ 291 **FDP_ACF.1.3　詳細化：**TSF は、次の追加規則、［割付：*セキュリティ属性に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に許可する、****利用者データアクセス制御 SFP と矛盾しないような****規則*］に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

¶ 292 **FDP_ACF.1.4　詳細化：**TSF は、以下の追加規則、［割付：*セキュリティ属性に基づいて、オブジェクトへのサブジェクトからのアクセスを明示的に拒否するような、****利用者データアクセス制御 SFP と矛盾しないような****規則*］に基づいて、サブジェクトからのオブジェクトへのアクセスを明示的に拒否しなければならない。

表 2　D.USER.DOC アクセス制御 SFP

		"作成"	"閲覧"	"改変"	"削除"
プリント	***操作:***	***プリントされる文書を投入***	***画像を閲覧またはプリント結果を出力***	***保存された文書を改変***	***保存された文書を削除***
	ジョブ所有者	(注 1)			
	U.ADMIN				
	U.NORMAL		拒否	拒否	拒否
	未認証	(条件 1)	拒否	拒否	拒否
スキャン	***操作:***	***スキャンする文書を投入***	***スキャンされた画像を閲覧***	***保存された画像を改変***	***保存された画像を削除***
	ジョブ所有者	(注 2)			
	U.ADMIN				
	U.NORMAL		拒否	拒否	拒否
	未認証	拒否	拒否	拒否	拒否

コピー	*操作:*	*コピーする文書を投入*	*スキャンされた画像を閲覧または印刷されたコピーを出力*	*保存された画像を改変*	*保存された画像を削除*
	ジョブ所有者	(注 2)			
	U.ADMIN				
	U.NORMAL		拒否	拒否	拒否
	未認証	拒否	拒否	拒否	拒否
ファクス送信	*操作:*	*ファクス送信文書を投入*	*スキャンされた画像を閲覧*	*保存された画像を改変*	*保存された画像を削除*
	ジョブ所有者	(注 2)			
	U.ADMIN				
	U.NORMAL		拒否	拒否	拒否
	未認証	拒否	拒否	拒否	拒否
ファクス受信	*操作:*	*ファクス受信と保存*	*ファクス画像を閲覧または印刷されたファクスを出力*	*受信ファクス画像を改変*	*受信ファクス画像を削除*
	ファクス所有者	(注 3)			
	U.ADMIN	(注 4)			
	U.NORMAL	(注 4)	拒否	拒否	拒否
	未認証		拒否	拒否	拒否
保存／取り出し	*操作:*	*文書を保存*	*保存文書を取り出す*	*保存された文書を改変*	*保存された文書を削除*
	ジョブ所有者	(注 1)			
	U.ADMIN				
	U.NORMAL		拒否	拒否	拒否
	未認証	(条件 1)	拒否	拒否	拒否

表 3　D.USER.JOB アクセス制御 SFP

		"作成"	"閲覧"	"改変"	"削除"
プリント	*操作:*	*プリントジョブを作成*	*プリントキュー／ログを閲覧*	*プリントジョブを改変*	*プリントジョブを取消し*
	ジョブ所有者	(注 1)			
	U.ADMIN				

	U.NORMAL			拒否	拒否
	未認証			拒否	拒否
スキャン	*操作:*	*スキャンジョブを作成*	*スキャン状態／ログを閲覧*	*スキャンジョブを改変*	*スキャンジョブを取消し*
	ジョブ所有者	(注 2)			
	U.ADMIN				
	U.NORMAL			拒否	拒否
	未認証	拒否		拒否	拒否
コピー	*操作:*	*コピージョブを作成*	*コピー状態／ログを閲覧*	*コピージョブを改変*	*コピージョブを取消し*
	ジョブ所有者	(注 2)			
	U.ADMIN				
	U.NORMAL			拒否	拒否
	未認証	拒否		拒否	拒否
ファクス送信	*操作:*	*ファクス送信ジョブを作成*	*ファクスジョブキュー／ログを閲覧*	*ファクス送信ジョブを改変*	*ファクス送信ジョブを取消し*
	ジョブ所有者	(注 2)			
	U.ADMIN				
	U.NORMAL			拒否	拒否
	未認証	拒否		拒否	拒否
ファクス受信	*操作:*	*ファクス受信ジョブを作成*	*ファクス受信状態／ログを閲覧*	*ファクス受信ジョブを改変*	*ファクス受信ジョブを取消し*
	Fax owner	(注 3)			
	U.ADMIN	(注 4)			
	U.NORMAL	(注 4)		拒否	拒否
	未認証			拒否	拒否
保存／取り出し	*操作:*	*保存／取り出しジョブを作成*	*保存／取り出しログを閲覧*	*保存／取り出しジョブを改変*	*保存／取り出しジョブを取消し*
	ジョブ所有者	(注 2)			
	U.ADMIN				
	U.NORMAL			拒否	拒否
	未認証	(条件 1)		拒否	拒否

¶ 293 *適用上の注釈：*

¶ 294 *一般に、ST 作成者は、提供された本 SFP に対して、より限定的な変更であれば、修正することができる。例として、ST 作成者は：TOE に存在しない文書処理機能に関連する規則を削除する、アクセスをさらに拒否するように規則を追加または修正する、またはいくつかのデータ（例えば、D.USER.JOB.PROT 及び D.USER.JOB.CONF）に対するアクセスをさらに制限するように利用者データを細分化することができる。表中の空欄は操作が許可されてもよいことを示しているが、許可されることは必須ではない。*

¶ 295 *特に、表 2 及び表 3 を参照しつつ：*

- *「拒否」と記述されたセルは、利用者（列）が操作（行）を実行することが許可されてはならないことを示している。ST 作成者はこれを上書きすることはできない。*
- *空欄となっているセルは、利用者が操作を実行することが許可されてもよいことを示している。しかし、ST 作成者は条件、または制限を追加したり、または全面的にパーミッションを拒否してもよい。*
- *「条件」と記述されたセルは、以下に指定される条件を満たしていることによって利用者が操作を実行することが許可されることが可能となる。空欄のセルのように、ST 作成者は、より多くの制限を付け加えることができる。*

¶ 296 ***条件 1：****許可されない利用者によって投入されたジョブは、TOE がジョブ所有者を特定するために使用できるクレデンシャルを含まなければならない。*

¶ 297 *表 2 及び表 3 で参照される以下の注についても参照されたい：*

¶ 298 ***注 1：****ジョブ所有者は、クレデンシャルによって特定されるか、またはプリントや保存のジョブを送信するプロセスの一部として利用者に割り付けられる。*

¶ 299 ***注 2：****ジョブ所有者は、スキャン、コピー、ファクス送信または取り出しジョブを起動するプロセスの一部として許可された利用者に割り付けられる。*

¶ 300 ***注 3：****受信されたファクスのジョブ所有者は、デフォルトまたは設定で割り付けられる。最低限、受信されたファクスの所有者は特定の利用者または U.ADMIN 役割に対して割り付けられる。*

¶ 301 ***注 4：PSTN ファクスは TOE の外部から受信され、それらは TOE の利用者により起動されない。***

¶ 302 **保証アクティビティ：**

¶ 303 ***TSS：***

¶ 304 評価者は、**表 2 及び表 3** に定義された SFP を実現する機能について TSS に記述され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。

¶ 305 ***操作ガイダンス：***

¶ 306 評価者は、操作ガイダンスに**表 2 及び表 3** に定義された SFP を実現する操作について、TSS における記述と一貫するように記述されていることを保証するためチェックする。

¶ 307 ***テスト：***

¶ 308 評価者は、**表 2 及び表 3** に定義された SFP を実現する機能をすべてのタイプのインタフェースと共に確認するためのテストを実行しなければならない（例えば、操作パネル、ウェブインタフェース）。

¶ 309 評価者テストは、次の観点を含めるべきである：

- **表 2 及び表 3** に定義されたすべてのオブジェクトタイプの代表的な一式の操作（操作が許可されるか、または拒否されるかのいずれかのケースを含む）
- アクセス制御で使用されるセキュリティ属性の設定の代表的な組み合わせ

4.7 クラス FIA：識別と認証

4.7.1 FIA_AFL.1 認証失敗時の取り扱い

(O.USER_I&A)
下位階層：　なし
依存性：　FIA_UAU.1 認証のタイミング

¶ 310 **FIA_AFL.1.1**　TSF は、［割付：*認証事象のリスト*］に関して、［選択：［割付：*正の整数値*］、［割付：*許容可能な値の範囲*］内における管理者設定可

能な正の整数値］回の不成功認証試行が生じたときを検出しなければならない。

¶ 311 **FIA_AFL.1.2**　不成功の認証試行が定義した回数 ［選択：に達する、を上回った］とき、TSF は、［割付：*アクションのリスト*］をしなければならない。

¶ 312 ***適用上の注釈：***

¶ 313 *本 SFR は、内部での識別認証のみに適用される。*

¶ 314 **保証アクティビティ：**

¶ 315 ***TSS：***

¶ 316 評価者は、認証失敗時のアクションの（認証事象の種別、不成功の認証試行の回数、実行されるアクション）に関して、SFR の定義と一貫した記述が TSS に含ま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。

¶ 317 ***操作ガイダンス：***

¶ 318 評価者は、SFR に定義された認証失敗時のアクションを実行するための設定方法が管理者ガイダンスに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。

¶ 319 ***テスト：***

¶ 320 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：

1. 評価者は、不成功の認証試行回数が SFR に定義された状態に達した時、SFR に定義されたアクションに従ったふるまいにより、それ以降の認証試行が成功しないことを保証するためにチェックしなければならない。
2. 評価者は、認証試行を再度有効化するための条件が SFR に定義されており、かつその条件が満たされている時に、認証試行が成功することを保証するためにチェックしなければならない。
3. 評価者は、複数の内部認証方式（例えば、パスワード認証、バイオメトリック認証）がある時、対象となるすべての認証方式について上記のテスト１と２を実行しなければならない。
4. 評価者は、認証試行を実装している複数のインタフェース（例えば、操作パネル、ウェブインタフェース）があるとき、それらのインタ

フェースについて上記テスト１と２を実行しなければならない。

4.7.2　FIA_ATD.1　利用者属性定義

(O.USER_AUTHORIZATION)
下位階層：　　なし
依存性：　　なし

¶321 **FIA_ATD.1.1**　TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない：[割付：*セキュリティ属性のリスト*]。

¶322 ***適用上の注釈：***

¶323 *セキュリティ属性のリストはサポートされる認証方式のそれぞれについてのすべての属性の結合であるべきである。*

¶324 **保証アクティビティ：**

¶325 ***TSS：***

¶326 評価者は、TOE が SFR を実装するために使用する利用者セキュリティ属性についての記述が TSS に含まれており、SFR の定義と一貫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。

4.7.3　FIA_PMG_EXT.1　拡張：パスワード管理

(O.USER_I&A)
下位階層：　　なし
依存性：　　なし

¶327 **FIA_PMG_EXT.1.1**　TSF は、利用者パスワードに対して、次のパスワード管理機能を提供しなければならない：

- パスワードは、アルファベットの大文字と小文字、数字、及び次の特殊文字：[選択：“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [割付：その他の文字]]の組み合わせから作成可能でなければならない；
- 最少パスワード長は、**管理者**によって設定可能でなければならない、かつ 15 文字以上のパスワードを**要求する能力を持って**いなければならない；

¶328 ***適用上の注釈：***

¶329 *本 SFR は、パスワードベースの単一要素による内部認証にのみ適用される。*

¶330 **保証アクティビティ：**

¶331 ***操作ガイダンス：***

¶332 評価者は、操作ガイダンスがパスワードの作成に関してセキュリティ管理者に説明を提供していること及び最少パスワード長の設定についての指示を提供していることを決定するために、操作ガイダンスを検査しなければならない。

¶333 ***テスト：***

¶334 評価者は、次のテストについても実行しなければならない。

¶335 評価者は、要件を満たすパスワード、または要件を満たさないパスワードのいずれかを何らかの方法で複数作成しなければならない。それぞれのパスワードについて、評価者は、TOE がパスワードをサポートしていることを検証しなければならない。評価者がすべての作成可能なパスワードをテストすることは要求されていない（または実現可能でない）が、評価者は、要件にリスト化されているすべての文字、規則の特性、及び最小のパスワード長がサポートされることを保証しなければならない、またテストのために選択された文字列が適切であることを説明しなければならない。

4.7.4 FIA_UAU.1　認証のタイミング

(O.USER_I&A)
下位階層：　なし
依存性：　FIA_UID.1 識別のタイミング

¶336 **FIA_UAU.1.1　詳細化：**TSF は、利用者が認証される前に利用者を代行して実行される[割付：***利用者データアクセス制御 SFP と矛盾せず、かつ D.TSF.CONF へのアクセスを提供せず、かつ任意の TSF データを変更しない*** *TSF 仲介アクションのリスト*]を許可しなければならない。

¶337 **FIA_UAU.1.2**　TSF は、その利用者を代行する他のあらゆる TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

¶338 ***適用上の注釈：***

¶ 339 *利用者認証は、TOE による内部で実行されるか、または外部 IT エンティティによる外部で実行されることがある。*

¶ 340 **保証アクティビティ：**

¶ 341 ***TSS：***

¶ 342 評価者は、TOE が提供するすべての識別認証メカニズム（例えば、内部認証や外部サーバによる認証）について TSS に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。

¶ 343 評価者は、識別と認証を実行するためのすべてのインタフェース（例えば、操作パネルまたはウェブインタフェースからの識別と認証）が TSS に識別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。

¶ 344 評価者は、TOE が外部認証サーバとの間で識別と認証を交換する時、識別と認証を実行する際に利用されるプロトコル（例えば、LDAP、Kerberos、OCSP）が TSS に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。

¶ 345 評価者は、識別と認証を実行する前に許可されるアクションについて TSS に含まれており、それが SFR の定義と一貫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。

¶ 346 ***操作ガイダンス：***

¶ 347 評価者は、TOE が提供する識別と認証の方式（例えば、外部認証、内部認証）についての記述がインタフェース（例えば、操作パネルまたはウェブインタフェースからの識別と認証）と同様に管理者ガイダンスに含まれており、それが ST（TSS）と一貫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。

¶ 348 ***テスト：***

¶ 349 評価者は、次のテストについても実行しなければならない：

1. 評価者は、許可されたデータを用いる時、識別と認証が成功し、TOE へのアクセスが可能となることを保証するためチェックしなければならない。
2. 評価者は、許可されないデータを用いる時、識別と認証が失敗し、TOE へのアクセスがそれ以後できなくなることを保証するためにチェックしなければならない。

¶ 350 評価者は、TOE がインタフェース（例、操作パネルから識別と認証、またはウェブインタフェース経由）と同様に TOE が提供する認証方式のそれぞれ（例、外部認証、内部認証）について上記のテストを実行しなければならない。

4.7.5 FIA_UAU.7 保護された認証フィードバック

(O.USER_I&A)
下位階層： なし
依存性： FIA_UAU.1 認証のタイミング

¶ 351 **FIA_UAU.7.1** TSF は、認証を行っている間、［割付：*フィードバックのリスト*］だけを利用者に提供しなければならない。

¶ 352 ***適用上の注釈：***

¶ 353 *FIA_UAU.7 は、TOE と対話する利用者の認証プロセスのみに適用される。*

¶ 354 **保証アクティビティ：**

¶ 355 ***TSS：***

¶ 356 評価者は、認証の処理中に利用者に対する認証情報のフィードバックについての記述が TSS に含まれており、SFR の定義と一貫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。

¶ 357 ***テスト：***

¶ 358 評価者は、次のテストについても実行しなければならない：

1. 評価者は、SFR で定義された情報のみが識別と認証の試行によるフィードバックのために提供されることを保証するために、チェックしなければならない。
2. 評価者は、TOE が提供するすべてのインタフェース（例えば、操作パネル、ウェブインタフェース経由の識別と認証）について上記のテスト 1 を実行しなければならない。

4.7.6 FIA_UID.1 識別のタイミング

(O.USER_I&A 及び O.ADMIN_ROLES)
下位階層： なし
依存性： なし

¶359 **FIA_UID.1.1　詳細化：** TSF は、利用者が識別される前に利用者を代行して実行される[割付：***利用者データアクセス制御 SFP と矛盾せず、かつ D.TSF.CONF へのアクセスを提供せず、かつ任意の TSF データを変更しない*** *TSF 仲介アクションのリスト*]を許可しなければならない。

¶360 **FIA_UID.1.2**　TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

¶361 ***適用上の注釈：***

¶362 *利用者の識別は TOE により内部で実行してもよいし、または外部 IT エンティティにより外部で実行してもよい。*

¶363 **保証アクティビティ：**

¶364 FIA_UAU.1 に関する保証アクティビティによって対応されている。

4.7.7　FIA_USB.1　利用者−サブジェクト結合

(O.USER_I&A)
下位階層：　なし
依存性：　FIA_ATD.1 利用者属性定義

¶365 **FIA_USB.1.1**　TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。：[割付：*利用者セキュリティ属性のリスト*]。

¶366 **FIA_USB.1.2**　TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない：[割付：*属性の最初の関連付けの規則*]。

¶367 **FIA_USB.1.3**　TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない：[割付：*属性の変更の規則*]。

¶368 **保証アクティビティ：**

¶369 ***TSS：***

¶370 評価者は、識別と認証に成功した利用者にセキュリティ属性を関連付ける規則についての記述が TSS に含まれており、SFR の定義と一貫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。

¶371 ***テスト：***

¶372 評価者は、次のテストについても実行しなければならない：

¶373 評価者は、TOE がサポートする役割ごと（例えば、利用者や管理者）に、SFR で定義されたセキュリティ属性が識別と認証を成功した利用者と関連付けされること（FDP_ACF のテストにおいて保証される）を保証するためにチェックしなければならない。

4.8 クラス FMT：セキュリティ管理

4.8.1 FMT_MOF.1 セキュリティ機能のふるまいの管理

(O.ADMIN_ROLES)
下位階層： なし.
依存性： FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

¶374 **FMT_MOF.1.1詳細化：** TSF は、機能[割付：機能のリスト]の[選択：*ふるまいを決定する*、*無効化する*、*有効化する*、*ふるまいを改変する*]能力を **U.ADMIN** に制限しなければならない。

¶375 **保証アクティビティ：**

¶376 ***TSS：***

¶377 評価者は、TOE が提供する管理機能の記述が機能を管理するために許可された利用者役割と共に TSS に含まれており、SFR の定義と一貫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。

¶378 評価者は、管理機能を操作するためのインタフェースを TSS が識別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。

¶379 ***操作ガイダンス：***

¶380 評価者は、SFR で定義された規定の役割の利用者が管理機能を操作するための操作方法について、管理者ガイダンスに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。

¶381 ***テスト：***

¶382 評価者は、次のテストについても実行しなければならない：

1. 評価者は、SFR で定義された規定の役割の利用者が管理者ガイダンスで指定された操作方法に従って管理機能を操作できることを保証するためにチェックしなければならない。

2. 評価者は、操作結果が適切に反映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。

3. 評価者は、U.NORMAL が管理機能を操作することが許可されていないことを保証するためにチェックしなければならない。

4.8.2 FMT_MSA.1　セキュリティ属性の管理

(O.ACCESS_CONTROL 及び O.USER_AUTHORIZATION)
下位階層：　なし.
依存性：　[FDP_ACC.1 サブセットアクセス制御、~~または FDP_IFC.1 サブセット情報フロー制御~~]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

¶ 383 **FMT_MSA.1.1　詳細化：**TSF は、セキュリティ属性[割付：*セキュリティ属性のリスト*]に対し［選択：*デフォルト値変更、問合せ、改変、削除、［割付：その他の操作］*］をする能力を[割付：*許可された識別された役割*]に制限するため、**利用者データアクセス制御 SFP** を実施しなければならない。

¶ 384 **保証アクティビティ：**

¶ 385 ***TSS：***

¶ 386 評価者は、セキュリティ属性への可能な操作とそれらのセキュリティ属性へ規定の役割についての記述が TSS に含まれており、SFR の定義と一貫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。

¶ 387 ***操作ガイダンス：***

¶ 388 評価者は、セキュリティ属性への可能な操作とそれらのセキュリティ属性へ与えられた役割についての記述が管理者ガイダンスに含まれており、SFR の定義と一貫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。

¶ 389 評価者は、変更されたセキュリティ属性のタイミングについて管理者ガイダンスに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。

¶ 390 ***テスト：***

¶ 391 評価者は、次のテストについても実行しなければならない：

1. 評価者は、SFR に定義された規定の役割の利用者が管理者ガイダンスにおいて指定された操作方法に従って、セキュリティ属性に対する操作を実行できることを保証するため、チェックしなければならない。
2. 評価者は、操作の結果が管理者ガイダンスにおいて指定されたとおり適切に反映されることを保証するため、チェックしなければならない。
3. 評価者は、SFR に定義された許可された役割の一部ではない利用者がセキュリティ属性に対する操作の実行が許可されないことを保証するため、チェックしなければならない。

4.8.3 FMT_MSA.3　静的属性初期化

（O.ACCESS_CONTROL 及び O.USER_AUTHORIZATION）

下位階層：　なし.

依存性：　FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

¶392 **FMT_MSA.3.1**　**詳細化：**TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択、以下から一つ選択：*制約的*、*許可的*、*[割付：その他の特性]*] のデフォルト値を与える**利用者データアクセス制御 SFP** を実施しなければならない。

¶393 **FMT_MSA.3.2**　**詳細化：**TSF は、オブジェクトや情報が生成されるとき、[**選択：*U.ADMIN, 役割なし***]がデフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

¶394 ***適用上の注釈：***

¶395 *FMT_MSA.3.2 は、デフォルト値が上書きすることできるセキュリティ属性へのみ適用される。*

¶396 **保証アクティビティ：**

¶397 ***TSS：***

¶398 評価者は、SFR に定義されたデフォルト値の特性を持つセキュリティ属性を生成するメカニズムについて TSS に記述され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。

¶ 399 *テスト：*

¶ 400 U.ADMIN が選択されている場合、本 SFR のテストは、FDP_ACF.1 のテストにおいて実行される。

4.8.4 FMT_MTD.1　TSF データの管理

(O.ACCESS CONTROL)
下位階層：　なし
依存性：　FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

¶ 401 **FMT_MTD.1.1詳細化：**TSF は、**特定された TSF データ上の特定された操作を実行する**能力を**表 4 で指定された役割に**制限しなければならない。

表 4 TSF データの管理

データ	操作	許可された役割
[割付：U.NORMAL が所有する TSF データのリスト 、または U.NORMAL が所有する文書またはジョブに関連付けされた TSF データのリスト]	[選択：デフォルトの変更、問合せ、改変、削除、消去、[割付：その他の操作]]	U.ADMIN、所有する U.NORMAL
[割付： U.NORMAL が所有しない TSF データのリスト]	[選択：デフォルトの変更、問合せ、改変、削除、消去、[割付：その他の操作]]	U.ADMIN
[割付：ソフトウェア、ファームウェア、及び関連する設定データのリス	[選択：デフォルトの変更、問合せ、改変、削除、消去、[割付：その	U.ADMIN

ト]	他の操作]]

¶ 402 **保証アクティビティ：**

¶ 403 ***操作ガイダンス：***

¶ 404 評価者は、SFR と一貫した管理操作と許可された役割について、管理者ガイダンスに記述され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。

¶ 405 評価者は、役割の割付がどのように管理されるかについて、管理者ガイダンスに記述され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。

¶ 406 評価者は、セキュリティ属性がどのように割付、管理されるかについて、管理者ガイダンスに記述され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。

¶ 407 評価者は、セキュリティ関連の規則（例えば、アクセス制御規則、タイムアウト、連続するログオン失敗の回数）がどのように設定されるかについて、管理者ガイダンスに記述され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。

¶ 408 ***テスト：***

¶ 409 評価者は、次のテストについても実行しなければならない：

1. 評価者は、SFR に定義された規定の役割の利用者が、管理者ガイダンスにおいて指定された操作方法に従って、TSF データに対する操作を実行できることを保証するため、チェックしなければならない。
2. 評価者は、操作の結果が管理者ガイダンスにおいて指定されたとおり適切に反映されることを保証するため、チェックしなければならない。
3. 評価者は、SFR に定義された規定の役割の利用者以外の利用者が、TSF データに対する操作を実行できないことを保証するため、チェックしなければならない。

4.8.5　**FMT_SMF.1　管理機能の特定**

(O.USER_AUTHORIZATION、O.ACCESS_CONTROL 及び O.ADMIN_ROLES)

下位階層：　なし

依存性：　なし

¶ 410　**FMT_SMF.1.1**　**詳細化：**TSF は、以下の管理機能：［割付： *TSF により提供される管理機能のリスト*］を実行可能でなければならない。

¶ 411　***適用上の注釈：***

¶ 412　*「TSF により提供される管理機能」に関して、ST 作成者は、本プロテクションプロファイルのセキュリティ対策方針をサポートする管理機能を検討するべきである。*

¶ 413　*管理機能は、FMT_MOF.1、FMT_MTD.1、FMT_MSA.1 において、許可され識別された役割に制限されるべきである。*

¶ 414　*ST 作成者は、明示的な管理性がなくてもセキュリティ対策方針が満たされるようなケースを識別することができる。*

¶ 415　*例えば、以下の管理機能がセキュリティ対策方針により分類されている：*

¶ 416　*O.USER_AUTHORIZATION、 O.USER_I&A、O.ADMIN_ROLES、O.ACCESS_CONTROL について：*

- *利用者管理（例、ローカル利用者を追加／変更／削除する）*
- *役割管理（例、利用者との役割の関係を割付／解除する）*
- *識別と認証を設定する（例ローカル及び外部の I&A を選択する）*
- *権限付与とアクセス制御を設定する（例、TOE 資源のアクセス制御リスト）*
- *外部 IT エンティティとの通信を設定する*

¶ 417　*O.UPDATE_VERIFICATION について：*

- *ソフトウェア更新を設定する*

¶ 418　*O.COMMS_PROTECTION について：*

- *ネットワーク通信を設定する*
- *システムまたはネットワークタイムソースを設定する*

¶ 419 *O.AUDIT について：*

- *監査サーバへのデータ送信を設定する*
- *システムまたはネットワークタイムソースを設定する*
- *内部監査ログ保存を設定する*

¶ 420 *O.STORAGE_ENCRYPTION、O.KEY_MATERIAL について：*

- *現地交換可能な不揮発性ストレージデバイスの暗号化とその起動を設定する*

¶ 421 *(オプション) O.IMAGE_OVERWRITE、O.PURGEDATA について：*

- *画像上書き機能と／またはその起動を設定する*
- *データ完全消去機能と／またはその起動を設定する*

¶ 422 **保証アクティビティ：**

¶ 423 ***TSS：***

¶ 424 評価者は、管理機能が SFR における割付と一貫し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。

¶ 425 ***操作ガイダンス：***

¶ 426 評価者は、管理機能が SFR における割付と一貫していること、及びそれらの操作が記述されていることを保証するためにガイダンス文書をチェックしなければならない。

4.8.6 FMT_SMR.1　セキュリティの役割

(O.ACCESS_CONTROL, O.USER_AUTHORIZATION, 及び O.ADMIN_ROLES)

下位階層：　なし

依存性：　FIA_UID.1 識別のタイミング

¶ 427 **FMT_SMR.1.1**　**詳細化：**TSF は、役割 **U.ADMIN、U.NORMAL** を維持になければならない。

¶ 428 **FMT_SMR.1.2**　TSF は、利用者を役割に関連付けできなければならない。

¶ 429 **保証アクティビティ：**

¶ 430 ***TSS：***

¶ 431 評価者は、TOE が維持するセキュリティ関連の役割の記述が TSS に含まれており、SFR の定義と一貫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。

¶ 432 *テスト：*

¶ 433 本 SFR のテストについては、FMT_MOF.1、FMT_MSA.1、及び FMT_MTD.1 のテストにおいて実行される。

4.9 クラス FPR：プライバシー

¶ 434 クラス FPR の要件はなし。

4.10 クラス FPT：TSF の保護

4.10.1 FPT_SKP_EXT.1　拡張：TSF データの保護

(O.COMMS_PROTECTION)
下位階層：　なし
依存性：　なし

¶ 435 **FPT_SKP_EXT.1.1** TSF は、すべての事前共有鍵、対称鍵、及びプライベート鍵の読み出しを防止しなければならない。

¶ 436 ***適用上の注釈：***

¶ 437 *本要件の意図は、管理者が「通常の」インタフェースを通して識別された（保存中または一時的な）鍵を読み出したり、閲覧したりできないことである。管理者がこのような鍵を閲覧するために直接メモリを読み出すことができると理解されているが、実際には些細な作業ではなく、管理者としての作業のかなりの仕事となるかもしれない。管理者は信頼できる職員と考えられるので、彼らはこのようなアクティビティを行おうとはしないと想定される。*

¶ 438 **保証アクティビティ：**

¶ 439 ***TSS：***

¶ 440 評価者は、あらゆる事前共有鍵、対称鍵、及びプライベート鍵がどのように保存されるか、及びそれらが、適用上の注釈に概説したとおり、その目的に特化して設計されたインタフェースを通して閲覧されることが不可能であることについて TSS に詳述されていることを決定するために TSS を検査しなければならない。これらの値が平文で保存されない場合、TSS にはそれらがどのように保護／見えなくしているかについて記述しなければならない。

4.10.2 FPT_STM.1　高信頼タイムスタンプ

(O.AUDIT)
下位階層：　なし
依存性：　なし

¶ 441 **FPT_STM.1.1**　TSF は、高信頼タイムスタンプを提供できなければならない。

¶ 442 ***適用上の注釈：***

¶ 443 *時刻は、信頼される管理者によって設定されるか、または信頼される外部 IT エンティティからネットワークサービス（例えば、NTP）によって設定される。*

¶ 444 **保証アクティビティ:**

¶ 445 ***TSS：***

¶ 446 評価者は、高信頼タイムスタンプが提供するメカニズムについて TSS に記述され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。

¶ 447 ***操作ガイダンス：***

¶ 448 評価者は、ガイダンスに時刻を設定する方法が記述され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。

¶ 449 ***テスト：***

¶ 450 評価者は、次のテストについても実行しなければならない：

1. 評価者は、時刻がガイダンスまたは外部ネットワークサービス（例えば、NTP）に従って正しく設定されることを保証するため、

チェックしなければならない。

2. 評価者は、タイムスタンプが適切に提供され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。

4.10.3 FPT_TST_EXT.1　拡張：TSF テスト

(O.TSF_SELF_TEST)
下位階層：　なし
依存性：　なし

¶ 451 **FPT_TST_EXT.1.1**　TSF は、TSF の正常動作を実証するために、初期起動時（及び電源投入時）に、自己テストのスイートを実行しなければならない。

¶ 452 ***適用上の注釈：***

¶ 453 *電源投入時の自己テストは、本 SFR が FCS_COP.1(b) で特定されるとおりのデジタル署名により、または FCS_COP.1(c) で特定されるハッシュにより、TSF イメージを検証することにより満たすことができる場合、TSF が操作可能となる前に実行されてもよい。*

¶ 454 **保証アクティビティ：**

¶ 455 ***TSS：***

¶ 456 評価者は、TSF によって起動時に実行される自己テストの詳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。；本記述は、実際に実行されるテストの概要（例えば、「メモリがテストされる」というよりも、「書き込んだものが一致することを保証するために、メモリの各番地に値を書き込み、それを読み出すことによってメモリがテストされる」が用いられなければならない）が本記述に含まれているべきである。評価者は、TSF が正しく動作していることを実証するために、テストが十分なものであることについて TSS にて議論がされていることを保証しなければならない。

¶ 457 ***操作ガイダンス：***

¶ 458 評価者は、このようなテストの結果、起こりうるエラー、管理者が取るべき対応のためのアクションについて、操作ガイダンスに記述されていることも保証しなければならない；これらの起こりうるエラーは TSS に記述されたものと一致しなければならない。

4.10.4 FPT_TUD_EXT.1　拡張：高信頼アップデート

(O.UPDATE_VERIFICATION)
下位階層：　なし
依存性：　[FCS_COP.1(b) 暗号操作（署名生成／検証）、または
FCS_COP.1(c) 暗号操作（ハッシュアルゴリズム）]

¶ 459 **FPT_TUD_EXT.1.1**　TSF は、許可された管理者に TOE ファームウェア／ソフトウェアの現在のバージョンを問い合わせる能力を提供しなければならない。

¶ 460 **FPT_TUD_EXT.1.2**　TSF は、許可された管理者に TOE のファームウェア／ソフトウェアへのアップデートを開始する能力を提供しなければならない。

¶ 461 **FPT_TUD_EXT.1.3** TSF は、それらのアップデートをインストールする前に、デジタル署名メカニズムと［選択：*公開ハッシュ*、*他の機能なし*］を用いて TOE へのファームウェア／ソフトウェアのアップデートを検証する手段を提供しなければならない。

¶ 462 ***適用上の注釈：***

¶ 463 *FPT_TUD_EXT.1.2 は、FPT_TUD_EXT.1.3 に従って検証されたものとして提供された自動化されたアップデートを「事前に許可する」ことを管理者に許可すると解釈してもよい。*

¶ 464 *デジタル署名メカニズムは、FCS_COP.1(b) で指定されている。公開ハッシュは FCS_COP.1(c) で指定された関数の一つによって生成される。ST 作成者は、TOE によって実装されたメカニズムを選択するべきである；両方のメカニズムを実装することも許容される。*

¶ 465 **保証アクティビティ：**

¶ 466 ***TSS：***

¶ 467 評価者は、アップデートのためにソフトウェアを検証するメカニズムについての記述が TSS に含まれており、SFR の定義と一貫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。

¶ 468 評価者は、アップデートを実行するインタフェースと同様に、TOE の現在のバージョンを管理者が得るためのインタフェースを TSS が識別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。

¶ 469 ***操作ガイダンス：***

¶ 470 評価者は、アップデート処理を開始するための操作方法と同様に、TOE のバージョンを得るための操作方法についての記述が管理者ガイダンスに含まれており、TSS の記述と一貫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。

¶ 471 *テスト：*

¶ 472 評価者は、次のテストについても実行しなければならない：

1. 評価者は、TOE の現在のバージョンが管理者ガイダンスに指定された操作方法によって適切に取得できることを保証するため、チェックしなければならない。
2. 評価者は、管理者ガイダンスに指定された操作方法によって、正当なアップデート用データを用いて、TOE のアップデート用のデータの検証が成功することを保証するため、チェックしなければならない。
3. 評価者は、正当なアップデート用のデータを用いて、管理者のみがアップデートを適用できることを保証するため、チェックしなければならない。
4. 評価者は、正常なアップデートが終了した後、TOE の現在のバージョンを得ることにより、アップデートが正しく実行されることを保証するため、チェックしなければならない。
5. 評価者は、管理者ガイダンスに指定された操作方法によって不正なアップデート用のデータを用いて、TOE のアップデート用のデータの検証が失敗す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、ハッシュ検証メカニズムとデジタル署名メカニズムが失敗するような場合についてもチェックしなければならない。)

4.11 クラス FRU：資源利用

¶ 473 クラス FRU 要件なし。

4.12 クラス FTA： TOE アクセス

4.12.1 FTA_SSL.3　TSF 起動による終了

(O.USER_I&A)
下位階層：　なし
依存性：　なし

¶ 474 **FTA_SSL.3.1** TSF は、[割付：*利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。

¶ 475 **保証アクティビティ：**

¶ 476 ***TSS：***

¶ 477 評価者は、利用者が非アクティブである指定された時間の後に、終了する利用者セションの種別（例えば、操作パネルまたはウェブインタフェース経由の利用者セション）について、TSS に記述され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。

¶ 478 ***操作ガイダンス：***

¶ 479 評価者は、管理者がセション終了までの時間間隔を設定できるとき、設定の方法についてガイダンスに記述され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。

¶ 480 ***テスト：***

¶ 481 評価者は次のテストについても実行しなければならない：

1. 設定可能な場合、評価者は、管理者ガイダンスにおいて指定された操作方法により、セション終了までの時間が設定可能であることを保証するため、チェックしなければならない。
2. 評価者は、指定された時間間隔の後に、セションが終了することを保証するため、チェックしなければならない。
3. 評価者は、TSS で識別されたすべての利用者セションについて、上記のテスト 1 と 2 を実行しなければならない。

4.13 クラス FTP：高信頼パス／チャネル

4.13.1 FTP_ITC.1　TSF 間高信頼チャネル

(O.COMMS_PROTECTION、 O.AUDIT)

下位階層：　なし

依存性：　[FCS_IPSEC_EXT.1 拡張：選択された IPsec、または
FCS_TLS_EXT.1 拡張：選択された TLS、または
FCS_SSH_EXT.1 拡張：選択された SSH、または
FCS_HTTPS_EXT.1 拡張：選択された HTTPS]。

¶ 482 **FTP_ITC.1.1　詳細化**：TSF は、それ自身と**以下の機能をサポートする許可された IT エンティティ：［選択：***認証サーバ、［割付：その他の機能］*］との間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び**暴露からの**チャネルデータの保護、**及びチャネルデータ改変の検知**を提供する高信頼通信チャネルを提供するために、**［選択：*IPsec*、*SSH*、*TLS*、*TLS／HTTPS*］を用い**なければならない。

¶ 483 **FTP_ITC.1.2　詳細化：**TSF は、TSF、**または許可された IT エンティティ**が、高信頼チャネルを介して通信を開始することを許可しなければならない。

¶ 484 **FTP_ITC.1.3　詳細化：**TSF は、［割付：*TSF が通信を開始できるサービスのリスト*］のために、高信頼チャネルを介して通信を開始しなければならない。

¶ 485 ***適用上の注釈:***

¶ 486 *FTP_ITC.1.3 における割付は、TOE と他の IT エンティティとの間の利用者データと TSF データの通信に関する秘匿性及び／または完全性の要件に対処するべきである。FTP_TRP.1 は、TOE とリモート利用者との間の対話型通信のために用いることを意図している。*

¶ 487 *上記の要件の意図は、TOE がその機能を実行するために対話する許可された IT エンティティとの外部通信を保護するために暗号プロトコルを使用することである。保護（列挙されたプロトコルの一つによる）は、最低限監査情報を収集するサーバとの通信のために要求される。認証サーバ(例えば、RADIUS)と通信する場合、ST 作成者は FTP_ITC.1.1 で「認証サーバ」を選択し、この接続は列挙されたプロトコルの一つによって保護されなければならない。他の許可された IT エンティティ（例えば NTP サーバ）が保護される場合、ST 作成者は適切な割付（それらのエンティティのため）と選択（その接続を保護するために使用するプロトコルのため）を行うこと。ST 作成者が選択を行*

った後、それらはプロトコル選択に関連する附属書 D.2 での詳細な要件を選択し、ST に追加すること。要するに、外部監査収集サーバへの接続は列挙されたプロトコルの一つによって保護する必要がある。外部認証サーバがサポートされる場合、列挙されたプロトコルの一つによって保護される必要がある。その他の外部サーバについて、外部通信は保護されることは要求されないが、保護が主張される場合、識別されたプロトコルの一つによって保護されなければならない。

¶ 488 *通信を開始する側についての要件はないが、ST 作成者は FTP_ITC.1.3 の割付に許可された IT エンティティとの通信を開始できる TOE のサービスを列挙すること。*

¶ 489 *本要件は、保護された通信が最初に確立された時に保護されるだけでなく、停止後の再開においても保護されることを暗示している。TOE 設定の一部がその他の通信を保護するためのトンネルを手動で設定する場合があり、停止後に TOE が（必要な）手動の介入で自動的に通信を再確立しようと試みた場合には、攻撃者が重要な情報を取得したり、接続を侵害したりするために作成される窓となってしまうかもしれない。*

¶ 490 **保証アクティビティ：**

¶ 491 ***TSS：***

¶ 492 評価者は、本要件で識別されている許可された IT エンティティとのすべての通信について、それぞれの通信メカニズムがその IT エンティティについて許可されたプロトコルの観点で識別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。評価者は、TSS に列挙されたすべてのプロトコルが ST の要件に指定され、含まれていることについても確認しなければならない。評価者は、操作ガイダンスが、それぞれの許可された IT エンティティとの許可されたプロトコルを確立するための指示及び接続が意図せずに切断された場合の復旧のための指示を含んでいることを確認しなければならない。

¶ 493 ***テスト：***

¶ 494 評価者は、次のテストについても実行しなければならない：

1. 評価者は、操作ガイダンスに記述されるとおり接続が設定され、通信が成功することを確認した上で、それぞれの許可された IT エンティティとの間のそれぞれのプロトコルを用いた通信が評価の

過程においてテストされることを保証しなければならない。

2. 本要件で定義されるとおり、TOE が開始できる各プロトコルについて、評価者は、実際に通信チャネルが TOE から開始できることを保証するため、操作ガイダンスに従わなければならない。

3. 評価者は、許可された IT エンティティとの間のそれぞれの通信チャネルについて、チャネルデータが平文で送信されないことを保証しなければならない。

4. 評価者は、テスト 1 においてテストされた、それぞれの許可された IT エンティティと関連するそれぞれのプロトコルについて、接続が物理的に中断されることを保証しなければならない。評価者は、物理的接続性が復旧されるとき、通信が適切に保護されることを保証しなければならない。

¶ 495　さらなる 保証アクティビティが特定のプロトコルに関連付けられる。

4.13.2 FTP_TRP.1(a)　高信頼パス（管理者用）

(O.COMMS_PROTECTION)
下位階層：　なし
依存性：　[FCS_IPSEC_EXT.1 拡張：選択された IPsec、または
FCS_TLS_EXT.1 拡張：選択された TLS、または
FCS_SSH_EXT.1 拡張：選択された SSH、または
FCS_HTTPS_EXT.1 拡張：選択された HTTPS]。

¶ 496　**FTP_TRP.1.1(a)　詳細化**：TSF は、それ自身とリモート**管理者**との間に、他の通信パスと論理的に区別され、その端点の保証された識別と、漏えいからの通信データの保護と通信データの改変の検知を提供する**高信頼**通信パスを提供するため、［**以下より少なくとも一つを選択：IPsec、 SSH、TLS、TLS/HTTPS**］**を使用**しなければならない。

¶ 497　**FTP_TRP.1.2(a)　詳細化：**TSF は、**リモート管理者**が、高信頼パスを介して通信を開始することを許可しなければならない。

¶ 498　**FTP_TRP.1.3(a)　詳細化：**TSF は、**最初の管理者認証及びすべてのリモート管理アクション**に対して、高信頼パスの使用を要求しなければならない。

¶ 499　***適用上の注釈:：***

¶ 500 *本要件は、許可されたリモート管理者が高信頼パスを介して、TOE とのすべての通信を開始すること、またすべてのリモート管理者による通信がパス上で実行されることを保証する。本高信頼通信パスを通過するデータは最初の選択で選ばれた定義済みのプロトコルに従って暗号化される。ST 作成者は、TOE がサポートするメカニズムを選択し、附属書 D.2 に詳述されたそれらの選択に関連する要件が、まだ存在してなければ、ST にコピーされていることを保証すること。*

¶ 501 **保証アクティビティ：**

¶ 502 ***TSS：***

¶ 503 評価者は、TOE のリモート管理方法が、どのようにそれらの通信が保護されるかと共に示されていることを決定するために、TSS を検査しなければならない。評価者は、TSS の TOE 管理サポートにおいて列挙されたすべてのプロトコルが要件で指定されたものと一貫しており、ST の要件に含まれていることについても確認しなければならない。

¶ 504 ***操作ガイダンス：***

¶ 505 評価者は、サポートされたそれぞれの方法について、リモート管理者セションを確立するための指示が操作ガイダンスに含まれていることを確認しなければならない。

¶ 506 ***テスト：***

¶ 507 評価者は、次のテストについても実行しなければならない：

1. 評価者は、（操作ガイダンスで）指定されたそれぞれのリモート管理方法を用いた通信が評価の過程でテストされることを、保証しなければならない。ここで、操作ガイダンスに記述されたとおりの接続を設定し、その通信が成功することを保証すること。
2. サポートされたそれぞれのリモート管理方法について、評価者は、リモート利用者が高信頼パスを起動せずにリモート管理セションを確立するために使用できるようなインタフェースが利用可能でないことを保証するために、操作ガイダンスに従わなければならない。
3. 評価者は、それぞれのリモート管理方法について、チャネルデータが平文で送信されないことを保証しなければならない。

¶ 508 さらなる保証アクティビティが特定のプロトコルに伴う。

4.13.3 FTP_TRP.1(b)　高信頼パス（非管理者用）

(O.COMMS_PROTECTION)
下位階層：　なし
依存性：　[FCS_IPSEC_EXT.1 拡張：選択された IPsec、または
FCS_TLS_EXT.1 拡張：選択された TLS、または
FCS_SSH_EXT.1 拡張：選択された SSH、または
FCS_HTTPS_EXT.1 拡張：選択された HTTPS]。

¶ 509 **FTP_TRP.1.1(b)　詳細化**：TSF は、それ自身とリモート利用者との間に、他の通信パスと論理的に区別され、その端点の保証された識別と、漏えいからの通信データの保護と通信データの改変の検知を提供する高信頼通信パスを提供するため、［**以下より少なくとも一つを選択：IPsec、 SSH、TLS、TLS/HTTPS**］**を使用**しなければならない。

¶ 510 **FTP_TRP.1.2(b)　詳細化：**TSF は、[選択：**TSF、リモート利用者**]が、高信頼パスを介して通信を開始することを許可しなければならない。

¶ 511 **FTP_TRP.1.3(b)　詳細化：**TSF は、**最初の利用者認証及びすべてのリモート利用者アクション**に対して、高信頼パスの使用を要求しなければならない。

¶ 512 ***適用上の注釈：***

¶ 513 *本要件は、許可されたリモート利用者が高信頼パスを介して、TOE とのすべての通信を開始すること、またすべてのリモート利用者による通信がこのパス (経路) 上で実行されることを保証する。本高信頼通信パスを通過するデータは最初の選択で選ばれた定義済みのプロトコルに従って暗号化される。ST 作成者は、TOE がサポートするメカニズムを選択し、附属書 D.2 に詳述されたそれらの選択に関連する要件または複数の要件が、まだ存在してなければ、ST にコピーされていることを保証すること。*

¶ 514 **保証アクティビティ：**

¶ 515 ***TSS：***

¶ 516 評価者は、管理者でない利用者用のリモート TOE アクセス方法が、どのようにそれらの通信が保護されるかと共に、示されていることを決定するために、TSS を検査しなければならない。

¶ 517 評価者は、TSS のリモート TOE アクセスのサポートにおいて列挙されたすべてのプロトコルが要件で指定されたものと一貫しており、ST の要件に含まれていることについても確認しなければならない。

¶ 518 *操作ガイダンス：*

¶ 519 評価者は、サポートされたそれぞれの方法についてリモート利用者セションを確立するための指示が操作ガイダンスに含まれていることを確認しなければならない。

¶ 520 *テスト：*

¶ 521 評価者は、次のテストについても実行しなければならない：

1. 評価者は、（操作ガイダンスで）指定されたそれぞれのリモート利用者アクセス方法を用いた通信が評価の過程でテストされることを保証しなければならない。ここで、操作ガイダンスに記述されたとおりの接続を設定し、その通信が成功することを保証すること。
2. サポートされたそれぞれのリモートアクセス方法について、評価者は、リモート利用者が高信頼パスを起動せずにリモート利用者セションを確立するために使用できるようなインタフェースが利用可能でないことを保証するために、操作ガイダンスに従わなければならない
3. 評価者は、リモート利用者アクセス方法のそれぞれについて、チャネルデータが平文で送信されないことを保証しなければならない。

¶ 522 さらなる保証アクティビティが特定のプロトコルに伴う。

4.14 セキュリティ機能要件根拠

¶ 523 本 PP の SFR の依存性はコモンクライテリア V3.1、パート 2 に含まれる SFR の依存性といくつかの点で違いが生じている。

¶ 524 本文書について、SFR についての依存性が一貫しており、このクラスの製品用に定義された使用事例や脅威シナリオにおいて適切であることを保証するために注意深いレビューが行われた。さらに、SFR 依存性は、本 PP にて定義されたが詳細化、繰り返し、及び拡張要件と一貫させるためにレビューされた。その結果として、SFR のいくつかの依存性は CC で定義されたものと

同じではないものがある。

¶ 525 SFR において実施される操作のみ（詳細化、繰り返し、及び操作を完了した選択と割付）は、CC で定義されたとおり、許されたものに厳密に従っている。これらの操作はいくつかの場合 SFR が CC パート 2 で定義されていない追加の依存性を持つ原因となっている。作成者は製品クラスにおける必要性と SFR で完結される操作から起因する依存性が、混乱や不必要な一貫しないセキュリティ機能の導入を避けることができると考えている。

¶ 526 SFR から削除された依存性は取消線で表示している。依存する SFR は本 PP から削除されており、それらは使用されていない。例えば：

- FPT_ITT.1 の依存性は通信プロトコル SFR から削除された、なぜなら HCD は本 PP の主旨において分散型 TOE ではないためである。
- FDP_ITC.1 または FDP_ITC.2 のいずれかの依存性は暗号 SFR から削除された、なぜならそのようなメカニズムは HCD PP において使用されていないからである。

5　セキュリティ保証要件 (APE_REQ)

¶ 527　本セクションは、CC に基づき評価者が実行する評価でのセキュリティ保証要件（SAR）を記述している。これらはセクション 4、附属書 B 、附属書 C 、及び附属書 D におけるセキュリティ機能要件（SFR）に対してすべて共通のものであり、個別の SFR に対する保証アクティビティについては、それぞれのセクションに記述されている。

¶ 528　ST 評価が承認された後、コモンクライテリア IT セキュリティ評価機関（ITSEF）は、TOE、必要な IT 環境、及び TOE ガイダンス文書を入手する。ST に記述された保証アクティビティ（ST または別文書のいずれかにおいて、TOE に合わせて ITSEF によって詳細化される）が ITSEF により実行される。これらのアクティビティは ITSEF 管理下で行われるが、同様に開発者からの支援を得ることが可能である。これらのアクティビティの結果は、認証のため、文書化されて（使用された管理者ガイダンスと共に）提出される。

¶ 529　各保証ファミリに関して、追加の文書／アクティビティを開発者が提供する必要がある場合、何が必要かを明確にするため、「開発者への注釈」が開発者アクションエレメントにて提供されている。

¶ 530　表 5 で指定された TOE セキュリティ保証要件は、本 PP のセクション 2.3 で識別された脅威に対抗するために必要な評価アクティビティを提供する。

表 5 TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネント記述
セキュリティターゲット評価	ASE_CCL.1	適合主張
	ASE_ECD.1	拡張コンポーネント定義
	ASE_INT.1	ST 概説
	ASE_OBJ.1	運用環境のセキュリティ対策方針
	ASE_REQ.1	主張されたセキュリティ要件
	ASE_SPD.1	セキュリティ課題定義
	ASE_TSS.1	TOE 要約仕様
開発	ADV_FSP.1	基本機能仕様
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	準備手続き
ライフサイクルサポート	ALC_CMC.1	TOE のラベル付け
	ALC_CMS.1	TOE の CM 範囲
テスト	ATE_IND.1	独立テスト-適合

脆弱性評定	AVA_VAN.1	脆弱性調査

5.1　クラス ASE：セキュリティターゲット評価

¶ 531　ST は、CEM に定義される ASE アクティビティとして評価される。さらに、TSS に含まれるべき TOE 技術種別に特有の必要な記述を求める保証アクティビティが PP に指定される。

¶ 532　附属書 E は、乱数ビット生成器におけるエントロピーの品質に関して提供されることが期待される情報についての記述を提供する。

¶ 533　鍵管理スキームの重要性により、本 PP は、開発者がその鍵管理実装の詳細な記述を提供することを要求する。本情報は、ST へ附属書として提出され、保護情報であることを記すことができる。このレベルの詳細情報は一般に公開されることは想定されていない。開発者の鍵管理記述の期待される詳細については、附属書 F を参照されたい。

5.2　クラス ADV：開発

¶ 534　本 PP に適合する TOE については、TOE に関する情報は、ST の TOE 要約仕様（TSS）部分と同様に、エンドユーザが利用可能なガイダンス文書にも含まれている。TOE 開発者が TSS を作成することは要求されてはいないが、TOE 開発者は、機能仕様に関連して TSS に含まれる製品の記述を一致させなければならない。セクション 4 、附属書 B 、附属書 C 、及び附属書 D に含まれる保証アクティビティは、TSS セクションとしてふさわしい内容を決定するために、ST 作成者に十分な情報を提供すべきである。

5.2.1　ADV_FSP.1　基本機能仕様

¶ 535　機能仕様は、TSF インタフェース (TSFI) を記述する。本 PP によって提供される保証のレベルにおいて、これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 PP に適合する TOE は必然的に TOE の利用者（管理利用者を含む）によって直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、この保証レベルではそのようなインタフェースそれ自体を特定することにはあまり意味がない。そのようなインタフェースは間接的なテストしかできないためである。本 PP のこのファミリに関するアクティビティは、機能仕様へ対応した形で TSS に提示さ

れるインタフェースと、AGD 文書に提示されるインタフェースの理解に焦点を絞るべきである。特定された保証アクティビティを満たすために、追加的な「機能仕様」文書が必要とされるべきではない。評価される必要のあるインタフェースは、独立した抽象的なリストとしてではなく、列挙された保証アクティビティを行うために必要な情報を通して特徴付けされる。

開発者アクションエレメント ：

¶ 536 ADV_FSP.1.1D

開発者は、機能仕様を提供しなければならない。

¶ 537 ADV_FSP.1.2D

開発者は、機能仕様から SFR への追跡を提供しなければならない。

¶ 538 開発者への注釈：

開発者は、機能仕様として適切な TSS 記述とガイダンス文書を提供しなければならない。TSS 記述はインタフェース設計の妥当性を確認するため、各 SFR に関連付けられた TSFI を識別する。開発者は最低限、TSS 記述とガイダンス文書の内容について一貫性を確認できるレベルで記述することが求められる。TSS 記述及びガイダンス文書の記述内容が評価において情報が不足している場合、追加の情報提供が求められることがある。外部インタフェースから直接の操作/確認ができない SFR について、開発者は追加の情報提供を求められることがある。

内容・提示エレメント：

¶ 539 ADV_FSP.1.1C

機能仕様は、SFR 実施及び SFR 支援の各 TSFI の目的と使用方法を記述しなければならない。

¶ 540 ADV_FSP.1.2C

機能仕様は、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なければならない。

¶ 541 ADV_FSP.1.3C

機能仕様は、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、その分類の根拠を示さなければならない。

¶ 542 ADV_FSP.1.4C

追跡は、機能仕様での TSFI に対する SFR の追跡を実証するものでなければならない。

評価者アクションエレメント：

¶ 543 ADV_FSP.1.1E

評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しな

¶ 544	ADV_FSP.1.2E	ければならない。 評価者は、機能仕様が、SFR の正確かつ完全な具体化であることを決定しなければならない。

¶ 545 **保証アクティビティ：**

¶ 546 ***TSS：***

¶ 547 評価者は、ガイダンス文書から識別可能な外部インタフェースの確認と、SFR を実現するために必要なすべてのインタフェースを TSS 記述が識別していることの検査を行わなければならない。

¶ 548 評価者は、TSS に記述された SFR に関連付けられた TSFI の識別情報の確認と、各インタフェースに関連する記述との一貫性の確認を行わなければならない。

¶ 549 評価者は、ガイダンス文書における TSFI ごとの目的、使用方法、パラメタの情報と同様に、TSS 記述における TSFI の識別情報に基づき、ST に定義された SFR が適切に実現され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。

¶ 550 各 SFR に特有の保証アクティビティがセクション 4 に記述されており、また、附属書 B 、附属書 C 、及び附属書 D からの適用可能な SFR も同様であり、評価者は、それらを本保証コンポーネントに追加することによって評価を実行しなければならない。

5.3 クラス AGD：ガイダンス文書

¶ 551 ガイダンス文書は、開発者のセキュリティターゲットと共に提供される。ガイダンスには、運用環境がセキュリティ機能上その役割を果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が含まれなければならない。文書化に際して、管理者が読解可能な非形式的な文体とするべきである。

¶ 552 ガイダンスは、ST で主張された、製品のサポートしているすべて運用環境について提供されなければならない。本ガイダンスには、以下が含まれる：

- その環境への TOE のインストールを成功させるための指示；及び
- 製品として、また、より大規模な運用環境のコンポーネントとして、TOE のセキュリティを管理するための指示。

¶ 553 特定のセキュリティ機能に関するガイダンスも提供される。このようなガイダンスに関する要件は、セクション 4 で指定された保証アクティビティ、及び附属書 B 、附属書 C 、及び附属書 D の適用可能な保証アクティビティに含まれている。

5.3.1 AGD_OPE.1　利用者操作ガイダンス

開発者アクションエレメント：

¶ 554 AGD_OPE.1.1D　開発者は、利用者操作ガイダンスを提供しなければならない。

¶ 555 開発者への注釈：　開発者は、評価者がチェックするガイダンスの詳細を確認するため、本コンポーネントに関する保証アクティビティをレビューするべきである。これらは、基準を満たすガイダンスを準備するために必要な情報を提供するだろう。

内容・提示エレメント：

¶ 556 AGD_OPE.1.1C　利用者操作ガイダンスは、適切な警告を含め、セキュアな処理環境で管理するべき、利用者がアクセス可能な機能と権限について、利用者の役割ごとに記述しなければならない。

¶ 557 AGD_OPE.1.2C　利用者操作ガイダンスは、TOE により提供された利用可能なインタフェースをセキュアな方法でどのように使用するかを利用者の役割ごとに記述しなければならない。

¶ 558 AGD_OPE.1.3C　利用者操作ガイダンスは、利用可能な機能とインタフェース、特に利用者の管理下にあるすべてのセキュリティパラメタを、必要に応じてセキュアな値を示し、利用者の役割ごとに記述しなければならない。

¶ 559 AGD_OPE.1.4C　利用者操作ガイダンスは、TSF の制御下にあるエンティティのセキュリティ特性の変更を含む、利用者がアクセス可能で実行が必要な機能に関連するセキュリティ関連事象の各タイプについて、利用者の役割ごとに

明確に提示しなければならない。

¶ 560 AGD_OPE.1.5C　利用者操作ガイダンスは、TOE の操作のすべての可能なモード（障害や操作誤りの後の操作を含む）、それらの結果、及びセキュアな運用を維持するために必要なことを識別しなければならない。

¶ 561 AGD_OPE.1.6C　利用者操作ガイダンスは、ST に記述された運用環境のセキュリティ対策方針を満たすために従うべきセキュリティ手段を、利用者の役割ごとに記述しなければならない。

¶ 562 AGD_OPE.1.7C　利用者操作ガイダンスは、明確で、合理的なものでなければならない。

評価者アクションエレメント：

¶ 563 AGD_OPE.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

¶ 564 **保証アクティビティ：**

¶ 565 ***操作ガイダンス：***

¶ 566 操作ガイダンスの内容は、セクション 4 の保証アクティビティ、及び附属書 B 、附属書 C 、及び附属書 D の適用可能な保証アクティビティ、及び CEM に従った TOE 評価によって確認される。

¶ 567 評価者は、次のガイダンスが提供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：

¶ 568 メンテナンスモードから通常の運用環境（評価構成）への移行の後、TOE が評価構成に戻ることを管理者が確認するための手続き。

¶ 569 ***適用上の注釈：***

¶ 570 *評価中、TOE は評価構成へ戻る。市場では、TOE はメンテナンスモードへ入る前の状態の構成に戻ってもよい。*

5.3.2 AGD_PRE.1　準備手続き

開発者アクションエレメント：

¶ 571 AGD_PRE.1.1D 開発者は、準備手続きを含めて TOE を提供しなければならない。

¶ 572 開発者への注釈： 操作ガイダンスと同様に、開発者は、準備手続きに関して必要とされる内容を決定するため、保証アクティビティを見るべきである。

内容・提示エレメント：

¶ 573 AGD_PRE.1.1C 準備手続きは、開発者の配付手続きに従って配付された TOE のセキュアな受入れに必要なすべてのステップを記述しなければならない。

¶ 574 AGD_PRE.1.2C 準備手続きには、TOE のセキュアな設置、及び ST に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべてのステップを記述しなければならない。

評価者アクションエレメント：

¶ 575 AGD_PRE.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

¶ 576 AGD_PRE.1.2E 評価者は、TOE が運用に向けてセキュアに準備されることを確認するために、準備手続きを適用しなければならない。

¶ 577 **保証アクティビティ：**

¶ 578 ***操作ガイダンス：***

¶ 579 評価者は、ST において主張された TOE のためのすべてのプラットフォームについて TOE の適切な対処をガイダンスが提供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。

5.4　クラス ALC：ライフサイクルサポート

¶ 580　本 PP に適合する TOE に提供される保証レベルにおいて、ライフサイクルサポートは、TOE ベンダの開発、構成管理プロセスの調査よりもむしろ、エンドユーザに見えるライフサイクルの側面に限定される。これは、製品の全体的な信頼に貢献するために開発者が実践する重要な役割を軽減するということではなく、むしろ、この保証レベルでの評価で利用可能な情報について反映したものである。

5.4.1　ALC_CMC.1　TOE のラベル付け

¶ 581　本コンポーネントは、TOE を識別することをターゲットとしている。どのように識別するかというと、同一ベンダの他の製品またはバージョンから TOE を区別でき、またエンドユーザによって調達される際に TOE を容易に指定できるようにすることである。

開発者アクションエレメント：

¶ 582　ALC_CMC.1.1D　開発者は、TOE 及び TOE の参照を提供しなければならない。

内容・提示エレメント：

¶ 583　ALC_CMC.1.1C　TOE は、その一意の参照でラベル付けされなければならない。

評価者アクションエレメント：

¶ 584　ALC_CMC.1.1E　評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

¶ 585　**保証アクティビティ：**

¶ 586　***操作ガイダンス：***

¶ 587　評価者は、ST の要件を満たすバージョンを特定するような（製品名／バージョン番号等の）識別子を ST が含んでいることを保証するため、ST をチェックしなければならない。評価者は、調達主体が ST におい

て特定されたとおりの TOE（適切な管理者ガイダンスを含めて）を調達するために使用するためにこの識別子が十分であることを保証しなければならない。さらに、評価者は、バージョン番号が ST に記載のものと一貫していることを保証するためのテスト用に受領した AGD ガイダンスと TOE サンプルをチェックしなければならない。ベンダが TOE を宣伝するためのウェブサイトを維持管理している場合、評価者は、ST における情報が製品を区別するために十分であることを保証するため、ウェブサイトの情報を検査しなければならない。

5.4.2 ALC_CMS.1　TOE の CM 範囲

¶ 588 TOE の範囲と関連する評価証拠要件を考慮すると、このコンポーネントの保証アクティビティは、ALC_CMC.1 に列挙された保証アクティビティによって対処されている。

開発者アクションエレメント：

¶ 589 ALC_CMS.1.1D 開発者は、TOE の構成リストを提供しなければならない。

内容・提示エレメント：

¶ 590 ALC_CMS.1.1C 構成リストは、TOE 自体、及び SAR が要求する評価証拠を含まなければならない。

¶ 591 ALC_CMS.1.2C 構成リストは、構成要素を一意に識別しなければならない。

評価者アクションエレメント：

¶ 592 ALC_CMS.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

¶ 593 **保証アクティビティ：**

¶ 594 ***操作ガイダンス：***

¶ 595 本 PP において「SAR によって要求される評価証拠」は、ST における情報と、AGD 要件の下で管理者及び利用者に提供されたガイダンスとの組み合わせに限定される。TOE が特定されることと識別が ST 及び

AGD ガイダンス（ALC_CMC.1 の保証アクティビティで行われたように）と一貫していることを保証することによって、評価者は、本コンポーネントにより要求される情報を暗黙的に確認する。

5.5 クラス ATE：テスト

¶ 596 テストは、システムの機能的観点について、設計又は実装の弱点を利用するのと同様の観点で明示する。前者は ATE_IND ファミリを通して行われるが、後者は AVA_VAN ファミリを通して行われる。本 PP で指定された保証レベルにおいては、TSS にて提示される利用可能な設計情報が制約されるため、テストは公開された機能とインタフェースに基づいたものとなる。評価プロセスの主なアウトプットの一つは、次の要件で指定されるようなテスト報告書である。

5.5.1 ATE_IND.1 独立テスト – 適合

¶ 597 テストは、提供された管理者文書（設定や操作を含む）と同様に、TSS に記述された機能についても確認するために実行されること。テストは、セクション 4 で指定された要件、及び附属書 B 、附属書 C 、及び附属書 D の適用可能な保証要件を満たしていることの確認にフォーカスするが、いくつかの追加テストがセクション 5 で SAR として指定されている。保証アクティビティは、これらのコンポーネントと関連付けられた最小限のテストアクティビティとして識別されている。評価者は、テスト計画と結果について文書化したテスト報告書を、本 PP への適合を主張するプラットフォーム／TOE の組み合わせに焦点を当てた適用範囲についての論拠と共に作成すること。

開発者アクションエレメント：

¶ 598 ATE_IND.1.1D 開発者は、テストのための TOE を提供しなければならない。

内容・提示エレメント：

¶ 599 ATE_IND.1.1C TOE は、テストに適していなければならない。

評価者アクションエレメント：

¶ 600 ATE_IND.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

¶ 601 ATE_IND.1.2E 評価者は、TSF が仕様とおりに動作することを確認するために、TSF インタフェースのサブセットをテストしなければならない。

¶ 602 **保証アクティビティ：**

¶ 603 *テスト：*

¶ 604 評価者は、システムのテストの観点について文書化したテスト計画書と報告書を作成しなければならない。テスト計画書は、本 PP の本文の保証アクティビティに含まれるすべてのテストアクションに対応すること。保証アクティビティで列挙されたテストごとに一つのテストケースを用意する必要はないが、評価者は、ST におけるそれぞれの適用可能なテスト要件に対応して、テスト計画書に文書化しなければならない。

¶ 605 テスト計画書には、テストされる製品モデルが識別される。テスト計画書には含まれないが ST に含まれる製品モデルについては、テスト計画書において、そのモデルをテストしないことについての正当化が提供されること。この正当化には、テストされるモデルとテストされないモデルとの違いに対応し、その違いが実行されるテストに影響しないという論拠が示されなければならない。単にその違いが影響しないと主張するだけでは十分ではなく、根拠が提供されなければならない。特に、ST に複数のモデル（製品名）が示されている場合、評価者は、言語仕様の違いについて、プリント機能のようなセキュリティ機能以外の機能における影響が、セキュリティ機能に及ぼす影響についても、この正当化を作成する際に考慮しなければならない。ST で主張されるすべての製品モデルがテストされる場合、このような根拠は必要ない。

¶ 606 テスト計画書には、テストされるそれぞれの製品モデルの構成が記述され、また AGD 文書に含まれるものを超えて必要な設定があれば、それも記述されること。評価者は、テストの一部または標準的なテストの事前条件として、それぞれのモデルの設置及び設定用 AGD 文書に従うと想定されていることに注意すべきである。特別なテストドライバまたはツールも含まれる。それぞれのドライバまたはツールについて、そのドライバまたはツールが TOE の機能の動作に悪影響を与えないと

いう論拠（単なる主張ではなく）が提供されること。

¶ 607 テスト計画書には、高レベルのテスト目的と共に、それらの目的を達成するために従うべきテスト手続きについても識別されること。これらの手続きには、特別な手続きの目標、その目標を達成するために用いられるテスト手順と期待される結果が含まれること。テスト報告書（テスト計画書に対して単に注釈を加えたバージョンであってもよい）には、テスト手続きが実行された時に行われたアクティビティが詳述され、また実際のテスト結果が含まれること。これは累積的な記述でなければならないので、失敗に終わったテストの実行が存在する場合、修正版がインストールされ、次にテスト再実行が成功した場合、報告書には、単なる「成功」結果だけではなく、「失敗」と「成功」結果（及びそれを補足する詳細情報）が記載されること。

5.6 クラス AVA：脆弱性評定

¶ 608 本プロテクションプロファイルの第一世代では、評価機関は、この種の製品においてどのような脆弱性が発見されているかについて知るため、公開情報を調査することが想定されている。多くの場合、これらの脆弱性には基本的な攻撃者を超える専門知識が要求される。侵入テストツールが作成され、評価機関に広く普及するまで、評価者は TOE におけるこれらの脆弱性についてのテストは期待されないだろう。評価機関は、ベンダ提供の文書によるこれらの脆弱性の可能性に関してコメントすることが期待される。この情報は侵入テストツールの開発と、将来のプロテクションプロファイルの開発に用いられることになる。

5.6.1 AVA_VAN.1 脆弱性調査

開発者アクションエレメント：

¶ 609 AVA_VAN.1.1D 開発者は、テストのための TOE を提供しなければならない。

内容・提示エレメント：

¶ 610 AVA_VAN.1.1C TOE は、テストに適していなければならない。

評価者アクションエレメント：

¶ 611 AVA_VAN.1.1E 評価者は、提供された情報が、証拠の内容・提示に対するすべての要件を満たしていることを確認しなければならない。

¶ 612 AVA_VAN.1.2E 評価者は、TOE の潜在的脆弱性を識別するために、公知の情報源の対策を実行しなければならない。

¶ 613 AVA_VAN.1.3E 評価者は、基本的な攻撃能力を持つ攻撃者からの攻撃に TOE が耐えられることを決定するため、識別された潜在的脆弱性に基づいて侵入テストを実施しなければならない。

¶ 614 **保証アクティビティ：**

¶ 615 *テスト：*

¶ 616 ATE_IND と同様に、評価者は、この要件に関連する自身の所見を文書化する報告書を作成しなければならない。本報告書は、物理的には ATE_IND で言及するテスト全般の報告書の一部でもよいし、あるいは別文書でもよい。評価者は、プリンティングデバイスや実装された一般的な通信プロトコルで見つかった脆弱性について、特定の TOE に関する脆弱性と同様に決定するため、公開情報の検索を行うこと。評価者は、報告書において、調べた情報源と発見した脆弱性について文書化すること。

¶ 617 発見したそれぞれの脆弱性について、評価者は、それが非該当であることを示す根拠を提供するか、あるいは脆弱性を確認するため（ATE_IND に提供されるガイドラインを用いて）テストを考案するかのいずれか適切な方を行う。適切かどうかは、その脆弱性を利用するために必要とされる攻撃ベクタの評定によって決定される。

¶ 618 例えば、ブートアップ時に、あるキーの組み合わせを押すことによって脆弱性が検出できる場合、本 PP の保証レベルにおいてはテストが適当と思われる。例えば、脆弱性の悪用に電子顕微鏡と液体窒素が必要とされる場合には、テストは適当ではなく、適切な正当化理由が示されることとなる。

5.7 セキュリティ保証要件根拠

¶ 619 これらのセキュリティ保証要件を選択する根拠は、想定される攻撃者の脅威レベルに基づいた最小限のセキュリティベースライン、TOE が配置される運用環境のセキュリティ、及び TOE 自身の相対的価値が定義されていることである。PP 全体の保証アクティビティは、セキュリティ保証要件を達成するための具体的な期待事項に合わせたガイダンスを提供するために使用されている。

附属書 A 定義と根拠表

A.1 利用者の定義

¶ 620 本 PP では、2 つの利用者分類が定義されている：

表 6 利用者分類

名称	分類名	定義
U.NORMAL	一般利用者	識別され、認証された利用者で、管理者役割を持たない利用者
U.ADMIN	管理者	識別され、認証された利用者で管理者役割を持つ利用者

¶ 621 適合 TOE は、追加の役割、補助的な役割、またはグループを定義してもよい。特に適合 TOE は、TOE のことなる側面を管理するための権限を持ついくつかの管理者役割を定義してもよい。

A.2 資産の定義

¶ 622 資産は、情報を保持または受信する TOE における受動的なエンティティである。本 PP では、資産は、オブジェクト（CC により定義されている）である。本 PP では 2 つの資産分類が定義されている：

表 7 資産分類

名称	資産分類	定義
D.USER	利用者データ	TSF の操作に影響を及ぼさない、利用者のために利用者によって作成されたデータ
D.TSF	TSF データ	TSF の操作に影響を与えるかもしれない TOE のための TOE によって作成されたデータ

¶ 623 適合 TOE は、追加の資産分類を定義することができる。

A.2.1 利用者データ

¶ 624 利用者データは、2 つの種別から構成される：

表 8　利用者データ種別

名称	利用者データ種別	定義
D.USER.DOC	利用者文書データ	電子的またはハードコピーの形式で、利用者の文書に含まれる情報
D.USER.JOB	利用者ジョブデータ	利用者の文書または文書処理ジョブに関連する情報

¶ 625　適合 TOE は、利用者データの追加の種別を定義できる。

A.2.2 TSF データ

¶ 626　TSF データは、2 つの種別から構成される：

表 9　TSF データ種別

名称	TSF データ種別	定義
D.TSF.PROT	保護された TSF データ	データの所有者でもなく、または管理者役割も持たない利用者によって、改ざんされた TSF データが TOE のセキュリティ影響を及ぼすかもしれないが、暴露については容認できるような TSF データ。
D.TSF.CONF	秘密の TSF データ	データの所有者でもなく、管理者役割も持たない利用者によって、暴露又は改ざんされた TSF データが、TOE のセキュリティに影響を及ぼすかもしれないような TSF データ。

¶ 627　適合 TOE は、TSF データの追加種別を定義してもよい。

A.3　脅威の定義

¶ 628　脅威は、TOE のセキュリティ方針を危殆化する可能性のある結果をもたらすアクションを実行する脅威エージェントによって定義される。

表 10　脅威

名称	定義
T.UNAUTHORIZED_ACCESS	攻撃者は、TOE のインタフェースを通じて、TOE 内の利用者文書データへアクセス（閲覧、改変、または削除）、または利用者ジョブデータを変更（改変または削除）するかもしれない。
T.TSF_COMPROMISE	攻撃者は、TOE のインタフェースを通じて、TOE 内の TSF データへの不正なアクセスを得るかもしれない。
T.TSF_FAILURE	TOE の操作が許可された場合、TSF の誤作動によって、セキュリティの損失を引き起こすかもしれない。
T.UNAUTHORIZED_UPDATE	攻撃者は、TOE に不正なソフトウェアをインストールするかもしれない。
T.NET_COMPROMISE	攻撃者は、ネットワーク通信をモニターしたり操作したりすることで、送信中のデータにアクセスしたり、TOE のセキュリティを侵害したりするかもしれない。

A.4　組織のセキュリティ方針の定義

¶ 629　組織のセキュリティ方針は、資産に対する脅威に基づいて定義するのは実用的ではない、または主に顧客の期待から生じる、セキュリティ対策方針の基礎を提供するために使用される。

表 11　組織のセキュリティ方針

名称	定義
P.AUTHORIZATION	利用者は、文書処理及び管理機能を実行する前に権限を付与されなければならない。
P.AUDIT	セキュリティ関連アクティビティは監査されなけ

	ればならず、またこのようなアクションのログは保護され、外部 IT エンティティへ送信されなければならない。
P.COMMS_PROTECTION	TOE は、LAN 上の他のデバイスに対し自身を識別できなければならない。
P.STORAGE_ENCRYPTION (条件付き必須)	TOE が利用者文書データまたは秘密の TSF データを現地交換可能な不揮発性ストレージデバイスに保存する場合、TOE はそれらのデバイス上のこのようなデータを暗号化すること。
P.KEY_MATERIAL (条件付き必須)	利用者文書データまたは秘密の TSF データの現地交換可能な不揮発性ストレージのための暗号鍵の生成に寄与するような、平文の鍵、サブマスク、乱数、またはその他のあらゆる値は、不正なアクセスから保護されなければならない、かつそのストレージデバイス上に保存されてはならない。
P.FAX_FLOW (条件付き必須)	TOE が PSTN ファクス機能を提供する場合、PSTN ファクス回線と LAN の間に分離を保証する。
P.IMAGE_OVERWRITE (オプション)	文書処理ジョブの終了または中止の際に、TOE はその現地交換可能な不揮発性ストレージデバイス上の残存画像データを上書き消去しなければならない。
P.PURGE_DATA (オプション)	TOE は、権限付与された者が、不揮発性ストレージデバイス上のすべての顧客が供給する利用者データ及び TSF データを永久に取り出しできないようにすることができる機能を提供しなければならない。

A.5　前提条件の定義

¶ 630　前提条件は、セキュリティ対策方針やセキュリティ機能要件が有効であるた

めに、満たされなければならない条件である。

表 12　前提条件

名称	定義
A.PHYSICAL	TOE、及び TOE が保存または処理するデータの価値に見合った物理的セキュリティが、その環境によって提供されることを想定する。
A.NETWORK	運用環境は、LAN インタフェースへの外部からの直接のアクセスから TOE を保護することを想定する。
A.TRUSTED_ADMIN	TOE 管理者は、サイトセキュリティ方針に従って TOE を管理すると、信頼されている。
A.TRAINED_USERS	許可された利用者は、サイトセキュリティ方針に従って TOE を使用するよう教育訓練を受けている。

A.6　TOE のセキュリティ対策方針の定義

表 13　TOE のセキュリティ対策方針

名称	定義
O.USER_I&A	TOE は、アクセス制御、利用者の権限付与、または管理者役割を要求する操作のため、利用者の識別及び認証を実行しなければならない。
O.ACCESS_CONTROL	TOE は、セキュリティ方針に従って、利用者データ及び TSF データを保護するため、アクセス制御を実施しなければならない。
O.USER_AUTHORIZATION	TOE は、セキュリティ方針に従って、利用者の権限付与を実行しなければならない。

O.ADMIN_ROLES	TOE は、許可された管理者のみが管理者機能の実行を許可されていることを保証しなければならない。
O.UPDATE_VERIFICATION	TOE は、ソフトウェアアップデートの真正性を検証するメカニズムを提供しなければならない。
O.TSF_SELF_TEST	TOE は、セキュリティ機能のサブセットが正常に動作していることを保証するため、セキュリティ機能のサブセットをテストしなければならない。
O.COMMS_PROTECTION	TOE は、利用者データ及び TSF データの LAN 通信を、不正なアクセス、リプレイ、及び送信元／宛先のなりすましから保護する機能を有していなければければならない。
O.AUDIT	TOE は、監査データを生成し、信頼される外部 IT エンティティへ送信可能でなければならない。オプションとして、TOE 内に監査データを保存してもよい。
O.STORAGE_ENCRYPTION（条件付き必須）	TOE が利用者文書データまたは秘密の TSF データを現地交換可能な不揮発性ストレージデバイスに保存する場合、TOE はそれらのデバイス上のこのようなデータを暗号化しなければならない。
O.KEY_MATERIAL（条件付き必須）	TOE は、現地交換可能な不揮発性ストレージ内の利用者文書データ又は秘密の TSF データを格納するための暗号鍵の生成に寄与するあらゆる平文の鍵、サブマスク、乱数又はその他の値を、不正アクセスから保護しなければならない；TOE は、そのような鍵材料が、その材料を使

	用するストレージデバイス上に平文で格納されないことを保証しなければならない。
O.FAX_NET_SEPARATION（条件付き必須）	TOE が PSTN ファクス機能を提供する場合、TOE は PSTN ファクス電話回線と LAN の分離をシステム設計または有効なセキュリティ機能により保証しなければならない。
O.IMAGE_OVERWRITE（オプション）	文書処理ジョブの完了または中断に際して、TOE は、現地交換可能な不揮発性ストレージデバイスから残存画像データを上書き消去しなければならない。
O.PURGE_DATA（オプション）	TOE は、許可された管理者が不揮発性ストレージデバイスからすべての顧客が供給する利用者データ及び TSF データを永久に取り出せないようにするために起動できる機能を提供する。

A.7　運用環境のセキュリティ対策方針の定義

表 14　運用環境のセキュリティ対策方針

名称	定義
OE.PHYSICAL_PROTECTION	運用環境は、TOE、及び TOE が保存または処理するデータの価値に見合った物理的セキュリティを提供しなければならない。
OE.NETWORK_PROTECTION	運用環境は、LAN インタフェースへの外部からの直接のアクセスから TOE を保護するためにネットワークセキュリティを提供しなければならない。

OE.ADMIN_TRUST	TOE 所有者は、管理者がその権限を悪意ある目的に使用しないという信頼を確立しなければならない。
OE.USER_TRAINING	TOE 所有者は、利用者がサイトセキュリティ方針を理解し、それに従う力量を持っていることを保証しなければならない。
OE.ADMIN_TRAINING	TOE 所有者は、管理者がサイトセキュリティ方針を理解し、TOE を正しく設定し、パスワードと鍵を相応に保護するために製造者のガイダンスを活用する力量を持っていることを保証しなければならない。

A.8　セキュリティ対策方針表

表 15　セキュリティ対策方針根拠

脅威／方針／前提条件	根拠
T.UNAUTHORIZED_ACCESS ***攻撃者は、TOE のインタフェースを通じて、TOE 内の利用者文書データへアクセス（閲覧、改変、または削除）、または利用者ジョブデータを変更(改変または削除)するかもしれない。***	O.ACCESS_CONTROL は、TOE 内の利用者データへのアクセスを許可された利用者に制限する。 O.USER_I&A は、アクセス制御の基礎を提供する。 O.ADMIN_ROLES は、利用者に権限付与し、アクセス制御を設定する能力を許可された管理者に制限する。
T.TSF_COMPROMISE ***攻撃者は、TOE のインタフェースを通じて、TOE 内の TSF データへの不正なアクセスを得るかもしれない。***	O.ACCESS_ CONTROL は、TOE 内の TSF データへのアクセスを許可された利用者に制限する。 O.USER_I&A は、アクセス制御の基礎を提供する。

	O.ADMIN_ROLES は、利用者に権限付与し、アクセス制御を設定する能力を、許可された管理者に制限する。
T.TSF_FAILURE ***TOE の操作が許可された場合、TSF の誤作動によって、セキュリティの損失を引き起こすかもしれない。***	O.TSF_SELF_TEST は、誤作動が検知された場合、TOE の運用を防止する。
T.UNAUTHORIZED_UPDATE ***攻撃者は、TOE に不正なソフトウェアをインストールするかもしれない。***	O.UPDATE_VERIFICATION は、ソフトウェアアップデートの真正性を検証する。
T.NET_COMPROMISE ***攻撃者は、ネットワーク通信をモニターしたり操作したりすることで、送信中のデータにアクセスしたり、TOE のセキュリティを侵害したりするかもしれない。***	O.COMMS_PROTECTION は、盗聴、リプレイ、及び中間者攻撃から LAN 通信を保護する。
P.AUTHORIZATION ***利用者は、文書処理及び管理機能を実行する前に権限を付与されなければならない。***	O.USER_AUTHORIZATION は、文書処理と管理者機能を実行する能力を許可された利用者に制限する。 O.USER_I&A は、権限付与の基礎を提供する。 O.ADMIN_ROLES は、利用者に権限付与する能力を許可された管理者に制限する。
P.AUDIT ***セキュリティ関連アクティビティは、監査されなければならず、またこのようなアクションのログは保護され、外部 IT エンティティへ送信されなけれ***	O.AUDIT は、監査データの生成を要求する。 O.ACCESS_CONTROL は、TOE 内の監査データへのアクセスを許可され

ばならない。	た利用者に制限する。 O.USER_AUTHORIZATION は、権限付与の基礎を提供する。
P.COMMS_PROTECTION ***TOE は、LAN 上の他のデバイスに対し自身を識別できなければならない。***	O.COMMS_PROTECTION は、中間者攻撃から LAN 通信を保護する。
P.STORAGE_ENCRYPTION (条件付き必須) ***TOE が利用者文書データまたは秘密の TSF データを現地交換可能な不揮発性ストレージデバイスに保存する場合、TOE はそれらのデバイス上のこのようなデータを暗号化すること。***	O.STORAGE_ENCRYPTION は、現地交換可能な不揮発性ストレージデバイスに保存される利用者文書データと秘密の TSF データを、デバイスが TOE 及びその運用環境から除去される場合、暴露から保護する。
P.KEY_MATERIAL (条件付き必須) *利用者文書データまたは秘密の TSF データの現地交換可能な不揮発性ストレージ用の暗号化鍵の生成に寄与するような、暗号化されていない鍵、サブマスク、乱数または任意の他の値は、そのストレージデバイス上に保存されてはならない。*	O.KEY_MATERIAL は、鍵及び鍵材料を不正アクセスから保護し、それらあらゆる鍵材料が平文の状態で、デバイス自身の暗号化のためにそれらの材料を使用するようなデバイス上に保存されていないことを保証する。
P.FAX_FLOW (条件付き必須) ***TOE が PSTN ファクス機能を提供する場合、それは PSTN ファクス回線と LAN の間に分離を保証する。***	O.FAX_NET_SEPARATION は、PSTN ファクス回線と LAN の間の分離を要求する。
P.IMAGE_OVERWRITE (オプション) *文書処理ジョブの終了または中止の際に、TOE は残存画像データをその現地交換可能な不揮発性ストレージデバイスから上書き消去しなければならな*	O.IMAGE_OVERWRITE は、文書処理ジョブの完了または中止した後に、現地交換可能な不揮発性ストレージデバイスから残存画像データを上書き消去する。

い。	.
P.PURGE_DATA (オプション) ***TOE は、権限付与された者が、現地交換可能な不揮発性ストレージデバイス上のすべての顧客が供給する利用者データ及び TSF データを永久に取り出せないようにすることができる機能を提供しなければならない。***	O.PURGE_DATA は、権限付与された者が、現地交換可能な不揮発性ストレージデバイスからすべての顧客が供給する利用者データ及び TSF データを永久に取り出せできないようにする機能を提供する。
A.PHYSICAL ***TOE、及び TOE が保存または処理するデータの価値に見合った物理的セキュリティが、その環境によって提供されることを想定する。***	OE.PHYSICAL_PROTECTION は、TOE のための保護された物理的な環境を確立する。
A.NETWORK ***運用環境は、LAN インタフェースへの外部からの直接のアクセスから TOE を保護することを想定する。***	OE.NETWORK_PROTECTION は、TOE のための保護された LAN 環境を確立する。
A.TRUSTED_ADMIN ***TOE 管理者は、サイトセキュリティ方針に従って TOE を管理すると、信頼されている。***	OE.ADMIN_TRUST は、管理者と信頼ある関係を築くための TOE 所有者の責任を確立する。
A.TRAINED_USERS ***許可された利用者は、サイトセキュリティ方針に従って TOE を使用するよう教育訓練を受けている。***	OE.ADMIN_TRAINING は、管理者に適切な教育訓練を提供するための TOE 所有者の責任を確立する。 OE.USER_TRAINING は、利用者に適切な教育訓練を提供するための TOE 所有者の責任を確立する。

A.9　拡張機能要件定義

A.9.1 FAU_STG_EXT　拡張：外部監査証跡格納

¶ 631 **ファミリのふるまい：**

¶ 632 本ファミリは、TOE から外部 IT エンティティへの監査データのセキュアな送信を保証する TSF の要件を定義する。

¶ 633 **コンポーネントのレベル付け：**

¶ 634 **FAU_STG_EXT.1** 外部監査証跡格納は、TSF がセキュアなプロトコルを実装して高信頼チャネルを使用することを要求する。

¶ 635 **管理：**

¶ 636 以下のアクションは FMT における管理機能と考えられる：

- TSF は、暗号機能を設定する能力を持っていなければならない。

¶ 637 **監査：**

¶ 638 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 639 **FAU_STG_EXT.1　拡張：外部監査証跡格納**

下位階層：　なし

依存性：　FAU_GEN.1 監査データ生成

FTP_ITC.1 TSF 間高信頼チャネル

¶ 640 **FAU_STG_EXT.1.1** TSF は、FTP_ITC.1 に従い、高信頼チャネルを用いて、外部 IT エンティティへ生成した監査データを送信できなければならない。

¶ 641 **根拠：**

¶ 642 TSF は、監査記録の保存とレビューのため、非 TOE の監査サーバに依存するような外部 IT エンティティへの生成された監査データの送信が要求される。このような監査記録の保存と監査記録のレビューを管理者に許可する能力は、その場合運用環境によって提供される。コモンクライテリアは、外部 IT エン

ティティへの監査データの送信に適した SFR を提供していない。

¶ 643 本拡張コンポーネントは、監査記録を保護するので、FAU クラスの一つのコンポーネントとする。

A.9.2 FCS_CKM_EXT　拡張：暗号鍵管理

¶ 644 **ファミリのふるまい：**

¶ 645 本ファミリは、暗号鍵の管理の側面に対処し、本拡張コンポーネントは暗号鍵破棄のためのものである。

¶ 646 **コンポーネントのレベル付け：**

FCS_CKM_EXT.4: 拡張：暗号鍵材料破棄	4

¶ 647 **FCS_CKM_EXT.4** 暗号鍵材料破棄は、鍵のみではなく、もはや不要となった鍵材料についても承認された方法で破棄されることを保証する。

¶ 648 **管理：**

¶ 649 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 650 **監査：**

¶ 651 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 652 **FCS_CKM_EXT.4　拡張：暗号鍵材料破棄**

下位階層：　なし

依存性：　[
FCS_CKM.1(a)　暗号鍵生成（非対称鍵），または
FCS_CKM.1(b)　暗号鍵生成(対称鍵)],
FCS_CKM.4 暗号鍵破棄

¶ 653 **FCS_CKM_EXT.4.1**　TSF は、すべての平文の秘密鍵及びプライベート

暗号鍵及び暗号クリティカルセキュリティパラメタがもはや不要となったとき、それらを破棄しなければならない。

¶ 654 **根拠：**

¶ 655 暗号鍵材料破棄は、もはや不要となった鍵及び鍵材料が承認された方法で破棄されることを保証するものであり、コモンクライテリアは暗号鍵材料破棄に適した SFR を提供していない。

¶ 656 本拡張コンポーネントは、暗号鍵及び鍵材料を暴露から保護するので、FCS クラスの一つのコンポーネントとする。

A.9.3 FCS_HTTPS_EXT　拡張：選択された HTTPS

¶ 657 **ファミリのふるまい：**

¶ 658 本ファミリのコンポーネントは、TOE とセキュリティ管理者の間のリモート管理セションを保護するための要件を定義する。本ファミリは HTTPS がどのように実装されるかを記述する。これは、FCS クラスに定義される新しいファミリである。

¶ 659 **コンポーネントのレベル付け：**

FCS_HTTPS_EXT.1 明示的：選択された HTTPS	1

¶ 660 **FCS_HTTPS_EXT.1** 選択された HTTPS は、RFC 2818 に従って実装され、TLS をサポートすることを要求する。

¶ 661 **管理：**

¶ 662 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 663 **監査：**

¶ 664 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- HTTPS セション確立の失敗

¶ 665 **FCS_HTTPS_EXT.1 拡張：選択された HTTPS**

下位階層：　　なし

依存性：　　なし

¶ 666 **FCS_HTTPS_EXT.1.1**　　TSF は、RFC 2818 に適合する HTTPS プロトコルを実装しなければならない。

¶ 667 **FCS_HTTPS_EXT.1.2**　　TSF は、FCS_TLS_EXT.1 で指定されるとおり、TLS を用いて HTTPS を実装しなければならない。

¶ 668 **根拠：**

¶ 669 HTTPS は、セキュア通信プロトコルの一つであり、コモンクライテリアは暗号アルゴリズムを用いた通信プロトコルに適した SFR を提供していない。

¶ 670 本拡張コンポーネントは、暗号アルゴリズムを用いて通信データを保護するので、FCS クラスの一つのコンポーネントとする。

A.9.4 FCS_IPSEC_EXT　拡張：選択された IPsec

¶ 671 **ファミリのふるまい：**

¶ 672 本ファミリは、IPsec を用いて通信を保護するための要件に対処する。

¶ 673 **コンポーネントのレベル付け：**

FCS_IPSEC_EXT.1 明示的：選択された IPsec	1

¶ 674 **FCS_IPSEC_EXT.1** IPsec は、IPsec が特定されたとおり実装されることを要求する。

¶ 675 **管理：**

¶ 676 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 677 **監査：**

¶ 678 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- IPsec SA 確立の失敗

¶ 679 **FCS_IPSEC_EXT.1　拡張：選択された IPsec**

下位階層：　なし

依存性：　FIA_PSK_EXT.1　拡張：事前共有鍵生成

FCS_COP.1(g) 暗号操作（鍵付ハッシュメッセージ認証）

¶ 680 **FCS_IPSEC_EXT.1.1**　TSF は、RFC4301 で指定されたとおり、IPsec アーキテクチャを実装しなければならない。

¶ 681 **FCS_IPSEC_EXT.1.2**　TSF は、［選択：トンネルモード、トランスポートモード］を実装しなければならない。

¶ 682 **FCS_IPSEC_EXT.1.3**　TSF は、他に一致しなかったものすべてに一致して破棄するような SPD における名目上の最終エントリを持っていなければならない。

¶ 683 **FCS_IPSEC_EXT.1.4**　TSF は、［選択：セキュアハッシュアルゴリズム（SHA）ベースの HMAC と共に AES-CBC-128（RFC 3602 によって指定された）、セキュアハッシュアルゴリズム（SHA）ベースの HMAC と共に AES-CBC-256（RFC 3602 によって指定された）、RFC 4106 で指定された AES-GCM-128、RFC 4106 で指定された AES-GCM-256、の暗号化アルゴリズム］を用いて、RFC 4303 で定義されたとおり、IPsec プロトコル ESP を実装しなければならない。

¶ 684 **FCS_IPSEC_EXT.1.5**　TSF は、次のプロトコルを実装しなければならない：［［選択：RFC 2407、2408、2409、 RFC 4109、［選択：拡張シーケンス番号のためのその他の RFC なし、拡張シーケンス番号のための RFC 4304］、及び［選択：ハッシュ関数のためのその他の RFC なし、ハッシュ関数のための RFC4868］で定義された IKEv1；RFC 5996（セクション 2.23 で指定された NAT トラバーサルのための必須のサポート付）、4307、及び［選択：ハッシュ関数のためのその他の RFC なし、ハッシュ関数のための RFC4868］で定義された IKEv2］。

¶ 685 **FCS_IPSEC_EXT.1.6**　TSF は、［選択：IKEv1、IKEv2］プロトコルにおける暗号化されたペイロードが、RFC3602 で指定された暗号化アルゴリズム AES-CBC-128、AES-CBC-256、及び［選択：RFC 5282 で指定された AES-GCM-128、AES-GCM-256、他のアルゴリズムなし］を使用することを保証しなければならない。

¶ 686 **FCS_IPSEC_EXT.1.7**　TSF は、IKEv1 フェーズ 1 鍵交換がメインモード

のみを使用することを確認しなければならない。

¶ 687 **FCS_IPSEC_EXT.1.8**　TSF は、［選択：IKEv2 の SA ライフタイムが［選択：パケット数／バイト数；時間の長さ、ここで時間の値はフェーズ 1 の SA で 24 時間とフェーズ 2 の SA で 8 時間に制限することができる］に基づき確立可能である；IKEv1 の SA ライフタイムが［選択：パケット数／バイト数；時間の長さ、ここで時間の値はフェーズ 1 の SA で 24 時間とフェーズ 2 の SA で 8 時間に制限することができる］に基づき確立可能である］ことを保証しなければならない。

¶ 688 **FCS_IPSEC_EXT.1.9**　TSF は、すべての IKE プロトコルが DH グループ 14（2048 ビット MODP）、及び［選択：24（2048 ビット MODP と 256 ビット POS）、19（256 ビットランダム ECP）、20（384 ビットランダム ECP）、5（1536 ビット MODP））、［割付：TOE により実装されたその他の DH グループ］、その他の DH グループなし］を実装していることを保証しなければならない。

¶ 689 **FCS_IPSEC_EXT.1.10**　TSF は、すべての IKE プロトコルが［選択：RSA、ECDSA］アルゴリズムと事前共有鍵を用いて、ピア認証を実行することを保証しなければならない。

¶ 690 **根拠：**

¶ 691 IPsec は、セキュア通信プロトコルの一つであり、コモンクライテリアは暗号アルゴリズムを用いた通信プロトコルに適した SFR を提供していない。

¶ 692 本拡張コンポーネントは、暗号アルゴリズムを用いて通信データを保護するため、FCS クラスの一つのコンポーネントとする。

A.9.5 FCS_KDF_EXT　拡張：暗号鍵導出

¶ 693 **ファミリのふるまい：**

¶ 694 本ファミリは、特定のサブマスクから導出される中間鍵による手段を特定する。

¶ 695 **コンポーネントのレベル付け：**

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

¶ 697 **管理：**

¶ 698 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 699 **監査：**

¶ 700 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 701 **FCS_KDF_EXT.1　拡張：暗号鍵導出**

下位階層：　なし

依存性：　FCS_COP.1(h)暗号操作(鍵付ハッシュメッセージ認証)、[選択された場合：FCS_RBG_EXT.1　拡張：暗号操作（乱数ビット生成）]

¶ 702 **FCS_KDF_EXT.1.1**　TSF は、[選択： FCS_RBG_EXT.1 で特定されたとおり RNG が生成したサブマスク、調整されたパスワードサブマスク、インポートされたサブマスク] を[選択：NIST SP800-108 [選択：カウンターモードでの KDF、フィードバックモードでの KDF、ダブルパイプライン繰返しモードでの KDF]、NIST SP800-132] に定義されるとおり、その出力が少なくとも BEV と等しいセキュリティ強度（ビット数において）となるような FCS_COP.1(h) で特定される鍵付ハッシュ関数を用いて中間鍵を導出することを受け入れなければならない。

A.9.6 FCS_KYC_EXT　拡張：暗号鍵操作 (鍵チェイニング)

¶ 703 **ファミリのふるまい：**

¶ 704 本ファミリは、ストレージ上の暗号化されたデータを究極的にセキュアにする、多層化された暗号鍵を用いるための仕様を提供する。

¶ 705 **コンポーネントのレベル付け：**

FCS_KYC_EXT.1 鍵チェイニング	1

¶ 706 **FCS_KYC_EXT.1** 鍵チェイニングは、TSF が鍵チェインを維持し、そのチェ

インの特性を指定することを要求する。

¶ 707 **管理：**

¶ 708 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 709 **監査：**

¶ 710 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 711 **FCS_KYC_EXT.1　拡張：鍵チェイニング**

下位階層：　なし

依存性：　［FCS_COP.1(e) 暗号操作（鍵ラッピング）、
FCS_SMC_EXT.1 拡張：サブマスク結合、
FCS_COP.1(i) 暗号操作（鍵配送）、
FCS_KDF_EXT.1 暗号操作（鍵導出）、及び／または
FCS_COP.1(f)　暗号操作 (鍵暗号化)］

¶ 712 **FCS_KYC_EXT.1.1**　TSF は、[選択：一つ、*BEV または DEK としてサブマスクを使用するもの；以下の方法を用いて一つまたは複数のサブマスクから BEV または DEK へ生成する中間鍵：*[選択： *FCS_COP.1(e) で特定される鍵ラッピング、FCS_SMC_EXT.1 で特定される鍵結合 (Key Combining)、FCS_COP.1(f) で特定される鍵暗号化、FCS_KDF_EXT.1 で特定される鍵導出 (Key Derivation)、FCS_COP.1(i) で特定される鍵配送（Key Transport）*]]の鍵チェインを維持しなければならない。ここで、[選択：128 ビット、256 ビット]の有効な強度を維持すること。

¶ 713 **根拠：**

¶ 714 鍵チェイニングは、TSF が鍵チェインを維持し、そのチェインの特性を指定することを保証する。しかし、コモンクライテリアは、暗号化されたデータを保護するための暗号鍵の複数階層の管理に適した SFR を提供していない。

¶ 715 本拡張コンポーネントは暗号アルゴリズムを用いて TSF データを保護するので、FCS クラスの一つのコンポーネントとする。

A.9.7 FCS_PCC_EXT　拡張：暗号パスワードの生成と調整

¶ 716 **ファミリのふるまい：**

¶ 717 本ファミリは、BEV を生成するために使用されるパスワードが堅牢であり、適切な長さのビット列を提供するよう調整されていることを保証する。

¶ 718 **コンポーネントのレベル付け：**

¶ 719

¶ 720 **FCS_PCC_EXT.1** 暗号パスワード生成と調整は、適切になされたパスワードの特定の成分と調整を TSF が受け入れることを要求する。

¶ 721 **管理：**

¶ 722 予見される管理アクションはない。

¶ 723 **監査：**

¶ 724 予見される監査対象事象はない。

¶ 725 **FCS_PCC_EXT.1　拡張：暗号パスワードの生成と調整**

下位階層：　なし

依存性：　FCS_COP.1(h) 暗号操作(鍵付ハッシュメッセージ認証)

¶ 726 **FCS_ PCC_EXT.1.1** パスワード認証ファクタを生成するために使用されるパスワードは、[割付：*64 以上の正の整数*]文字までの文字列を有効とし、｛大文字、小文字、数字、及び[割付：*その他の特殊文字*]｝からなる、また、特定された暗号アルゴリズム[HMAC-[選択：SHA-256、SHA-384、SHA-512]]に従い[割付：*1000 以上の正の整数*]回の繰り返しを行い、暗号鍵長[選択：128、256]を出力するパスワードベースの鍵導出関数を実行しなければならない。ここで、以下を満たすこと：[割付：*PBKDF 勧告または仕様*]。

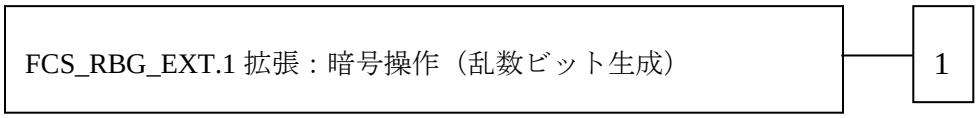
A.9.8 FCS_RBG_EXT　拡張：暗号操作（乱数ビット生成）

¶ 727 **ファミリのふるまい：**

¶ 728 本ファミリは、選択された規格に従って乱数ビット生成が実行され、エントロピー源によりシードされることを保証するため、ランダムヒット生成の要

件を定義する。

¶ 729 **コンポーネントのレベル付け：**



¶ 730 **FCS_RBG_EXT.1** 乱数ビット生成器は、選択された規格に従って乱数ビット生成が実行され、エントロピー源によりシードを供給されることを要求する。

¶ 731 **管理：**

¶ 732 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 733 **監査：**

¶ 734 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 735 **FCS_RBG_EXT.1　　拡張：乱数ビット生成**

下位階層：　　なし

依存性：　　なし

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

¶ 737 **FCS_RBG_EXT.1.2**　決定論的 RBG は、[選択：[割付：*ソフトウェアによるノイズ源の数*]のソフトウェアによるノイズ源、[割付：*ハードウェアによるノイズ源の数*]のハードウェアによるノイズ源]から、ISO/IEC 18031:2011 の表 C.1 「Security strength table for hash functions」に従って、いくつか生成する鍵とハッシュの中で最も大きいセキュリティ強度のものと少なくとも等しいような、[選択：128 ビット、256 ビット]のエントロピーを最小限持つように、エントロピーを蓄積するエントロピー源によってシードを供給されなければならない。

¶ 738 **根拠：**

¶ 739 乱数ビット／乱数は、鍵生成及び破棄のための SFR として使用される。コモ

ンクライテリアは乱数ビット生成に適した SFR を提供していない。

¶ 740 本拡張コンポーネントは、暗号鍵の強度を保証するので、FCS クラスの一つのコンポーネントとする。

A.9.9 FCS_SMC_EXT　拡張：サブマスク結合

¶ 741 **ファミリのふるまい：**

¶ 742 本ファミリは、TOE が BEV を導出または保護するために使用する 2 つ以上のサブマスクをサポートする場合、サブマスクを結合する手段を定義する。

¶ 743 **コンポーネントのレベル付け：**

¶ 744 **FCS_SMC_EXT.1** サブマスク結合は、TSF が予測可能なやり方でサブマスクを結合することを要求する。

¶ 745 **管理：**

¶ 746 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 747 **監査：**

¶ 748 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 749 **FCS_SMC_EXT.1　拡張：サブマスク結合**

下位階層：　なし

依存性：　FCS_COP.1(c)　暗号操作（ハッシュアルゴリズム）

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

¶ 751 **根拠：**

¶ 752 サブマスク結合は、BEV を導出または保護するために TSF がサブマスクを結合することを保証するものである。

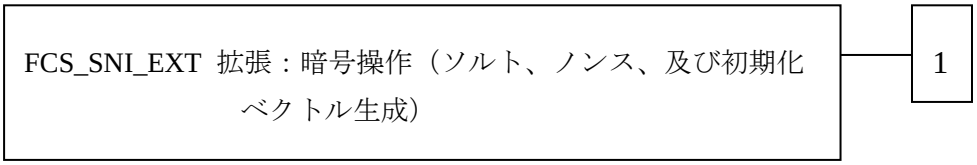
¶ 753 本拡張コンポーネントは、暗号アルゴリズムを用いて TSF データを保護するので、FCS クラスの一つのコンポーネントとする。

A.9.10 FCS_SNI_EXT　拡張：暗号操作（ソルト、ノンス、及び初期化ベクトル生成）

¶ 754 **ファミリのふるまい：**

¶ 755 本ファミリは、ソルト、ノンス及び IV がうまく生成されることを保証する。

¶ 756 **コンポーネントのレベル付け：**



¶ 757

¶ 758 **FCS_SNI_EXT.1** 暗号操作（ソルト、ノンス、及び初期化ベクトル生成）は、TOE の暗号コンポーネントにより使用されるソルト、ノンス及び IV の生成が特定された方法で実行されることを要求する。

¶ 759 **管理：**

¶ 760 予見される管理アクションはない。

¶ 761 **監査：**

¶ 762 予見される監査対象事象はない。

¶ 763 **FCS_SNI_EXT.1 拡張：暗号操作（ソルト、ノンス、及び初期化ベクトル）**

下位階層：　なし

依存性：　FCS_RBG_EXT.1 拡張：暗号操作(乱数ビット生成)

¶ 764 **FCS_SNI_EXT.1.1** TSF は、**FCS_RBG_EXT.1 で特定された RNG** により生成されたソルトのみを使用しなければならない。

¶ 765 **FCS_SNI_EXT.1.2** TSF は、[64]ビットの最小長で一意的なノンスのみを使用しなければならない。

¶ 766 **FCS_SNI_EXT.1.3** TSF は、以下の方法で IV を生成しなければならない：[

¶ 767 CBC： IV は、繰り返ししてはならない。

¶ 768 CCM：ノンスは、繰り返してはならない。

¶ 769 XTS： IV はない。 Tweak 値は、連続的に割り付けられ、任意の負でない整数で開始する、負でない整数、でなければならない。

¶ 770 GCM： IV は繰り返してはならない。GCM の呼び出し回数は、所与の秘密鍵について 2^32 を超えてはならない。

¶ 771].

A.9.11 FCS_SSH_EXT　拡張：選択された SSH

¶ 772 **ファミリのふるまい：**

¶ 773 本ファミリは、SSH プロトコルを用いてクライアントとサーバの間でデータを保護するため、サーバ及び／またはクライアントが SSH を提供する能力に対処する。

¶ 774 **コンポーネントのレベル付け：**

FCS_SSH_EXT.1 拡張：選択された SSH	1

¶ 775 **FCS_SSH_EXT.1** 選択された SSH は、指定されたとおりに SSH プロトコルを実装することを要求する。

¶ 776 **管理：**

¶ 777 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 778 **監査：**

¶ 779 FAU_GEN セキュリティ監査データが PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- SSH セション確立の失敗

¶ 780 **FCS_SSH_EXT.1　　拡張：選択された SSH**

下位階層：　　なし

依存性：　　なし

¶ 781 **FCS_SSH_EXT.1.1**　TSF は、RFC 4251、4252、4253、4254、及び［選択：5656、6668、その他の RFC なし］に適合する SSH プロトコルを実装しなければならない。

¶ 782 **FCS_SSH_EXT.1.2**　TSF は、SSH プロトコル実装が RFC 4252 に記述されている次の認証方法をサポートしていることを保証しなければならない：公開鍵ベース、パスワードベース。

¶ 783 **FCS_SSH_EXT.1.3**　TSF は、RFC 4253 に記述されているように、SSH トランスポート接続における［割付：*バイト数*］以上のパケットが廃棄されることを保証しなければならない。

¶ 784 **FCS_SSH_EXT.1.4**　TSF は、SSH トランスポート実装が、以下の暗号アルゴリズムを使用することを保証しなければならない：AES-CBC-128、AES-CBC-256、［選択：AEAD_AES_128_GCM、 AEAD_AES_256_GCM、その他のアルゴリズムなし］。

¶ 785 **FCS_SSH_EXT.1.5**　TSF は、SSH トランスポート実装が、公開鍵アルゴリズムとして、［選択：SSH_RSA、ecdsa-sha2-nistp256］及び［選択：PGP-SIGN-RSA、PGP-SIGN-DSS、ecdsa-sha2-nistp384、その他の公開鍵アルゴリズムなし］を使用することを保証しなければならない。

¶ 786 **FCS_SSH_EXT.1.6**　TSF は、SSH トランスポート接続において使用されるデータ真正性アルゴリズムが［選択： *HMAC-SHA1*、*HMAC-SHA1-96*、*HMAC-SHA2-256*、*HMAC-SHA2-512*］であることを保証しなければならない。

¶ 787 **FCS_SSH_EXT.1.7**　TSF は、diffie-hellman-group14-sha1 及び［選択：*ecdh-sha2-nistp256*、 *ecdh-sha2-nistp384*、*ecdh-sha2-nistp521*、*その他の方法なし*］が、SSH プロトコルで使用される、唯一の許可された鍵交換方法であることを保証しなければならない。

¶ 788 **根拠：**

¶ 789 SSH は、セキュア通信プロトコルの一つである。コモンクライテリアは暗号アルゴリズムを用いた通信プロトコルに適した SFR を提供していない。

¶ 790 本拡張コンポーネントは、暗号アルゴリズムを用いて通信データを保護するので、FCS クラスの一つのコンポーネントとする。

A.9.12 FCS_TLS_EXT　拡張：選択された TLS

¶ 791 **ファミリのふるまい：**

¶ 792 本ファミリは、TLS プロトコルを用いてクライアントとサーバの間でデータを保護するため、サーバ及び／またはクライアントが TLS を提供する能力に対処する。

¶ 793 **コンポーネントのレベル付け：**

FCS_TLS_EXT.1 拡張：選択された TLS	1

¶ 794 **FCS_TLS_EXT.1** 選択された TLS は、指定されたとおりに TLS プロトコルを実装することを要求する。

¶ 795 **管理：**

¶ 796 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 797 **監査：**

¶ 798 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- TLS セション確立の失敗

¶ 799 **FCS_TLS_EXT.1　　拡張：選択された TLS**

下位階層：　　なし

依存性：　　なし

¶ 800 **FCS_TLS_EXT.1.1**　TSF は、以下の暗号スイートをサポートしている以下のプロトコルの一つ以上［選択：*TLS 1.0（RFC 2246）*、*TLS 1.1（RFC 4346）*、*TLS 1.2（RFC 5246）*］を実装しなければならない：

¶ 801 必須の暗号スイート：

- TLS_RSA_WITH_AES_128_CBC_SHA

¶ 802 オプションの暗号スイート：

¶ 803 [選択：

- *なし*
- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*

- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_ SHA256*
- *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*

]。

¶ *804* **根拠：**

¶ *805* TLS は、セキュア通信プロトコルの一つである。コモンクライテリアは暗号アルゴリズムを用いた通信プロトコルに適した SFR を提供していない。

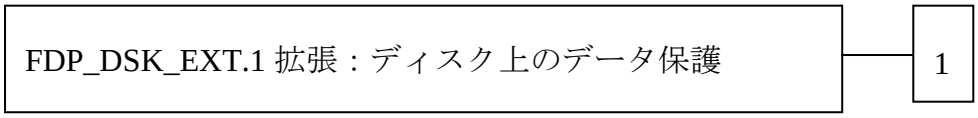
¶ *806* 本拡張コンポーネントは、暗号アルゴリズムを用いて通信データを保護するので、FCS クラスの一つのコンポーネントとする。

A.9.13 FDP_DSK_EXT　拡張：ディスク上のデータ保護

¶ *807* **ファミリのふるまい：**

¶ *808* 本ファミリは、ストレージに書き込まれたすべての保護されたデータの暗号化を義務付けるものである。

¶ *809* **コンポーネントのレベル付け：**



¶ *810* **FDP_DSK_EXT.1** 拡張：ディスク上のデータ保護は、現地交換可能な不揮発性ストレージデバイス上に秘密の TSF データまたは利用者データが平文で格納されないよう暗号化されることを要求する。

¶ 811 **管理：**

¶ 812 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 813 **監査：**

¶ 814 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 815 **FDP_DSK_EXT.1　　拡張：ディスク上のデータ保護**

下位階層：　　なし

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

¶ 816 **FDP_DSK_EXT.1.1**　TSF は、あらゆる現地交換可能な不揮発性ストレージデバイスが平文の利用者文書データ及び平文の秘密の TSF データを含んでいないように、[選択：FCS_COP.1(d)に従って暗号化を実行、*FDE EE cPP に適合した別の CC 認証された現地交換可能な自己暗号化不揮発性ストレージデバイスを使用*] しなければならない。

¶ 817 **FDP_DSK_EXT.1.2**　TSF は、利用者の介入なしにすべての保護データを暗号化しなければならない。

¶ 818 **根拠：**

¶ 819 拡張：ディスク上のデータ保護は、利用者の介入なしに秘密データの暗号化を指定するものである。コモンクライテリアは、ディスク上のデータ保護に適した SFR を提供していない。

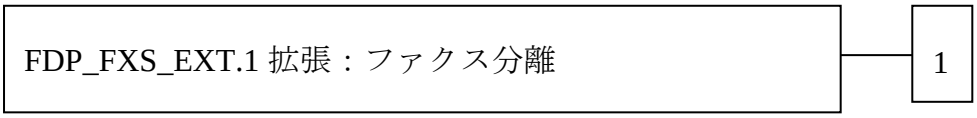
¶ 820 本拡張コンポーネントは、ディスク上のデータを保護するので、FDP クラスの一つのコンポーネントとする。

A.9.14 FDP_FXS_EXT　拡張：ファクス分離

¶ 821 **ファミリのふるまい：**

¶ 822 本ファミリは、TOE が接続される、ファクス PSTN 回線と LAN の間の分離に関する要件に対処する。

¶ 823 **コンポーネントのレベル付け：**



¶ 824 **FDP_FXS_EXT.1** ファクス分離は、TOE が接続される PSTN と LAN の間で、ネットワークブリッジを作るためにファクスインタフェースが利用できないことを要求する。

¶ 825 **管理：**

¶ 826 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 827 **監査：**

¶ 828 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 829 **FDP_FXS_EXT.1　拡張：ファクス分離**

下位階層：　なし

依存性：　なし

¶ 830 **FDP_FXS_EXT.1.1**　TSF は、ファクスプロトコルを用いた利用者データの送信または受信を除き、ファクスインタフェース経由の通信を禁止しなければならない。

¶ 831 **根拠：**

¶ 832 ファクス分離は、PSTN 回線からの攻撃に対して LAN を保護するものである。コモンクライテリアは、TSF または利用者データの保護に適した SFR を提供していない。

¶ 833 本拡張コンポーネントは、TSF データまたは利用者データを保護するので、FDP クラスの一つのコンポーネントとする。

A.9.15 FIA_PMG_EXT　拡張：パスワード管理

¶ 834 **ファミリのふるまい：**

¶ 835 本ファミリは、強度のあるパスワードとパスフレーズが選択され、維持されることを保証するための、管理者によって使用されるパスワード属性についての要件を定義する。

¶ 836 **コンポーネントのレベル付け：**

¶ 837 **FIA_PMG _EXT.1** パスワード管理は、TSF が、最小の長さ、最大のライフタイム、類似性の制限等のさまざまな作成要件を伴うパスワードをサポートすることを要求する。

¶ 838 **管理：**

¶ 839 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 840 **監査：**

¶ 841 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 842 **FIA_PMG _EXT.1　拡張：パスワード管理**

下位階層：　なし

依存性：　なし

¶ 843 **FIA_PMG _EXT.1.1** TSF は、利用者パスワードとして、次のパスワード管理機能を提供しなければならない：

- パスワードは、アルファベットの大文字と小文字、数字、及び次の特殊文字：[選択：“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [割付：その他の文字]]の組み合わせから作成可能でなければならない；
- 最少パスワード長は、**管理者**によって設定可能なければならない、かつ 15 文字以上のパスワードを要求する能力を持っていなければならない。

¶ 844 **根拠：**

¶ 845 パスワード管理は、通信の端点間の強い認証を保証するものである。コモン

クライテリアは、パスワード管理に適した SFR を提供していない。

¶ 846 本拡張コンポーネントは、パスワード管理の手段により TOE を保護するので、FIA クラスの一つのコンポーネントとする。

A.9.16 FIA_PSK_EXT　拡張：事前共有鍵生成

¶ 847 **ファミリのふるまい：**

¶ 848 本ファミリは、TSF が IPsec 用の事前共有鍵を使用できることを保証するための要件を定義する。

¶ 849 **コンポーネントのレベル付け：**

FIA_PSK_EXT.1 拡張：事前共有鍵生成	1

¶ 850 **FIA_PSK_EXT.1** 事前共有鍵生成は、IPsec 用の事前共有鍵を使用できることを保証する。

¶ 851 **管理：**

¶ 852 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 853 **監査：**

¶ 854 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 855 **FIA_PSK_EXT.1**　　拡張：事前共有鍵生成

下位階層：　　なし

依存性：　　FCS_RBG_EXT.1 拡張：暗号操作（乱数ビット生成）.

¶ 856 **FIA_PSK_EXT.1.1**　TSF は、IPsec 用の事前共有鍵を使用できなければならない。

¶ 857 **FIA_PSK_EXT.1.2**　TSF は、以下のようなテキストベースの事前共有鍵を許容できなければならない：

- 長さが 22 文字及び［選択：［割付：その他のサポートされた長さ］、そ

の他の長さなし］；

- 大文字、小文字、数字、及び（「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」、及び「)」を含む）特殊文字の組み合わせから作られる。

¶ 858 **FIA_PSK_EXT.1.3**　TSF は、［選択：SHA-1、SHA-256、SHA-512、［割付：テキスト文字列の調整方法］］を用いて、テキストベースの事前共有鍵を調整しなければならず、［選択：他の事前共有鍵を使用しない；ビットベースの事前共有鍵を受容する；FCS_RBG_EXT.1 で指定された乱数ビット生成器を用いてビットベースの事前共有鍵を生成する］ことができなければならない。

¶ 859 **根拠：**

¶ 860 事前共有鍵は、通信の端点間で強い認証を保証するものである。コモンクライテリアは、事前共有鍵生成に適した SFR を提供していない。

¶ 861 本拡張コンポーネントは、強い認証手段により TOE を保護するので、FIA クラスの一つのコンポーネントとする。

A.9.17 FPT_KYP_EXT　拡張：鍵及び鍵材料の保護

¶ 862 **ファミリのふるまい：**

¶ 863 本ファミリは、不揮発性ストレージに書き込まれた鍵及び鍵材料が保護されるための要件に対処する。

¶ 864 **コンポーネントのレベル付け：**

¶ 865

FPT_ KYP _EXT.1 拡張：鍵及び鍵材料の保護	1

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

¶ 867 **管理：**

¶ 868 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 869 **監査：**

¶ 870 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 871 **FPT_ KYP _EXT.1　拡張：鍵及び鍵材料の保護**

下位階層：　　なし

依存性：　　なし

¶ 872 **FPT_KYP_EXT.1.1**　TSF は、FCS_KYC_EXT.1 で特定される鍵チェインの一部であるような平文の鍵をあらゆる現地交換可能な不揮発性ストレージデバイスに保存してはならず、またそのデバイスの暗号化用に使用される平文のあらゆる鍵がデバイス上に保存されてはならない。

¶ 873 **根拠：**

¶ 874 鍵及び鍵材料の保護は、鍵及び鍵材料が平文で不揮発性ストレージに書き込まれないことを保証するものである。コモンクライテリアは、鍵及び鍵材料の保護に適した SFR を提供していない。

¶ 875 本拡張コンポーネントは、TSF データを保護するので、FPT クラスの一つのコンポーネントとする。

A.9.18 FPT_SKP_EXT　拡張： TSF データの保護

¶ 876 **ファミリのふるまい：**

¶ 877 本ファミリは、暗号鍵のような、TSF データを管理保護するための要件に対処する。これは、FPT クラスとしてモデル化された新しいファミリである。

¶ 878 **コンポーネントのレベル付け：**

¶ 879 **FPT_SKP_EXT.1**　TSF データの保護(すべての対称鍵の読み出し用)は、対称鍵があらゆる利用者またはサブジェクトにより読み出しの防止を要求する。本ファミリの唯一のコンポーネントである。

¶ 880 **管理：**

¶ 881 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 882 **監査：**

¶ 883 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 884 **FPT_SKP_EXT.1**　拡張：TSF データの保護

下位階層：　なし

依存性：　なし

¶ 885 **FPT_SKP_EXT.1.1**　TSF は、すべての事前共有鍵、対称鍵、及びプライベート鍵の読み出しを防止しなければならない。

¶ 886 **根拠：**

¶ 887 TSF データの保護は、事前共有鍵、対称鍵、プライベート鍵がセキュアに保護されることを保証する。コモンクライテリアは、このような TSF データの保護に適した SFR を提供していない。

¶ 888 本拡張コンポーネントは事前共有鍵を用いた強い認証手段により TOE を保護するので、FPT クラスの一つのコンポーネントとする。

A.9.19 FPT_TST_EXT　拡張：TSF テスト

¶ 889 **ファミリのふるまい：**

¶ 890 本ファミリは、選択された正しい動作についての TSF の自己テスト要件に対処する。

¶ 891 **コンポーネントのレベル付け：**

¶ 892 **FPT_TST_EXT.1** TSF テストは、TSF が正しく動作することを実証するために、初期起動時に動作する自己テストのスイートを要求する。

¶ 893 **管理：**

¶ 894 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 895 **監査：**

¶ 896 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 897 **FPT_TST_EXT.1　　拡張：TSF テスト**

下位階層：　　なし

依存性：　　なし

¶ 898 **FPT_TST_EXT.1.1**　TSF は、TSF の正常動作を実証するため、初期起動時（及び電源投入時）に、自己テストのスイートを実行しなければならない。

¶ 899 **根拠：**

¶ 900 TSF テストは、TSF が正しく動作できることを保証するものである。コモンクライテリアは、TSF テストに適した SFR を提供していない。特に、TSF テスト用に定義した SFR はない。

¶ 901 本拡張コンポーネントは、TOE を保護するので、FPT クラスの一つのコンポーネントとする。

A.9.20 FPT_TUD_EXT　拡張：高信頼アップデート

¶ 902 **ファミリのふるまい：**

¶ 903 本ファミリは、管理者のみが TOE のファームウェア／ソフトウェアをアップデートできること、及びこのようなファームウェア・ソフトウェアが本物であることを TSF が保証するための要件を定義する。

¶ 904 **コンポーネントのレベル付け：**

FPT_TUD_EXT.1 拡張：高信頼アップデート	1

¶ 905 **FPT_TUD_EXT.1** 拡張：高信頼アップデートは、アップデートの真正性とアクセス制御を保証する。

¶ 906 **管理：**

¶ 907 以下のアクションは FMT における管理機能と考えられる：

- 予見される管理アクションはない。

¶ 908 **監査：**

¶ 909 FAU_GEN セキュリティ監査データ生成が PP/ST に含まれている場合、以下のアクションは、監査対象にするべきである：

- 予見される監査対象事象はない。

¶ 910 **FPT_TUD_EXT.1** 拡張：高信頼アップデート

下位階層：　なし

依存性：　[FCS_COP.1(b)　暗号操作(署名生成／検証)、または
FCS_COP.1(c)　暗号操作(ハッシュアルゴリズム)]

¶ 911 **FPT_TUD_EXT.1.1**　TSF は、許可された管理者に TOE のファームウェア／ソフトウェアの現在のバージョンを問い合わせる能力を提供しなければならない。

¶ 912 **FPT_TUD_EXT.1.2**　TSF は、許可された管理者に TOE のファームウェア／ソフトウェアへのアップデートを開始する能力を提供しなければならない。

¶ 913 **FPT_TUD_EXT.1.3** TSF は、それらのアップデートをインストールする前に、デジタル署名メカニズムと［選択：*公開ハッシュ*、*他の機能なし*］を用いて TOE へのファームウェア／ソフトウェアのアップデートを検証する手段を提供しなければならない。

¶ 914 **根拠：**

¶ 915 ファームウェア／ソフトウェアは、TSF データの形式であり、コモンクライテリアは、ファームウェア／ソフトウェアの管理に適した SFR を提供していない。特に、TSF データをインポートするために定義した SFR はない。

¶ 916 本拡張コンポーネントは、TOE を保護するので、FPT クラスの一つのコンポーネントとする。

A.10 セキュリティ機能要件根拠表

表 16　セキュリティ機能要件の完全性

¶ 917　*凡例：

¶ 918　**R=必須**

¶ 919　**C=条件付き必須**

¶ 920　**O=オプション**

¶ 921　**S=選択**

¶ 922　**U=他の SFR への支援を行う SFR**

SFR: / Objective:	O.ACCESS_CONTROL	O.ADMIN_ROLES	O.AUDIT	O.COMMS_PROTECTION	O.FAX_NET_SEPARATION	O.IMAGE_OVERWRITE	O.KEY_MATERIAL	O.PURGE_DATA	O.STORAGE_ENCRYPTION	O.TSF_SELF_TEST	O.UPDATE_VERIFICATION	O.USER_AUTHORIZATION	O.USER_I&A
FAU_GEN.1			R										
FAU_GEN.2			R										
FAU_SAR.1			O										
FAU_SAR.2			O										
FAU_STG.1			O										
FAU_STG.4			O										
FAU_STG_EXT.1			R										
FCS_CKM.1(a)				R									
FCS_CKM.1(b)				R					S				
FCS_CKM.4				U				O	U				
FCS_CKM_EXT.4				U				O	U				
FCS_COP.1(a)				R									
FCS_COP.1(b)				S							S		
FCS_COP.1(c)									U		S		
FCS_COP.1(d)									U				
FCS_COP.1(e)									U				
FCS_COP.1(f)									U				
FCS_COP.1(g)				S									

SFR: / Objective:	O.ACCESS_CONTROL	O.ADMIN_ROLES	O.AUDIT	O.COMMS_PROTECTION	O.FAX_NET_SEPARATION	O.IMAGE_OVERWRITE	O.KEY_MATERIAL	O.PURGE_DATA	O.STORAGE_ENCRYPTION	O.TSF_SELF_TEST	O.UPDATE_VERIFICATION	O.USER_AUTHORIZATION	O.USER_I&A
FCS_COP.1(h)									O				
FCS_COP.1(i)									U				
FCS_HTTPS_EXT.1				S									
FCS_IPSEC_EXT.1				S									
FCS_KDF_EXT.1									O				
FCS_KYC_EXT.1									C				
FCS_PCC_EXT.1									O				
FCS_RBG_EXT.1				U					U				
FCS_SMC_EXT.1									S				
FCS_SNI_EXT.1									S				
FCS_SSH_EXT.1				S									
FCS_TLS_EXT.1				S									
FDP_ACC.1	R											R	
FDP_ACF.1	R											R	
FDP_DSK_EXT.1									C				
FDP_FXS_EXT.1					C								
FDP_RIP.1(a)						O							
FDP_RIP.1(b)								O					
FIA_AFL.1													U
FIA_ATD.1												U	
FIA_PMG_EXT.1													R
FIA_PSK_EXT.1				S									
FIA_UAU.1													R
FIA_UAU.7													R
FIA_UID.1		U											R
FIA_USB.1													R
FMT_MOF.1		R											
FMT_MSA.1	U											R	
FMT_MSA.3	U											R	
FMT_MTD.1	U												

SFR: / Objective:	O.ACCESS_CONTROL	O.ADMIN_ROLES	O.AUDIT	O.COMMS_PROTECTION	O.FAX_NET_SEPARATION	O.IMAGE_OVERWRITE	O.KEY_MATERIAL	O.PURGE_DATA	O.STORAGE_ENCRYPTION	O.TSF_SELF_TEST	O.UPDATE_VERIFICATION	O.USER_AUTHORIZATION	O.USER_I&A
FMT_SMF.1	U	R										R	
FMT_SMR.1	U	R										R	
FPT_KYP_EXT.1							C						
FPT_SKP_EXT.1				R									
FPT_STM.1			U										
FPT_TST_EXT.1										R			
FPT_TUD_EXT.1											R		
FTA_SSL.3													R
FTP_ITC.1			U	R									
FTP_TRP.1(a)				R									
FTP_TRP.1(b)				R									

表 17　セキュリティ機能要件根拠

Objective / SFR	Relationship	Rationale
O.ACCESS_CONTROL – **TOE はセキュリティ方針に従い利用者データと TSF データを保護するためアクセス制御を実施しなければならない。**		
FDP_ACC.1	Satisfies	本 SFR は、利用者データ及び TSF データへのアクセスを保護するために使用されるアクセス制御方針を定義する。
FDP_ACF.1	Satisfies	本 SFR は、資源、機能データへのアクセスが許可されまたは拒否される条件を識別し、アクセス制御方針を構成する特定の規則集を定義する。
FMT_MSA.1	Supports	製品の構成管理、セキュリティ設定、及び利用者属性や権限付与が運用セキュリティの維持に重要である。このような管理機能
FMT_MSA.3	Supports	
FMT_MTD.1	Supports	

FMT_SMF.1	Supports	は、グループとして、許可された管理者がシステムを設定する能力を提供し、利用者を追加及び削除し、システムデータ、資源、及び機能への利用者ごとの権限付与を与え、システムへプログラムコード（例、アップデート）を導入し、利用者役割を割付す。さらに、SFR は管理機能が管理機能を実行する権限を明示的に許可された利用者に限定することを要求する。
FMT_SMR.1	Supports	
O.ADMIN_ROLES – **TOE は許可された管理者のみに管理者機能の実行を許可することを保証しなければならない。**		
FIA_UID.1	Supports	本 SFR は、管理者権限付与を要求することなしにアクセスできるような TOE 管理機能を定義する。
FMT_MOF.1	Satisfies	本 SFR は、管理者が TOE の機能にアクセスするために要求される権限付与を定義する。
FMT_SMF.1	Satisfies	本 SFR は、TSF により提供される管理機能を定義する。
FMT_SMR.1	Satisfies	本 SFR は、管理者に認証と権限付与を決定するために割り付けることが可能な異なる役割を定義する。
O.COMMS_PROTECTION – **TOE は、利用者データ及び TSF データの LAN 通信を不正なアクセス、リプレイ、及び発信元／宛先なりすましから保護する能力を持たなければならない。**		
FCS_CKM.1(a)	Satisfies	本 SFR は、保護された通信中の鍵配送用に使用可能な鍵ペア生成のセキュアなアルゴリズムの使用を定義する。
FCS_CKM.1(b)	Satisfies	本 SFR は、通信保護用に使用可能な鍵生成用のセキュアなアルゴリズムの使用を定義する。
FCS_CKM.4	Supports	本 SFR は、消去する必要がある暗号鍵が復元できないことの保証を提供する FCS_CKM_EXT.4 で使用されるデータ消去方式を定義する。
FCS_CKM_EXT.4	Supports	本 SFR は、残存暗号データが保護された通信を侵害するために使用できないことを保証する。
FCS_COP.1(a)	Satisfies	本 SFR は、保護された通信で使用可能なセキュアな対称鍵アルゴリズムの使用を定義する。
FCS_COP.1(g)	Selection	本 SFR は、保護された通信で使用可能なセキュアな HMAC アルゴリズムの使用を定義する。
FCS_HTTPS_EXT.1	Selection	これらの SFR は、セキュリティ関連データ

FCS_IPSEC_EXT.1	Selection	の送信を保護するために使用可能なセキュアな通信プロトコルを定義する。
FCS_RBG_EXT.1	Supports	本 SFR は、理論的な最大強度を以て暗号機能を操作することを可能とする乱数ビット生成のセキュアな方法を定義することにより保護された通信をサポートする。
FCS_SSH_EXT.1	Selection	これらの SFR は、セキュリティ関連データの送信を保護するために使用可能なセキュアな通信プロトコルを定義する。
FCS_TLS_EXT.1	Selection	
FIA_PSK_EXT.1	Selection	本 SFR は、プロトコルのセキュアな実装を可能とする IPsec での事前共有鍵の使用を定義する。
FPT_SKP_EXT.1	Satisfies	本 SFR は、秘密暗号データが不正なアクセスから保護されることを保証することにより、保護された通信の侵害を防止する。
FTP_ITC.1	Satisfies	本 SFR は、保護された通信が要求されるインタフェース、及びそのインタフェースで送信するために使用される通信を保護するために使用される方法を定義する。
FTP_TRP.1(a)	Satisfies	本 SFR は、TOE との管理者対話をセキュアにするために使用される保護された通信パスを定義する。
FTP_TRP.1(b)	Satisfies	本 SFR は、TOE との利用者対話をセキュアにするために使用される保護された通信パスを定義する。
O.FAX_NET_SEPARATION(条件付き必須) – **TOE が PSTN ファクス機能を提供する場合、TOE は、PSTN ファクス電話回線と LAN の間の分離をシステム設計または能動的なセキュリティ機能により保証しなければならない。**		
FDP_FXS_EXT.1	Satisfies	本 SFR は、ファクス通信以外のすべての本インタフェースの使用を防止することでファクスインタフェースの分離を実施する。
O.IMAGE_OVERWRITE(オプション) **- 文書処理ジョブの完了または中止において、TOE は現地交換可能な不揮発性ストレージデバイスから残存画像データを上書き消去しなければならない。**		
FDP_RIP.1(a)	Satisfies	本 SFR は、利用者文書データのメモリ割当解除に際して文書データを上書き消去する TSF の能力を定義する。
O.KEY_MATERIAL(条件付き必須) – **TOE は、現地交換可能な不揮発性ストレージデバイスの利用者文書データ又は機密の TSF データを格納するための暗号鍵の生成に寄与するあらゆる平文の鍵、サブマスク、乱数又はその他の値を、不正アクセスから保護しなければならない；TOE は、そのような鍵材料が、その材料を使用するストレージデバイス上に平文で格納されないことを保証しなければならない。**		
FPT_KYP_EXT.1	Satisfies	本 SFR は、セキュアでない場所に保護されていない鍵データを保存することから防止する TSF の能力を定義する

O.PURGE_DATA(オプション) – **TOE は、許可された管理者がすべての顧客が提供した利用者データ及び TSF データが不揮発性ストレージデバイスから永久に取り出せないように起動すること可能な機能を提供する。**		
FCS_CKM.4	Satisfies	本 SFR は、FCS_CKM_EXT.4 で定義されたデータ完全消去を達成するために使用される物理的メカニズムを定義する。
FCS_CKM_EXT.4	Satisfies	本 SFR は、ストレージからデータを完全消去するための TSF の能力を定義する。
FDP_RIP.1(b)	Satisfies	本 TSF は、廃棄プロセスの一部としてすべての利用者データ及び TSF データを完全消去することを TSF に要求する。
O.STORAGE_ENCRYPTION(条件付き必須) – **TOE が利用者文書データまたは秘密の TSF データを現地交換可能な不揮発性ストレージデバイスに保存する場合、TOE は、それらのデバイス上のこのようなデータを暗号化しなければならない。**		
FCS_CKM.1(b)	Selection	本 SFR は、ストレージ暗号化で使用できる鍵生成のアルゴリズムを定義する。
FCS_CKM.4	Supports	本 SFR は、TOE から分離されたストレージデバイスの保存データが復元できないことを保証するため暗号鍵の適切な破棄に関する要件の定義を支援する。
FCS_CKM_EXT.4	Supports	本 SFR は、TOE から分離されたストレージデバイスの保存データが復元できないことを保証するため暗号鍵の適切な破棄に関する要件の定義を支援する。
FCS_COP.1(c)	Supports	本 SFR は、ユーザフレンドリーな方法で保存データを暗号化するための入力文字列をとしてより短いものを使用して強い暗号鍵を生成する能力を提供する。
FCS_COP.1(d)	Supports	本 SFR は保存データを保護するために使用されるデータ暗号アルゴリズムを定義する。
FCS_COP.1(e)	Supports	本 SFR は、保全データを暗号化する対称鍵をセキュアにするために使用される鍵ラップアルゴリズムを定義する。
FCS_COP.1(f)	Supports	本 SFR は、保全データを暗号化する対称鍵をセキュアにするために使用される鍵暗号化アルゴリズムを定義する。
FCS_COP.1(h)	Option	本 SFR は、鍵付ハッシュメッセージ認証で使用される暗号アルゴリズムを定義する。
FCS_COP.1(i)	Supports	本 SFR は、鍵配送用に使用される鍵配送アルゴリズムを定義する。
FCS_KDF_EXT.1	Option	本 SFR は、不正な暴露にさらされないような方法で鍵が生成されることを保証するため、TOE により使用される鍵導出関数を定義する。

FCS_KYC_EXT.1	Satisfies	本 SFR は、鍵材料の多階層セキュリティを提供するため、TOE により使用される鍵チェイニング方法を定義する。
FCS_PCC_EXT.1	Option	本 SFR は、パスワードデータを生成し、条件づけるために使用されるパスワードベース鍵導出関数を定義する。
FCS_RBG_EXT.1	Supports	本 SFR は、TOE の暗号アルゴリズムが理論的最大レベルのセキュリティで機能することを保証するために使用される乱数ビット生成アルゴリズムを定義する。
FCS_SNI_EXT.1	Selection	本 SFR は、暗号アルゴリズムが理論的最大強度で動作することを保証するために、ソルト、ノンス、及び初期化ベクトルに関するセキュアなパラメタ及び方法を定義する。
FCS_SMC_EXT.1	Selection	本 SFR は、BEV を保護するために使用されるサブマスクを結合する適切な方法を定義する。
FDP_DSK_EXT.1	Satisfies	本 SFR は、ディスクへ保存されるデータを暗号化することを TSF に要求する。
O.AUDIT - **TOE は、監査データを生成しなければならない、またそれを信頼される外部 IT エンティティへ送信する能力を持たなければならない。オプションとして、監査データを TOE に保存してもよい。**		
FAU_GEN.1	Satisfies	本 SFR は、TOE が監査データを生成し、各監査記録に含まれるフィールドを生成するための監査対象事象を定義する。
FAU_GEN.2	Satisfies	本 SFR は、利用者または管理者により実行されるすべてのアクティビティの帰属に適用する TOE の能力を定義する。
FAU_SAR.1	Option	本 SFR は、TOE に保存される監査データを読み出すための管理者の能力を定義する。
FAU_SAR.2	Option	本 SFR は、保存された監査データを不正なアクセスから保護する。
FAU_STG.1	Option	本 SFR は、監査データが信頼されないサブジェクトにより改変不可能であることを保証する。
FAU_STG.4	Option	本 SFR は、監査ストレージ空間が総当たり攻撃を受けるような事象に自動的に対処することにより監査データの可用性を保証する。
FAU_STG_EXT.1	Satisfies	本 SFR は、保護されたチャネルを用いて生成された監査データを外部 IT エンティティへ送信するための TSF の能力を定義する。
FPT_STM.1	Supports	本 SFR は、監査データが正しいタイムスタンプでラベル付けされていることを保証す

		る。
FTP_ITC.1	Supports	本 SFR は、監査データの送信が可能な保護された通信チャネルを定義する。
O.TSF_SELF_TEST – **TOE は、セキュリティ機能のサブセットが適切に動作していることを保証する支援のため、セキュリティ機能のいくつかのサブセットをテストしなければならない。**		
FPT_TST_EXT.1	Satisfies	本 SFR は、TOE にセキュリティ特性を主張する自己テストを実行する TSF の能力を定義する。
O.UPDATE_VERIFICATION – **TOE は、ソフトウェアアップデートの真正性を検証するメカニズムを提供しなければならない。**		
FCS_COP.1(b)	Selection	本 SFR は、TOE アップデートの真正性を検証するために使用されるデジタル署名サービスを定義する。
FCS_COP.1(c)	Selection	本 SFR は、TOE アップデートが改ざんされていないことを検証するために使用されるハッシュアルゴリズムを定義する。
FPT_TUD_EXT.1	Satisfies	本 SFR は、アップデートされる TOE の能力とアップデートが信頼されると知られている方法を定義する。
O.USER_AUTHORIZATION – **TOE はセキュリティ方針に従い利用者の権限付与を実行しなければならない。**		
FDP_ACC.1	Supports	本 SFR は、利用者の権限付与に従い、サブジェクト、オブジェクト、及び操作に関して利用者アクセス制御 SFP を実施する。
FDP_ACF.1	Supports	本 SFR は、利用者の権限付与に従い、属性に基づくオブジェクトに対する利用者アクセス制御 SFP を実施する。
FIA_ATD.1	Supports	本 SFR は、権限付与を定義するために使用可能な利用者に関連する属性を定義する。
FMT_MSA.1	Satisfies	本 SFR は、TSF により保護されているデータをアクセスするために要求される権限付与を定義する。
FMT_MSA.3	Satisfies	本 SFR は、TSF により保護されているデータのアクセスを支配するアクセス制御方針の実施のためのデフォルトセキュリティ属性を定義する。
FMT_SMF.1	Satisfies	本 SFR は、利用者権限付与を定義するために使用可能な TOE により提供される管理機能を定義する。
FMT_SMR.1	Satisfies	本 SFR は、利用者のグループへの権限付与を定義するために使用可能な管理者役割を定義する。
O.USER_I&A – **TOE は、アクセス制御、利用者権限付与、または管理者役割を要求する操作について、利用者の識別と認証を実行しなければならない。**		

FIA_AFL.1	Supports	本 SFR は、起こりうる不正な認証の試行回数を制限することにより、なりすましの可能性を減らし、認証機能を保護する。
FIA_PMG_EXT.1	Satisfies	本 SFR は、推測又は導出しにくい強いクレデンシャル(認証情報)を提供することで認証機能を保護する。
FIA_UAU.1	Satisfies	本 SFR は、認証せずに実行できる TOE 機能及び使用に際して認証が求められる機能を定義する。
FIA_UAU.7	Satisfies	本 SFR は、入力中の認証クレデンシャルを隠すことで認証機能を保護する。
FIA_UID.1	Satisfies	本 SFR は、識別なしに実行できる TOE 機能及び使用に際して識別を求められる機能を定義する。
FIA_USB.1	Satisfies	本 SFR は、識別された利用者が TOE への認証成功時に TSF への権限付与を支配する属性に関連していることの保証を提供する。
FTA_SSL.3	Satisfies	本 SFR は、利用者または管理者が意図しないセション終了によるなりすましの防止を支援する。

附属書 B 条件付き必須要件

¶ 923 TOE の構成がセクション 1.3.1.2 に指定された条件を満たす場合、次のセキュリティ機能要件は必須となる。

B.1 現地交換可能な不揮発性ストレージデバイス上の秘密のデータ

B.1.1 FPT_KYP_EXT.1 拡張：鍵及び鍵材料の保護

(O.KEY_MATERIAL)
下位階層： なし
依存性： なし

¶ 924 **FPT_KYP_EXT.1.1** TSF は、**あらゆる現地交換可能な不揮発性ストレージデバイス**に FCS_KYC_EXT.1 で特定される鍵チェインの一部である平文の鍵を保存してはならない。

¶ 925 **保証アクティビティ：**

¶ 926 ***KMD：***

¶ 927 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用いる方法の記述について、鍵管理記述（KMD：訳注「Key Management Description」）を検査しなければならない。

¶ 928 評価者は、不揮発性メモリに保存されるすべての鍵の保存場所と保護について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。

B.1.2 FCS_KYC_EXT.1 拡張：鍵チェイニング

(O.STORAGE_ENCRYPTION)
下位階層： なし
依存性： [FCS_COP.1(e) 暗号操作（鍵ラッピング）、
FCS_SMC_EXT.1 拡張：サブマスク結合、
FCS_COP.1(f) 暗号操作（鍵暗号化）、
FCS_KDF_EXT.1 暗号操作(鍵導出)、
及び／または
FCS_COP.1(i) 暗号操作（鍵配送）]

¶ 929 ***適用上の注釈：***

¶ 930 *本 SFR は、DEK または SED (自己暗号化ドライブ) をロック解除するための BEV のいずれかで終端する鍵チェインを形成する。パスワードが使用されない場合、鍵の保護を提供する DEK または BEV を形成する中間鍵のない一つの鍵チェインであってもよい。例えば、SED の DEK が SED に保存されず、電源起動時に解放される場合、一つの鍵チェインは許容される。*

¶ 931 **FCS_KYC_EXT.1.1** TSF は、[選択：一つ、 *BEV または DEK としてサブマスクを使用するもの；以下の方法を用いて BEV または DEK へ一つまたはそれ以上のサブマスクから生成する中間鍵：*[選択： *FCS_COP.1(e) で指定される鍵ラッピング、FCS_SMC_EXT.1 で指定される鍵結合 (key combining)、FCS_COP.1(f) で指定される鍵暗号化 (key encryption)、FCS_KDF_EXT.1 で指定される鍵導出 (key derivation)、FCS_COP.1(i) で指定される鍵配送 (key transport)*]]の鍵チェインを維持しなければならない。ここで、[選択：*128 ビット、256 ビット*]の有効な強度を維持すること。

¶ 932 ***適用上の注釈：***

¶ 933 *鍵チェイニングは、BEV（境界暗号化値）を究極的にセキュアにするため、暗号鍵の多層化を用いる方法である。中間鍵の数は、一つから多数へと（例えば、調整されたパスワード許可要素を用いたり、それを直接 BEV として用いたり）変わる。これがすべての鍵に適用され、BEV をラッピングまたは導出するために寄与する；保護されたストレージの領域におけるそれらを含めて（例えば、TPM 保存される鍵、比較値）。*

¶ 934 *BEV への多段の鍵チェインは、鍵チェイン要件を満たす限り、許容される。*

¶ 935 *一度、ST 作成者が鍵チェイン（ラッピングを解く、または暗号化鍵のいずれかによって）を作成する方法を選択したなら、それらは、本附属書から適切な要件を取り込む。いずれかまたはすべての方法を使用するような実装が許容される。*

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

¶ 937 保証アクティビティ

¶ 938 ***TSS：***

¶ 939 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 の長さについての高レベルの記述を TSS が含んでいることを検証しなければならない。

¶ 940 ***KMD：***

¶ 941 評価者は、すべての受け入れられる BEV に関する鍵階層の高レベル記述が 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。評価者は、鍵チェインの詳細が KMD に記述されていることを検査しなければならない。鍵チェインの記述は、鍵ラップ、サブマスク結合、または鍵暗号化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。

¶ 942 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危殆化されないことが 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。（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認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 Key Chain 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。

¶ 943 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。

B.1.3 FDP_DSK_EXT.1　拡張：ディスク上のデータ保護

(O.STORAGE_ENCRYPTION)
下位階層：　なし
依存性：　FCS_COP.1(d) 暗号操作(AES データ暗号化／復号)

¶ 944 **FDP_DSK_EXT.1.1**　TSF は、あらゆる**現地交換可能な不揮発性ストレージデバイス**が平文の**利用者文書データ及び平文の秘密の TSF データを含んでいない**ように、［選択：**FCS_COP.1(d)に従って暗号化を実行、FDE EE cPP に適合した別の CC 認証された現地交換可能な自己暗号化不揮発性ストレージデバイスを使用**］しなければならない。

¶ 945 ***適用上の注釈：***

¶ 946 *自己暗号化デバイスオプションが選択された場合、デバイスは現在のディスク全体暗号化プロテクションプロファイルに適合した評価を受けなければならない。ST 作成者は、承認されたプロテクションプロファイルについてCC スキームに相談するべきである。*

¶ 947 **FDP_DSK_EXT.1.2**　TSF は、利用者の介入なしにすべての保護データを暗号化しなければならない。

¶ 948 ***適用上の注釈：***

¶ 949 *本要件の意図は、あらゆる秘密のデータの暗号化がそのデータを保護するために利用者の選択に依存しないよう指定することである。FDP_DSK_EXT.1 で指定された暗号化は利用者に対して透過的に発生し、データを保護するための決定は利用者の裁量の範囲外である。*

¶ 950 **保証アクティビティ：**

¶ 951 以下の保証アクティビティにおいて、「デバイス」は、FDP_DSK_EXT.1 からの現地交換可能な不揮発性ストレージデバイスを参照する。TOE が一つよりも多い適用可能なデバイスを持つ場合、保証アクティビティはそれぞれのデバイスについて必ず実行されること。

¶ 952 ***TSS：***

¶ 953 評価者は、どのようにデータがデバイスに書かれるか、及び暗号化機能が適用される点について、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。

¶ 954 運用環境により提供される暗号機能について、評価者は本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、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。

¶ 955 評価者は、TOE の出荷時、あるいは利用者または管理者が最初にデバイスを設定する時に、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に TOE が実行するアクティビティによるデバイスの初期化について 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、暗号化されないデバイスの領域（例えば、秘密データを含まない部分、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。

TOE が複数のデバイス暗号化をサポートする場合、評価者は、すべてのデバイスを暗号化する初期化手続きを保証するため、管理者ガイダンスを検査しなければならない。

¶ 956 ***操作ガイダンス：***

¶ 957 評価者は、必要とされる予備的なあらゆる手順を含めて、デバイス暗号化機能を有効化するために必要な初期手順について記述されていることを決定するため、AGD をレビューしなければならない。ガイダンスは、暗号化を有効化するときまたは TOE の出荷時にすべてのデバイスが暗号化されることを保証するために十分な指示を提供しなければならない。

¶ 958 ***KMD：***

¶ 959 評価者は、データ暗号化エンジン、その構成品、実装（例えば、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（可能であれば）、暗号／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））についての詳細情報が、KMD に含まれていることを検証しなければならない。評価者は、主たる構成品（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。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。評価者は、ハードウェア暗号化の図がデータパス内の主たる構成品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識別していることを検証しなければならない。

¶ 960 評価者は、暗号化が有効化される時、TOE がすべての適用可能なデバイスを暗号化することを保証するために十分な指示を KMD が提供していることを検証しなければならない。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。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。

¶ 961 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。暗号化が有効化及び無効化され得る場合、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。評価者は、ソフトウェア開発者が暗号化されたドライブの検査をインバウンド、アウトバウンド（訳注：ストレージデバイスに対する制御用の経路とデータ用の経路を同じ経路で行う方式、及び別々の経路で行う方式）のいずれかで許可するような、及び既知の鍵でセットアップできるような特殊なツールを提供することを保証しなければならない。

¶ 962 *テスト：*

¶ 963 評価者は、次のテストを実行しなければならない：

¶ 964 テスト　1.　ストレージデバイスへデータを書き込む：利用者文書及び秘密の TSF データの書き込み処理を実施する TSFI を操作してストレージデバイスに書き込みを実行する。

¶ 965 テスト　2.　書き込んだデータが暗号化されていることを確認する：テスト 1 で書き込まれた暗号化された範囲に平文のデータが存在しないことを検証する；そして、適切な鍵及び鍵材料によりそのデータが復号されることを検証する。

¶ 966 利用者文書データ及び秘密の TSF データの書き込み用のすべての TSFI は上記テスト 1 及びテスト 2 によりテストされるべきである。

B.2　PSTN ファクス − ネットワーク間の分離

B.2.1 FDP_FXS_EXT.1　拡張：ファクス分離

(O.FAX_NET_SEPARATION)
下位階層：　なし
依存性：　なし

¶ 967 **FDP_FXS_EXT.1.1**　TSF は、ファクスプロトコルを用いた利用者データの送

信または受信を除き、ファクスインタフェース経由の通信を禁止しなければならない。

¶ 968 ***適用上の注釈：***

¶ 969 *FDP_FXS_EXT.1 は、ファクス-ネット分離が TSF によって実行される場合に要求される。*

¶ 970 **保証アクティビティ：**

¶ 971 以下の保証アクティビティは、TOE が PSTN 経由で送受信するファクス通信機能を有する場合に要求される。

¶ 972 ***TSS：***

¶ 973 評価者は、以下について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：

1. ファクスインタフェースの使用事例
2. ファクスモデムとサポートするファクスプロトコルの機能
3. ファクスインタフェース経由で送受信が許可されているデータ
4. TOE がファクスプロトコルを使用して利用者データを送受信するためのみに使用されることを実現する方法

¶ 974 ***操作ガイダンス：***

¶ 975 評価者は、用途及び利用可能な機能に関してファクスインタフェースの記述が操作ガイダンスに含まれ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。

¶ 976 ***テスト：***

¶ 977 評価者は、ファクスインタフェースがファクスプロトコルを用いた利用者データの送信または受信のみに使用されることを保証するためにテストしなければならない。テストは、TOE が本要件を実施する方法に依存するだろう。次のテストを使用し、さらに追加のテストにより補足しなければならない。または、次のテストで十分であることの根拠が求められる：

1. TOE がファクスキャリアプロトコルを用いる時データキャリアを使用する発呼を拒否し、着呼を受け付けることを検証する。例えば、これにより、PC モデムから TOE に直接モデムコマンドを発

行することで（ターミナルコマンド：「ATDT <TOE Fax 番号>」を発行）、ターミナルアプリケーションを用いて達成できる － TOE はそのコールの応答で切断するべきである。

2. TOE がファクスキャリアプロトコルを用いる時のみ（データキャリアのネゴシエーションを拒否し）、発呼においてネゴシエートすることを検証する。例えば、これにより、PC モデムを用いて、TOE からのコールを受け付けようと試みることで（TOE からのファクスジョブを <PC モデム番号>に発出し、PC がターミナルコマンド発行：「ATA」）達成できる － TOE はキャリアネゴシエートせずに切断するべきである。

附属書 C オプション要件

¶978 以下は、関連するセキュリティ機能要件に適合することにより追加できる、オプションのセキュリティ機能要件と組織のセキュリティ方針である。

C.1 内部の監査ログ格納

¶979 本セクションの SFR は、オプションの内部監査ログ格納機能をサポートするため、ST に含まれるべきものである。

C.1.1 FAU_SAR.1 監査レビュー

(O.AUDIT)
下位階層： なし
依存性： FAU_GEN.1 監査データ生成

¶980 **FAU_SAR.1.1** TSF は、[割付：***管理者***]が**すべての記録**を監査記録から読み出せるようにしなければならない。

¶981 **FAU_SAR.1.2** TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

¶982 **保証アクティビティ：**

¶983 次の 保証アクティビティは、TOE の内部に監査記録を格納する時に要求される。

¶984 ***TSS：***

¶985 評価者は、許可された利用者と監査機能を閲覧するための機能のみによって監査記録が閲覧可能であることについての記述が TSS に含まれ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。

¶986 評価者は、監査記録を読み出すインタフェースの使用方法（例えば、利用者の識別認証、権限付与の方法、及び監査記録の読出しのための方法）についての記述が TSS に含まれ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。

¶987 ***操作ガイダンス：***

¶988 評価者は、操作ガイダンスに監査記録の閲覧方法及び閲覧の形式が適切に記述され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。

¶ 989 *テスト：*

¶ 990 評価者は、次のテストについても実行しなければならない：

1. 評価者は、操作ガイダンスに従って監査記録を読み出すことにより、監査記録の形式が操作ガイダンスで指定されたとおり提供され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。
2. 評価者は、許可された利用者以外の者が監査記録を読み出せないことを保証するため、チェックしなければならない。
3. 評価者は、監査記録の読み出し操作により、すべての監査記録が読み出されることを保証するため、チェックしなければならない。

C.1.2 FAU_SAR.2　限定監査レビュー

(O.AUDIT)
下位階層：　なし
依存性：　FAU_SAR.1　監査レビュー

¶ 991 **FAU_SAR.2.1**　TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

¶ 992 **保証アクティビティ：**

¶ 993 *テスト：*

¶ 994 評価者は、FMT_SMF.1 で実行された一連のテストにおいて本機能に関連するテストが含まれていなければならない。

C.1.3 FAU_STG.1　保護された監査証跡格納

(O.AUDIT)
下位階層：　なし
依存性：　FAU_GEN.1　監査データ生成

¶ 995 **FAU_STG.1.1**　TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

¶ 996 **FAU_STG.1.2**　TSF は、監査証跡に格納された監査記録への不正な改変を**防止**できなければならない。

¶ 997 **保証アクティビティ：**

¶ 998 次の保証アクティビティは、TOE 内部に監査記録を格納する時、要求される。

¶ 999 ***TSS：***

¶ 1000 評価者は、監査記録を不正なアクセス（改変、削除）から防ぐ手段の記述が TSS に含まれ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。

¶ 1001 ***操作ガイダンス：***

¶ 1002 評価者は、監査記録へアクセスするためのインタフェースに関する記述が TSS 及び操作ガイダンスに含まれていること、及び監査記録を不正なアクセス（改変、削除）から防ぐ手段の記述が一貫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。

¶ 1003 ***テスト：***

¶ 1004 評価者は、次のテストについても実行しなければならない：

1. 評価者は、許可された利用者が監査記録にアクセスできることをテストしなければならない。
2. 評価者は、監査データに関する権限を持たない利用者が、監査記録にアクセスできないことをテストしなければならない。

C.1.4 FAU_STG.4　監査データ損失の防止

(O.AUDIT)
下位階層：　FAU_STG.3 監査データ消失の恐れ発生時のアクション
依存性：　FAU_STG.1 保護された監査証跡格納

¶ 1005 **FAU_STG.4.1**　詳細化： TSF は、監査証跡が満杯になった場合、［選択、以下からの一つのみ選択：~~*「監査事象の無視」*~~、*「特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止」*、*「最も古くに格納された監査記録への上書き」*］及び［割付：*監査格納失敗時にとられるその他のアクション*］を行わなければならない。

¶ 1006 **保証アクティビティ：**

¶ 1007 次の保証アクティビティは、TOE 内部に監査記録を格納する時、要求

される。

¶ 1008 ***TSS：***

¶ 1009 評価者は、監査記録が満杯になった場合に実行される処理についての記述が TSS に含まれていること、その記述が SFR の定義と一貫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。

¶ 1010 ***操作ガイダンス：***

¶ 1011 評価者は、監査記録の容量が満杯になった場合に実行される処理（許可利用者への通知等）についての記述が操作ガイダンスに含まれ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。

¶ 1012 ***テスト：***

¶ 1013 評価者は、次のテストについても実行しなければならない：

1. 評価者は、操作ガイダンスに従い監査対象事象を発生させることにより監査記録の容量が満杯になった後、監査対象事象を発生させる。
2. 評価者は、SFR で定義された処理が監査記録に対して適切に実行されることを保証するため、チェックしなければならない。

C.2　画像上書き

¶ 1014 本セクションにおける SFR は、オプションの画像上書き機能をサポートする ST に含まれるべきものである。

C.2.1 FDP_RIP.1(a)　サブセット残存情報保護

(O.IMAGE_OVERWRITE)
下位階層：　なし
依存性：　なし

¶ 1015 **FDP_RIP.1.1(a)　詳細化：** TSF は、次のオブジェクト**からの資源の割り当て解除**において、**データの上書き消去により**資源の以前のどの情報の内容も利用できなくすることを保証しなければならない：**D.USER.DOC**。

¶ 1016 **保証アクティビティ：**

¶ 1017 ***TSS：***

¶ 1018 評価者は、どこに画像データが保存され、いつどのようにそれが上書きされるかについての記述が包括的であることを保証するため、TSS を検査しなければならない。

¶ 1019 ***操作ガイダンス：***

¶ 1020 評価者は、画像上書き機能を有効化するための指示が操作ガイダンスに含ま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。

¶ 1021 ***テスト：***

¶ 1022 評価者は、FMT_SMF.1 において実施される一連のテストにおいて本機能に関するテストが含まれていなければならない。

C.3 データの完全削除

¶ 1023 本セクションにおける SFR は、オプションのデータの完全削除機能をサポートする ST に含まれるべきものである。

C.3.1 FDP_RIP.1(b)　サブセット残存情報保護

(O.PURGE_DATA)
下位階層：　なし
依存性：　なし

¶ 1024 **FDP_RIP.1.1(b)　詳細化：** TSF は、以下のオブジェクトについて、資源の以前**顧客が供給した**任意の情報の内容が**管理者の要求**により利用できなくすることを保証しなければならない：**D.USER、 D.TSF**。

¶ 1025 **保証アクティビティ：**

¶ 1026 ***TSS：***

¶ 1027 評価者は、どこのデータが完全消去され、どのようにそれが利用不可能となるについての記述が包括的であることを保証するため、TSS を検査しなければならない。

¶ 1028 ***操作ガイダンス：***

¶ 1029 評価者は、データの完全消去を起動するための指示が操作ガイダンスに含ま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。

¶ 1030 ***テスト：***

¶ 1031 評価者は、FMT_SMF.1 において実施される一連のテストにおいて本機能に関するテストが含まれていなければならない。

附属書 D 選択ベース要件

D.1　現地交換可能な不揮発性ストレージデバイス上の秘密のデータ

D.1.1 FCS_COP.1(d)　暗号操作（AES データ暗号化／復号）

（O.STORAGE _ENCRYPTION）

下位階層：　なし

依存性：　[~~FDP_ITC.1 セキュリティ属性なしの利用者データのインポート、または~~
~~FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~
FCS_CKM.1(b)　暗号鍵生成（対称鍵）]
FCS_CKM_EXT.4　拡張：暗号鍵材料破棄

¶ 1032 **FCS_COP.1.1(d)** TSF は、以下を満たす暗号鍵長［**選択：*128 ビット*、*256 ビット***］及び［**選択：*CBC*、*GCM* 、*XTS***］**モードに使用される**指定された暗号アルゴリズム **AES** に従って、暗号化及び復号を実行しなければならない：**ISO/IEC 18033-3 で指定された AES** 、［**選択：*ISO/IEC 10116 で指定された CBC*、*ISO/IEC 19772 で指定された GCM*、*IEEE 1619 で指定された XTS***］。

¶ 1033 ***適用上の注釈：***

¶ 1034 *本 PP は、ソフトウェ暗号化またはハードウェア暗号化を許容する。*

¶ 1035 *XTS モードが選択される場合、 IEEE 1619 に指定されるとおり、256 ビットまたは 512 ビットの暗号鍵が許容される。XTS-AES 鍵は、2 つの等しい長さの鍵に分割される-例えば、256 ビット鍵と XTS モードが選択される時、AES-128 が基礎となるアルゴリズムとして使用される。 512 ビット鍵と XTS モードが選択される時、AES-256 が使用される。*

¶ 1036 *本要件の意図は、ST 作成者が現地交換可能な不揮発性ストレージデバイスに関する AES 暗号化の適切な情報を選択できるような承認された AES モードを指定することである。最初の選択は、ST 作成者が TOE 実装に依ってサポートされるモードを示すべきである。2 番目の選択は FCS_CKM.1(b)用に指定されたものと同一の、使用される鍵長を示す。3 番目の選択は、最初の選択で選んだモードと一致しなければならない。複数のモードをサポートする場合、ST において本コンポーネントが繰り返されるとより明確になる。*

¶ 1037 **保証アクティビティ：**

¶ 1038 ***TSS：***

¶ 1039 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。

¶ 1040 ***操作ガイダンス：***

¶ 1041 複数の暗号モードがサポートされている場合、評価者は特定のモード・鍵長がエンドユーザによる選択の手法が記述されていることを決定するため、ガイダンス文書を検査すること。

¶ 1042 ***テスト：***

¶ 1043 次のテストは、SFR においてなされた選択に基づく条件付きのものである。

¶ 1044 **AES-CBC テスト**

¶ 1045 AES-CBC 既知解テスト

¶ 1046 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。

¶ 1047 **KAT-1.** AES-CBC の暗号化機能をテストするため、評価者は 10 個の平文の値のセットを供給し、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。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。

¶ 1048 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。

¶ 1049 **KAT-2.** AES-CBC の暗号化機能をテストするため、評価者は 10 個の鍵の値のセットを供給し、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。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。

¶ 1050 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。

¶ 1051 **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。

¶ 1052 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。

¶ 1053 **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。

¶ 1054 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。

¶ 1055 AES-CBC マルチブロックメッセージテスト

¶ 1056 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

号化することによって、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び、選んだ鍵及び IV によって、試験すべきモードを用いてメッセージを暗号化しなければならない。暗号文は、同一の平文メッセージを同一の鍵と IV によって既知の良好な実装を用いて暗号化した結果と比較されなければならない。

¶ 1057 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って、各モードについての復号機能も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び、選んだ鍵及び IV によって、試験すべきモードを用いてメッセージを復号しなければならない。平文は、同一の暗号文メッセージを同一の鍵と IV によって既知の良好な実装を用いて復号した結果と比較されなければならない。

¶ 1058 AES-CBC モンテカルロテスト

¶ 1059 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、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：

¶ 1060 # Input: PT, IV, Key

¶ 1061 for i = 1 to 1000:

¶ 1062 if i == 1:

¶ 1063 CT[1] = AES-CBC-Encrypt(Key, IV, PT)

¶ 1064 PT = IV

¶ 1065 else:

¶ 1066 CT[i] = AES-CBC-Encrypt(Key, PT)

¶ 1067 PT = CT[i-1]

¶ 1068 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って 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。

¶ 1069 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。

¶ 1070 AES-GCM テスト

¶ 1071 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 の認証済み暗号化機能をテストしなければならない：

¶ 1072 128 ビット及び 256 ビットの鍵

¶ 1073 **2 とおりの平文の長さ**. 一つの平文の長さは、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)。他の平文の長さは、128 ビットの整数倍であってはならない (サポートされる場合)。

¶ 1074 **3 とおりの AAD の長さ**. 一つの AAD 長は 0 としなければならない (サポートされる場合) 。一つの AAD 長は、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)。一つの AAD 長は、128 ビットの整数倍であってはならない(サポートされる場合) 。

¶ 1075 **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。

¶ 1076 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 認証済み暗号化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。

¶ 1077 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。

¶ 1078 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。

¶ 1079 XTS-AES テスト

¶ 1080 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：

¶ 1081 256 ビット (AES-128 用) 及び 512 ビット (AES-256 用) の鍵

¶ 1082 **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一つは、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一つは、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。

¶ 1083 評価者は、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暗号機能をテストし、XTS-AES 暗号化から得られた暗号文を取得しなければならない。

¶ 1084 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、0 から 255 の間の 10 進数であって、実装によって内部的に tweak 値へ変換されるものである。

¶ 1085 評価者は、暗号化と同一のテストを用い、平文の値を暗号文の値と置き換え、XTS-AES 暗号化を XTS-AES 復号と置き換えて、XTS-AES 復号機能をテストしなければならない。

D.1.2 FCS_COP.1(e)　暗号操作（鍵ラッピング）

（FCS_KYC_EXT.1.1 での選択）

下位階層：　なし

依存性：　[~~FDP_ITC.1 セキュリティ属性なしの利用者データのインポート、または~~

~~FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~

FCS_CKM.1(b) 暗号鍵生成（対称鍵）]

FCS_CKM_EXT.4 拡張：暗号鍵材料破棄

¶ 1086 **FCS_COP.1.1(e) 詳細化：** TSF は、以下の標準のリストに合致する、特定された暗号アルゴリズム **AES の以下のモード[選択：KW、KWP、GCM、**

CCM]と暗号鍵長**[選択：128 ビット、256 ビット]**に従って、鍵ラッピングを実行しなければならない：**[ISO/IEC 18033-3 (AES), [選択: NIST SP 800-38F, ISO/IEC 19772]**。

¶ 1087 ***適用上の注釈：***

¶ 1088 *本要件は、ST 作成者が FCS_KYC_EXT.1 において指定された鍵チェイニングのアプローチにおいて鍵ラッピングの使用を選択する場合、ST の本文において使用される。*

¶ 1089 **保証アクティビティ：**

¶ 1090 ***TSS：***

¶ 1091 評価者は、鍵ラップ機能の記述が TSS に含まれていることを検証しなければならない。また、鍵ラップが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使用していることを検証しなければならない。

¶ 1092 ***KMD：***

¶ 1093 評価者は、承認された方法を用いるすべての鍵がラップされることと、鍵ラップ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。

¶ 1094 ***テスト：***

¶ 1095 *評価者は、ラップされた鍵が本 SFR で指定されたモード及び鍵長での AES に従い、ラッピングの参照実装を用いた本 SFR で指定されたとおり、ラップされることを保証しなければならない。ラッピングアルゴリズムの本参照実装は、評価者または開発者により提供されたツールまたはプログラムであってもよい、これらの実装は開発者により提供された KMD 記述に依存している。*

D.1.3 FCS_COP.1(f)　暗号操作（鍵暗号化）

（FCS_KYC_EXT.1.1 での選択）

下位階層：　なし

依存性：　~~[FDP_ITC.1 セキュリティ属性なしの利用者データのインポート、または~~

~~FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~

FCS_CKM.1(b)　暗号鍵生成(対称鍵)
FCS_CKM_EXT.4　拡張： 暗号鍵材料破棄

¶1096 **FCS_COP.1.1(f)　詳細化：** TSF は、以下の標準のリストに合致する、特定された暗号アルゴリズム **AES の[選択：CBC、GCM]モード**と暗号鍵長**[選択：*128 ビット*、*256 ビット*]**に従って、**鍵暗号化及び復号**を実行しなければならない：**[ISO /IEC 18033-3 で指定される AES、 [選択：*ISO/IEC 10116 で指定される CBC*、 *ISO/IEC 19772 で指定される GCM*]**。

¶1097 ***適用上の注釈：***

¶1098 *本要件は、ST 作成者が FCS_KYC_EXT.1 において指定された鍵チェイニングのアプローチの一部として、鍵を保護するために AES 暗号化・復号の使用を選択する場合、ST の本文において使用される。*

¶1099 **保証アクティビティ：**

¶1100 ***TSS：***

¶1101 評価者は、TSS に鍵暗号化機能の記述が含まれていること検証しなければならず、また鍵暗号化が適切な仕様に従い承認された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。

¶1102 ***KMD：***

¶1103 評価者は、承認された手法を用いてすべての鍵が暗号化されたことと鍵暗号化がいつ発生するかについての記述が提供されることを保証するため、KMD をレビューしなければならない。

¶1104 ***テスト：***

¶1105 評価者は、暗号化を検証するため FCS_COP.1(d)のテストを使用しなければならない。

D.1.4 FCS_COP.1(i)　暗号操作（鍵配送）

（FCS_KYC_EXT.1 での選択）

下位階層：　　なし

依存性：　　[~~FDP_ITC.1 セキュリティ属性なしの利用者データのインポート、または~~
~~FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~

FCS_CKM.1(a) 暗号鍵生成（非対称鍵）

FCS_CKM_EXT.4 拡張：暗号鍵材料破棄

¶ 1106 **FCS_COP.1.1(i) 詳細化：**　TSF は、以下に合致する、特定された暗号アルゴリズム **RSA の以下のモード[選択：KTS-OAEP、KTS-KEM-KWS]**と暗号鍵長**[選択：2048、3072]**に従って、鍵配送を実行しなければならない：**NIST SP 800-56B, 改訂第 1 版**。

¶ 1107 ***適用上の注釈：***

¶ 1108 *本要件は、ST 作成者が FCS_KYC_EXT.1 で指定される鍵チェイニングにおいて鍵配送の使用を選択する場合、ST の本文で使用される。*

D.1.5 FCS_SMC_EXT.1　拡張：サブマスク結合

（FCS_KYC_EXT.1.1 での選択）

下位階層：　なし

依存性：　FCS_COP.1(c)　暗号操作(ハッシュアルゴリズム)

¶ 1109 **FCS_SMC_EXT.1.1** TSF は、中間鍵または BEV を生成するため、次の方法[選択：*排他的 OR（XOR）*、*SHA-256*、*SHA-512*]を用いてサブマスクを結合しなければならない。

¶ 1110 ***適用上の注釈:***

¶ 1111 *本要件は、製品が XOR または承認された SHA-ハッシュのいずれかを用いてさまざまなサブマスクを結合するように指定する。承認されたハッシュ関数は附属書 D.3.1 の FCS_COP.1(c)において記述される。*

¶ 1112 **保証アクティビティ：**

¶ 1113 ***TSS：***

¶ 1114 鍵が中間鍵を形成するために一緒に XOR される場合、TSS のセクションには、これがどのように実行されるかを識別されなければなければならない（例えば、順序についての要求事項、実行されるチェック等がある場合）。評価者は、生成された出力長が DEK 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についても確認しなければならない。

¶1115 ***KMD：***

¶1116 評価者は、承認された結合が使用され、それが鍵材料の弱体化または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。

¶1117 ***テスト：***

¶1118 *(条件付き)：複数の許可要素がある場合、評価者は、要求された許可要素の供給の失敗が暗号データへのアクセスに至らないことを保証しなければならない。*

D.2　保護された通信

¶1119 クラス FTP の要件に示されたとおり、適合する TOE が、管理者、または TOE の他の部分、または外部 IT エンティティとの間の通信チャネルのセキュリティ侵害に対する脅威を軽減できるための方法がいくつかある。（少なくとも）監査サーバとリモート管理者のための保護された接続性を提供するために、セキュアな通信プロトコル（IPsec、SSH、TLS、TLS/HTTPS）の一つを実装しなければならない。

¶1120 各プロトコルに関連した一意の要件があり；以下に指定される。FTP_ITC.1 及び FTP_TRP.1 のコンポーネントでの選択に依存して、ST 作成者は、関連の SFR と保証アクティビティを ST に含める必要がある。

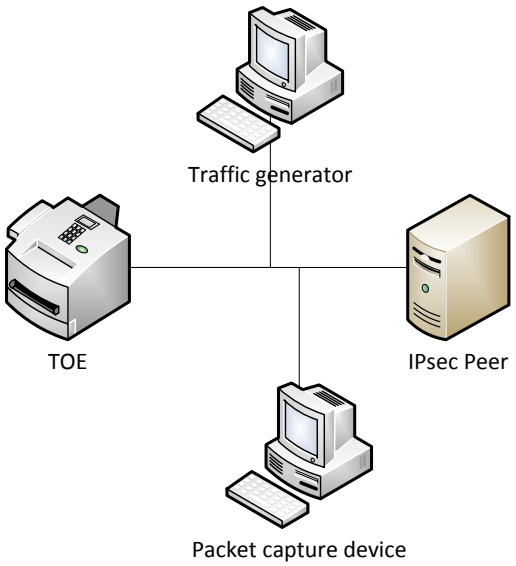
D.2.1 FCS_IPSEC_EXT.1　拡張：選択された IPsec

(FTP_ITC.1.1、FTP_TRP.1.1 での選択)
下位階層：　なし
依存性：　~~FPT_ITT.1 基本 TSF 内データ転送保護,~~
FIA_PSK_EXT.1　拡張：事前共有鍵の生成
FCS_COP.1(g) 暗号操作 (鍵付ハッシュメッセージ認証)

¶1121 ***適用上の注釈：***

¶1122 *TSF が本 PP の要件に従って RFC を実装していることを示すために、評価者は以下に列挙された保証アクティビティを実施しなければならない。*

¶1123 *TOE は、IPsec ピアとの通信に使用する接続を確立するために、IPsec プロトコルを使用することが要求されている。*



¶ 1124

¶ 1125 評価者は、上図のテスト環境と同等のテスト環境を最小限作成しなければならない。トラフィック・ジェネレータは、ネットワークパケットを構築するために使用され、評価者に ICMP、IPv4、IPv6、UDP、及び TCP パケットヘッダにおけるフィールドを操作する能力を提供することが期待されている。評価者は、テスト環境における相違点について、正当化する理由を提供しなければならない。

¶ 1126 **FCS_IPSEC_EXT.1.1** TSF は、RFC4301 で指定されたとおり、IPsec アーキテクチャを実装しなければならない。

¶ 1127 **保証アクティビティ：**

¶ 1128 ***操作ガイダンス：***

¶ 1129 評価者は、操作ガイダンスが管理者に対して、破棄、迂回、及び保護に関する規則を指定する SPD (訳注：セキュリティポリシーデータベース) へのエントリを構築する方法を指示していることを検証するため、操作ガイダンスを検査しなければならない。

¶ 1130 ***テスト：***

¶ 1131 評価者は、以下のテストを実行するために、TOE の構成を行うにあたり、操作ガイダンスを使用すること：

1. 評価者は、破棄(DISCARD)、迂回 (BYPASS)、及び保護 (PROTECT)に関する規則があるような SPD を構築しなければならない。規則の構築に使用される選択肢は、評価者が、それぞれのパケットが３つの規則の一つと一致するような、パケットヘッ

ダの適切なフィールドを持つ３つのネットワークパケットを送信できるよう異なっていなければならない。評価者は、監査証跡を介して観測し、パケットは TOE が期待とおりのふるまいをすることをキャプチャする：適切なパケットが破棄されたこと、改変なしに通過を許可されたこと、IPsec 実装により暗号化されたこと。

2. 評価者は、交互の操作–迂回及び保護–を持つ２つの同等な SPD エントリを考案しなければならない。そして、エントリは、２つの異なる順序で配置されるべきであり、それぞれの場合で評価者は、適切なパケットを生成し、パケットキャプチャと確認用のログを用いて、最初のエントリが実施されるか確認しなければならない。

3. 評価者は、２つのエントリが考案され一つが他方のサブセットである場合（特定アドレスとネットワークセグメント等）を除いて、上記の手順を繰り返さなければならない。再度、評価者は、規則の特異性に関わらず最初が実施されることを保証するため、両方の順序をテストするべきである。

¶ 1132 **FCS_IPSEC_EXT.1.2** TSF は、［選択：*トンネルモード*、*トランスポートモード*］を実装しなければならない。

¶ 1133 **保証アクティビティ：**

¶ 1134 ***TSS：***

¶ 1135 評価者は、TSS に（選択されたとおりの）トンネルモード及び／またはトランスポートモードで運用するため VPN が確立されることが可能であると記述されていることを保証するため、TSS をチェックすること。

¶ 1136 ***操作ガイダンス：***

¶ 1137 評価者は、選択されたそれぞれのモードにおける接続の設定方法についての指示が操作ガイダンスに含まれていることを確認しなければならない

¶ 1138 ***テスト：***

¶ 1139 評価者は、選ばれた選択に基づき、次のテストを実行しなければならない：

1. (条件付き)：トンネルモードが選択された場合、評価者は、操作

ガイダンスを使用して、TOE をトンネルモードで動作するよう設定し、IPsec ピアもトンネルモードで動作するよう設定する。評価者は、許可された SA がネゴシエートできることを保証するため、許可された暗号化アルゴリズム、認証方法等のいずれかを使用するよう TOE と IPsec ピアを設定する。そして、評価者は、クライアントから IPsec ピアへ接続するための接続を開始する。評価者は、トンネルモードを使用して、（例えば、監査証跡及びキャプチャされたパケット内で）接続の確立が成功したことを観測すること。

2. (条件付き)：トランスポートモードが選択された場合、評価者は、操作ガイダンスを使用して、TOE をトランスポートモードで動作するよう設定し、IPsec ピアもトランスポートモードで動作するよう設定する。評価者は、許可された SA がネゴシエートできることを保証するため、許可された暗号化アルゴリズム、認証方法等のいずれかを使用するよう TOE と IPsec ピアを設定する。そして、評価者は、クライアントから IPsec ピアへ接続するための接続を開始する。評価者は、トランスポートモードを使用して、（例えば、監査証跡及びキャプチャされたパケット内で）接続の確立が成功したことを観測すること。

¶ 1140 **FCS_IPSEC_EXT.1.3** TSF は、他に一致しなかったものすべてに一致し破棄するような SPD における名目上の最終エントリを持っていなければならない。

¶ 1141 **保証アクティビティ:**

¶ 1142 ***TSS：***

¶ 1143 評価者は、TSS が SPD に対するパケットの処理方法に関する記述、そして、一致する「規則」が見つからない場合、暗示的であれ明示的であれ、ネットワークパケットが破棄されるという最終的な規則が存在することについての記述を TSS が提供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。

¶ 1144 ***操作ガイダンス：***

¶ 1145 評価者は、SPD の構築方法に関する指示を操作ガイダンスが提供していることをチェックし、次のテストのため TOE を設定するためにそのガイダンスを使用すること。

¶ 1146 *テスト：*

¶ 1147 評価者は、次のテストを実行しなければならない：

¶ 1148 評価者は、SPD がネットワークパケットを破棄、迂回、及び保護する操作を含むエントリを持つように SPD を設定しなければならない。評価者は、FCS_IPSEC_EXT.1.1 の検証のために作成された SPD を使用することができる。評価者は、迂回エントリに合致するようなネットワークパケットを構築し、そのパケットを送信しなければならない。評価者は、ネットワークパケットが適切な宛先のインタフェースへ改変なしに通過されることを観測するべきである。そして、評価者は、パケットヘッダにおける一つのフィールドを改変しなければならない；そうして、評価者が作成したエントリにもはや一致しないように（前のエントリに一致しないパケットを破棄するような「TOE が作成した」最終的エントリがあるかもしれない）。評価者は、パケットを送信し、そのパケットが TOE のインタフェースのどれへも流れることを許可されていないことを観測する。

¶ 1149 **FCS_IPSEC_EXT.1.4** TSF は、［選択：*セキュアハッシュアルゴリズム（SHA）ベースの HMAC と共に AES-CBC-128（RFC 3602 によって指定された）、セキュアハッシュアルゴリズム（SHA）ベースの HMAC と共に AES-CBC-256（RFC 3602 によって指定された）、RFC 4106 で指定された AES-GCM-128、RFC 4106 で指定された AES-GCM-256、の暗号化アルゴリズム*］を用いて、RFC 4303 で定義されたとおり、IPsec プロトコル ESP を実装しなければならない。

¶ 1150 **保証アクティビティ：**

¶ 1151 ***TSS：***

¶ 1152 評価者は、選択された対称鍵暗号アルゴリズム（AES-CBC が選択された場合、SHA ベースの HMAC アルゴリズムと共に）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。選択された場合、評価者は、SHA ベースの HMAC アルゴリズムが、FCS_COP.1(g) 暗号操作（鍵付ハッシュメッセージ認証）で指定されたアルゴリズムに適合していることを保証すること。

¶ 1153 ***操作ガイダンス：***

¶ 1154 評価者は、操作ガイダンスが ST 作成者によって選択されたアルゴリズムを使用するために TOE の設定方法に関する指示を提供していること

を保証するため、操作ガイダンスをチェックすること。

¶ 1155 ***テスト：***

¶ 1156 評価者は次のテストについても実行しなければならない：

¶ 1157 評価者は、選択されたアルゴリズムのそれぞれを用いるために TOE を設定している操作ガイダンスに示されるとおりに TOE を設定しなければならない、また ESP を用いる接続を確立しようと試みなければならない。その接続は、それぞれのアルゴリズムについて、確立が成功するべきである。

¶ 1158 **FCS_IPSEC_EXT.1.5** TSF は、次のプロトコルを実装しなければならない：［選択：*RFC 2407*、*2408*、*2409*、 *RFC 4109*、［選択：*拡張シーケンス番号のためのその他の RFC なし*、*拡張シーケンス番号のための RFC 4304*］、*及び*［選択：*ハッシュ関数のためのその他の RFC なし*、*ハッシュ関数のための RFC4868*］*で定義された、フェーズ 1 メインモードを用いた IKEv1；RFC 5996*、［選択：*NAT トラバーサルのサポートなし*、*セクション 2. 23 で規定されるとおりの NAT トラバーサルの必須サポート付き*］、*及び*［選択：*ハッシュ関数のためのその他の RFC なし*、*ハッシュ関数のための RFC4868*］*で定義された IKEv2*］。

¶ 1159 ***適用上の注釈:***

¶ 1160 *IKEv1 または IKEv2 のいずれかのサポートが提供されなければならないが、適合する TOE は両方を提供可能である；最初の選択は、本選択を行うために使用される。IKEv1 については、要件は、RFC 4109 に記述されるとおり、追加／改変した RFC 2409 に適合する IKE 実装が要求されていると解釈されるべきである。RFC 4304 は、2 つ目の選択を用いて適合する TOE が指定できるような拡張したシーケンス番号のサポートを識別している。RFC 4868 は、IKEv1 及び IKEv2 の両方を用いて追加のハッシュ関数を識別する；これらの関数が実装される場合、3 つ目（IKEv1 の）及びの 4 つ目（IKEv2）の選択が使用される。*

¶ 1161 **保証アクティビティ：**

¶ 1162 ***TSS：***

¶ 1163 評価者は、IKEv1 及び／または IKEv2 が実装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。

¶ 1164 ***操作ガイダンス：***

¶ 1165 評価者は、操作ガイダンスが管理者に IKEv1 及び／または IKEv2（選択されたとおり）を使用するための TOE の設定の方法を指示していることを保証するため、操作ガイダンスをチェックしなければならない、また、IKEv2 が選択された場合、次のテストのため、NAT トラバーサルを実行するために TOE を設定するためにそのガイダンスを使用すること。

¶ 1166 ***テスト：***

¶ 1167 (条件付き)： IKEv2 が選択された場合、評価者は、TSS 及び RFC 5996、セクション 2.23 に記述されているとおり、NAT トラバーサル処理を実施できるように、TOE を設定しなければならない。評価者は、IPsec 接続を開始し、NAT トラバーサルが成功することを決定しなければならない。

¶ 1168 **FCS_IPSEC_EXT.1.6** TSF は、［選択：IKEv1、IKEv2］プロトコルにおける暗号化されたペイロードが、RFC 3602 で指定された暗号化アルゴリズム AES-CBC-128、AES-CBC-256、及び［選択：RFC 5282 で指定された AES-GCM-128、AES-GCM-256、他のアルゴリズムなし］を使用することを保証しなければならない。

¶ 1169 **保証アクティビティ：**

¶ 1170 ***TSS：***

¶ 1171 評価者は、TSS が IKEv1 及び／または IKEv2 ペイロードの暗号化に使用されたアルゴリズムを識別していること、そして、アルゴリズム AES-CBC-128、AES-CBC-256 が指定されていること、及び要件の選択においてその他が選択された場合、それらが TSS 議論に含まれることを保証しなければならない。

¶ 1172 ***操作ガイダンス：***

¶ 1173 評価者は、要件で選択された追加アルゴリズムと共に、必須のアルゴリズムの設定が操作ガイダンスに記述されていることを保証しなければならない。そして、選択されたそれぞれの暗号スイートに対する次のテストを実行するため、TOE の設定にそのガイダンスが使用されること。

¶ 1174 ***テスト：***

¶ 1175 評価者は、TOE を設定し、テスト用の暗号スイートを用いて、IKEv1

及び／または IKEv2 ペイロードを暗号化して、指示された暗号スイートを用いて暗号化したペイロードのみを受け入れるよう設定されたピアデバイスとの接続を確立しなければならない。評価者は、アルゴリズムがそのネゴシエーションに使用されたものであることを確認すること。

¶ 1176 **FCS_IPSEC_EXT.1.7** TSF は、IKEv1 フェーズ 1 鍵交換がメインモードのみを使用することを確認しなければならない。

¶ 1177 **保証アクティビティ：**

¶ 1178 ***TSS：***

¶ 1179 評価者は、TSS を検査して、TOE がサポートする IPsec プロトコルの記述において、アグレッシブモードが IKEv1 フェーズ 1 鍵交換で使用されないこと、及びメインモードのみが使用されることを保証するため、TSS を検査しなければならない。これは、設定可能なオプションであるかもしれない。

¶ 1180 ***操作ガイダンス：***

¶ 1181 操作の前に TOE の設定をモードが要求する場合、評価者は、操作ガイダンスにこの設定に関する指示が含まれていることを保証するため、操作ガイダンスをチェックしなければならない。

¶ 1182 ***テスト：***

¶ 1183 評価者は、次のテストについても実行しなければならない：

¶ 1184 (条件付き)：評価者は、操作ガイダンスで指示されているように、TOE を設定しなければならない、また、アグレッシブモードで IKEv1 フェーズ 1 接続を用いて接続を確立しようと試みなければならない。この試みは失敗するべきである。そして、評価者は、メインモード鍵交換がサポートされていることを示すべきである。このテストは、FCS_IPSEC_EXT.1.5 のプロトコル選択で、IKEv1 が上記において選択されない場合には、適用されない。

¶ 1185 **FCS_IPSEC_EXT.1.8** TSF は、［選択：IKEv2 の SA ライフタイムが［選択：パケット数／バイト数；時間の長さ、ここで時間の値はフェーズ 1 の SA で 24 時間とフェーズ 2 の SA で 8 時間に制限することができる］に基づき確立可能である；IKEv1 の SA ライフタイムが［選択：パケット数／バイト数；時間の長さ、ここで時間の値はフェーズ 1 の SA で 24 時間とフェー

ズ 2 の SA で 8 時間に制限することができる］に基づき確立可能である］ことを保証しなければならない。

¶ 1186 ***適用上の注釈：：***

¶ 1187 *ST 作成者は、実装において IKE のバージョンに基づく選択の権利が与えられている。ライフタイムの制限が設定可能な場合、評価者は、操作ガイダンスにこれらの値を設定する適切な指示が含まれていることを検証すること。*

¶ 1188 *SA ライフタイムに関する限り、TOE は、送信バイト数、または送信パケット数に基づきライフタイムを制限できる。パケットベースまたはボリュームベースの SA ライフタイムのどちらでも許容される；ST 作成者は、ライフタイム制限のいずれがサポートされるかを示すために、適切な選択をすること。*

¶ 1189 **保証アクティビティ：**

¶ 1190 ***操作ガイダンス：***

¶ 1191 評価者は、SA ライフタイムの値が設定可能であること、及びそれを実行する指示が操作ガイダンスに記述されていることを検証する。タイムベースの制限がサポートされる場合、評価者は、その値が 24 時間のフェーズ 1 の SA の値及び 8 時間のフェーズ 2 の SA の値を許可していることを保証する。現在、パケット数またはバイト数について必須の値はないが、評価者は、要件で選択された場合、これが設定可能であることを単に保証すること。

¶ 1192 この機能をテストする際、評価者はその両方について適切に設定されることを保証する必要がある。RFC(訳注：RFC4306 セクション 2.8)より「IKEv1 及び IKEv2 の違いは、IKEv1 の SA ではライフタイムはネゴシエートされたものであること。IKEv2 では、SA のそれぞれの端点が、SA におけるそれ自身のライフタイム方針の実施と必要なときに SA の鍵変更（rekeying）に責任がある。両端が異なるライフタイム方針を持っている場合、短いライフタイムを持つ側が常に鍵変更の要求を行うこととなる。両端が同じライフタイム方針を持っている場合、両方が同時に鍵変更を起動することが可能である（その場合、冗長な SA を生成する）。これが発生する確率を減らすため、鍵変更のタイミングリクエストには、神経質になるべきである。」

¶ 1193 ***テスト：***

¶ 1194 次のテストのそれぞれは、FCS_IPSEC_EXT.1.5 プロトコル選択において選択された IKE のそれぞれのバージョンについて実施されなければならない：

1. (条件付き)：評価者は、操作ガイダンスに従って、許可されたパケット（またはバイト）の数の観点より、最大のライフタイムを設定しなければならない。評価者は、SA を確立しなければならない、また、この SA を通したパケット（またはバイト）の許可された数を超えた時は、接続が再ネゴシエートされることを決定しなければならない。

2. (条件付き)::評価者は、フェーズ 1 の SA が確立されて、再度ネゴシエートされる前に 24 時間以上維持されることを試みるようなテストを構築しなければならない。評価者は、この SA が 24 時間以内に終了されるか、または再ネゴシエートされることを観測しなければならない。TOE が特定の方法で設定されるようなアクションが要求される場合、評価者は、TOE の設定機能が操作ガイダンスに文書化されたとおりに動くことを実証するテストを実施しなければならない。

3. (条件付き)：評価者は、ライフタイムが 24 時間ではなく 8 時間となることを除いて、フェーズ 2 の SA についてテスト 1 と同様のテストを実行しなければならない。

¶ 1195 **FCS_IPSEC_EXT.1.9** TSF は、すべての IKE プロトコルが DH グループ 14（2048 ビット MODP）、及び［選択：24（2048 ビット MODP と 256 ビット POS）、19（256 ビットランダム ECP）、20（384 ビットランダム ECP）、5（1536 ビット MODP））、［割付：TOE により実装されたその他の DH グループ］、その他の DH グループなし］を実装していることを保証しなければならない。

¶ 1196 ***適用上の注釈:***

¶ 1197 *上記は、TOE が DH グループ 14 をサポートすることを要求している。その他のグループがサポートされている場合、それらは、（グループ 24、19、20、及び 5 から）選択されるか、または上記割付で指定されるべきである；さもなければ、「その他の DH グループなし」が選択されるべきである。これは IKEv1／IKEv2 鍵交換に適用される。*

¶ 1198 **保証アクティビティ：**

¶ 1199 ***TSS：***

¶ 1200 評価者は、要件において指定された DH グループがサポートされているとおり TSS に列挙され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。それらが、複数の DH グループをサポートしている場合、評価者は、特定の DH グループが通信相手との間で指定される／ネゴシエートされる方法について TSS に記述されていることを保証するため、チェックすること。

¶ 1201 ***テスト：***

¶ 1202 評価者は、次のテストについても実行しなければならない（このテストは、例えば FCS_IPSEC_EXT.1.1 に関連するテスト等、本コンポーネントの他のテストと結合されるかもしれない）：

¶ 1203 それぞれのサポートされる DH グループについて、評価者は、すべての IKE プロトコルが特定の DH グループを用いてうまく完了できることを保証するため、テストしなければならない。

¶ 1204 **FCS_IPSEC_EXT.1.10** TSF は、すべての IKE プロトコルが［選択：RSA、ECDSA］アルゴリズムと事前共有鍵を用いて、ピア認証を実行することを保証しなければならない。

¶ 1205 ***適用上の注釈：***

¶ 1206 *選択されたアルゴリズムは FCS_COP.1(b)の適切な選択に対応するべきである。IPsec が TOE に含まれる場合、ST 作成者はまた附属書 D.2.6 より FIA_PSK_EXT についても含めること。*

¶ 1207 **保証アクティビティ：**

¶ 1208 ***TSS：***

¶ 1209 評価者は、TOE で使用される IKE ピア認証プロセスについての記述が TSS に含まれていること、及びこの記述が本要件で指定された署名アルゴリズムの使用を網羅していることをチェックしなければならない。

¶ 1210 ***テスト：***

¶ 1211 評価者は、次のテストについても実施しなければならない：

¶ 1212 それぞれのサポートされている署名アルゴリズムについて、評価者は、

そのアルゴリズムを使用したピア認証がうまく達成できること、及び接続の確立がうまくいくことをテストしなければならない。

D.2.2 FCS_TLS_EXT.1　拡張：選択された TLS

(FTP_ITC.1.1、FTP_TRP.1.1 での選択)
下位階層：　なし
依存性：　　なし

¶1213 **FCS_TLS_EXT.1.1** TSF は、以下の暗号スイートをサポートしている以下のプロトコルの一つ以上［選択：*TLS 1.0（RFC 2246）*、*TLS 1.1（RFC 4346）*、*TLS 1.2（RFC 5246）*］を実装しなければならない：

¶1214 必須の暗号スイート：

- TLS_RSA_WITH_AES_128_CBC_SHA

¶1215 オプションの暗号スイート：

¶1216 [選択：

- *なし*
- *TLS_RSA_WITH_AES_256_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_RSA_WITH_AES_256_CBC_ SHA256*
- *TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256*
- *TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384*

- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*

¶ 1217].

¶ 1218 ***適用上の注釈：***

¶ 1219 *ST 作成者は、TLS 実装を反映した適切な選択及び割付を行わなければならない。*

¶ 1220 *評価された構成でテストされるべき暗号スイートは、本要件により限定される。ST 作成者は、サポートされるオプションの暗号スイートを選択するべきである；必須のスイート以外にサポートされる暗号スイートがない場合は、「なし」が選択されるべきである。実装によってネゴシエートされるスイートが本要件における暗号スイートに限定されるように管理手順が実施される必要がある場合、適切な指示が AGD_OPE により求められるガイダンスに含まれている必要がある。*

¶ 1221 *上に列挙されたスイート B アルゴリズム（RFC6460）は、実装が推奨されるアルゴリズムである。TLS の要件は、CNSSP 15 及び NIST SP 800-131A に適合するため、 HCD PP の次期バージョンにおいて変更されるかもしれない。*

¶ 1222 **保証アクティビティ：**

¶ 1223 ***TSS：***

¶ 1224 評価者は、*サポートされる暗号スイートが指定されていることを保証するため、TSS における本プロトコルの実装の記述をチェックしなければならない。評価者は、指定された暗号スイートが本コンポーネントに列挙されたものと同一であ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。評価者は、TLS が TSS における記述(例えば、TOE により公表されている暗号スイートのセットが要件を満たすよう制限されなければならないかもしれない)に適合するように、TOE の設定に関する指示が操作ガイダンスに含まれていることを保証するため、*

操作ガイダンスについてもチェックしなければならない。

¶ 1225 ***テスト：***

¶ 1226 *評価者は、次のテストについても実行しなければならない：*

1. 評価者は、本要件で指定された暗号スイートのそれぞれを用いて TLS 接続を確立しなければならない。本接続は、より高いレベルのプロトコル、例えば、HTTPS セションの一部として、確立されるかもしれない。テストの意図を満たすため、暗号スイートのネゴシエーションの成功を観測すれば十分である；使用されている暗号スイート（例えば、暗号アルゴリズムが 128 ビット AES で、256 ビットの AES でない場合）を判別しようと試みる暗号化されたトラフィックの特性を検査する必要はない。

2. 評価者は、TOE と TLS ピアの間に中間者攻撃ツールをセットアップしなければならない、またトラフィックへ次の改変を行わなければならない：

   a. [条件： TOE がサーバである] Server Hello ハンドシェイクメッセージにおけるサーバのノンスの少なくとも 1 バイトを改変し、サーバがクライアントの Finished ハンドシェイクメッセージを拒否することを検証する。

   b. [条件： TOE がクライアントである] Server Hello ハンドシェイクメッセージにおけるサーバが選択した暗号スイートを Client Hello ハンドシェイクメッセージ中に存在しない暗号スイートに改変する。評価者は、クライアントが Server Hello を受信後、接続を拒否することを検証しなければならない。

   c. [条件： TOE がクライアントである] DHE または ECDHE 暗号スイートがサポートされている場合、サーバの KeyExchange ハンドシェイクメッセージの署名ブロックを改変し、クライアントが Server KeyExchange を受信後、接続を拒否することを検証すること。

   d. [条件： TOE がクライアントである] Server Finished ハンドシェイクメッセージ中のバイトを改変し、クライアントが受信に対する fatal alert を送信し、アプリケーションデータが送信されないことを検証すること。

D.2.3 FCS_SSH_EXT.1　拡張：選択された SSH

(FTP_ITC.1.1、FTP_TRP.1.1 での選択)

下位階層：　なし

依存性：　　なし

¶ 1227 **FCS_SSH_EXT.1.1**　TSF は、RFC 4251、4252、4253、4254、及び［選択：*5656*、*6668*、*その他の RFC なし*］に適合する SSH プロトコルを実装しなければならない。

¶ 1228 ***適用上の注釈：***

¶ 1229 *ST 作成者は、追加の RFC のどれに対して適合を主張するかを選択する。これらは、本コンポーネントの後続のエレメント（例、許可された暗号アルゴリズム）における選択と一貫している必要があることに注意すること。*

¶ 1230 *本 PP の次期バージョンにおいて、鍵変更(rekeying)に関する要件が追加されるかもしれない。本要件は、「TSF は、その鍵を用いて 228 パケットを超えて送信されないように、SSH 接続は鍵変更されることを保証しなければならない。」と読み替えることになる。*

¶ 1231 **FCS_SSH_EXT.1.2**　TSF は、SSH プロトコル実装が RFC 4252 に記述されている次の認証方法をサポートしていることを保証しなければならない：公開鍵ベース、パスワードベース。

¶ 1232 **保証アクティビティ：**

¶ 1233 ***TSS：***

¶ 1234 評価者は、認証に使用可能な公開鍵アルゴリズムについての記述が TSS に含まれていること、このリストが FCS_SSH_EXT.1.5 に適合すること、及びパスワードベース認証方法も許可され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。

¶ 1235 ***テスト：***

¶ 1236 評価者は、次のテストについても実施しなければならない：

1. 評価者は、サポートされているそれぞれの公開鍵アルゴリズムについて、TOE が利用者接続を認証するための公開鍵アルゴリズム

の使用をサポートしていることを示さなければならない。本テストをサポートするために要求されるあらゆる設定アクティビティが、操作ガイダンスにおける指示に従って実行されなければならない。

2. 操作ガイダンスを使用して、評価者はパスワードベース認証を許可するよう TOE を設定し、利用者が認証コードとしてパスワードを用いて SSH 越しに TOE への認証を成功できることを実証しなければならない。

¶ 1237 **FCS_SSH_EXT.1.3** TSF は、RFC 4253 に記述されているように、SSH トランスポート接続における［割付：*バイト数*］以上のパケットが廃棄されることを保証しなければならない。

¶ 1238 ***適用上の注釈：***

¶ 1239 *RFC 4253 は、「大きなパケット」の許容について、「妥当な長さ」のパケットであるかまたは廃棄するべきパケットかについての警告を提供している。割付は、TOE における「妥当な長さ」を定義することによって、ST 作成者によって最大許容パケットサイズが記入されるべきである。*

¶ 1240 **保証アクティビティ：**

¶ 1241 ***テスト：***

¶ 1242 評価者は、TOE が本コンポーネントで指定されたよりも長いパケットを受信した場合、パケットが廃棄されることを実証しなければならない。

¶ 1243 **FCS_SSH_EXT.1.4** TSF は、SSH トランスポート実装が、以下の暗号アルゴリズムを使用することを保証しなければならない：AES-CBC-128、AES-CBC-256、［選択：*AEAD_AES_128_GCM*、*AEAD_AES_256_GCM*、*その他のアルゴリズムなし*］。

¶ 1244 ***適用上の注釈：***

¶ 1245 *割付において、ST 作成者は、AES-GCM アルゴリズム、または AES-GCM がサポートされていない場合は、「その他のアルゴリズムなし」を選択することができる。AES-GCM が選択された場合、ST の FCS_COP のエントリと対応しているべきである。*

¶ 1246 **保証アクティビティ：**

¶ 1247 ***TSS：***

¶ 1248 評価者は、オプションの特性が指定されていること、及びサポートされている暗号アルゴリズムが同様に指定されていることを保証するため、TSS における本プロトコルの実装に関する記述をチェックしなければならない。評価者は、指定された暗号アルゴリズムが本コンポーネントで列挙されているものと同一であ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。評価者は、SSH が TSS における記述に適合するように(例えば、TOE により公表された一連のアルゴリズムが、要件を満たすよう限定されなければならないかもしれない)、操作ガイダンスが TOE の設定に関する指示を含んでいることを保証するために操作ガイダンスについてもチェックしなければならない。

¶ 1249 ***テスト：***

¶ 1250 評価者は、次のテストについても実行しなければならない：

¶ 1251 評価者は、本要件により指定されたそれぞれの暗号アルゴリズムを使用して、SSH 接続を確立しなければならない。テストの意図を満たすため、アルゴリズムのネゴシエーションに成功することを（LAN 上で）観測すれば十分である。

¶ 1252 **FCS_SSH_EXT.1.5** TSF は、SSH トランスポート実装が、公開鍵アルゴリズムとして、［選択：*SSH_RSA*、*ecdsa-sha2-nistp256*］及び［選択：*PGP-SIGN-RSA*、*PGP-SIGN-DSS*、*ecdsa-sha2-nistp384*、*その他の公開鍵アルゴリズムなし*］を使用することを保証しなければならない。

¶ 1253 **保証アクティビティ：**

¶ 1254 FCS_SSH_EXT.1.4 に関連する保証アクティビティにて、本要件を検証する。

¶ 1255 **FCS_SSH_EXT.1.6** TSF は、SSH トランスポート接続において使用されるデータ真正性アルゴリズムが［選択： *HMAC-SHA1*、*HMAC-SHA1-96*、*HMAC-SHA2-256*、*HMAC-SHA2-512*］であることを保証しなければならない。

¶ 1256 ***適用上の注釈：***

¶ 1257 *RFC 6668 は、SSH における sha2 アルゴリズムの使用を指定している。*

¶ 1258 **保証アクティビティ：**

¶ 1259 ***TSS：***

¶ 1260 評価者は、サポートされるデータ真正性アルゴリズムが TSS に列挙されていること、及びそのリストが本コンポーネントのリストに対応し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。評価者は、許可されたデータ真正性アルゴリズムのみが TOE との SSH 接続で使用されること（特に、「非」MAC アルゴリズムは許可されていないこと）を確認する方法についての管理者向けの指示を操作ガイダンスに含んでいることを保証するため、操作ガイダンスについてもチェックしなければならない。

¶ 1261 ***テスト：***

¶ 1262 評価者は、次のテストについても実行しなければならない：

¶ 1263 評価者は、本要件により指定されたそれぞれの真正性アルゴリズムを用いて、SSH 接続を確立しなければならない。テストの意図を満たすため、アルゴリズムのネゴシエーションの成功を（LAN 上で）観測することで十分である。

¶ 1264 **FCS_SSH_EXT.1.7** TSF は、diffie-hellman-group14-sha1 及び［選択：*ecdh-sha2-nistp256*、 *ecdh-sha2-nistp384*、*ecdh-sha2-nistp521*、*その他の方法なし*］が、SSH プロトコルで使用される、唯一の許可された鍵交換方法であることを保証しなければならない。

¶ 1265 **保証アクティビティ：**

¶ 1266 ***操作ガイダンス：***

¶ 1267 評価者は、SSH のためのすべての鍵交換が DH グループ 14、及び ST の選択より指定されたあらゆるグループを用いて実行されるように、セキュリティ管理者が TOE を設定することを許可するような設定情報が操作ガイダンスに含まれていることを保証しなければならない。この能力が TOE に「ハードコード」されている場合、評価者は、これが SSH プロトコルの議論において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。

¶ 1268 ***テスト：***

¶ 1269 評価者は次のテストについても実行しなければならない：

¶ 1270 評価者は、diffie-hellman-group1-sha1 鍵交換の実行を試行しなければならない、そして、その試行が失敗することを観測しなければならない。

それぞれの許可された鍵交換方法について、評価者は、その方法を用いた鍵交換の実施を試行しなければならない、そして、その試行が成功することを観測しなければならない。

D.2.4 FCS_HTTPS_EXT.1　拡張：選択された HTTPS

(FTP_ITC.1.1、FTP_TRP.1.1 での選択)

下位階層：　なし

依存性：　　なし

¶ 1271 **FCS_HTTPS_EXT.1.1** TSF は、RFC 2818 に適合する HTTPS プロトコルを実装しなければならない。

¶ 1272 ***適用上の注釈：***

¶ 1273 *ST 作成者は、識別された規格に実装がどのように適合しているかを決定するために十分な詳細情報を提供しなければならない；これは、本コンポーネントにエレメントを追加したり、TSS に詳細情報を追加したりすることによって実施することができる。*

¶ 1274 **FCS_HTTPS_EXT.1.2** TSF は、FCS_TLS_EXT.1 で指定されるとおり TLS を用いた HTTPS を実装しなければならない。

¶ 1275 **保証アクティビティ：**

¶ 1276 ***TSS：***

¶ 1277 評価者は、TLS プロトコルによって要求されるクライアント認証と、異なるレベルの処理スタックにて行われるセキュリティ管理者認証と、に焦点を当てて、TSS が管理者セションを確立するために HTTPS がどのように TLS を使用するかを明確にし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。

¶ 1278 ***テスト：***

¶ 1279 本アクティビティのテストは、TLS テストの一部として行われる；これは、TLS テストが TLS プロトコルレベルで実施される場合、テストが追加されることになる。

D.2.5 FCS_COP.1(g)　暗号操作 (鍵付ハッシュメッセージ認証)

(FCS_IPSEC_EXT.1.4 と共に選択)

下位階層：　なし

依存性：　~~[FDP_ITC.1 セキュリティ属性なしの利用者データのインポート、または~~
~~FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~
FCS_CKM.1(b)　暗号鍵生成(対称鍵)]
FCS_CKM_EXT.4　拡張：暗号鍵材料破棄

¶ 1280 **FCS_COP.1.1(g)　詳細化**：TSF は、以下を満たすメッセージダイジェスト長［選択：160、224、256、384、512］ビット、［割付：HMAC で利用される鍵長（ビット）］の鍵長、及び指定された暗号アルゴリズム HMAC-［選択: SHA-1、SHA-224、SHA-256、SHA-384、SHA-512］に従って、鍵付ハッシュメッセージ認証を実行しなければならない：FIPS PUB 198-1、「The Keyed-Hash Message Authentication Code」、及び FIPSPUB 180-3、「Secure Hash Standard」。

¶ 1281 **保証アクティビティ：**

¶ 1282 ***テスト：***

¶ 1283 評価者は、上記要件をテストする際のガイドとして、「The Keyed-Hash Message AuthenticationCode (HMAC) Validation System (HMACVS)」を使用しなければならない。これは、評価者がテスト中に検証可能なテストベクトルの生成が可能な、良いものであると知られているアルゴリズムの参照実装を持っていることを要求している。

D.2.6 FIA_PSK_EXT.1　拡張：事前共有鍵生成

(FCS_IPSEC_EXT.1.4 と共に選択)

下位階層：　なし

依存性：　FCS_RBG_EXT.1 拡張：暗号操作（乱数ビット生成）

¶ 1284 ***適用上の注釈：***

¶ 1285 *TOE は、IPsec プロトコルにおいて使用される事前共有鍵をサポートしなければならない。TOE によってサポートされる事前共有鍵には 2 種類あり、以下の要件で指定されるように、（必須の）テキストベースと（オプションの）ビットベースのものがある。最初の種類は、「テキストベースの事前共有鍵」と呼ばれ、利用者によって標準の文字セ*

ットから文字列として入力された事前共有鍵であり、パスワードに似ている。そのような事前共有鍵は、文字列がビット列として変換されるよう調整されなければならず、それが鍵として使用される。

¶ 1286 *2 つ目の種類は、「ビットベースの事前共有鍵」（他に標準的な用語がないため）と呼ばれる；これは、管理者からの命令により TSF によって生成された鍵、または管理者によって「直接型（direct form）」に入力された鍵のどちらかである。「直接型」というのは、テキストベースの事前共有鍵の場合と同様に、入力が「調整」なしで鍵として直接使用されることを意味する。その例としては、鍵を形成するビットを表す 16 進数字列がある。*

¶ 1287 *以下の要件は、TOE がテキストベースの事前共有鍵をサポート、及びオプションでビットベースの事前共有鍵をサポートしなければならないということを義務付ける。ただし、ビットベースの事前共有鍵の生成は TOE によって、または操作ガイダンスでなされるかもしれない。*

¶ 1288 **FIA_PSK_EXT.1.1**　TSF は、IPsec 用の事前共有鍵を使用できなければならない。

¶ 1289 **FIA_PSK_EXT.1.2**　TSF は、以下のようなテキストベースの事前共有鍵を許容できなければならない：

- 長さが 22 文字及び［選択：［割付：その他のサポートされた長さ］、その他の長さなし］；
- 大文字、小文字、数字、及び（「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」、及び「)」を含む）特殊文字の組み合わせから作られる。

¶ 1290 **FIA_PSK_EXT.1.3**　TSF は、［選択：SHA-1、SHA-256、SHA-512、［割付：テキスト文字列の調整方法］］を用いて、テキストベースの事前共有鍵を調整しなければならず、［選択：他の事前共有鍵を使用しない；ビットベースの事前共有鍵を受容する；FCS_RBG_EXT.1 で指定された乱数ビット生成器を用いてビットベースの事前共有鍵を生成する］ことができなければならない。

¶ 1291 ***適用上の注釈：***

¶ 1292 *テキストベースの事前共有鍵の長さについて、相互接続性を促進するために、共通の長さ（22 文字）が必要となる。他の長さがサポートさ*

れる場合は、それらを割付に列挙するべきである；この割付はまた、値の範囲（「5 から 55 文字の長さ」等）を指定することができる。

¶ 1293 *FIA_PSK_EXT.1.3 の 2 番目の選択において、ST 作成者は、管理者によって入力されたテキスト文字列が、鍵として使用されるビット列に「調整」される方法を書き込む。これは、指定のハッシュ関数の一つ、または割付のステートメントを通してその他の方法を使用することで実行される。「ビットベースの事前共有鍵」が選択される場合、ST 作成者は TSF がビットベースの事前共有鍵を単に受容するのか、またはそれらを生成することができるのか指定する。それらを生成する場合、本要件により指定された RBG を用いてそれらは生成されなければならないことと本要件が指定した。ビットベースの事前共有鍵の使用がサポートされていない場合、ST 作成者は「その他の事前共有鍵を使用しない」を選択すること。*

¶ 1294 **保証アクティビティ：**

¶ 1295 ***操作ガイダンス：***

¶ 1296 評価者は、操作ガイダンスが強固なテキストベースの事前共有鍵の構成に関するガイダンスを提供すること、及び（選択がさまざまな長さの鍵を入力できることを示唆する場合）操作ガイダンスが短いまたは長い事前共有鍵の長所に関する情報を提供すること、を決定するために操作ガイダンスを検査しなければならない。ガイダンスは、事前共有鍵として許容される文字を指定しなければならず、そのリストは、FIA_PSK_EXT.1.2 に含まれたリストのスーパーセットでなければならない。

¶ 1297 ***TSS：***

¶ 1298 評価者は、22 文字のテキストベースの事前共有鍵がサポートされていること、及びテキストベースの事前共有鍵を利用者によって入力されたキー入力（例、ASCII 表現）から IPsec によって使用されるビット列への変換が行われる調整が TSS に記述されていること、及びこの調整が FIA_PSK_EXT.1.3 の要件の最初の選択と一貫し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。割付が調整を指定するために使用される場合、評価者は TSS がこの調整について記述していることを確認すること。

¶ 1299 「ビットベースの事前共有鍵」が選択された場合、評価者は本要件で

識別されたそれぞれのプロトコルのためのビットベースの事前共有鍵を入力するのか、またはビットベースの事前共有鍵を生成するかのどちらか（またはその両方）についての指示が、操作ガイダンスに含まれていることを保証しなければならない。評価者は、TSS にビットベースの事前共有鍵が生成されるプロセス（TOE がこの機能をサポートする場合）が記述されていることを保証し、このプロセスが FCS_RBG_EXT.1 で指定された RBG を使用することを確認するため、TSS についても検査しなければならない。

¶ 1300 *テスト：*

¶ 1301 評価者は、次のテストについても実行しなければならない：

1. 評価者は、操作ガイダンスに適合する、すべての許容される文字の組み合わせを網羅した 22 文字の事前共有鍵を少なくとも 15 個以上作成しなければならず、それぞれの鍵でプロトコルネゴシエーションが成功できることを実証すること。

2. [条件付き]： TOE が複数の長さの事前共有鍵をサポートする場合、評価者は、最大限の長さ、最小限の長さ、及び無効な長さのものを用いて、テスト 1 を繰り返さなければならない。最低限及び最大限の長さのテストは成功するべきであり、無効な長さのテストは TOE によって拒否されなければならない。

3. [条件付き]：TOE がビットベースの事前共有鍵をサポートするが、そのような鍵を生成しない場合、評価者は、適切な長さのビットベースの事前共有鍵を入手し、操作ガイダンスの指示に従って入力しなければならない。そして、評価者は、その鍵でプロトコルネゴシエーションが成功できることを実証しなければならない。

4. [条件付き]：TOE がビットベースの事前共有鍵をサポートし、そのような鍵を生成する場合、評価者は、適切な長さのビットベースの事前共有鍵を生成し、操作ガイダンスの指示に従って入力しなければならない。そして、評価者は、その鍵でプロトコルネゴシエーションが成功できることを実証しなければならない。

D.3　高信頼アップデート

D.3.1 FCS_COP.1(c)　暗号操作（ハッシュアルゴリズム）

(FPT_TUD_EXT.1.3 で選択、または FCS_SNI_EXT.1.1 と共に選択)
下位階層：　　なし
依存性：　　なし

¶ 1302 **FCS_COP.1.1(c) 詳細化：** TSF は、以下：**[ISO/IEC 10118-3:2004]** に合致する [選択：***SHA-1***、***SHA-256***、***SHA-384***、 ***SHA-512***] に従った**暗号ハッシュサービス**を実行しなければならない。

¶ 1303 ***適用上の注釈 (O.STORAGE_ENCRYPTION):***

¶ 1304 *ハッシュの選択は、FCS_COP.1(d) で使用されるアルゴリズムの総合的な強度と一貫していなければならない。(SHA 256 は AES 128- ビット長の鍵に対して選択され、 SHA 512 は AES-256 ビット長の鍵に対して選択されるべきである) 規格の選択は選択されたアルゴリズムに基づき行われる。*

¶ 1305 *ベンダは、SHA-2 ファミリをサポートする更新されたプロトコルを実装するよう強く推奨される；更新されたプロトコルがサポートされるまで、本 PP は、SP 800-131A に適合する SHA-1 実装のサポートを許容する。*

¶ 1306 **保証アクティビティ：**

¶ 1307 ***TSS：***

¶ 1308 評価者は、ハッシュ関数とその他の TSF 暗号機能（例えば、デジタル署名検証機能）との関係が 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。

¶ 1309 ***操作ガイダンス ：***

¶ 1310 評価者は、必要とされるハッシュ長についての機能を設定するために実行しておく必要のある設定すべて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。

¶ 1311 ***テスト：***

¶ 1312 TSF ハッシュ関数は、2 つのモードのいずれかを実装することができる。最初のモードは、バイト指向モードである。このモードでは、TSF、整数バイト長のメッセージのみをハッシュする；すなわち、ハッシュ

されるメッセージ長（ビット）は 8 で割り切れる。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。

¶ 1313 評価者は、TSF によって実装され、本 PP の要件を満たすために使用さ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。

¶ 1314 **ショートメッセージテスト － ビット指向モード**

¶ 1315 評価者は、m+1 個のメッセージからなる入力セットを考案する。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分布する。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。評価者、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供される際に正しい結果が得られることを確認し保証する。

¶ 1316 **ショートメッセージテスト － バイト指向モード**

¶ 1317 評価者は、m/8+1 個のメッセージからなる入力セットを考案する。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分布し、各メッセージは整数バイトとなる。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、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供される際に正しい結果が得られることを確認し保証する。

¶ 1318 **選択されたロングメッセージテスト － ビット指向モード**

¶ 1319 評価者は、m 個のメッセージからなる入力セットを考案する。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 では、i 番目のメッセージ長は、512+99*i となる。ここで $1 \leq i \leq m$ とする。SHA-512 では、i 番目のメッセージ長は、1024+99*i となる。ここで $1 \leq i \leq m$ とする。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。評価者は、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供される際に正しい結果が得られることを確認し保証する。

¶ 1320 **選択されたロングメッセージテスト － バイト指向モード**

¶ 1321 評価者は、m/8 個のメッセージからなる入力セットを考案する。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 では、i 番目のメッセージ長は、512+8*99*i となる。ここで 1 ≤ i ≤ m/8 とする。SHA-512 では、i 番目のメッセージ長は、1024+8*99*i となる。ここで 1 ≤ i ≤ m/8 とする。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。評価者は、各メッセージのメッセージダイジェストを計算し、メッセージが TSF へ提供される際に正しい結果が得られることを確認し保証する。

¶ 1322 **疑似ランダム的に生成されたメッセージのテスト**

¶ 1323 本テストは、バイト指向の実装のみを対象とする。評価者は、n ビット長のシードをランダムに生成する。ここで n はテスト対象のハッシュ関するによって生成されるメッセージダイジェスト長とする。次に、評価者は、セキュアハッシュアルゴリズム検証システム（SHAVS）の Figure 1: Code for Generating Pseudorandom Messages で提供されるアルゴリズムに従って、100 個のメッセージとそのダイジェストのセットを考案する。そして、評価者は、それらのメッセージが TSF へ提供される際に正しい結果が得られることを確認し保証する。

D.4　パスフレーズによる鍵入力

¶ 1324 本セクションにおける SFR は、オプションのパスフレーズによる鍵入力機能をサポートする ST に含まれるべきものである。

D.4.1 FCS_PCC_EXT.1　拡張：暗号パスワードの生成と調整

(O. STORAGE_ENCRYPTION)

下位階層：　なし

依存性：　FCS_COP.1(h) 暗号操作（鍵付ハッシュメッセージ認証）

¶ 1325 **FCS_PCC_EXT.1.1** パスワード認証ファクタを生成するために使用されるパスワードは、[割付：*64 以上の正の整数*]文字までの文字列を有効とし、｛大文字、小文字、数字、及び[割付：*その他の特殊文字*]｝からなる、また、特定された暗号アルゴリズム[HMAC-[選択：*SHA-256*、*SHA-384*、*SHA-512*]]に従い[割付：*1000 以上の正の整数*]回の繰り返しを行い、暗号鍵長[選

択：*128*、*256*]を出力するパスワードベースの鍵導出関数を実行しなければならない。ここで、以下を満たすこと：[**NIST SP 800-132**]。

¶ 1326 **適用上の注釈：**

¶ 1327 *本 SFR は、ドライブ暗号化パスフレーズの手動入力が TOE によりサポートされている場合、条件付きで要求される。*

¶ 1328 **保証アクティビティ：**

¶ 1329 ***TSS：***

¶ 1330 評価者は、TOE がパスワードの生成を実行している方法が、長さや文字（数や種類）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。TSS もパスワードがどのように調整されているかの記述を提供しており、評価者はそれが要件を満たすことを保証する。

¶ 1331 ***KMD：***

¶ 1332 評価者は、BEV や中間鍵の構造が記述されていること、及び鍵サイズが ST 作成者による選択と一致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。

¶ 1333 評価者は、パスワード／パスフレーズが初めにエンコードされ、SHA アルゴリズムへ供給される方法が 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）が記述されなければならず、評価者は、本コンポーネント内の選択によりサポートされていることをハッシュ関数自身に関係する選択と同様に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、その機能へ入力され、上記で特定される BEV と同じ長さのサブマスクを形成するためにどのよう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。

¶ 1334 ***テスト：***

¶ 1335 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：

¶ 1336 テスト 1 ：TOE が最小の長さ 64 文字のパスワード／パスフレーズをサポートすることを保証する。

¶ 1337 テスト 2 ：TOE がパスワード／パスフレーズの最大数の文字の長さ、n（64 より大きい）をサポートする場合、TOE が n 文字よりも大きいものを受け入れないことを保証する。

¶ 1338 テスト３：TOE が ST 作成者により割り付けられ、サポートされているすべての文字からなるパスワードをサポートしていることを保証する。

D.4.2 FCS_KDF_EXT.1　拡張：暗号鍵導出

（O.STORAGE_ENCRYPTION）

下位階層：　なし

依存性：　FCS_COP.1(h) 暗号操作（鍵付ハッシュメッセージ認証）、[選択した場合：FCS_RBG_EXT.1　拡張：暗号操作（乱数ビット生成）]

¶ 1339 **FCS_KDF_EXT.1.1** TSF は、[選択： FCS_RBG_EXT.1 で特定されたとおり RNG が生成したサブマスク、調整されたパスワードサブマスク、インポートされたサブマスク] を[選択：NIST SP800-108 [選択：カウンターモードでの KDF、フィードバックモードでの KDF、ダブルパイプライン繰返しモードでの KDF]、NIST SP800-132] に定義されるとおり、その出力が少なくとも BEV と等しいセキュリティ強度（ビット数において）となるような FCS_COP.1(h)で特定される鍵付ハッシュ関数を用いて中間鍵を導出することを受け入れなければならない。

¶ 1340 **保証アクティビティ：**

¶ 1341 ***TSS：***

¶ 1342 評価者は、鍵導出関数の記述が TSS に含まれていることを検証しなければならない、また鍵導出が SP800-108 及び SP800-132 に従い承認された導出モードと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。

¶ 1343 ***KMD：***

¶ 1344 評価者は、使用されるすべての鍵が承認された方法を使い導出されること、及び鍵がいつどのように導出されるか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。

D.4.3 FCS_COP.1(h)　暗号操作（鍵付ハッシュメッセージ認証）

（FCS_PCC_EXT.1、FCS_KDF_EXT.1.1 と共に選択）

下位階層：　なし

依存性：　[~~FDP_ITC.1 セキュリティ属性なしの利用者データのインポート、または~~

~~FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または~~

FCS_CKM.1(b)　暗号鍵生成（対称鍵）]

FCS_COP.1(c)　暗号操作（ハッシュアルゴリズム）、

FCS_CKM_EXT.4　拡張：暗号鍵材料破棄

¶ 1345 **FCS_COP_EXT.1.1(h) 詳細化：**TSF は、以下を満たすような［選択: *HMAC-SHA-1*、*HMAC-SHA-256*、*HMAC-SHA-512*］及び暗号鍵長［割付：*HMAC で使用される鍵長（ビット）*］に従い、［**鍵付ハッシュメッセージ認証**］を実行しなければならない：［**ISO/IEC 9797-2:2011、Section 7 "MAC Algorithm 2"**；ISO/IEC 10118］。

¶ 1346 ***適用上の注釈：***

¶ 1347 *割付における鍵長[k]は、L1 及び L2 の間の範囲であること（適切なハッシュ関数として ISO/IEC 10118 で定められている、例えば、SHA-256 の場合 L1=512、L2=256）ここで、L2 ≤ k ≤ L1 とする。*

¶ 1348 **保証アクティビティ：**

¶ 1349 ***TSS：***

¶ 1350 評価者は、HMAC 関数で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：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。

¶ 1351 ***テスト：***

¶ 1352 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、テストデータの 15 セットを考案しなければならない。それぞれのセットは、鍵とメッセージデータから構成されなければならない。評価者は、テストデータの 3 セットについて HMAC タグを TSF に生成させなければならない。生成された MAC タグは、既知の良い実装を用いた同じ鍵による HMAC タグ生成結果と比較されなければならない。

D.4.4 FCS_SNI_EXT.1　拡張：暗号操作（ソルト、ノンス、及び初期化ベクトル生成）

(FCS_PCC_EXT.1、FCS_KDF_EXT.1.1 と共に選択)

下位階層：　　なし

依存性：　　FCS_RBG_EXT.1 拡張：暗号操作（乱数ビット生成）

¶ 1353 **FCS_SNI_EXT.1.1**　TSF は、**FCS_RBG_EXT.1 で特定された RNG** により生成されたソルトのみを使用しなければならない。

¶ 1354 **FCS_SNI_EXT.1.2**　TSF は、[64]ビットの最小長で一意的なノンスのみを使用しなければならない。

¶ 1355 **FCS_SNI_EXT.1.3**　TSF は、以下の方法で IV を生成しなければならない：[

- CBC： IV は、繰り返ししてはならない。
- CCM：ノンスは、繰り返してはならない。
- XTS： IV はない。 Tweak 値は、連続的に割り付けられ、任意の負でない整数で開始する、負でない整数、でなければならない。
- GCM： IV は繰り返してはならない。GCM の呼び出し回数は、所与の秘密鍵について 2^32 を超えてはならない。

¶ 1356]。

¶ 1357 ***適用上の注釈：***

¶ 1358 *本 SFR は、ドライブ暗号化パスフレーズの手動入力が TOE によりサポートされている場合の条件付きで要求される。*

¶ 1359 **保証アクティビティ：**

¶ 1360 ***TSS：***

¶ 1361 評価者は、ソルトの生成方法が 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 に記述された RBG を用いてソルトが生成されることを確認しなければならない。

¶ 1362 評価者は、ノンスが一意的に生成され、IV や tweak が（AES モードに基づき）どのように取り扱われるかについて 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、ノンスが一意的であること、及び 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。

附属書 E エントロピーに関する文書及び評定

¶ 1363 本附属書は、TOE により使用されるそれぞれのエントロピー源について要求される補足情報について記述している。

¶ 1364 エントロピー源の文書は、それを読んだ後、評価者が完全にエントロピー源を理解し、それがエントロピーを提供すると信頼できる理由を理解できるように、十分に詳細であるべきである。この文書には、設計の記述、エントロピーの正当化、運用条件、及びヘルステストという、複数の詳細なセクションが含まれるべきである。この文書は、TSS の一部である必要はない。

E.1 設計記述

¶ 1365 文書には、すべてのエントロピー源構成要素の相互作用を含めた、それぞれのエントロピー源の全体的な設計が含まれなければならない。これにはエントロピー源の操作が記述され、どのように動作するのか、どのようにエントロピーが作り出されるのか、及びどのように未処理（生の）データをエントロピー源の内部からテスト目的で取得することができるのかが含まれることになる。その文書では、エントロピー源の設計の概略が説明され、ランダム性がどこから由来し、次にどこへ渡されるのか、任意の生の出力の後処理（ハッシュ、XOR 等）、それが（どこに）保存されるのか、そして最後に、どのようにしてエントロピー源から出力されるのかを示すべきである。処理に課される条件（例えば、ブロッキング）があれば、それもエントロピー源の設計の中で記述されるべきである。図や例を利用することが推奨される。

¶ 1366 この設計にはエントロピー源のセキュリティ境界の内容の記述、及び境界外部の敵対者が単位当たりのエントロピーに影響を与えられないことがどのようにしてセキュリティ境界によって確認されるのかという記述が含まれなければならない。

¶ 1367 実装される場合、設計の記述は、第三者アプリケーションが RBG にエントロピーを追加する方法の記述を含まなければならない。電源オフと電源オンの間のあらゆる RBG 状態保存の記述は含まれるべきである。

E.2 エントロピーの正当化

¶ 1368 エントロピー源の予測不可能性がどこに由来し、エントロピー源が確率的なふるまいを示すことがなぜ確信できるのか（確率分布の説明と、その分布が特定のエントロピー源によって得られるという正当化を行うことは、これを記述する一つの方法である）という、技術的な議論が存在すべきである。こ

の議論には、期待される単位当たりのエントロピーの記述と、十分なエントロピーが TOE のランダム化シード供給プロセスへ与えられると確認する理由の記述が含まれる。この議論は、エントロピー源がエントロピーを含むビットを生成すると信頼できる理由の正当化の一部となる。

¶ 1369 エントロピーの正当化は、第三者アプリケーションからまたは再起動の間の状態保存から追加された、いかなるデータを含んではならない。

E.3　運用条件

¶ 1370 文書には、エントロピー源がランダムデータを生成すると期待される運用条件の範囲も含まれることになる。同様に、文書にはエントロピー源が十分なエントロピーを供給するとは、もはや保証されないような条件についても記述されなければならない。エントロピー源の故障または機能低下を検出するために使用される方法が含まれなければならない。

E.4　ヘルステスト

¶ 1371 さらに具体的には、すべてのエントロピー源ヘルステスト及びそれらの根拠は、文書化されることになる。これには、ヘルステストの記述、各ヘルステストが行われる頻度及び条件（例えば、起動時、連続的、またはオンデマンドで）、各ヘルステストに期待される結果、エントロピー源が故障した時の TOE のふるまい、及び各テストがエントロピー源において一つ以上の失敗を検知するために適切であると考えられる根拠を含む。

附属書 F 鍵管理記述

¶ 1372 製品の暗号鍵管理の文書化は十分詳細であるべきである、読んだ後で、評価者が十分に製品の鍵管理、鍵が適切に保護されていることを保証するための要件をどのように満たすかを理解するだろう。本文書化は、解説と図を含むべきである。本文書化は、TSS の一部として要求はされないーそれは、別文書として提出され、開発者の保護情報としてマークを付けることができる。

F.1 解説（Essay）

¶ 1373 解説は、鍵チェインにおけるすべての鍵について、以下の情報を提供する：

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

¶ 1374 解説は以下のトピックについても記述する：

¶ 1375 製品がサポートするすべての認証ファクタ、及びそれぞれのファクタがどのように取り扱われるか、あらゆる調整や　実施される組み合わせを含めた記述。

¶ 1376 検証がサポートされる場合、検証のために使用される値や検証を実行するために使用されるプロセスにどのようなものがあるかについても含め、検証のプロセスが記述されなければならない。このプロセスが鍵チェイン中の鍵がこのプロセスによって危殆化させられたり、暴露されたりしないことをどのように保証するかについて記述しなければならない。

¶ 1377 BEV の最終出力へと導く認証プロセス。このセクションは製品により使用される鍵チェインの詳細化をしなければならない。どの鍵が BEV の保護に使用されるか、それらが導出、鍵ラップ、または 2 つの要件の組合せをどのように満たすかについて、初期認証から BEV への直接のチェインを含めて記述しなければならない。その鍵チェインへ追加

されるあらゆる値、または鍵チェインとの対話、及びそれらの値が危殆化したり、または鍵チェインの総合的な強度を暴露したりしないことを保証する保護についても含めなければならない。

¶ 1378 図や解説は、チェインがすべての初期認証値に対する暗号技術的な総当たり攻撃なしに破壊されたりすることがないこと、及び BEV の有効強度が鍵チェインの全般にわたり維持されていることを保証するために、鍵階層を明確に説明する。

¶ 1379 データ暗号化エンジンの記述、その構成要素、及びその実装の詳細（例、ハードウェアについて：デバイスの主たる SOC または別チップのコプロセッサに集積されたもの、ソフトウェアについて：製品、ドライバ、ライブラリ（適用可能な場合）、暗号化／復号のための論理インタフェース、及び暗号化されない領域（例、ブートローダ、マスターブートレコード（MBR）と関連する部分、パーティションテーブル等））の初期化。記述は、デバイスのホストインタフェースからデバイスのデータを保存している永続的メディアへのデータフロー、データ暗号エンジンを迂回するようなデータについての条件に関する情報（例、暗号化されていないマスターブートレコード領域への読み出し-書き込み操作）についても含めるべきである。記述は、いつ利用者が暗号化を有効化するか、製品がすべてのハードストレージデバイスを暗号化するかを保証するためにすべてのプラットフォームを検証するために十分に詳細であるべきである。また、プラットフォームのブート初期化、暗号初期化プロセス、及びどのようなときに製品が暗号化を有効化するかについても記述するべきである。

¶ 1380 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記述することにより、鍵がもはや不要となった時に鍵を破棄するためのプロセス。

F.2　図

¶ 1381 図は、初期の認証ファクタから BEV までのすべての鍵及びチェインへ寄与するあらゆる鍵または値が含まれる。それぞれの鍵の暗号化強度を列挙し、チェインに沿ってそれぞれの鍵が鍵導出または鍵ラッピング（許容されるオプションから）のいずれかでどのように保護されるかについても示されなければならない。図は、チェインにおいてそれぞれの鍵が導出またはラップを解くために使用される入力を示すべきである。

¶ 1382 主な構成要素（メモリやプロセッサのような）及びそれらの間のデータパス、ハードウェアについては、デバイスのホストインタフェース及びデバイスのデータ保存のための永続的メディア、またはソフトウェアについては、利用者または管理者が最初に製品を設定する際にストレージデバイス全体を暗号化することを保証するために TOE が実行するアクティビティが必要とする初期ステップ、について示す機能（ブロック）図。ハードウェア暗号化図はデータ暗号化エンジンの位置とそのデータパスを示さなければならない。

¶ 1383 評価者は、ハードウェア暗号化図が主な構成要素とそのデータパスを示しデータ暗号化エンジンを明確に識別するために十分詳細であることを検証しなければならない。

附属書 G 用語

表 18　用語集

用語	定義	出典
Address Book（アドレス帳）	人の名前または物理的な位置を、機械が使用可能な宛先（例、ファクス電話番号、E メールアドレス、URL）と結びつける電子的保存メカニズム。	
Administrator（管理者）	TOE の一部分またはすべてを管理する権限が特別に付与され、そのアクションが TOE のセキュリティ方針に影響を与える可能性がある利用者。管理者は、TOE のセキュリティ方針の一部を上書きする機能を提供する特権を持つことができる。	[2600.1]
Asset（資産）	TOE 所有者が一般に価値があると認めるエンティティ。	[CC]
Assumption（前提条件）	運用環境の物理的、技術的、管理上の条件または要件で、TOE がセキュリティ機能を提供するために満たさなければならないもの。	
Commercial Off-The-Shelf **（市販の）**	商業用であり、市場で大量に販売される製品のことで、一般市民にとって入手可能であるのとまさに同じ形式で、政府と契約を結んで調達・使用されることが可能である。	[FAR]
Conditionally Mandatory Uses（条件付き必須用途）	TOE に存在する場合、セクション 1.3.1.2 に記述された用途の一つは、評価構成に含まれなければならない。	
Confidential (TSF) Data **秘密の（TSF）データ**	管理者またはデータの所有者でない利用者による暴露または改変のいずれかについて資産が TOE の運用上のセキュリティに影響がある資産。	[2600.1]

Create（作成）	ストレージ装置内のデータに値又は内容を割り当てること。文書処理ジョブの場合、その結果はジョブが起動することであることに注意。	
Credentials（認証情報、クレデンシャル）	利用者またはアプリケーションについての基本的な識別情報を特定する認証データの形式。認証情報は、認証情報を発行された個人、または認証情報の所持者かもしれない個人を、何らかの方法で結び付けることができる。前者は識別のため必要で、後者は様々な形式の権限付与として許容できるかもしれない。	[2600]
Decommission（廃棄）	運用環境における HCD を積極的な活用から撤退させる行動。地理的な位置及び／または所有権の変更も含む。	
Delete（削除）	ストレージ装置内のデータを参照できなくするか、さもなければ利用不可能とすること。文書処理ジョブの場合、その結果はジョブが終了することであることに注意。	
Document（文書）	一般的に永続性を持ち、人または機械によって読むことができる、その上に記録された媒体及び情報。	[610.12]
Document Processing（文書処理）	文書をプリント、スキャン、またはコピーすること。	
Document Processing Job（文書処理ジョブ）	文書に対する文書処理操作の実行を TOE に求める利用者の要求。	
External Authentication	TOE 利用者を認証するための外部 IT エンティティのサービスを使用する識別認証メカニズム。	

External IT Entity（外部 IT エンティティ）	（人間ではなく）IT デバイスである外部エンティティ。	[CC] defines “External Entity”
Field-Replaceable (Unit) **現地交換可能（ユニット）**	故障を修理するために現場で交換可能な最小部品。	[IEEE]
Hardcopy Device **（ハードコピーデバイス）**	電子的文書または画像の物理的媒体を生成または取り扱うシステム。このようなシステムはプリンタ、スキャナ、ファクス装置、デジタルコピー機、デジタル複合機、「オールインワン」及びその他の同様な製品。	[2600]
Internal Authentication **（内部認証）**	TOE の内部に含まれる識別と認証の機能。	
Job	ハードコピーデバイスへ投入される文書処理タスク。一つの処理タスクは一つまたは複数の文書を処理してもよい。	[2600.1]
Job Owner	ジョブを制御する権限を持っており、その文書へアクセスする利用者。通常、このような権限はジョブを投入したり、アクセス制御メカニズム、またはジョブに関連するクレデンシャル（認証情報）を得ることで得られる。	
Local Area Network（ローカルエリアネットワーク）	利用者の敷地内に位置するデータステーション間で、蓄積交換技術を用いず、直接のデータ通信をするためのシリアル転送が利用される非公開のデータネットワーク。	[8802-6]
Local User（ローカル利用者）	HCD と物理的に対話する利用者。	
Modify（改変）	ストレージ装置内のデータの値／内容を変更	

	すること。文書処理ジョブの場合、その結果はジョブの指示またはその他のパラメタが変更されることであることに注意。	
Multifunction Device（デジタル複合機）	複数機能または単一機能の装置に代わり、複数の機能で複合的な目的を達成するハードコピー装置。[Multifunction Printer 及び Multifunction Peripheral としても知られる]	[2600]
Network Printing（ネットワークプリント）	ネットワーク利用者によって行われるプリント動作。	
Network User（ネットワーク利用者）	ネットワーク上で HCD と交信する利用者。	
Nonvolatile Storage Device（不揮発性ストレージデバイス）	電源オフ時に消去しないデータを保存するコンピュータデバイス。	
Normal User（一般利用者）	TOE 内の利用者文書データを処理する機能を実行する権限のある利用者。	
Operational Environment（運用環境）	TOE が運用される環境。	[CC]
Optional Use	TOE に存在してもよい、セクション 1.3.1.3 に記述された用途の一つで、評価構成にオプションとして含まれてもよい。	
Organizational Security Policy（組織のセキュリティ方針）	組織に対するセキュリティ規則、手続き、またはガイドラインのセット。	[CC]
Output Tray（出力トレイ）	TOE のプリントされた出力のための受け皿。	
Protected (TSF) Data	管理者またはデータの所有者でない利用者による改変に関して、TOE の運用上のセキュリ	[2600.1]

	ティに影響があるが、暴露については許容可能な資産。	
Protection Profile（プロテクションプロファイル）	TOE の種別に対するセキュリティニーズについての実装に依存しないステートメント。	[CC]
Read（閲覧／読み出し）	ストレージ装置またはデータ媒体からデータにアクセスすること。（この場合、データ媒体はプリントされたアウトプットかもしれず、そのため、プリントジョブの出力は「閲覧/読み出し」操作となることに注意。	[610.12]
Redeploy（再配置）	HCD をある運用環境から別の運用環境に動かす動作。	
Required Use	評価構成における TOE に存在しなければならないセクション 1.3.1.1 に記述された用途の一つ。	
Security Assurance Requirement（セキュリティ保証要件）	TOE が SFR を満たすような保証の入手方法に関する記述。	[CC]
Security Functional Requirement（セキュリティ機能要件）	TOE のセキュリティ対策方針を標準化された言語に翻訳したもの。	[CC]
Security Objective（セキュリティ対策方針）	識別された脅威に対抗すること、及び／または識別された組織のセキュリティ方針及び／または前提条件を満たすことを目的とするステートメント。	[CC]
Security Target（セキュリティターゲット）	識別された特定の TOE に対するセキュリティニーズについての実装に依存するステートメント。	[CC]

Servicing（保守サービス）	HCD に修理や保守整備を行うこと。	
Standard Protection Profile（標準プロテクションプロファイル）	NIAP によって定義されたプロセスに従って開発されたプロテクションプロファイル。	
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。	[CC]
Temporary Storage （一時保存）	文書処理ジョブの完了後、TOE によって意図的に保持されないデータの保存。	
Threat（脅威）	敵対者の能力、意図、攻撃方法、または、TOE のセキュリティ方針を脅かす可能性のある状況や事象。	[2600.1]
TOE Owner（TOE 所有者）	TOE 資産を保護し、関連するセキュリティ方針を確立する責任を有する個人または組織。	[2600.1]
TOE Security Functionality（TOE セキュリティ機能）	SFR を適切に実施するために必要とされる TOE のすべてのハードウェア、ソフトウェア、及びファームウェアの複合機能。	[CC]
TSF Data（TSF データ）	SFR 実施が依存する TOE のふるまいのためのデータ。	[CC]
TSF interface（TSF インタフェース）	外部エンティティ（または、TSF 外にある TOE 内のサブジェクト）が TSF にデータを供給し、TSF からデータを受信し、TSF からサービスを呼び出す手段。	[CC]
Unauthorized Access（不正アクセス）	利用者がアクセスを許可されていない資源へのアクセス。	
User（利用者）	TOE の外部にあって TOE と対話することがで	[CC]

	きる人間または IT のエンティティ。	
User Data（利用者データ）	利用者に関するデータで、TSF のふるまいに影響を与えないもの。	[CC]
User Document Data（利用者文書データ）	利用者文書に含まれる情報からなる資産。ハードコピーまたは電子フォームのいずれかの形態の原本文書、画像データ、または原本文書及びプリントされたハードコピー出力を処理するようなハードコピーデバイスによって作成された残存の保存データを含む。	[2600.1]
User Job Data（利用者ジョブデータ）	TOE により処理される利用者文書または利用者ジョブについての情報からなる保護資産。	[2600.1]

出典：

[2600] IEEE Std. 2600™-2008 “IEEE Standard for Information Technology: Hardcopy Device and System Security”

[2600.1] IEEE Std. 2600.1™-2009 “IEEE Standard for a Protection Profile in Operational Environment A”

[610.12] IEEE Std 610.12-1990 “IEEE Standard Glossary of Software Engineering Terminology”

[8802-6] ISO /IEC 8802-6:1994 “Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 6”

[CC] ISO/IEC 15408-1:2009 "Information technology – Security techniques – Evaluation criteria for IT security – Part 1"

[FAR] United States Federal Acquisition Regulations

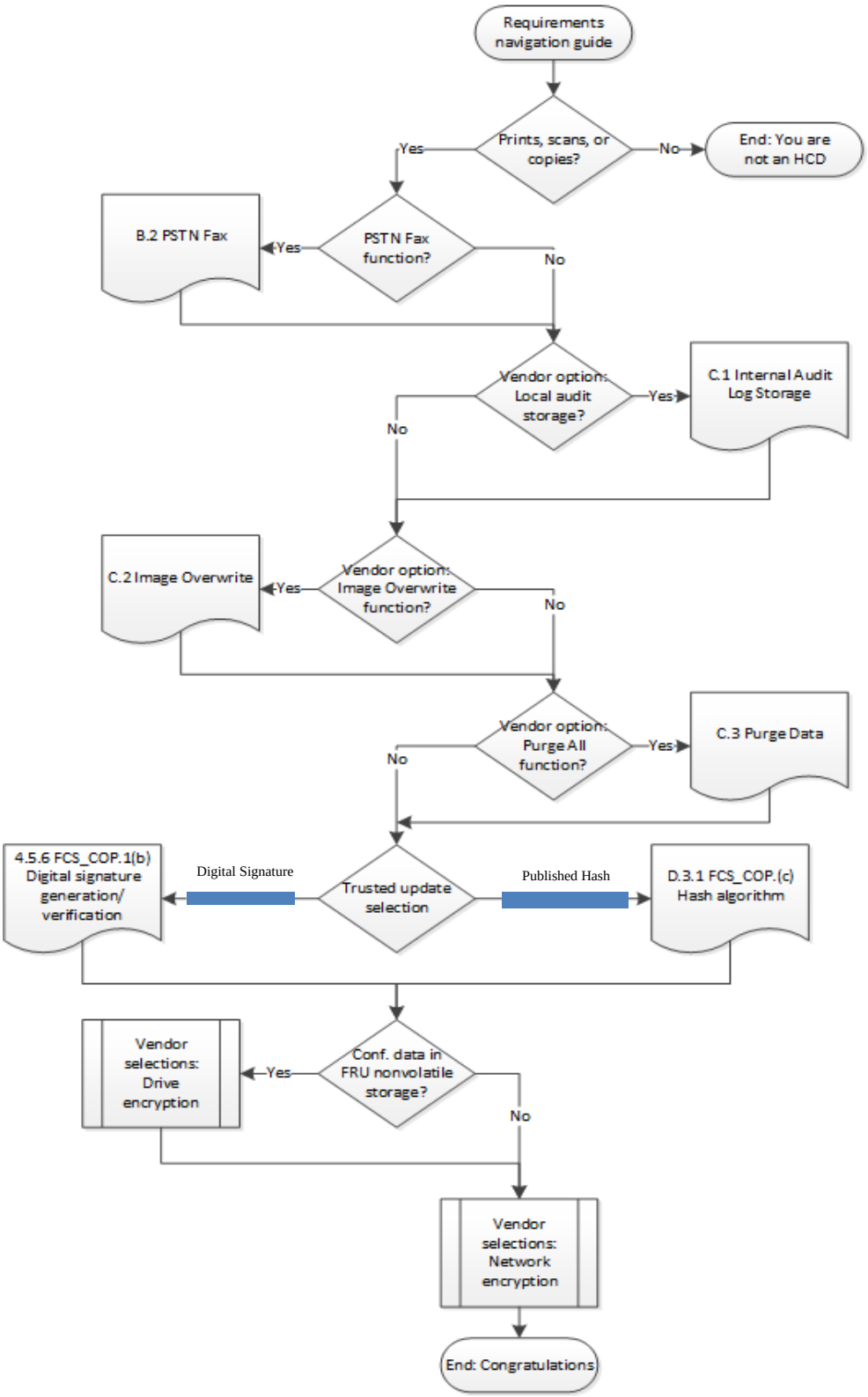
[IEEE] IEEE Standards Dictionary （ISBN 973-0-7381-2601-2）

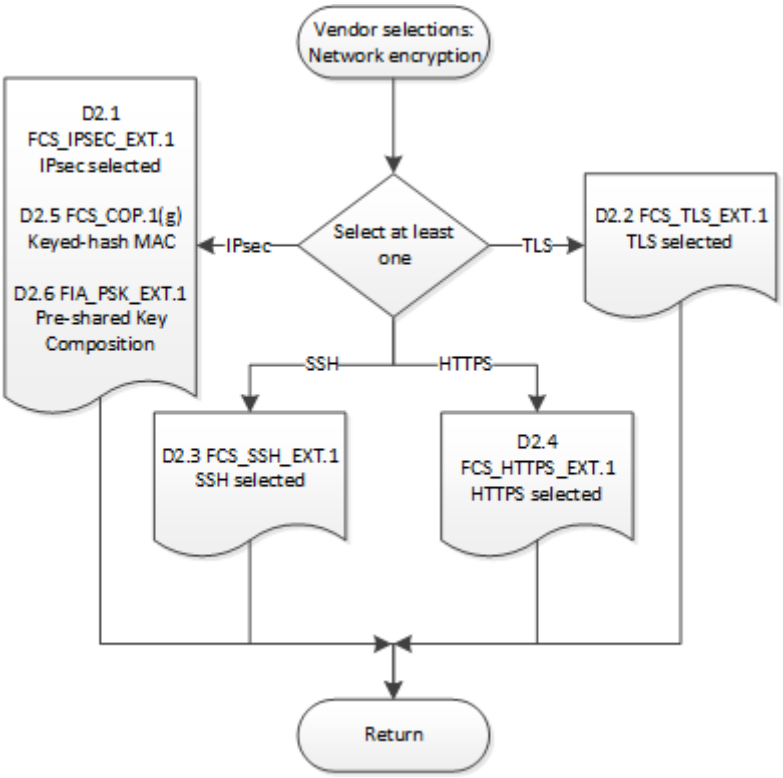
表 19　頭字語

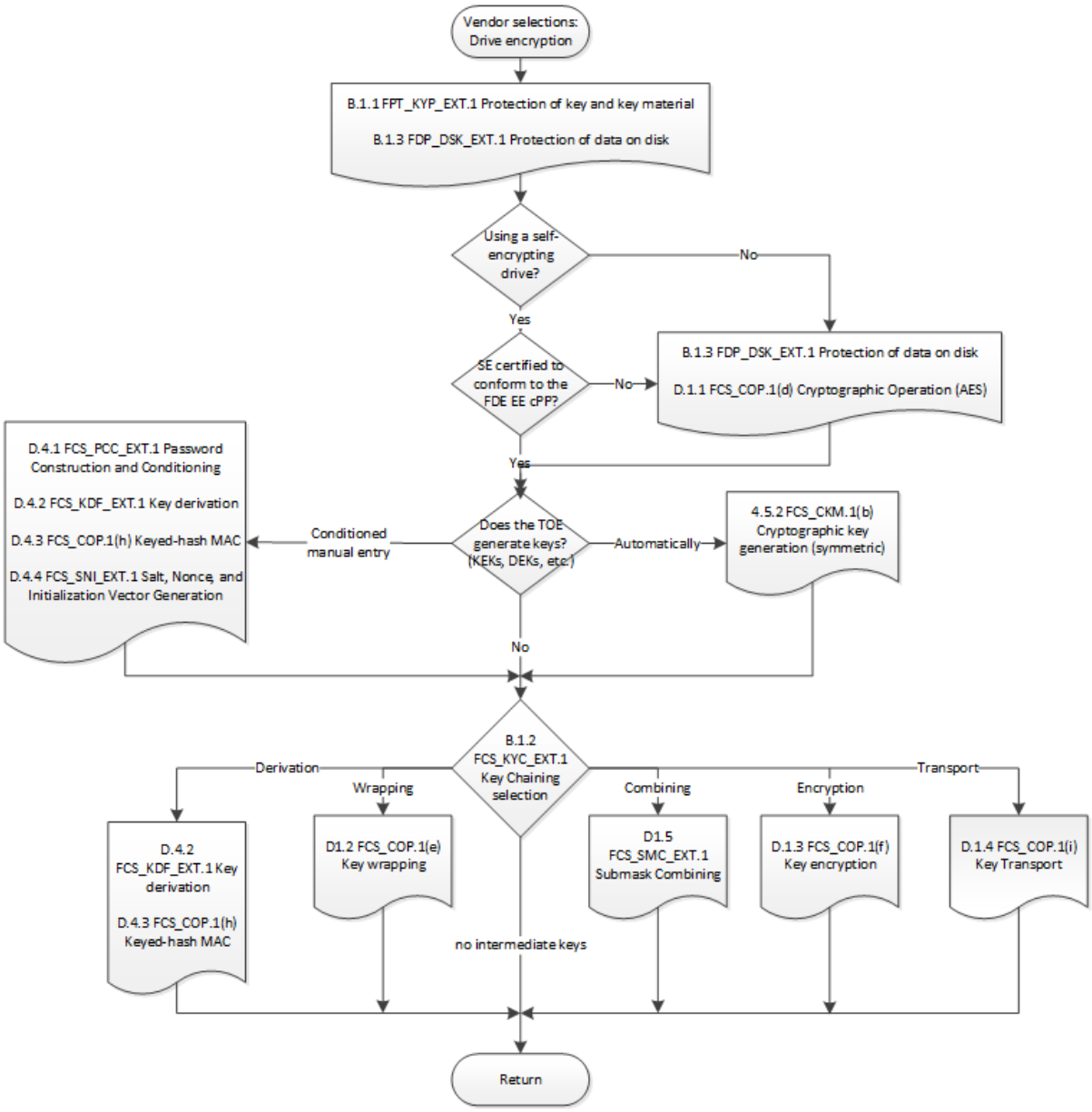
頭字語	定義
BEV	Border Encryption Value
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Service
COTS	Commercial Off-The-Shelf
EAL	Evaluation Assurance Level
HCD	Hardcopy Device
IPA	Information-technology Promotion Agency
I&A	Identification and Authentication
IT	Information Technology
JISEC	Japan Information technology Security Evaluation and Certification scheme
KDF	Key Derivation Function
KMD	Key Management Description
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MFD	Multifunction Device
MFP	Multifunction Printer, Multifunction Peripheral
NIAP	National Information Assurance Partnership
OCSP	Online Certificate Status Protocol

OSP	Organizational Security Policy
PP	Protection Profile
PSTN	Public Switched Telephone Network
RBG	Random Bit Generator
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SPP	Standard Protection Profile
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
TSS	TOE Summary Specification

附属書 H プロテクションプロファイルナビゲーションガイド




Vendor selections:
Network encryption
D2.1
FCS_IPSEC_EXT.1
IPsec selected
D2.5 FCS_COP.1(g)
Keyed-hash MAC
D2.6 FIA_PSK_EXT.1
Pre-shared Key
Composition
IPsec
Select at least
one
TLS
D2.2 FCS_TLS_EXT.1
TLS selected
SSH
HTTPS
D2.3 FCS_SSH_EXT.1
SSH selected
D2.4
FCS_HTTPS_EXT.1
HTTPS selected
Return


Vendor selections: Drive encryption
B.1.1 FPT_KYP_EXT.1 Protection of key and key material
B.1.3 FDP_DSK_EXT.1 Protection of data on disk
Using a self-encrypting drive?
No
Yes
SE certified to conform to the FDE EE cPP?
No
B.1.3 FDP_DSK_EXT.1 Protection of data on disk
D.1.1 FCS_COP.1(d) Cryptographic Operation (AES)
Yes
D.4.1 FCS_PCC_EXT.1 Password Construction and Conditioning
D.4.2 FCS_KDF_EXT.1 Key derivation
D.4.3 FCS_COP.1(h) Keyed-hash MAC
D.4.4 FCS_SNI_EXT.1 Salt, Nonce, and Initialization Vector Generation
Conditioned manual entry
Does the TOE generate keys? (KEKs, DEKs, etc.)
Automatically
4.5.2 FCS_CKM.1(b) Cryptographic key generation (symmetric)
No
B.1.2 FCS_KYC_EXT.1 Key Chaining selection
Derivation
Wrapping
Combining
Encryption
Transport
D.4.2 FCS_KDF_EXT.1 Key derivation
D.4.3 FCS_COP.1(h) Keyed-hash MAC
D1.2 FCS_COP.1(e) Key wrapping
D1.5 FCS_SMC_EXT.1 Submask Combining
D.1.3 FCS_COP.1(f) Key encryption
D.1.4 FCS_COP.1(i) Key Transport
no intermediate keys
Return