ステートフルトラフィックフィルタファイアウォールの
コラボラティブプロテクションプロファイル

バージョン 1.0
2015 年 2 月 27 日

平成 28 年 1 月 15 日　翻訳 暫定第 0.2 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

謝辞

本コラボラティブプロテクションプロファイル (cPP) は、産業界、政府機関、コモンクライテリア評価機関、及び学術会員メンバーからの代表者の参加する、Network international Technical Community によって開発された。

0. 序文

0.1 本書の目的

本書は、ステートフルトラフィックフィルタファイアウォールのセキュリティ機能要件 (SFR) 及びセキュリティ保証要件 (SAR) を記述するコモンクライテリア (CC) コラボラティブプロテクションプロファイル (cPP) として提示する。製品が本 cPP の SFR を満たしているかどうかを決定するために評価者が実行するアクションを特定する評価アクティビティは、 [SD-ND] 及び [SD-FW] に記述される。

0.2 本書の適用範囲

開発及び評価プロセスにおける cPP の適用範囲は、情報技術セキュリティ評価のためのコモンクライテリア [CC] に記述されている。特に、cPP は TOE の一般的な種別に対する IT セキュリティ要件を定義し、[CC1, Section C.1] に記述された要件を満たすためにその TOE によって提供されるべき機能及び保証のセキュリティ対策を特定する。

0.3 意図される読者

本 cPP が対象読者は、開発者、CC 消費者、システムインテグレータ、評価者及びスキーム(評価認証制度関係者)である。

cPP 及び SD には、軽微な編集上の誤りが含まれるかもしれないが、cPP は常に更新される生きた文書として認識されており、iTC は継続的に更新及び改訂を行っていく。何か問題があれば、NDFW iTC へ報告されたい。

0.4 関連する文書

コモンクライテリア [1]

[CC1] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 1：概説と一般モデル
CCMB-2012-09-001、バージョン 3.1 改訂第 4 版、2012 年 9 月。

[CC2] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 2：セキュリティ機能コンポーネント
CCMB-2012-09-002、バージョン 3.1 改訂第 4 版、2012 年 9 月。

[CC3] 情報技術セキュリティ評価のためのコモンクライテリア、
パート 3：セキュリティ保証コンポーネント
CCMB-2012-09-003、バージョン 3.1 改訂第 4 版、2012 年 9 月。

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

[CEM] 情報技術セキュリティ評価のための共通方法、
評価方法
CCMB-2012-09-004、バージョン 3.1 改訂第 4 版、2012 年 9 月。

その他の文書

[SD-FW] ステートフルトラフィックフィルタファイアウォール cPP 評価アクティビティ、バージョン 1.0、2015 年 2 月 27 日

[SD-ND] ネットワークデバイス cPP の評価アクティビティ、バージョン 1.0、2015 年 2 月 27 日

0.5 改版履歴

バージョン	日付	説明
1.0	2015 年 2 月 27 日	正式リリース
0.4	2015 年 1 月 26 日	CCDB レビューからのコメントを取り込み
0.3	2014 年 10 月 17 日	サポート文書の CCDB レビューに伴うドラフト版のリリース
0.2	2014 年 10 月 13 日	iTC レビュー用、公開レビューのコメントに対応した内部ドラフト
0.1	2014 年 9 月 05 日	公開レビュー用ドラフト発行

目次

図 / 表

1. PP 序説

1.1 PP 参照識別

PP 参照：collaborative Protection Profile for Stateful traffic Filter Firewalls
ステートフルトラフィックフィルタファイアウォールのコラボラティブプロテクションプロファイル

PP バージョン：1.0

PP 日付：2015 年 2 月 27 日

1.2 TOE 概要

本コラボラティブプロテクションプロファイル (cPP) は、ステートフルトラフィックフィルタファイアウォール評価用の要件を定義する。このような製品は、一般に境界を保護するデバイスであり、専用ファイアウォール、ルータ、またはスイッチ等のようなもので、接続されたネットワーク間の情報フローを制御するように設計されたものまである。場合によっては、セキュリティ機能を実装したファイアウォールは 2 つの分離されたネットワーク (信頼されたまたは保護された飛び地と、インターネットのような信頼されない内部または外部ネットワーク) を遮断する役割を果たすが、これは数多くの適用可能な事例の 1 つに過ぎない。通常、ファイアウォールは複数の物理的ネットワーク接続を有し、幅広い設定とネットワーク情報フローポリシーを可能とする。

分散型の TOE は、本 cPP の現バージョンの適用範囲外であるが、次バージョンの適用範囲に含まれることが期待される。

1.3 TOE 使用事例

本 PP は、特にネットワークレイヤ 3 及び 4 のステートフルトラフィックフィルタリングを実行するファイアウォールを対象とする。ステートフルトラフィックフィルタファイアウォールは、2 つ以上の異なるネットワークへ接続されたハードウェアとソフトウェアから構成されたデバイスであり、エンタープライズネットワーク全体の基盤としての役割を持つ。

ステートフルトラフィックフィルタリングは、ファイアウォールがそれを通過する各コネクションの状態を追跡し、正当なフローとみなされないパケットを破棄する能力を持つという発想である。TCP シーケンス番号、ACK、IP オプション等の情報もダイナミックステートテーブルにメトリクスを保存することによって保持される。パケットを受け入れ、破棄、またはログ出力を決定する際のその他の検討事項は、送信元及び宛先 IP アドレス及びポート、あるいは送信元または宛先アドレスが設定されたインタフェースと不一致の場合である。

本 PP の将来のドラフトが構想されており、オプション機能 (例、トランスペアレントモード等) が含まれることになる。将来のファイアウォール PP は、追加の機能 (例、アプリケーションフィルタリング等) を特定するために使用されることになる。本 PP において、このような追加の機能は、ここで定義されたセキュリティ要件に何らかの影響を及ぼし得る場合を除いて、評価目的では単に無視される。本 PP への適合評価される多くのデバイスは NAT または PAT を実行する能力を持つが、この能力を特定する要件は存在しない。

2. CC への適合

参考資料 [CC1]、[CC2] 及び [CC3] により定義されるとおり、本 cPP は：

- コモンクライテリア v3.1、改訂第 4 版の要件へ適合し
- パート 2 拡張、パート 3 適合であり
- その他のいかなる PP への適合も主張しない。

cPP 評価へ適用される方法は、 [CEM] に定義されている。本 cPP は、以下の保証ファミリを満たしている：APE_CCL.1，APE_ECD.1，APE_INT.1，APE_OBJ.1，APE_REQ.1 及び APE_SPD.1。

本 cPP に適合するためには、TOE は完全適合 (Exact Conformance) を論証しなければならない。完全適合は、CC に定義されている正確適合 (Strict Conformance) のサブセットとして、本 cPP のセクション 5 のすべての要件 (これらは必須要件である) を含み、本 cPP の附属書 A (これらはオプション SFR である) または附属書 B (これらは選択ベース SFR であって、その一部は他の SFR における選択に従って必須とされる)の要件を含む可能性のある ST として定義されている。繰り返しは許容されるが、いかなる追加の要件 (CC パート 2 または 3 からのもの、または本 cPP に既に含まれているもの以外の拡張コンポーネントの定義からのもの) も ST に含めることは許容されない。さらに、本 cPP のセクション 5 のいかなる要件も、省略は許されない。

3. セキュリティ課題定義

ステートフルトラフィックフィルタファイアウォール (ステートフルパケットインスペクションの利用に最適化されたレイヤ 3 及び 4 (IP 及び TCP/UDP) のネットワークトラフィックをフィルタするデバイスと定義される) は、明確に定義され記述された脅威 (訳注：の顕在化) の軽減を目標とする最小限のベースライン要件を提供することを意図している。

それは、既知のアクティブな (及び許可された) コネクションへのパケットを許可し、それ以外を破棄するための照合する能力を持つ。ファイアウォールは、2 つの別々のネットワークセキュリティドメイン間の境界デバイスとしての役割を果たすことが多く、またそれゆえ、最小限の共通セキュリティ機能を提供しなければならない。これらの機能要件は、ファイアウォールとの正当な通信、監査機能、利用者アクセス、アップデートプロセス、及び重要なコンポーネントの自己テスト手続きを定義する。

3.1 脅威

ステートフルトラフィックフィルタファイアウォールの脅威は、以下のセクションのデバイスの機能領域に従ってグループ化されている。

3.1.1 ファイアウォールとの通信

ファイアウォールは、他のネットワークデバイスや他のネットワークエンティティとの間で通信する。この通信の端点は、地理的にも論理的にも遠く離れている可能性があり、さまざまな他のシステムを通過するかもしれない。中間のシステムは、ファイアウォールとの不正な通信を行ったり、許可された通信がセキュリティ侵害を受けたりするような機会を提供するような、信頼できないものであるかもしれない。ファイアウォールのセキュリティ機能は、任意の重要なネットワークトラフィック (管理トラフィック、認証トラフィック、監査トラフィック等) を保護できなければならない。ファイアウォールとの通信は、許可された通信と不当な通信という 2 つのカテゴリに分類される。

許可された通信には、設計され意図されたとおりに、ファイアウォール宛へ及びファイアウォールからの、ポリシーによって許可される通常のネットワークトラフィックが含まれる。これには、通信を保護するためのセキュアなチャネルが要求され、ファイアウォール管理、及び認証または監査ログサーバとの通信等の重要なネットワークトラフィックが含まれる。ファイアウォールのセキュリティ機能には、許可された通信のみが許されることを保証する機能、及び重要なネットワークトラフィック用のセキュアなチャネルを提供する機能が含まれる。それ以外の任意の通信は、不当な通信と考えられる。

本 cPP 中で対処されるファイアウォール通信への主たる脅威は、重要なネットワークトラフィックに対するアクセス、改変、あるいは暴露を試行する、外部の、許可されないエンティティに焦点を絞っている。暗号アルゴリズムの不十分な選択、または非標準トンネルプロトコルの使用は、容易に推測できるパスワードやデフォルトパスワードの使用等の弱い管理者クレデンシャルと同様に、脅威エージェントに対してファイアウォールへの不正なアクセスを許可することになる。弱い暗号または暗号化なしでは、トラフィックの保護はほとんどまたは全く提供されないため、ほとんど労力なしで脅威エージェントが重要なデータを読み出したり、操作したり、あるいは制御することができてしまう。非標準のトンネルプロトコルは、ファイアウォールの相互接続性を制限してしまうだけでなく、ピアレビューによる規格化が提供する保証及び信頼を欠くことになる。

3.1.1.1 T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

脅威エージェントは、管理者セションまたはファイアウォールとネットワークデバイスとの間のセションへのアクセスを提供するような、ファイアウォールに対する管理者としてのなりすまし、管理者に対するファイアウォールとしてのなりすまし、管理者セション (全体、または選択された部分) のリプレイ、または中間者攻撃を行う等の不正な手段によって、ファイアウォールへの管理者アクセスの取得を試行するかもしれない。管理者アクセスの取得が成功すると、ファイアウォール及びその存在するネットワークのセキュリティ機能を危殆化するような、悪意のあるアクションが可能となる。

3.1.1.2 T.WEAK_CRYPTOGRAPHY

脅威エージェントは、弱い暗号アルゴリズムを悪用したり、鍵空間に対する暗号の総当たり攻撃を行ったりするかもしれない。不十分に選択された暗号アルゴリズム、モード、及び鍵長は、攻撃者にアルゴリズムのセキュリティの危殆化または鍵空間の総当たり攻撃を許し、不正なアクセスを与えて最小限の労力でトラフィックの読み出し、操作、及び／または制御を許すことになる。

3.1.1.3 T.UNTRUSTED_COMMUNICATION_CHANNELS

脅威エージェントは、重要なネットワークトラフィックを保護するために標準化されたセキュアなトンネルプロトコルを使用していないファイアウォールへの攻撃を試行するかもしれない。攻撃者は、中間者攻撃、リプレイ攻撃等を成功させるために、不十分な設計のプロトコルや不十分な鍵管理を利用するかもしれない。攻撃が成功すれば、重要なネットワークトラフィックの機密性及び完全性が失われる結果となり、またファイアウォール自体のセキュリティの危殆化がもたらされる可能性もある。

3.1.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS

脅威エージェントは、例えば推測可能だったり平文として転送されたりする共有パスワード等、端点を認証するための弱い方法を用いるセキュアなプロトコルを利用するかもしれない。その結果は、不十分な設計のプロトコルと同一であり、攻撃者が管理者または他のデバイスになりすましたり、攻撃者がネットワークストリームに割り込んで中間者攻撃を行ったりすることができてしまう。その結果、重要なネットワークトラフィックが暴露され、機密性及び完全性が失われ、ファイアウォール自体がセキュリティ侵害を受ける可能性がある。

3.1.2 有効なアップデート

ファイアウォールのソフトウェア及びファームウェアのアップデートは、ファイアウォールのセキュリティ機能が維持されることを保証するために必要である。適用されるべきアップデートの供給元及び内容は、暗号技術的な手段によって検証されなければならない；そうでなければ、無効な供給元が、ファイアウォールのセキュリティ機能を迂回するような、独自のファームウェアやソフトウェアのアップデートを書き込むことができてしまう。暗号技術的な手段によるソフトウェアまたはファームウェアアップデートの供給元及び内容を検証する方法には、通常アップデートのハッシュがディジタル的に署名されるような暗号署名スキームが含まれる。

ソフトウェアまたはファームウェアのパッチ適用されていないバージョンは、脅威エージェントが既知の脆弱性を用いてセキュリティ機能の迂回を試行することに対してファイアウォールが影響を受ける状態のままにさせてしまう。検証されていないアップデート、またはセキュアでない、または弱い暗号を用いて検証されたアップデートは、アップデートされたソフトウェアやファームウェアが、自分たちに都合のよいようにソフトウェアやファームウェアを改変しようとする脅威エージェントに対して脆弱な状態にさせてしまう。

3.1.2.1 T.UPDATE_COMPROMISE

脅威エージェントは、デバイスのセキュリティ機能を弱体化させるようなソフトウェアまたはファームウェアの危殆化したアップデートを提供しようとするかもしれない。検証されていないアップデート、またはセキュアでない暗号または弱い暗号を用いて検証されたアップデートは、アップデートファームウェアに不正な改変に対する脆弱性を残してしまう。

3.1.3 監査されたアクティビティ

ファイアウォールの監査は、管理者がデバイスの状態を監視するための重要なツールである。これは、管理者の説明責任、セキュリティ機能アクティビティ報告、事象の再構築、及び問題分析を行う手段を提供する。デバイスアクティビティへの応答として行われた処理が、セキュリティ機能の故障またはセキュリティ侵害を示してくれるかもしれない。セキュリティ機能に影響するアクティビティの表示が生成及び監視されていなければ、そのようなアクティビティが発生しても管理者に気付かれないかもしれない。さらに、記録が生成されず保持されない場合、ネットワークの再構築及びセキュリティ侵害の規模を理解する能力に対して悪影響を与える可能性がある。さらなる懸念は、記録された監査データに対する改変または不正な削除からの保護である。これは、TOE 内で発生することもあれば、監査データの外部ストレージデバイスへの転送中に発生することもある。

本 cPP は、ファイアウォールが監査データを生成すること、及びその監査データを高信頼ネットワークエンティティ (例えば、syslog サーバ) へ送信する機能を有することを要求していることに注意されたい。

3.1.3.1 T.UNDETECTED_ACTIVITY

脅威エージェントは、管理者に気付かれずにファイアウォールのセキュリティ機能をアクセスしたり、変更したり、及び／または改変したりしようとするかもしれない。この結果として、攻撃者がデバイスをセキュリティ侵害するための手段 (例、設定ミス、製品の欠陥等) を発見しても、管理者はデバイスがセキュリティ侵害を受けたことに全く気付かない可能性がある。

3.1.4 管理者及びファイアウォールの認証情報及びデータ

ファイアウォールには、セキュアに保存されなければない、かつ許可されたエンティティに対してアクセスを適切制限しなければならない、データ及びクレデンシャルが含まれている。例としては、ファイアウォールのファームウェア、ソフトウェア、セキュアチャネル用の設定認証クレデンシャル、及び管理者クレデンシャル等が含まれる。ファイアウォール及び管理者の鍵、鍵材料、及び認証クレデンシャルは、不正な暴露及び改変から保護される必要がある。さらに、ファイアウォールのセキュリティ機能は、管理者パスワードのような、デフォルトの認証クレデンシャルが変更されることを要求する必要がある。

設定ファイルの中の暗号化されていないクレデンシャルまたはセキュアチャネルセション鍵へのアクセスのような、セキュアなストレージの欠如及びクレデンシャルやデータへの不適切なアクセスは、攻撃者に対して、ファイアウォールへのアクセスの取得を許すだけでなく、みせかけの許可された設定の改変や中間者攻撃によるネットワークのセキュリティの危殆化を引き起こす可能性がある。これらの攻撃によって、許可されないエンティティが許可された管理者のクレデンシャルを用いて管理機能へのアクセスを取得し、管理機能を実行し、許可された端点としてすべてのトラフィックを傍受することができてしまう。この結果として、セキュリティ侵害の検知及びネットワークの再構築に困難が生じ、管理者及びファイアウォールデータへの不正なアクセスの継続を許してしまう可能性がある。

3.1.4.1 T.SECURITY_FUNCTIONALITY_COMPROMISE

脅威エージェントは、ファイアウォール及びその重要なデータへの継続的なアクセスを可能とするような、クレデンシャルやファイアウォールデータのセキュリティの危殆化を引き起こすかもしれない。クレデンシャルのセキュリティの危殆化には、攻撃者のクレデンシャルによる既存のクレデンシャルの置き換え、既存のクレデンシャルの改変、もしくは攻撃者により使用される管理者またはファイアウォールクレデンシャルの取得が含まれる。

3.1.4.2 T.PASSWORD_CRACKING

脅威エージェントは、ファイアウォールへの特権アクセスを取得するため、弱い管理パスワードを利用できるかもしれない。ファイアウォールへの特権アクセスを取得すれば、攻撃者はネットワークトラフィックへの無制限アクセスを提供してしまい、また他のネットワークデバイスとの信頼関係の利用を許可するかもしれない。

3.1.5 ファイアウォール構成要素の故障

ファイアウォールのセキュリティメカニズムは、信頼のルートからより複雑な一連のメカニズムが構築されるのが一般的である。故障は、ファイアウォールのセキュリティ機能の危殆化を引き起こす可能性がある。起動時及び実行中の両方でセキュリティ上重要な構成要素の自己テストを行うファイアウォールは、ファイアウォールのセキュリティ機能の信頼性を保証する。

3.1.5.1 T.SECURITY_FUNCTIONALITY_FAILURE

ファイアウォールの構成要素は、起動時または運用中に、ファイアウォールのセキュリティ機能の危殆化または故障により、ファイアウォールが攻撃者の影響を受け、機能しなくなるかもしれない。

3.1.6 情報の不正な暴露

保護されたネットワーク上のデバイスは、保護されたネットワークの外部に位置するデバイスにより示される脅威、許可されないアクティビティの試行にさらされるかもしれない。既知の悪意のある外部のデバイスが、保護されたネットワーク上のデバイスと通信できる場合、または保護されたネットワーク上のデバイスが、そのような外部のデバイスとの通信を確立できる場合には、それらの内部のデバイスは、情報の許可されない暴露を許してしまうかもしれない。

侵入の観点からは、ステートフルトラフィックフィルタファイアウォールは、保護されたネットワーク上の特定の*宛先*ネットワークアドレス及びポートのみへのアクセスに制限する役割を果たす。これらの制限により、一般的なネットワークポートスキャンは、保護されたネットワークまたはマシンへの到達を防止でき、また保護されたネットワーク上の情報へのアクセスは、識別されたネットワークノード上の具体的に設定されたポート (例、指定された企業ウェブサーバからのウェブページ等) から取得可能なものに制限することができる。さらに、アクセスを特定の*送信元*アドレス及びポートのみに制限することもでき、これによって特定のネットワークまたはネットワークノードによる保護されたネットワークへのアクセスをブロックでき、さらに情報の暴露の可能性を制限することもできる。

漏えいの観点からは、ステートフルトラフィックフィルタファイアウォールは、保護されたネットワーク上で動作するネットワークノードが他のネットワークと接続及び通信できる方法を制限する役割を、それらが情報を発信できる方法と相手先を制限することで果たす。特定の外部ネットワークを完全にブロックすることができ、外向きのトラフィックを特定のアドレス及び／またはポートに制限することもできる。その代わりに、例えば、外向きのコネクションが、侵出 (流出) によるデータの不適切な暴露をさらに低減させるために、許可されたプロキシまたはフィルタを通るようにルーティングされることを保証する

ため、保護されたネットワーク上のネットワークノードが利用可能な外向きの選択肢を注意深く管理することができる。

3.1.6.1 T.NETWORK_DISCLOSURE

攻撃者は、それらのマシンが提供しているサービス (ポート) と同様に、マシンの IP アドレスを取得し、ネットワーク上に存在するマシンを決定するため、サブネットの「マッピング」を試行するかもしれない。この情報は、エクスポートされているサービスを介してそれらのマシンへの攻撃を仕掛けるために使われるかもしれない。

3.1.7 サービスへの不適切なアクセス

保護されたネットワークの外部に位置するデバイスが、保護されたネットワーク内部からのアクセスのみを意図した保護されたネットワーク上に位置するサービスの行使を試みるかもしれない。同様に、保護されたネットワークの外部に位置するデバイスが、保護されたネットワーク内部からのアクセスには不適切なサービスを提供するかもしれない。

内向きの観点からは、ステートフルトラフィックフィルタファイアウォールは、外部からの利用を意図したネットワークサーバのみが意図されたポートのみを介してアクセス可能であるように設定することができる。これは、保護されたネットワーク内部での利用またはアクセスのみを意図したネットワークサーバまたはサービスへ、保護されたネットワークの外部のネットワークエンティティがアクセスする可能性を低減する役割を果たす。

外向きの観点からは、ステートフルトラフィックフィルタファイアウォールは、特定の外部サービス (例、宛先ポートに基づく等) のみが保護されたネットワーク内部からアクセスできるように設定することができる。例えば、外部メールサービスへのアクセスをブロックすることによって、制御下にない電子メールサーバへのアクセスを禁止するようなコーポレートポリシーを強制することができる。外部サーバは代替ポート上でサービスを提供できるため、ステートフルトラフィックフィルタファイアウォールの有効性は、この点に関してはある程度制限されていることに注意されたい。これは、例えばアプリケーションフィルタファイアウォールがより信頼性の高い保護を提供できる分野である。

3.1.7.1 T. NETWORK_ACCESS

サブネット上のマシンによってエクスポートされているサービスの知識があれば、攻撃者はこれらのサービスに対する攻撃を仕掛けることによって、これらのサービスの悪用を試行するかもしれない。

3.1.8 サービスの誤使用

「保護された」ネットワークの外部に位置するデバイスは、保護されたネットワーク内部で提供される特定の*公開された*サービスへのアクセスを許可されている一方で、それらの許可された公開されたサービスとの通信中に不適切なアクティビティを試行するかもしれない。また保護されたネットワークの内部から提供される特定のサービスが、保護されたネットワーク外部からアクセスされた際にも、リスクを生じるかもしれない。ファイアウォールは、ネットワークインタフェースについての特定された規則を単に強制することに注意すべきである。保護されたまたは高信頼のネットワークという概念は、規則セットを構築する際に有用な抽象化である。

内向きの観点からは、外部ネットワーク上で動作するエンティティは、一般的に、所与の保護されたネットワークのポリシーの利用に束縛されないと想定される。それでもなお、ステートフルトラフィックフィルタファイアウォールは、公的に利用可能なサービスの公表された利用ステートメントへの違反を示す可能性のあるポリシー違反をログ出力することができる。

外向きの観点からは、ステートフルトラフィックフィルタファイアウォールは、保護されたネットワークの利用ポリシーの強制及び監視に役立つように設定することができる。他の脅威の項で説明したように、ステートフルトラフィックフィルタファイアウォールは、データの発信、外部サーバへのアクセス、及びサービスの中断さえも制限する役割を果たすことができる ― これらのすべては、保護されたネットワークの利用ポリシーと関連している可能性があり、それゆえ何らかの意味で強制の対象となる。さらに、ステートフルトラフィックフィルタファイアウォールは、保護されたネットワークと外部ネットワーク間にわたるネットワークの利用をログ出力するように設定することができ、その結果として、利用ポリシー違反の可能性を識別する役割を果たすことができる。

3.1.8.1 T.NETWORK_MISUSE

攻撃者は、サイトのセキュリティポリシーが意図しない方法で、マシンがエクスポートしているサービスの利用を試行するかもしれない。例えば、攻撃者は、他のマシンへの攻撃を仕掛ける時に、攻撃者のマシンを「匿名化」するためにサービスを利用できてしまうかもしれない。

3.1.9 悪意のあるトラフィック

ステートフルトラフィックフィルタファイアウォールは、悪意のある、または不正なパケットに対する保護についても提供する。例えば、接続状態情報の改変のような攻撃及びリプレイ攻撃に対する保護を提供することになる。これらの攻撃は、ファイアウォール、またはそれによって保護されるデバイスが、許可されないアクセスを許したり、あるいはサービス妨害 (DoS) さえ行ったりさせることができてしまうかもしれない。

3.1.9.1 T.MALICIOUS_TRAFFIC

攻撃者は、ターゲットマシンの UDP/TCP ポートを待ち受けているネットワークスタックまたはサービスをクラッシュさせようとして、マシンへ不正なパケットの送信を試みるかもしれない。

3.2 前提条件

本セクションでは、ファイアウォールの脅威及びセキュリティ要件の識別における前提条件について記述する。ファイアウォールは、これらの領域のいずれにおいても保証を提供することは期待されず、またその結果として、関連する脅威 (訳注：の顕在化) を低減するための要件は含まれない。

3.2.1 A.PHYSICAL_PROTECTION

ファイアウォールは、その運用環境において物理的に保護されており、セキュリティを危殆化したり、及び／またはファイアウォールの物理的な相互接続と正しい動作に干渉したりするような物理的攻撃の対象とはならないと想定される。この保護は、ファイアウォール及びそれに含まれるデータを保護するために十分であると想定される。結果として、本 cPP には、物理的な改ざん保護またはその他の物理的攻撃の低減に関する要件は一切含まれない。本 cPP は、許可されないエンティティがデータを抽出したり、その他の制御を迂回したり、あるいはその他の方法でファイアウォールの操作を許すような、ファイアウォールへの物理アクセスに対して製品が防御することを期待していない。

[OE.PHYSICAL]

3.2.2 A.LIMITED_FUNCTIONALITY

ファイアウォールは、そのコア機能としてネットワーク及びフィルタ機能を提供し、また汎用コンピューティングとみなされるような機能／サービスは提供しないと想定される。例えば、ファイアウォールは、 (ネットワーク／フィルタ機能とは無関係な) 汎用アプリケーション用のコンピューティングプラットフォームを提供するべきでない。

[OE.NO_GENERAL_PURPOSE]

3.2.3 A.TRUSTED_ADMINSTRATOR

ファイアウォールのセキュリティ管理者は、信頼され、かつ組織のセキュリティの利益を最優先に行動すると想定される。これには、適切に訓練され、ポリシーに従い、かつガイダンス文書を順守することが含まれる。管理者は、パスワード／クレデンシャルが十分な強度とエントロピーを持つことを保証し、ファイアウォールを管理する際に悪意を持たないと信頼されている。ファイアウォールには、ファイアウォールのセキュリティを迂回または危殆化させようと積極的に働きかけるような悪意のある管理者に対して防御できるとは期待されない。

[OE.TRUSTED_ADMIN]

3.2.4 A.REGULAR_UPDATES

ファイアウォールのファームウェア及びソフトウェアは、既知の脆弱性による製品アップデートのリリースに対応して定期的に管理者によってアップデートされると想定される。

[OE.UPDATES]

3.2.5 A.ADMIN_CREDENTIALS_SECURE

ファイアウォールへアクセスするために使用される管理者のクレデンシャル (プライベート鍵) は、それが動作するホストプラットフォームによって保護される。

[OE.ADMIN_CREDENTIALS_SECURE]

3.3 組織のセキュリティ方針

組織のセキュリティ方針は、組織がそのセキュリティニーズへ対処するために課している一連の規則、実践、及び手続きである。本 cPP の目的について、以下のセクションで、単一のポリシーが記述されている。

3.3.1 P.ACCESS_BANNER

TOE は、使用の制限、法的な合意、または TOE へアクセスすることによって利用者が同意することになるその他の任意の適切な情報について記述した、初期バナーを表示しなければならない。

[FTA_TAB.1]

4. セキュリティ対策方針

4.1 運用環境のセキュリティ対策方針

以下のサブセクションで、運用環境の対策方針を記述する。

4.1.1 OE.PHYSICAL

TOE 及びそれに含まれるデータの価値に見合った物理的セキュリティが環境によって提供される。

4.1.2 OE.NO_GENERAL_PURPOSE

TOE の動作、管理、及びサポートに必要なサービス以外の、TOE 上で利用可能な汎用コンピューティング機能 (例、コンパイラやユーザアプリケーション等) は存在しない。

4.1.3 OE.TRUSTED_ADMIN

TOE 管理者は、信頼された方法ですべてのガイダンス文書に従い適用すると信頼される。

4.1.4 OE.UPDATES

TOE のファームウェア及びソフトウェアは、既知の脆弱性による製品アップデートのリリースに対応して定期的に管理者によりアップデートされる。

4.1.5 OE.ADMIN_CREDENTIALS_SECURE

TOE へアクセスするために使用される管理者のクレデンシャル (プライベート鍵) は、それが動作するその他の任意のプラットフォーム上で保護されなければならない。

5. セキュリティ機能要件

個別のセキュリティ機能要件は、以下のセクションに特定されている。本セクションの SFR は、あらゆる適合 TOE が満たさなければならない必須 SFR である。これらの SFR でなされた選択に応じて、附属書 B の選択ベース SFR の一部も含まれる必要がある。また追加のオプション SFR を、附属書 A に列挙されたものから採択してもよい。

[SD] に定義される評価アクティビティには、TOE が SFR に適合していることを決定するために評価者が実行するアクションが記述されている。従って、これらの評価アクティビティの内容は、TOE 開発者に要求される評価用提供物件に対する更なる洞察を提供することになる。

5.1 表記法

SFR の記述に用いられる表記法は以下のとおり：

- 割付：*イタリック体*のテキストで示す。
- PP 作成者によってなされた詳細化 : 必要に応じて、**太字テキスト**及び ~~取り消し線~~ で示す。
- 選択：下線付きテキスト で示す。
- 選択中の割付：*イタリック体の下線付きテキスト* で示す。
- 繰り返し：例えば (1), (2), (3) 等、繰り返し回数を括弧内に付記し、及び／または「/」で始まる文字列を追加して示す。

拡張 SFR は、SFR 名の後にラベル「EXT」を付けることによって識別される。

5.2 SFR アーキテクチャ

図 1、図 2、図 3、図 4、図 5 及び図 6 は、セクション 5.3～5.11、附属書 A 及び附属書 B のセキュリティ機能要件と、TOE が提供する基盤となる機能領域及び操作との間の結び付きを図示したものである。この図では、TOE の利用に関する SFR の文脈を提供しているが、その他のセクションでは [CC2] の抽象クラス及びファミリグループによってグループ分けして SFR を定義している。

一般的に、ST により要求される附属書 B からの SFR は、他の SFR で行われた選択により決定される。例えば： (それぞれ 5.10.1.1 及び 5.10.2.1 における) FTP_ITC.1 及び FTP_TRP.1 は、それぞれ SFR によって記述されるセキュアチャネルのタイプにおいて使用されるプロトコルの選択を含んでいる。ここでのプロトコルの選択が、セクション B.2.1 のプロトコル特有 SFR のどれが ST に要求されるかについても決定する。

附属書 A の SFR は、それらが TOE によって提供される場合に ST に含めることができるが、TOE が本 cPP への適合を主張するために必須ではない。

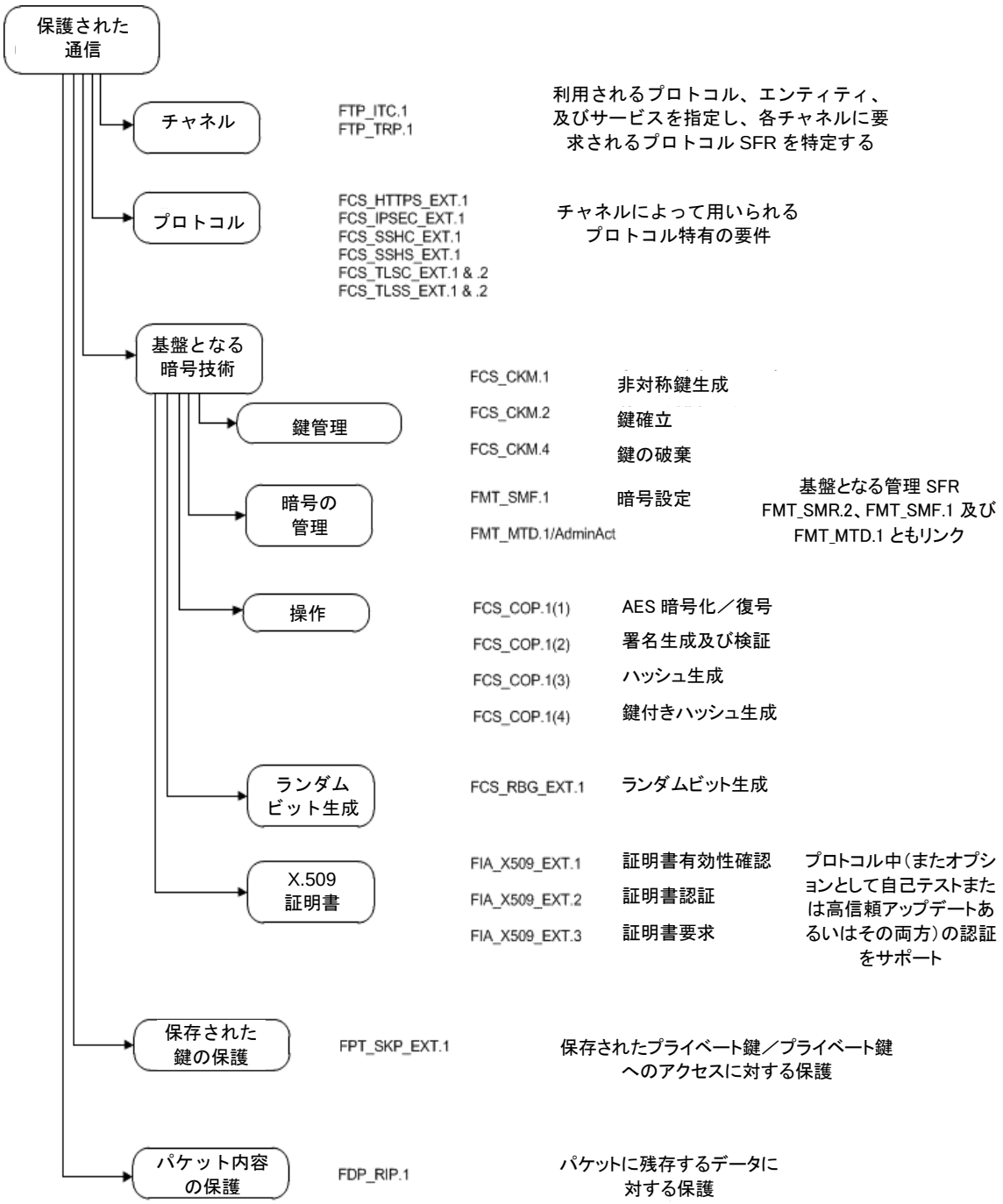


図 1：保護された通信の SFR アーキテクチャ

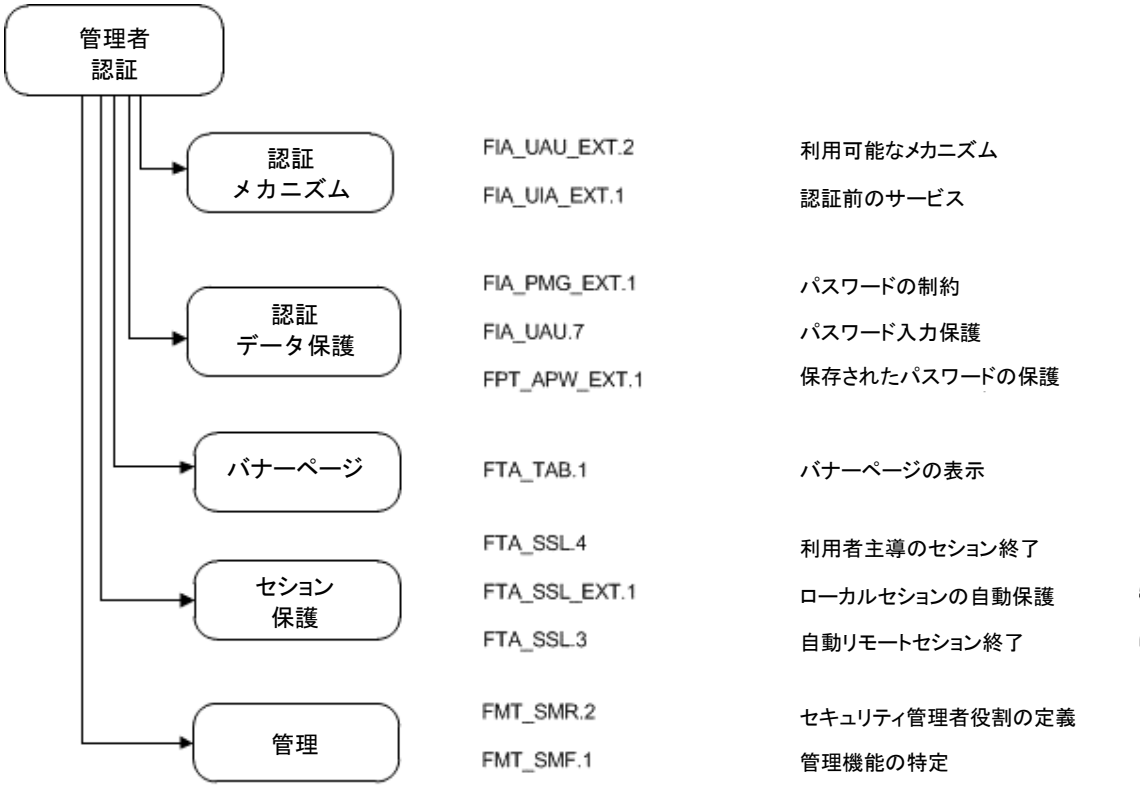


図 2：管理者認証の SFR アーキテクチャ

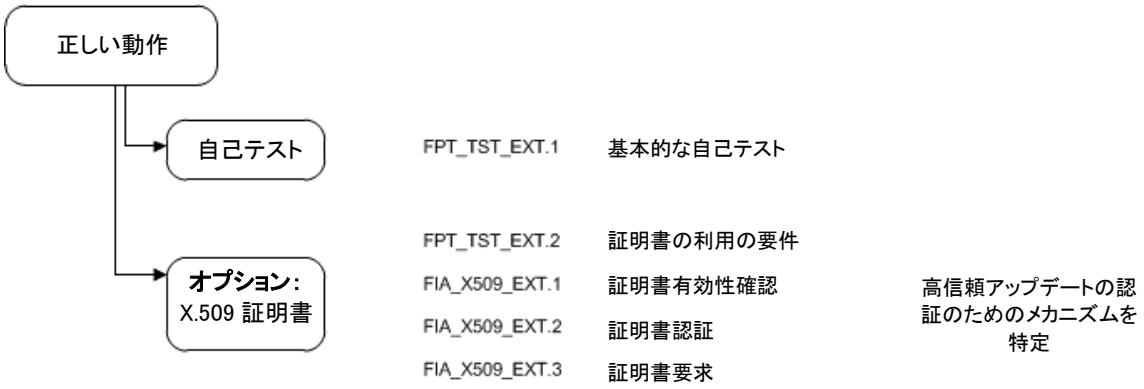


図 3：正しい動作の SFR アーキテクチャ

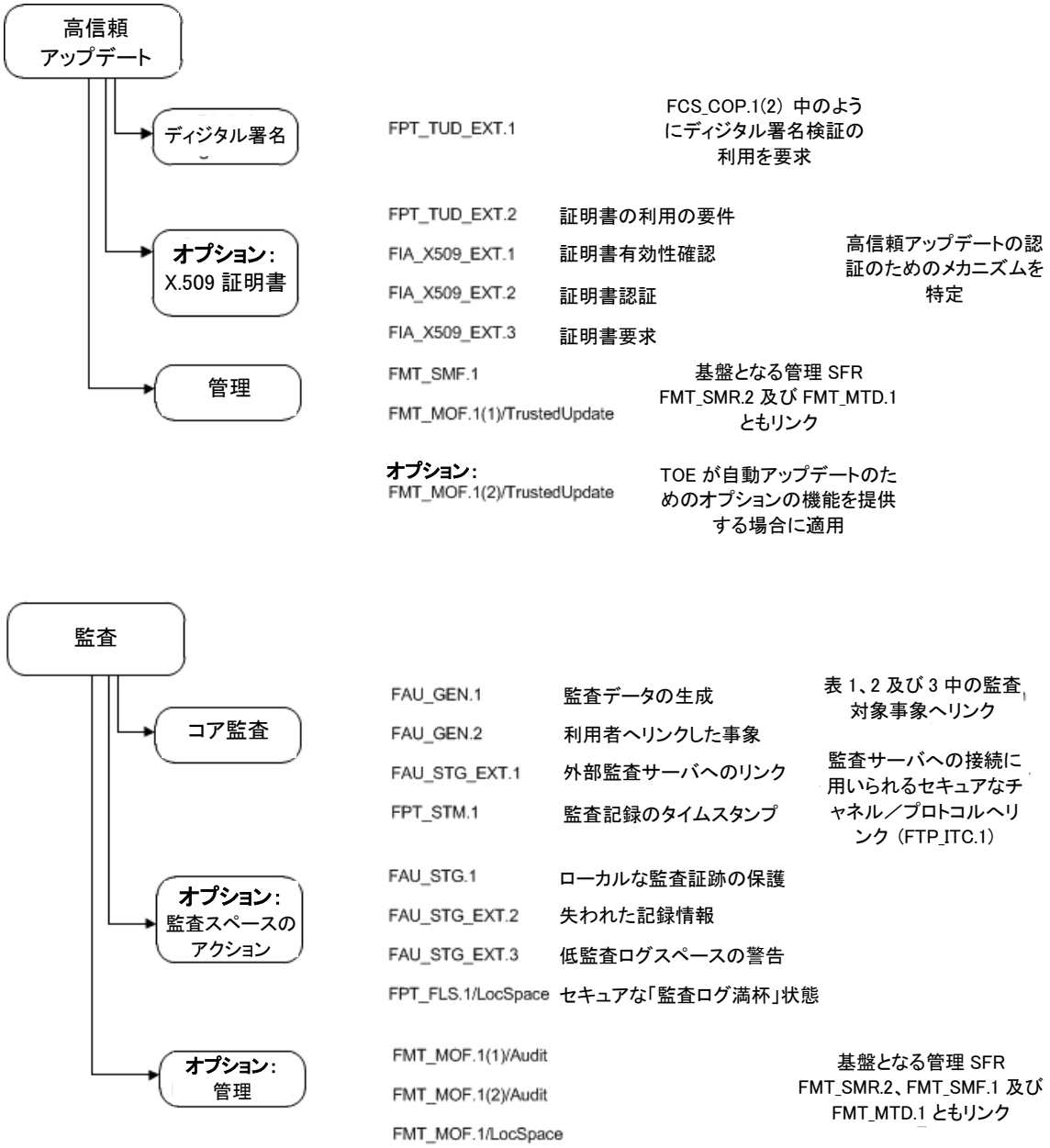


図 4：高信頼アップデートと監査の SFR アーキテクチャ

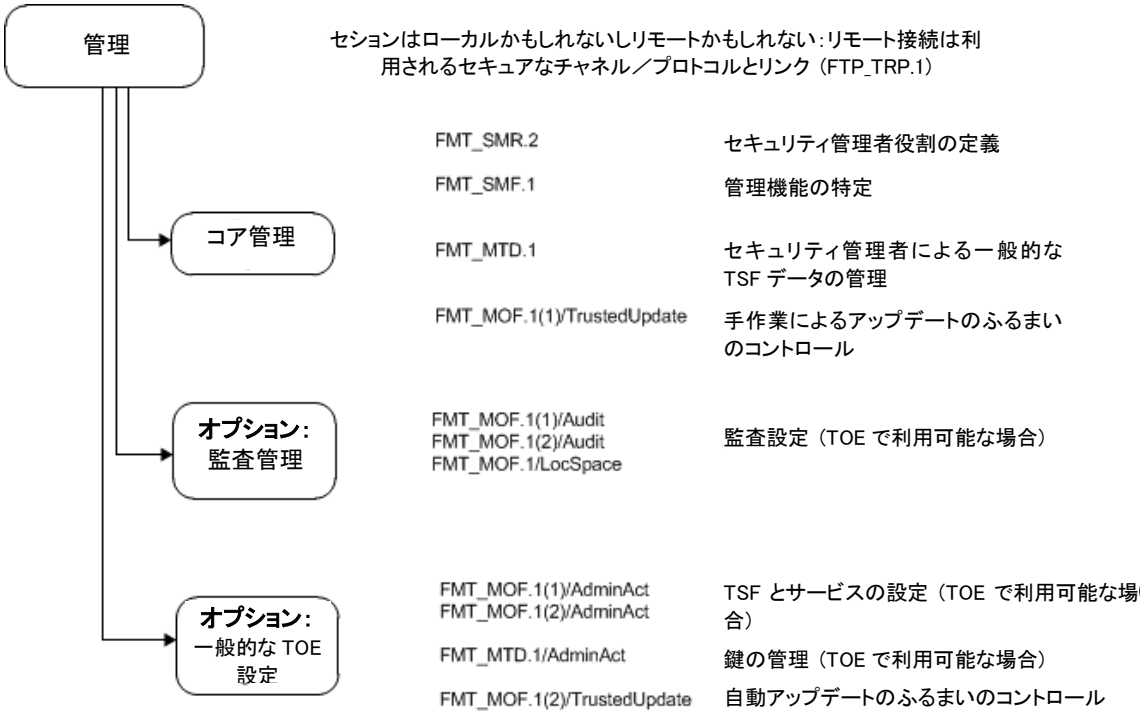


図 5：管理の SFR アーキテクチャ

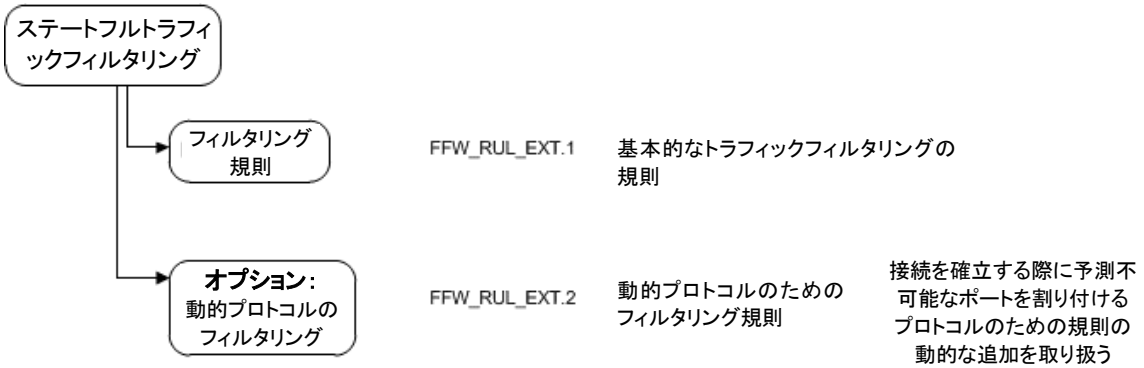


図 6：ファイアウォールの SFR アーキテクチャ

5.3 セキュリティ監査 (FAU)

5.3.1 セキュリティ監査データ生成 (FAU_GEN)

システムの設定及び／または動作に意図的や意図的でない問題をセキュリティ管理者が発見できるような情報の存在を保証するため、適合 TOE はそのようなアクティビティを検出する目的で監査データを生成する機能を持つ。管理アクティビティの監査によって、システムが正しく設定されていない場合に是正アクションを促進するために用いられ得る情報が提供される。選択されたシステム事象の監査によって、TOE の重要な部分の故障 (例えば暗号提供プロセスが動作していない) や疑わしい性質の異常なアクティビティ (例えば疑わしい時間での管理セションの確立、セション確立またはシステムへの認証のたび重な

る失敗) の徴候の提供が可能となる。

場合によっては、TOE や監査情報のレビューを担当する管理者を飽和させてしまうような大量の監査情報が作成されるかもしれない。TOE は、外部の高信頼エンティティへ監査情報を送信できなければならない。この情報には、信頼できるタイムスタンプが伴っていなければならない。これは、外部デバイスへ送信された際に情報の順序付けに役立つ。

監査サーバとの通信の途絶は、問題となる。この脅威を低減する方策はいくつか存在するが、本 cPP では特定のアクションが取られることを義務付けていない；このアクションによって、どの程度まで監査情報が保存されると共に TOE がその機能責任を果たし続けられるかによって、特定の環境における TOE の適合性に関する決定が行われるべきである。

5.3.1.1 FAU_GEN.1 監査データ生成

FAU_GEN.1	監査データ生成

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：

a) 監査機能の起動及び終了；

b) 監査のレベルが 特定されない すべての監査対象事象；及び

c) *以下から構成されるすべての管理アクション：*

- *管理者ログイン及びログアウト (管理者に個別利用者アカウントが必要とされる場合は利用者アカウントの名前がログ出力されなければならない)。*
- *セキュリティ関連の設定変更 (変更が起こったという情報に加えて、何が変更されたかがログ出力されなければならない)。*
- *暗号鍵の生成／インポート、変更、または削除 (アクションそのものに加えて、一意の鍵の名称または鍵の参照がログ出力されなければならない)。*
- *パスワードのリセット (関連する利用者アカウントの名称がログ出力されなければならない)。*
- *サービスの開始及び停止 (該当する場合)*
- *選択： [その他のアクションなし、割付： [その他の特権の使用のリスト]]；*

d) *表 1 に列挙される具体的に定義された監査対象事象。*

適用上の注釈 1

「管理者アクション」のリストが不完全と考えられる場合、監査される追加の管理者アクションを列挙するため、選択における割付が使用されるべきである。

ST 作成者は、監査事象の表への相互参照を、ST への適切な相互参照で置き換える。またこれには、ST に含まれるオプション SFR 及び選択ベース SFR に対応する表 3 及び表 4 の関連する部分が含まれなければならない。

適用上の注釈 2

ST 作成者は、他の監査対象事象を直接表中に含めることができる。監査対象事象は、提示されたリストには限定されない。

TSS には、暗号鍵の生成／インポート、変更、または削除の管理タスクに対応する鍵を識別するため、どの情報がログ出力されるかを識別するべきである。

FAU_GEN.1.1 に関して、「サービス」という用語は、高信頼パス及び高信頼チャネル通信、オンデマンドの自己テスト、高信頼アップデート及び管理者セション (高信頼パスの下に存在するもの) (例えば netconf) を指している。

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：

a) 事象の日付・時刻、事象種別、サブジェクトの識別情報、事象の結果 (成功または失敗)；及び

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 の *3 列目に指定される情報。*

FFW_RUL_EXT.1	「ログ出力」操作を設定されたルールの適用	送信元及び宛先アドレス 送信元及び宛先ポート トランスポート層プロトコル TOE インタフェース
	過多なネットワークトラフィックのため破棄されたパケットの提示	パケットを処理不能であった TOE インタフェース パケット破棄を引き起こしたルールの識別子

表 1

適用上の注釈 3

ST 作成者は、監査事象の表への相互参照を、ST への適切な相互参照で置き換える。またこれには、ST に含まれるオプション SFR 及び選択ベース SFR に対応する表 3 及び表 4 の関連する部分についても含まれなければならない。

要件	監査対象事象	追加監査記録の内容
FAU_GEN.1	なし。	なし。
FAU_GEN.2	なし。	なし。
FAU_STG_EXT.1	なし。	なし。
FCS_CKM.1	なし。	なし。
FCS_CKM.2	なし。	なし。
FCS_CKM.4	なし。	なし。

FCS_COP.1(1)	なし。	なし。
FCS_COP.1(2)	なし。	なし。
FCS_COP.1(3)	なし。	なし。
FCS_COP.1(4)	なし。	なし。
FCS_RBG_EXT.1	なし。	なし。
FDP_RIP.2	なし。	なし。
FIA_PMG_EXT.1	なし。	なし。
FIA_UIA_EXT.1	識別と認証のメカニズムの利用すべて。	提供された利用者の識別情報、試行の生成元 (例えば、IP アドレス)。
FIA_UAU_EXT.2	識別と認証のメカニズムの利用すべて。	試行の生成元 (例えば、IP アドレス)。
FIA_UAU.7	なし。	なし。
FIA_X509_EXT.1	証明書有効性確認の不成功の試行	失敗の理由。
FIA_X509_EXT.2	なし。	なし。
FIA_X509_EXT.3	なし。	なし。
FMT_MOF.1(1)/TrustedUpdate	手動アップデートを開始する任意の試行	なし。
FMT_MTD.1	TSFデータの管理アクティビティすべて。	なし。
FMT_SMF.1	なし。	なし。
FMT_SMR.2	なし。	なし。
FPT_SKP_EXT.1	なし。	なし。
FPT_APW_EXT.1	なし。	なし。
FPT_TST_EXT.1	なし。	なし。
FPT_TUD_EXT.1	アップデートの開始 ; アップデート試行の結果 (成功または失敗)。	追加的情報なし。
FPT_STM.1	時刻の変更。	時刻の変更前と変更後の値。成功及び失敗した時刻を変更する試行の生成元 (例えば、IP アドレス)。
FTA_SSL_EXT.1	対話セションのロック解除を意図した任意の試行。	なし。
FTA_SSL.3	セションロックメカニズムによるリモートセショ	なし。

	ンの終了。	
FTA_SSL.4	対話セションの終了。	なし。
FTA_TAB.1	なし。	なし。
FTP_ITC.1	高信頼チャネルの初期化。高信頼チャネルの終了。高信頼チャネル機能の失敗。	失敗した高信頼チャネル確立試行のイニシエータ及びターゲットの識別情報。
FTP_TRP.1	高信頼パスの初期化。高信頼パスの終了。高信頼パス機能の失敗。	要求された利用者識別情報の識別。
FFW_RUL_EXT.1	「ロギング」操作を設定されたルールの適用	送信元及び送信先アドレス 送信元及び送信先ポート トランスポート層プロトコル TOE インタフェース
	過大なネットワークトラフィックのため破棄されたパケットの示唆	パケットを処理できなかった TOE インタフェース パケットの破棄を引き起こしたルールの識別子

表 1：セキュリティ機能要件及び監査対象事象

適用上の注釈 4

追加の監査事象が、附属書 A 及び附属書 B から採択されたオプション及び選択ベースの要件により、TOE へ適用されること。従って ST 作成者は、表 3 及び表 4 に指定された対応する追加の事象を含めなければならない。

FIA_X509_EXT.1 の監査事象は、以下を保証することにより、TOE が証明書有効性確認を完了することができない場合に対応する。

- *basicConstraints 拡張が存在し、すべての CA 証明書について、cA フラグが TRUE にセットされていること。*
- *信頼済み階層上の CA のディジタル署名の検証*
- *CRL の読み出し／アクセスまたは OCSP サーバへのアクセス。*

これらのチェックのいずれかが失敗した場合には、その失敗に伴う監査事象が監査ログへ書き込まれるべきである。

5.3.1.2 FAU_GEN.2 利用者識別情報の関連付け

FAU_GEN.2	**利用者識別情報の関連付け**

FAU_GEN.2.1 識別された利用者のアクションがもたらす監査事象に対し、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。

5.3.2 セキュリティ監査事象格納 (拡張—FAU_STG_EXT)

ネットワークデバイス TOE には、すべての監査証跡格納そのものの責任を負うことは期待されていない。生成時にデータをローカルに保存すること、及びこのローカルな格納容量が超過した場合に何らかの適切なアクションを取ることは要求されているが、TOE は外部監査証跡ストレージを有効化するため、外部監査サーバへのセキュアなリンクを確立することも要求されている。

5.3.2.1 FAU_ STG_EXT.1 保護された監査事象格納

FAU_STG_EXT.1	保護された監査事象格納

FAU_STG_EXT.1.1 TSF は、生成された監査データを外部 IT エンティティへ FTP_ITC.1 に従った高信頼チャネルを用いて送信できなければならない。

適用上の注釈 5

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オプションの選択について、TOE は監査記録の格納とレビューに関して非 TOE 監査サーバに依存している。これらの監査記録の格納、及びこれらの監査記録のレビューを管理者に許可する能力は、その場合の運用環境により提供される。

FAU_STG_EXT.1.2 TSF は、生成された監査データを TOE それ自体に格納できなければならない。

FAU_STG_EXT.1.3 TSF は、監査データのローカルな格納用領域が満杯の場合、 [選択：*新たな監査データを破棄、以下の規則に従って以前の監査記録を上書き：[割付：以前の監査記録を上書きする規則]*、 *[割付：その他のアクション]*] しなければならない。

適用上の注釈 6

ローカルな格納用領域が満杯の場合、外部ログサーバが代替の格納用領域として使用されるかもしれない。この場合、「その他のアクション」は「外部 IT エンティティへ新たな監査データを送信する」と定義できるであろう。

5.4 暗号サポート (FCS)

5.4.1 暗号鍵管理 (FCS_CKM)

本セクションでは、TOE のその他のセキュリティ特性の基盤となる暗号要件を定義し、鍵生成及びランダムビット生成、鍵確立方法、鍵の破壊、ならびに AES 暗号化／復号、署名検証、ハッシュ生成、及び鍵付きハッシュ生成を提供するさまざまな種類の暗号操作をカバーする。

これらの SFR は、附属書 B のプロトコルレベルの選択ベース SFR の実装をサポートする。

5.4.1.1 FCS_CKM.1 暗号鍵生成 (詳細化)

FCS_CKM.1	暗号鍵生成

FCS_CKM.1.1 TSF は、~~以下の[割付：*標準のリスト*]に合致する、~~指定された暗号鍵生成アルゴリズム： [選択：

- ***2048 ビット以上の暗号鍵長を用い、以下を満たす RSA スキーム：FIPS PUB 186-4, "Digital Signature Standard (DSS)", 附属書 B.3；***

- ***「NIST 曲線」 [選択：P-256、P-384、P-521] を用い、以下を満たす ECC スキーム： FIPS PUB 186-4, "Digital Signature Standard (DSS)", 附属書 B.4；***
- ***2048 ビット以上の暗号鍵長を用い、以下を満たすFFC スキーム：FIPS PUB 186-4, "Digital Signature Standard (DSS)", 附属書 B.1***

] ~~及び指定された暗号鍵長 [割付：*暗号鍵長*]~~に従って、**非対称**暗号鍵を生成しなければならない。

適用上の注釈 7

ST 作成者は、鍵確立及びデバイス認証のために使用されるすべての鍵生成スキームを選択すること。鍵生成が鍵確立用に使用される場合、FCS_CKM.2.1 におけるスキーム及び選択された暗号プロトコルがその選択と一致しなければならない。鍵生成がデバイス認証用に使用される場合、公開鍵は X.509v3 証明書と関連付けられることが期待されている。

TOE が RSA 鍵確立スキームにおける受信側として動作する場合、TOE が RSA 鍵生成を実装する必要はない。

5.4.1.2 FCS_CKM.2 暗号鍵確立 (詳細化)

FCS_CKM.2	**暗号鍵 <u>確立</u>**

FCS_CKM.2.1 TSF は、~~以下の[割付：*標準のリスト*]に合致する、~~指定された**鍵確立**方法：<u>[選択：</u>

- ***RSA ベースの鍵確立スキームであって、以下を満たすもの： NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"；***
- ***楕円曲線ベースの鍵確立スキームであって、以下を満たすもの：NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"；***
- ***有限体ベースの鍵確立スキームであって、以下を満たすもの：NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";***

]に従って暗号**鍵確立**を**行わ**なければならない。

適用上の注釈 8

これは、鍵配付ではなく鍵確立を取り扱うための SFR、FCS_CKM.2 としての詳細化である。

ST 作成者は、選択された暗号プロトコル用に使用されるすべての鍵確立スキームを選択すること。

RSA ベースの鍵確立スキームは、NIST SP 800-56B のセクション 9 に記述されている；しかし、セクション 9 は SP 800-56B の他のセクションの実装に依存している。TOE が RSA 鍵確立スキームにおける受信側として動作する場合、TOE が RSA 鍵生成を実装する必要はない。

鍵確立スキーム用に使用される楕円曲線は、FCS_CKM.1.1 に指定された曲線と相関する。

有限体ベースの鍵確立スキーム用に使用されるドメインパラメタは、FCS_CKM.1.1 に従って鍵生成により指定されること。

5.4.1.3 FCS_CKM.4 暗号鍵破棄

FCS_CKM.4	暗号鍵破棄

FCS_CKM.4.1 TSF は、以下の：*標準なし*に合致する、指定された暗号鍵破棄方法*[選択：*

- *揮発性メモリについては、 [選択：TSF の RBG を用いた疑似ランダムパタンからなる、ゼロからなる] 一回の直接上書きと、それに続く読み出し検証により、破棄が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した場合、処理が再度繰り返されなければならない。*
- *不揮発性 EEPROM については、(FCS_RBG_EXT.1 で指定されるとおり) TSF の RBG を用いた疑似ランダムパタンからなる一回の直接上書きと、それに続く読み出し検証により破棄が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した場合、処理が再度繰り返されなければならない。*
- *不揮発性フラッシュメモリについては、 [選択：ゼロからなる一回の直接上書き、ブロック消去] とそれに続く読み出し検証により破棄が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した場合、処理が再度繰り返されなければならない。*
- *EEPROM とフラッシュメモリ以外の不揮発性メモリについては、毎回書き込み前に変更されたランダムパタンで 3 回以上上書きすることにより破棄が実行されなければならない。*

]

に従って、暗号鍵を破棄しなければならない。

5.4.2 暗号操作 (FCS_COP)

5.4.2.1 FCS_COP.1 暗号操作

FCS_COP.1(1)	暗号操作 (AES データ暗号化／復号)

FCS_COP.1.1(1) TSF は、以下の標準に合致する、*[選択：CBC、GCM]* モードで使用される、特定された暗号アルゴリズム *AES* と暗号鍵長 *[選択：128 ビット、192 ビット、256 ビット]* に従って、*暗号化／復号*を実行しなければならない： *ISO 18033-3 で特定される AES、 [選択：ISO 10116 で特定される CBC、ISO 19772 で特定される GCM]*。

適用上の注釈 9

FCS_COP.1.1(1) の最初の選択については、ST 作成者は AES が動作する 1 つまたは複数のモードを選択すべきである。第 2 の選択については、ST 作成者はこの機能によってサポートされる鍵長を選択すべきである。ここで選択されたモード及び鍵長は、高信頼チャネル要件においてなされる暗号スイートの選択に対応すること。

FCS_COP.1(2)	暗号操作 (署名生成及び検証)

FCS_COP.1.1(2) TSF は、以下の標準に合致する、特定された暗号アルゴリズム [選択：

- *RSA ディジタル署名アルゴリズム及び [割付：2048 ビット以上] の暗号鍵長 (**モジュラス**)*、
- *楕円曲線ディジタル署名アルゴリズム及び [割付：256 ビット以上] の暗号鍵長*

]

に従って、*暗号署名サービス (生成及び検証)* を実行しなければならない [選択：

- *RSA スキームについて：PKCS #1 v2.1 Signature Schemes RSASSA-PSS または RSASSA-PKCS2v1_5 あるいはその両方を用いる FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5 ;ISO/IEC 9796-2, Digital signature scheme 2 または Digital Signature scheme 3*、
- *ECDSA スキームについて：「NIST 曲線」P-256、P-384、及び [選択：P-521、その他の曲線なし] を実装する FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 及び附属書 D ; ISO/IEC 14888-3, Section 6.4*

]。

適用上の注釈 10

ST 作成者は、ディジタル署名を行うために実装されたアルゴリズムを選択すべきである。選択された 1 つまたは複数のアルゴリズムについて、ST 作成者は適切な割付／選択を行ってそのアルゴリズムに実装されるパラメタを特定すべきである。

FCS_COP.1(3)	暗号操作 (ハッシュアルゴリズム)

FCS_COP.1.1(3) TSF は、以下の標準に合致する、特定された暗号アルゴリズム [*選択:SHA-1*、*SHA 256*、*SHA 384*、*SHA 512*、*その他のアルゴリズムなし*] ~~と暗号鍵長 [割付：*暗号鍵長*]~~ に従って、*暗号ハッシュサービス*を実行しなければならない： *ISO/IEC 10118-3:2004*。

適用上の注釈 11

ベンダには、SHA-2 ファミリをサポートする改訂されたプロトコルの実装が強く推奨される。改訂されたプロトコルがサポートされるまでは、本 PP は SP 800-131A に適合した SHA-1 の実装を許す。

ハッシュの選択は、FCS_COP.1(1) 及び FCS_COP.1(2) に用いられるアルゴリズムの全体的な強度と一貫すべきである (例えば、128 ビットの鍵については SHA 256)。

FCS_COP.1(4)	暗号操作 (鍵付きハッシュアルゴリズム)

FCS_COP.1.1(4) TSF は、以下の標準に合致する、特定された暗号アルゴリズム *[選択：HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512]* と暗号鍵長 [割付：*HMAC に用いられる (ビット単位の) 鍵長*] **ならびにメッセージダイジェスト長 *[選択：160、256、384、512] ビット***に従って、*鍵付きハッシュによるメッセージ認証*を実行しなければならない：*ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*。

適用上の注釈 12

割付における鍵長 [k] は、L1 と L2 の間の範囲内にあること (適切なハッシュ関数について

ISO/IEC 10118 に定義されている)。例えば、SHA-256 について、L1=512、L2=256、ここで L2<=k<=L1 とする。

5.4.3 ランダムビット生成 (拡張—FCS_RBG_EXT)

5.4.3.1 FCS_RBG_EXT.1 ランダムビット生成

FCS_RBG_EXT.1	ランダムビット生成

FCS_RBG_EXT.1.1 TSF は、ISO/IEC 18031:2011 に従って、[選択：*Hash_DRBG (任意)* 、*HMAC_DRBG (任意)* 、*CTR_DRBG (AES)*] を用いて、すべての決定論的ランダムビット生成サービスを実行しなければならない。

FCS_RBG_EXT.1.2 決定論的 RBG は、[選択： *[割付：ソフトウェアベースのノイズ源の数] 個のソフトウェアベースのノイズ源、 [割付：ハードウェアベースのノイズ源の数] 個のハードウェアベースのノイズ源*] からエントロピーを、ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”に従って、生成される鍵とハッシュの最大セキュリティ強度と少なくとも等しいだけの、 [選択：*128 ビット、192 ビット、256 ビット*] の最小エントロピーを有するように蓄積する、少なくとも 1 つのエントロピー源によってシードが供給されなければならない。

適用上の注釈 13

FCS_RBG_EXT.1.2 の最初の選択については、ST は少なくとも 1 つのノイズ源の種別を選択する。TOE に同一種別のノイズ源が複数含まれる場合、ST 作成者はノイズ源のそれぞれの種別について割付に適切な数字を当てはめる (例えば、2 個のソフトウェアベースのノイズ源、1 個のハードウェアベースのノイズ源)。本エレメントについて評価アクティビティに要求される文書化及びテストは、必然的に ST で示された各ノイズ源を網羅すること。

ISO/IEC 18031:2011 には、3 つの異なる乱数生成方法が含まれている。これらはそれぞれ、基盤となる暗号プリミティブ (ハッシュ関数／暗号) に依存している。 ST 作成者は利用される関数を選択し、要件に用いられる具体的な基盤となる暗号プリミティブを含めること。特定されたハッシュ関数 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) はいずれも Hash_DRBG または HMAC_DRBG 用として許可されるが、CTR_DRBG には AES ベースの実装のみが許可される。

ここで用いられる AES 実装の鍵長が利用者データの暗号化に用いられるものと異なる場合には、FCS_COP.1 を調整するか、または異なる鍵長を反映して繰り返す必要があるかもしれない。FCS_RBG_EXT.1.2 の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する。

5.5 利用者データ保護 (FDP)

本セクションは、TOE が新たなパケットの送信時に古いパケットの情報を再利用しないことを保証することを要求する。

5.5.1 残存情報保護 (FDP_RIP)

5.5.1.1 FDP_RIP.2 全残存情報保護

FDP_RIP.2	全残存情報保護

FDP_RIP.2.1 TSF は、すべてのオブジェクト [選択：*への資源の割り当て、からの資源の割り当て解除*] において、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。

適用上の注釈 14

本要件における「資源」とは、TOE を通過して (セキュリティ管理者が TOE へ接続する時のような「へ」の対語として) 送信されるネットワークパケットである。懸念されるのは、一度ネットワークパケットが送信された後も、そのパケットによって使用されたバッファまたはメモリ領域にそのパケットからのデータがまだ含まれており、そしてそのバッファが再利用された場合、それらのデータが残ったまま新たなパケットに入り込むことである。

5.6 識別と認証 (FIA)

管理者が TOE と対話する信頼できる手段を提供するため、TOE はパスワードベースのログオンメカニズムを提供する。管理者は強いパスワードを構成する能力を有し、またパスワードが定期的に変更されなければならないようなメカニズムを用意しなければならない。管理者によって入力されるパスワードを攻撃者が観察できるかもしれない場合の攻撃を避けるため、パスワードはログオン中に見えなくされなければならない。セションロックまたはセション終了もまた、アカウントが不正に使用されるリスクを低減するために実装されなければならない。パスワードは見えない形で保存されなければならず、またパスワードが平文で表示されるような形でパスワードまたはパスワードファイルを特に読み出すためのインタフェースが提供されてはならない。

5.6.1 パスワード管理 (拡張—FIA_PMG_EXT)

5.6.1.1 FIA_PMG_EXT.1 パスワード管理

FIA_PMG_EXT.1	パスワード管理

FIA_PMG_EXT.1.1 TSF は、管理者パスワードとして、以下のパスワード管理機能を提供しなければならない：

a) パスワードは、アルファベットの大文字及び小文字、数字、ならびに以下の特殊文字：[選択：“!”、“@”、“#”、“$”、“%”、“^”、“&”、“”、“(“、“)”、[割付：その他の文字]] の任意の組み合わせによって構成できなければならない；*

b) 最小のパスワード長は、セキュリティ管理者によって設定可能でなければならず、かつ 15 文字以上のパスワードがサポートされなければならない。

適用上の注釈 15

ST 作成者は、TOE によってサポートされる特殊文字を選択する。これらには、割付を用いてサポートされる追加の特殊文字が、オプションとして列挙されてもよい。「管理者パスワード」は、ローカルコンソールで、SSH 及び HTTPS 等、パスワードをサポートするプロトコル上で、またはセキュリティターゲットで他の SFR をサポートする設定データを許可するため、管理者によって用いられるパスワードを意味する。

5.6.2 利用者の識別と認証 (拡張—FIA_UIA_EXT)

5.6.2.1 FIA_UIA_EXT.1 利用者の識別と認証

FIA_UIA_EXT.1	利用者の識別と認証

FIA_UIA_EXT.1.1 TSF は、非 TOE エンティティが識別と認証のプロセスを開始する前に、

以下のアクションを許可しなければならない：

- FTA_TAB.1 に従って警告バナーを表示すること；
- [選択：*その他のアクションなし、 [割付：サービスのリスト、非 TOE の要求に応じて TSF によって行われるアクション。]*]

FIA_UIA_EXT.1.2 TSF は、その管理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、各管理利用者の識別と認証の成功を要求しなければならない。

適用上の注釈 16

本要件は、TOE を介した接続によって提供されるサービスではなく、直接 TOE から提供されるサービスの利用者 (管理者及び外部 IT エンティティ) に適用される。識別と認証に先立って外部エンティティにサービスはほとんど提供されないようにすべきであるが、何らかのサービス (おそらく ICMP echo) が提供される場合、それらが割付ステートメントに列挙されるべきである；それ以外の場合には、「その他のアクションなし」が選択されるべきである。

認証は、ローカルコンソールを介する場合、またはパスワードをサポートするプロトコル (SSH 等) を介する場合は、パスワードベースであってもよいし、証明書ベースであってもよい (SSH、TLS 等)。

外部 IT エンティティ (例、監査サーバまたは NTP サーバ) との通信については、そのような接続は FTP_ITC.1 に従って行われなければならず、そのプロトコルが識別と認証を行う。これは、そのような通信 (例、認証サーバへの IPsec 接続の確立) が割付にて特定される必要はないであろうことを意味する。接続の確立は、識別と認証のプロセスの起動として「カウント」されるためである。

5.6.3 利用者認証 (FIA_UAU) (拡張—FIA_UAU_EXT)

5.6.3.1 FIA_UAU_EXT.2 パスワードに基づく認証メカニズム

FIA_UAU_EXT.2	パスワードに基づく認証メカニズム

FIA_UAU_EXT.2.1 TSF は、ローカルなパスワードに基づく認証メカニズム、 [選択： *[割付：1 つまたは複数のその他の認証メカニズム]*、*なし*] を提供して管理利用者の認証を行わなければならない。

適用上の注釈 17

割付は、追加のローカル認証メカニズムがサポートされていれば、それを特定するために用いられるべきである。ローカル認証メカニズムは、ローカルコンソールを介して行われるものと定義される。リモート管理者セション (及びそれに関連付けられた認証メカニズム) は、FTP_TRP.1 に特定される。

5.6.3.2 FIA_UAU.7 保護された認証フィードバック

FIA_UAU.7	保護された認証フィードバック

FIA_UAU.7.1 TSF は、ローカルコンソール上で認証を行っている間、*見えなくされたフィードバック*だけを管理利用者に提供しなければならない。

適用上の注釈 18

「見えなくされたフィードバック」とは、利用者によって入力された任意の認証データの

目に見える表示 (パスワードのエコーバック等) を行わないことを意味するが、進捗のあいまい化された表示 (各文字の代わりにアスタリスク等) は提供されてもよい。また、認証データについて何らかの示唆を与えるかもしれない任意の情報を、TSF が認証プロセス中に利用者へ返さないことも意味する。

5.6.4 X.509 証明書を用いた認証 (拡張—FIA_X509_EXT)

5.6.4.1 FIA_X509_EXT.1 X.509 証明書有効性確認

FIA_X509_EXT.1	X.509 証明書有効性確認

FIA_X509_EXT.1.1 TSF は、以下の規則に従って、証明書の有効性を確認しなければならない：

- RFC 5280 証明書有効性確認及び証明書パス検証。
- 証明書パスは、信頼済み CA 証明書で終端しなければならない。
- TSF は、すべての CA 証明書について、basicConstraints 拡張の存在と CA フラグが TRUE にセットされていることを保証することによって、証明書パスを検証しなければならない。
- TSF は、[選択：*RFC 2560 に特定されるオンライン証明書状態プロトコル (OCSP)*、*RFC 5759 に特定される証明書失効リスト (CRL)*] を用いて証明書の失効状態を検証しなければならない。
- TSF は、以下の規則に従って extendedKeyUsage フィールドを検証しなければならない：
    - *高信頼アップデート及び実行可能コードの完全性検証用の証明書は、extendedKeyUsage フィールドにコード署名目的 (OID 1.3.6.1.5.5.7.3.3 を持つ id-kp 3) を持たなければならない。*
    - *TLS 用のサーバ証明書は、extendedKeyUsage フィールドにサーバ認証目的 (OID 1.3.6.1.5.5.7.3.1 を持つ id-kp 1) を持たなければならない。*
    - *TLS に提示されるクライアント証明書は、extendedKeyUsage フィールドにクライアント認証目的 (OID 1.3.6.1.5.5.7.3.2 を持つ id-kp 2) を持たなければならない。*
    - *OCSP 応答に提示される OCSP 証明書は、extendedKeyUsage フィールドに OCSP 署名目的 (OID 1.3.6.1.5.5.7.3.9 を持つ id-kp 9) を持たなければならない。*

適用上の注釈 19

FIA_X509_EXT.1.1 には、証明書の有効性確認を行うための規則が列挙されている。ST 作成者は、失効状態が OCSP か CRL のどちらを用いて検証されるか選択する。高信頼チャネル／パスのプロトコルは、証明書の利用が必須である；この用途は、extendedKeyUsage 規則が検証されることが必須である。

証明書の有効性確認は、プラットフォームによって管理されているルート格納にある信頼済みルート CA 証明書で終端することが期待される。

FIA_X509_EXT.1.2 TSF は、basicConstraints 拡張が存在し CA フラグが TRUE にセットされている場合にのみ、証明書を CA 証明書として取り扱わなければならない。

適用上の注釈 20

本要件は、TSF によって用いられ、処理される証明書に適用され、信頼済み CA 証明書として追加され得る証明書に限定する。

5.6.4.2 FIA_X509_EXT.2 X.509 証明書認証

FIA_X509_EXT.2	X.509 証明書認証

FIA_X509_EXT.2.1 TSF は、RFC 5280 によって定義される X.509v3 証明書を用いて、[選択：*IPsec*、*TLS*、*HTTPS*、*SSH*]、及び [選択：*システムソフトウェアアップデート用のコード署名*、*完全性検証用のコード署名*、*[割付：その他の用途]*、*追加の用途なし*] の認証をサポートしなければならない。

適用上の注釈 21

ST 作成者の選択は、FTP_ITC.1.1 の選択と一致すること。証明書は、システムソフトウェアの高信頼アップデート (FPT_TUD_EXT.1) 及び完全性検証 (FPT_TST_EXT.2) 用にオプションとして用いられてもよい。

FIA_X509_EXT.2.2 TSF が証明書の有効性を決定するためのコネクションを確立できない時、TSF は [選択：*このような場合には証明書を受容するかどうかの選択を管理者に許可する*、*証明書を受容する*、*証明書を受容しない*] ようにしなければならない。

適用上の注釈 22

CRL のダウンロードにせよ、OCSP の実行にせよ、証明書の失効状態をチェックするためにコネクションを確立しなくてはならない場合が多々生ずる。この選択は、(例えば、ネットワークエラーのため) そのようなコネクションが確立できない場合のふるまいを記述するために用いられる。TOE が、証明書は FIA_X509_EXT.1 における他の全ての規則に従って有効であると決定した場合、選択に示されるふるまいによって有効性が決定される。証明書が FIA_X509_EXT.1 における他の有効性確認規則のいずれかに失敗する場合、TOE はその証明書を受容してはならない。ST 作成者によって管理者設定オプションが選択された場合、ST 作成者はまた FMT_SMF.1 における対応する機能をも選択すること。

5.6.4.3 FIA_X509_EXT.3 X.509 証明書要求

FIA_X509_EXT.3.1 TSF は、RFC 2986 に指定されるように証明書要求メッセージを生成するとともに、その要求に以下の情報を提供できなければならない：公開鍵、及び [選択：*デバイス固有情報*、*コモン名 (Common Name)*、*組織 (Organization)*、*組織単位 (Organizational Unit)*、*国 (Country)*]。

適用上の注釈 23

公開鍵は、FCS_CKM.1(1) に特定されるように TOE が生成する公開鍵―プライベート鍵ペアの、公開鍵の部分である。

FIA_X509_EXT.3.2 TSF は、CA 証明書応答の受信に際して、ルート CA からの証明書のチェインの有効性を確認しなければならない。

5.7 セキュリティ管理 (FMT)

本セクションで要求される管理機能は、セキュリティ管理者役割をサポートするために要求される機能、ならびに他の SFR (FMT_SMF.1) に含まれる設定可能な側面、TSF データの一般的な管理 (FMT_MTD.1)、及び TOE アップデートの有効化 (FMT_MOF.1(1)/Trusted Update) の管理を取り扱う一連の基本的なセキュリティ管理機能について記述する。

これらの主要な管理要件は、TOE 機能に従って、セクション A.3 のオプション要件及びセクション B.4 の選択ベース要件において補足されている。

5.7.1 TSF における機能の管理 (FMT_MOF)

5.7.1.1 FMT_MOF.1(1)/TrustedUpdate セキュリティ機能のふるまいの管理

FMT_MOF.1(1)/TrustedUpdate	**セキュリティ機能のふるまいの管理**

FMT_MOF.1.1(1)/TrustedUpdate TSF は、*手動アップデートを行う*機能を 有効化 する能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 24

FMT_MOF.1(1)/TrustedUpdate は、手動アップデートの開始をセキュリティ管理者に制限する。

5.7.2 TSF データの管理 (FMT_MTD)

5.7.2.1 FMT_MTD.1 TSF データの管理

FMT_MTD.1	**TSF データの管理**

FMT_MTD.1.1 TSF は、*TSF データを 管理する* 能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 25

「管理」という言葉には、作成、初期化、閲覧、デフォルト変更、改変、削除、消去、及び追加が含まれるが、これらには限定されない。本 SFR には、セキュリティ管理者による利用者パスワードのリセットも含まれる。

5.7.3 管理機能の特定 (FMT_SMF)

5.7.3.1 FMT_SMF.1 管理機能の特定

FMT_SMF.1	**管理機能の特定**

FMT_SMF.1.1 TSF は、下記の管理機能を実行することができなければならない：

- *TOE をローカル及びリモートに管理する能力；*
- *アクセスバナーを設定する能力；*
- *セションの終了またはロックまでのセション非アクティブ時間を設定する能力；*
- *TOE をアップデートし、アップデートのインストールに先立ってディジタル署名機能を用いてそのアップデートを検証する能力；*
- *ファイアウォールの規則を設定する能力；*
- *[選択：*
    - *監査のふるまいを設定する能力；*
    - *FIA_UIA_EXT.1 に特定されるように、エンティティが識別され認証される*

前に利用可能な TOE が提供するサービスのリストを設定する能力；
- *暗号機能を設定する能力；*
- *その他の機能なし。]*

適用上の注釈 26

TOE は、ローカル及びリモート管理のための機能を提供しなければならない。これには、FTA_TAB.1 のアクセスバナー及びFTA_SSL.3 及びFTA_SSL.4 のセション非アクティブ時間を設定する能力が含まれる。項目「TOE をアップデートし、アップデートのインストールに先立ってディジタル署名機能を用いてそのアップデートを検証する能力」には、FMT_MOF.1(1)/TrustedUpdate 、 FMT_MOF.1(2)/TrustedUpdate (ST に含まれる場合)、FIA_X509_EXT.2.2 及びFPT_TUD_EXT.2.2 (ST に含まれ、またこれらに管理者によって設定可能なアクションが含まれる場合) からの関連する管理機能が含まれる。同様に、選択「監査のふるまいを設定する能力」には、FMT_MOF.1(1)/Audit 、 FMT_MOF.1(2)/Audit 、FMT_MOF.1.1(1)/AdminAct、FMT_MOF.1.1(2)/AdminAct 及びFMT_MOF.1/LocSpace (これらの SFR のうち ST に含まれるものすべてについて) からの関連する管理機能が含まれる。TOE が管理者に監査のふるまいを設定、あるいは識別または認証に先立って利用可能なサービスを設定する能力を提供する場合、もしくは TOE 上の暗号化機能のいずれかが設定可能な場合には、ST 作成者は 2 番目の選択内で適切な 1 つまたは複数の選択を行い、それ以外の場合には「その他の機能なし」を選択する。

5.7.4 セキュリティ管理役割 (FMT_SMR)

5.7.4.1 FMT_SMR.2 セキュリティ役割における制限

FMT_SMR.2	セキュリティ役割における制限

FMT_SMR.2.1 TSF は、以下の役割を維持管理しなければならない：

- *セキュリティ管理者。*

FMT_SMR.2.2 TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.2.3 TSF は、以下の条件

- *セキュリティ管理者役割は、ローカルに TOE を管理できなければならない；*
- *セキュリティ管理者役割は、リモートに TOE を管理できなければならない*

が満たされることを保証しなければならない。

適用上の注釈 27

FMT_SMR.2.3 は、ローカルコンソールを介して、及びリモートメカニズム (IPsec, SSH, TLS, TLS/HTTPS) を介して、セキュリティ管理者が TOE を管理できることを要求する。

5.8 TSF の保護 (FPT)

本セクションでは、TOE が鍵やパスワードなどの重要なセキュリティデータを保護するための要件、TOE の継続した正しい動作 (ファームウェアまたはソフトウェアの完全性検証失敗の検出を含む) を監視する自己テストを提供するための要件、及び TOE ファームウェア／ソフトウェアへのアップデートのための高信頼方法を提供するための要件を定義する。さらに、TOE には FAU_GEN ファミリの下で正確な監査記録をサポートするために高信頼

タイムスタンプを提供することが要求される。

5.8.1 TSF データの保護 (拡張—FPT_SKP_EXT)

5.8.1.1 FPT_SKP_EXT.1 TSF データの保護 (すべての対称鍵の読み出し)

FPT_SKP_EXT.1	TSF データの保護 (すべての対称鍵の読み出し)

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が読み出しを防止しなければならない。

適用上の注釈 28

本要件の意図は、デバイスが鍵、鍵材料、及び認証クレデンシャルを許可されない暴露から保護することである。このデータは、それらが割り当てられたセキュリティ機能の目的のためにのみアクセスされるべきであり、また他のいかなる時にもそれらが表示／アクセスされる必要はない。本要件は、これらが存在すること、使用中であること、または依然として有効であることの示唆をデバイスが提供することを妨げるものではない。しかし本要件は、その値をあからさまに読み出すことを制限する。

5.8.2 管理者パスワードの保護 (拡張—FPT_APW_EXT)

5.8.2.1 FPT_APW_EXT.1 管理者パスワードの保護

FPT_APW_EXT.1	管理者パスワードの保護

FPT_APW_EXT.1.1 TSF は、パスワードを平文以外の形態で保存しなければならない。

FPT_APW_EXT.1.2 TSF は、平文パスワードの読み出しを防止しなければならない。

適用上の注釈 29

本要件の意図は、生のパスワード認証データが平文で保存されず、また利用者または管理者の誰も平文パスワードを「通常の」インタフェースを介して読み出すことができないことである。もちろん全能の管理者は、直接メモリを読み出してパスワードを取り出すことができるだろうが、そのようなことはしないと信頼されている。

5.8.3 TSF テスト (拡張—FPT_TST_EXT)

TSF によって利用される基盤となるセキュリティメカニズムの故障の一部を検出するため、TSF は自己テストを行う。この自己テストの範囲は製品開発者へ任されているが、一連の自己テストがより包括的であれば、エンタープライズアーキテクチャが開発されるプラットフォームとして、より信頼できるものになるはずである。

(本コンポーネントについては、選択ベース要件が附属書 B に存在する)

5.8.3.1 FPT_TST_EXT.1 TSF テスト (拡張)

FPT_TST_EXT.1	TSF テスト

FPT_TST_EXT.1.1 TSF は、TSF の正しい動作を実証するために、[選択: *初期立ち上げ中 (電源投入時に)*、*通常運用中周期的に*、*許可利用者の要求時に*、*条件 [割付：自己テストが動作すべき条件] 下で*] 以下の自己テストのスイートを実行しなければならない: [割付: *TSF によって実行される自己テストのリスト*]。

適用上の注釈 30

自己テストは、初期立ち上げ中 (電源投入時に) 実行されることが期待される。その他の選択肢は、それらが初期立ち上げ中に実行されない理由を開発者が正当化できる場合にのみ、使用されるべきである。SFR を満たすために必要な暗号機能の正しい動作と同様に、ファームウェア及びソフトウェアの完全性の検証のための自己テストが、少なくとも実行されることが期待されている。起動中にすべての自己テストが実行されるのではないような場合、本 SFR を複数繰り返して、適切な選択肢が選択されるように使用すること。本 cPP の将来のバージョンで、自己テストのスイートは、少なくとも、measurement を実行するコンポーネントの自己テストを含む、Measured ブートのメカニズム (訳注：TPM 等を用いて保護されたブートプロセスによるテスト等) が含まれることが要求されることになる。

適用上の注釈 31

自己テストメカニズムによって証明書が用いられる場合 (例、完全性検証用の署名検証のため等)、証明書は、FIA_X509_EXT.1 に従って有効性確認され、かつ FIA_X509_EXT.2.1 で選択されるべきである。さらに、FPT_TST_EXT.2 が ST に含まれなければならない。

5.8.4 高信頼アップデート (FPT_TUD_EXT)

セキュリティ管理者がシステムアップデートの信頼性検証に失敗することは、システム全体のセキュリティの危殆化を引き起こすかもしれない。アップデートの生成元への信頼を確立するために、アップデートを調達し、TOE が提供するディジタル署名メカニズムを介してアップデートを暗号技術的にチェックし、アップデートをシステムへインストールするため、システムは暗号メカニズム及び手続きを提供することができる。このプロセスが完全に自動化されるという要件は存在しないが、アップデート上の署名が有効であることを管理者が保証する方法に加えて、手動で行われなければならないあらゆる手続きがガイダンス文書に詳述されること。

(本ファミリについては、選択ベース要件が附属書 B に存在する)

5.8.4.1 FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1	高信頼アップデート

FPT_TUD_EXT.1.1 TSF は、*セキュリティ管理者に* TOE ファームウェア／ソフトウェアの一番最近にインストールされたバージョンと同様に、TOE ファームウェア／ソフトウェアの現在実行中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。

適用上の注釈 32

現在動作中 (実行中) のバージョンは、一番最近にインストールされたバージョンではないかもしれない。例えば、アップデートはインストールされたが、このアップデートが動作するためにはシステムのリブートが必要かもしれない。従って、問い合わせには一番最近にインストールされたアップデートと一番最近に実行されたバージョンの両方が示されるべきであることを明確にしておく必要がある。

FPT_TUD_EXT.1.2 TSF は、*セキュリティ管理者に* TOE ファームウェア／ソフトウェアへのアップデートを手動で開始する能力及び [選択 : *アップデートの自動的なチェックをサポートする、自動アップデートをサポートする、その他のアップデートメカニズムなし*] 能力を提供しなければならない。

適用上の注釈 33

FPT_TUD_EXT.1.2 での選択は、アップデートの自動的なチェックのサポートと自動アップデートのサポートとを区別している。最初の選択肢は新たなアップデートが利用可能であるかどうか TOE がチェックしてこれを管理者へ通知すること (例、管理セション中のメッセージによって、ログファイルによって) を意味しているが、実際にアップデートを実行するためには管理者による何らかのアクションを必要としている。第 2 の選択肢は、TOE がアップデートをチェックして、利用可能かどうかに応じてそれを自動的にインストールすることを意味している。

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

適用上の注釈 34

FPT_TUD_EXT.1.3 での選択において参照されるディジタル署名メカニズムは、FCS_COP.1(2) に特定されるアルゴリズムの 1 つである。FPT_TUD_EXT.1.3 において参照される公開ハッシュは、FCS_COP.1(3) に特定される機能の 1 つによって生成される。ST 作成者は、TOE によって実装されるメカニズムを選択すべきである；両方のメカニズムを実装することは受け入れ可能である。

適用上の注釈 35

本 cPP の将来のバージョンは、高信頼アップデートにディジタル署名メカニズムの利用を義務付けることになる。

適用上の注釈 36

アップデート検証メカニズムによって証明書が用いられる場合、証明書は FIA_X509_EXT.1 に従って有効性確認され、また FIA_X509_EXT.2.1 で選択されるべきである。さらに、FPT_TUD_EXT.2 が ST に含まれなければならない。

適用上の注釈 37

本 SFR における「アップデート」とは、不揮発性のシステム常駐ソフトウェアコンポーネントを、別のものと置き換えるプロセスを意味する。前者は NV イメージと呼ばれ、後者はアップデートイメージと呼ばれる。アップデートイメージは通常 NV イメージよりも新しいが、これは要件ではない。システム所有者がコンポーネントをより古いバージョンへロールバックすることを望むような正当な場合が存在する (例えば、コンポーネント製造業者が欠陥のあるアップデートをリリースしたり、アップデート中にはもはや存在しない文書化されていない機能にシステムが依存していたりする場合)。同様に、所有者は故障したストレージから回復させるために、NV イメージと同一のバージョンでアップデートすることを望むかもしれない。

TSF のすべての個別のソフトウェアコンポーネント (例えば、アプリケーション、ドライバ、カーネル、ファームウェア) は、対応する製造業者によってディジタル署名され、その後アップデートを行うメカニズムによって検証されるべきである。コンポーネントは異なる製造業者によって署名されるかもしれないことが認識されるため、アップデートプロセスが

アップデートと NV イメージの両方が同一の製造業者によって製造されたこと (例えば、公開鍵を比較することによって) または正当な署名鍵によって署名されたこと (例えば、X.509 証明書を使用する際に証明書の有効性確認が成功すること) を検証することは必須である。

5.8.5 タイムスタンプ (FPT_STM)

5.8.5.1 FPT_STM.1 高信頼タイムスタンプ

FPT_STM.1	高信頼タイムスタンプ

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。

適用上の注釈 38

TSF は、それ自体では TOE のロケーションの現在時刻に関する信頼できる情報を提供しないが、管理者によって手動で、または NTP サーバを用いることによって提供される、外部の時刻及び日付情報に依存する。「高信頼タイムスタンプ」という用語は、外部的に提供される時刻及び日付情報の厳密な使用、及び変更前と変更後の時刻に関する情報を含めた時刻設定へのすべての変更のログ出力を指す。この情報を用いて、すべての監査データの実際の時刻を計算することが可能である。

5.9 TOE アクセス (FTA)

本セクションでは、TOE 上で実施される管理セションのセキュリティに関連した要件を特定する。特に、ローカルとリモート両方のセションは非アクティブ時間を監視され、時間間隔の閾値に達した際にロックまたは終了される。また管理者は自分の対話セションを積極的に終了できなければならず、また各セションの開始時に注意喚起通知が表示されなければならない。

5.9.1 TSF 起動セションロック (拡張—FTA_SSL_EXT)

5.9.1.1 FTA_SSL_EXT.1 TSF 起動セションロック

FTA_SSL_EXT.1	TSF 起動セションロック

FTA_SSL_EXT.1.1 TSF は、ローカルの対話型セションについて、 [選択：

- *セションのロック—セションのロック解除以外の利用者のデータアクセス／表示デバイスのアクティビティを禁止し、そしてセションのロック解除に先立って TSF への管理者再認証を要求すること；*
- *セションの終了*]

を、セキュリティ管理者によって特定される非アクティブ時間間隔後に行わなければならない。

5.9.2 セションロックと終了 (FTA_SSL)

5.9.2.1 FTA_SSL.3 TSF 起動による終了

FTA_SSL.3	TSF 起動による終了

FTA_SSL.3.1 詳細化：TSF は、*セキュリティ管理者によって設定可能なセション非アクテ*

*ィブ時間間隔後*に、**リモート**対話セションを終了しなければならない。

5.9.2.2 FTA_SSL.4 利用者起動による終了

FTA_SSL.4	利用者起動による終了

FTA_SSL.4.1 詳細化：TSF は、**管理者**自身の対話セションの、**管理者**主導による終了を許可しなければならない。

5.9.3 TOE アクセスバナー (FTA_TAB)

5.9.3.1 FTA_TAB.1 デフォルト TOE アクセスバナー

FTA_TAB.1	デフォルト TOE アクセスバナー

FTA_TAB.1.1 詳細化：管理利用者セションを確立する前に、TSF は、**セキュリティ管理者によって特定される** TOE の利用に関する勧告的**通知及び同意**警告メッセージを表示しなければならない。

適用上の注釈 39

本要件は、人間の利用者と TOE との間の対話型セションに適用されることが意図されている。接続を確立する IT エンティティまたはプログラム的な接続 (例えば、ネットワーク経由のリモート手続き呼び出し) が本要件によって網羅されることは要求されない。

5.10 高信頼パス／チャネル (FTP)

TOE への、そして TOE からの機密性のあるデータの送信に関する問題へ対処するため、適合 TOE は自分自身と端点との間のこれらの通信パスへ暗号化を提供する。これらのチャネルは、4 つの標準プロトコルの 1 つ (以上) を用いて実装される：IPsec、TLS、HTTPS、及び SSH。これらのプロトコルは、さまざまな実装上の選択を提供する RFC によって特定される。相互接続性と暗号攻撃への耐性を提供するための要件が、これらの選択の一部 (特に、暗号プリミティブに関するもの) に課されている。

通信に暴露からの保護 (及び改変の検出) を提供する以外に、記述された各プロトコル (IPsec、SSH、TLS、及び HTTPS) は暗号技術的にセキュアな方法で各端点の双方向認証を提供する。これは、たとえ 2 つの端点の間に悪意のある攻撃者が存在したとしても、通信パスのどちらかの端点に対してその通信の相手方として攻撃者が取って代わろうとする試行は検出されるであろうことを意味する。

5.10.1 高信頼チャネル (FTP_ITC)

5.10.1.1 FTP_ITC.1 TSF 間高信頼チャネル (詳細化)

FTP_ITC.1	TSF 間高信頼チャネル

FTP_ITC.1.1 TSF は **[選択：*IPsec*、*SSH*、*TLS*、*HTTPS*] を用いて**、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、及びチャネルデータの暴露からの保護及びチャネルデータの改変の検知を提供する、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：監査サーバ、 [選択：*認証サーバ*、*割付：[その他の機能]*]** との間の高信頼通信チャネルを提供**できる**なければならない。

FTP_ITC.1.2 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。

FTP_ITC.1.3 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。

適用上の注釈 40

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が用いられ得る手段を提供することである。TOE は、列挙されたプロトコルの少なくとも 1 つを用いて、監査情報を収集するサーバとの通信を行う。認証サーバ (例えば、RADIUS) との通信を行う場合には、ST 作成者は FTP_ITC.1.1 で「認証サーバ」を選択し、またこの接続は列挙されたプロトコルの 1 つによって保護されることが可能でなければならない。その他の許可された 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 (これらのエンティティについて) 及び選択 (これらの接続を保護するために用いられるプロトコルについて) を行う。ST 作成者は TOE のサポートする 1 つまたは複数のメカニズムを選択し、そしてそれらの選択に対応する附属書B の詳細なプロトコルの要件がST に含まれることを保証する。TLS が選択される場合、ST 作成者は FCS_TLSC_EXT.1 ではなく FCS_TLSC_EXT.2 を主張することになる。

通信を開始する側に関する要件は存在しないが、ST 作成者は TOE が許可された IT エンティティとの通信を開始できるサービスを FTP_ITC.1.3 の割付において列挙する。

本要件は、通信が最初に確立される際だけではなく、中断後に再開する際にも保護されることを意味している。TOE 設定の一部に、他の通信を保護するトンネルを手作業で設定することが含まれる場合があるかもしれない。また中断後に TOE が (必要とされる) 人手での介入を伴って自動的に通信の再確立を試行する場合、攻撃者が重要な情報を得たり接続を危殆化できたりするウィンドウが形成されることがあるかもしれない。

5.10.2 高信頼パス (FTP_TRP)

5.10.2.1 FTP_TRP.1 高信頼パス (詳細化)

FTP_TRP.1	**高信頼パス**

FTP_TRP.1.1 TSF は **[選択：*IPsec, SSH, TLS, HTTPS*] を用いて**、他の通信パスとは論理的に区別され、その端点の保証された識別、及び通信データの *暴露からの保護及びチャネルデータの改変の検知を提供する* 、それ自身と **許可されたリモート管理者** との間の通信パスを提供できなければならない。

FTP_TRP.1.2 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。

FTP_TRP.1.3 TSF は、**最初の管理者認証及びすべてのリモート管理者アクション** について、高信頼パスを用いることを要求しなければならない。

適用上の注釈 41

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、及びリモート管理者による TOE とのすべての通信はこのパス上で行われることを保証する。この高信頼通信チャネルを通過するデータは、最初の選択で選ばれたプロトコルに定義されるように暗号化される。ST 作成者は TOE のサポートする 1 つまたは複数のメカニズムを選択し、そしてそれらの選択に対応する附属書 B の詳細なプロトコルの要件が ST に含まれることを保証する。

5.11 ファイアウォール (FFW)

5.11.1 ステートフルトラフィックフィルタファイアウォール (FFW_RUL_EXT)

許可されない情報の暴露、サービスへの不適切なアクセス、サービスの誤使用、サービスの中断または拒否、及びネットワークベースの調査に関連する課題に対処するため、適合 TOE は、ステートフルトラフィックフィルタファイアウォール機能を実装する。その機能は、確立されたコネクション情報と同様に、該当するネットワークトラフィックの発信側 (送信元) 及び／または受信側 (宛先) のネットワークノードのネットワークアドレス及びポートに基づいて、保護されたネットワークとその他の接続されたネットワークとの間のネットワークトラフィックのフローを制限する。

ステートフルパケットインスペクションは、TOE を介して流れるパケットの動作に役立てるために使用される。TOE インタフェースにおいて処理される各パケットに対する規則 (ルールセット) を適用するよりもむしろ、TOE は、パケットが「承認済み」の確立されたコネクションに属するかどうかを決定する。パケットが確立されたセションの一部であるかどうかを決定するために用いられる属性のミニマムセットは、TCP 及び UDP について必須であり、また ST 作成者は TCP セション用と考えられる属性を拡張することが許可され、かつ、もし彼らが望む場合には ICMP プロトコルを追加することが許可される。

適合 TOE は、ネットワークトラフィックのフローをログ出力する能力を実装する。具体的には、TOE は、設定されたルールに一致するようなネットワークトラフィックがあった場合、「ログ出力」するようなファイアウォール特有のファイアウォールルールを管理者が設定する手段を提供する。結果として、「ログ出力」するように設定されたファイアウォールルールに一致するかどうかの検証は、一致した時はいつでも参考情報としての事象のログ出力が行われることになる。

5.11.1.1 FFW_RUL_EXT.1 ステートフルトラフィックフィルタリング

FFW_RUL_EXT.1	ステートフルトラフィックフィルタリング

FFW_RUL_EXT.1.1 TSF は、TOE によって処理されるネットワークパケットにステートフルトラフィックフィルタリングを実行しなければならない。

適用上の注釈 42

本エレメントは、TOE のインタフェースで処理されるネットワークパケットに適用されるポリシー (ステートフルトラフィックフィルタリング) を識別する。TOE のインタフェースで受信されたすべてのパケットは、このポリシーを表現する規則 (ルールセット) が適用されるか、あるいは確立されたコネクションに属するそのパケットであることを決定されるかのいずれかである。本コンポーネントの残りのエレメントは、ポリシーの詳細を提供する。

本要件は、ネットワークインタフェースがネットワークトラフィックによって飽和 (saturated)／圧倒 (overwhelmed) されている場合であっても強制される。

TOE は、これには基盤となるプラットフォームも含まれるが、フローを許可するルールが規則 (ルールセット) に含まれることなしに、またはフローを許可された確立されたコネクションにパケットが属していると思われることなしに、ネットワークパケットのフローを許可できないことに注意することは重要である。この原則は、TOE の起動中にも、また TOE が直面するかもしれない故障の際にも、成り立たなければならない。

FFW_RUL_EXT.1.2 TSF は、以下のネットワークプロトコルフィールドを用いたステート

フルトラフィックフィルタリングの定義を許可しなければならない：

- ICMPv4
  - Type
  - Code
- ICMPv6
  - Type
  - Code
- IPv4
  - 送信元アドレス
  - 宛先アドレス
  - トランスポート層プロトコル
- IPv6
  - 送信元アドレス
  - 宛先アドレス
  - トランスポート層プロトコル
  - [選択：*IPv6 拡張ヘッダタイプ [割付：IPv6 拡張ヘッダのフィールドのリスト]*、*その他のフィールドなし*]
- TCP
  - 送信元ポート
  - 宛先ポート
- UDP
  - 送信元ポート
  - 宛先ポート
- 及び個別のインタフェース。

適用上の注釈 43

本エレメントは、本要件によって強制されるべきルールを構築する際に適用可能なさまざまな属性を識別する － 適用されるインタフェースは TOE の特性であって、残りの識別された属性は関連する RFC で定義される。「トランスポート層プロトコル』は、IPv4/IPv6 のフィールドであって、TCP、UDP、ICMP、または GRE 等の該当するプロトコルを識別することに注意されたい。IPv6 拡張ヘッダは、RFC 2460 で定義されており、ST 作成者は、サポートされる各拡張ヘッダのどのフィールドがインスペクションのルールの構築における属性として使用されるかを指定することができる。また、上記で識別された「インタフェース」は、該当するネットワークトラフィックが受信された、または送信される外部ポートである。

FFW_RUL_EXT.1.3 TSF は、ステートフルトラフィックフィルタリングのルールに関連付けるために、以下の操作を許可しなければならない：その操作をログ出力しつつ、許可または破棄する。

適用上の注釈 44

本エレメントは、ネットワークトラフィックと照合するために使用されるルールに関連し得る操作を定義する。ログ出力されるべきデータは、表 1 のセキュリティ監査要件に識別されることに注意されたい。

FFW_RUL_EXT.1	「ログ出力」操作を設定されたルールの適用	送信元及び宛先アドレス 送信元及び宛先ポート トランスポート層プロトコル TOE インタフェース
	過大なネットワークトラフィックのため破棄されたパケットの表示	パケットを処理できなかった TOE インタフェース パケットの破棄の原因であるルールの識別子

FFW_RUL_EXT.1.4 TSF は、個別の各ネットワークインタフェースに、ステートフルトラフィックフィルタリングのルールが割り当てられることを許可しなければならない。

適用上の注釈 45

本エレメントは、ルールがどこに割り当てが可能かを識別する。具体的には、適合 TOE は、レイヤ 3 及び 4 のネットワークトラフィックを取り扱う、利用可能な個別の各ネットワークインタフェースに対して、フィルタリングルールを割り当てることができなければならない。個別のネットワークインタフェースは、物理的、または論理的なものでもよいが、必ずしもネットワークの観点から可視であることは要求されない (例、それに IP アドレスが割り当てられている必要はない)。

各インタフェースに別々の規則(ルールセット)が存在しても、あるいは何らかの形でルールを特定のインタフェースに関連付けるような共有の規則 (ルールセット) が存在してもよいことに注意されたい。

FFW_RUL_EXT.1.5 TSF は、以下を実行しなければならない：

a) 以下のプロトコル用の許可された確立されたセションにルールが一致する場合、ステートフルトラフィックフィルタリングルールをさらに処理することなく、ネットワークパケットを受け入れる:以下のネットワークパケット属性に基づく TCP、UDP、[選択：*ICMP*、*その他のプロトコルなし*] :

1. TCP:送信元及び宛先アドレス、送信元及び宛先ポート、シーケンス番号、フラグ；
2. UDP：送信元及び宛先アドレス、送信元及び宛先ポート；
3. [選択：*「ICMP：送信元及び宛先アドレス、タイプ、 [選択：コード、 [割付：照合対象の属性のリスト]]」、その他のプロトコルなし*]。

b) 以下に基づいて、確立された一連のトラフィックフローから既存のトラフィックフローを削除する： [選択：*セション非アクティブタイムアウト、予期される情報フローの完了*]。

適用上の注釈 46

本エレメントは、セションが確立でき、またセションを用いて設定されたルールを完全に処理することなくトラフィックフローの決定を行えるように、TOE が状態を決定及び管理可能なプロトコルが識別されることを要求する。また本エレメントは、ネットワークパケットが一致し、セションを確立したことを決定するために使用される属性が識別されることも要求する。

ICMP がひとつのプロトコルとして選択される場合、パケットが確立された「コネクション」に属するかどうかを決定する時に、送信元及び宛先アドレスが考慮されるよう要求される。タイプ及びコード属性は、ICMP パケットが確立されたコネクションフローに予測されているものであるかどうかの決定において、より堅牢な機能を提供するために使用され得る。例えば、echo 要求が受信されていない場合、echo 応答がフローの一部であることは期待されないであろう。ICMP 属性用の選択におけるオープンな割付は、IPv6 属性を使用するかもしれない実装のために残されている。

本エレメントの項目 b) は、TCP パケットに FIN フラグを持ついずれかの端点により起動された TCP セションの終了等の事象を観測することにより、確立された情報フローが確立された一連の情報フローから削除されるべきであることをファイアウォールが決定できる方法についての特定を要求している。プロトコルが異なる形で取り扱われる場合、ST がそれらの違いを識別することが期待される。

FFW_RUL_EXT.1.6 TSF は、すべてのネットワークトラフィックにおいて、以下のデフォルトのステートフルトラフィックフィルタリングのルールを強制しなければならない：

a) TSF は、無効なフラグメントであるパケットを破棄し、またその [選択：*カウント*、*ログ出力*] ができなければならない；
b) TSF は、完全に再構成ができないフラグメント化されたパケットを破棄し、またその [選択：*カウント*、*ログ出力*] ができなければならない；
c) TSF は、ネットワークパケットの送信元アドレスがブロードキャストネットワーク上にあると定義されるようなパケットを破棄し、またその*ログ出力*ができなければならない；
d) TSF は、ネットワークパケットの送信元アドレスがマルチキャストネットワーク上にあると定義されるようなパケットを破棄し、またその*ログ出力*ができなければならない；TSF は、ネットワークパケットの送信元アドレスがループバックアドレスであると定義されるようなパケットを破棄し、またその*ログ出力*ができなければならない；
e) TSF は、ネットワークパケットの送信元または宛先アドレスが、IPv4 について RFC 5735 に特定されるとおり、未指定 (すなわち、0.0.0.0) または「将来のために予約された」アドレス (すなわち、240.0.0.0/4) であると定義されるようなネットワークパケットを破棄し、またそのログ出力ができなければならない；
f) TSF は、ネットワークパケットの送信元または宛先アドレスが、IPv6 について RFC 3513 に特定されるとおり、「未指定アドレス」または「将来のために予約された」アドレス (すなわち、以下のアドレス範囲：2000::/3 にないユニキャストアドレス) であると定義されるようなネットワークパケットを破棄し、またそのログ出力ができなければならない；
g) TSF は、以下の IP オプションを持つネットワークパケットを破棄し、またそのログ出力ができなければならない：ルーズソースルーティング (Loose Source Routing)、ストリクトソースルーティング (Strict Source Routing)、またはレコードルート (Record Route)；及び
h) [選択： *[割付：TOE によって強制されるその他のデフォルトのルール]*、*その他のルールなし*]。

適用上の注釈 47

本 cPP の将来のバージョンは、設定を適用する必要なしに、これらのデフォルトのルールを TOE が実装することを要求することになる。

FFW_RUL_EXT.1.7 TSF は、以下のルールに従った破棄及びログ出力ができなければならない：

a) TSF は、ネットワークパケットの送信元アドレスが、ネットワークパケットを受信したネットワークインタフェースのアドレスと等しいような、ネットワークパケットを破棄し、またそのログ出力ができなければならない；
b) TSF は、ネットワークパケットの送信元または宛先アドレスがリンクローカルアドレスであるようなネットワークパケットを破棄し、またそのログ出力ができなければならない；
c) TSF は、ネットワークパケットの送信元アドレスが、ネットワークパケットを受信したネットワークインタフェースと関連するネットワークに属さないような、ネットワークパケットを破棄し、またそのログ出力ができなければならない。

適用上の注釈 48

これらのルールは設定されることがあることに注意されたい。

FFW_RUL_EXT.1.8 TSF は、管理者が定義した順序で、該当するステートフルトラフィックフィルタリングのルールを処理しなければならない。

適用上の注釈 49

本エレメントは、照合のために処理されるように設定されたフィルタリングのルールの順序を管理者が定義できることを要求する。フィルタリングルールは、許可されたセションが確立されていない場合、または動的なルールが作成されている場合にのみ、適用される。

FFW_RUL_EXT.1.9 TSF は、照合するルールが識別されない場合、パケットフローを拒否しなければならない。

適用上の注釈 50

本エレメントは、パケットが確立されたセションの一部である場合を除いて、適用されるルールが存在しない際のふるまいは常にネットワークトラフィックの拒否であることを要求しており、その他の操作は要求されないが、必ずしも禁止されているわけではない。

FFW_RUL_EXT.1.10 TSF は、*ハーフオープンした TCP コネクションを*、管理者が定義した数に制限できなければならない。*設定された制限に達した際には、新たなコネクション試行は破棄されなければならず、また破棄した事象は [選択：カウント、ログ出力] されなければならない。*

適用上の注釈 51

ハーフオープンした TCP 接続は、RFC 793 に定義される完全な 3 ウェイハンドシェイクを完了していないものである。不完全な TCP 接続、すなわち 3 ウェイハンドシェイクの SYN 及び SYN-ACK の部分を完了したものは、エンドホスト及びそのトラフィック経路中のステートフルトラフィックフィルタリングデバイスの貴重な資源を消費し、またその量が十分であれば、サービス拒否条件をもたらす可能性がある。自分自身、及び任意の保護を目的としたサービスを保護するため、適合 TOE はハーフオープンした TCP コネクションの数を制限できなければならない。

6. セキュリティ保証要件

本 cPP は、評価者が評価の対象となる文書を評価し、独立テストを実施するための範囲を設定するため、セキュリティ保証要件 (SAR) を識別する。

本セクションには、本 cPP に対する評価で必要とされる、CC パート 3 の SAR 一式が列挙されている。実行されるべき個別のアクティビティは、 [SD] に特定されている。

本 cPP に適合するために作成された ST に対する TOE 評価についての一般的なモデルは以下のとおりである：ST が評価可能と承認された後、ITSEF は、TOE、IT 支援環境 (必要な場合)、及び TOE のガイダンス文書を入手する。ITSEF は、ASE 及び ALC の SAR について情報技術セキュリティ評価のための共通方法 (CEM) により義務付けられたアクションを実行することが期待されている。ITSEF は、TOE 中に具体化される特定の技術に適用されるようにその他の CEM 保証要件の解釈として意図された、SD に含まれる評価アクティビティについても、実行すること。また SD に取り込まれている保証アクティビティは、TOE が cPP に適合することを実証するために開発者が何を提供する必要があるかについての明確な説明についても提供している。

TOE のセキュリティ保証要件は、表 2 に識別される。

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

表 2：セキュリティ保証要件

6.1 ASE：セキュリティターゲット

ST は、CEM に定義される ASE アクティビティにより評価される。さらに、SD にて特定される評価アクティビティであり、TOE の技術タイプに特有の TSS に含まれるべき必要な記述を要求する評価アクティビティが、存在するかもしれない。

附属書 D は、ランダムビット生成器のエントロピー品質に関して、提供されると期待される情報の記述を提供している。

ASE_TSS.1.1C 詳細化：TOE 要約仕様は、TOE がどのように各 SFR を満たすのかを記述しなければならない。**エントロピー分析の場合、TSS はエントロピーについての必須の補足情報と共に用いられる。**

セキュリティターゲットの完全適合の要件は、セクション 2 及び [SD-ND, 3.1] において記述されている。

6.2 ADV：開発

TOE についての設計情報は、ST の TSS 部分、及び本 cPP が要求する公知とされるべきでない必須の補足情報と同様に、エンドユーザが利用可能なガイダンス文書に含まれている。

6.2.1 基本機能仕様 (ADV_FSP.1)

機能仕様は、TOE のセキュリティ機能インタフェース (TSFI) を記述する。これらのインタフェースの形式的または完全な仕様は必要とされない。さらに、本 cPP に適合する TOE は必然的に TOE の利用者によって直接呼び出すことのできない運用環境へのインタフェースを持つことになるため、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ことから、そのようなインタフェースそれ自体の記述を特定することにはあまり意味がない。本 cPP では、本ファミリの評価アクティビティは、TSS に存在する機能仕様に対応したインタフェース及び AGD 文書に存在するインタフェースを理解することにフォーカスしている。SD において特定された評価アクティビティを満たすために、追加の「機能仕様」文書は、必要とはされない。

SD の評価アクティビティは、該当する SFR と関連付けられている；これらは SFR と直接関連しているため、ADV_FSP.1.2D エレメントのトレースは、すでに暗黙的になされており、追加の文書は必要とされない。

6.3 AGD：ガイダンス文書

ガイダンス文書は、ST と共に提供される。ガイダンスには、運用環境がセキュリティ機能に対する役割を果たすことができることを IT 要員が検証する方法の記述が含まれなければならない。この文書は、非形式的なスタイル（口語体）で IT 要員が読みやすい形であるべきである。

ガイダンスは、ST で主張されたとおり、製品がサポートしているすべての運用環境に関して提供されなければならない。このガイダンスには、以下が含まれる：

- その環境において TSF を正常にインストールするための指示；及び
- 製品として、またより大規模な運用環境のコンポーネントとして、TSF のセキュリティを管理するための指示；及び
- 保護された管理機能を提供するための指示。

特定のセキュリティ機能に関するガイダンスも提供されなければならない；そのようなガイダンスに関する要件は、SD で特定される評価アクティビティに含まれている。

6.3.1 利用者操作ガイダンス (AGD_OPE.1)

利用者操作ガイダンスは、必ずしも単一の文書に含まれている必要はない。利用者、管理者及びアプリケーション開発者向けのガイダンスが、複数の文書またはウェブページに分散されていてもよい。

開発者は、評価者がチェックすることになるガイダンスの詳細を確認するために、SD に含まれる評価アクティビティをレビューすべきである。これによって、受け入れ可能なガイダンスの作成に必要な情報が提供されることになる。

6.3.2 準備手続き (AGD_PRE.1)

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に評価アクティビティを確認すべきである。

6.4 ALC クラス：ライフサイクルサポート

本 cPP に適合する TOE に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの検査よりもむしろ、ライフサイクルのエンドユーザから見えるような側面に限定されている。これは、製品の全般的な信頼性の向上に開発者の実践が果たす重要な役割を軽減することを意味していない；むしろ、本保証レベルでの評価で利用可能な情報を反映したものである。

6.4.1 TOE のラベル付け (ALC_CMC.1)

本コンポーネントは、TOE を同一ベンダの他の製品またはバージョンから区別でき、またエンドユーザによって調達される際に容易に指定できるように、TOE を識別することを目標としている。ラベルは、「ハードラベル」 (例、金属への刻印、紙ラベル等) または「ソフトラベル」 (例えば、問い合わせ時に電子的に提示されるもの等) からなる。

評価者は、ALC_CMC.1 と関連付けられた CEM ワークユニットを実行する。

6.4.2 TOE CM 範囲 (ALC_CMS.1)

TOE の適用範囲とそれに関連した評価証拠の要件を考慮して、評価者は ALC_CMS.1 に関連する CEM ワークユニットを実行する。

6.5 ATE クラス：テスト

テストは、システムの機能的な側面と、及び設計または実装の弱点を利用するような側面について特定される。前者は ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 cPP については、テストは公表された機能及びインタフェースに基づき、設計情報の利用可能性に依存して行われる。評価プロセスの主要なアウトプットのひとつは、以下の要件に特定されるテスト報告書である。

6.5.1 独立テスト—適合 (ATE_IND.1)

テストは、TSS とガイダンス文書 (「評価される構成」の指示を含む) に記述された機能を確認するために実施される。テストで重視されるのは、セクション 5 に特定された要件が満たされていることを確認することである。SD における評価アクティビティは、SFR への適合を検証するために必要な具体的なテストアクティビティを識別している。評価者は、本 cPP への適合を主張するプラットフォーム／TOE の組み合わせにフォーカスしたカバレージの論拠とともに、テストの計画及び結果を文書化したテスト報告書を作成する。

6.6 AVA クラス：脆弱性評定

本 cPP の第一世代として、iTC は、これらの種類の製品にどのような脆弱性が発見されているのかを見つけるために公開情報源を調査することが期待され、その内容を AVA_VAN の議論へ提供することが期待される。ほとんどの場合、これらの脆弱性には、基本的な攻撃能力を持つ攻撃者を超える高度な知識が要求される。本情報は、将来のプロテクションプロファイルの開発において活用されるだろう。

6.6.1 脆弱性調査 (AVA_VAN.1)

[SD]の附属書 A に、脆弱性分析を実行する際の評価者へのガイドが提供されている。

A. オプションの要件

本 cPP の序説で示したように、ベースライン要件 (TOE により実行されなければならないもの) は、本 cPP の本体に含まれている。さらに、2 種類のその他の種別の要件が附属書 A 及び B に特定されている。

(本附属書における) 最初の種別は、ST に含まれることが可能な要件ではあるが、TOE が本 cPP への適合を主張するためには必須とされないものである。 (附属書 B における) 第 2 の種類は、cPP の他の SFR における選択に基づいた要件である：特定の選択がなされた場合には、その附属書の追加の要件が ST の本文に含まれる必要がある (例、高信頼チャネル要件で選択された暗号プロトコル等)。

A.1 オプションの SFR の監査事象

要件	監査対象事象	追加監査記録の内容
FAU_STG.1	なし。	なし。
FAU_STG_EXT.2	なし。	なし。
FAU_STG_EXT.3	監査事象用格納領域の空き容量低下に関する警告。	なし。
FMT_MOF.1(1)/Audit	外部 IT エンティティへの監査データ送信のふるまいの変更。	なし。
FMT_MOF.1(2)/Audit	監査データの取り扱いのふるまいの変更。	なし。
FMT_MOF.1(1)/AdminAct	TSF のふるまいの変更。	なし。
FMT_MOF.1(2)/AdminAct	サービスの開始及び停止。	なし。
FMT_MOF.1(1)/LocSpace	ローカルの監査格納領域が満杯となった際の監査機能のふるまいの変更。	なし。
FMT_MTD.1/AdminAct	暗号鍵の変更、削除、生成／インポート。	なし。
FPT_FLS.1/Local Audit Storage Space Full	なし。	なし。
FFW_RUL_EXT.2	ST で定義される。	ST で定義される。

表 3：TOE オプションの SFR 及び監査対象事象

A.2 セキュリティ監査 (FAU)

A.2.1 セキュリティ監査事象格納 (FAU_STG.1 及び拡張—FAU_STG_EXT)

監査データのローカルな格納領域は TOE そのものが必要としてもよく、またその場合 TOE は FAU_STG.1 に記述されるような不正な改変 (削除を含む) に対する監査証跡の保護を主張してもよい。またネットワークデバイスの監査データのローカルな格納領域には限りがあるので、ローカル格納領域を超過した場合には監査データが失われる可能性がある。セキュリティ管理者は、監査記録の破棄、上書き等された回数に興味があるかもしれない。この回数は、継続的に生成される監査データによって格納領域の超過が発生した後、深刻な問題が発生したかどうかの指標として役立つかもしれない。従って、ネットワークデバイスのこれらオプションの機能を表現するために FAU_STG_EXT.2 及び FAU_STG_EXT.3 が定義される。

A.2.1.1 FAU_STG.1 保護された監査証跡格納

FAU_STG.1	保護された監査証跡格納

FAU_STG.1.1 TSF は、監査証跡に保存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。

FAU_STG.1.2 TSF は、監査証跡に保存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。

A.2.1.2 FAU_ STG_EXT.2 失われた監査データのカウント

FAU_STG_EXT.2	失われた監査データのカウント

FAU_STG_EXT.2.1 TSF は、ローカルの格納領域が満杯となり、TSF が FAU_STG_EXT.1.3 に定義されるアクションの 1 つを取った場合、 [選択：*破棄された*、*上書きされた*、*割付：その他の情報*] 監査記録の数についての情報を提供しなければならない。

適用上の注釈 52

このオプションは、TOE が本機能をサポートする場合に選ばれるべきである。

監査記録のローカルの格納領域が管理者によって消去される場合、SFR の選択に関連するカウンタはその初期値 (おそらくは 0) にリセットされるべきである。ガイダンス文書には、管理者が監査記録のローカルな格納領域を消去する際の監査データの喪失に関する管理者への警告が含まれるべきである。

A.2.1.3 FAU_ STG_EXT.3 ローカルの格納領域に関する警告の表示

FAU_STG_EXT.3	ローカルの格納領域に関する警告の表示

FAU_STG_EXT.3.1 TSF は、監査データを格納するためのローカルの格納領域が使い尽くされたり、ローカルの格納領域が不十分なため TOE が監査データを喪失する前に、警告を生成して利用者へ通知しなければならない。

適用上の注釈 53

このオプションは、監査データのローカルの格納領域が使い尽くされる前に TOE が警告を生成して利用者へ通知する場合に選択されるべきである。これは、監査対象事象がローカルの格納領域のみに格納される場合に役立つかもしれない。

FAU_STG_EXT.1.3 により要求される警告メッセージが利用者へ通知可能であることは保証される必要がある。事象発生時に管理者セションがアクティブであることは保証できないため、この通知は監査ログそのものにより行われるべきである。

A.3 セキュリティ管理 (FMT)

A.3.1 TSF における機能の管理 (FMT_MOF)

A.3.1.1 FMT_MOF.1 セキュリティ機能のふるまいの管理

FMT_MOF.1(1)/Audit	セキュリティ機能のふるまいの管理

FMT_MOF.1.1(1)/Audit TSF は、*外部 IT エンティティへの監査データの送信*の機能の*ふるまいを決定する、ふるまいを変更する*能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 54

FMT_MOF.1(1)/Audit は、FAU_STG_EXT.1.1 に定義された外部 IT エンティティへ監査データを送信するための送信プロトコルが設定可能な場合は常に選ばれるべきである。

FMT_MOF.1(2)/Audit	セキュリティ機能のふるまいの管理

FMT_MOF.1.1(2)/Audit TSF は、*監査データの取り扱い*の機能の*ふるまいを決定する、ふるまいを変更する*能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 55

FMT_MOF.1(2)/Audit は、監査データの取り扱いが設定可能である場合にのみ、選ばれるべきである。「監査データの取り扱い」という用語は、SFR FAU_STG_EXT.1.2、FAU_STG_EXT.1.3、及び FAU_STG_EXT.2 の選択及び割付の異なる選択肢に対応する。

FMT_MOF.1(1)/AdminAct	セキュリティ機能のふるまいの管理

FMT_MOF.1.1(1)/AdminAct TSF は、*TOE セキュリティ機能*の機能の*ふるまいを変更する*能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 56

FMT_MOF.1(1)/AdminAct は、TOE セキュリティ機能のふるまいが設定可能である場合にのみ、選ばれるべきである。

FMT_MOF.1(2)/AdminAct	セキュリティ機能のふるまいの管理

FMT_MOF.1.1(2)/AdminAct TSF は、*サービス*の機能を 有効化、無効化 する能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 57

FMT_MOF.1(2)/AdminAct は、セキュリティ管理者がサービスを開始及び停止する能力を有する場合にのみ、選ばれるべきである。

FMT_MOF.1/LocSpace	セキュリティ機能のふるまいの管理

FMT_MOF.1.1/LocSpace TSF は、*ローカルの監査格納領域が満杯の際の監査機能*の機能の*ふるまいを決定する、ふるまいを変更する*能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 58

FMT_MOF.1/LocSpace は、ローカルな監査格納領域が満杯の際の監査機能のふるまいが設定可能である場合にのみ、選ばれるべきである。

A.3.2 TSF データの管理 (FMT_MTD)

A.3.2.1 FMT_MTD.1/AdminAct TSF データの管理

FMT_MTD.1/AdminAct	TSF データの管理

FMT_MTD.1.1/AdminAct TSF は、*暗号鍵を変更、削除、生成／インポートする*能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 59

FMT_MTD.1.1/AdminAct は、セキュリティ管理者によって暗号鍵が変更、削除、または生成／インポート可能である場合にのみ、選ばれるべきである。

A.4 TSF の保護 (FPT)

A.4.1 フェイルセキュア (FPT_FLS)

A.4.1.1 FPT_FLS.1/LocSpace セキュアな状態を保持した障害

FPT_FLS.1/LocSpace	セキュアな状態を保持した障害

FPT_FLS.1.1/LocSpace TSF は、以下の種類の故障が生じた際、セキュアな状態を保持しなければならない：*監査データのローカルの格納領域が満杯*。

適用上の注釈 60

監査データ用ローカル格納領域がこれ以上利用できないような場合に、TOE がすべてのセキュリティ機能を停止するよう設定されている (すなわち、セキュアな状態を保持する) 場合に、本 SFR は追加される必要がある。これにより、攻撃者は、追加の監査事象を生成することによって自分のアクションを隠蔽することができなくなるであろう。このふるまいは、FAU_STG_EXT.1.3 の選択の最後の割付 (すなわち、「それ以外の選択肢」) でモデル化されることが期待される。

A.5 ファイアウォール (FFW)

A.5.1 ステートフルトラフィックフィルタファイアウォール (FFW_RUL)

A.5.1.1 FFW_RUL_EXT.2 動的プロトコルのステートフルフィルタリング

FFW_RUL_EXT.2	動的プロトコルのステートフルフィルタリング

FFW_RUL_EXT.2.1 TSF は、以下のネットワークプロトコル用のネットワークトラフィックのフローを許可するルールの定義またはセションの確立を動的に実行しなければならない [選択：*FTP*、*SIP*、*H.323*： *[割付：その他のサポートされるプロトコル]*、*その他のプロトコルなし*]。

適用上の注釈 61

本エレメントは、たとえ既存のルールがそのフローを明示的には許可しない場合であっても、ネットワークトラフィックフローをファイアウォールが許可することを要求するような、より複雑なプロトコルの特定を要求している。例えば、FTP プロトコルは、利用者がファイルを転送しようとする場合、制御コネクションとデータコネクションの両方を要求する。ポート 21 (FTP サーバの制御ポート) 及びポート 20 (アクティブモードでのサーバのデータポート) というウェルノウンポートが利用される一方で、クライアント側では 1023 よりも大きいランダムなポートが利用される。パッシブモードでは、FTP サーバはポート 20 の代わりに 1023 よりも大きなランダムなポートを利用するかもしれない。データコネクションは、パッシブモードではクライアントにより起動され、アクティブモードでは FTP サーバにより起動される。

これらの種類のプロトコルでは、ルールセットによって拒否されるように見える場合であっても、「新しい」コネクションの確立が許可される (例、クライアント、または潜在的にサーバにより、どのランダムなポートが利用されるかを予測するできないルールであるため、コネクションを拒否するようなデフォルトのルールが適用されるように見えるかもしれない)。TSF は、トラフィックのフローを制御する動的なルールを作成するかもしれないし、または TSF は、RFC または同等の規格で特定されるプロトコル実装の予測に基づいて新しいコネクションが確立されることを暗黙に許可するかもしれない。

任意のネットワークパケットが、レイヤ 4 (TCP/UDP) よりも高いレイヤで検査されること

が全く期待されていないことに注意することが重要である。本要件は、予測不可能な UDP/TCP ポートを持つ期待されるコネクションが正しく確立されることを許可するように、ファイアウォールへルールが動的に挿入されるような条件を、ST 作成者が特定することを単純に要求する。

ST 作成者が追加のプロトコルを含める場合、上記の FTP についてなされたものと同様に、プロトコルのふるまいを特定する RFC または同等の規格が識別されなければならない。

B. 選択ベースの要件

本 PP の序説で示したように、本 PP の本体にはベースライン要件 (TOE またはその基盤となるプラットフォームによって行われなければならないもの) が含まれている。これ以外にも PP の本文中の選択に基づく追加の要件が存在し、特定の選択がなされた場合には、以下の追加の要件が含まれることが必要となる。

B.1 選択ベース SFR の監査事象

要件	監査対象事象	追加監査記録の内容
FCS_HTTPS_EXT.1	HTTPS セション確立の失敗	失敗の理由
FCS_IPSEC_EXT.1	IPsec SA の確立失敗	失敗の理由
FCS_SSHC_EXT.1	SSH セション確立の失敗	失敗の理由
	SSH 鍵変更(rekeying)の成功	接続の非 TOE 側端点 (IP アドレス)
FCS_SSHS_EXT.1	SSH セション確立の失敗	失敗の理由
	SSH 鍵変更(rekeying)の成功	接続の非 TOE 側端点 (IP アドレス)
FCS_TLSC_EXT.1	TLS セションの確立失敗	失敗の理由
FCS_TLSC_EXT.2	TLS セションの確立失敗	失敗の理由
FCS_TLSS_EXT.1	TLS セションの確立失敗	失敗の理由
FCS_TLSS_EXT.2	TLS セションの確立失敗	失敗の理由
FPT_TST_EXT.2	自己テストの失敗	失敗の理由 (無効な証明書の識別子を含む)
FPT_TUD_EXT.2	アップデートの失敗	失敗の理由 (無効な証明書の識別子を含む)
FMT_MOF.1(2)/TrustedUpdate	アップデートの自動チェックまたは自動アップデートの有効化または無効化。	なし。

表 4：選択ベースの SFR 及び監査対象事象

B.2 暗号サポート (FCS)

B.2.1 暗号プロトコル (拡張—FCS_HTTPS_EXT, FCS_ IPSEC_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

B.2.1.1 FCS_HTTPS_EXT.1 HTTPS プロトコル

FCS_HTTPS_EXT.1	HTTPS プロトコル

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。

適用上の注釈 62

ST 作成者は、特定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、本コンポーネントへエレメントを追加するか、または TSS に詳細情報を追加するか、のいずれかによって達成することができる。

FCS_HTTPS_EXT.1.2 TSF は、TLS を用いた HTTPS を実装しなければならない。

FCS_HTTPS_EXT.1.3 TSF は、ピア証明書が無効とみなされる場合、 [選択：*コネクションを確立しない、コネクションを確立するための認可を要求する、その他のアクションなし*] を行わなければならない。

適用上の注釈 63

有効性は、RFC 5280 に従い、証明書パス、有効期限、及び失効状態により決定される。

B.2.1.2 FCS_IPSEC_EXT.1 IPsec プロトコル

ネットワークデバイスの通信の端点は、地理的にも論理的にも遠く離れている可能性があり、さまざまな他のシステムを通過するかもしれない。ネットワークデバイスのセキュリティ機能は、任意の重要なネットワークトラフィック (管理トラフィック、認証トラフィック、監査トラフィック等) を保護できなければならない。ネットワークデバイスと外部 IT エンティティとの間の相互認証された通信チャネルを提供するひとつの方法は、IPsec を実装することである。

IPsec は、本 cPP の必須のコンポーネントではない。TOE が IPsec を実装する場合、何を保護するために IPsec プロトコルが実装されるかを定義するために FTP_ITC.1 及び／または FTP_TRP.1 の対応する選択が行われるべきである。

IPsec はピアツーピアのプロトコルであるため、クライアント要件とサーバ要件へ分離される必要はない。

FCS_IPSEC_EXT.1	**IPsec プロトコル**

FCS_IPSEC_EXT.1.1 TSF は、RFC 4301 に特定される IPsec アーキテクチャを実装しなければならない。

適用上の注釈 64

RFC 4301 は、セキュリティポリシーデータベース (SPD) を用いて IP トラフィックを保護する IPsec の実装を要求する。SPD は、IP パケットがどのように取り扱われるべきかを定義するために用いられる：パケットを保護 (PROTECT) する (例えば、パケットを暗号化する)、IPsec サービスをバイパス (BYPASS) する (例えば、暗号化なし)、またはパケットを廃棄 (DISCARD) する (例えば、パケットを破棄 (drop) する)。SPD は、ルータのアクセス制御リスト、ファイアウォールの規則(ルールセット)、「伝統的」な SPD 等、さまざまな方法で実装できる。実装の詳細にかかわらず、パケットが「ルール」に「一致」して、その結果アクションが実行されるという「ルール」がある。

ルールを順序付ける手段は存在しなければならないが、SPD が IP パケットを区別でき、それぞれにルールを適用できる限り、順序付けの一般的アプローチは必須ではない。複数の SPD (各ネットワークインタフェースに 1 つ) が存在してもよいが、これは必須ではない。

FCS_IPSEC_EXT.1.2 TSF は、SPD のいずれかに一致する名目的な最終エントリ、さもなければ一致せず廃棄されるようなエントリを持たなければならない。

FCS_IPSEC_EXT.1.3 TSF は、トランスポートモード及び [選択：*トンネルモード、その他のモードなし*] を実装しなければならない。

FCS_IPSEC_EXT.1.4 TSF は、暗号アルゴリズム AES-CBC-128、AES-CBC-256 (両者とも RFC 3602 により特定される) 及び [選択：*AES-GCM-128 (RFC 4106 で特定される)、AES-GCM-256 (RFC 4106 で特定される)、その他のアルゴリズムなし*] を用いて、セキュアハッシュアルゴリズム (SHA) ベースの HMAC とともに、RFC 4303 により定義される IPsec プロトコル ESP を実装しなければならない。

FCS_IPSEC_EXT.1.5 TSF は、以下のプロトコルを実装しなければならない：[選択：

- *IKEv1 として、RFC 2407、2408、2409、RFC 4109、[選択：拡張シーケンス番号についてその他の RFC なし、拡張シーケンス番号について RFC 4304]、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] において定義され、フェーズ 1 交換にメインモードを用いたもの；*
- *IKEv2 として、RFC 5996 及び [選択：NAT トラバーサルのサポートなし、RFC 5996 のセクション 2.23 で特定された NAT トラバーサルのサポートを必須とする]、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] において定義されたもの*

]。

適用上の注釈 65

TOE が IKEv1 用または IKEv2 用に SHA-2 ハッシュアルゴリズムを実装する場合、ST 作成者は RFC 4868 を選択すること。ST 作成者が IKEv1 を選択する場合、FCS_IPSEC_EXT.1.15 もまた ST に含まれなければならない。IKEv2 は、2016 年の第 3 四半期以降に評価に入る TOE については必須となるだろう。

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、暗号アルゴリズム RFC 3602 で特定される AES-CBC-128、AES-CBC-256 及び [選択：*RFC 5282 で特定される AES-GCM-128*、*AES-GCM-256*、*その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。

適用上の注釈 66

AES-GCM-128 及び AES-GCM-256 は、IKEv2 もまた選択されている場合にのみ選択が可能である。IKEv1 には AES-GCM を定義する RFC が存在しないためである。

FCS_IPSEC_EXT.1.7 TSF は、以下を保証しなければならない[選択：

- *IKEv1 フェーズ 1 の SA ライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること*
  [選択：
  - *バイト数；*
  - *ライフタイムの長さ、ここで時間の値は [割付：24 を含む整数範囲] 時間以内で設定可能；*

  ]；
- *IKEv2 の SA ライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること*
  [選択：
  - *バイト数；*
  - *ライフタイムの長さ、ここで時間の値は [割付：24 を含む整数範囲] 時間以内で設定可能*

  ]

]。

適用上の注釈 67

ST 作成者は、IKEv1 要件または IKEv2 要件のいずれかを (または、FCS_IPSEC_EXT.1.5 の選択によっては両方を) 選択すること。ST 作成者は、数量ベースのライフタイムまたは時間ベースのライフタイムのいずれか (または、その組み合わせ) を選択すること。本要件は、セキュリティ管理者が設定可能なライフタイムを提供することにより達成されなければならない (AGD_OPE により義務付けられる文書における適切な指示を用いて)。ハードコードされた制限は、本要件を満たさない。一般的には、実装のパラメタを設定するための指示が、SA のライフタイムを含めて、AGD_OPE のために作成されたガイダンス文書に含まれているべきである。

FCS_IPSEC_EXT.1.8 TSF は、以下を保証しなければならない[選択：

- *IKEv1 フェーズ 2 の SA ライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること*
  [選択：
  - *バイト数；*
  - *ライフタイムの長さ、ここで時間の値は [割付：8 を含む整数範囲] 時間以内で設定可能；*

  ]；
- *IKEv2 Child SA のライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること*
  [選択：

- *バイト数；*
- *ライフタイムの長さ、ここで時間の値は [割付：8 を含む整数範囲] 時間以内で設定可能；*

]

]。

適用上の注釈 68

ST 作成者は、IKEv1 要件または IKEv2 要件のいずれかを (または、FCS_IPSEC_EXT.1.5 の選択によっては両方を) 選択すること。ST 作成者は、数量ベースのライフタイムまたは時間ベースのライフタイムのいずれか (または、その組み合わせ) を選択すること。本要件は、セキュリティ管理者が設定可能なライフタイムを提供することにより達成されなければならない (AGD_OPE により義務付けられた文書における適切な指示を用いて)。ハードコードされた制限は、本要件を満たさない。一般的に、実装におけるパラメタを設定の指示が、SA のライフタイムを含めて、AGD_OPE 用に作成されたガイダンス文書に含まれているべきである。

FCS_IPSEC_EXT.1.9 TSF は、FCS_RBG_EXT.1 で特定されるランダムビット生成器を用いて、少なくとも [割付：*ネゴシエーションされた Diffie-Hellman グループのセキュリティ強度の少なくとも 2 倍である(1 つまたは複数) ビット数*] ビットを有するような、IKE の Diffie-Hellman 鍵交換に用いられる秘密値 x (g^x mod p における「x」) を生成しなければならない。

適用上の注釈 69

DH グループ 19 及び 20 については、「x」の値は生成元の点 G に対する乗数である。

実装によって、異なる Diffie-Hellman グループを SA の形成に用いるようなネゴシエーションが許されるかもしれないため、FCS_IPSEC_EXT.1.9 での割付は複数の値を含めてもよい。サポートされる各 DH グループについて、ST 作成者は、その DH グループに関連付けられるセキュリティ強度 (「セキュリティビット数」) を決定するため、NIST SP 800-57 "Recommendation for Key Management –Part 1: General" の表 2 を参照すること。それぞれの一意の値がその時、本エレメントの割付への記入に使用されること。例えば、DH グループ 14 (2048 ビット MODP) とグループ 20 (NIST 曲線 P-384 を用いた ECDH) をサポートする実装を想定してみよう。表 2 から、グループ 14 のセキュリティビット数は 112 であり、グループ 20 については 192 である。

FCS_IPSEC_EXT.1.10 TSF は、 [選択：*IKEv1*、*IKEv2*] 交換に使用される、以下の長さのノンスを生成しなければならない [選択：

- *[割付:ネゴシエーションされた Diffie-Hellman グループと関連付けられたセキュリティ強度]；*
- *少なくとも 128 ビット長で、 ネゴシエーションされた疑似乱数関数 (PRF) ハッシュの出力サイズの少なくとも半分の長さ*

] 。

適用上の注釈 70

ST 作成者は、IKEv2 もまた選択されている場合、ノンス長について 2 番目の選択肢を選択しなければならない (RFC 5996 でこれが義務付けられているため)。ST 作成者は、IKEv1 についてはどちらの選択肢を選択してもよい。

ノンス長の最初の選択肢については、実装によって異なる Diffie-Hellman グループを SA の

形成に用いるようなネゴシエーションが許されるかもしれないため、FCS_IPSEC_EXT.1.10 の割付は複数の値を含んでもよい。サポートされる各 DH グループについて、ST 作成者はその DH グループに関連付けられるセキュリティ強度 (「セキュリティビット数」) を決定するため、NIST SP 800-57 "Recommendation for Key Management –Part 1: General" の表 2 を参照すること。それぞれの一意の値がその時、本エレメントの割付への記入に使用されること。例えば、DH グループ 14 (2048 ビット MODP) とグループ 20 (NIST 曲線 P-384 を用いた ECDH) をサポートする実装を想定してみよう。表 2 から、グループ 14 のセキュリティビット数は 112 であり、グループ 20 については 192 である。

DH グループがネゴシエーションされる前にノンスが交換されるかもしれないため、使用されるノンスは鍵交換におけるすべての TOE が選択した提案をサポートするのに十分大きなものであるべきである。

FCS_IPSEC_EXT.1.11 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：*19 (256 ビットランダム ECP)*、*5 (1536 ビット MODP)*、*24 (256 ビット POS 付の 2048 ビット MODP)*、*20 (384 ビットランダム ECP)*、*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。

適用上の注釈 71

この選択は、サポートされた追加の DH グループを特定するために使用されること。これは、IKEv1 及び IKEv2 鍵交換に適用される。2015 年の第 3 四半期以降に評価に入る製品については、DH グループ 19 (256 ビットランダム ECP) 及び DH グループ 20 (384 ビットランダム ECP) が要求されることになる。追加の DH グループが何か特定される場合、それらは FCS_CKM.1 に列挙される要件 (確立される一時的鍵 (ephemeral keys) の意味で) に適合しなければならないことに注意すべきである。

FCS_IPSEC_EXT.1.12 TSF は、デフォルトで [選択：*IKEv1 フェーズ 1*、*IKEv2 IKE_SA*] 接続を保護するためにネゴシエーションされる対称鍵暗号アルゴリズムの強度 (鍵のビット数の意味で) が [選択：*IKEv1 フェーズ 2*、*IIKEv2 CHILD_SA*] 接続を保護するためにネゴシエーションされる対称鍵暗号アルゴリズムの強度 (鍵のビット数の意味で) よりも大きいか、等しいことを保証できなければならない。

適用上の注釈 72

ST 作成者は、TOE による実装に基づいて IKE 選択肢のいずれか、または両方を選択すること。もちろん、選択された IKE バージョンは、本エレメントだけでなく、本コンポーネントの他のエレメントの他の選択とも一貫しているべきである。本機能が設定可能であることは受け入れ可能であるが、評価される構成でのデフォルト構成 (「箱から出した状態」または AGD 文書における設定ガイダンスによる) では、本機能を有効化しなければならない。

FCS_IPSEC_EXT.1.13 TSF は、すべての IKE プロトコルが RFC 4945 に適合する X.509v3 証明書及び [選択：*事前共有鍵*、*その他の方法なし*] を用いる [選択：*RSA*、*ECDSA*] を用いてピア認証が実行されることを保証しなければならない。

適用上の注釈 73

本 PP に適合するため、少なくとも 1 つの公開鍵ベースのピア認証方法が必須となる；何が実装されているかを反映するため、ST 作成者によって 1 つ以上の公開鍵スキームが選択されること。ST 作成者は、使用されるアルゴリズム (及び鍵生成機能、提供される場合) を反映した適切な FCS 要件が、それらの方法のサポートのため列挙されていることについても保証すること。TSS には、これらのアルゴリズムが用いられる方法も詳述されることになる (例えば、RFC 2409 では公開鍵を用いる 3 つの認証方法が特定されている；サポートされるそれぞれが TSS において記述される) ことに注意されたい。ECDSA X.509v3 証明書を用いる

ピア認証は、2015 年の第3 四半期以降に評価に入る TOE について必須となるだろう。

FCS_IPSEC_EXT.1.14 TSF は、有効な証明書を持っているピアへの高信頼チャネルのみを確立しなければならない。

適用上の注釈 74

サポートされるピア証明書アルゴリズムは FCS_IPSEC_EXT.1.1 と同じであること。

B.2.1.3 FCS_SSHC_EXT.1 SSH クライアントプロトコル

FCS_SSHC_EXT.1	**SSH クライアントプロトコル**

FCS_SSHC_EXT.1.1 TSF は、RFC 4251、4252、4253、4254、及び [選択 : *5647*、*5656*、*6187*、*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。

適用上の注釈 75

ST 作成者は、適合主張されている追加の RFC を選択すること。これらは、本コンポーネントの後のエレメントにおける選択 (例えば、許可される暗号アルゴリズム) と一貫している必要があることに注意されたい。RFC 4253 は、特定の暗号アルゴリズムが「必須」であることを指示している。これは、そのアルゴリズムが利用のため有効化されなければならないことではなく、実装がそのサポートを含まれなければならないことを意味する。「必須」と示されているが本コンポーネントの後のエレメントに列挙されないアルゴリズムが実装されていることを保証することは、本要件の保証アクティビティの適用範囲外である。

FCS_SSHC_EXT.1.2 TSF は、SSH プロトコルの実装が RFC 4252 に記述される以下の認証方法をサポートすることを保証しなければならない：公開鍵ベースもの、パスワードベースのもの。

FCS_SSHC_EXT.1.3 TSF は、RFC 4253 に記述されるように、SSH トランスポート接続中の [割付：*バイト数*] より大きさのパケットが破棄されることを保証しなければならない。

適用上の注釈 76

RFC 4253 は、そのパケットが「合理的な長さ」でなければ破棄されるべきという警告と共に「大きなパケット」の受け入れを提供している。割付は、ST 作成者により受け入れられる最大のパケット長、すなわち TOE の「合理的な長さ」を定義しつつ、記入されるべきである。

FCS_SSHC_EXT.1.4 TSF は、SSH トランスポートの実装が以下の暗号化アルゴリズムを使用し、他のすべての暗号アルゴリズムを拒否することを保証しなければならない：*aes128-cbc*、*aes256-cbc*、 *[選択 : AEAD_AES_128_GCM*、*AEAD_AES_256_GCM*、*その他のアルゴリズムなし]*。

適用上の注釈 77

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの利用を特定している。RFC 5647 に記述されるように、AEAD_AES_128_GCM 及び AEAD_AES_256_GCM を暗号化アルゴリズムとして選ぶことができるのは、同一のアルゴリズムが MAC アルゴリズムとして用いられる場合のみである。割付で、ST 作成者は AES-GCM アルゴリズムを選択するか、あるいは AES-GCM がサポートされない場合は「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 が選択される場合、対応する FCS_COP エントリが ST に存在すべきである。

FCS_SSHC_EXT.1.5 TSF は、SSH トランスポートの実装がその公開鍵アルゴリズムとして

[選択：ssh-rsa、ecdsa-sha2-nistp256] 及び *[選択：ecdsa-sha2-nistp384、x509v3-ecdsa-sha2-nistp256、x509v3-ecdsa-sha2-nistp384、その他の公開鍵アルゴリズムなし]* を使用し、他のすべての公開鍵アルゴリズムを拒否することを保証しなければならない。

適用上の注釈 78

ssh-rsa のみを選択するような実装は、NIST SP 800-131A に推奨されるような SSH 認証のためのディジタル署名生成における 112 ビットのセキュリティ強度を達成しないことになる。本プロファイルの将来のバージョンでは、ssh-rsa は選択肢から削除されるかもしれない。x509v3-ecdsa-sha2-nistp256 または x509v3-ecdsa-sha2-nistp384 が選択される場合には、FCS_SSHC_EXT.1.9 において信頼済み認証局のリストが選択されなければならない。

FCS_SSHC_EXT.1.6 TSF は、SSH トランスポートの実装がそのデータ完全性 MAC アルゴリズムとして *[選択：hmac-sha1、hmac-sha1-96、hmac-sha2-256、hmac-sha2-512]* 及び *[選択：AEAD_AES_128_GCM、AEAD_AES_256_GCM、その他の MAC アルゴリズムなし]* を使用し、他のすべての MAC アルゴリズムを拒否することを保証しなければならない。

適用上の注釈 79

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの利用を特定している。RFC 5647 に記述されるように、AEAD_AES_128_GCM 及び AEAD_AES_256_GCM を MAC アルゴリズムとして選ぶことができるのは、同じアルゴリズムが暗号化アルゴリズムとして使用される場合のみである。RFC 6668 は、SSH における sha2 アルゴリズムの使用を特定している。

FCS_SSHC_EXT.1.7 TSF は、 *[選択：diffie-hellman-group14-sha1、ecdh-sha2-nistp256]* 及び *[選択：ecdh-sha2-nistp384、ecdh-sha2-nistp521、その他の方法なし]* のみが SSH プロトコル用に使用が許可される鍵交換方法であることを保証しなければならない。

FCS_SSHC_EXT.1.8 TSF は、2^28 を超えない数のパケットがその鍵を用いて送信された後に SSH 接続が鍵変更されることを保証しなければならない。

FCS_SSHC_EXT.1.9 TSF は、SSH クライアントが RFC 4251 のセクション 4.1 に記述されるように、各ホスト名に対応する公開鍵と対応付けるローカルなデータベースまたは [選択：*信頼済み認証局のリスト、その他の方法なし*] を用いる SSH サーバの識別情報を認証することを保証しなければならない。

適用上の注釈 80

信頼済み認証局のリストは、FCS_SSHC_EXT.1.5 において x509v3-ecdsa-sha2-nistp256 または x509v3-ecdsa-sha2-nistp384 が指定される場合にのみ選択できる。

B.2.1.4 FCS_SSHS_EXT.1 SSH サーバプロトコル

FCS_SSHS_EXT.1	**SSH サーバプロトコル**

FCS_SSHS_EXT.1.1 TSF は、RFC 4251、4252、4253、4254、及び [選択：*5647*、*5656*、*6187*、*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。

適用上の注釈 81

ST 作成者は、適合主張されている追加の RFC を選択すること。これらは、本コンポーネントの後のエレメントにおける選択 (例えば、許可される暗号アルゴリズム) と一貫している必要があることに注意されたい。RFC 4253 は、特定の暗号アルゴリズムが「必須」であることを示している。これは、そのアルゴリズムが利用のため有効化されなければならないことではなく、実装がサポートを含んでいなければならないことを意味する。「必須」と示

されているが本コンポーネントの後のエレメントに列挙されないアルゴリズムが実装されていることを保証することは、本要件の保証アクティビティの適用範囲外である。

FCS_SSHS_EXT.1.2 TSF は、SSH プロトコルの実装が RFC 4252 に記述される以下の認証方法をサポートすることを保証しなければならない：公開鍵ベースもの、パスワードベースのもの。

FCS_SSHS_EXT.1.3 TSF は、RFC 4253 に記述されるように、SSH トランスポート接続中の [割付：*バイト数*] を超える大きさのパケットが破棄されることを保証しなければならない。

適用上の注釈 82

RFC 4253 は、そのパケットが「合理的な長さ」でなければ破棄されるべきという警告と共に「大きなパケット」の受け入れを提供している。割付は、ST 作成者により受け入れられる最大のパケット長、すなわち TOE の「合理的な長さ 」を定義しつつ、記入されるべきである。

FCS_SSHS_EXT.1.4 TSF は、SSH トランスポートの実装が以下の暗号化アルゴリズムを使用し、他のすべての暗号アルゴリズムを拒否することを保証しなければならない：*aes128-cbc*、*aes256-cbc*、 *[選択：AEAD_AES_128_GCM*、*AEAD_AES_256_GCM*、*その他のアルゴリズムなし]*。

適用上の注釈 83

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの使用を特定している。RFC 5647 に記述されるように、AEAD_AES_128_GCM 及び AEAD_AES_256_GCM を暗号化アルゴリズムとして選ぶことができるのは、同じアルゴリズムが MAC アルゴリズムとして用いられる場合のみである。割付で、ST 作成者は AES-GCM アルゴリズムを選択するか、または AES-GCM がサポートされない場合は「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 が選択される場合、対応する FCS_COP エントリが ST に存在すべきである。

FCS_SSHS_EXT.1.5 TSF は、SSH トランスポートの実装がその公開鍵アルゴリズムとして *[選択：ssh-rsa 、 ecdsa-sha2-nistp256] 及び [選択：ecdsa-sha2-nistp384 、 x509v3-ecdsa-sha2-nistp256*、*x509v3-ecdsa-sha2-nistp384*、*その他の公開鍵アルゴリズムなし]* を使用し、他のすべての公開鍵アルゴリズムを拒否することを保証しなければならない。

適用上の注釈 84

ssh-rsa のみを選択するような実装は、NIST SP 800-131A に推奨されるような SSH 認証のためのディジタル署名生成における 112 ビットのセキュリティ強度を達成しないことになる。本プロファイルの将来の版では、ssh-rsa は選択肢から削除されるかもしれない。

FCS_SSHS_EXT.1.6 TSF は、SSH トランスポートの実装がその MAC アルゴリズムとして *[選択：hmac-sha1 、 hmac-sha1-96 、 hmac-sha2-256 、 hmac-sha2-512] 及び [選択：AEAD_AES_128_GCM*、*AEAD_AES_256_GCM*、*その他の MAC アルゴリズムなし]* を使用し、他のすべての MAC アルゴリズムを拒否することを保証しなければならない。

適用上の注釈 85

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの使用を特定している。RFC 5647 に記述されるように、AEAD_AES_128_GCM 及び AEAD_AES_256_GCM を MAC アルゴリズムとして選ぶことができるのは、同じアルゴリズムが暗号化アルゴリズムとして用いられる場合のみである。RFC 6668 は、SSH における sha2 アルゴリズムの使用を特定している。

FCS_SSHS_EXT.1.7 TSF は、*[選択:diffie-hellman-group14-sha1*、*ecdh-sha2-nistp256] 及び [選*

択：ecdh-sha2-nistp384、*ecdh-sha2-nistp521*、*その他の方法なし]* のみが SSH プロトコル用に使用が許可される鍵交換方法であることを保証しなければならない。

FCS_SSHS_EXT.1.8 TSF は、2^28 を超えない数のパケットがその鍵を用いて送信された後に SSH 接続が鍵変更されることを保証しなければならない。

B.2.1.5 FCS_TLSC_EXT.1 TLS クライアントプロトコル

TLS は、本 cPP の必須のコンポーネントではない。TOE が TLS を実装する場合、何を保護するために TLS プロトコルが実装されるかを定義するために FTP_ITC.1、または FTP_TRP.1 の対応する選択が行われるべきである。

TOE は、TLS セションにおいて、クライアント、サーバ、またはその両方として動作することがある。要件は、これらの違いを考慮して TLS クライアント (FCS_TLSC_EXT) と TLS サーバ (FCS_TLSS_EXT) 要件に分離されている。主張された TLS セションで TOE がクライアントとして動作する場合、ST 作成者は FCS_TLSC_EXT 要件を主張すべきである。

さらに、TLS は、クライアント認証が行われるかもしれないし、行われないかもしれない。ST 作成者は、TOE がクライアント認証をサポートしない場合、FCS_TLSC_EXT.1 及び FCS_TLSS_EXT.1 を主張しなければならない。ST 作成者は、TOE によりクライアント認証が行われる場合、FCS_TLSC_EXT.2 及び FCS_TLSS_EXT.2 を主張するべきである。FTP_ITC.1 における外部 IT エンティティとの高信頼通信チャネルを提供する手段として TLS が選択される場合には、FCS_TLSC_EXT.2 が要求される。

FCS_TLSC_EXT.1	**TLS クライアントプロトコル**

FCS_TLSC_EXT.1.1 TSF は、以下の暗号スイートをサポートする [選択 : *TLS 1.2 (RFC 5246)*、*TLS 1.1 (RFC 4346)*] を実装しなければならない :

- *必須の暗号スイート：*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA*
- *[選択：オプションの暗号スイート：*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
  - *その他の暗号スイートなし]*。

適用上の注釈 86

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。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べきである；必須スイート以外にサポートされる暗号スイートが存在しない場合には、「なし」が選択されるべきである。テスト環境におけるサーバ上で評価される構成で管理的に使用されることが可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっている。

これらの要件は、新たな TLS バージョンが IETF により標準化されるので、見直しが予定されている。

本 cPP の将来のバージョンにおいて、すべての TOE に対して TLS v1.2 が必須となる。

FCS_TLSC_EXT.1.2 TSF は、提示された識別子が参照識別子と一致することを RFC 6125 に従って検証しなければならない。

適用上の注釈 87

識別子の検証のための規則は、RFC 6125 のセクション 6 に記述されている。参照識別子は、利用者により (例、ウェブブラウザへの URL 入力またはリンクのクリック等)、設定により (例、メールサーバまたは認証サーバの名前の設定等)、またはアプリケーションにより (例、API のパラメタ等)、アプリケーションサービスに応じて確立される。単一の参照識別子の生成元ドメイン及びアプリケーションサービス種別 (例、HTTP、SIP、LDAP 等) に基づき、クライアントは受け入れ可能なすべての参照識別子、例えば証明書のサブジェクト名フィールドのコモン名、及びサブジェクト別名フィールドの (大文字と小文字を区別しない) DNS 名、URI 名、及びサービス名等を確立する。クライアントは、その時、このすべての受け入れ可能な参照識別子のリストを、TLS サーバの証明書において提示された識別子と比較する。

望ましい検証方法は、DNS 名、URI 名、またはサービス名を用いたサブジェクト別名である。コモン名を用いる検証は、上位互換性 (backward compatibility) の目的で要求される。さらに、サブジェクト名またはサブジェクト別名中の IP アドレスの使用のサポートは、ベストプラクティスに反するため推奨されないが、実装されてもよい。最後に、クライアントは、ワイルドカードを用いた参照識別子の構築を避けるべきである。しかし、提示された識別子がワイルドカードを含む場合には、クライアントは一致に関するベストプラクティスに従わなければならない；これらのベストプラクティスは、保証アクティビティに取り込まれている。

FCS_TLSC_EXT.1.3 TSF は、ピア証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない。

適用上の注釈 88

有効性は、識別子の検証、証明書パス、有効期限、及び失効状態により、RFC 5280 に従って決定されること。証明書の有効性は、FIA_X509_EXT.1 用に実行されるテストに従いテストされること。

FCS_TLSC_EXT.1.4 TSF は、Client Hello における Supported Elliptic Curves Extension に以下の NIST 曲線を提示しなければならない： *[選択：secp256r1、secp384r1、secp521r1、またはなし]* 及びその他の曲線なし。

適用上の注釈 89

楕円曲線を伴う暗号スイートが FCS_TLSC_EXT.1.1 において選択された場合、1 つ以上の曲線の選択が必須となる。楕円曲線を伴う暗号スイートが FCS_TLS_EXT.1.1 において選択さ

れない場合、「なし」が選択されるべきである。

本要件は、認証及び鍵共有のために許可される楕円曲線を、FCS_COP.1(2) 及びFCS_CKM.1 ならびに FCS_CKM.2 からの NIST 曲線に制限している。本拡張は、楕円曲線暗号スイートをサポートするクライアントについては必須となる。

B.2.1.6 FCS_TLSC_EXT.2 認証を伴う TLS クライアントプロトコル

(セクション B.2.1.5 の序文を参照のこと)

FCS_TLSC_EXT.2	認証を伴う TLS クライアントプロトコル

FCS_TLSC_EXT.2.1 TSF は、以下の暗号スイートをサポートする [選択 : *TLS 1.2 (RFC 5246)*、*TLS 1.1 (RFC 4346)*] を実装しなければならない :

- *必須の暗号スイート :*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA*
- *[選択 : オプションの暗号スイート :*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
  - *その他の暗号スイートなし]。*

適用上の注釈 90

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。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存在しない場合には、「なし」が選択されるべきである。テスト環境におけるサーバ上で評価される構成で管理者に使用されることが可能な暗号スイートを制限する必要がある。上記 Suite B アルゴリズム (RFC 6460) は、実装が望まれるアルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっている。

これらの要件は、新たな TLS バージョンが IETF により標準化されるので、見直しが予定されている。

本 cPP の将来の版では、すべての TOE について TLS v1.2 が要求されることになる。

FCS_TLSC_EXT.2.2 TSF は、提示された識別子が参照識別子と一致することを RFC 6125 に従って検証しなければならない。

適用上の注釈 91

識別子の検証のための規則は、RFC 6125 のセクション 6 に記述されている。参照識別子は利用者により (例、ウェブブラウザへの URL 入力またはリンクのクリック等)、設定により (例、メールサーバまたは認証サーバの名前の設定等)、またはアプリケーションにより (例、API のパラメタ等)、アプリケーションサービスに応じて確立される。単一の参照識別子の生成元ドメイン及びアプリケーションサービス種別 (例、HTTP、SIP、LDAP 等) に基づき、クライアントは受け入れ可能なすべての参照識別子、例えば証明書のサブジェクト名フィールドのコモン名、及びサブジェクト別名フィールドの (大文字と小文字を区別しない) DNS 名、URI 名、及びサービス名等を確立する。クライアントは、その時、このすべての受け入れ可能な参照識別子のリストを、TLS サーバの証明書において提示された識別子と比較する。

望ましい検証方法は、DNS 名、URI 名、またはサービス名を用いたサブジェクト別名である。コモン名を用いる検証は、上位互換性 (backward compatibility) の目的で要求される。さらに、サブジェクト名またはサブジェクト別名中の IP アドレスの使用のサポートは、ベストプラクティスに反するため推奨されないが、実装されてもよい。最後に、クライアントは、ワイルドカードを用いた参照識別子の構築を避けるべきである。しかし、提示された識別子がワイルドカードを含む場合には、クライアントは一致に関するベストプラクティスに従わなければならない；これらのベストプラクティスは、保証アクティビティに取り込まれている。

FCS_TLSC_EXT.2.3 TSF は、ピア証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない。

適用上の注釈 92

有効性は、識別子の検証、証明書パス、有効期限、及び失効状態により、RFC 5280 に従って決定されること。証明書の有効性は、FIA_X509_EXT.1 用に実行されるテストに従いテストされなければならない。

FCS_TLSC_EXT.2.4 TSF は、Client Hello における Supported Elliptic Curves Extension において、以下の NIST 曲線を提示しなければならない: *[選択：secp256r1、secp384r1、secp521r1、またはなし]* 及びその他の曲線なし。

適用上の注釈 93

楕円曲線を伴う暗号スイートが FCS_TLSC_EXT.2.1 において選択された場合、1 つ以上の曲線の選択が必須となる。楕円曲線を伴う暗号スイートが FCS_TLS_EXT.2.1 において全く選択されなかった場合、「なし」が選択されるべきである。

本要件は、認証及び鍵共有のために許可される楕円曲線を、FCS_COP.1(2) 及び FCS_CKM.1 ならびに FCS_CKM.2 からの NIST 曲線に制限している。本拡張は、楕円曲線暗号スイートをサポートするクライアントについては必須となる。

FCS_TLSC_EXT.2.5 TSF は、X.509v3 証明書を用いる相互認証をサポートしなければならない。

適用上の注釈 94

TLS 用の X.509v3 証明書の使用は、FIA_X509_EXT.2.1 において対処される。本要件は、クライアントが TLS 相互認証を行うために TLS サーバへ証明書を提示できなければならないことを追加している。

B.2.1.7 FCS_TLSS_EXT.1 TLS サーバプロトコル

B.2.1.5 で述べたように、TOE は TLS セションにおいて、クライアント、サーバ、またはその両方として動作し得る。TOE が主張される TLS セションにおいてサーバとして動作する場合 (FTP_ITC.1、または FTP_TRP.1)、ST 作成者は FCS_TLSS_EXT 要件を主張すべきである。

TLS は、相互認証が行われるかもしれないし、行われないかもしれない。ST 作成者は、TOE が相互認証をサポートしない場合、FCS_TLSS_EXT.1 を主張しなければならない。ST 作成者は、相互認証が TOE によりサポートされる場合、FCS_TLSS_EXT.2 を主張すべきである。

FCS_TLSS_EXT.1	**TLS サーバプロトコル**

FCS_TLSS_EXT.1.1 TSF は、以下の暗号スイートをサポートする [選択:*TLS 1.2 (RFC 5246)*、*TLS 1.1 (RFC 4346)*] を実装しなければならない:

- *必須の暗号スイート:*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA*
- *[選択:オプションの暗号スイート:*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
  - *その他の暗号スイートなし]。*

適用上の注釈 95

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。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べきである;必須スイート以外にサポートされる暗号スイートが存在しない場合には、「なし」が選択されるべきである。テスト環境におけるサーバ上で評価される構成で管理者に使用されることが可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっている。

これらの要件は、新たな TLS バージョンが IETF により標準化されるので、見直しが予定されている。

本 cPP の将来のバージョンにおいて、すべての TOE に対して TLS v1.2 が必須となる。

FCS_TLSS_EXT.1.2 TSF は、SSL 1.0、SSL 2.0、SSL 3.0、TLS 1.0、及び [選択:*TLS 1.1*、*TLS*

1.2、なし] を要求するクライアントからの接続を拒否しなければならない。

適用上の注釈 96

すべてのバージョンの SSL、及び TLS v1.0 は拒否されること。FCS_TLSS_EXT.1.1 において選択されなかったあらゆる TLS のバージョンが、ここで選択されるべきである。

FCS_TLSS_EXT.1.3 TSF は、鍵長 2048 ビット及び [選択：*3072 ビット、4096 ビット、その他の鍵長なし*] の RSA、及び [選択：*NIST 曲線 [選択：secp256r1, secp384r1] 及びその他の曲線なし；鍵長 2048 ビット及び [選択:3072 ビット、その他のサイズなし] の Diffie-Hellman パラメタ； その他なし*] を用いて、鍵確立パラメタを生成しなければならない。

適用上の注釈 97

ST にて、FCS_TLSS_EXT.1.1 における DHE または ECDHE 暗号スイートが列挙される場合、ST は、本要件における Diffie-Hellman または NIST 曲線の選択を含まなければならない。FMT_SMF.1 は、TLS 接続のセキュリティ強度を確立するために、鍵共有パラメタの設定を要求する。

B.2.1.8 FCS_TLSS_EXT.2 相互認証を伴う TLS サーバプロトコル

(セクション B.2.1.7 の序文を参照のこと。)

FCS_TLSS_EXT.2	**相互認証を伴う TLS サーバプロトコル**

FCS_TLSS_EXT.2.1 TSF は、以下の暗号スイートをサポートする [選択：*TLS 1.2 (RFC 5246)、TLS 1.1 (RFC 4346)*] を実装しなければならない：

- *必須の暗号スイート：*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA*
- *[選択：オプションの暗号スイート：*
  - *RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA*
  - *RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
  - *RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*
  - *その他の暗号スイートなし]。*

適用上の注釈 98

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。

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存在しない場合には、「なし」が選択されるべきである。テスト環境におけるサーバ上で評価される構成で管理者に使用されることが可能な暗号スイートを制限する必要がある。上記 Suite B アルゴリズム (RFC 6460) は、実装が望まれるアルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっている。

これらの要件は、新たな TLS バージョンが IETF により標準化されるので、見直しが予定されている。

本 cPP の将来のバージョンにおいて、すべての TOE について TLS v1.2 が必須となる。

FCS_TLSS_EXT.2.2 TSF は、SSL 1.0、SSL 2.0、SSL 3.0、TLS 1.0、及び [選択：*TLS 1.1*、*TLS 1.2*、*なし*] を要求するクライアントからの接続を拒否しなければならない。

適用上の注釈 99

すべてのバージョンの SSL、及び TLS v1.0 は拒否されなければならない。FCS_TLSS_EXT.2.1 において選択されなかったあらゆる TLS のバージョンが、ここで選択されるべきである。

FCS_TLSS_EXT.2.3 TSF は、鍵長 2048 ビット及び [*選択：3072 ビット、4096 ビット、その他の鍵長なし*] の RSA、及び [*選択：NIST 曲線 [選択：secp256r1, secp384r1] 及びその他の曲線なし；鍵長 2048 ビット及び [選択:3072 ビット、その他のサイズなし] の Diffie-Hellman パラメタ； その他なし*]を用いて、鍵確立パラメタを生成しなければならない。

適用上の注釈 100

ST にて、FCS_TLSS_EXT.2.1 における DHE または ECDHE 暗号スイートが列挙される場合、ST は、本要件における Diffie-Hellman または NIST 曲線の選択が含まれなければならない。FMT_SMF.1 は、TLS 接続のセキュリティ強度を確立するために、鍵共有パラメタの設定を要求する。

FCS_TLSS_EXT.2.4 TSF は、X.509v3 証明書を用いて、TLS クライアントの相互認証をサポートしなければならない。

FCS_TLSS_EXT.2.5 TSF は、ピア証明書が無効である場合。高信頼チャネルを確立してはならない。

適用上の注釈 101

TLS のための X.509v3 証明書の使用は、FIA_X509_EXT.2.1 において対処される。本要件は、本用途が TLS 相互認証用のクライアント側証明書のサポートを含まなければならないことを追加している。

有効性は、証明書パス、有効期限、及び失効状態により、RFC 5280 に従って決定される。証明書の有効性は、FIA_X509_EXT.1 用に実行されるテストに従って、テストされなければならない。

FCS_TLSS_EXT.2.6 TSF は、証明書に含まれる識別名 (DN) またはサブジェクト別名 (SAN) がピアに期待される識別子に一致しない場合、高信頼チャネルを確立してはならない。

適用上の注釈 102

ピア識別子は、証明書のサブジェクト名フィールドまたはサブジェクト別名拡張に存在し得る。期待される識別子は、設定されてもよいし、ピアによって用いられるドメイン名、IP

アドレス、利用者名、または電子メールアドレスと比較されたり、あるいは比較のためディレクトリサーバへ渡されたりしてもよい。一致するかどうかの検証は、ビットごとの比較により実行されるべきである。

B.3 TSF の保護 (FPT)

B.3.1 TSF 自己テスト (拡張)

B.3.1.1 FPT_TST_EXT.2 証明書ベースの自己テスト

FPT_TST_EXT.2	証明書ベースの自己テスト

FPT_TST_EXT.2.1 TSF は、自己テストに証明書が用いられ、かつ対応する証明書が無効とみなされる場合、自己テストを失敗させなければならない。

適用上の注釈 103

証明書は、オプションとして自己テストに用いることができる (FPT_TST_EXT.1.1)。証明書が自己テストに用いられる場合、本エレメントが ST に含まれなければならない。FIA_X509_EXT.2.1 において「完全性検証のためのコード署名」が選択される場合、FPT_TST_EXT.2 が ST へ含まれなければならない。

有効性は、証明書パス、有効期限、及び失効状態により、FIA_X509_EXT.1 に従って決定される。

B.3.2 高信頼アップデート (FPT_TUD_EXT)

B.3.2.1 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート

FPT_TUD_EXT.2	証明書ベースの高信頼アップデート

FPT_TUD_EXT.2.1 TSF は、コード署名証明書が無効とみなされる場合にはアップデートをインストールしてはならない。

FPT_TUD_EXT.2.2 証明書の有効期限が過ぎたために証明書が無効とみなされる際、TSF は、 [選択：*このような場合には証明書を受け入れるかどうかの選択を管理者に許可する、証明書を受け入れる、証明書を受け入れない*] ようにしなければならない。

適用上の注釈 104

証明書は、オプションとして、システムソフトウェアアップデートのコード署名用に使用してもよい (FPT_TUD_EXT.1.3)。証明書がアップデートの検証用に使用される場合、本エレメントが ST に含まれなければならない。FIA_X509_EXT.2.1 において「システムソフトウェアアップデートのコード署名」が選択される場合、FPT_TUD_EXT.2 が ST に含まれなければならない。X.509 証明書の使用は、高信頼アップデートに公開ハッシュのみがサポートされる場合には適用されない。

有効性は、証明書パス、有効期限、及び失効状態により、FIA_X509_EXT.1 に従って決定される。有効期限の過ぎた証明書について、ST 作成者は、その証明書が受け入れられなければならないか、拒否されなければならないか、またはその証明書を受け入れるか拒否するかの選択を管理者に委ねるかを、選択すること。

B.4 セキュリティ管理 (FMT)

B.4.1 TSF 内の機能の管理 (FMT_MOF)

B.4.1.1 FMT_MOF.1(2)/TrustedUpdate セキュリティ機能のふるまいの管理

FMT_MOF.1(2)/TrustedUpdate　セキュリティ機能のふるまいの管理

FMT_MOF.1.1(2)/TrustedUpdate TSF は、機能 [*選択：アップデートの自動的なチェック、自動アップデート*] を 有効化、無効化 する能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 105

FMT_MOF.1(2)/TrustedUpdate は、TOE が自動アップデートをサポートし、その有効化及び無効化を許す場合にのみ適用される。自動アップデートの有効化及び無効化は、セキュリティ管理者に制限される。

C. 拡張コンポーネントの定義

本附属書には、附属書 A 及び B で用いられるものを含め、本 cPP で用いられる拡張要件の定義が含まれる。

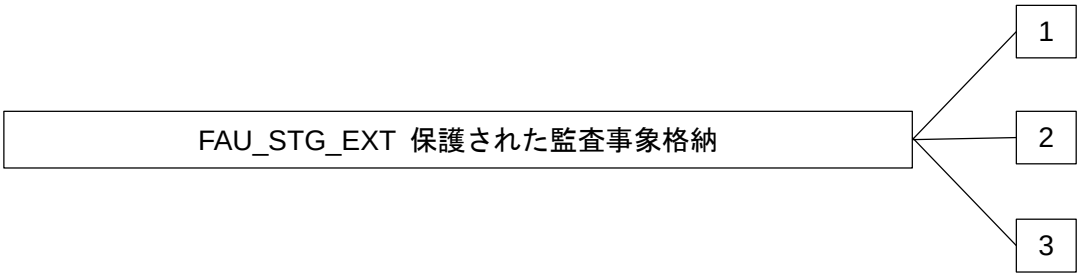
C.1 セキュリティ監査 (FAU)

C.1.1 保護された監査事象格納 (FAU_STG_EXT)

ファミリのふるまい

本コンポーネントは、TSF が TOE と外部 IT エンティティとの間で監査データをセキュアに送信できるための要件を定義する。

コンポーネントのレベル付け



FAU_STG_EXT.1 保護された監査事象格納は、セキュアなプロトコルを実装し高信頼チャネルを用いることを TSF に要求する。

FAU_STG_EXT.2 失われた監査データのカウントは、監査ログが満杯になった際に影響を受ける監査記録に関する情報を提供することを TSF に要求する。

FAU_STG_EXT.3 ローカルな格納領域に関する警告の表示は、監査ログが満杯になる前に警告を生成することを TSF に要求する。

管理：FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3

以下のアクションは、FMT における管理機能と考えられる：

a) TSF は、暗号機能を設定する能力を持たなければならない。

監査：FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 監査の必要なし。

C.1.1.1 FAU_ STG_EXT.1 保護された監査事象格納

FAU_STG_EXT.1	保護された監査事象格納

下位階層： なし

依存性： FAU_GEN.1 監査データの生成
FTP_ITC.1 TSF 間高信頼チャネル

FAU_STG_EXT.1.1 TSF は、FTP_ITC に従った高信頼チャネルを用いて外部 IT エンティティへ、生成された監査データを送信できなければならない。

適用上の注釈 106

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オプションの選択について、TOE は監査記録の格納とレビューに関して非 TOE 監査サーバに依存している。これらの監査記録の格納、及びこれらの監査記録のレビューを管理者に許可する能力は、その場合の運用環境により提供される。

FAU_STG_EXT.1.2 TSF は、生成された監査データを TOE それ自体に格納できなければならない。

FAU_STG_EXT.1.3 TSF は、監査データのローカルな格納用領域が満杯の場合、 [選択：*新たな監査データを破棄*、*以下の規則に従って以前の監査記録を上書き：[割付：以前の監査記録を上書きする規則]*、 *[割付：その他のアクション]*] しなければならない。

適用上の注釈 107

ローカルな格納用領域が満杯の場合、外部ログサーバが代替的な格納用領域として使用されるかもしれない。この場合、「その他のアクション」は「外部 IT エンティティへ新たな監査データを送信する」と定義できるであろう。

C.1.1.2 FAU_ STG_EXT.2 失われた監査データのカウント

FAU_STG_EXT.2	失われた監査データのカウント

下位階層： なし

依存性： FAU_GEN.1 監査データの生成
FAU_STG_EXT.1 外部監査証跡格納

FAU_STG_EXT.2.1 TSF は、ローカルな格納領域が満杯となり TSF が FAU_STG_EXT.1.3 に定義されるアクションの 1 つを取った場合、 [選択：*破棄された*、*上書きされた*、*割付：その他の情報*] 監査記録の数についての情報を提供しなければならない。

適用上の注釈 108

このオプションは、TOE が本機能をサポートする場合に選択されるべきである。

監査記録のローカルな格納領域が管理者によって消去される場合、SFR の選択に関連するカウンタはその初期値 (おそらくは 0) にリセットされるべきである。ガイダンス文書には、管理者が監査記録のローカルな格納領域を消去する際の監査データの喪失に関する管理者への警告が含まれるべきである。

C.1.1.3 FAU_ STG_EXT.3 ローカルな格納領域に関する警告の表示

FAU_STG_EXT.3	ローカルな格納領域に関する警告の表示

FAU_STG_EXT.3.1 TSF は、監査データを格納するためのローカルな格納領域が使い尽くされたり、ローカルな格納領域が不十分なため TOE が監査データを喪失する前に、警告を生成して利用者へ通知しなければならない。

適用上の注釈 109

このオプションは、監査データのローカルの格納領域が使い尽くされる前に TOE が警告を生成して利用者へ通知する場合に選択されるべきである。これは、監査対象事象がローカルの格納領域のみに格納される場合に役立つかもしれない。

FAU_STG_EXT.1.3 により要求される警告メッセージが利用者へ通知可能であることは保証される必要がある。事象発生時に管理者セションがアクティブであることは保証できないため、この通知は監査ログそのものによって行われるべきである。

C.2 暗号サポート (FCS)

C.2.1 ランダムビット生成 (FCS_RBG_EXT)

C.2.1.1 FCS_RBG_EXT.1 ランダムビット生成

ファミリのふるまい

本ファミリのコンポーネントは、ランダムビット／乱数生成の要件に対応する。これは、FCS クラスに定義される新たなファミリである。

コンポーネントのレベル付け

FCS_RBG_EXT ランダムビット生成	1

FCS_RBG_EXT.1 ランダムビット生成は、ランダムビット生成が選択された標準に従い、エントロピー源によってシードを供給されて行われることを要求する。

管理：FCS_RBG_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない

監査：FCS_RBG_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 最小：ランダム化プロセスの失敗

FCS_RBG_EXT.1	**ランダムビット生成**

下位階層： なし

依存性： なし

FCS_RBG_EXT.1.1 TSF は、ISO/IEC 18031:2011 に従って、[*選択：Hash_DRBG (任意)* 、*HMAC_DRBG (任意)* 、*CTR_DRBG (AES)*] を用いて、すべての決定論的ランダムビット生成サービスを実行しなければならない。

FCS_RBG_EXT.1.2 決定論的 RBG は、[選択： *[割付：ソフトウェアベースのノイズ源の数] 個のソフトウェアベースのノイズ源*、 *[割付：ハードウェアベースのノイズ源の数] 個のハードウェアベースのノイズ源*] からのエントロピーを、ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”に従い、生成される鍵とハッシュの最大セキュリティ強度と少なくとも等しいだけの、[選択：*128 ビット*、*192 ビット*、*256 ビット*] の最小エントロピーを有するように蓄積する、少なくとも 1 つのエントロピー源によってシードが供給されなければならない。

適用上の注釈 110

FCS_RBG_EXT.1.2 の最初の選択については、ST は少なくとも 1 つのノイズ源の種別を選択すること。TOE に同一種別のノイズ源が複数含まれる場合、ST 作成者はノイズ源のそれぞれの種別について割付に適切な数字を当てはめる (例えば、2 個のソフトウェアベースのノイズ源、1 個のハードウェアベースのノイズ源)。本エレメントについて評価アクティビティに要求される文書化及びテストは、必然的に ST で示された各ノイズ源を網羅すること。

ISO/IEC 18031:2011 には、3 つの異なる乱数生成方法が含まれている。これらはそれぞれ、基盤となる暗号プリミティブ (ハッシュ関数／暗号) に依存している。 ST 作成者は使用される関数を選択し、要件に用いられる具体的な基盤となる暗号プリミティブを含めること。特定されたハッシュ関数 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) はいずれも Hash_DRBG または HMAC_DRBG 用として許可されるが、CTR_DRBG には AES ベースの実装のみが許可される。

C.2.2 暗号プロトコル (拡張—FCS_HTTPS_EXT, FCS_ IPSEC_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

C.2.2.1 FCS_HTTPS_EXT.1 HTTPS プロトコル

ファミリのふるまい

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と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、どのように HTTPS が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たなファミリである。

コンポーネントのレベル付け

FCS_HTTPS_EXT HTTPS プロトコル	1

FCS_HTTPS_EXT.1 HTTPS は、RFC 2818 に従って HTTPS が実装され、TLS をサポートすることを要求する。

管理：FCS_HTTPS_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_HTTPS_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 予見される監査対象事象はない。

FCS_HTTPS_EXT.1	**HTTPS プロトコル**

下位階層： なし

依存性： FCS_TLS_EXT.1 TLS プロトコル

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。

FCS_HTTPS_EXT.1.2 TSF は、TLS を用いた HTTPS プロトコルを実装しなければならない。

FCS_HTTPS_EXT.1.3 TSF は、ピア証明書が無効とみなされる場合、 [選択：*接続を確立しない*、*接続を確立するための許可を要求する*、 *[割付：その他のアクション]*] を実行しなければならない。

C.2.2.2 FCS_IPSEC_EXT.1 IPsec プロトコル

ファミリのふるまい

本ファミリのコンポーネントは、IPsec を用いて通信を保護するための要件に対応する。

コンポーネントのレベル付け

FCS_IPSEC_EXT IPsec プロトコル	1

FCS_IPSEC_EXT.1 IPsec は、特定されたとおりに IPsec が実装されることを要求する。

管理：FCS_IPSEC_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) SA ライフタイムの設定

監査：FCS_IPSEC_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) TOE によって処理されるネットワークパケットを廃棄 (DISCARD)、バイパス (BYPASS)、保護 (PROTECT) するための決定

b) IPsec SA の確立失敗

c) IPsec SA の確立

d) IPsec SA の終了

e) IKEv2 から IKEv1 交換への「ダウン」ネゴシエーション

FCS_IPSEC_EXT.1	**インターネットプロトコルセキュリティ (IPsec) 通信**

下位階層： なし

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)
FCS_COP.1(2) 暗号操作 (署名の検証)
FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)
FCS_RBG_EXT.1 ランダムビット生成

FCS_IPSEC_EXT.1.1 TSF は、RFC 4301 で特定される IPsec アーキテクチャを実装しなければならない。

適用上の注釈 111

RFC 4301 は、セキュリティポリシーデータベース (SPD) を用いて IP トラフィックを保護する IPsec の実装を要求する。SPD は、IP パケットがどのように取り扱われるべきかを定義するために用いられる：パケットを保護 (PROTECT) する (例えば、パケットを暗号化する)、IPsec サービスをバイパス (BYPASS) する (例えば、暗号化なし)、またはパケットを廃棄 (DISCARD) する (例えば、パケットを破棄 (drop) する)。SPD は、ルータのアクセス制御リスト、ファイアウォールの規則セット、「伝統的」な SPD 等、さまざまな方法で実装できる。実装の詳細にかかわらず、パケットが「規則」に「一致」して、その結果アクションが実行されるという「規則」がある。

規則を順序付ける手段はなければならないが、SPD が IP パケットを区別でき、それぞれに規則を適用できる限り、順序付けの一般的アプローチは必須ではない。複数の SPD があってもよい (各ネットワークインタフェースに 1 つ) が、これは必須ではない。

FCS_IPSEC_EXT.1.2 TSF は、SPD のいずれかに一致する名目的な最終エントリ、さもなければ一致せず廃棄されるようなエントリを持たなければならない。

FCS_IPSEC_EXT.1.3 TSF は、トランスポートモード及び [選択：*トンネルモード、その他のモードなし*] を実装しなければならない。

FCS_IPSEC_EXT.1.4 TSF は、暗号アルゴリズム AES-CBC-128、AES-CBC-256 (両者とも RFC 3602 によって特定される) 及び [選択：*AES-GCM-128 (RFC 4106 で特定される)*、*AES-GCM-256 (RFC 4106 で特定される)*、*その他のアルゴリズムなし*] とセキュアハッシュアルゴリズム (SHA) ベースの HMAC と共に、RFC 4303 によって定義される IPsec プロトコル ESP を実装しなければならない。

FCS_IPSEC_EXT.1.5 TSF は、以下のプロトコルを実装しなければならない：[選択：

- *IKEv1 として、RFC 2407、2408、2409、RFC 4109、[選択：拡張シーケンス番号についてその他の RFC なし、拡張シーケンス番号について RFC 4304]、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] に定義される、フェーズ 1 交換にメインモードを用いたもの；*
- *IKEv2 として、RFC 5996 [選択：NAT トラバーサルのサポートなし、RFC 5996 のセクション 2.23 に特定される NAT トラバーサルのサポートが必須)]、及び [選択：ハッシュ関数についてその他の RFC なし、ハッシュ関数について RFC 4868] に定義されたもの*]。

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、暗号アルゴリズムとして RFC 3602 に特定される AES-CBC-128、AES-CBC-256 及び [選択：*RFC 5282 に特定される AES-GCM-128*、*AES-GCM-256*、*その他のアルゴリズム*

なし] を使用することを保証しなければならない。

適用上の注釈 112

AES-GCM-128 及び AES-GCM-256 は、IKEv2 も選択されている場合にのみ選択され得る。IKEv1 には AES-GCM を定義する RFC が存在しないためである。

FCS_IPSEC_EXT.1.7 TSF は、以下を保証しなければならない [選択：

- *IKEv1 フェーズ 1 の SA ライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること [選択：*
  - *バイト数；*
  - *ライフタイムの長さ、ここで時間の値は [割付：24 を含む整数範囲] 時間以内で設定可能；*

  ]；
- *IKEv2 の SA ライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること [選択：*
  - *バイト数；*
  - *ライフタイムの長さ、ここで時間の値は [割付：24 を含む整数範囲] 時間以内で設定可能*

  ]

]。

適用上の注釈 113

ST 作成者は、IKEv1 要件または IKEv2 要件のいずれかを (または、FCS_IPSEC_EXT.1.5 の選択によっては両方を) 選択すること。ST 作成者は、数量ベースのライフタイムまたは時間ベースのライフタイムのいずれか (または、その組み合わせ) を選択すること。本要件は、セキュリティ管理者によって設定可能なライフタイムを提供することにより達成されなければならない (AGD_OPE によって義務付けられる文書中に適切な指示を用いて)。ハードコードされた制限は、本要件を満たさない。一般的には、実装のパラメタを設定するための指示が、SA のライフタイムを含めて、AGD_OPE のために作成されたガイダンス文書に含まれているべきである。

FCS_IPSEC_EXT.1.8 TSF は、以下を保証しなければならない [選択：

- *IKEv1 フェーズ 2 の SA ライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること [選択：*
  - *バイト数；*
  - *ライフタイムの長さ、ここで時間の値は [割付：8 を含む整数範囲] 時間以内で設定可能；*

  ]；
- *IKEv2 Child SA のライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること [選択：*
  - *バイト数；*
  - *ライフタイムの長さ、ここで時間の値は [割付：8 を含む整数範囲] 時間以内で設定可能；*

]

]。

適用上の注釈 114

ST 作成者は、IKEv1 要件または IKEv2 要件のいずれかを (または、FCS_IPSEC_EXT.1.5 の選択によっては両方を) 選択する。ST 作成者は、数量ベースのライフタイムまたは時間ベースのライフタイムのいずれか (または、その組み合わせ) を選択すること要件は、セキュリティ管理者によって設定可能なライフタイムを提供することにより達成されなければならない (AGD_OPE によって義務付けられる文書中に適切な指示を用いて)。ハードコードされた制限は、本要件を満たさない。一般的には、実装のパラメタを設定するための指示が、SA のライフタイムを含めて、AGD_OPE のために作成されたガイダンス文書に含まれているべきである。

FCS_IPSEC_EXT.1.9 TSF は、FCS_RBG_EXT.1 で特定されたランダムビット生成器を用いて、少なくとも [割付：*ネゴシエーションされた Diffie-Hellman グループのセキュリティ強度の少なくとも 2 倍のビット数 (1 つまたは複数)*] のビット長を有するような、IKE Diffie-Hellman 鍵交換に用いられる秘密の値 x (g^x mod p における「x」) を生成しなければならない。

適用上の注釈 115

DH グループ 19 及び 20 については、「x」の値は生成元の点 G に対する乗数である。

実装によって、異なる Diffie-Hellman グループを SA の形成に用いるようなネゴシエーションが許されるかもしれないため、FCS_IPSEC_EXT.1.9 での割付は複数の値を含めてもよい。サポートされる各 DH グループについて、ST 作成者は、その DH グループに関連付けられるセキュリティ強度 (「セキュリティビット数」) を決定するため、NIST SP 800-57 "Recommendation for Key Management –Part 1: General" の表 2 を参照すること。それぞれの一意な値がその時、本エレメントの割付に記入するために使用される。例えば、DH グループ 14 (2048 ビット MODP) とグループ 20 (NIST 曲線 P-384 を用いた ECDH) をサポートする実装を想定してみよう。表 2 から、グループ 14 のセキュリティビット数は 112 であり、グループ 20 については 192 である。

FCS_IPSEC_EXT.1.10 TSF は、 [選択：*IKEv1*、*IKEv2*] 交換に使用される、以下の長さのノンスを生成しなければならない[選択：

- *[割付:ネゴシエーションされた Diffie-Hellman グループと関連付けられたセキュリティ強度]；*
- *少なくとも 128 ビットで、 ネゴシエーションされた疑似乱数関数 (PRF) ハッシュの出力サイズの少なくとも半分の長さ*

]。

適用上の注釈 116

ST 作成者は、IKEv2 もまた選択されている場合、ノンス長について 2 番目の選択肢を選択しなければならない (RFC 5996 でこれが義務付けられているため)。ST 作成者は、IKEv1 についてはどちらの選択肢を選択してもよい。

ノンス長の最初の選択肢については、実装によって異なる Diffie-Hellman グループを SA の形成に用いるようなネゴシエーションが許されるかもしれないため、FCS_IPSEC_EXT.1.10 の割付は複数の値を含むかもしれない。サポートされる各 DH グループについて、ST 作成者は、その DH グループに関連付けられるセキュリティ強度 (「セキュリティビット数」) を決定するため、NIST SP 800-57 "Recommendation for Key Management –Part 1: General" の表 2

を参照すること。それぞれの一意な値その時、本エレメントの割付に記入するために使用される。例えば、DH グループ 14 (2048 ビット MODP) とグループ 20 (NIST 曲線 P-384 を用いた ECDH) をサポートする実装を想定してみよう。表 2 から、グループ 14 のセキュリティビット数は 112 であり、グループ 20 については 192 である。

DH グループがネゴシエーションされる前にノンスが交換されるかもしれないため、使用されるノンスは鍵交換におけるすべての TOE が選択した提案をサポートするのに十分大きなものであるべきである。

FCS_IPSEC_EXT.1.11 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：*19 (256 ビットランダム ECP)*、*5 (1536 ビット MODP)*、*24 (2048 ビット MODP と 256 ビット POS)*、*20 (384 ビットランダム ECP)*、*[割付：TOE の実装するその他の DH グループ]*、*その他の DH グループなし*] が実装されることを保証しなければならない。

FCS_IPSEC_EXT.1.12 TSF は、デフォルトで [選択：*IKEv1 フェーズ 1*、*IKEv2 IKE_SA*] 接続を保護するためにネゴシエーションされる対称鍵暗号アルゴリズムの強度 (鍵のビット数の意味で) が [選択：*IKEv1 フェーズ 2*、*IIKEv2 CHILD_SA*] 接続を保護するためにネゴシエーションされる対称鍵暗号アルゴリズムの強度 (鍵のビット数の意味で) よりも大きいか、等しいことを保証できなければならない。

適用上の注釈 117

ST 作成者は、TOE による実装に基づいて IKE 選択肢のいずれか、あるいは両方を選択すること。本機能が構成可能であることは受け入れ可能であるが、評価される構成でのデフォルト構成 (「箱から出した状態」または AGD 文書中の構成ガイダンスによる) では、本機能を有効化しなければならない。

FCS_IPSEC_EXT.1.13 TSF は、すべての IKE プロトコルが RFC 4945 に適合する X.509v3 証明書及び [選択：*事前共有鍵*、*その他の方法なし*]を用いる [選択：*RSA*、*ECDSA*] を用いたピア認証が実行されることを保証しなければならない。

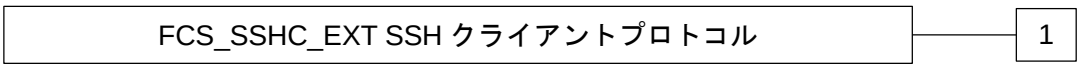
FCS_IPSEC_EXT.1.14 TSF は、有効な証明書を持っているピアへの高信頼チャネルのみを確立しなければならない。

C.2.2.3 FCS_SSHC_EXT.1 SSH クライアント

ファミリのふるまい

本ファミリのコンポーネントは、SSH プロトコルを用いてクライアントとサーバとの間のデータを保護するためにクライアントが SSH を利用する能力に対応する。

コンポーネントのレベル付け



FCS_SSHC_EXT.1 SSH クライアントは、特定されたとおりに SSH のクライアント側が実装されることを要求する。

管理：FCS_SSHC_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_SSHC_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) SSH セションの確立失敗

b) SSH セションの確立

c) SSH セションの終了

FCS_SSHC_EXT.1	**SSH クライアントプロトコル**

下位階層： なし

依存性： FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)
FCS_COP.1(2) 暗号操作 (署名の検証)
FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)

FCS_SSHC_EXT.1.1 TSF は、RFC 4251、4252、4253、4254、及び [選択：*5647*、*5656*、*6187*、*6668*、*その他の RFC なし*] に準拠する SSH プロトコルを実装しなければならない。

適用上の注釈 118

ST 作成者は、適合主張されている追加の RFC を選択すること。これらは、本コンポーネントの後のエレメントにおける選択 (例えば、許可される暗号アルゴリズム) と一貫している必要があることに注意されたい。RFC 4253 は、特定の暗号アルゴリズムが「必須」であることを指示している。これは、そのアルゴリズムが利用のため有効化されなければならないことではなく、実装がそのサポートを含んでいなければならないことを意味する。「必須」と示されているが本コンポーネントの後のエレメントに列挙されないアルゴリズムが実装されていることを保証することは、本要件の保証アクティビティの適用範囲外である。

FCS_SSHC_EXT.1.2 TSF は、SSH プロトコルの実装が RFC 4252 に記述される以下の認証方法をサポートすることを保証しなければならない：公開鍵ベースのもの、パスワードベ

ースのもの。

FCS_SSHC_EXT.1.3 TSF は、RFC 4253 に記述されるように、SSH トランスポート接続中の [割付：*バイト数*] より大きいパケットが破棄されることを保証しなければならない。

適用上の注釈 119

RFC 4253 は、そのパケットが「合理的な長さ」でなければ破棄されるべきという警告と共に「大きなパケット」の受け入れを提供している。割付は、ST 作成者により受け入れられる最大のパケット長、すなわち TOE の「合理的な長さ」を定義しつつ、記入されるべきである。

FCS_SSHC_EXT.1.4 TSF は、SSH トランスポートの実装が以下の暗号化アルゴリズムを使用し、他のすべての暗号アルゴリズムを拒否することを保証しなければならない：[割付：*暗号化アルゴリズムのリスト*]。

FCS_SSHC_EXT.1.5 TSF は、SSH トランスポートの実装がその公開鍵アルゴリズムとして [割付：*公開鍵アルゴリズムのリスト*] を使用し、他のすべての公開鍵アルゴリズムを拒否することを保証しなければならない。

FCS_SSHC_EXT.1.6 TSF は、SSH トランスポートの実装がそのデータ完全性 MAC アルゴリズムとして [割付：*データ完全性 MAC アルゴリズムのリスト*] を使用し、他のすべての MAC アルゴリズムを拒否することを保証しなければならない。

FCS_SSHC_EXT.1.7 TSF は、 [割付：*鍵交換方法のリスト*] のみが SSH プロトコル用に使用が許可される鍵交換方法であることを保証しなければならない。

FCS_SSHC_EXT.1.8 TSF は、2^28 を超えない数のパケットがその鍵を用いて送信された後に SSH 接続が鍵変更されることを保証しなければならない。

FCS_SSHC_EXT.1.9 TSF は、SSH クライアントが RFC 4251 のセクション 4.1 に記述されるように、各ホスト名に対応する公開鍵と対応するローカルなデータベースまたは [選択：*信頼済み認証局のリスト*、*その他の方法なし*] を用いる SSH サーバの識別情報を認証することを保証しなければならない。

適用上の注釈 120

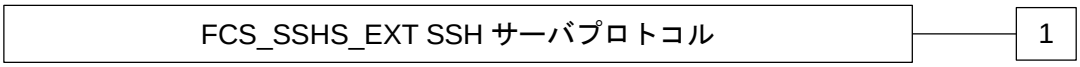
信頼済み認証局のリストは、FCS_SSHC_EXT.1.5 において x509v3-ecdsa-sha2-nistp256 または x509v3-ecdsa-sha2-nistp384 が指定される場合にのみ選択できる。

C.2.2.4 FCS_SSHS_EXT.1 SSH サーバプロトコル

ファミリのふるまい

本ファミリのコンポーネントは、SSH プロトコルを用いてクライアントとサーバとの間のデータを保護するためにサーバが SSH を提供する能力に対応する。

コンポーネントのレベル付け



FCS_SSHS_EXT.1 SSH サーバは、SSH のサーバ側が指定どおり実装されることを要求する。

管理：FCS_SSHS_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_SSHS_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) SSH セションの確立失敗

b) SSH セションの確立

c) SSH セションの終了

FCS_SSHS_EXT.1	**SSH サーバプロトコル**

下位階層： なし

依存性： FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)
FCS_COP.1(2) 暗号操作 (署名の検証)
FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)

FCS_SSHS_EXT.1.1 TSF は、RFC 4251、4252、4253、4254、及び [選択：*5647*、*5656*、*6187*、*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。

適用上の注釈 121

ST 作成者は、適合主張されている追加の RFC を選択すること。これらは、本コンポーネントの後のエレメントにおける選択 (例えば、許可される暗号アルゴリズム) と一貫している必要があることに注意されたい。RFC 4253 は、特定の暗号アルゴリズムが「必須」であることを指示している。これは、そのアルゴリズムが利用のため有効化されなければならないことではなく、実装がそのサポートを含んでいなければならないことを意味する。「必須」と示されているが本コンポーネントの後のエレメントに列挙されないアルゴリズムの実装を保証することは、本要件の保証アクティビティの適用範囲外である。

FCS_SSHS_EXT.1.2 TSF は、SSH プロトコルの実装が RFC 4252 に記述される以下の認証方法をサポートすることを保証しなければならない：公開鍵ベースのもの、パスワードベースのもの。

FCS_SSHS_EXT.1.3 TSF は、RFC 4253 に記述されるように、SSH トランスポート接続中の [割付：*バイト数*] より大きいパケットが破棄されることを保証しなければならない 。

適用上の注釈 122

RFC 4253 は、そのパケットが「合理的な長さ」でなければ破棄されるべきという警告と共に「大きなパケット」の受け入れを提供している。割付には、ST 作成者により受け入れられる最大のパケット長、すなわち TOE の「合理的な長さ」を定義しつつ、記入されるべきである。

FCS_SSHS_EXT.1.4 TSF は、SSH トランスポートの実装が以下の暗号化アルゴリズムを使用し、他のすべての暗号アルゴリズムを拒否することを保証しなければならない：[割付：*暗号化アルゴリズム*]。

FCS_SSHS_EXT.1.5 TSF は、SSH トランスポートの実装がその公開鍵アルゴリズムとして [割付：*公開鍵アルゴリズムのリスト*] を使用し、他のすべての公開鍵アルゴリズムを拒否することを保証しなければならない。

FCS_SSHS_EXT.1.6 TSF は、SSH トランスポートの実装がその MAC アルゴリズムとして [割付：*MAC アルゴリズムのリスト*] を使用し、他のすべての MAC アルゴリズムを拒否することを保証しなければならない。

FCS_SSHS_EXT.1.7 TSF は、 [割付：*鍵交換方法のリスト*] のみが SSH プロトコルに利用が許可される鍵交換方法であることを保証しなければならない。

FCS_SSHS_EXT.1.8 TSF は、2^28 を超えない数のパケットがその鍵を用いて送信された後に SSH 接続が鍵変更されることを保証しなければならない。

C.2.2.5 FCS_TLSC_EXT TLS クライアントプロトコル

ファミリのふるまい

本ファミリのコンポーネントは、TLS プロトコルを用いてクライアントとサーバとの間のデータを保護するためにクライアントが TLS プロトコルを利用する能力に対応する。

コンポーネントのレベル付け

FCS_TLSC_EXT.1 TLS クライアントは、特定されたとおりに TLS のクライアント側が実装されることを要求する。

FCS_TLSC_EXT.2 TLS クライアントは、TLS のクライアント側の実装に相互認証が含まれることを要求する。

管理：FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) TLS セションの確立失敗

b) TLS セションの確立

c) TLS セションの終了

FCS_TLSC_EXT.1	**TLS クライアントプロトコル**

下位階層： なし

依存性： FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)
FCS_COP.1(2) 暗号操作 (署名の検証)
FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)
FCS_RBG_EXT.1 ランダムビット生成

FCS_TLSC_EXT.1.1 TSF は、以下の暗号スイートをサポートする [選択 : *TLS 1.2 (RFC 5246)*、*TLS 1.1 (RFC 4346)*] を実装しなければならない :

- *必須の暗号スイート：*
  - *[割付 : 必須の暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
- *[選択：オプションの暗号スイート：*
  - *[割付：オプションの暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
  - *その他の暗号スイートなし]]。*

適用上の注釈 123

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっていることに注意されたい。

FCS_TLSC_EXT.1.2 TSF は、提示された識別子が参照識別子と一致することを RFC 6125 に従って検証しなければならない。

適用上の注釈 124

識別子の検証のための規則は、RFC 6125 のセクション 6 に記述されている。参照識別子は利用者により (例、ウェブブラウザへの URL 入力またはリンクのクリック等)、設定により (例、メールサーバまたは認証サーバの名前の設定等)、またはアプリケーションにより (例、API のパラメタ等) アプリケーションサービスに応じて確立される。単一の参照識別子の生成元ドメイン及びアプリケーションサービス種別 (例、HTTP、SIP、LDAP 等) に基づき、クライアントは受け入れ可能なすべての参照識別子、例えば、証明書のサブジェクト名フィールドのコモン名、及びサブジェクト別名フィールドの (大文字と小文字を区別しない) DNS 名、URI 名、及びサービス名を確立する。クライアントは、その時、このすべての受け入れ可能な参照識別子のリストを、TLS サーバの証明書において提示された識別子と比較する。

FCS_TLSC_EXT.1.3 TSF は、ピア証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない。

適用上の注釈 125

有効性は、識別子の検証、証明書パス、有効期限、及び失効状態により、RFC 5280 に従っ

て決定されること。

FCS_TLSC_EXT.1.4 TSF は、Client Hello における Supported Elliptic Curves Extension に以下の NIST 曲線を提示しなければならない： [割付：*「なし」の選択肢を含むサポートされる曲線のリスト*]。

適用上の注釈 126

楕円曲線を伴う暗号スイートが FCS_TLSC_EXT.1.1 において選択された場合、1 つ以上の曲線の選択が必須となる。楕円曲線を伴う暗号スイートが FCS_TLS_EXT.1.1 においてひとつも選択されない場合、「なし」が選択されるべきである。

本要件は、認証及び鍵共有のために許可される楕円曲線を、FCS_COP.1(2) 及び FCS_CKM.1 ならびに FCS_CKM.2 からの NIST 曲線に制限している。本拡張は、楕円曲線暗号スイートをサポートするクライアントについては必須となる。

FCS_TLSC_EXT.2	**認証を伴う TLS クライアントプロトコル**

下位階層： FCS_TLSC_EXT.1 TLS クライアントプロトコル

依存性： FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)
FCS_COP.1(2) 暗号操作 (署名の検証)
FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)
FCS_RBG_EXT.1 ランダムビット生成

FCS_TLSC_EXT.2.1 TSF は、以下の暗号スイートをサポートする [選択：*TLS 1.2 (RFC 5246)*、*TLS 1.1 (RFC 4346)*] を実装しなければならない：

- *必須の暗号スイート：*
  - *[割付：必須の暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
- *[選択：オプションの暗号スイート：*
  - *[割付：オプションの暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
  - *その他の暗号スイートなし]]。*

適用上の注釈 127

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっていることに注意されたい。

FCS_TLSC_EXT.2.2 TSF は、提示された識別子が参照識別子と一致することを RFC 6125 に従って検証しなければならない。

適用上の注釈 128

識別子の検証のための規則は、RFC 6125 のセクション 6 に記述されている。参照識別子は利用者により (例、ウェブブラウザへの URL 入力またはリンクのクリック等)、設定により (例、メールサーバまたは認証サーバの名前の設定等)、またはアプリケーションにより (例、API のパラメタ等)、アプリケーションサービスに応じて確立される。単一の参照識別子の生成元ドメイン及びアプリケーションサービス種別 (例、HTTP、SIP、LDAP 等) に基づき、クライアントは受け入れ可能なすべての参照識別子、例えば証明書のサブジェクト名フィ

ールドのコモン名ならびにサブジェクト別名フィールドの (大文字と小文字を区別しない) DNS 名、URI 名、及びサービス名を確立する。クライアントは、その時、このすべての受け入れ可能な参照識別子のリストを、TLS サーバの証明書において提示された識別子と比較する。

FCS_TLSC_EXT.2.3 TSF は、ピア証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない。

適用上の注釈 129

有効性は識別子の検証、証明書パス、有効期限、及び失効状態により、RFC 5280 に従って決定されること。

FCS_TLSC_EXT.2.4 TSF は、Client Hello における Supported Elliptic Curves Extension において、以下の NIST 曲線を提示しなければならない： [割付：*「なし」の選択肢を含むサポートされる曲線のリスト*]。

FCS_TLSC_EXT.2.5 TSF は、X.509v3 証明書を用いる相互認証をサポートしなければならない。

適用上の注釈 130

TLS 用の X.509v3 証明書の使用は、FIA_X509_EXT.2.1 において対処される。本要件は、クライアントが TLS 相互認証を行うために TLS サーバへ証明書を提示できなければならないことがこの用途に含まれなければならないことを追加すること。

C.2.2.6 FCS_TLSS_EXT TLS サーバプロトコル

ファミリのふるまい

本ファミリのコンポーネントは、TLS プロトコルを用いてクライアントとサーバとの間のデータを保護するためにサーバが TLS を利用する能力に対応する。

コンポーネントのレベル付け

FCS_TLSS_EXT.1 TLS サーバは、特定されたとおりに、TLS のサーバ側が実装されることを要求する。

FCS_TLSS_EXT.2 TLS サーバは、TLS の実装に相互認証が含まれることを要求する。

管理：FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) TLS セションの確立失敗

b) TLS セションの確立

c) TLS セションの終了

FCS_TLSS_EXT.1	**TLS サーバプロトコル**

下位階層： なし

依存性： FCS_CKM.1 暗号鍵の生成
FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)
FCS_COP.1(2) 暗号操作 (署名の検証)
FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)
FCS_RBG_EXT.1 ランダムビット生成

FCS_TLSS_EXT.1.1 TSF は、以下の暗号スイートをサポートする [選択：*TLS 1.2 (RFC 5246)*、*TLS 1.1 (RFC 4346)*] を実装しなければならない：

- *必須の暗号スイート：*
  - *[割付：必須の暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
- *[選択：オプションの暗号スイート：*
  - *[割付：オプションの暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
  - *その他の暗号スイートなし]]*。

適用上の注釈 131

評価される構成においてテストされるべき暗号スイートは、本要件によって制限されている。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっていることに注意されたい。

FCS_TLSS_EXT.1.2 TSF は、SSL 1.0、SSL 2.0、SSL 3.0、TLS 1.0、及び [選択：*TLS 1.1*、*TLS 1.2*、*なし*] を要求するクライアントからの接続を拒否しなければならない。

適用上の注釈 132

FCS_TLSS_EXT.1.1 において選択されなかったあらゆる TLS のバージョンが、ここで選択されるべきである。

FCS_TLSS_EXT.1.3 TSF は、鍵長 2048 ビット及び [選択：*3072 ビット*、*4096 ビット*、*その他の鍵長なし*] の RSA、及び [選択：[割付：*楕円曲線のリスト*] ; [割付：*Diffie-Hellman パラメタサイズのリスト*]]を用いて鍵確立パラメタを生成しなければならない。

適用上の注釈 133

割付は、FCS_TLSS_EXT.1.1 において行われた割付に基づいて記入されることになる。

FCS_TLSS_EXT.2	**相互認証を伴う TLS サーバプロトコル**

下位階層： FCS_TLSS_EXT.1 TLS サーバプロトコル

依存性： FCS_CKM.1 暗号鍵の生成
FCS_COP.1(1) 暗号操作 (AES データ暗号化／復号)
FCS_COP.1(2) 暗号操作 (署名の検証)
FCS_COP.1(3) 暗号操作 (ハッシュアルゴリズム)
FCS_RBG_EXT.1 ランダムビット生成

FCS_TLSS_EXT.2.1 TSF は、以下の暗号スイートをサポートする [選択：*TLS 1.2 (RFC 5246)*、*TLS 1.1 (RFC 4346)*] を実装しなければならない：

- *必須の暗号スイート：*
  - *[割付：必須の暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
- *[選択：オプションの暗号スイート：*
  - *[割付：オプションの暗号スイートのリスト及びそれぞれが定義される RFC への参照]*
  - *その他の暗号スイートなし]]。*

適用上の注釈 134

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっていることに注意されたい。

FCS_TLSS_EXT.2.2 TSF は、SSL 1.0、SSL 2.0、SSL 3.0、TLS 1.0、及び [選択：*TLS 1.1*、*TLS 1.2*、*なし*] を要求するクライアントからの接続を拒否しなければならない。

適用上の注釈 135

FCS_TLSS_EXT.2.1 において選択されなかったあらゆる TLS のバージョンが、ここで選択さ

れるべきである 。

FCS_TLSS_EXT.2.3 TSF は、鍵長 2048 ビット及び [選択：*3072 ビット、4096 ビット、その他の鍵長なし*] の RSA、及び [選択：*[割付：楕円曲線のリスト] ；[割付：Diffie-Hellman パラメタサイズのリスト]*]を用いて鍵確立パラメタを生成しなければならない。

適用上の注釈 136

割付は、FCS_TLSS_EXT.2.1 において行われた割付に基づいて記入されることになる。

FCS_TLSS_EXT.2.4 TSF は、X.509v3 証明書を用いた相互認証をサポートしなければならない。

適用上の注釈 137

TLS のための X.509v3 証明書の使用は、FIA_X509_EXT.2.1 において対処される。本要件は、本用途に TLS 相互認証用のクライアント側証明書のサポートが含まれなければならないことを追加している。

FCS_TLSS_EXT.2.5 TSF は、ピア証明書が無効である場合、高信頼チャネルを確立してはならない。

適用上の注釈 138

有効性は、証明書パス、有効期限、及び失効状態により、RFC 5280 に従って決定される。

FCS_TLSS_EXT.2.6 TSF は、証明書に含まれる識別名 (DN) またはサブジェクト別名 (SAN) がピアに期待される識別子と一致しない場合、高信頼チャネルを確立してはならない。

適用上の注釈 139

本要件は、相互認証 TLS を行う TOE にのみ適用される (FCS_TLSS_EXT.2.4)。ピア識別子は、証明書のサブジェクト名フィールドまたはサブジェクト別名拡張に存在する。期待される識別子は、設定されてもよいし、あるいはピアによって用いられるドメイン名、IP アドレス、利用者名、または電子メールアドレスと比較されたり、または比較のためディレクトリサーバへ渡されたりしてもよい。

C.3 ファイアウォール (FFW)

C.3.1 ステートフルトラフィックフィルタファイアウォール (FFW_RUL_EXT)

ファミリのふるまい

本要件は、ステートフルトラフィックフィルタファイアウォールのふるまいを特定するために用いられる。TOE がフィルタ可能なネットワークプロトコルに加えて、規則セットを構築するために管理者によって利用可能な属性が、本コンポーネントにおいて特定される。どのように規則セットが処理されるか (すなわち、順序) が、TOE の側に期待される任意のデフォルトのふるまいと共に、特定される。

コンポーネントのレベル付け

FFW_RUL_EXT.1 ステートフルトラフィックフィルタフィルタリングは、許可された管理者によって設定された規則セットに基づいてネットワークトラフィックをフィルタすることを TOE に要求する。

管理：FFW_RUL_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) ネットワークインタフェース上の規則セットの有効化／無効化

b) 規則セットの設定

c) 資源の利用を管理する規則の特定

監査：FFW_RUL_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 最小：

- 規則セットにおける規則をネットワークパケットへ適用した結果 (すなわち、破棄、許可)
- 規則セットの設定
- 過大なネットワークトラフィックのため破棄されたパケットの表示

C.3.1.1 FFW_RUL_EXT.1 ステートフルトラフィックフィルタリング

FFW_RUL_EXT.1	**ステートフルトラフィックフィルタリング**

下位階層： なし

依存性： なし

FFW_RUL_EXT.1.1 TSF は、TOE によって処理されるネットワークパケットにステートフルトラフィックフィルタリングを実行しなければならない。

FFW_RUL_EXT.1.2 TSF は、以下のネットワークプロトコルフィールドを使用してステートフルトラフィックフィルタリングの定義を許可しなければならない： [割付：*規則セットによってサポートされる属性のリスト*]。

FFW_RUL_EXT.1.3 TSF は、以下の操作をステートフルトラフィックフィルタリングの規則に関連付けることを許可しなければならない：許可または破棄、その操作をログ出力する機能と共に。

FFW_RUL_EXT.1.4 TSF は、ステートフルトラフィックフィルタリングの規則が、個別の各ネットワークインタフェースに割り当てられることを許可しなければならない。

FFW_RUL_EXT.1.5 TSF は、以下を実行しなければならない：

a) 以下のプロトコル： [割付：*状態が維持管理されるサポートされるプロトコルのリスト*] に関して、以下のネットワークパケットの属性： [割付：*プロトコルのそれぞれに関連付けられた属性のリスト*] に基づいて、許可され確立されたセションに一致する場合、ステートフルトラフィックフィルタリングをさらに処理することなくネットワークパケットを受け入れる。

b) 以下： [選択：*セション非アクティブタイムアウト*、*予期された情報フローの完了*] に基づいて、一連の確立されたトラフィックフローから既存のトラフィックフローを削除する。

FFW_RUL_EXT.1.6 TSF は、すべてのネットワークトラフィックへ、以下のデフォルトのステートフルトラフィックフィルタリングの規則を強制しなければならない： [割付：*ネットワークトラフィックのフローへ適用されるデフォルト規則のリスト*]。

FFW_RUL_EXT.1.7 TSF は、以下の規則に従って。破棄及びログ出力を実行できなければならない： [割付：*TOE が強制可能な特定の規則のリスト*]

FFW_RUL_EXT.1.8 TSF は、管理者が定義した順序で、該当するステートフルトラフィックフィルタリングの規則を処理しなければならない。

FFW_RUL_EXT.1.9 TSF は、一致を検証する規則が識別されない場合、パケットフローを拒否しなければならない。

FFW_RUL_EXT.1.10 TSF は、 [割付：*資源の利用を管理する規則*] を、管理者が定義した数に制限できなければならない。

C.3.1.2 FFW_RUL_EXT.2 動的プロトコルのステートフルフィルタリング

FFW_RUL_EXT.2	**動的プロトコルのステートフルフィルタリング**

下位階層： なし

依存性： なし

FFW_RUL_EXT.2.1 TSF は、以下のネットワークプロトコル [割付：*サポートされるプロトコルのリスト*] に関して、ネットワークトラフィックのフローを許可する規則の定義またはセションの確立を動的に実行しなければならない。

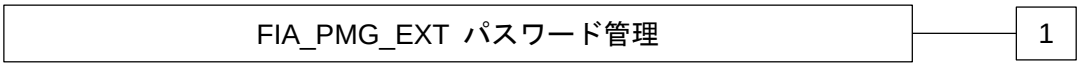
C.4 識別と認証 (FIA)

C.4.1 パスワード管理 (FIA_PMG_EXT)

ファミリのふるまい

TOE は、強いパスワード及びパスフレーズが選ばれて維持できることを保証するために、管理利用者によって用いられるパスワードの属性を定義する。

コンポーネントのレベル付け



FIA_PMG_EXT.1 パスワード管理は、さまざまな構成要件、最小の長さ、最大のライフタイム、及び類似性の制約を持つパスワードを TSF がサポートすることを要求する。

管理：FIA_PMG_EXT.1

管理機能なし。

監査：FIA_PMG_EXT.1

具体的な監査要件なし。

C.4.1.1 FIA_PMG_EXT.1 パスワード管理

FIA_PMG_EXT.1	**パスワード管理**

下位階層： なし

依存性： なし

FIA_PMG_EXT.1.1 TSF は、管理者パスワードについて、以下のパスワード管理機能を提供しなければならない：

a) パスワードは、大文字及び小文字、数字、ならびに以下の特殊文字： [選択：“!”、“@”、“#”、“$”、“%”、“^”、“&”、“”、“(“、“)”、[割付：その他の文字]]の任意の組み合わせによって構成できなければならない；*

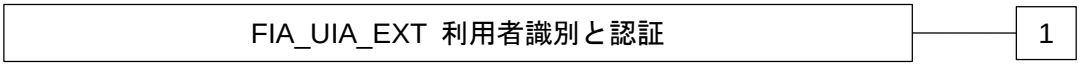
b) 最小のパスワード長は、セキュリティ管理者によって設定可能でなければならず、また 15 文字以上のパスワードがサポートされなければならない。

C.4.2 利用者識別と認証 (FIA_UIA_EXT)

ファミリのふるまい

TSF は、非 TOE エンティティが識別と認証のプロセスを経る前に、特定の指定されたアクションを許す。

コンポーネントのレベル付け



FIA_UIA_EXT.1 利用者識別と認証は、管理者 (リモート管理者を含む) が TOE によって識別され認証され、通信パスの端点の保証を提供することを要求する。また、TOE が何らかの仲介機能を行う前に、すべての利用者が識別され認証されることも保証する

管理：FIA_UIA_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) エンティティが識別され認証される前に利用可能な TOE サービスのリストを設定する能力；

監査：FIA_UIA_EXT.N

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 識別と認証のメカニズムの利用すべて

b) 提供された利用者識別情報、試行の生成元 (例えば、IP アドレス)

C.4.2.1 FIA_UIA_EXT.1 利用者識別と認証

FIA_UIA_EXT.1	**利用者識別と認証**

下位階層： なし

依存性： FTA_TAB.1 デフォルト TOE アクセスバナー

FIA_UIA_EXT.1.1 TSF は、非 TOE エンティティに識別と認証のプロセスを開始することを要求する前に、以下のアクションを許可しなければならない：

- FTA_TAB.1 に従って警告バナーを表示すること；
- [選択：*その他のアクションなし*、 *[割付：サービスのリスト、非 TOE の要求に応じて TSF により実行されるアクション。]*]

FIA_UIA_EXT.1.2 TSF は、その管理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、各管理利用者に識別と認証が成功することを要求しなければならない。

C.4.3 利用者認証 (FIA_UAU) (FIA_UAU_EXT)

ファミリのふるまい

ローカルベースの管理利用者認証メカニズムを提供する

コンポーネントのレベル付け

FIA_UAU_EXT パスワードベースの認証メカニズム	2

FIA_UAU_EXT.2 パスワードベースの認証メカニズムは、管理利用者にローカルの認証メカニズムを提供する。

管理：FIA_UAU_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) なし

監査：FIA_UAU_EXT.2

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 最小：認証メカニズムのすべての使用

C.4.3.1 FIA_UAU_EXT.2 パスワードベースの認証メカニズム

FIA_UAU_EXT.2	**パスワードベースの認証メカニズム**

下位階層： なし

依存性： なし

FIA_UAU_EXT.2.1 TSF は、管理利用者の認証を実行するため、ローカルのパスワードベースの認証メカニズム、 [選択： *[割付：その他の認証メカニズム]*、*なし*] を提供しなければならない。

C.4.4 X.509 証明書を用いた認証 (拡張—FIA_X509_EXT)

ファミリのふるまい

本ファミリは、TSF によって実行される機能について、ふるまい、管理、及び X.509 証明書の使用を定義する。本ファミリのコンポーネントは、具体的な規則に従った証明書の有効性確認、プロトコル及び完全性検証用の認証のための証明書の使用、及び証明書要求の生成を要求する。

コンポーネントのレベル付け

FIA_X509_EXT.1 X509 証明書有効性確認は、TSF が、コンポーネントにおいて特定される RFC 及び規則に従って証明書をチェックし、有効性確認することを要求する。

FIA_X509_EXT.2 X509 証明書認証は、TSF が、証明書を要求する完全性検証及びその他の機能と同様に、証明書をサポートするプロトコルにおいてピア認証を行うために証明書を使用することを要求する。

FIA_X509_EXT.3 X509 証明書要求は、TSF が、証明書要求メッセージを生成し、応答を検証できることを要求する。

管理：FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

以下のアクションは、FMT における管理機能と考えられる：

a) インポートされた X.509v3 証明書の削除

b) X.509v3 証明書のインポート及び削除の承認

c) 証明書要求の開始

監査：FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 最小：具体的な監査要件はない。

C.4.4.1 FIA_X509_EXT.1 X.509 証明書有効性確認

FIA_X509_EXT.1	X.509 証明書有効性確認

下位階層： なし

依存性： なし

FIA_X509_EXT.1.1 TSF は、以下の規則に従って証明書の有効性を確認しなければならない：

- RFC 5280 証明書有効性確認及び証明書パス検証。
- 証明書パスは、信頼済み CA 証明書で終端しなければならない。
- TSF は、すべての CA 証明書について、basicConstraints 拡張の存在と CA フラグが TRUE にセットされていることを保証し、証明書パスを検証しなければならない。
- TSF は、[選択：*RFC 2560 に特定されるオンライン証明書状態プロトコル (OCSP)*、*RFC 5759 に特定される証明書失効リスト (CRL)*] を用いて、証明書の失効状態を検証しなければならない。
- TSF は、以下の規則に従って extendedKeyUsage フィールドを検証しなければならない：[割付：*検証が必要な extendedKeyUsage フィールドの内容を定める規則*]。

適用上の注釈 140

FIA_X509_EXT.1.1 には、証明書有効性確認を行うための規則が列挙されている。ST 作成者は、失効状態が OCSP か CRL のどちらを用いて検証されるかを選択する。ST 作成者は、ST の他の要件に適用され得る規則を割付に記入する。例えば、証明書を使用する TLS 等のプロトコルが ST に特定されている場合、extendedKeyUsage フィールドの具体的な値 (例えば、「サーバ認証目的」) が指定される。

FIA_X509_EXT.1.2 TSF は、basicConstraints 拡張に CA フラグが TRUE にセットされている場合にのみ、証明書を CA 証明書として取り扱わなければならない。

適用上の注釈 141

本要件は、TSF によって使用され処理される証明書に適用され、証明書を信頼済み CA 証明書として追加できるように制限する。

C.4.4.2 FIA_X509_EXT.2 X509 証明書認証

FIA_X509_EXT.2	**X.509 証明書認証**

下位階層： なし

依存性： なし

FIA_X509_EXT.2.1 TSF は、[選択：*IPsec*、*TLS*、*HTTPS*、*SSH*、*[割付：その他のプロトコル]*、*プロトコルなし*]、及び [選択：*システムソフトウェアアップデートのコード署名*、*完全性検証用のコード署名*、*[割付：その他の用途]*、*追加用途なし*] のための認証をサポートするため、RFC 5280 によって定義されるように X.509v3 証明書を使用しなければならない。

適用上の注釈 142

TOE が証明書を用いたピア認証を行う通信プロトコルの実装を特定する場合、ST 作成者は具体的なプロトコルを選択するか、または割付けるかのいずれかを行う；それ以外の場合は、「プロトコルなし」を選択すること。TOE は、その他の目的のためにも証明書を使用してもよい；2 番目の選択及び割付は、これらの場合に使用される。

FIA_X509_EXT.2.2 TSF が、証明書の有効性を決定するためのコネクションを確立できない時、TSF は [選択：*このような場合には証明書を受け入れるかどうかの選択を管理者に許可する*、*証明書を受け入れる*、*証明書を受け入れない*] ようにしなければならない。

適用上の注釈 143

CRL のダウンロード、OCSP の実行のいずれにおいても、証明書の失効状態をチェックするためにコネクションを確立しなくてはならない場合は多々生ずる。本選択は、(例えば、ネットワークエラーのため) このようなコネクションが確立できない場合のふるまいを記述するために用いられる。TOE が、FIA_X509_EXT.1 のその他の全ての規則に従って証明書の有効性を決定する場合、選択で示されたふるまいにより有効性が決定される。

C.4.4.3 FIA_X509_EXT.3 X.509 証明書要求

FIA_X509_EXT.3	X.509 証明書要求

下位階層： なし

依存性： なし

FIA_X509_EXT.3.1 TSF は、RFC 2986 に指定される証明書要求メッセージを生成しなければならず、本要求において以下の情報を提供できなければならない：公開鍵及び [選択：*デバイス固有情報*、*コモン名(Common Name)*、*組織 (Organization)*、*組織単位 (Organizational Unit)*、*国 (Country)*、*[割付：その他の情報]*]。

FIA_X509_EXT.3.2 TSF は、CA 証明書応答の受信の際、ルート CA からの証明書のチェインの有効性を確認しなければならない。

C.5 TSF の保護 (FPT)

C.5.1 TSF データの保護 (FPT_SKP_EXT)

ファミリのふるまい

本ファミリのコンポーネントは、暗号鍵等の TSF データを管理し保護するための要件に対処する。これは、FPT_PTD クラスにならってモデル化される新たなファミリである。

コンポーネントのレベル付け

FPT_SKP_EXT TSF データの保護	1

FPT_SKP_EXT.1 TSF データの保護 (すべての対称鍵の読み出しについて) は、あらゆる利用者またはサブジェクトによる対称鍵の読み出しが防止することを要求する。これは、本ファミリの唯一のコンポーネントである。

管理：FPT_SKP_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FPT_SKP_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 予見される監査対象事象はない。

C.5.1.1 FPT_SKP_EXT.1 TSF データの保護 (すべての対称鍵の読み出しについて)

FPT_SKP_EXT.1	TSF データの保護 (すべての対称鍵の読み出しについて)

下位階層： なし

依存性： なし

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。

適用上の注釈 144

本要件の意図は、デバイスが、鍵、鍵材料、及び認証クレデンシャルを不正な暴露から保護することである。本データは、それらが割り当てられたセキュリティ機能の目的のためにのみアクセスされるべきであり、また他のいかなる時にもそれらが表示／アクセスされる必要はない。本要件は、これらが存在し、使用中であり、まだ有効であることをデバイスが示すことを妨げるものではない。しかし、本要件は、それらの値をあからさまに読み出すことを制限している。

C.5.2 管理者パスワードの保護 (FPT_APW_EXT)

C.5.2.1 FPT_APW_EXT.1 管理者パスワードの保護

ファミリのふるまい

本ファミリのコンポーネントによって､TSF がパスワード等の平文のクレデンシャルデータを不正な暴露から保護することが保証する。

コンポーネントのレベル付け

FPT_APW_EXT.1 管理者パスワードの保護は、TSF が、あらゆる利用者またはサブジェクトによる平文のクレデンシャルデータの読み出しを防止することを要求する。

管理：FPT_APW_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 管理機能なし。

監査：FPT_APW_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 監査の必要なし。

FPT_APW_EXT.1	管理者パスワードの保護

下位階層： なし

依存性： なし

FPT_APW_EXT.1.1 TSF は、パスワードを平文でない形態で保存しなければならない。

FPT_APW_EXT.1.2 TSF は、平文パスワードの読み出しを防止しなければならない。

C.5.3 TSF 自己テスト

C.5.3.1 FPT_TST_EXT.1 TSF テスト

ファミリのふるまい

本ファミリのコンポーネントは、選択された正常動作について TSF を自己テストするための要件に対処する。

コンポーネントのレベル付け

FPT_TST_EXT.1 TSF 自己テストは、TSF の正常動作を実証するために初期立ち上げ中に自己テストのスイートが実行されることを要求する。

FPT_TST_EXT.2 証明書に基づく自己テストは、自己テストの一部として証明書が用いられる場合に適用され、証明書が無効である場合に自己テストが失敗することを要求する。

管理：FPT_TST_EXT.1, FPT_TST_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) 管理機能なし。

監査：FPT_TST_EXT.1, FPT_TST_EXT.2

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) TSF の自己テストが完了したことの通知

FPT_TST_EXT.1	**TSF のテスト**

下位階層： なし

依存性： なし

FPT_TST_EXT.1.1 TSF は、TSF の正常動作を実証するため、[選択：*初期立ち上げ中 (電源投入時に)*、*通常運用中定期的に*、*許可利用者の要求時に*、*以下の条件 [割付：自己テストが行われるべき条件] 下で*] 以下の自己テストのスイートを実行しなければならない： [割付：*TSF によって実行される自己テストのリスト*]。

適用上の注釈 145

自己テストは、初期立ち上げ中 (電源投入時に) 実行されることが期待される。その他の選択肢は、それらが初期立ち上げ中に実行されない理由を開発者が正当化できる場合にのみ、使用されるべきである。SFR を満たすために必要な暗号機能の正常動作と同様に、ファームウェア及びソフトウェアの完全性の検証のための自己テストが、すくなくとも実行される

ことが期待される。起動中にすべての自己テストが行われない場合、本 SFR を複数繰返して、適切な選択肢を選択されるように使用すること。本 cPP の将来のバージョンで、自己テストのスイートは、少なくとも、measurement を実行するコンポーネントの自己テストを含む、Measured ブートのメカニズム (訳注：TPM 等を用いて保護されたブートプロセスによるテスト等) が含まれることが要求されることになる。

適用上の注釈 146

自己テストメカニズムにより証明書が使用される場合 (例、完全性検証用の署名検証のため等)、証明書は FIA_X509_EXT.1 に従って有効性確認され、かつ FIA_X509_EXT.2.1 で選択がなされるべきである。さらに、FPT_TST_EXT.2 が ST に含まれなければならない。

FPT_TST_EXT.2	**証明書ベースの自己テスト**

下位階層： なし

依存性： なし

FPT_TST_EXT.2.1 TSF は、自己テストに証明書が使用され、かつ対応する証明書が無効とみなされる場合、自己テストを失敗させなければならない。

適用上の注釈 147

証明書は、オプションとして自己テスト用に使用することができる (FPT_TST_EXT.1.1)。証明書が自己テスト用に使用される場合、本エレメントが ST に含まれなければならない。FIA_X509_EXT.2.1 で「完全性検証のためのコード署名」が選択される場合、FPT_TST_EXT.2 が ST へ含まれなければならない。

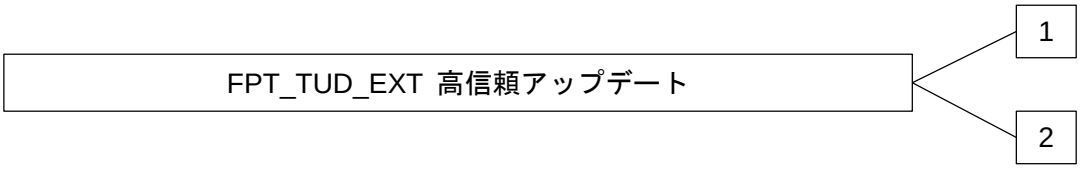
有効性は、証明書パス、有効期限、及び失効状態により、FIA_X509_EXT.1 に従って決定される。

C.5.4 高信頼アップデート (FPT_TUD_EXT)

ファミリのふるまい

本ファミリのコンポーネントは、TOE のファームウェア及び／またはソフトウェアをアップデートするための要件に対処する。

コンポーネントのレベル付け



FPT_TUD_EXT.1 高信頼アップデートは、インストールの前にアップデートを検証する能力を含め、TOE のファームウェア及びソフトウェアをアップデートするために提供される管理ツールを要求する。

FPT_TUD_EXT.2 証明書に基づく高信頼アップデートは、高信頼アップデートの一部として証明書が使用する時に適用され、証明書が無効である場合にアップデートがインストールされないことを要求する。

管理：FPT_TUD_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) TOE をアップデートする能力及びアップデートを検証する能力

b) ディジタル署名機能 (FCS_COP.1(2)) を用いて TOE をアップデートする能力及びアップデートを検証する能力ならびに [選択：*その他の機能なし*、 *[割付：アップデート機能を支援するために用いられるその他の暗号機能 (またはその他の機能)]*]

c) TOE をアップデートする能力、及びこれらのアップデートをインストールする前に [選択：*ディジタル署名*、*公開ハッシュ*、*その他のメカニズムなし*] 機能を用いてアップデートを検証する能力

監査：FPT_TUD_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) アップデートプロセスの開始。

b) アップデートの完全性検証のあらゆる失敗。

C.5.4.1 FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1	**高信頼アップデート**

下位階層： なし

依存性： FCS_COP.1(1) 暗号操作 (暗号署名に関して)、または FCS_COP.1(3) 暗号操作 (暗号ハッシュに関して)

FPT_TUD_EXT.1.1 TSF は [割付 : *許可された利用者*] に TOE ファームウェア／ソフトウェアの一番最近にインストールされたバージョンと同様に、TOE ファームウェア／ソフトウェアの現在実行中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。

適用上の注釈 148

現在動作中 (実行中) のバージョンは、一番最近にインストールされたバージョンではないかもしれない。例えば、アップデートはインストールされたが、このアップデートが動作するためにはシステムのリブートが必要かもしれない。従って、問い合わせには一番最近にインストールされたアップデートと一番最近に実行されたバージョンの両方が示されるべきであることを明確にしておく必要がある。

FPT_TUD_EXT.1.2 TSF は [割付 : *許可された利用者*] に TOE ファームウェア／ソフトウェアへのアップデートを手動で開始する能力及び [選択 : *アップデートの自動的なチェックをサポートする*、*自動アップデートをサポートする*、*その他のアップデートメカニズムなし*] 能力を提供しなければならない。

適用上の注釈 149

FPT_TUD_EXT.1.2 の選択は、アップデートの自動的なチェックのサポートと自動アップデートのサポートとを区別している。最初の選択肢は、新たなアップデートが利用可能であるかどうかを TOE がチェックしてこれを管理者へ通知すること (例、管理セション中のメッセージによって、ログファイルによって等) を意味しているが、実際にアップデートを実行するためには管理者による何らかのアクションを必要としている。第 2 の選択肢は、TOE がアップデートをチェックして、利用可能かどうかに応じてそれを自動的にインストールすることを意味している。

FPT_TUD_EXT.1.3 TSF は、それらのファームウェア／ソフトウェアのアップデートをイン

ストールする前に、 [選択：*ディジタル署名メカニズム*、*公開ハッシュ*] を用いて、TOE のアップデートを認証 (訳注：完全性検証) する手段を提供しなければならない。

適用上の注釈 150

FPT_TUD_EXT.1.3 の選択において参照されるディジタル署名メカニズムは、FCS_COP.1(2) で指定されるアルゴリズムの 1 つであること。FPT_TUD_EXT.1.3 において参照される公開ハッシュは、FCS_COP.1(3) で指定される機能の 1 つによって生成されること。ST 作成者は、TOE により実装されるメカニズムを選択すべきである；両方のメカニズムを実装することは受け入れ可能である。

適用上の注釈 151

本 cPP の将来のバージョンは、高信頼アップデートにディジタル署名メカニズムの使用を義務付けることになる。

適用上の注釈 152

アップデート検証メカニズムによって証明書が使用される場合、証明書は FIA_X509_EXT.1 に従って有効性確認され、また FIA_X509_EXT.2.1 で選択されるべきである。さらに、FPT_TUD_EXT.2 が ST に含まれなければならない。

適用上の注釈 153

本 SFR において「アップデート」とは、不揮発性のシステム常駐ソフトウェアコンポーネントを、別のものと置き換えるプロセスを意味する。前者は NV イメージと呼ばれ、後者はアップデートイメージと呼ばれる。アップデートイメージは通常 NV イメージよりも新しいが、これは要件ではない。システム所有者がコンポーネントをより古いバージョンへロールバックすることを望むような正当なケースは存在する (例えば、コンポーネント製造業者が欠陥のあるアップデートをリリースしたり、アップデート中にはもはや存在しない文書化されていない機能にシステムが依存していたりする場合等)。同様に、所有者は故障したストレージから回復させるために、NV イメージと同一のバージョンでアップデートすることを望むかもしれない。

TSF のすべての個別のソフトウェアコンポーネント (例えば、アプリケーション、ドライバ、カーネル、ファームウェア) は、対応する製造業者によってディジタル署名され、その後アップデートを行うメカニズムによって検証されるべきである。コンポーネントは異なる製造業者によって署名されるかもしれないことが認識されるため、アップデートプロセスがアップデートと NV イメージの両方が同一の製造業者によって製造されたこと (例えば、公開鍵を比較することによって) または正当な署名鍵によって署名されたこと (例えば、X.509 証明書を使用する際に証明書の有効性確認が成功すること) を検証することは必須である。

C.5.4.2 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート

FPT_TUD_EXT.2	**証明書ベースの高信頼アップデート**

下位階層： なし

依存性： FPT_TUD_EXT.1

FPT_TUD_EXT.2.1 TSF は、コード署名証明書が無効とみなされる場合にはアップデートをインストールしてはならない。

FPT_TUD_EXT.2.2 証明書の有効期限が過ぎたために証明書が無効とみなされる時、TSF は [選択：*このような場合には証明書を受け入れるかどうかの選択を管理者に許可する*、*証明*

書を受け入れる、証明書を受け入れない] ようにしなければならない。

適用上の注釈 154

証明書は、オプションとして、システムソフトウェアアップデートのコード署名に使用してもよい (FPT_TUD_EXT.1.3)。証明書がアップデートの検証用に使用される場合、本エレメントが ST に含まれなければならない。FIA_X509_EXT.2.1 において「システムソフトウェアアップデートのコード署名」が選択される場合、FPT_TUD_EXT.2 が ST へ含まれなければならない。

有効性は、証明書パス、有効期限、及び失効状態により FIA_X509_EXT.1 に従って決定されること。有効期限の過ぎた証明書について、ST 作成者は、その証明書が受け入れられなければならないか、拒否されなければならないか、またはその証明書を受けいれるか拒否するかの選択を管理者に委ねるかを選択する。

C.6 TOE アクセス (FTA)

C.6.1 FTA_SSL_EXT.1 TSF 起動セションロック

ファミリのふるまい

本ファミリ中のコンポーネントは、TSF 主導及び利用者主導のロック、ロック解除、及び対話セションの終了を行うための要件に対応する。

拡張された FTA_SSL_EXT ファミリは、FTA_SSL ファミリに基づくものである。

コンポーネントのレベル付け

FTA_SSL_EXT：TSF 起動セションロック	1

FTA_SSL_EXT.1 TSF 起動セションロックは、特定された非アクティブ時間間隔の後に対話セションのシステム起動によるロックを要求する。これは、本ファミリの唯一のコンポーネントである。

管理：FTA_SSL_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

c) 個別の利用者に関してロックアウトが発生する利用者非アクティブ時間の指定。

監査：FTA_SSL_EXT.1

FAU_GEN セキュリティ監査データの生成が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) 対話セションをロック解除しようとするあらゆる試行。

FTA_SSL_EXT.1	**TSF 起動セションロック**

下位階層： なし

依存性： FIA_UAU.1 認証のタイミング

FTA_SSL_EXT.1.1 TSF は、ローカルな対話セションに関して、 [選択：

- *セションのロック―セションのロック解除以外の利用者のデータアクセス／表示デバイスのアクティビティを禁止し、そしてセションのロック解除に先立ってTSFへの管理者再認証を要求すること；*
- *セションの終了*]

を、セキュリティ管理者によって特定される非アクティブ時間間隔後に行わなければならない。

D. エントロピーに関する文書及び評定

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

エントロピー源に関する文書は、それを読んだ後で、評価者が完全にエントロピー源を理解し、それが十分にエントロピーを供給すると信頼できる理由を完全に理解できるように、十分に詳細であるべきである。その文書には、設計記述、エントロピーの正当化、動作条件及びヘルステストという、複数の詳細なセクションが含まれるべきである。その文書が、TSS の一部である必要はない。

D.1 設計記述

文書には、すべてのエントロピー源の構成要素の相互作用を含め、各エントロピー源の全体的な設計が含まれなければならない。製品に含まれるサードパーティのエントロピー源についても、設計に関して共有可能なあらゆる情報が含まれるべきである。

文書には、どのようにエントロピーが作り出されるのか、及びテストの目的で未処理 (生の) データをエントロピー源の内部からどのように取り出せるかを含め、エントロピー源の動作を記述すること。その文書では、エントロピー源の設計の概略説明 (ウォークスルー) が行われ、エントロピーがどこに由来し、次にどこへエントロピー出力が渡されるのか、生の出力に対するあらゆる後処理 (ハッシュ、XOR 等)、もし保存される場合にはどこに保存されるのか、そして最後に、どのようにエントロピー源から出力されるのかを示すべきである。処理に課されるあらゆる条件 (例えば、ブロッキング等) があれば、それについてもエントロピー源の設計の中で記述されるべきである。図や例を利用することが推奨される。

この設計には、エントロピー源のセキュリティ境界の内容の記述、及び境界外部の敵対者がエントロピー割合に影響を与えることができないことをセキュリティ境界がどのように保証するかについての記述も含まれなければならない。

サードパーティのアプリケーションが RBG へエントロピーを追加できる方法が実装されている場合、設計記述にはその記述が含まれなければならない。電源切断から電源投入までの間で保存される RBG 状態があれば、その記述が含まれなければならない。

D.2 エントロピーの正当化

エントロピー源の予測不可能性がどこに由来し、(この特定の TOE による) RBG 出力を使う複数の用途に対して、十分なエントロピーをエントロピー源が供給できることをなぜ確信できるのかについての技術的な議論が存在すべきである。この議論には、期待される最小エントロピー割合 (即ち、情報源データの 1 ビットまたは 1 バイト当たりの最小エントロピー (ビット単位)) の記述と、十分なエントロピーが TOE の攪拌シード生成処理へ投入されることを説明する記述を含むこと。この説明は、なぜエントロピー源がエントロピーを含むビット列を生成すると確信できる理由の正当化の一部となる。

期待される最小エントロピー割合を正当化するために必要な情報量は、製品に含まれるエントロピー源の種別に依存する。

開発者が提供するエントロピー源について、最小エントロピー割合を正当化するため、大量の生の情報源ビットが収集され、統計学的なテストが実行され、統計学的なテストから最小エントロピー割合が決定されることが期待される。現時点では、特定の統計学的なテストは要求されないが、各出力における最小エントロピーの量を決定するために何らかのテストが必要であることが想定される。

サードパーティが提供するエントロピー源について、TOE ベンダは、エントロピー源の設計及び生のエントロピーデータへのアクセスが制限されるため、文書にはこのサードパーティ情報源から取得される最小エントロピー割合の見積りが示されること。ベンダが最小エントロピー割合を「想定」することは受け入れ可能だが、この想定は提供される文書に明確に記述されなければならない。特に、最小エントロピーの見積りは特定されなければならず、その想定が ST に含まれなければならない。

エントロピー源の種別にかかわらず、正当化は、ST に示されるエントロピーで DRBG が初期化される方法が含まれること。例えば、最小エントロピー割合に DRBG へシード値を供給するために使用される情報源のデータ量が乗算されること、または情報源のデータ量に基づき期待されるエントロピー割合が明示的に示され、統計学的な量と比較されることを検証することによって行われる。DRBG へシード値を供給するために使用される情報源のデータ量が明確でなく、または計算された量が明示的にシードと関連付けられていない場合、文書化は完結したとは考えられない。

エントロピー正当化には、サードパーティのアプリケーションからの追加データも、再起動の間で保存される状態からの追加データも、一切含めてはならない。

D.3 動作条件

エントロピー割合は、エントロピー源それ自体が制御できない条件によって影響を受けることがある。例えば、電源電圧、周波数、温度、及び電源投入後の経過時間等は、エントロピー源の動作に影響し得る、要因のほんの数例である。このように、文書にはエントロピー源が乱数データを生成すると期待される動作条件の範囲も記述されることになる。同様に、文書にはエントロピー源が十分なエントロピーを供給するとは、もはや保証されない条件についても記述されなければならない。エントロピー源の故障または機能低下を検出するための方法が、含まれなければならない。

D.4 ヘルステスト

さらに具体的には、すべてのエントロピー源のヘルステスト及びそれらの根拠が、文書化されること。これには、ヘルステストの記述、各ヘルステストが実行される頻度や条件 (例えば、起動時、連続的、またはオンデマンド)、各ヘルステストでの期待される結果、エントロピー源の故障時における TOE のふるまい、及び各テストがエントロピー源において 1 つ以上の故障を検出するために適切であるという確信を示す根拠を含むこと。

E. 用語集

用語	意味
Administrator (管理者)	セキュリティ管理者を参照。
Assurance (保証)	TOE が SFR を満たしているという確信の根拠 [CC1]。
Key Chaining (鍵チェイン)	複数層の暗号化鍵を用いて、データを保護する方法。最上位層の鍵が、データを暗号化する下位層の鍵を暗号化する；この方法は、任意の数の層を持つことができる。
Security Administrator (セキュリティ管理者)	「管理者」という用語と「セキュリティ管理者」という用語は、現時点では本文書において区別なく用いられる。
Target of Evaluation (評価対象)	ソフトウェア、ファームウェア、またはハードウェアあるいはそれらを組み合わせたセットで、ガイダンスが伴うことがある。[CC1]
TSF (TOE セキュリティ機能)	TOE のすべてのハードウェアとソフトウェア、そしてファームウェアから構成されるセットであって、SFR の正しい強制のために信頼されなければならないもの。[CC1]
TSF Data (TSF データ)	TSF の運用のためのデータであって、要件の強制が依存しているもの。

その他のコモンクライテリアの略語及び用語については、[CC1] を参照されたい。

F. 略語

略語	意味
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
CA	Certificate Authority (認証局)
CBC	Cipher Block Chaining
CRL	Certificate Revocation List (証明書失効リスト)
DH	Diffie-Hellman
DSA	Digital Signature Algorithm (ディジタル署名アルゴリズム)
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm (楕円曲線ディジタル署名アルゴリズム)
EEPROM	Electrically Erasable Programmable Read-Only Memory (電気的消去可能プログラマブル読み出し専用メモリ)
FIPS	Federal Information Processing Standards (米国連邦情報処理規格)
GCM	Galois Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HTTPS	HyperText Transfer Protocol Secure
IP	Internet Protocol (インターネットプロトコル)
IPsec	Internet Protocol Security (インターネットプロトコルセキュリティ)
NIST	National Institute of Standards and Technology (米国国立標準技術研究所)
OCSP	Online Certificate Status Protocol (オンライン証明書状態プロトコル)
PP	Protection Profile (プロテクションプロファイル)
RBG	Random Bit Generator (乱数ビット生成器)
RSA	Rivest Shamir Adleman Algorithm
SD	Supporting Document (サポート文書)
SHA	Secure Hash Algorithm (セキュアハッシュアルゴリズム)
SSH	Secure Shell (セキュアシェル)
ST	Security Target (セキュリティターゲット)
TLS	Transport Layer Security (トランスポート層セキュリティ)
TOE	Target of Evaluation (評価対象)
TSF	TOE Security Functionality (TOE セキュリティ機能)
TSS	TOE Summary Specification (TOE 要約仕様)
VPN	Virtual Private Network (仮想プライベートネットワーク)
XTS	XEX (XOR Encrypt XOR) Tweakable Block Cipher with Ciphertext Stealing