エンタープライズセキュリティ管理
ID とクレデンシャル情報管理の
標準プロテクションプロファイル

本書は、米国政府 DoD 傘下の NSA 情報保証局で作成したプロテクションプロファイルの一部を調達要件の検討のため、参考として日本語に直訳したものです。IT セキュリティ評価及び認証制度における適合 PP として利用する場合は、正式な文書である英語版のみとなります。

正式な文書は、以下の URL よりダウンロード可能です。

https://www.niap-ccevs.org/pp/pp_esm_icm_v2.1.pdf

2013 年 10 月 24 日

バージョン 2.1

平成 26 年 12 月 5 日　翻訳 暫定第 0.1 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

文書履歴

バージョン	日付	コメント
1.0	2011 年 7 月 13 日	最初の完成版
1.1	2012 年 5 月 22 日	ESM アクセス制御及びポリシー管理 PP との整合のため更新
1.2	2012 年 7 月 9 日～ 2012 年 8 月 8 日	バージョン 1.1 に関して受け付けたコメントに加えて、CA、Tom Benkhart、及び ESM Telecon からのコメントに対応して更新
1.3	2012 年 8 月 8 日～ 2012 年 8 月 10 日	ESM Telecon からの詳細な変更。クレデンシャル情報の更新に関する最終的な問題の解決。
1.4	2012 年 8 月 31 日	最終版。すべての変更を受け入れた。
1.5	2013 年 6 月 13 日	ESM 認証サーバ PP の適用範囲及びフォーマットとの一貫性、ESM 技術コミュニティのフィードバック、ならびに暗号に関する CCEVS のインプットに基づく変更を行った。
2.1	2013 年 10 月 24 日	アクセス制御プロテクションプロファイルと一貫性を持たせるため、バージョンを 2.1 に更新

目次

図の目次

表の目次

1 プロテクションプロファイル (PP) 序論

1.1 はじめに

本節は、プロテクションプロファイル (PP) がプロテクションプロファイルレジストリを通じて登録されることを可能とするために必要な文書管理及び概括的な情報をが含んでいる。識別情報は、PP を識別し、分類し、登録し、かつ相互参照するために必要なラベル付け及び記述情報を提供する。概要は、叙述形式でプロファイルを要約し、潜在的な利用者が、PP が興味を惹くものかどうか判断するために十分な情報を提供する。本プロファイルの正式な識別情報は、附属書 F - 識別情報に記述されている。

1.2 ESM プロテクションプロファイルスイートの概要

エンタープライズセキュリティ管理 (ESM) は、組織[2]内の一連の IT 資産の集中的な管理をするために使用される製品／製品コンポーネント[1] のスイートを指す。

現在の ESM プロテクションプロファイルスイートでは、以下のエンタープライズポリシータイプの定義を許可するプロファイルが定義されている。

- **アクセス制御ポリシー**：定義されたオブジェクト (IT 資産または資源) に対する定義されたサブジェクト (行為者) の具体的なアクションを権限付与又は拒否するポリシー。
- **識別情報とクレデンシャル情報ポリシー**: サブジェクトの識別、認証、権限付与、及びアカウンタビリティのために使用される属性を定義し維持するポリシー。
- **オブジェクト属性ポリシー**：オブジェクトのために使用される属性を定義し維持するポリシー。
- **認証ポリシー**：利用者がエンタープライズのシステムに認証することができる環境を定義するポリシー。

[1] 注：技術的な意味では「製品」は不正確な用語であるが、他の用語 (例えば「システム」など) も同様に不十分であり、また多義的である。ESM「システム」中のさまざまな「製品」は別個の製品かもしれないが、単純に副次的製品 (subproducts) であったり、あるいは ST に記述されるより大規模な製品中の機能であったりするかもしれない。「製品」という用語を使うのは、ST が *システム* (特定のミッションのために設計された製品の統合化された集まり) ではなく *製品* を記述するものであり、従って PP は製品 (または製品のコンポーネント) を特定ベンダの実装から独立した方法で記述することが一般的であるという、単純な理由によるものである。

[2] 注: 全体的なエンタープライズは組織の境界を越えることがあるという事実を反映して、ESM での使用においては「エンタープライズ」という用語はしばしば「組織」の代わりに用いられる。

- **セキュア構成ポリシー**：IT 資産のベースライン構成を定義するポリシー。
- **監査ポリシー**：監査データがどのように収集され、集積され、報告され、エンタープライズ全体にわかって維持されるかを定義するポリシー。

様々なポリシーを使い、実施する ESM 製品／製品コンポーネントは、次のセキュリティタイプを提供する。

- **予防的 (Preventative)**：エンタープライズが定義する中心的なポリシーの侵害であると判明した場合は、IT 資産に対して実行されるアクションが禁止される。
- **検知的 (Detective)**：不安定で、悪意のあるパタン、又はエンタープライズにまたがる不適切なふるまいを検知することができるように、利用者及び IT 資産のふるまいが監査され、集積される。
- **反応的 (Reactive)**：IT 資産は安全で組織的に定義された中心的な定義と対比され、不一致が確認される場合、処置が講じられる。

ESM 機能には、3 つの種類が存在する。第 1 の種類は*ポリシー定義 (policy definition)* であって、IT 資産のセットのふるまいを規定するために用いられる集中的な組織のポリシーを定義するために用いられる。これは、以下の例により示される：

- セキュア構成管理製品は、システム上に常駐するソフトウェア資産の受容可能なセット、またはそのシステムのアプリケーションの 1 つ以上の構成を規定するポリシーを定義できる。
- ポリシー管理製品は、操作を要求するサブジェクト及びその操作が作用するオブジェクトに基づいて、特定のシステムに対して許可される操作及び許可されない操作を定義できる。

第 2 の種類は*ポリシー利用 (policy consumption)* であって、定義されたポリシーを取得し、保持し、そして永続的に実施する。これは、以下の例により示される：

- システムに常駐するアクセス制御製品は、定義されたアクセス制御ポリシーをポリシー管理から受け取ることができる。次にそれを保存して、別の指示があるまですべてのサブジェクトがそれを順守することを永続的に保証する。
- システムにデータ損失防止アクセス制御を実施するアクセス制御製品は、定義された機密性レベルを特定の種類のオブジェクトに関連付ける定義されたアクセス属性ポリシーを、ポリシー管理から受け取ることができる。このポリシーを保存して、オブジェクトに割付けられた機密性属性に基づいて、オブジェクトがシステムから切り離されることを永続的に阻止する。

3 番目の種類の*ポリシー実施 (policy enforcement)* は、別の場所で定義されたポリシーに、そのポリシーのソースからの問い合わせまたはコマンドの結果として作用する。これは、以下の例により示される：

- 管理者は、ポリシー管理製品を管理するため、それへのログインを試行する。管理者の認証要求は認証サーバへ提出され、認証サーバは定義された認証ポリシーを適用して、その要求が権限付与されるべき (should) かどうかを決定する。次にポリシー管理製品が認証サーバの判断を実施し、それに従ってアクセスを許可または拒否する。
- セキュア構成管理製品は、環境中に展開されたソフトウェアが最新であることを保証するためのポリシーを定義する。アクセスコントロール製品が、古いバージョンであることが判明する。セキュア構成管理製品はアクセス制御製品へ、パッチを適用する指示を発行する。引き続きセキュア構成管理ポリシーは、アクセス制御製品がこの指示に従って行動することにより実施される。

これら 3 種類の ESM 機能は、ESM プロテクションプロファイルのスイート全体で説明される。

ESM PP スイートは 6 つのプロテクションプロファイルから構成され、それらは以下のように特徴づけることができる。

表 1. ESM プロテクションプロファイルスイートの要約

プロテクションプロファイル	アクセス制御ポリシー	識別情報とクレデンシャル情報ポリシー	オブジェクト属性ポリシー	認証ポリシー	セキュア構成ポリシー	監査ポリシー
ESM アクセス制御のプロテクションプロファイル	C	C	C		E	$C_{(1)}$
ESM ポリシー管理のプロテクションプロファイル	D	C/E	$D/C_{(2)}$	$E_{(3)}$	E	$C_{(1)}/D_{(5)}$
ESM 識別情報とクレデンシャル情報管理のプロテクションプロファイル		D	$C/D_{(2)}$	$E_{(3)}$	E	$C_{(1)}$
ESM 認証サーバのプロテクションプロファイル		$E/D_{(4)}$		$D/E_{(3)}$	E	$C_{(1)}$
ESM 監査サーバのプロテクショ		E		$E_{(3)}$	E	$C_{(1)}/D_{(1)}$

ンプロファイル						
ESM セキュア構成管理のプロテクションプロファイル		E		$E_{(3)}$	D/E	$C_{(1)}$/D
C = 利用及び実施、D = 定義、E = 実施						

注意：
1) 監査ポリシーは、どのイベントを監査すべきか TOE が決定する際に利用される。あるいは、デファクト監査ポリシーが監査サーバ TOE 内部でのみ定義され、それにより収集されたデータの管理的に定義されたサブセットを廃棄してもよい。
2) オブジェクト属性は、識別情報とクレデンシャル情報管理 PP またはポリシー管理 PP のいずれかで定義されるが、両方では定義されない。
3) 認証ポリシーは、認証サーバが認証要求を TOE へ仲介するかもしれないという意味で、実施される。
4) 具体的には、認証サーバが強度のある秘密ポリシーを定義する可能性が考えられる。
5) 具体的には、アクセス制御 TOE により監査されるアクセス制御イベントをポリシー管理 TOE が定義する可能性がある。

1.3 ESM 識別情報とクレデンシャル情報管理のプロテクションプロファイルの概要

本プロテクションプロファイルは、**識別情報とクレデンシャル情報の管理を実施する ESM の側面**に重点を置いている。識別情報とクレデンシャル情報を管理する製品は、エンタープライズ内に存在するサブジェクトへクレデンシャル情報を生成し発行する。また、これらのサブジェクトと関連付けられた組織的属性の維持も行う。サブジェクトが自分の識別情報を検証する手段を提供し、これらのサブジェクトとエンタープライズとの関係性を決定することにより、識別情報とクレデンシャル情報の管理製品はエンタープライズの責任追跡性とアクセス制御をサポートできる。

一意であいまいさのない識別情報の確立は、クレデンシャル情報や認証属性の発行と管理を可能とする重要で基盤的な機能である。識別情報という概念は、クレデンシャル情報や属性データを関連付けることのできる個人へ割付けられた、その一意の識別子を意味する。

個人が ESM システム内の利用者として識別されるためには、登録 (enroll) されなければならない (must)。登録とは、サブジェクトへ一意の識別子を割付け、クレデンシャル情報を生成及び発行し、利用者へ属性を定義し、そしてこれらのデータを利用する任意のリポジトリへ伝達する行為を意味する。TSF には、これらのコンポーネントへこのデータをセキュアに送信できることが必要とされる。

本 PP に適合する TOE には、以下のふるまいを示すことが期待される。

- サブジェクトの配備 (新たなサブジェクトを組織のリポジトリへ登録し、組織に定義された属性をサブジェクトへ関連付けたり関連付けを削除したりすること)
- 利用者の識別情報と関連付けられたクレデンシャル情報の発行及び維持

- クレデンシャル情報の状態の公表と変更 (有効、保留、あるいは終了など)
- 自分自身と、互換性のあるポリシー管理及び認証サーバ ESM 製品との間の適切な高信頼チャネルの確立
- 構成変更及びサブジェクトの識別と認証アクティビティの監査証跡の生成
- 監査データの高信頼リポジトリへの書き込み
- 高信頼チャネルを介した識別情報とクレデンシャル情報の属性データのセキュアな送信

本 PP では、あたかも TOE がスタンドアローン製品に属しているかのように TOE の機能を定義しているが、これらの機能の一部または全部は ESM ポリシー管理 (PM) 製品にも属しているかもしれない。本 PP への適合を主張する ST が作成される場合、これらの機能の配分が明確に描写されなければならない (must)。

本 PP が、ESM PP ファミリ中の数多くのプロテクションプロファイルのひとつであることに注意すること。本 PP は単独ではなく、ESM システム中のひとつのコンポーネントとしての利用が意図されている。最低限、少なくとも 1 つの互換性のある認証サーバ製品が識別されなければならない (must)。互換性は、TOE により定義される識別情報とクレデンシャル情報を認証するその製品の能力により定義される。組織内でアクセス制御が実装される方法により、ポリシー管理やアクセス制御、そして監査のための ESM PP ソリューションも実装が必要となるかもしれない。これらのコンポーネントのいずれかが組織のベースラインを背景として展開されることが期待される場合、セキュア構成管理ソリューションもまた展開される必要があるかもしれない。顧客がすべて該当する ESM PP 評価済み製品を利用せずにソリューションを展開した場合、エンタープライズアーキテクチャの全体的なセキュリティを深刻に危殆化させてしまうおそれがある。

図 1 に、TOE が展開されることが期待される文脈を基本的なレベルで示した。TOE はシステム上に存在し、1 つ以上のサブジェクトデータのリポジトリへのインタフェースを提供する。1 人以上の割付管理者へ、TOE を利用してこのデータを必要に応じて操作する権限が与えられる。サブジェクトデータは、他の ESM コンポーネントがそれぞれの職務を遂行するために必要に応じて用いられる。例えば、ポリシー管理者は、ある部門のメンバーに特定の Web アプリケーションへのアクセスを権限付与するポリシーを作成しようとするかもしれない。これを行うためにポリシー管理製品は、この部門への所属を明示する属性か、そこに属するサブジェクトのリストのいずれかを取り出すことができなければならない (must)。これは、関連するリポジトリのデータへアクセスすることにより行われることになる。

また監査データも高信頼リポジトリへ書き込むことができ、そこで ESM 監査サーバの標準プロテクションプロファイルに準拠した製品により他のデータストリームと共に集計できる。

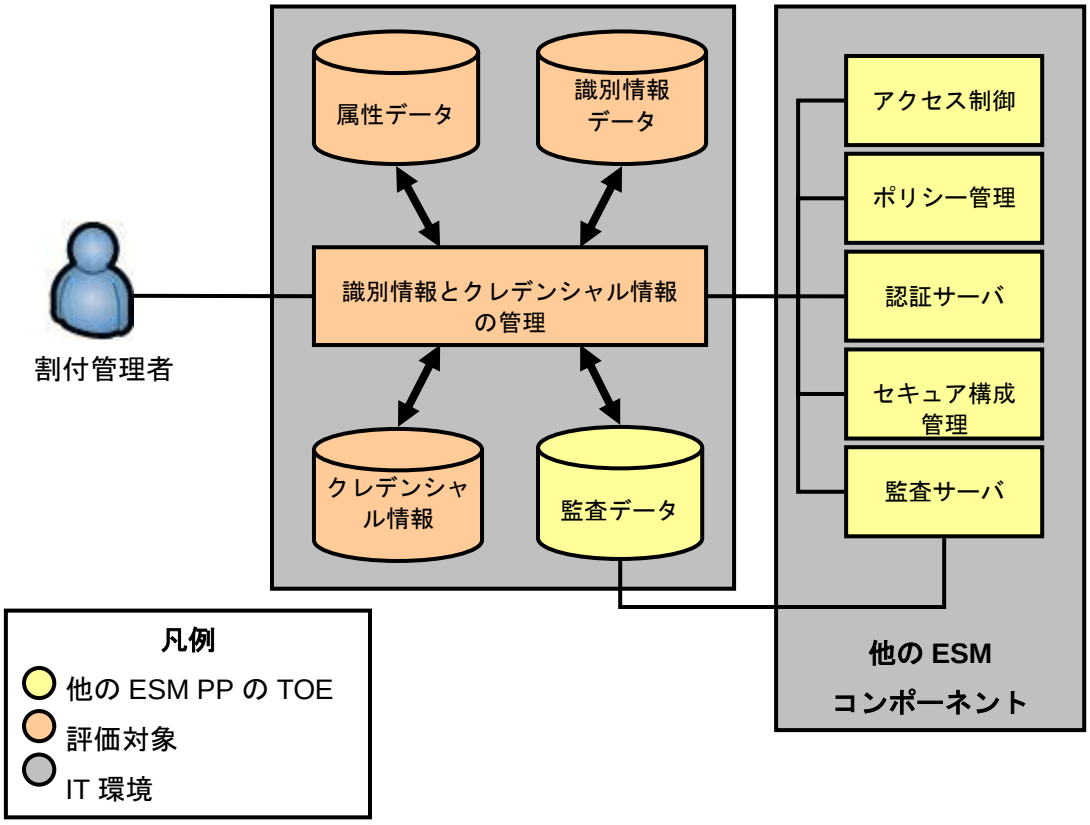

図 1. プロテクションプロファイルの文脈

1.4 適合評価対象

識別情報とクレデンシャル情報管理製品の目的は、エンタープライズ内で識別情報とクレデンシャル情報を管理し、属性を利用者と関連付けることである。また、これらの属性の一部またはすべてを維持する能力を持つかもしれない。これにより、ESM ソリューションが全体としてエンタープライズ内でアクションを行う個人を識別でき、また識別されたサブジェクトの特権に基づいて他の ESM が適切なアクションを取ることができる。

TOE はハードウェアとして、ソフトウェアとして、冗長性のある分散システムとして、またはサーバ上の単一のエージェントとして展開される可能性がある。TSF は、本プロテクションプロファイルの節 6 に規定されたすべての機能を含まなければならない (must)。TOE は、本プロテクションプロファイルの附属書 C に指定されるオプションの SFR のいずれかを主張してもよい。これがなされた場合、TOE のセキュリティターゲットにより、

本プロテクションプロファイルの節 7 に定義されたセキュリティ課題定義へ適切な置き換えが行われなければならない (must)。オプションの SFR を取り込むことは、正確適合への違反とはみなされない。これらの状況を取り扱うための具体的な指示が、証拠資料の開発者と評価機関の両方に提供されるからである。

TOE は、より大規模な ESM システム内のサブシステムであることが期待される。ESM 製品全体が、すべての適用される ESM プロテクションプロファイルに対して評価されることが期待される。

1.5 共通機能

本プロテクションプロファイルでは、ある ESM 設定において識別情報とクレデンシャル情報の管理を行うことが可能なすべての製品により満たされることが期待される要件のセットを定義する。識別情報の管理とは、エンティティへ一意の識別子を定義することを意味する。これらの識別子は次に属性の集合と関連付けられ、この属性の集合は他の製品により、これらのエンティティが ESM の展開中のオブジェクトと相互作用することが許可される範囲を決定するために用いられる。クレデンシャル情報の管理は、識別情報の主張 (claim) または属性の主張 (assertion) をサポートするために用いられる、クレデンシャル情報の保証された生成と検証を提供する。利用者が特定のサブジェクトとしての認証を成功させると、そのサブジェクトが関連付けられた識別情報データは、エンタープライズ内でのそのアクティビティの継続期間中、それへ束縛される。

ESM プロテクションプロファイルへの適合を主張する製品が、**組織的に定義される**サブジェクト及び属性を取扱うことは必須である。言いかえれば、TOE は、可能な限り、利用者の既存の組織のリポジトリと利用者属性を利用すべきである (should)。ESM 製品の意図は、サブジェクトの*集中化された*定義と属性データを提供することである。ST 作成者は、TOE が利用する組織のデータ、データが受信される信頼されるソース、及び (SAML アサーションや X.509 証明書のような) このデータが解釈されるメカニズムを定義しなければならない (must)。

シングルサインオン (SSO) または外部属性の権威ある検証を利用するために複数ドメインが統合される場合に、フェデレーションと呼ばれる。フェデレーションは、潜在的に、同一製品の複数インスタンス間や 2 つの異機種の製品間で確立される可能性がある。TOE がフェデレーションを確立できる場合、ST 作成者はその実現方法を示さなければならない (must)。また、バックエンドチャネルを介して TOE が外部エンティティと交換する属性があれば、その属性及びその交換が行われる方法についても言及が必要である。

1.6 関連するプロテクションプロファイル

本プロテクションプロファイルは、エンタープライズセキュリティ管理 (ESM) 製品を対象として作成された一連のプロテクションプロファイルの一つである。以下のプロテクションプロファイルが、本プロテクションプロファイルを補完する。

- ESM アクセス制御の標準プロテクションプロファイル
- ESM ポリシー管理の標準プロテクションプロファイル
- ESM 監査管理の標準プロテクションプロファイル
- ESM セキュア構成管理の標準プロテクションプロファイル
- ESM 認証サーバの標準プロテクションプロファイル

本プロテクションプロファイルへの適合を主張する製品は、互換性のある環境製品であって他のプロテクションプロファイルへ適合するものを識別することが期待される。しかし、本プロテクションプロファイルのスイートは生まれたばかりであるため、すべての依存する製品にプロテクションプロファイルへの適合を義務付けることは、まだ可能ではない。検証されていない依存する製品は、関連する国家スキームによるケースバイケースの決定に基づいて、運用環境の受容可能な一部であるとみなすことができる。

1.7 複数のプロテクションプロファイルの主張

ESM ファミリのプロテクションプロファイルでは、類似した、また相補的な機能が数多く定義されている。数多くの製品が、同一の TOE の一部として、複数の PP の機能を実装することが予測される。以下のガイドラインは、セキュリティターゲットの著者及び評価機関が、そのような製品を正しく効果的に表現できるよう導くための例と共に開発されたものである。

- TOE が複数の PP への互換性のある機能を実行する場合、すべての該当する PP への適合が主張されなければならない (must)。

例：環境の資源へのアクセス制御を行うメカニズムと、このメカニズムを構成する手段との両方を提供する単一の製品は、アクセス制御 PP とポリシー管理 PP の両方への適合を主張することが期待される。

例：システムまたはアプリケーションのセキュリティ設定の構成と、これらのエンティティのログ記録の集計の両方に利用できる単一の製品は、監査サーバ PP とセキュア構成管理 PP の両方への適合を主張することが期待されるかもしれない。

- 複数の PP が主張された場合、重複する SFR は、その SFR の個別のコピーそれぞれがそれ自体として満たされることが明らかである限り、集約されてもよい。

例：識別情報とクレデンシャル情報管理 PP と認証サーバ PP の両方への適合を主張する単一の製品は、各 PP の個別の FAU_GEN.1 要件が主張され、その後満たされている限り、FAU_GEN.1 を単一の繰返しとして表現してもよい。

- 複数の PP が主張される場合、異なる SFR やセキュリティ課題定義エレメントであって同一の名称を持つものは、それぞれの元のソースが明確に参照された上で、両方とも取り込まれなければならない (must)。

例：脅威 T.FORGE は、アクセス制御 PP とポリシー管理 PP の両方に、異なる言い回しで存在する。両方の PP への適合を主張する製品は、これらの脅威の両方を低減しなければならない (must)。ST には、この脅威の両方のインスタンスが、どちらのインスタンスがどちらの主張される PP からのものかという識別と共に、取り込まれなければならない。

- 複数 PP の主張に、トランザクションの「両端」の 2 つの SFR が定義される場合、両側が一貫していなければならず (must)、またテストの単一の繰返しで十分である。

例：アクセス制御 PP とポリシー管理 PP の両方への適合を主張する単一の製品は、アクセス制御ポリシーの定義と利用の両方を行うための要件を持つことになる。この場合、定義されるべきポリシーデータを定義する割付と、利用されるべきポリシーデータを定義する割付は、同一になることが期待される。そして、これらのポリシーの定義及び利用を行う TOE の能力のテストは、同時に行われる。

- 主張される PP の一方が、他の主張される PP の一部である機能について運用環境を参照している場合、この機能は TSF の一部であると解釈されなければならない (must)。

例 1：アクセス制御 PP では、運用環境中のポリシー管理製品から TOE がアクセス制御ポリシーを受け取ることが前提となっている。しかし、製品がアクセス制御 PP とポリシー管理 PP の両方への適合を主張する場合、これらのポリシーは実際には運用環境ではなく、TOE の別の部分から受け取られることになる。これは、各 PP が個別のコンポーネントの視点から書かれているためである。このような場合、どんな場合に「運用環境」が実際には「他の主張される PP の TSF であって TOE の一部でもある」を意味するのか、明確にすることが期待される。

例 2：拡張要件 ESM_EAU.2 のタイトルは、「エンタープライズ認証への依存」となっている。この要件の意図は、TOE が認証サーバに、自分の代理として管理者の認証を取り扱う

ことを許可することである。製品が、識別情報とクレデンシャル情報管理 PP に加えて認証サーバ PP への適合を主張する場合、その製品が依存する「エンタープライズ」認証は、実際には自分自身の認証サーバコンポーネントである。このような場合、依存される特定のコンポーネントを TOE が含むため、TOE がこの機能の提供を自分自身に依存することを明確にすることが期待される。

- 複数の PP への適合を主張する TOE がコンポーネント間のリモートネットワークインタフェースを持っている場合、これらのインタフェースは文書化及びテストの目的については外部インタフェースとして取り扱われなければならない (must)。

例：アクセス制御 PP とポリシー管理 PP の両方への適合を主張する TOE が、各コンポーネントを異なるシステムに配置しているかもしれない。2 つの TOE コンポーネント間のインタフェースが技術的には内部インタフェースである場合でも、ST 作成者はこのインタフェースを FTP_ITC.1 に関して論じなければならない (must)。その後評価者は、あたかもこのインタフェースが TSF と運用環境との間の接続を表現しているかのように、テストしなければならない (must)。

これらの結合ルールは、ST 作成者へのその他の任意のガイダンスと共に、ST 開発中には遵守され、また ST 評価プロセスの一部としてチェックされるべきである (should)。ESM スイートが成熟するに従って、ASE 保証アクティビティがチェックされる対象となるこれらの ST 開発ステートメントのすべてを取り込む付属文書が開発されることになる。

1.8 文書の構成

第 1 章では、プロテクションプロファイルの概論的資料が提供される。

第 2 章では、プロテクションプロファイルへ該当する適合主張が言明される。

第 3 章では、TOE に対して行われる可能性のある脅威の種類が定義される。

第 4 章では、TOE が満たすことを期待される対策方針が定義され、これらの対策方針への適合を例証するセキュリティ機能要件が列挙される。

第 5 章では、本プロテクションプロファイル中で用いられる拡張コンポーネントが定義される。

第 6 章では、TOE がプロテクションプロファイルに適合するために主張されなければならない (must) セキュリティ機能要件及びセキュリティ保証要件が列挙され、説明される。

第 7 章では、プロテクションプロファイルで定義された前提条件、脅威、対策方針、及び

要件の間の対応付けが提供される。

第 8 章では、プロテクションプロファイルに適用される前提条件、脅威、及び対策方針が定義される。

本文書には、以下の附属書も含まれる。

- 0 (訳注 :「附属書 A」の間違い) この附属書では、参考資料のリストを提供し、本文書において使用されている頭字語が定義される。
- 附属書 B - 認証と認定の活動への TOE の適合性が迅速に識別できるよう、プロテクションプロファイルのその他の標準との関係について記述する。
- 附属書 C - 適合 TOE に取り込むことができるオプションの要件、これらのオプションの要件において取り込まれなければならない環境、及びその要件が満たされていることを検証するために評価者により実行されるべき保証アクティビティを定義する。
- 附属書 D - 文書中において使用される表記法について記述する。
- 附属書 E - 文書中において使用される用語を定義する。
- 附属書 F - 正式な PP 識別情報を提供する。

2 適合主張

2.1 CC 適合主張

本プロテクションプロファイルは、*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* バージョン 3.1 改定第 4 版 2012 年 9 月 (CCMB-2012-09-001) に適合している。

本プロテクションプロファイルは、CC パート 2 拡張及び CC パート 3 に適合する。

2.2 PP 適合主張

本プロテクションプロファイルは、いかなる他の PP への適合をも主張しない。

2.3 パッケージ適合主張

本プロテクションプロファイルは、要件追加された EAL1 のパッケージであることを主張する。

2.4 ST 適合要件

本プロテクションプロファイルへの適合を主張するセキュリティターゲットは、CC パート 1 の節 D.2 に定義される正確 PP 適合の最低基準を満たさなければならない (must)。

ST は、本 PP の節 6 に定義される保証要件をすべて取り込むことにより、本 PP への正確適合を主張しなければならない (must)。ST は、PP の附属書 C に定義される 1 つ以上のオプション要件を追加的に主張してもよい。ST 作成者は、前提条件、TOE の対策方針、及び環境の対策方針を、主張されるオプション要件及び PP の節 7 に提供される指示と一貫した形で作成しなければならない (must)。

本 PP では、規定された要件の意図と、ベンダが要件を満たすための方法に関する期待とを、さらに明確化し説明するために、適用上の注意が提供される。ST の評価者には、ST 及びその記述された TOE が本 PP 中のすべての言明を含むだけでなく、適用上の注意により言明される期待をも満たすと決定することにより、正確適合を保証することが期待される。

保証に関しては、本 PP に含まれるものと同一の保証要件が ST に含まれることと、本 PP 中に言明されるすべての保証アクティビティが行われることが期待される。

TOE が、本 PP に関連するが PP に記述されていない機能を公開していると ST 作成者が信じる場合、ST 作成者にはその国家検証スキーム及び ESM 技術コミュニティに相談し、本文書へオプションの機能を追加する可能性について議論することが推奨される。

3 脅威

以下の節では、TOE に適用される脅威を列挙する。

3.1 管理者の過誤

悪意を持つか不注意な管理者が、定義されたセキュリティ要件と一貫性のないやり方で TOE を構成または運用する場合、TOE により提供されるセキュリティ機能は的外れになってしまうかもしれない。例えば、そのようなセキュリティ機能は暗号化された通信を有効としなかったり、適切なパスワードポリシーを構成しなかったり、あるいは過剰な管理特権を必要としない利用者へ割り当てたりするかもしれない。TSF により完全にそのような事故を防止することはできないが、明確な管理ガイダンスを配付することにより意図しない過誤を減らすことが期待でき、また (受容不可能な利用方法のもたらす結果を明確に列挙した) 受容可能な利用方法のバナーの表示により、悪意のあるアクティビティのいくぶんかを思いとどまらせることができるかもしれない。

[T.ADMIN_ERROR]

3.2 クレデンシャル情報、識別情報、及び ESM データの暴露

エンタープライズセキュリティ管理アーキテクチャは、機能するためにリモートデバイス間でデータが送信されることをほぼ保証必要とする。TOE は、ESM 展開内のリモートリポジトリへ、クレデンシャル情報または属性データ、あるいはその両方を送信するかもしれない。また TOE は環境内の別の場所からリモートで検証されるべきデータを受信するかもしれないし、リモートに配置された集中リポジトリへ監査データを書き込むかもしれない。これらのデータが通過中、十分にセキュアな高信頼チャネルにより保護されていなければ、意図せぬ暴露が引き起こされるかもしれない。これらのデータへアクセス可能な攻撃者は、それを偵察目的に利用したり、あるいは既知の有効な情報をリプレイすることにより有効な利用者またはエンティティへのなりすましを試みたりすることができてしまう。

[T.EAVES]

3.3 TOE 機能への不当なアクセス

TSF がその管理者を適切に識別、認証、及び権限付与しなければ、その管理機能が適切に実行されているという保証は存在しないことになる。認証機能の設計または実装が不十分であれば、攻撃者がネットワーク上で盗聴を行って、本物の認証情報を盗み出して利用したり、認証機能を完全にバイパスしたりできてしまう。認証機能の堅牢さが不十分であれ

ば、力ずくの推定による不法な侵入のおそれが増大する。データ保護機能の設計または実装が不十分であれば、アクセス制御チェックがバイパスされ、特権昇格が可能となってしまう。攻撃者が識別情報データを管理する能力へ不法にアクセスする手法がどうであれ、その結果として生じる組織の識別情報とクレデンシャル情報管理の完全性が危殆化することは同じである。

[T.UNAUTH]

3.4 偽の TOE 保証

TOE により作成された情報が信頼されたソースからのものであり、適切に実施されるべき (should) ものであるという保証を提供するため、TOE は依存する製品へその真正性を主張することが可能であるべきである (should)。しかし、通信チャネルが暴露から十分に保護されていなければ、攻撃者がデータの配付を傍受して、依存する製品へ偽の識別情報またはクレデンシャル情報あるいはその両方を提供できるかもしれない。結果として、これらの依存する製品は正しいデータを利用せず、運用の観点からは全く不具合が見当たらないため、それに引き続くセキュリティ違反を検出することがより困難となってしまう可能性がある。

[T.FALSIFY]

3.5 偽の識別情報とクレデンシャル情報の対応付け

TOE は、依存する製品へ識別情報とクレデンシャル情報を提供するため、これらと通信を行わなければならない (must)。このデータを伝送するために用いられる通信チャネルが適切に保護されていなければ、攻撃者はトラフィックを傍受して改変し、偽の識別情報とクレデンシャル情報の対応付けや認証判断を提供することが可能となり、ESM アーキテクチャの全体的な機能を崩壊させてしまうかもしれない。あるいは、TOE が例えばフェデレーションに含まれるような属性データの別個の権威あるソースとインタフェースする場合、攻撃者がこのインタフェースを用いて無効な属性データを TOE へ提供できるかもしれないという脅威が存在する。これにより攻撃者は、保護されたリソースへアクセスが可能となったり、正当な利用者がアクセスできるべき (should) オブジェクトや機能へアクセスすることを禁じたりできるようになる可能性がある。

[T.FORGE]

3.6 隠ぺいされたアクション

組織内にエンタープライズセキュリティ管理ソリューションを実装する理由のひとつは、透明性 (transparency) と責任追跡性 (accountability) を提供することである。このため、

TOE には自分の識別情報とクレデンシャル情報管理機能の実施を監視し監査する機能を提供することが期待される。攻撃者が監査データを改変したり、その記録を妨害したりできるとすれば、発見されるリスクを減らしながらシステムの弱点を探ることが可能となってしまう。同様に、TOE が自分自身に対して取られた異常な、または悪意のあるアクションの識別や監査を行わなかったとすれば、検出されずにそのふるまいが改変される可能性が存在することになる。もしこのようなことが発生した場合、そのセキュリティ機能が適切に動作していることは保証できなくなるであろう。

[T.MASK]

3.7 不十分な属性

識別情報とクレデンシャル情報の管理製品は、互換性のある ESM 製品が利用できる十分な属性を提供するポリシーを作成できなければならない (must)。不十分な属性は、意図しないアクティビティを許可したり間違って正当な利用を制限したりするため、アクセス制御の効果をなくしてしまうおそれがある。

[T.INSUFFATR]

3.8 弱い認証機能

管理特権を定義する TSF の能力は、TSF の認証機能に力ずくの推定を行うことが可能であれば、悪意のある利用を防止することはできない。TSF は、攻撃者が力ずくで TOE への認証を行う能力を制限するために、十分なログイン障害 (frustration) メカニズムを提供しなければならない (must)。

[T.WEAKIA]

3.9 クレデンシャル情報の不十分な保護

クレデンシャル情報が送信中に保護されていたとしても、それらが TOE プラットフォーム上で保存されている際に保護されるとは限らない。TOE は、抽出やリプレイが引き起こされないような形態で、クレデンシャル情報を保存しなければならない (must)。

[T.RAWCRED]

4 セキュリティ対策方針

以下の節では、TSF により満たされることが期待されるセキュリティ対策方針を記述する。TOE が複数のエンタープライズセキュリティ管理 PP への適合を主張する場合、他の ESM 製品またはコンポーネントへの任意の参照は、TOE の分散コンポーネントへの参照と解釈される。TSF は、対策方針が適用されるインタフェースが運用環境へのものであるか TOE の分散コンポーネントへのものであるかにかかわらず、対策方針を満たすことが期待される。

オプションの SFR (附属書 C に定義される) の取り込みまたは除外は、TOE により主張される対策方針及びそれを満たす SFR に影響する。オプションの SFR の取り込みまたは除外により、セキュリティ課題定義がどのような影響を受けるかに関するガイダンスについては、節 7 を参照すること。

4.1 ESM コンポーネントの検証

TOE は他の ESM 製品へセキュリティデータを提供する責任を負う可能性があるため、TSF が潜在的受信者の識別情報を検証できることは重要である。さらに、TSF はそれ自身の識別情報を確認するための情報を提供して、他の ESM コンポーネント (または、それ自体の分散コンポーネント) が受信したデータが有効であることを保証できるようにすべきである (should)。最後に、コンポーネント間で送信されるデータは、通過中に暴露から保護されなければならない (must)。これらの機能が実装されなければ、組織のセキュリティデータが危殆化し、さらなる攻撃の土台を提供してしまうおそれがある。

(O.ACCESSID, O.EAVES, O.SELFID: ESM_EID.2, FTP_ITC.1)

4.2 システム監視

不正な TOE の構成変更や保護されたオブジェクトに対する悪意のあるアクティビティの試行を識別するため、TOE には監査イベントを生成する能力を提供することが期待される。この監査証跡は、サブジェクトデータへの変更及び、ESM アーキテクチャに応じて、認証機能の利用を識別することにより、システムの動作への管理的知見を提供できるべきである (should)。TOE のアーキテクチャに応じて、監査データは TOE の内部へ、あるいは外部リポジトリへ、保存され得る。

本 PP は、監査リポジトリがアクセス不可能である場合に何らかの特定のアクションが取られることを義務付けてはいない。ST 作成者は、この場合に TOE が示すふるまいを文書化すべきである (should)。

(O.AUDIT: FAU_GEN.1, FAU_SEL.1 (オプション), FAU_STG_EXT.1, FPT_STM.1 (オプション))

4.3 堅牢な TOE アクセス

巧妙でない攻撃者が推定を繰り返して TOE への不法な認証を試行した場合、それが成功する確率は以下の 2 つの要因に依存する。認証機能へアクセスしている時間にどれほどの数の認証試行を行うことができるかと、個別の試行が成功する確率である。TOE には、これらの要因のそれぞれに対してセキュリティを向上させるメカニズムを実装するか、あるいはそれを行う外部定義された認証ポリシーを実施するか、いずれかが期待される。また TOE は (附属書**エラー！ 参照ソースが見つかりません。（訳注：C.4 ）**に定義されるオプションの SFR により) セションの確立を拒否したり、確立されたセションを中断または終了させたりする機能を提供することもできる。

管理者のクレデンシャル情報と認証が運用環境により取り扱われる場合、TSF へ堅牢なアクセスを提供する責任は適切なポリシーを定義する運用環境エンティティへ課される (OE.ROBUST)。

(O.ROBUST: FIA_AFL.1 (オプション), FIA_SOS.1 (オプション), FTA_TSE.1 (オプション), FTA_SSL_EXT.1 (オプション), FTA_SSL.3 (オプション), FTA_SSL.4 (オプション))

4.4 機密通信

TOE は、他の ESM 製品 (または、それ自体の分散コンポーネント) へ、及びそれらから伝送される監査、ポリシー、識別情報、あるいはクレデンシャル情報の機密性と完全性を保護するために、十分に強靭で十分に信頼できる暗号アルゴリズムを用いて、TOE への、及び TOE からの、あるいは分散 TOE コンポーネント間の通過中のデータを保護すべきである (should)。運用環境から伝送される ESM 関連データを保護しなければ、攻撃者がデータを学習して運用環境の別の部分を危殆化させることを助けてしまうかもしれない。これらの通過中のデータを保護するため、TOE には暗号プロトコルを実装することが期待される。しかし、プロトコルにより使用される暗号プリミティブは TOE により実装されてもよいし、運用環境により提供される機能を用いてもよい。セキュアなチャネルが確立されてしまえば、それ以降、必要に応じてエンタープライズにわたって ESM データを送信するためにそれは使われることになる。

(O.ACCESSID, O.AUTH, O.INTEGRITY, O.PROTCOMMS, O.SELFID: ESM_ACT.1, ESM_EAU.2, ESM_EID.2, FCS_IPSEC_EXT.1 (オプション), FCS_SSH_EXT.1 (オプション), FCS_TLS_EXT.1 (オプション), FCS_HTTPS_EXT.1 (オプション), FIA_USB.1, FMT_MOF.1, FPT_SKP_EXT.1, FTP_ITC.1, FTP_TRP.1)

4.5 保護されたクレデンシャル情報

送信されるクレデンシャル情報を保護することは、クレデンシャル情報保護の全体像の一部にすぎない。クレデンシャル情報が TOE により保存される際に、それが生の平文の形でアクセスできず､またその後リプレイされて利用者へのなりすましに利用されないよう、保護することも不可欠である。

(O.PROTCRED: FPT_APW_EXT.1)

4.6 識別情報の定義

TOE の主要な目的は、識別情報データの属性の権威としての役目を果たすことである。これを行うため、TSF は利用者を定義し、利用者に属する識別情報属性を定義し、そして必要な際にこのデータを他の ESM コンポーネントへセキュアに送信できなければならない (must)。さらに、エンタープライズのニーズに応じて、TSF は人間以外のエンティティ (NPE) またはオブジェクトを定義し、その属性を維持し、そしてその属性を送信できる必要があるかもしれない。

(O.IDENT, O.EXPORT: ESM_ICD.1, ESM_ICT.1, ESM_ATD.1 (オプション))

4.7 完全性の保証

TOE は、他の ESM コンポーネントから取得したセキュリティ情報の完全性を検証するために､自分が受信する暗号化されたデータを解釈できなければならない (must)。また TOE は、自分が他の ESM コンポーネントへ送信するデータが信頼されるように、その完全性を主張するメカニズムを提供しなければならない (must)。この対策方針の意図は、改変されていないことが証明できるデータにのみ基づいて TOE が動作することを保証することである。またこの対策方針は、TOE から発せられるデータの完全性が検証可能であることも保証している。TOE は、内部に暗号機能を取り込むか、サードパーティのオペレーティングシステムや暗号スイートを活用して暗号機能を提供することが期待される。

(O.INTEGRITY: FTP_ITC.1)

4.8 正当な管理

識別情報とクレデンシャル情報の管理を適切に促進するため、TSF は何らかの方法でサブジェクトデータの定義と変更を可能としなければならない (must)。このことに加えて、TSF は自分のふるまいに関して管理権限を持つことが許可されている個人と、その権限が適用されるべき (should) 範囲を決定できなければならない (must)。これにより、ESM の他の部分により利用されるセキュリティデータが信頼できる個人によりのみ変更されることを保証する。

(O.AUTH, O.MANAGE: ESM_EAU.2, ESM_EID.2, FIA_USB.1, FMT_MTD.1 (オプション), FMT_SMF.1, FMT_SMR.1, FTP_TRP.1)

4.9 アクセスバナー表示

TOE の適切な使用方法に関するガイダンスが遵守される確率を高めるため、認証に先立ってその受容可能な使用方法を定義するバナーを表示することが TOE には期待される。またこれにより監視の法的な通告が行われるため、何らかの法的な捜査があった場合に監査データが証拠として認められることが可能となる。

(O.BANNER: FTA_TAB.1)

4.10暗号サービス

TOE は、送信する識別情報データの機密性及び完全性を保証するために、また必要に応じてそれ自身と運用環境との間の高信頼通信を提供するために、暗号プリミティブ (暗号化、復号、ランダムビット生成など) を利用できなければならない (must)。これらのサービス自体は、TOE の一部であってもよいし (O.CRYPTO)、運用環境により実装されてもよい (OE.CRYPTO)。

(O.CRYPTO: FCS_CKM.1 (オプション), FCS_CKM_EXT.4 (オプション), FCS_COP.1(1) (オプション), FCS_COP.1(2) (オプション), FCS_COP.1(3) (オプション), FCS_COP.1(4) (オプション), FCS_RBG_EXT.1 (オプション))

5 拡張コンポーネントの定義

本節では、本 PP 内で記述されるすべての拡張コンポーネントの定義が提供される。これには、節**エラー！参照ソースが見つかりません。（訳注：）**に指定される要求されるコンポーネントと、附属書 C に指定されるオプションのコンポーネントの両方が含まれる。

一部の拡張クラスとファミリは複数の拡張要件を参照しているが、その一部のみが本 PP で実際に利用されていることに注意すること。これは、読者に拡張ファミリの適用範囲をよりよく認識してもらうため、及び PP にまたがって一貫性のある形で提示するためである。TOE の適用範囲が本 PP 自体に制限される場合、ここで議論されるが節 6.1 には含まれない拡張コンポーネントは取り込まれないことになる。

5.1 ESM クラス：エンタープライズセキュリティ管理

ESM クラスは、集中化されたアクセス制御、認証、セキュアな構成、及び監査ポリシーの定義、利用、及び実施をサポートする機能要件を規定する。このクラスで定義される機能要件は、エンタープライズセキュリティ管理の目的を達成するために TSF が運用環境と相互作用する具体的な手法を定義することにより、CC パート 2 で定義されるものとは異なっている。

5.1.1 ESM_ATD 属性の定義

ファミリのふるまい

本ファミリの要件により、後にアクセス制御ポリシーの定義と実施に用いることのできる運用環境の属性に関する属性を、権威を持って定義する能力を TSF が有することを保証する。

コンポーネントのレベル付け

本ファミリには、ESM_ATD.1 及び ESM_ATD.2 という 2 つのコンポーネントが存在する。これらは、互いに階層構造をなしていない。ESM_ATD.1 オブジェクト属性の定義は、TSF がポリシーに関連したオブジェクト属性の何らかのセットを定義できることを要求する。ESM_ATD.2 サブジェクト属性の定義は、TSF がポリシーに関連したサブジェクト属性[3]の何らかのセットを定義できることを要求する。両方の場合で、これらの属性は後に制御下

[3] 別の言い方をすれば、アクセス制御コンポーネントにより実施されるポリシーに関連した属性。サブジェクトは、識別情報及びクレデンシャル情報に関連した追加的属性を持っているかもしれない。サブジェクト属性の管理を行う能力は、ポリシー管理コンポーネントにおいてはオプションである。システム設計者は、その能力を識別情報とクレデンシャル情報管理コンポーネントの中で提供することを選択してもよい。

にある運用環境中のエンティティと関連付けられ、アクセス制御の取り扱いに用いられることが期待される。オブジェクト属性の例としては、実施アクセス制御 (MAC) 環境に用いられるセキュリティラベルや、組織のイントラネット内に存在するウェブページと関連付け可能な保護レベルが挙げられる。サブジェクト属性の例としては、定義済み識別情報と関連付けられるであろうクリアランスまたは MAC 範囲が挙げられる。

5.1.1.1 ESM_ATD.1 オブジェクト属性の定義

ESM_ATD.1 コンポーネントは、オブジェクト属性の規定に関する要件を定義する。これにより、TSF により定義される属性データを他の ESM 製品が利用して、それら自身のセキュリティ機能を実施することが可能となる。ESM_ATD.1 要件が付け加えられた理由は、運用環境中に存在するオブジェクトと関連付けられる属性を定義する TSF の能力に関する要件が、CC パート 2 には欠けているためである。

下位階層：	他のコンポーネントなし
依存性：	依存性なし。
ESM_ATD.1.1	TSF は、個別オブジェクトに属するセキュリティ属性の以下のリストを維持しなければならない (shall)： [***割付：オブジェクトセキュリティ属性のリスト***]。
適用上の注意：	*オブジェクトセキュリティ属性は、最終的にアクセス制御の決定の際に考慮されるが、利用者にもポリシーにも関連付けられていない属性を意味する。マルチレベルのセキュリティのアクセス制御ポリシーを定義する TOE は、資源と関連付け可能なセキュリティラベルを定義して、ポリシーがこれらの資源へ適用できるようにする必要があるかもしれない。*
ESM_ATD.1.2	TSF は、セキュリティ属性を個別オブジェクトと関連付けることができなければならない (shall)。

管理：ESM_ATD.1

以下のアクションは、FMT における管理機能とみなすことができる：

a) オブジェクト属性の定義。

b) 属性とオブジェクトとの関連付け。

監査： ESM_ATD.1

ESM_ATD.1 オブジェクト属性の定義が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should) :

a) 最小：オブジェクト属性の定義。

b) 最小：属性とオブジェクトとの関連付け。

5.1.2 ESM_EAU エンタープライズ認証

ファミリのふるまい

本ファミリの要件により、TSF が管理者、利用者、またはその他のサブジェクトを認証する目的で外部エンティティと相互作用する能力を有することを保証する。

コンポーネントのレベル付け

本ファミリには、ESM_EAU.1、ESM_EAU.2、ESM_EAU.5、及び ESM_EAU.6 という 4 つの非階層コンポーネントが存在する。

ESM_EAU.1 エンタープライズ認証は、TSF が外部エンティティの定義済みのセットから認証要求を受信し、何らかのプロトコルを用いてそれらを検証し、そして要求を行ったエンティティへ決定の結果を返すことができることを要求する。ESM_EAU.1 は、認証サーバの能力に特有である。従って、これについては ESM 認証サーバのプロテクションプロファイルでのみ、さらに論じられる。

ESM_EAU.2 エンタープライズ認証への依存は、ESM_EAU.1 の逆である。これは TSF に、認証を運用環境で行わせ、そしてそれをあたかも TSF が自分で認証を行ったかのように利用することを可能とする。

ESM_EAU.5 複数のエンタープライズ認証メカニズムは、TSF がマルチファクタ認証を提供することを可能とする。ESM_EAU.5 は、認証サーバの能力に特有である。従って、これについては ESM 認証サーバプロテクションプロファイルでのみ、さらに論じられる。

ESM_EAU.6 エンタープライズ再認証は、確立済みのセションについて TSF が再認証チャレンジを発行することを可能とする。ESM_EAU.1 は、認証サーバの能力に特有である。従って、これについては ESM 認証サーバプロテクションプロファイルでのみ、さらに論じられる。

ESM_EAU.5 及び ESM_EAU.6 は、それぞれ FIA_UAU.5 及び FIA_UAU.6 から導出されたものであることに注意すること。これらには、類似性を強調するため、対応する CC パート 2 と同一のコンポーネントレベルがそれぞれ割付けられた。

5.1.2.1 ESM_EAU.2 エンタープライズ認証への依存

ESM_EAU ファミリは、エンタープライズ利用者認証を利用するための要件を定義する。これにより、この属性データを他の ESM 製品が利用して、それら自身のセキュリティ機能を実施することが可能となる。これは、CC パート 2 に指定される FIA_UAU.1 及び FIA_UAU.2 とは異なる。これらの要件は、TSF により仲介されるアクティビティを実行するために TSF への認証を行う利用者へ特有に適用されるためである。ESM_EAU.2 は、TSF が自分自身で認証を行うことを実施されるのではなく、TOE に代わって運用環境へ送付され得る認証要求を発行する能力に適用される。

下位階層：	他のコンポーネントなし。
依存性：	ESM_EID.2 エンタープライズ識別への依存
ESM_EAU.2.1	TSF は、サブジェクト認証を [選択：[***割付： サブジェクト認証を担当する識別された 1 つまたは複数の TOE コンポーネント***]、[***割付： サブジェクト認証を担当する識別された 1 つまたは複数の運用環境コンポーネント***]] に依存しなければならない (shall)。
適用上の注意：	*このように識別されようとしているサブジェクトが TSF の利用者または管理者である場合、1 つまたは複数の割付に 1 つ以上の認証サーバが記入されることが期待される。本プロテクションプロファイルの将来のバージョンは、この割付中に指名されたエンティティがエンタープライズセキュリティ管理認証サーバの標準プロテクションプロファイルに適合することを要求するかもしれない。*
ESM_EAU.2.2	TSF はすべてのサブジェクトに、そのサブジェクトに代わってそれ以外の TSF 仲介アクションを許可する前に、認証が成功することを要求しなければならない (shall)。
適用上の注意：	*TSF が 2 つの異なる手法を利用してサブジェクトの 2 つの異なるセットを認証する場合、ST 作成者はそれぞれの手法についてこの SFR の異なる繰り返しを作成することにより、これを提示しなければならない (must)。*

管理：ESM_EAU.2

以下のアクションは、FMT における管理機能とみなすことができる：

a) TSF に代わって認証を行うために利用されるエンティティの規定。

監査：ESM_EAU.2

ESM_EAU.2 エンタープライズ認証への依存が PP/ST に含まれる場合､以下のアクションが監査可能であるべきである (should)：

a) 最小：認証メカニズムの利用すべて。

5.1.3 ESM_EID エンタープライズ識別

ファミリのふるまい

本ファミリの要件により、TSF が管理者、利用者、またはその他のサブジェクトを識別する目的で外部エンティティと相互作用する能力を有することを保証する。

コンポーネントのレベル付け

本ファミリには、EESM_EID.1 及び ESM_EID.2 いう 2 つの非階層コンポーネントが存在する。

ESM_EID.1 エンタープライズ識別は、TSF が外部エンティティの定義済みのセットから識別要求を受信できることを要求する。これらの識別要求は、次にエンタープライズ認証の入力として利用される。ESM_EID.1 は、認証サーバの能力に特有である。従って、これについては ESM 認証サーバプロテクションプロファイルでのみ、さらに論じられる。

ESM_EID.2 エンタープライズ識別への依存は、ESM_EID.1 の逆である。これにより TSF が、運用環境中で主張された識別情報の有効性を受け入れることができる。

5.1.3.1 ESM_EID.2 エンタープライズ識別への依存

ESM_EID ファミリは、エンタープライズ利用者識別を利用するための要件を定義する。これにより、それに続くエンタープライズ利用者認証の実行が可能となる。これは、CC パート 2 に指定される FIA_UID.1 及び FIA_UID.2 とは異なる。これらの要件は、TSF により仲介されるアクティビティを実行するために識別情報を TSF へ提示される利用者へ特有に適用されるためである。ESM_EID.2 は、TSF が自分自身で識別要求を行うのではなく、運用環境から識別情報を提示され、これを有効なものとして取り扱う能力に適用される。

下位階層： 他のコンポーネントなし。

依存性： 依存性なし。

ESM_EID.2.1 TSF は、サブジェクト識別を [選択：[***割付： サブジェクト識別を担当する 1 つまたは複数の TOE コンポーネント***]、[***割付：サブジェクト識別を担当する 1 つまたは複数の運用環境コンポーネント***]] に依存しなければならない (shall)。

適用上の注意： *このように識別されようとしているサブジェクトが TSF の利用者または管理者である場合、1 つまたは複数の割付に 1 つ以上の認証サーバが記入されることが期待される。本プロテクションプロファイルの将来のバージョンは、この割付中に指名されたエンティティがエンタープライズセキュリティ管理認証サーバの標準プロテクションプロファイルに適合することを要求するかもしれない。*

ESM_EID.2.2 TSF はすべてのサブジェクトに、そのサブジェクトに代わってそれ以外の TSF 仲介アクションを許可する前に、識別が成功することを要求しなければならない (shall)。

適用上の注意： *TSF が 2 つの異なる手法を利用してサブジェクトの 2 つの異なるセットを識別する場合、ST 作成者はそれぞれの手法についてこの SFR の異なる繰り返しを作成することにより、これを提示しなければならない (must)。*

管理：ESM_EID.2

予見される管理アクティビティは存在しない。

監査：ESM_EID.2

予見される監査対象イベントは存在しない。

5.1.4 ESM_ICD 識別情報とクレデンシャル情報の定義

ファミリのふるまい

本ファミリの要件により、後に他の ESM 製品により様々な目的に用いることのできる利用者属性を、権威を持って定義する能力を TSF が有することを保証する。

コンポーネントのレベル付け

本ファミリには、ESM_ICD.1 という唯一のコンポーネントが存在する。ESM_ICD.1 識別情報とクレデンシャル情報の定義は、識別情報またはクレデンシャル情報あるいはその両方の属性の何らかのセットを TSF が定義できることを要求する。これらの属性は、他の

ESM 製品により、これらの製品のセキュリティ要件を満たすために用いられることが期待される。この要件により、例えばエンタープライズ利用者認証に用いられる認証クレデンシャル情報などの属性や、アクセス制御ポリシー定義に用いられる組織の役割属性を定義することも可能かもしれない。

5.1.4.1 ESM_ICD.1 識別情報とクレデンシャル情報の定義

ESM_ICD ファミリは、エンタープライズ利用者属性の定義に関する要件を定義する。これにより、この属性データを他の ESM 製品が利用して、それら自身のセキュリティ機能を実施することが可能となる。ESM_ICD.1 要件が付け加えられた理由は、運用環境中に存在する利用者に関する属性データを定義する TSF の能力に関する要件が、CC パート 2 には欠けているためである。これは、必ずしも TOE へアクセスするとは限らない利用者へ適用されるため、FIA_ATD.1 とは異なる。

下位階層：	他のコンポーネントなし。
依存性：	依存性なし。
ESM_ICD.1.1	TSF は、他のエンタープライズセキュリティ管理製品と共に用いられる識別情報とクレデンシャル情報のデータを定義する能力を提供しなければならない (shall)。
適用上の注意：	*セキュリティ関連の識別情報とクレデンシャル情報の属性は、他の ESM 製品が自分のセキュリティ機能の実施に用いる利用者属性の完全なセットを構成しなければならない (must)。利用者 ID やパスワードなどのデータは、認証に用いられるためセキュリティ関連である。利用者の組織の役割、役職、あるいは地理的な位置などのデータは、アクセス制御ポリシーがこれらのデータを利用することが期待される場合、セキュリティ関連かもしれない。電話番号などのデータは、セキュリティ関連ではないことが多い。*
ESM_ICD.1.2	TSF は、以下のセキュリティ関連の識別情報とクレデンシャル情報の属性をエンタープライズ利用者に定義しなければならない (shall)：クレデンシャル情報のライフタイム、クレデンシャル情報の状態、 [***割付：TSF がエンタープライズ利用者へ関連付けることが可能な任意の追加的セキュリティ関連の識別情報とクレデンシャル情報の属性のリスト***]。
ESM_ICD.1.3	TSF は、一意に識別されるデータを割り当てることにより、エ

ンタープライズ利用者を登録する能力を提供しなければならない (shall)。

適用上の注意：2 人の利用者が、同一のクレデンシャル情報データを持つことは可能である。ESM_ICD.1.3 の意図は、特定のエンタープライズ利用者を一意に識別するように維持される追加的情報が存在すべきである、ということである。

ESM_ICD.1.4 TSF は、定義されたセキュリティ関連属性を登録されたエンタープライズ利用者へ関連付ける能力を提供しなければならない (shall)。

ESM_ICD.1.5 TSF は、エンタープライズ利用者のクレデンシャル情報の状態を問い合わせる能力を提供しなければならない (shall)。

ESM_ICD.1.6 TSF は、エンタープライズ利用者のクレデンシャル情報を失効させる能力を提供しなければならない (shall)。

ESM_ICD.1.7 TSF は、適合性のある認証サーバ ESM 製品にエンタープライズ利用者のクレデンシャル情報を更新する能力を提供しなければならない (shall)。

ESM_ICD.1.8 TSF は、定義されたエンタープライズ利用者クレデンシャル情報が以下の強度ルールを満たすことを保証しなければならない (shall)。

a) パスワードによるクレデンシャル情報については、以下のルールが適用される。

1. パスワードは、以下の文字セットのサブセットから構成されることができなければならない (shall)： [***割付：パスワードの入力に関してTSF でサポートされる文字セットのリスト***] であって、以下の値を含むもの [***割付：サポートされる文字セットのそれぞれについて、サポートされる文字のリスト***]；及び

適用上の注意： *英語の文字セットについては、文字の種類には26 個の大文字、26 個の小文字、10 個の数字、ならびに 10 個の特殊文字 "!"、"@"、"#"、"$"、"%"、"^"、"&"、"*"、"("及び ")"が含まれることが期待される。英語以外の文字セットが TOE でサポートされ*

る場合、ST 作成者はサポートされる文字セットとともに、これらのセットのサブカテゴリのそれぞれに許容可能な文字空間を規定しなければならない (must)。

2. パスワードの最小の長さは管理者により設定可能であって、15 文字以上のパスワードがサポートされなければならず (shall)、さらに

適用上の注意： *最小パスワード長とパスワードの文字空間に基づくパスワードの組み合わせの数は、10^{14} を超えるものでなければならない (must)。これは、72 個の文字セットを用いる最小の長さが8 文字の英語パスワードにより満たされる。*

3. パスワードを構成する文字に要求される文字の種類と数を規定するパスワードの構成ルールが管理者により設定可能でなければならず (shall)、さらに

4. パスワードは、その利用者により用いられたパスワードの、管理者により設定可能な直近の世代数以内で再利用されてはならない (shall not)。

b) パスワードによらないクレデンシャル情報については、以下のルールが適用される。

1. 秘密が、その秘密のライフタイム内に攻撃者により取得される確率は、2^{-20} 未満であること。

管理：ESM_ICD.1

以下のアクションは、FMT における管理機能とみなすことができる：

a) 識別情報とクレデンシャル情報データの作成と変更。

監査：ESM_ICD.1

ESM_ICD.1 識別情報とクレデンシャル情報の定義が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)。

a) 最小：識別情報とクレデンシャル情報データの作成と変更。

5.1.5 ESM_ICT 識別情報とクレデンシャル情報の送信

ファミリのふるまい

本ファミリの要件により、TSF が利用者属性を他の ESM 製品へ送信する能力を有することを保証する。

コンポーネントのレベル付け

本ファミリには、ESM_ICT.1 という唯一のコンポーネントが存在する。ESM_ICT.1 識別情報とクレデンシャル情報の送信は、ESM_ICD.1 または ESM_ATD.1 (オプション) により定義される識別情報またはクレデンシャル情報データあるいはその両方を、TSF 外部の互換性のある正当な ESM 製品へ、ST 作成者により定義される条件の下で TOE が送信することを要求する。

5.1.5.1 ESM_ICT.1 識別情報とクレデンシャル情報の送信

ESM_ICT ファミリは、エンタープライズ利用者属性の送信に関する要件を定義する。これにより、TSF により定義される属性データを他の ESM 製品が利用して、それら自身のセキュリティ機能を実施することが可能となる。ESM_ICT.1 要件が付け加えられた理由は、運用環境中に存在する利用者に関する属性データを、他の高信頼 IT 製品であって自分のセキュリティ機能を行うためにそのデータを利用するものへ配付する TSF の能力に関する要件が、CC パート 2 には欠けているためである。

下位階層：	他のコンポーネントなし。
依存性：	ESM_ICD.1 識別情報とクレデンシャル情報の定義
ESM_ICT.1	TSF は、[選択：「識別情報とクレデンシャル情報のデータ」、「識別情報とクレデンシャル情報、及びオブジェクト属性のデータ」] を、互換性があり正当なエンタープライズセキュリティ管理製品へ、以下の状況の下で [選択：1 つ以上を選択：データの作成または変更の直後に、定期的な間隔で、製品の要求に応じて、 [***割付：その他の状況***]] 送信しなければならない (shall)。
適用上の注意：	*この要件の意図は、TSF がその定義する識別情報とクレデンシャル情報のデータをタイムリーな形で運用環境が利用できるようにすることにより、様々なポリシーの実施に正しいデータが使われているという保証が存在することを、保証することである。割付が選択された場合、それは意図を反映しなければならない (must)。*

管理：ESM_ICT.1

以下のアクションは、FMT における管理機能とみなすことができる：

a) 送信されるべき特定の識別情報またはクレデンシャル情報あるいはその両方のデータの値の規定。

b) 送信されるべき特定のオブジェクト属性の規定。

c) このデータが送信される状況の規定。

d) このデータが送信される送信先の規定。

監査：ESM_ICT.1

ESM_ICT.1 識別情報とクレデンシャル情報の送信が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)。

a) 最小：識別情報とクレデンシャル情報のデータ (及び、該当する場合オブジェクトの属性) の、外部プロセスまたはリポジトリへの送信。

5.2 FAU クラス：セキュリティ監査

5.2.1 FAU_STG_EXT.1 外部監査証跡ストレージ

FAU_STG_EXT ファミリは、ローカルな、または外部 IT エンティティへの監査データの記録に関する要件を定義する。監査データとは、FAU_GEN.1 を満たす結果として作成された情報を意味する。これは、監査データがどのように扱われるべきか (should) を論じているため、セキュリティ監査に関係する。FAU_STG_EXT.1 要件が付け加えられた理由は、特定のセキュアなやり方で 1 つ以上の特定の外部リポジトリへ監査データを書き込む TSF の能力を実証するとともに、ローカルな一時的ストレージの可能性をサポートする監査ストレージ要件が、CC パート 2 には欠けているためである。[4]

下位階層：	他のコンポーネントなし。
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、一般監査データを [***割付：外部 IT エンティティまたは***]

[4] FAU_STG.1 は、附属書 C 中のオプション要件として取り扱うこともできたであろう。しかし、ローカルなストレージのみを持つシステムが存在するかもしれず、そのため FAU_STG_EXT.1 もまたオプションとする必要が生じるかもしれない。これら 2 つを単一の、オプションではない SFR に統合することにより、保護された監査のストレージと送信が義務付けられる一方で、引き続き ESM 機能を統合した「一体型」製品もサポートされる。

「TOE 内部ストレージ」あるいはその両方の空でないリスト]へ送信できなければならない (shall)。

適用上の注意： *「送信」という用語は、TOE が主導する情報の伝送と、外部 IT エンティティからの要求に応じた TOE の情報伝送の両方を意図している。*

適用上の注意： *外部 IT エンティティの例としては、外部マシン上の監査サーバ ESM コンポーネント、TOE とプラットフォームを共有する評価済みオペレーティングシステム、あるいは集中型ロギングコンポーネントなどが考えられるであろう。複数ソースへの送信は許容される。*

FAU_STG_EXT.1.2 TSF は、あらゆる外部 IT エンティティへの生成された監査データの送信が、FTP_ITC.1 に定義される高信頼チャネルを用いて行われることを保証しなければならない (shall)。

FAU_STG_EXT.1.3 TSF は、生成された監査データのあらゆる TOE 内部ストレージが、以下のとおりであることを保証しなければならない (shall)：

1) TOE 内の監査証跡に格納された監査記録を不正な削除から保護すること、及び

2) TOE 内の監査証跡に格納された監査記録への不正な改変を防止すること。

管理：FAU_STG_EXT.1

以下のアクションは、FMT における管理機能とみなすことができる：

a) 生成された監査データを受信する外部 IT エンティティの規定。

監査：FAU_STG_EXT.1

FAU_STG_EXT.1 外部監査証跡ストレージが PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)：

a) 基本：生成された監査データを受信するために用いられる外部 IT エンティティとの通信の確立及び途絶。

5.3 FCS クラス：暗号サポート

5.3.1 FCS_CKM_EXT.4 暗号鍵のゼロ化

FCS_CKM_EXT ファミリは、暗号鍵の削除に関する要件を定義する。FCS_CKM_EXT.4 要件は、CC パート 2 の対応する要件よりも高度の鍵生成に関する限定性を提供するために追加された。

下位階層：	他のコンポーネントなし。
依存性：	依存性なし。
FCS_CKM_EXT.4.1	TSF は、必要でなくなったとき、すべての平文の秘密鍵とプライベート暗号鍵と暗号セキュリティパラメタをゼロ化しなければならない (shall)。

管理：FCS_CKM_EXT.4

予見される管理アクションは存在しない。

監査：FCS_CKM_EXT.4

FCS_CKM_EXT.4 暗号鍵のゼロ化が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)。

a) 基本：鍵ゼロ化プロセスの失敗。

5.3.2 FCS_HTTPS_EXT HTTPS

ファミリのふるまい

本ファミリの要件により、TSF が承認済みの暗号規格に従って HTTPS プロトコルを実装することを保証する。

コンポーネントのレベル付け

本ファミリには、FCS_HTTPS_EXT.1 という唯一のコンポーネントが存在する。FCS_HTTPS_EXT.1 HTTPS は、TOE が定義された規格に従って HTTPS を実装することを要求する。

5.3.2.1 FCS_HTTPS_EXT.1 HTTPS

下位階層：	他のコンポーネントなし。
依存性：	FCS_TLS_EXT.1 TLS

FCS_HTTPS_EXT.1.1 TSF は、RFC 2818 に準拠する HTTPS プロトコルを実装しなければならない (shall)。

適用上の注意： *ST 作成者は、実装がどのように識別した規格に適合しているかを決定するため、十分な詳細情報を提供しなければならない (must)；TSS に追加の詳細情報を追加することで達成できる。*

FCS_HTTPS_EXT.1.2 TSF は、FCS_TLS_EXT.1 に指定された TLS を用いて HTTPS を実装しなければならない (shall)。

管理：FCS_HTTPS_EXT.1

予見される管理アクションは存在しない。

監査：FCS_HTTPS_EXT.1

FCS_HTTPS_EXT.1 HTTPS が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)：

a) 基本：セションの確立失敗。

b) 基本：セションの確立／終了。

5.3.3 FCS_IPSEC_EXT IPsec

ファミリのふるまい

本ファミリの要件により、TSF が承認済みの暗号規格に従って IPsec プロトコルを実行することを保証する。

コンポーネントのレベル付け

本ファミリには、FCS_IPSEC_EXT.1 という唯一のコンポーネントが存在する。FCS_IPSEC_EXT.1 IPsec は、TOE が定義された規格に従って IPsec を実装することを要求する。

5.3.3.1 FCS_IPSEC_EXT.1 IPsec

下位階層： 他のコンポーネントなし。

依存性： FCS_COP.1 暗号操作

FCS_IPSEC_EXT.1.1 TSF は、RFC 4303 に定義される IPsec プロトコルの ESP を、暗号アルゴリズム AES-CBC-128、AES-CBC-256 (両者とも

RFC 3602 により指定される)、 [選択：その他のアルゴリズムなし、RFC 4106 に指定される AES-GCM-128、AES-GCM-256] を用い、また [選択、少なくとも 1 つを選択：RFC 2407、2408、2409、RFC 4109、RFC 2407、2408、2409、RFC 4109、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 IKEv1；RFC 5996 (節 2.23 に指定される NAT トラバーサルのサポートが必須)、4307、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 IKEv2] を用いて実装しなければならない (shall)。

適用上の注意： *最初の選択は、サポートされる追加的暗号アルゴリズムを識別するために用いられる。IKEv1 か IKEv2 のいずれかのサポートが提供されなければならない (must) が、適合する TOE は両方を提供できる；2 番目の選択は、これを選ぶために用いられる。IKEv1 については、RFC 4109 に記述された追加／変更を含め、RFC 2409 に準拠する IKE の実装を要求しているものと解釈されるべきである。RFC 4868 は、IKEv1 と IKEv2 の両方に用いられる追加的ハッシュ関数を識別している；これらの関数が実装される場合、3 番目 (IKEv1 について) 及び 4 番目 (IKEv2 について) の選択を用いることができる。IKEv2 は、2014 年 1 月 1 日以降、要求されることになる。*

FCS_IPSEC_EXT.1.2 TSF は、IKEv1 フェーズ 1 交換ではメインモードのみが用いられることを保証しなければならない (shall)。

FCS_IPSEC_EXT.1.3 TSF は、IKEv1 SA ライフタイムがフェーズ 1 SA については 24 時間、フェーズ 2 SA については 8 時間に制限できることを保証しなければならない (shall)。

適用上の注意： *上記の要件は、セキュリティ管理者により構成可能なライフタイムを (必要に応じて、適切な FMT 要件及び AGD_OPE により義務付けられる文書中の指示と共に) 提供すること、または制限を実装に「ハードコーディング」することの、いずれかの手段により達成できる。*

FCS_IPSEC_EXT.1.4 TSF は、IKEv1 SA ライフタイムがフェーズ 2 SA について [***割付：100 - 200 の範囲の数値***] MB のトラフィックに制限できる

ことを保証しなければならない (shall)。

適用上の注意： *上記の要件は、セキュリティ管理者により構成可能なライフタイムを (適切な FMT 要件及び AGD_OPE により義務付けられる文書中の指示と共に) 提供すること、または制限を実装に「ハードコーディング」することの、いずれかの手段により達成できる。ST 作成者は、要件により指定される範囲でデータの量を選択する。*

FCS_IPSEC_EXT.1.5 TSF は、すべての IKE プロトコルに DH グループ 14 (2048 ビット MODP)、及び [選択：24 (2048 ビット MODP と 256 ビット POS)、19 (256 ビットランダム ECP)、20 (384 ビットランダム ECP)、[***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] が実行されることを保証しなければならない (shall)。

適用上の注意： *上記は TOE が DH グループ 14 をサポートすることを要求している。他のグループがサポートされる場合、それらは選択 (グループ 24、19、及び 20) されるか上記の割付に指定されるべきである (should)；それ以外の場合「その他の DH グループなし」が選択されるべきである (should)。これは、IKEv1 及び (実装されていれば) IKEv2 鍵交換に適用される。本 PP の将来のバージョンでは、DH グループ 19 (256 ビットランダム ECP) 及び 20 (ビットランダム ECP) が要求されることになる。*

FCS_IPSEC_EXT.1.6 TSF は、すべての IKE プロトコルに [選択：DSA、rDSA、ECDSA] アルゴリズム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 (shall)。

適用上の注意： *選択されたアルゴリズムは、FCS_COP.1(2) の適切な選択と対応しているべきである (should)。*

FCS_IPSEC_EXT.1.7 TSF は、その IPsec 接続の認証に用いられる事前共有鍵の使用を (RFC 中で参照されているように) サポートしなければならない (shall)。

FCS_IPSEC_EXT.1.8 TSF は、以下をサポートしなければならない (shall)：

1. 事前共有鍵は、大文字及び小文字、数字、ならびに特殊文字： [選択：“!”、“@”、“#”、“$”、“%”、“^”、“&”、“*”、

“(“、“)”、[***割付：その他の文字***] の任意の組み合わせにより構成できなければならない (shall)；

2. 22 文字及び [選択：[***割付：その他のサポートされる長さ***]、その他の長さなし] の事前共有鍵。

適用上の注意： *ST 作成者は、TOE により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的な特殊文字が、オプションとして列挙されてもよい。事前共有鍵の長さについては、相互運用性の向上に資するため、共通の長さ (22 文字) が必要とされる。他の長さがサポートされる場合、それが割付中に列挙されるべきである (should)；またこの割付には、値の範囲 (例えば「5 から 55 文字まで」) を規定することもできる。*

管理：FCS_IPSEC_EXT.1

予見される管理アクションは存在しない。

監査：FCS_ IPSEC _EXT.1

FCS_ IPSEC _EXT.1 IPsec が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)：

a) 基本：SA の確立失敗。

b) 基本：SA の確立／終了。

5.3.4 FCS_RBG_EXT ランダムビット生成

ファミリのふるまい

本ファミリの要件により、TSF が権限付与された暗号規格に従って乱数を生成することを保証する。

コンポーネントのレベル付け

本ファミリには、FCS_RBG_EXT.1 という唯一のコンポーネントが存在する。FCS_RBG_EXT.1 暗号操作 (ランダムビット生成) は、TOE が定義された規格に従ってランダムビット生成を行うことを要求する。

5.3.4.1 FCS_RBG_EXT.1 暗号操作 (ランダムビット生成)

下位階層： 他のコンポーネントなし。

依存性：	依存性なし。
FCS_RBG_EXT.1.1	TSF は、 [選択、1 つを選択：[選択：Hash_DRBG (任意) 、HMAC_DRBG (任意) 、CTR_DRBG (AES) 、Dual_EC_DRBG (任意)] を用いる NIST Special Publication 800-90、FIPS Pub 140-2 附属書 C：AES を用いる X9.31 附属書 2.4] であって、[選択、1 つを選択：(1) 1 つ以上の独立したハードウェアベースの雑音源、(2) 1 つ以上の独立したソフトウェアベースの雑音源、(3) ハードウェアベースとソフトウェアベースの雑音源の組み合わせ] からエントロピーを蓄積するエントロピー源によりシードを供給されるものに従って、すべてのランダムビット生成 (RBG) サービスを行わなければならない (shall) 。
FCS_RBG_EXT.1.2	決定論的 RBG は、鍵とそれが生成する権限付与ファクタとの中で最も長いビット長と少なくとも等しい、最小で [選択、1 つを選択：128 ビット、256 ビット] のエントロピーによりシードが供給されなければならない (shall)。

管理：FCS_RBG_EXT.1

予見される管理アクションは存在しない。

監査：FCS_RBG_EXT.1

FCS_RBG_EXT.1 暗号操作 (ランダムビット生成) が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)。

a) 基本：ランダム化プロセスの失敗。

5.3.5 FCS_SSH_EXT SSH

ファミリのふるまい

本ファミリの要件により、TSF が権限付与された暗号規格に従って SSH プロトコルを実装することを保証する。

コンポーネントのレベル付け

本ファミリには、FCS_SSH_EXT.1 という唯一のコンポーネントが存在する。FCS_SSH_EXT.1 SSH は、TOE が定義された規格に従って SSH を実装することを要求する。

5.3.5.1 FCS_SSH_EXT.1 SSH

下位階層： 他のコンポーネントなし。

依存性： FCS_COP.1 暗号操作

FCS_SSH_EXT.1.1 TSF は、RFC 4251、4252、4253、及び 4254 に準拠する SSH プロトコルを実装しなければならない (shall)。

適用上の注意： *ST 作成者は、識別された 1 つまたは複数の規格に実装がどのように準拠しているかを決定するために十分な詳細を提供しなければならない (must)。これは、TSS 中に追加的詳細を追加することにより、達成できる。本 PP の将来のバージョンでは、鍵更新に関して要件が追加されることになる。この要件は、「TSF は、その鍵を用いて 2^{28} 以下のパケットが通過した後に SSH 接続が鍵更新されることを保証しなければならない (shall)」となる。*

FCS_SSH_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手法をサポートすることを保証しなければならない (shall)：公開鍵に基づくもの、パスワードに基づくもの。

FCS_SSH_EXT.1.3 TSF は、RFC 4253 に記述されるように、SSH トランスポート中の [***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 (shall)。

適用上の注意： *RFC 4253 は、「大きなパケット (large packets)」の受け入れを、そのパケットが「合理的な長さ (reasonable length)」でなければ破棄されるべき (should) という注意と共に規定している。割付には受け入れられる最大のパケットサイズが ST 作成者により記入され、これにより TOE の「合理的な長さ (reasonable length)」が定義されるべきである (should)。*

FCS_SSH_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用いることを保証しなければならない (shall)：AES-CBC-128、AES-CBC-256、[選択：AEAD_AES_128_GCM、AEAD_AES_256_GCM、その他のアルゴリズムなし]。

適用上の注意： *割付の中で、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「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 中に存在すべきである (should)。2010 年 12 月に NDPP v1.0 が公開されて以降、商用ネットワークデバイスにおける AES-GCM のサポートの普及に関してかなりの進歩が見られた。将来に公開される本 PP の更新されたバージョンでは、AES-GCM が要求される一方で AES-CBC がオプションとなることは十分にあり得る。

FCS_SSH_EXT.1.5 TSF は、SSH トランスポートの実装がその 1 つまたは複数の公開鍵アルゴリズムとして SSH_RSA 及び [選択：PGP-SIGN-RSA、PGP-SIGN-DSS、その他の公開鍵アルゴリズムなし] を用いることを保証しなければならない (shall)。

適用上の注意： *RFC 4253 は、要求される (required) 公開鍵アルゴリズムと許可できる (allowable) 公開鍵アルゴリズムを規定している。この要件により SSH-RSA は「要求される (required)」ものとなり、またその他 2 つが ST 中で主張できるようになる。ST 作成者は、SSH_RSA のみが実装される場合「その他の公開鍵アルゴリズムなし」を選択して、適切な選択を行うべきである (should)。*

FCS_SSH_EXT.1.6 TSF は、SSH トランスポート接続に用いられるデータ完全性アルゴリズムが [選択 : hmac-sha1、hmac-sha1-96、hmac-md5、hmac-md5-96] であることを保証しなければならない (shall)。

FCS_SSH_EXT.1.7 TSF は、diffie-hellman-group14-sha1 が SSH プロトコルに用いられる唯一の許可される鍵交換手法であることを保証しなければならない (shall)。

管理：FCS_SSH_EXT.1

予見される管理アクションは存在しない。

監査：FCS_SSH_EXT.1

FCS_SSH_EXT.1 SSH が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)：

a) 基本：セションの確立失敗。

b) 基本：セションの確立／終了。

5.3.6 FCS_TLS_EXT TLS

ファミリのふるまい

本ファミリの要件により､TSF が権限付与された暗号規格に従って TLS プロトコルを実装することを保証する。

コンポーネントのレベル付け

本ファミリには、FCS_TLS_EXT.1 という唯一のコンポーネントが存在する。FCS_TLS_EXT.1 TLS は、TOE が定義された規格に従って TLS を実装することを要求する。

5.3.6.1 FCS_TLS_EXT.1 TLS

下位階層： 他のコンポーネントなし。

依存性： FCS_COP.1 暗号操作

FCS_TLS_EXT.1.1 TSF は、以下の暗号スイートをサポートする以下の 1 つ以上のプロトコル [選択 : TLS 1.0 (RFC 2246)、TLS 1.1 (RFC 4346)、TLS 1.2 (RFC 5246)] を実装しなければならない (shall)：

必須暗号スイート：

TLS_RSA_WITH_AES_128_CBC_SHA

オプションの暗号スイート：

[選択：

なし

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS_RSA_WITH_AES_128_CBC_SHA256

TLS_RSA_WITH_AES_256_CBC_SHA256

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

]。

適用上の注意： *ST 作成者は、TLS の実装を反映した適切な選択及び割付を行わなければならない (must)。ST 作成者は、識別された 1 つまたは複数の規格に実装がどのように準拠しているかを決定するために十分な詳細を提供しなければならない (must)。これは、このコンポーネントへエレメントを追加することにより、または TSS 中の追加的詳細により、達成できる。*

評価される構成に用いられる暗号スイートは、この要件により制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである (should)。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、「なし」が選択されるべきである (should)。実装によりネゴシエーションされるスイートをこの要件中のものに制限するために管理手順が取られる必要がある場合、AGD_OPE により要求されるガイダンス中にその適切な指示が含まれる必要がある。上に列挙した Suite B アルゴリズム (RFC 5430) は、実装に望ましいアルゴリズムである。2010 年 12 月に NDPP v1.0 が公開されて以降、商用デバイスにおける TLS 1.2 の普及に関してあまり進歩が見られない。本 PP の将来の版では TLS 1.2 (RFC 5246) のサポートが要求されることになる；しかし、本 PP の次のバージョンには TLS 1.2 のサポート要件が含まれないが、SSL 2.0 または SSL 3.0 を用いたすべての接続試行を拒否する手段を TOE が提供することが要求されることは十分にあり得る。

管理：FCS_TLS_EXT.1

予見される管理アクションは存在しない。

監査：FCS_TLS_EXT.1

FCS_TLS_EXT.1 TLS が PP/ST に含まれる場合、以下のアクションが監査可能であるべき

である (should) :

a) 基本：セションの確立失敗。

b) 基本：セションの確立／終了。

5.4 FPT クラス：TSF の保護

5.4.1 FPT_APW_EXT 保存クレデンシャル情報の保護

ファミリのふるまい

本ファミリの要件により、TSF がクレデンシャル情報データを暴露から保護することを保証する。

コンポーネントのレベル付け

本ファミリには、FPT_APW_EXT.1 という唯一のコンポーネントが存在する。FPT_APW_EXT.1 保存されたクレデンシャル情報の保護は、TOE がクレデンシャル情報を平文以外の形態で保存すること、及び平文クレデンシャル情報の読み出しを防止することを要求する。

5.4.1.1 FPT_APW_EXT.1 保存クレデンシャル情報の保護

この SFR は、クレデンシャル情報 (管理利用者のクレデンシャル情報またはエンタープライズ利用者のクレデンシャル情報のいずれか) を TOE が保存しなければならない (must) 際の TOE のふるまいを記述する。コモンクライテリアには同等の要件が存在しないため、明示的な要件が必要とされた。これは、ネットワークデバイスのプロテクションプロファイルに定義された要件に基づいている。

下位階層：	他のコンポーネントなし。
依存性：	依存性なし。
FPT_APW_EXT.1.1	TSF は、クレデンシャル情報を平文以外の形態で保存しなければならない (shall)。
FPT_APW_EXT.1.2	TSF は、平文のクレデンシャル情報が読み出されることを防止しなければならない (shall)。

管理：FPT_APW_EXT.1

予見される管理アクションは存在しない。

監査：FPT_APW_EXT.1

予見される監査対象アクションは存在しない。

5.4.1 FPT_SKP_EXT 秘密鍵パラメタの保護（訳注：5.4.2）

ファミリのふるまい

本ファミリの要件により、TSF がクレデンシャル情報データを暴露から保護することを保証する。

コンポーネントのレベル付け

本ファミリには、FPT_SKP_EXT.1 という唯一のコンポーネントが存在する。FPT_SKP_EXT.1 秘密鍵パラメタの保護は、秘密暗号データを読み出すためのメカニズムが存在しないことを TOE が保証することを要求する。

5.4.1.1 FPT_SKP_EXT.1 秘密鍵パラメタの保護（訳注：5.4.2.1 ）

この SFR は、ここで包括的に秘密鍵パラメタと呼ぶ事前共有鍵、対称鍵、及びプライベート鍵を取り扱う際の TOE のふるまいを記述する。コモンクライテリアには同等の要件が存在しないため、明示的な要件が必要とされた。これは、ネットワークデバイスのプロテクションプロファイルに定義された要件に基づいている。

下位階層：	他のコンポーネントなし。
依存性：	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が読み出されることを防止しなければならない (shall)。

管理：FPT_SKP_EXT.1

予見される管理アクションは存在しない。

管理：FPT_SKP_EXT.1

予見される監査対象アクションは存在しない。

5.5 FTA クラス：TOE アクセス

5.5.1 FTA_SSL_EXT.1 TSF 起動セションロック

この SFR は、TOE がセションロックを開始しなければならない (must) 際の TOE のふるまいを記述する。コモンクライテリア中の基本要件に定められたロックを行うアクション

の対象範囲を狭め、規定するために、明示的な要件が必要とされた。

下位階層： 他のコンポーネントなし。

依存性： 依存性なし。

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

- セションロック—表示デバイスを消去または上書きし、現在のコンテンツを判読不能とし、セション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、そしてセションロック解除に先立って TSF への利用者再認証を要求すること；
- セションの終了

] を、正当な管理者により指定される非アクティブ継続時間後に行わなければならない (shall)。

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みなすことができる：

a) 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規定、

b) ロックアウトが発生するデフォルトの利用者非アクティブ時間の規定、

c) セションロック解除に先立って発生すべき (should) イベントの管理。

監査：FTA_SSL_EXT.1

FTA_SSL_EXT.1 が PP/ST に含まれる場合、以下のアクションが監査可能であるべきである (should)：

a) 最小：セションロックメカニズムによる対話セションのロック。

b) 最小：対話セションのロック解除の成功。

c) 基本：対話セションのロック解除のあらゆる試行。

6 セキュリティ要件

本文書中の要件は、機能要件と保証要件の 2 つのセットに大別される。前者の機能要件のセットはコモンクライテリアから引用されたものであり、監査及びポリシーの実施に関するコア要件に対応する。本 PP の機能要件は、CC のパート 2 から引用されたものであり、セキュリティ対策方針の形式的な実体化である。これらの要件は、TOE のセキュアな運用をサポートすることに関連している。

セキュリティ保証要件 (SAR) は、典型的には SFR とは分離して PP へ挿入され列挙される。そして、選択された SAR に基づいた評価中には CEM が参照される。コモンクライテリアのセキュリティ保証要件と、TOE として識別される特有の技術の性質のため、よりカスタム化されたアプローチが本 PP では取られている。本 PP でも SAR は文脈に応じて完全を期して節 6.2 に列挙されているが、評価者が SFR と SAR のそれぞれについてこの TOE に行う必要のあるアクティビティの大半は、「***保証アクティビティ***」のパラグラフに詳述されている。保証アクティビティは、評価を完了するために行われなければならない (must) アクティビティの規範的な記述である。保証アクティビティは本 PP の 2 か所に配置されている。特定の SFR と関連付けられたものはそれらの SFR と共に配置され、SFR と独立したものは節 6.2 に詳述されている。保証アクティビティは、実際にはカスタム化された評価の方法論であり、読みやすさと理解しやすさ、そして便宜のためインラインに提示されていることに注意すること。

SFR と直接関連付けられるアクティビティについては、各 SFR の後に 1 つ以上の保証アクティビティが列挙され、適合デバイスに必要とされる保証を実現するために行われる必要のあるアクティビティが詳述される。

SFR とは独立したアクティビティを必要とする SAR については、実現される必要のある追加的保証アクティビティが、その SAR と関連付けられた特定の保証アクティビティが書かれる対象となった SFR への参照とともに、節 6.2 に示されている。

本プロテクションプロファイルの将来の世代では、実際の製品評価から得られた教訓に基づいた、より詳細な保証アクティビティを提供することになるかもしれない。

6.1 セキュリティ機能要件

本 PP のセキュリティ機能要件は以下のコンポーネントから構成されており、**エラー！参照ソースが見つかりません。**にその概要を示す。これらの要件に用いられたフォーマットは、附属書 D.1 - 操作に定義されている。

表 2. TOE 機能コンポーネント

機能コンポーネント	
ESM_ATD.1 (オプション)	オブジェクト属性の定義 *(オプション–附属書 C.1.1 に定義される)*
ESM_EAU.2	エンタープライズ認証への依存
ESM_EID.2	エンタープライズ識別への依存
ESM_ICD.1	識別情報とクレデンシャル情報の定義
ESM_ICT.1	識別情報とクレデンシャル情報の送信
FAU_GEN.1	監査データの生成
FAU_SEL.1 (オプション)	選択可能な監査 *(オプション – 附属書 C.3.1 に定義される)*
FAU_STG_EXT.1	外部監査証跡ストレージ
FCS_CKM.1 (オプション)	暗号鍵の生成 (非対称鍵に関して) *(オプション – 附属書 C.8.1 に定義される)*
FCS_CKM_EXT.4 (オプション)	暗号鍵のゼロ化 *(オプション – 附属書 C.8.2 に定義される)*
FCS_COP.1(1) (オプション)	暗号操作 (データの暗号化／復号に関して) *(オプション – 附属書 C.8.3 に定義される)*
FCS_COP.1(2) (オプション)	暗号操作 (暗号署名に関して) *(オプション – 附属書 C.8.4 に定義される)*
FCS_COP.1(3) (オプション)	暗号操作 (暗号ハッシュに関して) *(オプション – 附属書 C.8.5 に定義される)*
FCS_COP.1(4) (オプション)	暗号操作 (鍵付きメッセージ認証に関して) *(オプション – 附属書 C.8.6 に定義される)*
FCS_HTTPS_EXT.1 (オプション)	HTTPS *(オプション – 附属書 C.8.7 に定義される)*
FCS_IPSEC_EXT.1 (オプション)	IPsec *(オプション – 附属書 C.8.8 に定義される)*
FCS_RBG_EXT.1 (オプション)	暗号操作 (ランダムビット生成) *(オプション – 附属書 C.8.9 に定義される)*
FCS_SSH_EXT.1 (オプション)	SSH *(オプション – 附属書 C.8.10 に定義される)*
FCS_TLS_EXT.1 (オプション)	TLS *(オプション – 附属書 C.8.11 に定義される)*
FIA_AFL.1 (オプション)	認証失敗の取り扱い

機能コンポーネント	
	(オプション - 附属書 C.7.1 に定義される)
FIA_SOS.1 (オプション)	秘密の検証 *(オプション - 附属書 C.2.1 に定義される)*
FIA_USB.1	利用者−サブジェクト束縛
FMT_MOF.1	機能のふるまいの管理
FMT_MTD.1	TSF データの管理 *(オプション - 附属書 C.5.1 に定義される)*
FMT_SMF.1	管理機能の仕様
FMT_SMR.1	セキュリティ管理の役割
FPT_APW_EXT.1	保存されたクレデンシャル情報の保護
FPT_SKP_EXT.1	プライベート鍵パラメタの保護
FPT_STM.1 (オプション)	高信頼タイムスタンプ *(附属書 C.6.1 に定義される)*
FTA_SSL_EXT.1 (オプション)	TSF 主導のセションのロック *(オプション - 附属書 C.4.1 に定義される)*
FTA_SSL.3 (オプション)	TSF 主導の終了 *(オプション - 附属書 C.4.2 に定義される)*
FTA_SSL.4 (オプション)	利用者主導の終了 *(オプション - 附属書 C.4.3 に定義される)*
FTA_TAB.1	TOE アクセスバナー
FTA_TSE.1 (オプション)	TOE セションの確立 *(オプション - 附属書 C.7.2 に定義される)*
FTP_ITC.1	TSF 間高信頼チャネル
FTP_TRP.1	高信頼パス

6.1.1 PP 適用上の注意

6.1.1.1 利用

PP 中の多くの要件の後には、各要件の背景にある意図を読者が確認できるよう、適用上の注意が提供されている。ST 作成者は、これらの適用上の注意を ST に再提示してはならない (must not)。

6.1.1.2 構成上の理念

一連の ESM PP は、ESM 製品の様々な機能を包含するように作成された、関連するプロ

テクションプロファイルのファミリを表現している。ESM PP ファミリ中の複数の PP への適合を主張する ST については、適用上の注意を用いて ESM コンポーネントが互いにどのように関連しているかを明記することが ST 作成者に推奨される。これは、異なる ESM 機能の CC の概念に応じてどのようにその製品の部分を評価すべきかを決定するうえで、読者を助けることになる。

例えば、ESM の複数の部分は単一のアプライアンスとして、ポリシー実施メカニズムをも含む一連の冗長サーバとして、あるいは単一のサーバへ報告を行う個別クライアントシステム上に実施ポイントが存在するクライアント・サーバ展開として、展開できる。適用上の注意を用いることにより、ESM システムのアーキテクチャに基づいて、主張が不必要な要件を容易に決定できる。

6.1.2 ESM クラス：エンタープライズセキュリティ管理

ESM_EAU.2 エンタープライズ認証への依存

下位階層：	他のコンポーネントなし。
ESM_EAU.2.1	TSF は、サブジェクト認証を [選択：[***割付： サブジェクト認証を担当する識別された 1 つまたは複数の TOE コンポーネント***]、[***割付： サブジェクト認証を担当する識別された 1 つまたは複数の運用環境コンポーネント***]] に依存しなければならない (shall)。
適用上の注意：	*このように識別されようとしているサブジェクトが TSF の利用者または管理者である場合、1 つまたは複数の割付に 1 つ以上の認証サーバが記入されることが期待される。本プロテクションプロファイルの将来のバージョンは、この割付中に指名されたエンティティがエンタープライズセキュリティ管理認証サーバの標準プロテクションプロファイルに適合することを要求するかもしれない。*
ESM_EAU.2.2	TSF はすべてのサブジェクトに、そのサブジェクトに代わってそれ以外の TSF 仲介アクションを許可する前に、認証が成功することを要求しなければならない (shall)。
適用上の注意：	*TSF が2 つの異なる手法を利用してサブジェクトの2 つの異なるセットを認証する場合、ST 作成者はそれぞれの手法についてこの SFR の異なる繰り返しを作成することにより、これを提示しなければならない (must)。*

依存性： ESM_EID.2 エンタープライズ識別への依存

保証アクティビティ：

評価者は、TSF が使用する認証を要求するものとして記述されているか、また TOE へ認証される利用者または IT エンティティのそれぞれの種類ごとに、用いられる識別情報と権限付与メカニズムが記述されているかを決定するために TSS をチェックしなければならない (shall)。また評価者は、TSF により用いられる認証メカニズムのそれぞれについて、SFR を繰り返すことによりこの情報が適切に提示されていることをチェックして保証しなければならない (shall)。

評価者は、TOE へのアクセスを要求している対話的利用者が認証されているかどうかを TOE がどのように決定しているか、そして TOE が受領する認証クレデンシャル情報または識別情報の主張をどのように検証しているかを決定するため、操作ガイダンスをチェックしなければならない (shall)。何らかの IT エンティティが TOE に認証要求を行う場合、評価者は、これらのエンティティがどのように認証されるか、認証の設定をするためにどのような設定の手順が行われなければならないか (must) 識別されていることを検証するため、操作ガイダンスについてもチェックしなければならない (shall)。

評価者は、有効な識別と認証情報を提供せずに TOE へアクセスすると、TSF へのアクセスがその後拒否されることを確認することにより、この機能をテストしなければならない (shall)。何らかの IT エンティティが TOE に認証要求を行う場合、評価者はこれらの IT エンティティに無効な識別と認証情報を提供するよう指示し、そしてこれらが TSF へアクセスできないことを確認しなければならない (shall)。

識別と認証のポジティブテストは、他の要件によりテストされると想定されていることを注意すること。認証が成功することは、TSF を管理するための (またおそらくは、TSF が外部 IT エンティティと相互作用するための) 前提条件だからである。

ESM_EID.2 エンタープライズ識別への依存

下位階層： 他のコンポーネントなし。

ESM_EID.2.1 TSF は、サブジェクト識別を [選択： [***割付： サブジェクト識別を担当する 1 つまたは複数の TOE コンポーネント***]、[***割付: サブジェクト識別を担当する 1 つまたは複数の運用環境コンポーネント***]] に依存しなければならない (shall)。

適用上の注意： *このように識別されるサブジェクトが TSF の利用者または管理者である場合、1 つまたは複数の割付に 1 つ以上の認証サー*

バが記入されると期待されている。本プロテクションプロファイルの将来のバージョンは、この割付で指名されたエンティティがエンタープライズセキュリティ管理認証サーバの標準プロテクションプロファイルに適合することを要求するかもしれない。

ESM_EID.2.2　TSF はすべてのサブジェクトに、そのサブジェクトに代わってそれ以外の TSF 仲介アクションを許可する前に、識別が成功することを要求しなければならない (shall)。

適用上の注意：　*TSF が2 つの異なる手法を利用してサブジェクトの2 つの異なるセットを識別する場合、ST 作成者はそれぞれの手法についてこの SFR の異なる繰り返しを作成することにより、これを提示しなければならない (must)。*

依存性：　依存性なし。

保証アクティビティ：

この機能は、対話的利用者と正当な IT エンティティの両方に対して、ESM_EAU.2 と組み合わせて検証される。

ESM_ICD.1 識別情報とクレデンシャル情報の定義

下位階層：　他のコンポーネントなし。

ESM_ICD.1.1　TSF は、他のエンタープライズセキュリティ管理製品と共に用いられる識別情報とクレデンシャル情報のデータを定義する能力を提供しなければならない (shall)。

ESM_ICD.1.2　TSF は、以下のセキュリティ関連の識別情報とクレデンシャル情報の属性をエンタープライズ利用者に定義しなければならない (shall)：クレデンシャル情報のライフタイム、クレデンシャル情報の状態、 [***割付：TSF がエンタープライズ利用者へ関連付けることが可能な任意の追加的セキュリティ関連の識別情報とクレデンシャル情報の属性のリスト***]。

適用上の注意：　*セキュリティ関連の識別情報とクレデンシャル情報の属性は、他の ESM 製品が自分のセキュリティ機能の実施に用いる利用者属性の完全なセットを構成しなければならない (must)。利用者 ID やパスワードなどのデータは、認証に用いられるためセキ*

ュリティ関連である。利用者の組織の役割、役職、あるいは地理的な位置などのデータは、アクセス制御ポリシーがこれらのデータを利用することが期待される場合、セキュリティ関連かもしれない。電話番号などのデータは、セキュリティ関連ではないことが多い。

ESM_ICD.1.3 TSF は、一意に識別されるデータを割り当てることにより、エンタープライズ利用者を登録する能力を提供しなければならない (shall)。

適用上の注意：2 人の利用者が、同一のクレデンシャル情報データを持つことは可能である。ESM_ICD.1.3 の意図は、特定のエンタープライズ利用者を一意に識別するように維持される追加的情報が存在すべきである、ということである。

ESM_ICD.1.4 TSF は、定義されたセキュリティ関連属性を登録されたエンタープライズ利用者へ関連付ける能力を提供しなければならない (shall)。

適用上の注意： *セキュリティ属性をエンタープライズ利用者へ関連付ける行為は、クレデンシャル情報の発行とそれらの状態の管理を含むことが期待される。*

ESM_ICD.1.5 TSF は、エンタープライズ利用者のクレデンシャル情報の状態を問い合わせる能力を提供しなければならない (shall)。

ESM_ICD.1.6 TSF は、エンタープライズ利用者のクレデンシャル情報を失効させる能力を提供しなければならない (shall)。

ESM_ICD.1.7 TSF は、互換性のある認証サーバ ESM 製品にエンタープライズ利用者のクレデンシャル情報を更新する能力を提供しなければならない (shall)。

ESM_ICD.1.8 TSF は、定義されたエンタープライズ利用者クレデンシャル情報が以下の強度ルールを満たすことを保証しなければならない (shall)。

a) パスワードによるクレデンシャル情報については、以下のルールが適用される。

1. パスワードは、以下の文字セットのサブセットから構成さ

れることができなければならない (shall)： [***割付：パスワードの入力に関してTSF でサポートされる文字セットのリスト***] であって、以下の値を含むもの [***割付：サポートされる文字セットのそれぞれについて、サポートされる文字のリスト***]；及び

適用上の注意： *英語の文字セットについては、文字の種類には26 個の大文字、26 個の小文字、10 個の数字、ならびに 10 個の特殊文字 "!"、"@"、"#"、"$"、"%"、"^"、"&"、"*"、"("及び ")"が含まれることが期待される。英語以外の文字セットが TOE でサポートされる場合、ST 作成者はサポートされる文字セットとともに、これらのセットのサブカテゴリのそれぞれに許容可能な文字空間を規定しなければならない (must)。*

2. パスワードの最小の長さは管理者により設定可能であって、15 文字以上のパスワードがサポートされなければならず (shall)、さらに

適用上の注意： *最小パスワード長とパスワードの文字空間に基づくパスワードの組み合わせの数は、10^{14} を超えるものでなければならない (must)。これは、72 個の文字セットを用いる最小の長さが8 文字の英語パスワードにより満たされる。*

3. パスワードを構成する文字に要求される文字の種類と数を規定するパスワードの構成ルールが管理者により設定可能でなければならず (shall)、さらに

4. パスワードは、その利用者により用いられたパスワードの、管理者により設定可能な直近の世代数以内で再利用されてはならない (shall not)。

b) パスワードによらないクレデンシャル情報については、以下のルールが適用される。

1. 秘密が、その秘密のライフタイム内に攻撃者により取得される確率は、2^{-20} 未満であること。

依存性： 依存性なし。

保証アクティビティ：

評価者は TSS をレビューして、適合性のある ESM 製品が識別されていること、またこれらの製品により用いられる識別情報とクレデンシャル情報のデータが記述されていることを検証しなければならない (shall)。評価者は、適合性のある製品について公開文書をレビューし、これらが実際に TSS により主張されているのと互換性のある形でデータを取り扱っていることを検証しなければならない (shall)。

評価者は、どのように識別情報とクレデンシャル情報のデータが TOE へ供給されるか、そしてこのデータが識別されるか、示されていることを検証するために、操作ガイダンスをレビューしなければならない (shall)。

評価者は、TOE を用いて識別情報とクレデンシャル情報データを作成し、このデータを適合性のある ESM 製品へ送信して利用させることにより、この機能をテストしなければならない (shall)。これらのテストは、クレデンシャル情報の複雑性要件を実施する能力を含め、SFR に記述されたあらゆる機能を動かさなければならない (shall)。次に評価者は、データが適切に適用されたことを確認するために、識別情報とクレデンシャル情報データを利用する適合性のある ESM 製品上で基本的な識別情報とクレデンシャル情報関連のアクション[5]を行う。

クレデンシャル情報の複雑性に関する要件について：収集されるクレデンシャル情報の形態を識別するために、評価者は TSS と操作ガイダンスを検査しなければならない (shall)。

a. *パスワードによるクレデンシャル情報について、評価者は ST に指定されるすべてのパスワードの作成、構成、及びエージング要件が TSS 及び AGD で議論されていることを識別し、そしてこれらの機能をひとつずつテスト (例えば、パスワードの最小の長さを 6 に設定し、7 文字のパスワードと 16 文字のパスワードが両方とも受け入れられることを確認し、次に最小の長さを 8 に変更して、7 文字のパスワードは拒否されるが 16 文字のパスワードは受け入れられることを確認) しなければならない (shall)*

b. *パスワードによらないクレデンシャル情報について、評価者は基本的な機能の強度分析を行って、認証メカニズムの解空間とパスワード試行を行うことのできる頻度を決定しなければならない (shall)。例えば、認証が 1 時間に 1 回の試行を行える 4 つの数字の PIN であれば、この要件には合格しないであろう。認証メカニズムの強度が機能強度測定基準により額面どおりに決定できない場合 (例えば、生体認証メカニズムが用いられる場合)、ベンダは機能の強度の何らかの証拠資料を提供しなければならない (shall)。*

[5] つまり、境界条件の徹底的なテストは必要とされない。

ESM_ICT.1 識別情報とクレデンシャル情報の送信

下位階層： 他のコンポーネントなし。

ESM_ICT.1.1 TSF は、 [選択：「識別情報とクレデンシャル情報のデータ」、「識別情報とクレデンシャル情報、及びオブジェクト属性のデータ」] を、互換性があり正当なエンタープライズセキュリティ管理製品へ、以下の状況の下で [選択：1 つ以上を選択：データの作成または変更の直後に、定期的な間隔で、互換性のあるセキュア構成管理製品の要求に応じて、 [***割付：その他の状況***] 送信しなければならない (shall)。

適用上の注意： *この要件の意図は、様々なポリシーの実施に正しいデータが使われていることを保証するため、TSF がその定義する識別情報とクレデンシャル情報のデータをタイムリーに運用環境が利用できるようにしていることを保証することである。割付が選択された場合、その意図が反映されなければならない (must)。*

「互換性のあるセキュア構成管理製品の要求に応じて」が選択された場合、ST 作成者は互換性のある 1 つまたは複数の製品を示さなければならない (must)。

依存性： ESM_ICD.1 識別情報とクレデンシャル情報の定義

保証アクティビティ：

評価者は、1 つまたは複数の適用上の注意により提供されるガイダンスと一貫した形で割付が行われていることを決定するために、TSS をチェックしなければならない (shall)。また評価者は TSS をチェックして、他の ESM 製品へ TSF が送信する ESM データと、その送信が引き起こされる状況が記述されていることを確認しなければならない (shall)。

評価者は操作ガイダンスをレビューして、識別情報、クレデンシャル情報 (及び潜在的にオブジェクト属性) データを作成及び更新する方法、ならびに新たな、または更新されたデータがそれを利用する ESM 製品に送信される状況 (及び、該当する場合それらの状況を管理する方法) を決定しなければならない (shall)。

評価者は、互換性のある ESM 製品を入手することにより、この能力をテストしなければならない (shall)。

評価者は、ICM 及び他の ESM 製品の両方について操作ガイダンス中の手順に従って、示されたデータ (すなわち、識別情報、クレデンシャル情報、及び潜在的にオブジェクト属

性データ) を作成して、SFR に定義された状況に応じて、定義されたデータが互換性のある ESM 製品へ送信されインストールが成功することを保証しなければならない (shall)[6]*。換言すれば、 (a) 新たなデータの作成後に送信するように選択が行われている場合、評価者は新たなデータを作成し、合理的な送信ウィンドウが経過した後に、その新たなデータがインストールされていることを確認しなければならず (shall)、(b) 定期的に送信するように選択が行われている場合、評価者は新たなデータを作成し、定期的な時間間隔が経過するまで待ってから、新たなデータが適切な ESM コンポーネント中に存在することを確認しなければならず (shall)、あるいは (c) 互換性のあるセキュア構成管理コンポーネントの要求に応じて送信するように選択が行われている場合、評価者はデータを作成し、セキュアな構成管理コンポーネントを用いて送信を要求し、そして適切な ESM コンポーネントがそのデータを受信しインストールしていることを確認しなければならない (shall)。ST 作成者が「その他の状況」を指定している場合、同様のテストを実施して、それらの状況下での送信が確認されなければならない (shall)。*

次に評価者は先ほど作成したデータに変更を加えた後に先ほどの手順を繰り返し、更新されたデータが SFR に規定された状況に応じて互換性のある ESM コンポーネントへ送信されることを保証しなければならない (shall)。最後に、データの更新はデータの削除を包含するため、評価者はこのプロセスをもう一度、今回はデータを削除して繰り返し、互換性のある ESM コンポーネントからアクティブなデータとしてのそのデータが取り除かれることを保証しなければならない (shall)。

注意：このテストは、ESM_ICD.1 のテストと組み合わせて行われることになるだろう。

6.1.3 セキュリティ監査 (FAU)

FAU_GEN.1 監査データの生成

下位階層： 他のコンポーネントなし。

FAU_GEN.1.1 TSF は、以下の監査対象イベントの監査記録を生成できなければならない (shall)。

a) 監査機能の開始及び終了；ならびに

b) 監査のレベルが [規定されていない] 表 3 に識別されるすべての監査対象イベント；*及び*

[6] テストの目的においては、互換性のある ESM 製品を同等のグループにグループ分けした上で、1 つのグループから 1 つのメンバーだけをテストすれば十分にそのグループのすべてのメンバーをカバーできるという論拠を提供することは許容可能である。

c) [*割付：その他の監査対象イベント*]。

表 3. 監査対象イベント

コンポーネント	イベント	追加的情報
ESM_ATD.1 (オプション)	オブジェクト属性の定義	定義された属性の識別情報
ESM_ATD.1 (オプション)	オブジェクトと属性との関連付け	オブジェクトと属性の識別情報
ESM_EAU.2	認証メカニズムの利用すべて	なし
ESM_ICD.1	識別情報とクレデンシャル情報データの作成または変更	変更された 1 つまたは複数の属性
ESM_ICD.1	サブジェクトの登録または変更	作成または変更されたサブジェクト、変更された 1 つまたは複数の属性 (該当する場合)
ESM_ICT.1	情報を送信しようとするすべての試行	送信が試行された送信先
FAU_STG_EXT.1	監査サーバとの通信の確立及び途絶	監査サーバの識別情報
FCS_CKM.1 (オプション)	鍵生成アクティビティの失敗	なし
FCS_CKM_EXT.4 (オプション)	鍵ゼロ化プロセスの失敗	ゼロ化を要求または引き起こしたサブジェクトの識別情報、クリアされようとしていたオブジェクトまたはエンティティの識別情報
FCS_COP.1(1) (オプション)	暗号化または復号の失敗	操作の暗号モード、暗号化／復号されようとしていたオブジェクトの名称／識別子
FCS_COP.1(2) (オプション)	暗号署名の失敗	操作の暗号モード、署名／検証されようとしていたオブジェクトの名称／識別子
FCS_COP.1(3) (オプション)	ハッシュ機能の失敗	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子
FCS_COP.1(4) (オプション)	非データ完全性暗号ハッシュの失敗	操作の暗号モード、ハッシュされようとしていたオブジェクトの名称／識別子
FCS_HTTPS_EXT.1	HTTPS セションの確立	接続の TOE とは反対側のエンドポイント

コンポーネント	イベント	追加的情報
(オプション)	失敗	(IP アドレス)、失敗の理由 (該当する場合)
FCS_IPSEC_EXT.1 (オプション)	SA の確立失敗、SA の確立／終了	接続の TOE とは反対側のエンドポイント (IP アドレス)、失敗の理由 (該当する場合)
FCS_RBG_EXT.1 (オプション)	ランダム化プロセスの失敗	なし
FCS_SSH_EXT.1 (オプション)	HTTPS セションの確立失敗	接続の TOE とは反対側のエンドポイント (IP アドレス)、失敗の理由 (該当する場合)
FCS_TLS_EXT.1 (オプション)	HTTPS セションの確立失敗	接続の TOE とは反対側のエンドポイント (IP アドレス)、失敗の理由 (該当する場合)
FIA_AFL.1 (オプション)	不成功に終わった認証試行の閾値への到達、閾値へ到達した際に取られたアクション、及び通常状態へ復帰するために取られたアクションがあればそのアクション	閾値へ到達した際に取られたアクション
FIA_SOS.1 (オプション)	任意のテストされた秘密の、TSF による拒否または受け入れ	なし
FIA_SOS.1 (オプション)	定義された品質測定基準への任意の変更の識別	品質測定基準へなされた変更
FMT_MOF.1	TSF 機能のふるまいの変更すべて	なし
FMT_SMF.1	管理機能の利用	行われた管理機能
FTA_SSL_EXT.1 (オプション)	すべてのセションロック及びロック解除イベント	なし
FTA_SSL.3 (オプション)	すべてのセション終了イベント	なし
FTA_SSL.4 (オプション)	すべてのセション終了イベント	なし
FTA_TSE.1	セション確立の拒否	なし

コンポーネント	イベント	追加的情報
(オプション)		
FTP_ITC.1	高信頼チャネル機能の利用すべて	高信頼チャネルのイニシエータ及びターゲットの識別情報
FTP_TRP.1	高信頼パス機能の利用すべて	該当する場合、すべての高信頼パス機能と関連付けられた利用者の識別情報

FAU_GEN.1.2 TSF は、監査記録のそれぞれに、少なくとも以下の情報を記録しなければならない (shall)。

a) イベントの日付及び時刻、イベントの種類、サブジェクトの識別情報 (該当する場合)、及びイベントの結果 (成功または失敗)、ならびに

b) 監査イベントの種類のそれぞれについて、PP/ST に含まれる機能コンポーネントの監査対象イベントの定義に基づいた、 [***割付：その他の監査関連情報***]。

適用上の注意： *責任者を識別するために十分な情報と、その責任者により取られた具体的なアクションが、 a) 項で取り込まれた情報によりすでに対処されていない場合、「その他の監査関連情報」にはこれらが含まれなければならない (must)。*

依存性： FPT_STM.1 高信頼タイムスタンプ

保証アクティビティ：

評価者は TSS をチェックして、監査対象イベントが要約され監査記録の内容が記述されていることを保証しなければならない (shall)。

評価者は操作ガイダンスをチェックして、監査対象イベントのすべてが列挙されていること、及び監査記録の種類のそれぞれについてその内容の記述が提供されていることを保証しなければならない (shall)。すべての監査記録のフォーマットの種類がカバーされなければならず (shall)、また各フィールドの簡潔な記述が含まれなければならない (shall)。評価者は、PP により義務付けられるすべての監査イベントの種類が記述され、フィールドの記述には FAU_GEN 1.2 に要求される情報と、表 3 に指定される追加的情報が含まれることをチェックして確認しなければならない (shall)。

評価者は、PP に指定される要件を実施するために必要な、TOE に実装されるメカニズム

の構成 (有効化及び無効化を含む) を可能とする管理インタフェース (サブコマンド､スクリプト、及び構成ファイルを含む) を決定するために、操作ガイダンスと、利用できるインタフェース文書があればそれをレビューしなければならない (shall)。評価者は、これを行うために採用した方法論または手法を文書化しなければならない (shall)。評価者はこのアクティビティを、AGD_OPE ガイダンスが要件を満たしていることの保証と関連付けられたアクティビティの一部として行ってもよい。このリストを利用して、評価者はセキュリティ関連管理インタフェースのそれぞれに、そのイベントに適切な情報を記録する監査イベントが対応していることを確認しなければならない (shall)。

評価者は、ST に定義されている、または前述の 2 つのアクティビティで識別された、あるいはその両方のイベントすべてについて､TOE に監査記録を生成させることにより TOE の監査機能をテストしなければならない (shall)。次に評価者は、監査記録がリポジトリへ書き込まれ、そこには ST により定義される属性が含まれていることを決定するために、ST、操作ガイダンス、または開発証拠資料 (利用できる場合) により定義される監査リポジトリをチェックしなければならない (shall)。

このテストは、他の機能の実施と組み合わせて行ってもよい。例えば、間違った認証秘密が入力された際に監査記録が生成されると ST に規定されている場合、識別と認証のテストの結果として監査記録が生成されることが期待できる。また評価者は、ログの内容が TOE 上で行われたアクティビティと一貫していることもチェックして保証しなければならない (shall)。例えば、利用者からのクレデンシャル情報を失効させるようなテストが行われた場合、そのイベントの監査ログには失効操作が正しく示されているべきである (should)。

FAU_STG_EXT.1 外部監査証跡ストレージ

下位階層： 他のコンポーネントなし。

FAU_STG_EXT.1.1 TSF は、一般監査データを [***割付：外部 IT エンティティまたは「TOE 内部ストレージ」あるいはその両方の空でないリスト***] へ送信できなければならない (shall)。

適用上の注意： *「送信」という用語は、TOE が主導する情報の伝送と、外部 IT エンティティからの要求に応じた TOE の情報伝送の両方に対応することを意図している。*

外部 IT エンティティの例としては､同一またはリモートプラットフォーム上の監査サーバ ESM コンポーネント、TOE とプラットフォームを共有する評価済みオペレーティングシステム、

あるいは集中型ロギングコンポーネントなどが考えられるであろう。複数ソースへの送信は許容される。

FAU_STG_EXT.1.2 TSF は、あらゆる外部 IT エンティティへの生成された監査データの送信が、FTP_ITC.1 に定義される高信頼チャネルを用いて行われることを保証しなければならない (shall)。

FAU_STG_EXT.1.3 TSF は、生成された監査データのあらゆる TOE 内部ストレージが、以下のとおりであることを保証しなければならない (shall)：

a) TOE 内部監査証跡に保存された監査記録を、不正な削除から保護すること；及び

b) TOE 内部監査証跡に保存された監査記録への不正な変更を防止すること。

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

適用上の注意： *この要件は、生成された監査データを 1 つ以上の外部 IT エンティティまたは製品へ送信する能力を提供するものである。また、ローカルなストレージと生成された監査データの保護もサポートする (おそらく、外部 IT エンティティとの通信が利用できない際の一時的な手段として)。ST 作成者は、この要件に指定される外部 IT エンティティが利用できなくなった際に監査データがどのように記録されるのか、そして通信が再確立された際に同期がどのように達成されるのかを示さなければならない (must)。*

保証アクティビティ：

評価者は、TOE がその監査データを保存する場所と、その場所がリモートの場合そのデータを通過中に保護するために用いられる高信頼チャネルが、TSS に記述されていることを決定するために TSS をチェックしなければならない (shall)。

評価者は、監査ストレージを設定するために必要な任意の構成ステップが列挙されていることを決定するために、操作ガイダンスをチェックしなければならない (shall)。また監査データがリモートリポジトリに保存される場合、評価者は、このリポジトリへのインタフェースに関する議論が、リポジトリへの接続が確立される方法、データが渡される方法、

そしてリポジトリへの接続が失われてその後再確立された際に何が起こるのかを含めて、提供されていることを決定するために、操作ガイダンスをチェックしなければならない (shall)。

評価者は、構成された監査の送信先のそれぞれに、監査記録の同一のセットが受信されていることを確認することにより、FAU_GEN.1 のテストと組み合わせてこの機能をテストしなければならない (shall)。また評価者は、外部監査ストレージへの接続を利用できない状態として、TOE 上で監査対象イベントを発生させ、接続を再確立し、そして外部監査証跡ストレージがローカルなストレージと同期していることを確認しなければならない (shall)。FAU_GEN.1 のテストと同様に、このテストは他の機能の実施と組み合わせて行うことができる。最後に、この要件は FTP_ITC.1 により確立される高信頼チャネル上で監査記録が送信されることを明確に要求しているため、その要件の検証を行うことにより、この要件のこの部分は十分に例証される。

6.1.4 暗号サポート (FCS)

TOE の暗号要件は、TSF により実装されてもよいし、ESM 以外の運用環境コンポーネントに依存して実装されてもよい。ここで期待されるのは、ベンダが独自にユニークで冗長な暗号機能を実装することを強要することではなく、すでに検証済みの暗号アルゴリズムのスイートが TSF に利用できることである。ST には、TSF によりどの暗号機能が利用されるのかが明確に示されなければならない (must)。暗号機能がどこに存在しようと、期待される能力は同一である。

TOE により実装される暗号プロトコルをサポートするために必要とされる暗号要件については、附属書 C.8 を参照すること。

6.1.5 識別と認証 (FIA)

FIA_USB.1 利用者−サブジェクト束縛

下位階層：	他のコンポーネントなし。
FIA_USB.1.1	TSF は、以下の利用者セキュリティ属性を、その利用者に代わって動作するサブジェクトと関連付けなければならない (shall)： [***割付：利用者セキュリティ属性のリスト***]。
FIA_USB.1.2	TSF は、利用者セキュリティ属性とその利用者に代わって動作するサブジェクトとを最初に関連付ける際に、以下のルールを実施しなければならない (shall)： [***割付：属性の最初の関連付けのルール***]。

FIA_USB.1.3　TSF は、その利用者に代わって動作するサブジェクトへ関連付けられた利用者セキュリティ属性への変更を規定する、以下のルールを実施しなければならない (shall)： [***割付：属性の変更のルール***]。

依存性：　FIA_ATD.1 利用者属性の定義

保証アクティビティ：

評価者は、最初の割付の際とそれらへ何らかの変更が行われた際の両方について、管理者へ割付けられているセキュリティ属性と、これらの属性と管理者が関連付けられている手段が記述されているかを決定するために TSS をチェックしなければならない (shall)。

評価者は、外部データソースが起動され、TSF により制御される利用者データと対応付けられるメカニズムが記述されていることを検証するために、操作ガイダンスをチェックしなければならない (shall)。

評価者は、ST に定義される通り外部ソースからの利用者情報を受容するように TSF を構成することにより、この機能をテストしなければならない (shall)。次に評価者はこれらの手法を用いて認証アクティビティを行い、各インスタンスで認証が成功することを検証しなければならない (shall)。サブジェクトのそれぞれに割付けられた定義済み特権に基づいて、利用者認証が彼らの外部定義された属性及び TSF のアクセス制御ポリシーの構成と一貫していることを決定するために、評価者は次に様々な管理テストを行わなければならない (shall)。例えば、LDAP リポジトリ中で定義された利用者があるグループに属しており、そのグループのメンバーがデータのあるセットに対して読み出しのみのアクセス権しか持たないように TSF が構成されている場合、評価者はその利用者として TSF へ認証を行い、TSF の制御下のサブジェクトとして彼らがそのデータへの書き込みアクセス権を持たないことを検証しなければならない (shall)。これにより、TSF が利用者を取り扱う方法に関連した利用者の識別情報データの側面が、外部ソースから適切に取り込まれ、利用者に何が行えるかを決定するために利用されることが検証される。

6.1.6 セキュリティ管理 (FMT)

FMT_MOF.1 機能のふるまいの管理

下位階層：　他のコンポーネントなし。

FMT_MOF.1　TSF は機能： [***割付：機能のリスト***] の [選択：ふるまいを決定する、無効化を行う、有効化を行う、ふるまいを変更する] 能力を、 [***割付：正当な識別された役割***] に制限しなければなら

ない (shall)。

適用上の注意： *最初の割付は、FMT_SMF.1 に定義される管理機能と対応していることが期待される。*

2 番目の割付は、FMT_SMR.1 に識別される役割と対応していることが期待される。

依存性： FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の仕様

保証アクティビティ：

評価者は、1 つまたは複数の適用上の注意により提供されるガイダンスと一貫した形で割付が行われていることを決定するために、TSS をチェックしなければならない (shall)。また評価者は TSS をチェックして、要求される管理機能及びこれを行うために要求される権限付与を TSF が行う能力が記述されていることを確認しなければならない (shall)。

評価者は、これらの属性の管理に対してどのような制約が課されているか、そして TSF がそれらをどのように実施するかを決定するために、操作ガイダンスをレビューしなければならない (shall)。例えば、管理権限が役割ベースのものであれば、操作ガイダンスにこれが示されなければならない (shall)。

評価者は、1 つ以上の適切な特権を持つ管理アカウントを用いて TSF にアクセスし、ST 及び操作ガイダンスに記述される管理機能が、操作ガイダンス中に提供される任意の指示と一貫した形で管理できることを決定することにより、この機能をテストしなければならない (shall)。TSF が正当な互換性のあるセキュア構成管理製品により構成可能である場合、評価者はまた TSF を管理するようにそのような製品を構成し、定義された管理アクティビティをこの製品を用いて行わなければならない (shall)。さらに、このふるまいへの任意のアクセスの制約は、関連する文書と一貫した形で実施されるべきである (should)。評価者は、特権を持たない 1 つ以上のアカウントを用いて利用可能な管理機能のサンプルの実行を試行し、そのアクティビティが拒否されるか利用できないことを確認することにより、これをテストしなければならない (shall)。

FMT_SMF.1 管理機能の仕様

下位階層： 他のコンポーネントなし。

FMT_SMF.1 TSF は、以下の管理機能を行えなければならない (shall)： [***割付：TSF により提供される管理機能のリスト***]。

依存性： 依存性なし。

適用上の注意： 管理機能は、最も広いレベルにおいて、最低でも以下の表 4 に指定される機能を含まなければならない (must)。ST 作成者は、定義された機能が文書のそれ以外の部分で主張されるあらゆる機能的ふるまいを管理するのに十分であることを保証しなければならない (must)。

表 4. TOE 管理機能

要件	管理アクティビティ
ESM_ATD.1 (オプション)	オブジェクト属性の定義 オブジェクトと属性との関連付け
ESM_EAU.2	対話的利用者と正当な IT エンティティの両方に関する認証データの管理 (TSF により管理される場合)
ESM_EID.2	対話的利用者と正当な IT エンティティの両方に関する認証データの管理 (TSF により管理される場合)
ESM_ICD.1	利用者と関連付け可能な識別情報とクレデンシャル情報データの定義 (活性化、中断、クレデンシャル情報の失効など)
ESM_ICD.1	クレデンシャル情報の状態の管理
ESM_ICD.1	リポジトリへの利用者の登録
ESM_ICT.1	識別情報とクレデンシャル情報データ (及び、該当する場合オブジェクト属性) の送信が行われる状況の構成
FAU_SEL.1 (オプション)	管理対象イベントの構成
FAU_STG_EXT.1	外部監査ストレージの場所の構成
FIA_AFL.1 (オプション)	認証試行の不成功の閾値の管理 認証失敗の際に取られるアクションの管理
FIA_SOS.1 (オプション)	秘密を検証するために用いられる測定基準の管理
FIA_USB.1	デフォルトのサブジェクトセキュリティ属性の定義、サブジェクトセキュリティ属性の変更
FMT_MOF.1	セキュリティ機能と対話可能な利用者のセットの管理
FMT_SMR.1	特定の役割に属する利用者の管理
FTA_SSL_EXT.1 (オプション)	セション終了の非アクティブ継続時間の構成
FTA_SSL.3 (オプション)	セション終了の非アクティブ継続時間の構成
FTA_TAB.1	バナーの維持
FTA_TSE.1 (オプション)	セション確立条件の管理

要件	管理アクティビティ
FTP_ITC.1	高信頼チャネルを要求するアクションの構成 (該当する場合)
FTP_TRP.1	高信頼パスを要求するアクションの構成 (該当する場合)

保証アクティビティ：

評価者は、利用可能な管理機能が要約されていることを決定するために TSS をチェックしなければならない (shall)。

評価者は、TSF に対して行うことのできる管理機能のすべてと、それらを行う方法、そしてそれらにより何が達成されるか定義されていることを決定するために、操作ガイダンスをチェックしなければならない (shall)。

評価者は、TOE へアクセスして、定義された管理機能のすべてが存在すること、これらが規定されたやり方で行えること、そしてこれらが文書化された機能を達成することを検証することにより、この機能をテストしなければならない (shall)。

FMT_SMR.1 セキュリティ管理役割

下位階層： 他のコンポーネントなし。

FMT_SMR.1.1 TSF は、役割 [**割付：権限を持つ識別された役割**] を維持しなければならない (shall)。

適用上の注意： *本プロテクションプロファイルでは割付管理者という用語を用いて、識別情報とクレデンシャル情報 (及び潜在的にオブジェクト) 属性を定義し管理する権限のある個人を表している。これは、この権限が個人へ与えられるべきである (should) ということを反映した論理的な構成概念として解釈されるべきであり (should)、この権限を持つ誰かを TSF が「割付管理者」という用語で表現しなければならない (must) ということを明示的に義務付けるものではない。*

FMT_SMR.1.2 TSF は、利用者を役割と関連付けることができなければならない (shall)。

適用上の注意： *利用者に代わって動作する正当な互換性のあるセキュア構成管理製品もまた、役割と関連付けられ得る。*

依存性： FIA_UID.1 認証のタイミング

保証アクティビティ：

評価者は TSS をレビューして、TOE に定義されている役割を決定しなければならない (shall)。また評価者は TSS をレビューして、この SFR により定義される役割が、管理権限付与がどのように決定されるかという議論の際に一貫して参照されていることを検証しなければならない (shall)。

評価者は、利用者へ役割を割付ける方法に関する指示が提供されていることを検証するために、操作ガイダンスをレビューしなければならない (shall)。すべての利用者へ自動的に割付けられる単一の役割のみを TSF が提供する場合、評価者は操作ガイダンスをレビューしてこの事実が主張されていることを検証しなければならない (shall)。

評価者は、操作ガイダンスにより指定される形で TOE を用いて利用できる役割のそれぞれを異なる利用者へ関連付けることにより、この能力をテストしなければならない (shall)。追加的な役割を定義する能力を TSF が提供する場合、評価者は少なくとも 1 つの新たな役割を作成して、利用者がそれに割付可能であることを保証しなければならない (shall)。管理要件のその他の保証アクティビティには評価者が TOE 上の異なる役割を帯びることが必要とされるため、これらのテストアクティビティはそれらの他の保証アクティビティを行う過程で対応されることもあり得る。

6.1.7 TSF の保護

FPT_APW_EXT.1 保存されたクレデンシャル情報の保護

下位階層：	他のコンポーネントなし。
FPT_APW_EXT.1.1	TSF は、クレデンシャル情報を平文以外の形態で保存しなければならない (shall)。
FPT_APW_EXT.1.2	TSF は、平文のクレデンシャル情報が読み出されることを防止しなければならない (shall)。
適用上の注意：	*この要件の意図は、生の認証データが平文で保存されず、またいかなる利用者または管理者も生の認証データを「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であれば、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。* *TOE が外部の識別情報とクレデンシャル情報管理製品を利用してその管理者認証データを定義する場合、この SFR の目的は、*

そのデータのコピーが入力される際 TOE により保存または保持されないことを保証することである。

依存性： 依存性なし。

保証アクティビティ：

評価者は、FPT_SKP_EXT.1 により対処されるプライベート鍵を除き、TSF により利用または保存されるすべての認証データと、平文のクレデンシャル情報データを保存の際にあいまい化するために用いられる手法が詳述されていることを決定するため、TSS を検査しなければならない (shall)。これには、TOE が運用環境中のサービスへアクセスするために用いる任意のクレデンシャル情報データ (保存されたスクリプトに見いだされるようなもの) と、TOE が利用者の認証を行う場合 TOE により保存されるクレデンシャル情報データが含まれる。また TSS には、適用上の注意に概説したように、特にその目的に設計することンタフェースを通して閲覧できないようにクレデンシャル情報が保存されることを保証するために用いられるメカニズムも記述されなければならない (shall)。あるいは、認証データの権威リポジトリが運用環境中にあるため TOE により保存されることがない場合、そのことが TSS に詳述されなければならない (shall)。

この SFR には、操作ガイダンスのアクティビティは存在しない。

評価者は、すべての識別されたクレデンシャル情報リポジトリをレビューして、クレデンシャル情報があいまい化されて保存されること、そしてリポジトリが管理者以外の利用者からアクセスできないことを保証することにより、この SFR をテストしなければならない (shall)。管理者は同様に、運用環境中のシステムへアクセスするために用いられるメカニズムのすべてのスクリプトとストレージをレビューして、クレデンシャル情報があいまい化されて保存されること、そしてデータが管理者以外の利用者からアクセスできないようにシステムが構成されていることを保証しなければならない (shall)。

FPT_SKP_EXT.1 秘密鍵パラメタの保護

下位階層： 他のコンポーネントなし。

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が読み出されることを防止しなければならない (shall)。

適用上の注意： *この要件の意図は、識別された鍵 (保存されたもの、または短期的なもの) を「通常の」インタフェースを介して管理者が読み出したり閲覧したりできないことである。管理者が直接メモリを読み出してこれらの鍵を閲覧することが可能であることは*

理解されているが、それは簡単なタスクではなく、管理者の側での多大な作業を要求し得る。管理者は高信頼エージェントであると見なされるため、彼らはそのようなアクティビティを試みないだろうと想定される。

依存性： 依存性なし。

保証アクティビティ：

評価者は、任意の事前共有鍵、対称鍵、及びプライベート鍵がどのように保存されるか、そして特にその目的に設計することンタフェースを通してそれらを閲覧できないことが詳述されていることを決定するため、TSS を検査しなければならない (shall)。これらの値が平文で保存されない場合、TSS にはそれらがどのように保護／あいまい化されるか記述されなければならない (shall)。

この SFR には、操作ガイダンスまたはテストのアクティビティは存在しない。

6.1.8 TOE アクセス (FTA)

注意：本ファミリの SFR は、管理ユーザの利用者セションに適用される。

FTA_TAB.1 TOE アクセスバナー

下位階層： 他のコンポーネントなし。

FTA_TAB.1.1 *詳細化：*利用者セション確立前に、TSF は、TOE の不正な使用に関する注意を喚起する*設定可能な*警告メッセージを表示しなければならない (shall)。

依存性： 依存性なし。

保証アクティビティ：

評価者は、管理者の認証に先立って設定可能なバナーを表示する TSF の能力が論じられていることを決定するために、TSS をチェックしなければならない (shall)。

評価者は、TOE バナーが表示及び設定される方法を決定するため、操作ガイダンスをレビューしなければならない (shall)。

バナーがデフォルトでは表示されない場合、評価者はその表示を有効化するために操作ガイダンスに従って TOE を構成しなければならない (shall)。次に評価者は TOE へのアクセスを試行し、TOE バナーが存在することを検証しなければならない (shall)。該当する場合、評価者は FMT_SMF.1 に定義される規格に従った TOE アクセスバナーを変更するため

の機能の利用を試行して、TOE アクセスバナーが適切に更新されることも検証すること。

6.1.9 高信頼パス／チャネル (FTP)

FTP_ITC.1 TSF 間高信頼チャネル

下位階層：	他のコンポーネントなし。
FTP_ITC.1.1	*詳細化：*TSF は、それ自身と*正当な IT エンティティ*との間に、*[選択：[**割付：FCS に規定されたサービスにより実装された 1 つまたは複数の暗号プロトコル**]、[**割付：運用環境中のコンポーネントにより実装された明確に定義された FIPS 準拠プロトコル**]]* 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、及び改変及び暴露からのチャネルデータの保護を提供する*高信頼*通信チャネルを提供しなければならない (shall)。
適用上の注意：	*ST 作成者は、FCS サービスが TSF 内部のものか、運用環境により提供されるものかを示さなければならない (must)。*
FTP_ITC.1.2	TSF は、[選択：TSF、他の高信頼 IT 製品] が、高信頼チャネルを介して通信を開始するのを許可しなければならない (shall)。
FTP_ITC.1.3	*詳細化：*TSF は、*ポリシーデータの送信*、[***割付：その他の機能***] 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 (shall)。
適用上の注意：	*ST 作成者は、TOE が他の ESM 製品と行うすべての保護された通信 (監査データの送信、識別情報データの要求など) を割付に記述しなければならない (must)。認証応答の伝送は、その送信に用いられる高信頼チャネルが、応答を提供する製品により開始されるか、あるいは当初のチャレンジの伝送を行うために用いられた TSF により開始されたものと同一のチャネルであるかのいずれかであると想定されるため、ここに列挙されないことに注意すること。* *TOE が複数の PP への適合を主張する場合、TOE の分散コンポーネントへのリモートインタフェースはここに主張されるとともに、あたかも運用環境へのインタフェースであるかのように評価されなければならない (must)。*

依存性： 依存性なし。

保証アクティビティ：

評価者は、1 つまたは複数の適用上の注意により提供されるガイダンスと一貫した形で割付が行われていることを決定するために、TSS をチェックしなければならない (shall)。また評価者は TSS をチェックして、確立される高信頼チャネルとそれにより用いられるプロトコルが識別されていることを確認しなければならない (shall)。サードパーティの暗号が用いられる場合、評価者は用いられる具体的なサードパーティ製品と、それらがセキュア化を担当する 1 つまたは複数のチャネルが識別されていることをチェックして保証しなければならない (shall)。また評価者は TSS をチェックして、セキュアな通信が利用される手段に関する議論が提供されていることを保証しなければならない (shall)。これに基づいて、以下の分析が必要とされる。

- *暗号機能が TOE 内部のものである場合、評価者はその製品が FIPS 140-2 (米国またはカナダでの評価の場合) または評価が実施される国における同等の国家標準により有効性が確認されていることを検証しなければならない (shall)。*
- *暗号機能が運用環境により提供される場合、評価者は設計文書をレビューして暗号機能が利用される方法を確認し、その製品が FIPS 140-2 (米国またはカナダでの評価の場合) または評価が実施される国における同等の国家標準により有効性が確認されていることを検証しなければならない (shall)。*

評価者は、セキュアな通信が有効化されるメカニズムを決定するため、操作ガイダンスをチェックしなければならない (shall)。

評価者は、TOE 上でセキュアな通信を有効化してローカルネットワーク上にパケットスニファを設置することにより、この機能をテストしなければならない (shall)。次に TOE を用いて、それが通信するすべての高信頼 IT 製品との通信を要求するアクションを行い、TOE へ、または TOE からのキャプチャされたパケットトラフィックを確認して、その内容があいまい化されていることを保証しなければならない (shall)。

FTP_TRP.1 高信頼パス

下位階層： 他のコンポーネントなし。

FTP_TRP.1.1 *詳細化：*TSF は、それ自身と [リモート] 利用者との間に、*[選択：[**割付：FCS に規定されたサービスにより実装された 1 つまたは複数の暗号プロトコル**]、[**割付：運用環境中のコンポーネントにより実装された明確に定義された FIPS 準拠プロトコ*

ル]] を用いて、他の通信パスと論理的に区別され、その端点の保証された識別と、[改変、暴露] からの通信データの保護を提供する通信パスを提供しなければならない (shall)。

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

FTP_TRP.1.3　*詳細化:*TSF は、*最初の利用者認証、管理機能の実行*に対して、高信頼パスの利用を要求しなければならない (shall)。

依存性：　依存性なし。

保証アクティビティ：

評価者は TSS をチェックして、高信頼パスの確立に用いられる 1 つまたは複数のプロトコルが識別されていることを保証しなければならない (shall)。サードパーティの暗号が用いられる場合、評価者は用いられる具体的なサードパーティ製品が識別されていることをチェックして保証しなければならない (shall)。

評価者は操作ガイダンスをチェックして、例えば HTTPS を介したウェブアプリケーションなど、利用者が TOE と対話する手法が議論されていることを確認しなければならない (shall)。また評価者は操作ガイダンスをチェックして、TOE への高信頼パスが確立されるメカニズムが議論されているかどうかと、この確立に役立てるため TSF が依存している環境コンポーネントが (もしあれば) 何かを決定しなければならない (shall)。

評価者は、FTP_ITC.1 に関する保証アクティビティと同様のやり方で、この機能をテストしなければならない (shall)。利用者と TOE との間で送信されるデータがあいまい化されている場合、高信頼パスが確立されていると推定できる。

6.1.10 満たされていない依存性

本節では、本 PP のために選択された要件の依存性として列挙されたが、主張されていないセキュリティ機能要件 (SFR) について詳述する。そのような要件のそれぞれについて、それを除外した根拠が提供されている。

FIA_ATD.1　この SFR は、FIA_USB.1 に関して満たされていない依存性である。ESM_ICD.1 が同様なやり方で依存性を満たすことが期待されるため、これは含まれていない。

FIA_UAU.1　この SFR は、FIA_AFL.1 に関して満たされていない依存性である。ESM_EAU.2 が、同等の機能を提供することによりこの

	依存性を満たす。
FIA_UID.1	この SFR は、FMT_SMR.1 に関して満たされていない依存性である。ESM_EID.2 が、同等の機能を提供することによりこの依存性を満たす。
FPT_STM.1	この SFR は、FAU_GEN.1 に関して満たされていない依存性である。TOE は必ずしも独自のシステムクロックを含んでいるとは期待できないため、この要件は含まれていない。ST 作成者は、システム時間の原点を決定するため、評価対象の ESM 全体を検査しなければならない (must)。評価（訳注：評価対象）の境界が内部システムクロックを用いる ESM アプライアンス全体である場合、FPT_STM.1 が主張されなければならない (must)。しかし、ホストオペレーティングシステムや NTP サーバ等の環境コンポーネントに ESM が依存している場合、正確なシステム時間を環境の対策方針として提示することが受容可能な代替策である。

6.2 セキュリティ保証要件

節 8.4.1 の TOE に関するセキュリティ対策方針は、節 8.2 に識別される脅威へ対処するために構築された。節 6.1 (及び附属書 C - アーキテクチャの変動と追加的要件) のセキュリティ機能要件 (SFR) は、セキュリティ対策方針の形式的な実体化である。PP は EAL1 からセキュリティ保証要件 (SAR) を選び出し、評価者が評価の対象となる文書を評定して独立テストを行う範囲を設定する。

節 6.1 への概論に示したように、本節には CC からの SAR の完全なセットが含まれている一方で、評価者により行われるべき保証アクティビティは本節と共に節 6.1 (及び附属書 C - アーキテクチャの変動と追加的要件) の両方で詳述されている。

それぞれのファミリには、(もしあれば) 開発者により提供される必要のある追加的文書／アクティビティを明確にするため、開発者アクションエレメントについて「開発者への注意」が提供される。内容／提示及び評価者アクティビティエレメントについては、エレメントごとにではなく、ファミリ全体について追加的アクティビティ (節 6.1 にすでに含まれているものに加えて) が記述されている。さらに、本節に記述された保証アクティビティは、節 6.1 に規定されたものとは相補的な関係にある。

TOE のセキュリティ保証要件は表 5 に要約されており、本 PP の節 8.2 に識別される脅威へ対処するために要求される管理及び評価アクティビティが識別されている。節 6.3 では、

本節のセキュリティ保証要件を選択したことについての簡潔な正当化が提供される。

表 5. TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネントの記述
開発	ADV_FSP.1	基本機能仕様
ガイダンス文書	AGD_OPE.1	利用者操作ガイダンス
	AGD_PRE.1	利用者準備ガイダンス
ライフサイクルサポート	ALC_CMC.1	TOE のラベル付け
	ALC_CMS.1	TOE CM カバレージ
テスト	ATE_IND.1	独立テスト—適合
脆弱性の評定	AVA_VAN.1	脆弱性調査

6.2.1 ADV クラス：開発

本 PP に適合する TOE については、TOE に関する情報は ST の TOE 要約仕様 (TSS) 部分とともに、エンドユーザに利用可能なガイダンス文書にも含まれることが予想される[7]。TOE 開発者が TSS を作成することは要求されてはいないが、TOE 開発者は TSS に含まれる製品の記述を、機能仕様との関連において一致させなければならない (must)。各 SFR と関連付けられる保証アクティビティは、TSS 節にふさわしい内容を決定するために十分な情報を ST 作成者へ提供すべきである (should)。

6.2.1.1 基本機能仕様 (ADV_FSP.1)

機能仕様は、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規定は必要とされない。さらに、本 PP に適合する TOE は必然的に TOE の利用者により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それ自体を規定することにはあまり意味がない。そのようなインタフェースは間接的なテストしかできないためである。本 PP の本ファミリに関するアクティビティは、機能仕様へ対応した形で TSS に提示されるインタフェースと AGD 文書に提示されるインタフェースを理解することに焦点をしぼらなければならない (must)。規定された保証アクティビティを満たすために、追加的な「機能仕様」文書が必要とされるべきではない (should not)。

[7] 独占的 (proprietary) な詳細が必要とされる場合、開発者には追加的な文書を提供するという選択肢もあるが、ほとんどすべての情報は公共向けの文書に含まれるべきである (should)。

評価される必要のあるインタフェースは、独立した抽象的なリストとしてではなく、列挙された保証アクティビティを行うために必要な情報を通して特徴づけされる。

開発者アクションエレメント：

ADV_FSP.1.1D　開発者は、機能仕様を提供しなければならない (shall)。

ADV_FSP.1.2D　開発者は、機能仕様から SFR への追跡を提供しなければならない (shall)。

開発者への注意：　本節の概論で述べたように、機能仕様は AGD_OPE 及び AGD_PRE 文書に含まれる情報と、ST の TSS に提供される情報との組み合わせで構成される。これにはまた、公的に利用可能な任意のプロトコルまたは開発証拠資料中で参照されている API 文書あるいはその両方が含まれることになる。機能仕様中の保証アクティビティは、文書及び TSS 節に存在すべき (should) 証拠資料を参照している。これらは SFR と直接関連付けられているため、エレメント ADV_FSP.1.2D 中の追跡は暗黙にはすでになされており、追加的な文書は必要とされない。

内容・提示エレメント：

ADV_FSP.1.1C　機能仕様は、SFR 実施及び SFR 支援の各 TSFI の目的と使用方法を記述しなければならない (shall)。

ADV_FSP.1.2C　機能仕様は、SFR 実施及び SFR 支援の各 TSFI に関連するすべてのパラメタを識別しなければならない (shall)。

ADV_FSP.1.3C　機能仕様は、暗黙的に SFR 非干渉として分類されているインタフェースについて、その分類の根拠を示さなければならない (shall)。

ADV_FSP.1.4C　追跡は、機能仕様での TSFI に対する SFR の追跡を実証するものでなければならない (shall)。

評価者アクションエレメント：

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

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

保証アクティビティ：

これらの SAR に関連付けられた具体的な保証アクティビティは存在しない。機能仕様文書は各 SFR に記述された評価アクティビティと、AGD、ATE、及び AVA SAR に関して記述されたその他のアクティビティをサポートするために提供されている。機能仕様情報の内容についての要件は、行われるその他の保証アクティビティの特質により暗黙に評定される。不十分なインタフェース情報しか存在しなかったために評価者がアクティビティを行うことができなかった場合、十分な機能仕様が提供されていなかったことになる。例えば、TOE が暗号アルゴリズムの鍵長を設定する機能を提供しているが、この機能を行うためのインタフェースを指定していない場合、FMT_SMF に関連付けられた保証アクティビティは失敗することになるだろう。

評価者は、TOE が傍受する、または協業するインタフェースのセットが TOE 機能仕様に記述されていることを検証しなければならない (shall)。評価者はこれらのインタフェースの記述を検査して、それらの呼び出しに関する十分な記述が含まれていることを検証しなければならない (shall)。

6.2.2 AGD クラス：ガイダンス文書

ガイダンス文書は、開発者のセキュリティターゲットと共に提供される。ガイダンスには、運用環境がセキュリティ機能にそれ自身の役割を果たすことができることを正当な利用者が検証する方法の記述が含まれなければならない (must)。本文書は、正当な利用者により読解可能な非形式的なスタイルでなければならない (must)。

製品がサポートすると ST で主張されているすべての運用環境について、ガイダンスが提供されなければならない (must)。このガイダンスには、以下が含まれる。

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

また、TOE がシステムの起動中に改変されたりシステム起動シーケンスから完全に取り除かれたりできないように、ホストオペレーティングシステム上で TOE を安全な構成へブートする方法に関するガイダンスも提供されなければならない (must)。さらに、信頼されないサブジェクトによる無効化 (例えばシャットダウン) を防止するように製品を構成する方法も記述されなければならない (must)。

また、特定のセキュリティ機能に関するガイダンスも提供される。そのようなガイダンスに関する要件は、各 SFR と共に規定された保証アクティビティに含まれている。

6.2.2.1 利用者操作ガイダンス (AGD_OPE.1)

開発者アクションエレメント：

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

開発者への注意： ここで繰返し情報を提示するのではなく、開発者はこのコンポーネント及び SFR に関する保証アクティビティをレビューして、評価者がチェックすることになるガイダンスの詳細を理解すべきである (should)。これにより、受容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。

内容・提示エレメント：

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

適用上の注意： *評価者は、この記述が完全かつ正確なものであることを保証するため、TOE 上のこれらの利用者アクセス可能な機能を実行しなければならない (must)。*

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

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

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

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

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

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

評価者アクションエレメント：

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

保証アクティビティ：

操作ガイダンスの内容の一部は、各 SFR に付随する保証アクティビティにより検証されることになる。また、以下の追加情報も必要となる。

操作ガイダンスには、TOE の評価される構成と関連付けられた暗号エンジンを構成するための指示が含まれなければならない (shall)。TOE の CC 評価の中で、他の暗号エンジンの利用が評価もテストもされなかったという警告が、管理者へ与えられなければならない (shall)。

6.2.2.2　準備手続き (AGD_PRE.1)

開発者アクションエレメント：

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

開発者への注意：　操作ガイダンスと同様に、開発者は保証アクティビティを調査して準備手続きに関して必要とされる内容を決定すべきである (should)。

内容・提示エレメント：

AGD_ PRE.1.1C　準備手続きは、開発者の配付手続きに従って配付された TOE

のセキュアな受け入れに必要なすべてのステップを記述しなければならない (shall)。

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

評価者アクションエレメント：

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

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

保証アクティビティ：

上の概論で述べたように、特に TOE の機能要件をサポートする運用環境の構成にあたっては、文書に関して多大な期待が存在する。評価者は、TOE に提供されたガイダンスが、ST 中に TOE について主張されているすべてのプラットフォーム (すなわち、ハードウェアとオペレーティングシステムの組み合わせ) へ十分に対応していることをチェックして保証しなければならない (shall)。

6.2.3 ALC クラス：ライフサイクルサポート

本 PP 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調査ではなく、ライフサイクルのエンドユーザに可視の側面に限定される。これは、製品の全体的な信頼度の向上に開発者のプラクティスが果たす重要な役割を減じようとするものではない。そうではなく、この保証レベルにおける評価に関して利用可能とされるべき情報を反映したものである。

6.2.3.1 TOE のラベル付け (ALC_CMC.1)

このコンポーネントは、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り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。

開発者アクションエレメント：

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

(shall)。

内容・提示エレメント：

ALC_CMC.1.1C　TOE は、その一意な参照でラベル付けされなければならない(shall)。

評価者アクションエレメント：

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

保証アクティビティ：

評価者はST をチェックして、ST の要件を満たすバージョンを具体的に識別する識別情報(製品名／バージョン番号など) が含まれていることを保証しなければならない (shall)。さらに、評価者はAGD ガイダンス及びテスト用に受け取ったTOE サンプルをチェックして、バージョン番号がST 中のものと一貫していることを保証しなければならない (shall)。ベンダがTOE を宣伝するウェブサイトを維持している場合、評価者は、ST 中の情報がその製品を識別するために十分であることを保証するため、そのウェブサイト上の情報を検査しなければならない (shall)。

6.2.3.2　TOE CM カバレージ (ALC_CMS.1)

TOE の対象範囲とそれに関連した評価証拠の要件を考慮して、このコンポーネントの保証アクティビティは ALC_CMC.1 に関して列挙された保証アクティビティによりカバーされる。

開発者アクションエレメント：

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

内容・提示エレメント：

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

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

評価者アクションエレメント：

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

保証アクティビティ：

本 PP において「SAR により要求される評価証拠」は、ST 中の情報と、AGD 要件の下で管理者及び利用者に提供されるガイダンスとの組み合わせに限られる。TOE が具体的に識別され、その識別情報が ST 及び AGD ガイダンスの内容と一貫していることを (ALC_CMC.1 に関する評価アクティビティ中で行われるように) 保証することにより、評価者はこのコンポーネントにより要求される情報を暗黙に確認する。

6.2.4 ATE クラス：テスト

テストは、システムの機能的側面と、設計または実装の弱点を利用する側面について指定される。前者は ATE_IND ファミリにより行われるが、後者は AVA_VAN ファミリにより行われる。本 PP に規定された保証レベルにおいては、テストは通知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、以下の要件に指定されるテスト報告である。

6.2.4.1 独立テスト—適合 (ATE_IND.1)

テストは、TSS と提供された管理 (構成及び操作を含む) 文書に記述された機能を確認するために行われる。テストで重視されるのは、各 SFR に規定された要件が満たされていることの確認であるが、いくつかの追加的テストが節 6.2 中の SAR について規定されている。保証アクティビティは、これらのコンポーネントと関連付けられた最小テストアクティビティを識別する。評価者は、テストの計画及び結果、ならびに本 PP への適合を主張するプラットフォーム／TOE の組み合わせに焦点を絞ったカバレージの論拠を文書化した、テスト報告を作成する。

開発者アクションエレメント：

ATE_IND.1.1D　開発者は、テストのために TOE を提供しなければならない (shall)。

内容・提示エレメント：

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

評価者アクションエレメント：

ATE_IND.1.1E　評価者は、提供された情報が、証拠の内容・提示のすべての要

件を満たしていることを確認しなければならない (shall)。

ATE_IND.1.2E　評価者は、TSF が仕様どおりに動作することを確認するために、TSF のサブセットをテストしなければならない (shall)。

保証アクティビティ：

評価者は、システムのテストの側面を文書化したテスト計画とテスト報告を作成しなければならない (shall)。テスト計画は、本 PP の保証アクティビティの本体に含まれるすべてのテストアクションをカバーする。保証アクティビティ中に列挙されたテストのそれぞれについて 1 つのテストケースを用意する必要はないが、ST 中の該当するテスト要件のそれぞれがカバーされていることを評価者はテスト計画中に文書化しなければならない (shall)。

テスト計画にはテストされるプラットフォームが識別され、そしてテスト計画には含まれないが ST に含まれるプラットフォームについては、そのプラットフォームをテストしないことについての正当化をテスト計画が提供する。この正当化には、テストされるプラットフォームとテストされないプラットフォームとの違いを取り上げ、行われようとしているテストにその違いが影響しないという論拠を示さなければならない (shall)。単にその違いが影響しないと主張するだけでは十分ではなく、根拠が提供されなければならない (shall)。ST 中に主張されるすべてのプラットフォームがテストされる場合、根拠は必要とされない。

テスト計画にはテストされるべき各プラットフォームの構成が記述され、また AGD 文書に含まれるもの以外に必要な設定があれば、それも記述される。テストの一部としての、または標準的なテスト前の条件としての、各プラットフォームの設置及び設定について、評価者が AGD 文書にしたがうことが期待されていることには注意すべきである (should)。これには、特別なテストドライバまたはツールも含まれるかもしれない。ドライバまたはツールのそれぞれについて、そのドライバまたはツールが TOE 及びそのプラットフォームによる機能の実行に悪影響を与えないという、(単なる主張ではなく) 論拠が提供される。またこれには、用いられるべき暗号エンジンの構成が含まれる。このエンジンにより実装される暗号アルゴリズムは、本 PP により規定され、評価される暗号プロトコル (IPsec, TLS/HTTPS, SSH) により用いられるものである。

テスト計画には、高レベルのテスト目的とともに、これらの目的を達成するために行われるべきテスト手順も識別される。これらの手順には、期待される結果も含まれる。テスト報告 (テスト計画へ単に注釈を加えたものであってもよい) には、テスト手順が実施された際に行われたアクティビティが詳述され、またテストの実際の結果が含まれる。これは累積的な記述でなければならない (shall)。従って失敗に終わったテストの実行が存在し、

修正がインストールされ、そして次にテストの再実行が成功した場合、報告には単なる「成功」の結果だけではなく、「失敗」及び「成功」の結果 (及びそれを支持する詳細) が示される。

6.2.5 AVA クラス：脆弱性評定

本プロテクションプロファイルの第一世代については、オープンソースの調査を行って、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出すことが評価機関に期待される。多くの場合、これらの脆弱性には基本的な攻撃者を超える巧妙さが必要とされる。ペネトレーションツールが作成されて評価機関へあまねく配付されるまでは、評価者には TOE 中のこれらの脆弱性のテストを行うことは期待されない。評価機関には、ベンダにより提供された文書を考慮して、これらの脆弱性の存在する可能性についてコメントすることが期待される。この情報はペネトレーションテストツールの開発と、将来のプロテクションプロファイルの開発のために用いられることになる。

6.2.5.1 脆弱性調査 (AVA_VAN.1)

開発者アクションエレメント：

AVA_VAN.1.1D 開発者は、テストのために TOE を提供しなければならない (shall)。

内容・提示エレメント：

AVA_VAN.1.1C TOE は、テストに適したものでなければならない (shall)。

評価者アクションエレメント：

AVA_VAN.1.1E 評価者は、提供された情報が、証拠の内容。提示のすべての要件を満たしていることを確認しなければならない (shall)。

AVA_VAN.1.2E 評価者は、TOE の潜在的脆弱性を識別するために、公知の情報源の探索を実行しなければならない (shall)。

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

保証アクティビティ：

ATE_IND と同様に、評価者は報告を作成し、この要件に関連する自分たちの結論を文書化しなければならない (shall)。この報告は、物理的には ATE_IND に言及される全体的なテ

スト報告の一部であってもよいし、あるいは別個の文書であってもよい。評価者は、公開情報の検索を行って、このカテゴリの ESM アプリケーション一般に発見されている脆弱性と、特定の TOE に関する脆弱性を決定する。評価者は、参考としたソースと発見された脆弱性を報告中に文書化する。発見された脆弱性のそれぞれについて、評価者はそれが該当しないことを示す根拠を提供するか、あるいはそのほうが適切であれば脆弱性を確認するためのテストを (ATE_IND に提供されるガイドラインを用いて) 策定するかのどちらかを行う。どちらが適切かは、その脆弱性を利用するために必要とされる攻撃ベクトルの評定により決定される。例えば、ブート時にあるキーの組み合わせを押すことにより脆弱性が検出できる場合、本 PP の保証レベルにおいてはテストが適切であろう。例えば、脆弱性の悪用に電子顕微鏡と液体窒素が必要とされる場合、テストは適切ではなく、適切な根拠が策定されることになるであろう。

6.3 セキュリティ保証要件の根拠

これらのセキュリティ保証要件を選択した根拠は、本 PP がこの技術に関する最初の米国政府プロテクションプロファイルだからである。これらの種類の製品に脆弱性が発見された場合、より厳格なセキュリティ保証要件が、現実のベンダのプラクティスに基づいて義務付けられることになる。

7 セキュリティ課題定義の根拠

本節では、セキュリティ課題定義において定義された脅威と対策方針との間の対応付けに加えて、前提条件と環境の対策方針との間の対応付けを識別する。さらに、これらの対応付けが適切であることが確認できるように、列挙された対策方針を満たすために用いられる SFR に基づいた根拠が提供される。これらの対応付けが特定のオプションの SFR が主張されているかどうかにより変化する状況では、ST 作成者を援助するために根拠の末尾に**太字のテキスト**が追加されている。

表 6. 前提条件、環境の対策方針、及び根拠

前提条件	対策方針	根拠
A.CRYPTO (オプション) — TOE は、運用環境により提供される暗号プリミティブを利用して、暗号サービスを行うこと。	**OE.CRYPTO (オプション)** — 運用環境は、通信の機密性や完全性を保証するなどのサービスを提供するために TOE が利用可能な暗号プリミティブを提供すること。	ベンダは、典型的には運用環境に実装された暗号プリミティブの利用に依存して、TOE により提供される暗号プロトコルを実行することが期待される。TOE が自分自身で暗号プリミティブを提供する場合、これは環境ではなく TOE の対策方針となる。
A.ENROLLMENT — クレデンシャル情報の割り当ての前に、利用者の識別情報を確認する定義された登録プロセスが存在すること。	**OE.ENROLLMENT** — 運用環境は、クレデンシャル情報の割り当ての前に、利用者の識別情報を確認する定義された登録プロセスを提供すること。	NIST SP 800-63 では、個人のクレデンシャル情報を割り当てる前に個人の識別情報を確認するプロセスを有することの重要性が強調されている。このプロセスが、その確認を提供する前提となる。
A.ESM — TOE は、セキュリティデータを共有するために他の ESM 製品との接続性を確立できること。	**OE.MANAGEMENT** — 運用環境は、TOE により維持される識別情報とクレデンシャル情報データを利用する認証サーバコンポーネントを提供すること。	TOE が他の ESM 製品へ接続を確立できるよう、これらの製品はすでに運用環境中に展開されていなければならない (must)。特に、認証サーバコンポーネントは TOE により提供される識別情報データを利用する準備が整っていなければならず、さもなければ TOE は展開される環境へ便益を提供できない。**TOE がエンタープライズセキュリティ管理認証サーバの標準プロテクションプロファイルへの適合を主張する場合、この対策方針は運用環境ではなく TSF により満**

前提条件	対策方針	根拠
		たされるとみなされる。
A.FEDERATE — TOE と属性データを交換する第三者エンティティが信頼されていることが前提となる。	**OE.FEDERATE** — TOE が高信頼外部エンティティと交換するデータは信頼されている。	フェデレーション関係にある場合のように、TOE が属性の交換や検証のために第三者エンティティ (例えば、異なる組織に展開されている同一製品の別のインスタンス) を利用する場合、これらのエンティティが信頼されていることを前提とすることが必要となる。これらが異なるネットワークに存在し、従って TOE の管理者がそれらのセキュリティを保証するための直接的なアクションを取ることができないことは、ありそうなことである。
A.MANAGE — TOE のインストール、構成、及び運用を行うために割り当てられた、1 人以上の適格な個人が存在すること。	**OE.ADMIN** — TOE 内でサブジェクト識別情報から属性への対応付けの提供を担当する、1 人以上の運用環境の管理者が存在すること。	特定の個人を割り当てて TSF を管理することにより、管理アクティビティが適切に行われるという保証が提供される。
	OE.INSTAL — TOE の担当者は、IT セキュリティと一貫した形で TOE が配付され、インストールされ、管理され、そして運用されることを保証しなければならない (shall)。	特定の個人を割り当てて TOE をインストールすることにより、評価済み構成と一貫した形でインストールされるという保証が提供される。
	OE.PERSON — TOE 管理者として勤務する要員は、注意深く選定され、また TOE の適切な運用について教育されなければならない (shall)。	管理要員が保証審査及び訓練されることは、彼らが悪意のある、または不注意なアクティビティを行うリスクを低減することに役立つ。
A.ROBUST (オプション) — 運用環境は、認証中に攻撃者が本物の利用者になりすます能力を低減するメカニズムを TOE に提供すること。	**OE.ROBUST (オプション)** — 運用環境は、認証中に攻撃者が本物の利用者になりすます能力を低減するメカニズムを提供すること。	ESM 展開は全体として、ブルートフォース認証攻撃が TSF に対して用いられて成功するリスクを低減し、認証の許容可能な条件 (例えば、曜日、時間、場所) を定義するログイン障害 (frustration) メカニズムを提供することが期待される。TSF がこのメカニズムを提供しない場合、ESM 展開のどこかからこの能力を受け取ることが期待

前提条件	対策方針	根拠
		される。 **ST に FIA_AFL.1 、FIA_SOS.1、及び FTA_TSE.1 が主張される場合、堅牢な TOE 認証は TSF により提供されることになるため、ST 作成者はこの対応付けを除外しなければならない (must)。**
A.SYSTIME (オプション) — TOE は、運用環境から高信頼時間データを受け取ること。	**OE.SYSTIME (オプション)** — 運用環境は、TOE へ高信頼時間データを提供すること。	TSF は、その監査記録の作成に高信頼時間データを利用することが期待される。TOE がソフトウェアベースの製品である場合、TSF がこの時間データを、運用環境中のシステムクロックや NTP サーバなどのソースから受け取ることが期待される。 **ST に FPT_STM.1 が主張される場合、システム時間機能は TSF により提供されることになるため、ST 作成者はこの対応付けを除外しなければならない (must)。**

表 7. 方針、脅威、対策方針、及び根拠

方針及び脅威	対策方針	根拠
P.BANNER — TOE は、使用の制限、法的な合意、またはシステムへアクセスすることにより利用者が同意することになる任意のその他の適切な情報を記述した、初期バナーを表示しなければならない (shall)。	**O.BANNER** — TOE は、TOE の利用に関して注意を喚起する警告を表示すること。	**FTA_TAB.1** TOE がバナーを表示するという要件は、この方針が保証実装されるために十分である。
T.ADMIN_ERROR — 管理者が TOE に正しくないインストールまたは構成を行い、その結果としてセキュリティメカニズムの効果がなくなるおそれがある。	**O.MANAGE** — TOE は認証管理者へ、TSF を管理する機能を提供すること。	**FMT_MOF.1** **FMT_MTD.1 (オプション)** **FMT_SMF.1** 認証済み利用者が異なる管理機能を実行するために特定の特権を持つことを要求することにより、TSF は職務の分離を実施し、不適切な管理的ふるまいの影響を限定できる。
	OE.ADMIN — TOE 内でサブジェクト識別情報から属性への対応付けの提供を担	この対策方針は指名された管理者が TOE の操作を行うことを TOE に要求している。これにより、TOE が適切に管理及び構成されるとい

方針及び脅威	対策方針	根拠
	当する、1 人以上の運用環境の管理者が存在すること。	う多少の保証が提供される。
	OE.INSTAL — TOE の担当者は、IT セキュリティと一貫した形で TOE が配付され、インストールされ、管理され、そして運用されることを保証しなければならない (shall)。	この対策方針は、TOE が評価済み構成と一貫した形でインストールされることを保証することにより、管理エラーの脅威を低減する。
	OE.PERSON — TOE 管理者として勤務する要員は、注意深く選定され、また TOE の適切な運用について教育されなければならない (shall)。	この対策方針は、管理者が TOE へアクセスする前に適切に審査及び訓練されることを保証することにより、管理エラーの脅威を低減する。
T.EAVES — 悪意のある利用者が、TOE データへの不当なアクセスを得るためにネットワークトラフィックを盗聴するおそれがある。	**O.CRYPTO** — TOE は、通信の機密性や完全性を保証するなどのサービスを提供するために利用可能な暗号プリミティブを提供すること。	**FCS_CKM.1 (オプション)** **FCS_CKM_EXT.4 (オプション)** **FCS_COP.1(1) (オプション)** **FCS_COP.1(2) (オプション)** **FCS_COP.1(3) (オプション)** **FCS_COP.1(4) (オプション)** **FCS_RBG_EXT.1 (オプション)** 暗号プリミティブを提供することにより、TOE が高信頼チャネル及びパスを確立し維持することが可能となる。 **上に列挙された暗号要件が ST に主張されない場合、ST 作成者は A.CRYPTO 及び OE.CRYPTO を主張して、本 PP の表 6 及び表 7 に基づいてこれらを対応付けなければならない (must)。**
	O.PROTCOMMS — TOE は、管理者、分散 TOE の他の部分、及び正当な IT エンティティへ、保護された通信チャネルを提供すること。	**FCS_HTTPS_EXT.1 (オプション)** **FCS_IPSEC_EXT.1 (オプション)** **FCS_SSH_EXT.1 (オプション)** **FCS_TLS_EXT.1 (オプション)** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** 高信頼チャネル及びパスの実装により、通信が盗聴から保護されることが保証なる。
	O.EAVES — TOE は、サードパーティ暗	**FTP_ITC.1** **FTP_TRP.1**

方針及び脅威	対策方針	根拠
	号スイートを活用するか、暗号アルゴリズムを利用する能力を取り込むことにより、自分自身への、及び自分自身からの通信チャネルをセキュアにすること。	外部通信に高信頼チャネル及びパスを確立することにより、送信されたデータが不正な当事者へ暴露されたり、不正な当事者により改変されたりしないという妥当な保証が TOE に提供される。
	OE.CRYPTO — 運用環境は、通信の機密性や完全性を保証するなどのサービスを提供するために TOE が利用可能な暗号プリミティブを提供すること。	運用環境が TOE の要求に応じて暗号プリミティブを実装すれば、必要な際に TSF が高信頼チャネル及びパスを確立し維持することが可能となる。 **ST に上記の O.CRYPTO に対応付けられた暗号要件が主張される場合、ST 作成者はこの対策方針を対応付けから除外しなければならない (must)。**
T.FALSIFY — 悪意のある利用者が TOE の識別情報を偽造して、TOE からのものであると称した偽のデータを送信し、ESM 展開へ無効なデータを提供するおそれがある。	**O.CRYPTO** — TOE は、通信の機密性や完全性を保証するなどのサービスを提供するために利用可能な暗号プリミティブを提供すること。	**FCS_CKM.1 (オプション)** **FCS_CKM_EXT.4 (オプション)** **FCS_COP.1(1) (オプション)** **FCS_COP.1(2) (オプション)** **FCS_COP.1(3) (オプション)** **FCS_COP.1(4) (オプション)** **FCS_RBG_EXT.1 (オプション)** 暗号プリミティブを提供することにより、TOE が高信頼チャネル及びパスを確立し維持することが可能となる。 **上に列挙された暗号要件が ST に主張されない場合、ST 作成者は A.CRYPTO 及び OE.CRYPTO を主張して、本 PP の表 6 及び表 7 に基づいてこれらを対応付けなければならない (must)。**
	O.INTEGRITY — TOE は、識別情報、クレデンシャル情報、あるいは権限付与データの完全性を主張する能力を提供すること。	**FTP_ITC.1** 完全性が検証可能な方法で TSF がデータを送信できるならば、そのデータが悪意のあるエージェントにより通過中に改変されるリスクは低減される。
	O.PROTCOMMS — TOE は、管理者、分散 TOE の他の部分、及び正当な IT エンティティへ、保護された通信チャネルを提供	**FCS_HTTPS_EXT.1 (オプション)** **FCS_IPSEC_EXT.1 (オプション)** **FCS_SSH_EXT.1 (オプション)** **FCS_TLS_EXT.1 (オプション)** **FPT_SKP_EXT.1** **FTP_ITC.1**

方針及び脅威	対策方針	根拠
	すること。	**FTP_TRP.1** TOE と他の ESM 製品との間に高信頼チャネルを実装することにより、TOE がこのチャネル上でデータを送信する際にその識別情報をセキュアに主張することを保証する。
	O.SELFID — TOE は、ESM 展開内の従属するマシンへの識別情報、クレデンシャル情報、あるいは権限付与データの送信の際に、自分の識別情報を ESM 展開へ確認させることができること。	**ESM_EID.2** **FTP_ITC.1** 高信頼チャネルを確立し、TSF が自分自身の識別情報を他の ESM コンポーネントへ検証させる手段を提供することにより、送信されたデータのソースを信頼でき、TOE が詐称されるリスクが低減される。
	OE.CRYPTO — 運用環境は、通信の機密性や完全性を保証するなどのサービスを提供するために TOE が利用可能な暗号プリミティブを提供すること。	運用環境が TOE の要求に応じて暗号プリミティブを実装すれば、必要な際に TSF が高信頼チャネル及びパスを確立し維持することが可能となる。 **ST に上記の O.CRYPTO に対応付けられた暗号要件が主張される場合、ST 作成者はこの対策方針を対応付けから除外しなければならない (must)。**
T.FORGE — 悪意のある利用者が、セキュリティ属性データの受信を不法に要求したり TOE へ無効なデータを提供したりするために、外部エンティティの識別情報を偽造するおそれがある。	**O.ACCESSID** — TOE には、他の ESM 製品へのデータの配付に先立って、それらの識別情報を検証する能力が含まれること。	**FTP_ITC.1** エンドポイントの識別を提供する高信頼チャネルを確立することにより、TSF は自分が送信し得るあらゆるデータが有効な ESM コンポーネントへのみ到達することを主張できる。
	O.CRYPTO — TOE は、通信の機密性や完全性を保証するなどのサービスを提供するために利用可能な暗号プリミティブを提供すること。	**FCS_CKM.1 (オプション)** **FCS_CKM_EXT.4 (オプション)** **FCS_COP.1(1) (オプション)** **FCS_COP.1(2) (オプション)** **FCS_COP.1(3) (オプション)** **FCS_COP.1(4) (オプション)** **FCS_RBG_EXT.1 (オプション)** 暗号プリミティブを提供することにより、TOE が高信頼チャネル及びパスを確立し維持することが可能となる。 **上に列挙された暗号要件が ST に主張されない場合、ST 作成者は A.CRYPTO 及び OE.CRYPTO を主張して、本 PP の表 6 及び表 7 に基**

方針及び脅威	対策方針	根拠
		づいてこれらを対応付けなければならない (must)。
	O.PROTCOMMS — TOE は、管理者、分散 TOE の他の部分、及び正当な IT エンティティへ、保護された通信チャネルを提供すること。	**FCS_HTTPS_EXT.1 (オプション)** **FCS_IPSEC_EXT.1 (オプション)** **FCS_SSH_EXT.1 (オプション)** **FCS_TLS_EXT.1 (オプション)** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** TOE と他の ESM 製品との間に高信頼チャネルを実装することにより、TOE がそれへアクセスする外部エンティティの識別情報を検証する手段を持つことを保証する。
	OE.CRYPTO — 運用環境は、通信の機密性や完全性を保証するなどのサービスを提供するために TOE が利用可能な暗号プリミティブを提供すること。	運用環境が TOE の要求に応じて暗号プリミティブを実装すれば、必要な際に TSF が高信頼チャネル及びパスを確立し維持することが可能となる。 **ST に上記の O.CRYPTO に対応付けられた暗号要件が主張される場合、ST 作成者はこの対策方針を対応付けから除外しなければならない (must)。**
	OE.FEDERATE — TOE が高信頼外部エンティティと交換するデータは信頼されている。	TOE が自分の維持する特定の属性データを提供したり検証したりするために外部属性オーソリティを利用する場合、これらのエンティティが作成するデータが信頼されるために、これらのエンティティの真正性が信頼されなければならない (must)。
T.INSUFFATR — 割付管理者が TOE を利用して権限付与とアクセス制御を利用できるほど十分に詳細な認証情報、クレデンシャル情報、及び属性を定義できず、不当なアクティビティを許したり正当なアクティビティを禁止したりするような他の ESM 製品のふるまいが引き起こされてしまうおそれがある。	**O.IDENT** — TOE は割付管理者へ、詳細な識別情報とクレデンシャル情報属性を定義できる能力を提供すること。	**ESM_ICD.1** **ESM_ATD.1 (オプション)** 識別情報とクレデンシャル情報の管理製品は、サブジェクト (及びオプションとしてオブジェクト) 属性を定義できる能力を提供しなければならない (must)。これらの属性は、他の ESM による使用をサポートするのに十分でなければならず (must)、またポリシー管理コンポーネントにより定義されるポリシーをサポートするのに十分でなければならない (must)。これにより、互換性のある製品のアクセス制御機能の完全なセットが利用できる強靭なポリシーが作成されるこ

方針及び脅威	対策方針	根拠
		とを保証する。
T.MASK — 悪意のある利用者が自分のアクションの隠ぺいを試みて、監査データが不正確に記録されたり、全く記録されなかったりする結果が引き起こされるおそれがある。	**O.AUDIT** — TOE は、TOE により保護された資源へのアクセスを利用者が試みたことを検出できる、セキュリティ関連イベントを生成及び記録する手段を提供すること。	**FAU_GEN.1** **FAU_SEL.1 (オプション)** **FAU_STG_EXT.1** **FPT_STM.1 (オプション)** セキュリティ関連イベントがログに記録されバックアップされているならば、攻撃者は自分に責任が及ばないようなアクションを行うことが難しくなる。これにより、適切なオーソリティが記録されたデータをレビューして、TOE への攻撃に関する情報を取得できるようになる。 **ST に FPT_STM.1 が主張されない場合、ST 作成者は A.SYSTIME 及び OE.SYSTIME を主張して、本 PP の表 6 及び表 7 に基づいてこれらを対応付けなければならない (must)。**
	OE.SYSTIME — TOE は、運用環境から高信頼時間データを受け取ること。	この対策方針は、TOE に対して行われたアクティビティのタイミングとシーケンスの正確な記録を提供することにより、監査データの正確さを保証するために役立つ。 **ST に FPT_STM.1 が主張される場合、ST 作成者はこの対策方針を対応付けから除外しなければならない (must)。**
T.RAWCRED — 悪意のある利用者が、他の利用者になりすますためにリプレイされるおそれのあるクレデンシャル情報を取得するために、保存されたクレデンシャル情報データへ直接アクセスしようとするおそれがある。	**O.PROTCRED** — TOE は、保存されたクレデンシャル情報を保護できること。	**FPT_APW_EXT.1** 識別情報とクレデンシャル情報の管理製品は、保存されたクレデンシャル情報が生のリプレイ可能な形態でアクセスされないように、それらを保存しなければならない (must)。
T.UNAUTH — 悪意のある利用者が、TOE の管理機能を不法に利用するために TOE の識別、認証、あるいは権限付与メカニズムをバイパスするおそれがある。	**O.AUTH** — TOE は、要求された認証試行をセキュアに検証するとともに、検証されたサブジェクトが TSF と対話できる範囲を決定するメカニズムを提供すること。	**ESM_EAU.2** **SM_EID.2** **FIA_USB.1** **FMT_SMR.1** **FTP_TRP.1** TOE が、すべての TSF 仲介アクティビティが高信頼パスを介した認証の後に行われ、また認証中に利用者が定義済み役割に束縛されることを要求する場合、攻撃者は TSF に対して不正なアクションを行う

方針及び脅威	対策方針	根拠
		ことが不可能となる。
	O.CRYPTO — TOE は、通信の機密性や完全性を保証するなどのサービスを提供するために利用可能な暗号プリミティブを提供すること。	**FCS_CKM.1 (オプション)** **FCS_CKM_EXT.4 (オプション)** **FCS_COP.1(1) (オプション)** **FCS_COP.1(2) (オプション)** **FCS_COP.1(3) (オプション)** **FCS_COP.1(4) (オプション)** **FCS_RBG_EXT.1 (オプション)** 暗号プリミティブを提供することにより、TOE が高信頼チャネル及びパスを確立し維持することが可能となる。 **上に列挙された暗号要件が ST に主張されない場合、ST 作成者は A.CRYPTO 及び OE.CRYPTO を主張して、本 PP の表 6 及び表 7 に基づいてこれらを対応付けなければならない (must)。**
	O.MANAGE — TOE は認証管理者へ、TSF を管理する機能を提供すること。	**FMT_MOF.1** **FMT_MTD.1 (オプション)** **FMT_SMF.1** 認証済み利用者が異なる管理機能を実行するために特定の特権を持つことを要求することにより、TSF は職務の分離を実施し、不適切な管理的ふるまいの影響を限定できる。
	O.PROTCOMMS — TOE は、管理者、分散 TOE の他の部分、及び正当な IT エンティティへ、保護された通信チャネルを提供すること。	**FCS_HTTPS_EXT.1 (オプション)** **FCS_IPSEC_EXT.1 (オプション)** **FCS_SSH_EXT.1 (オプション)** **FCS_TLS_EXT.1 (オプション)** **FTP_ITC.1** **FTP_TRP.1** 暗号プロトコルを実装することにより、TOE は不正な管理につながるおそれのある通過中のデータの改変を防止できる。
	OE.CRYPTO — 運用環境は、通信の機密性や完全性を保証するなどのサービスを提供するために TOE が利用可能な暗号プリミティブを提供すること。	運用環境が TOE の要求に応じて暗号プリミティブを実装すれば、必要な際に TSF が高信頼チャネル及びパスを確立し維持することが可能となる。 **ST に上記の O.CRYPTO に対応付けられた暗号要件が主張される場合、ST 作成者はこの対策方針を対応付けから除外しなければならない (must)。**
T.WEAKIA — 悪意のある利用者が、認証クレデンシャル	**O.ROBUST** — TOE は、認証中に攻撃者が	**FIA_AFL.1 (オプション)** **FIA_SOS.1 (オプション)**

方針及び脅威	対策方針	根拠
情報の力ずくの推定により TSF から不法に認証されるおそれがある。	本物の利用者になりすます能力を低減するメカニズムを提供すること。	**FTA_SSL_EXT.1 (オプション)** **FTA_SSL.3 (オプション)** **FTA_SSL.4 (オプション)** **FTA_TSE.1 (オプション)** TOE が強度のある秘密のポリシーを利用者パスワードへ適用するならば、個々の推定によりパスワードの識別が成功する確率は低下する。TOE が認証の失敗の取り扱いを適用するならば、攻撃者が行える個々の推定の数は減少する。TOE がセション拒否機能を提供する場合、受容不可能な状況で行われたログイン試行を拒否する。TOE が管理者の非アクティブ状態によるセションのロック及び終了を行う場合、放置されたセションがハイジャックされる確率は低下する。 **ST に FIA_AFL.1、FIA_SOS.1、及び FTA_TSE.1 が主張されない場合、ST 作成者は A.ROBUST 及び OE.ROBUST を主張して、本 PP の表 6 及び表 7 に基づいてこれらを対応付けなければならない (must)。**
	OE.ROBUST — 運用環境は、認証中に攻撃者が本物の利用者になりすます能力を低減するメカニズムを提供すること。	この対策方針は、秘密の強度、認証の失敗、及び TSF により実施されるセション拒否機能を外部で定義することにより、TOE への管理アクセスが堅牢であることを保証することに役立つ。 **TSF への管理的認証に適用されるような形で ST に FIA_AFL.1、FIA_SOS.1、及び FTA_TSE.1 が主張される場合、ST 作成者はこの対策方針を対応付けから除外しなければならない (must)。**

8 セキュリティ課題定義

以下の節には、PP の前提条件、脅威、対策方針、及び組織のセキュリティ方針が列挙されている。

8.1 前提条件

以下のサブ節に列挙する具体的な条件が、TOE の運用環境に存在することが前提となる。これらの前提条件には、TOE セキュリティ要件の開発における実質的な事実と、TOE の使用にあたって不可欠な環境条件の両方が含まれる。

8.1.1 接続性に関する前提条件

表 8. 接続性に関する前提条件

前提条件の名称	前提条件の定義
A.CRYPTO (オプション)	TOE は、運用環境により提供される暗号プリミティブを利用して、暗号サービスを行うこと。
A.ESM	TOE は、セキュリティデータを共有するために他の ESM 製品との接続性を確立できること。
A.FEDERATE	TOE と属性データを交換する第三者エンティティが信頼されていることが前提となる。
A.ROBUST (オプション)	運用環境は、認証中に攻撃者が本物の利用者になりすます能力を低減するメカニズムを TOE に提供すること。
A.SYSTIME (オプション)	TOE は、運用環境から高信頼時間データを受け取ること。

8.1.2 物理的前提条件

本プロテクションプロファイルには、物理的前提条件は規定されない。

8.1.3 人的前提条件

表 9. 人的前提条件

前提条件の名称	前提条件の定義
A.MANAGE	TOE のインストール、構成、及び運用を行うために割り当てられた、1 人以上の適格な個人が存在すること。
A.ENROLLMENT	クレデンシャル情報の割り当ての前に、利用者の識別情報を確認する定義された登録プロセスが存在すること。

8.2 脅威

以下に TOE へ適用される脅威を列挙する。これらの脅威は、TOE の正しくない動作を引き起こしたり、攻撃者が許可なく TOE セキュリティ機能 (TSF) データを取得することを

引き起こしたりするおそれのある攻撃に関連したものである。

表 10. 脅威

脅威の名称	脅威の定義
T.ADMIN_ERROR	管理者が意図せず TOE に正しくないインストールまたは構成を行い、その結果としてセキュリティメカニズムの効果がなくなるおそれがある。
T.EAVES	悪意のある利用者が、TOE データへの不当なアクセスを得るためにネットワークトラフィックを盗聴するおそれがある。
T.FALSIFY	悪意のある利用者が TOE の識別情報を偽造して、TOE からのものであると称した偽のデータを送信し、ESM 展開へ無効なデータを提供するおそれがある。
T.FORGE	悪意のある利用者が、セキュリティ属性データの受信を不法に要求したり TOE へ無効なデータを提供したりするために、外部エンティティの識別情報を偽造するおそれがある。
T.INSUFFATR	割付管理者が TOE を利用して権限付与とアクセス制御を利用できるほど十分に詳細な認証情報、クレデンシャル情報、及び属性を定義できず、不当なアクティビティを許可したり正当なアクティビティを禁止したりするような他の ESM 製品のふるまいが引き起こされてしまうおそれがある。
T.MASK	悪意のある利用者が自分のアクションの隠ぺいを試みて、監査データが不正確に記録されたり、全く記録されなかったりする結果が引き起こされるおそれがある。
T.RAWCRED	悪意のある利用者が、他の利用者になりすますためにリプレイされるおそれのあるクレデンシャル情報を取得するために、保存されたクレデンシャル情報データへ直接アクセスしようとするおそれがある。
T.UNAUTH	悪意のある利用者が、TOE の管理機能を不法に利用するために TOE の識別、認証、あるいは権限付与メカニズムをバイパスするおそれがある。
T.WEAKIA	悪意のある利用者が、認証クレデンシャル情報の力ずくの推定により TSF から不法に認証されるおそれがある。

8.3 組織のセキュリティ方針

以下に TOE へ適用される組織のセキュリティ方針を列挙する。

表 11. 組織のセキュリティ方針

前提条件の名称	前提条件の定義
P.BANNER[8]	TOE は、使用の制限、法的な合意、またはその他のシステムへアクセスすることにより利用者が同意することになる任意の適切な情報を記述した、初期バナーを表示しなければならない (shall)。

[8] この方針は、NIST SP 800-53 における管理策 AC-8 に基づくものである。

8.4 セキュリティ対策方針

本 PP に定義された脅威が適切に低減されることを保証するため、TOE と運用環境の両方に関するセキュリティ対策方針が満たされなければならない (must)。これらを以下の節に列挙する。

8.4.1 TOE に関するセキュリティ対策方針

以下のセキュリティ対策方針は、期待される TOE の特徴である。節 7 には、これらの対策方針が本 PP に定義されたセキュリティ機能要件とどのように関係しているかが記述されている。

表 12. TOE のセキュリティ対策方針

対策方針	TOE セキュリティ対策方針の定義
O.ACCESSID	TOE には、他の ESM 製品へのデータの配付に先立って、それらの識別情報を検証する能力が含まれること。
O.AUDIT	TOE は、TOE により保護された資源へのアクセスを利用者が試みたことを検出できる、セキュリティ関連イベントを生成及び記録する手段を提供すること。
O.AUTH	TOE は、要求された認証試行を検証するとともに、検証されたサブジェクトが TSF と対話できる範囲を決定するメカニズムを提供すること。
O.BANNER	TOE は、TOE の利用に関して注意を喚起する警告を表示すること。
O.CRYPTO (オプション)	TOE は、通信の機密性や完全性を保証するなどのサービスを提供するために利用可能な暗号プリミティブを提供すること。
O.EXPORT	TOE は、セキュアなチャネルを用いて高信頼 IT 製品へ利用者属性を送信する能力を提供すること。
O.IDENT	TOE は割付管理者へ、詳細な識別情報とクレデンシャル情報属性を定義できる能力を提供すること。
O.INTEGRITY	TOE は、識別情報、クレデンシャル情報、あるいは権限付与データの完全性を主張する能力を提供すること。
O.MANAGE	TOE は割付管理者へ、TSF を管理する機能を提供すること。
O.PROTCOMMS	TOE は、管理者、分散 TOE の他の部分、及び正当な IT エンティティへ、保護された通信チャネルを提供すること。
O.PROTCRED	TOE は、保存されたクレデンシャル情報を保護できること。
O.ROBUST (オプション)	TOE は、認証中に攻撃者が本物の利用者になりすます能力を低減するメカニズムを提供すること。
O.SELFID	TOE は、ESM 展開内の従属するマシンへの識別情報、クレデンシャル情報、あるいは権限付与データの送信の際に、自分の識別情報を ESM 展開へ確認させることができること。

8.4.2 運用環境に関するセキュリティ対策方針

以下のセキュリティ対策方針は、TOE が展開される運用環境に期待される特徴である。

表 13. 運用環境のセキュリティ対策方針

対策方針	環境セキュリティ対策方針の定義
OE.ADMIN	TOE 内でサブジェクト識別情報から属性への対応付けの提供を担当する、1 人以上の運用環境の管理者が存在すること。
OE.CRYPTO (オプション)	運用環境は、通信の機密性や完全性を保証するために用いられる暗号メカニズムを提供すること。
OE.ENROLLMENT	運用環境は、クレデンシャル情報の割り当ての前に、利用者の識別情報を確認する定義された登録プロセスを提供すること。
OE.FEDERATE	TOE が高信頼外部エンティティと交換するデータは信頼されている。
OE.INSTALL	OE の担当者は、IT セキュリティと一貫した形で TOE が配付され、インストールされ、管理され、そして運用されることを保証しなければならない (shall)。
OE.MANAGEMENT	運用環境は、TOE により維持される識別情報とクレデンシャル情報データを利用する認証サーバコンポーネントを提供すること。
OE.PERSON	TOE 管理者として勤務する要員は、注意深く選定され、また TOE の適切な運用について教育されなければならない (shall)。
OE.ROBUST (オプション)	運用環境は、認証中に攻撃者が本物の利用者になりすます能力を低減するメカニズムを提供すること。
OE.SYSTIME (オプション)	運用環境は、TOE へ高信頼時間データを提供すること。

附属書A： 参考表と参照資料

A.1 参照資料

[1] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1, June 13, 2013

[2] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Access Control, version 2.1, June 13, 2013

[3] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Secure Configuration Management, version TBD, forthcoming

[4] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Audit Server, version TBD, forthcoming

[5] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Authentication Server, version TBD, forthcoming

[6] National Information Assurance Partnership, Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4, September, 2012

[7] American National Standards Institute, ANSI X9.80 Prime Number Generation, Primality Testing, and Primality Certificates, 2005

[8] National Institute of Standards and Technology, NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007

[9] National Institute of Standards and Technology, NIST Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009

[10] National Institute of Standards and Technology, FIPS PUB 186-3 Digital Signature Standard (DSS), June 2009

[11] National Institute of Standards and Technology, NIST Special Publication 800-57 Recommendation for Key Management, March 2007

[12] National Institute of Standards and Technology, FIPS PUB 197 Advanced Encryption

Standard, November 2001

[13] National Institute of Standards and Technology, NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001

[14] National Institute of Standards and Technology, NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[15] National Institute of Standards and Technology, NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

[16] National Institute of Standards and Technology, NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM), November 2007

[17] National Institute of Standards and Technology, NIST Special Publication 800-38E Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010

[18] National Institute of Standards and Technology, The Advanced Encryption Standard Algorithm Validation Suite (AESAVS), November 2002

[19] National Institute of Standards and Technology, The XTS-AES Validation System (XTSVS), March 2011

[20] National Institute of Standards and Technology, The CMAC Validation System (CMACVS), March 2006

[21]National Institute of Standards and Technology, The CCM Validation System (CCMVS), March 2006

[22] National Institute of Standards and Technology, The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS), February 2009

[23] National Institute of Standards and Technology, The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS), June 2011

[24] National Institute of Standards and Technology, The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS), June 2011

[25] National Institute of Standards and Technology, The RSA Validation System (RSAVS), November 2004

[26] National Institute of Standards and Technology, FIPS PUB 180-3 Secure Hash Standard (SHS), October 2008

[27] National Institute of Standards and Technology, The Secure Hash Algorithm Validation System (SHAVS), July 2004

[28] National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS), December 2004

[29] National Institute of Standards and Technology, NIST Special Publication 800-90 Recommendation for Random Number Generation, March 2007

[30] National Institute of Standards and Technology, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001

[31] National Institute of Standards and Technology, The Random Number Generator Validation System (RNGVS), January 2005

[32] National Institute of Standards and Technology, NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, January 2005

[33] Aerospace Corporation, “Exploding 800-53: An Analysis of NIST SP 800-53 Revision 3 as Completed by CNSSI 1253”, March 2003. Aerospace Technical Operating Report TOR-2012(8506)-5. Distribution restricted to US Government and US Government Contractors.

A.2 頭字語

表 14. 頭字語と定義

用語	定義
CC	Common Criteria (コモンクライテリア)
COI	Communities of Interest
CNSS	Committee on National Security Systems
ESM	Enterprise Security Management (エンタープライズセキュリティ管理)
FIPS	Federal Information Processing Standard (連邦情報処理規格)
HTTP	Hypertext Transfer Protocol (ハイパーテキスト転送プロトコル)

用語	定義
I&C	Identity and Credential (識別情報とクレデンシャル情報)
IKE	Internet Key Exchange (インターネット鍵交換)
IP	Internet Protocol (インターネットプロトコル)
IT	Information Technology (情報技術)
LDAP	Lightweight Directory Access Protocol (ライトウェイト ディレクトリ アクセス プロトコル)
NIST	National Institute of Standards and Technology (アメリカ国立標準技術研究所)
NPE	Non-Person Entity (人間以外のエンティティ)
NTP	Network Time Protocol (ネットワーク タイム プロトコル)
OE	Operational Environment (運用環境)
OS	Operating System (オペレーティング システム)
OSP	Organizational Security Policy (組織のセキュリティ方針)
PM	Policy Management (ポリシー管理)
PP	Protection Profile (プロテクションプロファイル)
RFC	Request for Comment
SA	Security Association
SAML	Security Assertion Markup Language (セキュリティ アサーション マークアップ言語)
SAR	Security Assurance Requirement (セキュリティ保証要件)
SFR	Security Functional Requirement (セキュリティ機能要件)
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 Function (TOE セキュリティ機能)
TSFI	TOE Security Function Interface (TOE セキュリティ機能インタフェース)
VPN	Virtual Private Network (仮想プライベートネットワーク)

附属書B： NIST SP 800-53/CNSS 1253 マッピング

本節は、TOE を使用することで満たすことが可能な他の関連する規格からの要件を示すデータを列挙する。本情報は、CC の観点からは必要とされないが、これをセキュリティターゲットへ取り込むことにより、その配備において複数の規格への適合が必要とされる場合、省略可能な冗長な作業を識別する上で、読者の助けになるだろう。

以下の表には、本 PP の一部として定義された拡張要件、拡張又は非標準の形で PP に適用されるかもしれない標準 CC 要件及びそれらへ適用する NIST 800-53 セキュリティ管理策が列挙されている。来るべき NIST SP 800-53 改訂 4 版には、NIST 800-53 と CC パート 2 及び 3 に定義される CC 要件との間の対応付けが定義される。将来の日付で CCEVS ウェブサイト上に公表されることになる。これは、本 PP で主張されている残りの要件へのセキュリティ管理策のマッピングのために使われることになる。

主張された SFR 及び SAR へ適用可能な NIST 800-53 管理策は、Aerospace Technical Operating Report TOR-2012(8506)-5, “Exploding 800-53: An Analysis of NIST SP 800-53 Revision 3 as Completed by CNSSI 1253”を参照することにより CNSSI 1253 へのマッピングが可能である。

以下に列挙したガイドラインは、本 PP への正確適合が主張されている前提に基づくことに注意すること。ST 作成者が複数の PP への適合を主張することにより TOE に要件追加を行っている場合、ここに文書化していない追加の管理策が適用されているかもしれない。

表 15. NIST 800-53 要件との適合性

SFR		NIST 800-53 管理策[9]		コメント及び意見
ESM_ATD.1 (オプション)	**属性の定義** オブジェクト属性の定義	AC-3	**アクセス制御の実施**	**部分的。**この管理策では、ポリシー実施に不可欠なオブジェクト属性が定義される。この割付はポリシーと一貫するように記入されるべきであり (should)、またこの強化策の適用可能性は定義されたポリシーに依存する。
		AC-3(3)	**アクセス制御の実施** | 実施アクセス制御	**部分的。**この管理策では、ポリシー実施に不可欠なオブジェクト属性が定義される。この割付はポリシーと一貫するように記入されるべきであり (should)、またこの強化策の適用可能性は定義されたポリシーに依存する。

[9] この表は、NIST SP 800-53 改訂 4 版を反映している。改訂 3 版との大きな違いは、適宜注記される。

SFR		NIST 800-53 管理策[9]		コメント及び意見
				注記：改訂 3 版の AC-3(3) は、実施アクセス制御と役割ベースのアクセス制御の両方に用いられる。
		AC-3(4)	**アクセス制御の実施** | 任意アクセス制御	**部分的。**この管理策では、ポリシー実施に不可欠なオブジェクト属性が定義される。この割付はポリシーと一貫するように記入されるべきであり (should)、またこの強化策の適用可能性は定義されたポリシーに依存する。
		AC-3(7)	**アクセス制御の実施** | 役割ベースのアクセス制御	**部分的。**この管理策では、ポリシー実施に不可欠なオブジェクト属性が定義される。この割付はポリシーと一貫するように記入されるべきであり (should)、またこの強化策の適用可能性は定義されたポリシーに依存する。 (改訂 4 版のみ)
ESM_EAU.2	**エンタープライズ認証** エンタープライズ認証への依存	IA-2	**識別と認証 (組織の利用者)**	**部分的。**これは、組織の利用者の認証に対応する。
ESM_EID.2	**エンタープライズ識別** エンタープライズ識別への依存	IA-2	識別と認証 (組織の利用者)	**部分的。**これは、組織の利用者の識別に対応する。
ESM_ICD.1	**識別情報とクレデンシャル情報の定義** 識別情報とクレデンシャル情報の定義			**マッピングなし。**これに対応する管理策は存在しないようである。SFR では、TSF により定義されるエンタープライズ利用者に関する識別情報またはクレデンシャル情報あるいはその両方のデータが定義される。
ESM_ICT.1	**識別情報とクレデンシャル情報の送信** 識別情報とクレデンシャル情報の送信			**マッピングなし。**これに対応する管理策は存在しないようである。SFR では、定義された識別情報またはクレデンシャル情報あるいはその両方のデータの送信に関する条件が定義される。
FAU_STG_EXT.1	**セキュリティ監査イベントストレージ** 外部監査証	AU-9	**監査情報の保護**	**部分的。**SFR は管理策の基本的な意図に対応するが、監査データが書き込まれるリポジトリ／エンティティはそのデータの不正な改変をさらに防止しなければならない (must)。し

SFR		NIST 800-53 管理策[9]		コメント及び意見
	跡ストレージ			かし、管理策は監査証跡だけではなく、監査ツール (これは SFR ではカバーされていない) も保護する。
FCS_CKM.1 (オプション)	暗号鍵の管理 暗号鍵生成	SC-12	**暗号鍵の確立と管理**	**部分的。**SFR は、800-53 管理策の側面の 1 つに対応している。規格及びプロトコルの割付は、必要とされる要件追加に対して比較される必要がある。
		注記：改定 3 版では、NIST 800-53 管理策は、鍵の管理の様々な側面 (生成、配付、アクセス、及び破壊) の間に区別をしていない。		
FCS_CKM_EXT.4 (オプション)	暗号鍵の管理 暗号鍵の破棄	SC-12	**暗号鍵の確立と管理**	**部分的。**SFR は、800-53 管理策の側面の 1 つに対応する。規格及びプロトコルの割付は、要求される要件追加に対して比較される必要がある。
		注記：改定 3 版では、NIST 800-53 管理策は、鍵の管理の様々な側面 (生成、配付、アクセス、及び破壊) の間に区別をしていない。		
FCS_HTTPS_EXT.1 (オプション)	HTTPS HTTPS	SC-8	**伝送される情報の機密性と完全性**	**部分的。**TOE が通信を暗号化する能力により、通過中のデータの機密性と完全性を保証する。このデータの物理的な保護は、運用環境により定義される。
		SC-8(1)	**伝送される情報の機密性と完全性** | 暗号またはそれに代わる物理的保護	部分的。これは、暗号を使用するという要件に対応する。
		SC-13	**暗号保護**	**部分的。**これは、暗号を使用するという要件に対応する。管理策中の割付は、選択された暗号の種類に対応すべきである (should)。US での評価には、SC-13(1) もまた適用され得る。
		注記：改訂 3 版では、SC-9 及び SC-9(1) もまた適用可能である。改訂 3 版は、送信の完全性 (SC-8) と送信の機密性 (SC-9) を区別していた。改訂 4 版では、SC-8 と SC-9 が、保護の種類を提供する割付を持つ単一の管理策に統合された。		
FCS_IPSEC_EXT.1 (オプション)	IPSEC IPSEC	SC-8	**伝送される情報の機密性と完全性**	**部分的。**TOE が通信を暗号化する能力により、通過中のデータの機密性と完全性を保証する。このデータの物理的な保護は、運用環境により定義される。
		SC-8(1)	**伝送される情報の機密性と完全性** | 暗号またはそれに代わる物理的保護	**部分的。**これは、暗号を使用するという要件に対応する。
		SC-13	**暗号保護**	**部分的。**これは、暗号を使用すると

SFR		NIST 800-53 管理策[9]		コメント及び意見
				いう要件に対応する。管理策中の割付は、選択された暗号の種類に対応すべきである (should)。US での評価には、SC-13(1) もまた適用され得る。
		注記：改訂 3 版では、SC-9 及び SC-9(1) もまた適用可能である。改訂 3 版は、送信の完全性 (SC-8) と送信の機密性 (SC-9) を区別していた。改訂 4 版では、SC-8 と SC-9 が、保護の種類を提供する割付を持つ単一の管理策に統合された。		
FCS_RBG_EXT.1 (オプション)	ランダムビット生成 ランダムビット生成	SC-13	**暗号保護** (改訂 4 版のみ)	**部分的。**管理策中の割付は、乱数及びエントロピーの品質要件に対応して記入されるべきである (should)。
		注記：改訂 3 版では、SC-13 中に乱数生成品質要件を規定する条項は存在しなかった。		
FCS_SSH_EXT.1 (オプション)	SSH SSH	SC-8	**伝送される情報の機密性と完全性**	**部分的。**TOE が通信を暗号化する能力により、通過中のデータの機密性と完全性を保証する。このデータの物理的な保護は、運用環境により定義される。
		SC-8(1)	**伝送される情報の機密性と完全性** | 暗号またはそれに代わる物理的保護	**部分的。**これは、暗号を使用するという要件に対応する。
		SC-13	**暗号保護**	**部分的。**これは、暗号を使用するという要件に対応する。管理策中の割付は、選択された暗号の種類に対応すべきである (should)。US での評価には、SC-13(1) もまた適用され得る。
		注記：改訂 3 版では、SC-9 及び SC-9(1) もまた適用可能である。改訂 3 版は、送信の完全性 (SC-8) と送信の機密性 (SC-9) を区別していた。改訂 4 版では、SC-8 と SC-9 が、保護の種類を提供する割付を持つ単一の管理策に統合された。		
FCS_TLS_EXT.1 (オプション)	TLS TLS	SC-8	**伝送される情報の機密性と完全性**	**部分的。**TOE が通信を暗号化する能力により、通過中のデータの機密性と完全性を保証する。このデータの物理的な保護は、運用環境により定義される。
		SC-8(1)	**伝送される情報の機密性と完全性** | 暗号またはそれに代わる物理的保護	**部分的。**これは、暗号を使用するという要件に対応する。
		SC-13	**暗号保護**	**部分的。**これは、暗号を使用するという要件に対応する。管理策中の割付は、選択された暗号の種類に対応

SFR		NIST 800-53 管理策[9]		コメント及び意見
				すべきである (should)。US での評価には、SC-13(1) もまた適用され得る。
		注記：改訂 3 版では、SC-9 及び SC-9(1) もまた適用可能である。改訂 3 版は、送信の完全性 (SC-8) と送信の機密性 (SC-9) を区別していた。改訂 4 版では、SC-8 と SC-9 が、保護の種類を提供する割付を持つ単一の管理策に統合された。		
FPT_APW_EXT.1	TSF の保護 保存されたクレデンシャル情報の保護	IA-5	**認証子の管理**	**部分的。**管理策の h) 項、不正な暴露及び改変からの認証子の内容の保護に対応する。
FMT_MTD.1 (オプション)	TSF データの管理 TSF データの管理	SI-9	**情報入力の制限** | 情報入力を正当な人物に制限する能力 (改訂 3 版のみ)	**部分的。**SFR はこの管理策を暗黙に示しているようであるが、SFR のほうが遥かに具体的である。
		注記：SI-9 は改訂 4 版では撤回され、その能力は AC-2 (アカウント管理)、AC-3 (アクセス制御の実施)、AC-5 (職責の分離)、及び AC-6 (最小特権) に取り込まれた。		
FPT_APW_EXT.1	保存されたクレデンシャル情報の保護 保存されたクレデンシャル情報の保護	IA-5	**認証子の管理**	**部分的。**この SFR は、認証データが不正な暴露及び改変から保護されることを要求する管理策の部分に対応する。
		IA-5(1)	**認証子の管理** | パスワードベースの認証	これは、パスワードがあいまい化されて保存されることを要求する管理策の部分に対応する。
FPT_SKP_EXT.1	プライベート鍵パラメタの保護 プライベート鍵パラメタの保護	IA-5	**認証子の管理**	**部分的。**この SFR は、認証データが不正な暴露及び改変から保護されることを要求する管理策の部分に対応する。
		SC-12	**暗号鍵の確立と管理**	**部分的。**これは、鍵のストレージについて論じた管理策の部分に対応する。
FTA_SSL_EXT.1 (オプション)	セションのロックと終了 TSF 主導の終了	AC-11	**セションのロック**	**部分的。**FTA_SSL_EXT.1 は、システム主導によるセションのロックを提供する。
		AC-11(1)	**セションのロック** | スクリーンセーバーによる	**完全。**FTA_SSL_EXT.1 は、システム主導によるセションのロックを提供する。

附属書C： アーキテクチャのバリエーションと追加要件

C.1 オブジェクト属性データ

少なくとも、本プロテクションプロファイルは適合 TOE がサブジェクト属性データの定義と維持ができることを要求している。しかし、ESM 全体にはオブジェクト属性データの定義と維持の機能も要求される。ESM アクセス制御の概念は、何らかの属性のセットを持つサブジェクトが、それ自身の属性のセットを持つオブジェクトに対する操作を要求することを前提としている。ポリシーは、これら 2 つの属性のセットに基づいて操作が試行される際、どのアクションが取られるべきか (should) を決定する。

従って ESM は、サブジェクトとオブジェクト両方の属性データを定義し維持する機能を含まなければならない (must)。これは、本プロテクションプロファイルと ESM ポリシー管理の標準プロテクションプロファイルの両方についてのオプションコンポーネントである。本 PP への適合主張する TOE にこの機能が含まれていない場合、ST 作成者は運用環境において信頼できる属性データのソースを示さなければならない (must)。

本機能が提供される場合、以下の SFR が ST に含まれなければならない (must)。

C.1.1 ESM_ATD.1 オブジェクト属性の定義

下位階層：	他のコンポーネントなし。
ESM_ATD.1.1	TSF は、個別オブジェクトに属するセキュリティ属性の以下のリストを維持しなければならない (shall)： [***割付：オブジェクトセキュリティ属性のリスト***]。
適用上の注意：	*オブジェクトセキュリティ属性は、最終的にアクセス制御の決定の際に考慮されるが、利用者にもアクセス制御ポリシーにも関連付けられていない属性を意味する。マルチレベルセキュリティのアクセス制御ポリシーを定義する TOE は、資源と関連付け可能な定義済みセキュリティラベルを用いて、ポリシーがこれらの資源へ適用できるようにする必要があるかもしれない。*
ESM_ATD.1.2	TSF は、セキュリティ属性を個別オブジェクトと関連付けることができなければならない (shall)。
依存性：	依存性なし。

保証アクティビティ：

評価者は、TOE により定義されるオブジェクト属性とその定義の目的が記述されていることを保証するため、TSS をチェックしなければならない (shall)。

評価者は、オブジェクト属性を定義し構成する方法に関する指示が提供されていることを保証するため、操作ガイダンスをチェックしなければならない (shall)。

評価者は、ポリシー管理製品を用いて定義済み属性を利用するアクセス制御ポリシーを作成し、アクセス制御製品にこれを利用させることにより、この機能をテストしなければならない (shall)。次に評価者は、ポリシーと関連付けられたオブジェクト属性に基づいてアクセス制御製品により許可されるアクションと、アクセス制御製品により拒否されるアクションとを実行しなければならない (shall)。

C.2 パスワードポリシーの定義

TOE がパスワードポリシーを定義することは要求されていない。この機能は、典型的には識別情報とクレデンシャル情報の管理製品に関連付けられることが期待される。しかし、TSF が設定可能なパスワードポリシーを定義することはあり得る。例えば、TOE が利用者にセルフサービスのパスワード変更 (附属書 C.5 を参照) を許可している場合、設定可能なパスワードポリシーが運用環境とは独立して許容可能な変更を規定するかもしれない。これが事実である場合、以下の要件が主張されなければならない (must)。

C.2.1 FIA_SOS.1 秘密の検証

下位階層：　他のコンポーネントなし。

FIA_SOS.1.1　TSF は、秘密が以下を満たすことを検証するメカニズムを提供しなければならない (shall)。

a) 環境のパスワードによる認証については、以下のルールが適用される。

1. パスワードは、以下の文字セットのサブセットから構成されることができなければならない (shall)： [割付：パスワードの入力に関してTSF でサポートされる文字セットのリスト] であって、以下の値を含むもの [割付：サポートされる文字セットのそれぞれについて、サポートされる文字のリスト]；及び

適用上の注意：　英語の文字セットについては、文字の種類には26 個の大文字、26 個の小文字、10 個の数字、ならびに 10 個の特殊文字 "!"、"@"、"#"、"$"、"%"、"^"、"&"、""、"("及び ")"が含まれること*

が期待される。英語以外の文字セットが TOE でサポートされる場合、ST 作成者はサポートされる文字セットとともに、これらのセットのサブカテゴリのそれぞれに許容可能な文字空間を規定しなければならない (must)。

2. パスワードの最小の長さは管理者により設定可能であって、16 文字以上のパスワードがサポートされなければならず (shall)、さらに

適用上の注意： *最小パスワード長とパスワードの文字空間に基づくパスワードの組み合わせの数は、10^{14} を超えるものでなければならない (must)。これは、72 個の文字セットを用いる最小の長さが 8 文字の英語パスワードとほぼ同等である。*

3. パスワードを構成する文字に要求される文字の種類と数を規定するパスワードの構成ルールが管理者により設定可能でなければならず (shall)、さらに

4. パスワードは、管理者により構成可能な最大ライフタイムを持たなければならず (shall)、さらに

5. 新たなパスワードは、最低でも管理者により指定される文字数だけ、以前のパスワードからの変更を含まなければならず (shall)、さらに

6. パスワードは、その利用者により用いられたパスワードの、管理者により設定可能な直近の世代数以内で再利用されてはならない (shall not)。

b) パスワードによらない認証については、以下のルールが適用される。

1. 秘密が、その秘密のライフタイム内に攻撃者により取得される確率は、2^{-20} 未満であること。

依存性： 依存性なし。

保証アクティビティ：

評価者は、TOE の秘密機能の強度が SFR と一貫した詳細のレベルまで論じられていることを検証するため、TSS をチェックしなければならない (shall)。

評価者は、パスワードの設定、再利用、及びエージングに関する、あるいはパスワードによらないクレデンシャル情報に関する TOE の実施について管理者へ情報が提供されていることを検証するため、操作ガイダンスをチェックしなければならない (shall)。TOE がパスワードによるクレデンシャル情報をサポートしない場合、評価者は TSF により用いられるクレデンシャル情報とそれが TOE へ供給される方法に関する情報が操作ガイダンスに提供されていることをチェックして検証しなければならない (shall)。

評価者は、設定可能な秘密の強度のポリシーの側面と、それを設定するために管理者がどのような手順を行う必要があるか、論じられていることを検証するため、操作ガイダンスについてもチェックしなければならない (shall)。

評価者は、この機能を以下のようにテストしなければならない (shall)。

- *パスワードによる認証がサポートされる場合、評価者は長さと構成の要件が TSS に記述される通り機能することを検証するために、有効なパスワードと無効なパスワードを供給しなければならない (shall)。評価者は、パスワードを設定して適切な長さの時間後に有効期限が過ぎることを確認することにより、パスワードのエージング要件をテストしなければならない (shall)。評価者は、一連の有効な変更パスワードと無効な変更パスワードを供給し、まず変更されたパスワードが十分に異なっていなければならない (must) ことをテストし、次に一定回数のうちにはパスワードが再利用できないことをテストすることにより、再利用要件をテストしなければならない (shall)。*

- *- パスワードによる認証がサポートされる場合、評価者は操作ガイダンスに記述される手順を行って、パスワードポリシーの設定可能なパラメタのそれぞれを変更し、パラメタの変更前と変更後にパスワードを供給して変更が適切に実施されることを検証しなければならない (shall)。*

- *- パスワードによらない認証がサポートされる場合、評価者は操作ガイダンスに記述される手順に従ってクレデンシャル情報を作成しなければならない (shall)。次に評価者は、そのクレデンシャル情報を TOE に提供するとアクセスが許可され、無効なクレデンシャル情報が拒否されることを確認しなければならない (shall)。この例は、指紋生体情報である。この場合、評価者は利用者アカウントを彼ら自身の指紋と関連付けることになるだろう。そして彼らは、自分の指紋を提供することにより自分のアカウントへログオンし、また他の誰かが代わりに自分の指紋を提供することを試行した際には失敗することを確認することになるだろう。*

パスワードによらない認証のみがサポートされる場合、ベンダまたは公開研究あるいはそ

の両方により提供される証拠資料を用いて、力ずくの推定がありそうにないことを評価者が正当化すれば十分である。

C.3 選択可能監査

TOE が選択可能な監査を実行することは要求されていない。しかし、場合によりは、TSF により監査されるイベントのセットが設定可能であるかもしれない。

これが事実である場合、以下のアクティビティが行われなければならない (must)。

- 以下に記述される FAU_SEL.1 が主張されなければならない (must)
- この機能を行う責任のあるエンティティ (TSF またはセキュア構成管理などの外部製品) が識別されなければならない (must)
- このエンティティがリモートの場合、TOE とこのエンティティとの間の通信は、FTP_ITC.1 に定義される高信頼チャネルにより保護されなければならない (must)
- TSF が外部エンティティにより設定される場合、このエンティティが負う役割は FMT_SMR.1 により識別されなければならず (must)、またエンティティがこの役割へ束縛されるプロセスは FIA_USB.1 に識別されなければならない (must)

C.3.1 FAU_SEL.1 選択的監査

下位階層：　他のコンポーネントなし。

FAU_SEL.1.1　*詳細化：*TSF は、以下の属性に基づいて、*[選択：運用環境中の [**割付：ESM 製品**]、ローカル定義]* からのすべての監査対象イベントのセットから監査されるべきイベントのセットを選択できなければならない (shall)：

a. [選択：オブジェクトの識別情報、利用者の識別情報、サブジェクトの識別情報、ホストの識別情報、イベントの種類]；及び

b. [***割付：監査の選択がそれに基づいて行われる追加的属性のリスト***]

適用上の注意：　*ST 作成者は、監査対象イベントのセットが定義される方法を示さなければならない (must)。例えば、TSF を利用している管理者により設定可能かもしれないし、あるいはリモートの高信*

頼 IT エンティティから TOE へ利用のために送信された監査ポリシー中で定義されるかもしれない。

依存性： FAU_GEN.1 監査データの生成

FMT_MTD.1 TSF データの管理

保証アクティビティ：

評価者は、選択的監査を行う TSF の能力が論じられており、また監査される監査イベントが選択される 1 つまたは複数のメカニズムが要約されていることを決定するために、TSS をチェックしなければならない (shall)。

評価者は、監査対象イベントのセットとされることが可能な選択を決定するために操作ガイダンスをチェックしなければならず (shall)、またセキュリティターゲット中に識別される選択のすべてがそれに含まれることを確認しなければならない (shall)。

評価者は、FMT_MOF.1 に定義されるすべての許容可能なベクトルを用いて TOE を以下のように設定することにより、この機能をテストしなければならない (shall)：

- *すべての選択可能な監査対象イベントが有効化される*
- *すべての選択可能な監査対象イベントが無効化される*
- *一部の選択可能な監査対象イベントが有効化される*

これらの設定のそれぞれについて、評価者はすべての選択可能な監査対象イベントを実行し、監査データのレビューにより、それぞれの設定において有効化することベントのみが記録されることを確認しなければならない (shall)。

C.4 セション管理

TSF はセションのロック、ロック解除、及び終了の機能を定義することを要求されていない。しかし、TOE がこれらの機能を実際に行う場合、ST 作成者は以下の要件を取り込んでもよい。

C.4.1 FTA_SSL_EXT.1 TSF 手動のセションのロック

下位階層： 他のコンポーネントなし。

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—表示デバイスを消去または上書きし、現在のコンテンツを判読不能とし、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 への利用者再認証を要求すること；

- セションの終了

] を、正当な管理者により指定される非アクティブ継続時間後に行わなければならない (shall)。

依存性： 依存性なし。

保証アクティビティ：

評価者は、非アクティブ状態がローカル管理セションについて取り扱われる方法が論じられていることを決定するために、TSS をチェックしなければならない (shall)。

評価者は、ローカル対話セションがそのアイドル時間閾値を超えた際に何が起こるか記述されていることを決定するために、操作ガイダンスをチェックしなければならない (shall)。また評価者は、アイドル時間閾値を設定する方法、及び該当する場合、アイドル時間閾値を超えた際に TSF が行うふるまいを設定する方法が記述されていることを検証するために操作ガイダンスをチェックしなければならない (shall)。

評価者は、操作ガイダンスに従ってコンポーネント中に参照される非アクティブ継続時間をいくつかの異なる値に設定することにより、この機能をテストしなければならない (shall)。設定された時間間隔のそれぞれについて、評価者は TOE とのローカルな対話セションを確立する。次に評価者は、設定された時間間隔の後に、そのセションがロックされるか終了されることを確認する。コンポーネントからロックが選択されている場合、次いで評価者はセションのロック解除を試行する際に再認証が必要であることを保証する。

C.4.2 FTA_SSL.3 TSF 手動の終了

下位階層： 他のコンポーネントなし。

FTA_SSL.3.1 *詳細化：*TSF は、[*正当な管理者により設定可能なセション非アクティブ継続時間*] の後に、リモート対話セションを終了しなければならない (shall)。

依存性： 依存性なし。

保証アクティビティ：

評価者は、非アクティブ状態がリモート管理セションについて取り扱われる方法が論じら

れていることを決定するために、TSS をチェックしなければならない (shall)。

評価者は、アイドル時間閾値を設定する方法が記述されていることを検証するために、操作ガイダンスをチェックしなければならない (shall)。

評価者は、操作ガイダンスに従ってコンポーネント中に参照される非アクティブ継続時間をいくつかの異なる値に設定することにより、この機能をテストしなければならない (shall)。これらは少なくとも、操作ガイダンスに指定される許容可能な最小値及び最大値、ならびにその他の値から設定されなければならない (shall)。設定された時間間隔のそれぞれについて、評価者は TOE とのリモート対話セションを確立する。次に評価者は、設定された時間間隔の後に、そのセションが終了されることを確認する。

C.4.3 FTA_SSL.4 利用者主導の終了

下位階層：	他のコンポーネントなし。
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*主導の終了を許可しなければならない (shall)。
依存性：	依存性なし。

保証アクティビティ：

評価者は、管理者が自分自身のセションを終了できる能力が論じられていることを決定するために、TSS をチェックしなければならない (shall)。

評価者は、TOE のサポートする管理インタフェースのそれぞれについて、管理者が自分自身の管理セションを終了する方法が記述されていることを検証するために、操作ガイダンスをチェックしなければならない (shall)。

評価者は、管理インタフェースを用いて TOE とのセションを確立することにより、この機能をテストしなければならない (shall)。次に評価者は操作ガイダンスに従ってセションを退出またはログオフし、セションが終了されることを確認する。該当する場合、TOE のサポートする管理インタフェースのそれぞれについて評価者はこのテストを繰り返さなければならない (shall)。

C.5 環境の認証データの管理

場合によりは、識別情報とクレデンシャル情報管理製品により権威を持って定義される属性を管理する能力を、TOE が提供することが期待される。例えば、セルフサービスのオプションでは、TOE が識別情報とクレデンシャル情報管理製品とインタフェースして、利用者が自分のパスワードを変更できるようにすることが許可されるかもしれない。このよう

な状況では、ST 作成者は以下の要件を主張してもよい。

C.5.1 FMT_MTD.1 TSF データの管理

下位階層：　他のコンポーネントなし。

FMT_MTD.1.1　TSF は、[***割付：認証データのリスト***] の [選択：デフォルトの変更、問い合わせ、変更、削除、クリア、[***割付：その他の操作***]] を行う能力を、 [***割付：正当な識別された役割***] に制限しなければならない (shall)。

適用上の注意：　*認証データは、TSF 外部のリポジトリに保存できる。例えば、TSF は環境の LDAP サーバに保存されているパスワードの利用者セルフサービス変更を利用するかもしれない。*

依存性：　FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の仕様

保証アクティビティ：

評価者は、TOE の利用する認証データが保存されるリポジトリを決定するために、TSS をレビューしなければならない (shall)。また評価者は、このリポジトリとの通信がセキュア化されている方法も決定しなければならない (shall)。

評価者は、管理可能なデータと、誰がこのデータを管理できるのかがが含まれていることを決定するために、操作ガイダンスをレビューしなければならない (shall)。これは、利用者管理とセルフサービスを区別するために、複数の役割に分離されてもよい。例えば、セキュリティ管理者と特定の利用者の両方が、その利用者自身のパスワードを変更できるかもしれない。

評価者は、識別された管理アクティビティを権限のある役割で行って、それが許可されることを確認することにより、この機能をテストしなければならない (shall)。また評価者は、これらのアクティビティを権限のない役割で行って、それが許可されないことを決定しなければならない (shall)。最後に、評価者は TSF と認証データリポジトリとの間のインタフェース上で FTP_ITC.1 のテストを繰り返すことにより、これら 2 つのコンポーネント間の通信がセキュア化されていることを検証しなければならない (shall)。

C.6 タイムスタンプ

本プロテクションプロファイルは、タイムスタンプが運用環境により提供されるだろうという前提条件の下に書かれた。TOE がアプライアンスとして実装される場合、タイムスタンプ機能は TOE 内部のものであるかもしれない。これが事実である場合、以下の SFR が取り込まれなければならない (must)。

C.6.1 FPT_STM.1 高信頼タイムスタンプ

下位階層：	他のコンポーネントなし。
FPT_STM.1.1	TSF は、自分自身で使用するための高信頼タイムスタンプを提供できなければならない (shall)。
依存性：	依存性なし。

保証アクティビティ：

評価者は、TOE にシステムクロックが含まれていることが論じられていることを決定するために、TSS をチェックしなければならない (shall)。

評価者は、時刻を設定する方法が管理者に指示されていることを保証するため、操作ガイダンスを検査する。TOE が NTP サーバの利用をサポートする場合、操作ガイダンスには TOE と NTP サーバとの間の通信パスが確立される方法と、この通信をサポートするために TOE 上の NTP クライアントに必要な任意の設定が指示される。

評価者は、操作ガイダンスの評価を通じて TOE がクロックを初期化し開始する方法を決定しなければならない (shall)。次に評価者はこれらの指示に従ってクロックを既知の値に設定し、クロックが信頼できる形で単調増加することを確認 (参照用計時器具との比較で十分である) しなければならない (shall)。他の TOE 機能の行使により、評価者はタイムスタンプの値が適切に用いられることを確認しなければならない (shall)。TOE が NTP サーバとの接続を確立するために複数のプロトコルをサポートしている場合、評価者は操作ガイダンスに主張されるサポートされるプロトコルのそれぞれを用いてこのテストを行わなければならない (shall)。

C.7 認証ポリシーの定義

一般的には、TOE へログオンする管理者の定義及び認証は他の ESM で行われることが期待される。このため、許容可能な認証のポリシーが TSF により定義されないことは多い。しかし、それでも TSF が自分自身の認証ポリシーを定義することは可能である。これが事実である場合、以下の要件が主張されなければならない (must)。

C.7.1 FIA_AFL.1 認証失敗時の取り扱い

下位階層： 他のコンポーネントなし。

FIA_AFL.1.1 TSF は、[***割付：認証イベントのリスト***] に関して、[選択：[***割付：正の整数値***]、[***割付：受容可能な値の範囲***] 内における管理者設定可能な正の整数値] 回の不成功認証試行が生じたときを検出しなければならない (shall)。

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

依存性： FIA_UAU.1 認証のタイミング

保証アクティビティ：

評価者は、認証失敗時の取り扱い機能が SFR を支持するのに十分なほど詳細に記述されていることを決定するために、TSS をチェックしなければならない (shall)。

評価者は操作ガイダンスをチェックして、認証失敗時の取り扱いに関する議論が存在しセキュリティターゲット中の表現と一貫していることを検証しなければならない (shall)。

評価者は、TSF の認証機能を利用して意図的に正しくないクレデンシャル情報を入力することにより、この機能をテストしなければならない (shall)。評価者は、十分な回数の認証試行の不成功の後、適切なアクションが発生することを確認しなければならない (shall)。また評価者は TSF を利用して操作ガイダンスと一貫したやり方で閾値を再構成し、それが変更可能であることも検証しなければならない (shall)。

C.7.2 FTA_TSE.1 TOE によるセションの確立

下位階層： 他のコンポーネントなし。

FTA_TSE.1.1 TSF は、[選択：日付、時刻、[***割付：その他の属性***]] に基づいてセションの確立を拒否できなければならない (shall)。

依存性： 依存性なし。

保証アクティビティ：

評価者は、それに基づいてセションが拒否され得る属性のすべてが具体的に定義されていることを決定するため、TSS を検査しなければならない (shall)。

評価者は、TSS に識別される属性のそれぞれを構成するためのガイダンスが含まれることを決定するため、操作ガイダンスを検査しなければならない (shall)。

評価者は、まず TOE へ完全なセションを確立することにより、この機能をテストしなければならない (shall)。次に評価者は操作ガイダンスに従って、属性の識別の値に基づいて、そのアクセスが拒否されるように TOE を構成する。次いで評価者は属性設定に反する (例えば、その場所が時刻に基づいて拒否される) セションの確立を試行しなければならない (shall)。評価者は、そのセションの確立試行が失敗することを確認しなければならない (shall)。

C.8 暗号機能要件

本プロテクションプロファイルは、オペレーティングシステムや暗号ライブラリなどのサードパーティ技術を用いて TOE を保護する暗号機能を提供することを、TOE 開発者に許可すると共に推奨するように作成された。TOE が自分自身で内部暗号機能を提供しサードパーティ技術に依存していない場合、以下の要件もまた考慮されなければならない (must)。

適用される要件

1. ST 作成者は、この製品にこのシナリオが存在することを明確にしなければならない (must)。
2. 評価者は、ST 内にこの附属書の要件を主張しなければならない (must)。
3. 開発者は、この附属書の要件が適切に対処されているという保証証拠資料を提供しなければならない (must)。
4. 評価者は、この附属書の要件内に言及される機能をテストするためのテストを考案し行わなければならない (must)。

これらの要件は、OS または暗号ライブラリに機能の実行を依存するのではなく、TOE が自分自身の暗号機能を実行する場合にのみ主張されなければならない (must)。これらの要件は、IPsec 仮想プライベートネットワーク (VPN) ゲートウェイのセキュリティ要件から取られた。これらの要件を定義するために用いられる暗号規格は、米国に特有のものであることに注意すること。他の国により監督されるべき評価については、同等の国家標準が ST 作成者により用いられなければならない (must)。

C.8.1 FCS_CKM.1 暗号鍵生成 (非対称鍵に関して)

下位階層： 他のコンポーネントなし。

FCS_CKM.1.1 *詳細化：*TSF は、以下に従って*鍵確立に用いられる非対称*暗号鍵を生成しなければならない (shall)：

[*選択：*

- *有限体ベースの鍵確立スキームについては、NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"；*
- *楕円曲線ベースの鍵確立スキームならびに「NIST 曲線」P-256、P-384 及び [選択：P-521、その他の曲線なし] (FIPS PUB 186-3, "Digital Signature Standard" の定義による) の実装については、NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"*
- *RSA ベースの鍵確立スキームについては、NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"]*

及び [***112 ビットの等価安全性 (bits of security) と同等、またはそれよりも大きい***] 規定された暗号鍵サイズであって、以下：[***最初の選択で定義された規格***] を満たすもの。

適用上の注意： *このコンポーネントは、TOE により用いられる様々な暗号プロトコル (例えば IPsec) の鍵確立の目的で用いられる公開鍵／プライベート鍵ペアを TOE が生成できることを要求する。複数のスキームがサポートされている場合、ST 作成者はこの要件を繰り返してこの機能を取り込まなければならない (must)。用いられるスキームは、ST 作成者により選択の中から選ばれることになる。*

用いられるべきドメインパラメタは本 PP のプロトコル要件により規定されているため、TOE がドメインパラメタを生成することは期待されておらず、従って本 PP に規定されたプロトコルに TOE が準拠する際には追加的なドメインパラメタの検証は必要とされない。

2048 ビットの DSA 及び rDSA 鍵の生成された鍵の強度は、等価安全性が 112 ビットと同等、またはそれよりも大きい必要がある。同等の鍵強度に関する情報については、NIST Special Publication 800-57, "Recommendation for Key Management" を参照すること。

依存性： [FCS_CKM.2 暗号鍵の配付、または

FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵の破棄

保証アクティビティ：

評価者は、ST 作成者により行われた選択に応じて、上記の要件を試験する際のガイドとして"The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS)"、"The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)"、及び"The RSA Validation System (RSA2VS)"の鍵ペア生成部分を用いなければならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの信頼できる参照実装を評価者が有していることが必要となる。

行われた選択に応じて TSF が 800-56A または 800-56B あるいはその両方に適合していることを示すため、評価者は TSS に以下の情報が含まれることを保証しなければならない (shall)。

- *TSS には、TOE が適合する 1 つまたは複数の適切な 800-56 規格のすべての節が列挙されていなければならない (shall)。*
- *TSS に列挙された該当する節のそれぞれについて、「しなければならない (shall)」でない言明（すなわち、「してはならない (shall not)」、「すべきである (should)」、及び「すべきでない (should not)」）のすべてにおいて、そのようなオプションを TOE が実装している場合、それが TSS に記述されなければならない (shall)。含まれる機能が規格においては「してはならない (shall not)」または「すべきでない (should not)」とされている場合、TOE により実装されたセキュリティ方針に対してこれが悪影響を与えない理由の根拠が TSS に提供されなければならない (shall)。*
- *800-56A 及び 800-56B (選択に応じて) の該当する節のそれぞれにおいて、「しなければならない (shall)」または「すべきである (should)」との言明に関連した機能が欠けている場合、それが記述されなければならない (shall)；*

- *TOE が実施すべきセキュリティ要件に影響する可能性のある TOE に特有の拡張、文書に含まれていない処理、または文書により許可された代案の実装が存在する場合、それが記述されなければならない (shall)。*

C.8.2 FCS_CKM_EXT.4 暗号鍵のゼロ化

下位階層： 他のコンポーネントなし。

FCS_CKM_EXT.4.1 TSF は、すべての平文の秘密及び秘密暗号鍵ならびに暗号セキュリティパラメタを、もはや必要とされなくなった際にゼロ化しなければならない (shall)。

適用上の注意： *あらゆるセキュリティ関連情報 (鍵や認証データ、そしてパスワードなど) は、セキュリティ上重要なデータの暴露または改変を防止するため、もはや使われなくなった際にはゼロ化されなければならない (shall)。*

上述のゼロ化は、平文鍵または暗号クリティカルセキュリティパラメタあるいはその両方のすべての中間ストレージ領域 (すなわち、メモリバッファなど任意のストレージであって、そのようなデータの経路中に含まれるもの) に、その鍵または暗号クリティカルセキュリティパラメタあるいはその両方が別の場所へ転送された際に適用される。

依存性： 依存性なし。

保証アクティビティ：

評価者は、秘密鍵 (対称鍵暗号化に用いられる鍵)、プライベート鍵、及び鍵の生成に用いられるクリティカルセキュリティパラメタのそれぞれが、それらがゼロ化される時点 (例えば、使用直後、システムのシャットダウン時など)、及び行われるゼロ化手続きの種類 (ゼロで上書き、ランダムパターンで三回上書き、など) と共に TSS に記述されていることをチェックして保証しなければならない (shall)。保護されるべきマテリアルの保存に異なる種類のメモリが用いられる場合、評価者はデータが保存されるメモリに応じたゼロ化手続き (例えば、「フラッシュメモリ上に保存される秘密鍵はゼロで一回上書きすることによりゼロ化されるが、内部ハードドライブ上に保存される秘密鍵は書き込みごとに変化するランダムパターンを三回上書きすることによりゼロ化される」) が TSS に記述されていることをチェックして保証しなければならない (shall)。

C.8.3 FCS_COP.1(1) 暗号操作 (データの暗号化／復号に関して)

下位階層： 他のコンポーネントなし。

FCS_COP.1.1(1) *詳細化：*TSF は、規定された暗号アルゴリズム *[割付：1 つ以上のモード]* で動作する *AES* であって、暗号鍵サイズが *128* ビット、*256* ビット、及び *[選択：192 ビット、その他の鍵サイズなし]* の、以下を満たすものに従って*暗号化及び復号*を行わなければならない (shall)。

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

適用上の注意： *割付については、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しなければならない (must)。最初の選択については、ST 作成者はこの機能によりサポートされる鍵サイズを選択しなければならない (must)。第 2 の選択については、ST 作成者は割付中に規定されたモードを記述する規格を選択しなければならない (must)。*

依存性： [FDP_ITC.1 セキュリティ属性の伴わない利用者データのインポート、または

FDP_ITC.2 セキュリティ属性の伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵の破棄

保証アクティビティ：

評価者は、上記の要件をテストする際のガイドとして"The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)"、"The XTS-AES Validation System (XTSVS)"、"The CMAC Validation System (CMACVS)"、"The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)"、及び"The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (これらの文書は

http://csrc.nist.gov/groups/STM/cavp/index.html から入手できる) から、上記の要件において選択されたモードに適切なテストを用いなければならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの参照実装を評価者が有していることが必要となる。

C.8.4 FCS_COP.1(2) 暗号操作 (暗号署名に関して)

下位階層： 他のコンポーネントなし。

FCS_COP.1.1(2) *詳細化：*TSF は、*選択：*

(1) 2048 ビット以上の鍵サイズ (モジュラス) を用いたデジタル署名アルゴリズム (DSA)、

(2) 2048 ビット以上の鍵サイズ (モジュラス) を用いた RSA デジタル署名アルゴリズム (rDSA)、または

(3) 256 ビット以上の鍵サイズを用いた楕円曲線デジタル署名 (ECDSA)

であって、以下を満たすものに従って*暗号署名サービス*を行わなければならない (shall)。

デジタル署名アルゴリズムの場合：

- *FIPS PUB 186-3, "Digital Signature Standard"; または*

RSA デジタル署名アルゴリズムの場合：

- *FIPS PUB 186-3, "Digital Signature Standard"; または*

楕円曲線デジタル署名アルゴリズムの場合：

- *FIPS PUB 186-3, "Digital Signature Standard"; 及び*
- *TSF は、「NIST 曲線」P-256、P-384 及び [選択：P-521、その他の曲線なし] (FIPS PUB 186-3, "Digital Signature Standard" の定義による) を実装しなければならない (shall)。*

適用上の注意： *暗号署名に関する好ましいアプローチとして、本 PP の将来の版では楕円曲線が要求されることになる。*

ST 作成者は、デ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しなければならない (must)。2 つ以上のアルゴリズムが利用できる場合、この要件 (及び対応する FCS_CKM.1 要件) はその機能を規定するために繰り返されなければならない (must)。選択された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規定しなければならない (must)。

楕円曲線ベースの方式に関しては、鍵サイズは基点の位数の 2 の対数を示す。デジタル署名に関する好ましいアプローチとして、本 PP の将来の版では ECDSA が要求されることになる。

依存性： [FDP_ITC.1 セキュリティ属性の伴わない利用者データのインポート、または

FDP_ITC.2 セキュリティ属性の伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵の破棄

保証アクティビティ：

評価者は、"The FIPS 186-3 Digital Signature Algorithm Validation System (DSAVS)"、"The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)" 及び "The RSA Validation System (RSA2VS)" の署名生成及び署名検証の部分を上記の要件をテストする際のガイドとして利用しなければならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの参照実装を評価者が有していることが必要となる。

C.8.5 FCS_COP.1(3) 暗号操作 (暗号ハッシュに関して)

下位階層： 他のコンポーネントなし。

FCS_COP.1.1(3) *詳細化：*TSF は、規定された暗号アルゴリズム *[選択：SHA-1、SHA 256、SHA 384]* であって、メッセージダイジェストのサイズが *[選択：160、256、384]* ビットの、以下：*FIPS Pub 180-3,*

“Secure Hash Standard” を満たすものに従って*暗号ハッシュサービス*を行わなければならない (shall)。

適用上の注意： *PP のこのバージョンでは、SHA-1 の使用は TLS についてのみ後方互換性の理由により許可される。PP の次のバージョンでは、SHA-1 の使用は完全に除外されることになるだろう。*

ハッシュアルゴリズムの選択は、メッセージダイジェストサイズの選択と対応していなければならない (shall)。例えば、SHA-1 が選択された場合、唯一の有効なメッセージダイジェストサイズの選択は 160 ビットとなる。

依存性： [FDP_ITC.1 セキュリティ属性の伴わない利用者データのインポート、または

FDP_ITC.2 セキュリティ属性の伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵の破棄

保証アクティビティ：

評価者は、上記の要件をテストする際のガイドとして"The Secure Hash Algorithm Validation System (SHAVS)"を用いなければならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの参照実装を評価者が有していることが必要となる。

C.8.6 FCS_COP.1(4) 暗号操作 (鍵付きハッシュによるメッセージ認証)

下位階層： 他のコンポーネントなし。

FCS_COP.1.1(4) *詳細化：*TSF は、規定された暗号アルゴリズム *HMAC-[選択：SHA-1、SHA-256、SHA-384]* であって、*鍵サイズが [割付：HMAC に用いられる (ビット単位の) 鍵サイズ]*、そしてメッセージダイジェストのサイズが *[選択：160、256、384]* ビットの、以下：*FIPS PUB 198-1, “The Keyed-Hash Message Authentication Code”、及び FIPS PUB 180-3, “Secure Hash Standard”* を満たすものに従って*鍵付きハッシュによるメッセージ認証*を行わなければならない (shall)。

適用上の注意： *PP のこのバージョンでは、SHA-1 の使用は TLS についてのみ後方互換性の理由により許可される。PP の次のバージョンでは、SHA-1 の使用は完全に除外されることになるだろう。*

ハッシュアルゴリズムの選択は、メッセージダイジェストサイズの選択と対応していなければならない (must)。例えば、HMAC-SHA-256 が選択された場合、唯一の有効なメッセージダイジェストサイズの選択は 256 ビットとなる。

上記のメッセージダイジェストサイズは、基盤として用いられるハッシュアルゴリズムに対応する。ハッシュの計算後に HMAC の出力を切り捨てることは、様々なアプリケーションにおいて適切なステップであることに注意すること。このことは、この要件への適合性を無効とするものではないが、切り捨てが行われること、最終出力のサイズ、そしてこの切り捨てが準拠する規格が ST に言明されなければならない (must)。

依存性： [FDP_ITC.1 セキュリティ属性の伴わない利用者データのインポート、または

FDP_ITC.2 セキュリティ属性の伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵の破棄

保証アクティビティ：

評価者は、上記の要件をテストする際のガイドとして"The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" を用いなければならない (shall)。このためには、テスト中に検証可能なテストベクトルを作成できるアルゴリズムの参照実装を評価者が有していることが必要となる。

C.8.7 FCS_HTTPS_EXT.1 HTTPS

下位階層： 他のコンポーネントなし。

依存性： FCS_TLS_EXT.1 TLS

FCS_HTTPS_EXT.1.1 TSF は、RFC 2818 に準拠する HTTPS プロトコルを実装しなければならない (shall)。

適用上の注意： *ST 作成者は、識別された 1 つまたは複数の規格に実装がどのように準拠しているかを決定するために十分な詳細を提供しなければならない (must)。これは、このコンポーネントへエレメントを追加することにより、または TSS 中の追加的詳細により、達成できる。*

FCS_HTTPS_EXT.1.2 TSF は、FCS_TLS_EXT.1 に指定される TLS を用いて HTTPS を実装しなければならない (shall)。

依存性： FCS_TLS_EXT.1 TLS

保証アクティビティ：

評価者は TSS をチェックして、HTTPS が TLS を用いて管理セションを確立する方法に関して明確であることを、TLS プロトコルにより要求されるクライアント認証が存在する場合、処理スタックの異なるレベルで行われ得るセキュリティ管理者認証と対比してそれに注目しながら、保証しなければならない (shall)。評価者は TSS をチェックして、このプロトコルと関連付けられた FCS 要件中の暗号機能 (FCS_COP.1(1) など) が暗号機能の実行に用いられる方法が記述されていることを検証しなければならない (shall)。運用環境により提供される暗号機能については、評価者は TSS をチェックして、(ST 中に識別されるプラットフォームのそれぞれについて) この機能を呼び出すために TOE により使われるインタフェースが記述されていることを保証しなければならない (shall)。

この要件に関しては、操作ガイダンスに対して行われるべき保証アクティビティは存在しない。

このアクティビティのテストは、TLS テストの一部として行われる。これは、TLS テストが TLS プロトコルレベルで行われる場合、追加的なテストとなるかもしれない。

C.8.8 FCS_IPSEC_EXT.1 IPsec

下位階層： 他のコンポーネントなし。

FCS_IPSEC_EXT.1.1 TSF は、RFC 4303 に定義される IPsec プロトコルの ESP を、暗号アルゴリズム AES-CBC-128、AES-CBC-256 (両者とも RFC 3602 により指定される)、 [選択：その他のアルゴリズムなし、RFC 4106 に指定される AES-GCM-128、AES-GCM-256] を用い、また [選択、少なくとも 1 つを選択：RFC 2407、2408、2409、RFC 4109、RFC 2407、2408、2409、RFC 4109、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 IKEv1; RFC 5996 (節 2.23 に指定される NAT トラバーサルのサポートが必須)、4307、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 IKEv2] を用いて実装しなければならない (shall)。

適用上の注意： *最初の選択は、サポートされる追加的暗号アルゴリズムを識別するために用いられる。IKEv1 か IKEv2 のいずれかのサポートが提供されなければならない (must) が、適合する TOE は両方を提供できる;2 番目の選択は、これを選ぶために用いられる。IKEv1 については、RFC 4109 に記述された追加／変更を含め、RFC 2409 に準拠する IKE の実装を要求しているものと解釈されるべきである。RFC 4868 は、IKEv1 と IKEv2 の両方に用いられる追加的ハッシュ関数を識別している；これらの関数が実装される場合、3 番目 (IKEv1 について) 及び 4 番目 (IKEv2 について) の選択を用いることができる。IKEv2 は、2014 年 1 月 1 日以降、要求されることになる。*

FCS_IPSEC_EXT.1.2 TSF は、IKEv1 フェーズ 1 交換ではメインモードのみが用いられることを保証しなければならない (shall)。

FCS_IPSEC_EXT.1.3 TSF は、IKEv1 SA ライフタイムがフェーズ 1 SA については 24 時間、フェーズ 2 SA については 8 時間に制限できることを保証しなければならない (shall)。

適用上の注意： *上記の要件は、セキュリティ管理者により構成可能なライフタイムを (必要に応じて、適切な FMT 要件及び AGD_OPE により義務付けられる文書中の指示と共に) 提供すること、または制限を実装に「ハードコーディング」することの、いずれかの手段により達成できる。*

FCS_IPSEC_EXT.1.4 TSF は、IKEv1 SA ライフタイムがフェーズ 2 SA について [***割付：100 - 200 の範囲の数値***] MB のトラフィックに制限できることを保証しなければならない (shall)。

適用上の注意： *上記の要件は、セキュリティ管理者により構成可能なライフタイムを (適切な FMT 要件及び AGD_OPE により義務付けられる文書中の指示と共に) 提供すること、または制限を実装に「ハードコーディング」することの、いずれかの手段により達成で*

きる。ST 作成者は、要件により指定される範囲でデータの量を選択する。

FCS_IPSEC_EXT.1.5 TSF は、すべての IKE プロトコルに DH グループ 14 (2048 ビット MODP)、及び [選択：24 (2048 ビット MODP と 256 ビット POS)、19 (256 ビットランダム ECP)、20 (384 ビットランダム ECP)、 [***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 (shall)。

適用上の注意： *上記は TOE が DH グループ 14 をサポートすることを要求している。他のグループがサポートされる場合、それらは選択 (グループ 24、19、及び 20) されるか上記の割付中に指定されるべきである (should)；それ以外の場合「その他の DH グループなし」が選択されるべきである (should)。これは、IKEv1 及び (実装されていれば) IKEv2 鍵交換に適用される。本 PP の将来のバージョンでは、DH グループ 19 (256 ビットランダム ECP) 及び 20 (ビットランダム ECP) が要求されることになる。*

FCS_IPSEC_EXT.1.6 TSF は、すべての IKE プロトコルに [選択：DSA、rDSA、ECDSA] アルゴリズムを用いたピア認証が実装されることを保証しなければならない (shall)。

適用上の注意： *選択されたアルゴリズムは、FCS_COP.1(2) の適切な選択と対応しているべきである (should)。*

FCS_IPSEC_EXT.1.7 TSF は、その IPsec 接続の認証に用いられる事前共有鍵の使用を (RFC 中で参照されているように) サポートしなければならない (shall)。

FCS_IPSEC_EXT.1.8 TSF は、以下をサポートしなければならない (shall)：

1. 事前共有鍵は、大文字及び小文字、数字、ならびに特殊文字： [選択：“!”、“@”、“#”、“$”、“%”、“^”、“&”、“*”、“(“、“)”、[***割付：その他の文字***] の任意の組み合わせにより構成できなければならない (shall)；
2. 22 文字及び [選択：[***割付：その他のサポートされる長さ***]、その他の長さなし] の事前共有鍵。

適用上の注意： *ST 作成者は、TOE により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的な特殊文字が、オプションとして列挙されてもよい。事前共有鍵の長さについては、相互運用性の向上に資するため、共通の長さ (22 文字) が必要とされる。他の長さがサポートされる場合、それが割付中に列挙されるべきである (should)；またこの割付には、値の範囲 (例えば「5 から 55 文字まで」) を規定することもできる。*

依存性： FCS_COP.1 暗号操作

保証アクティビティ：

評価者は、以下を検証するため、TSS を検査しなければならない (shall)：

1. *要件中に指定される RFC から、完全性保護に用いられるハッシュ関数が規定されていること。*
2. *「機密性のみ」ESP モードが無効化される方法が記述されていること。*
3. *TOE でサポートされている IPsec プロトコルの記述において、IKEv1 フェーズ 1 交換にアグレッシブモードが使用されずメインモードのみが使用されることが言明されていること。*
4. *IKEv1 SA (フェーズ 1 とフェーズ 2 の両方) について、ライフタイムが確立される方法が記述されていること。*
5. *IKEv1 フェーズ 2 SA のライフタイム (所与の SA を利用して流れることが許可されるトラフィックの量に関して) が確立される方法が記述されていること。*
6. *要件に指定される DH グループがサポートされるものとして列挙される方法が記述されていること。1 つよりも多くの DH グループがサポートされる場合、特定の DH グループをピアとの間で指定／ネゴシエーションする方法が記述されていること。*
7. *事前共有鍵が確立され IPsec 接続の認証に用いられる方法が TSS に記述されていること。この記述には、事前共有鍵を生成できる TOE と、単純に事前共有鍵を利用するだけの TOE との両方について、事前共有鍵の確立が実現される方法が示されていなければならない (shall)。*
8. *このプロトコルと関連付けられた FCS 要件中の暗号機能 (FCS_COP.1(1) など) が暗号機能の実行に用いられる方法が記述されていること。運用環境により提供さ*

れる暗号機能については、評価者は以下のアクティビティを行わなければならない (shall)。

a. 運用環境を構成する代表的なプラットフォームのリスト (ハードウェア及びソフトウェア) が ST に含まれることを保証する。

b. TSS をチェックして、(ST 中に識別されるプラットフォームのそれぞれについて) この機能を呼び出すために TOE により使われるインタフェースが記述されていることを保証する。

c. ST 中に識別されたプラットフォームのそれぞれについて、OE 文書をチェックして前のステップで識別することンタフェースが存在することを保証する。

評価者は、以下を決定するため、操作ガイダンスを検査しなければならない (shall) :

1. *接続の暗号パラメタが管理者により設定可能な場合、これらのパラメタを設定するための指示、これらのパラメタを用いて IPsec 接続を確立する方法、そして評価される構成においてどのパラメタ値が許可されるかが提供されていること。*
2. *「機密性のみ」モードを保証無効化するために必要な任意の構成と、パケット全体を保護するためトンネルモードが望ましい ESP モードであることを示す助言が存在することが記述されていること。*
3. *メインモードを利用する前に TOE を構成するための指示が含まれていること (そのような構成が必要な場合)。*
4. *IKEv1 SA のライフタイムを構成するための指示が含まれていること (これらの値が構成可能な場合)。*
5. *所与の SA を利用して流れることができるトラフィックの最大量を構成するための指示が含まれていること (この値が構成可能な場合)。*
6. *事前共有鍵が生成され TOE に対して確立される方法が記述されていること。この記述には、事前共有鍵を生成できる TOE と、単純に事前共有鍵を利用するだけの TOE との両方について、事前共有鍵の確立が実現される方法が示されていなければならない (shall)。*
7. *強靭な鍵を生成するガイダンスや許可される文字セットを含め、事前共有鍵の生成について記述されていること。また評価者は、このガイダンスが要件を満たさなくなるような形で事前共有鍵を制限していないこともチェックしなければならない (shall)。管理者が (操作ガイダンスに違反して) 要件に適合しない鍵を選ぶことが*

できる一方で、その鍵がこのコンポーネントに指定されるルールを満たすことを TOE がチェックするという要件は存在しないことは注意すべきである (should)。しかし、管理者が上記のルールに (そして操作ガイダンスに) 適合するパスワードを作成することを選んだとすれば、TOE はそのような選択を禁止すべきではない (should not)。

また評価者は、以下のテストを行わなければならない (shall)。これらのテストの側面は、個別のテストそれぞれが満たされることを例証できる限り、結合されてもよいことに注意すること。

- *テスト 1 : 評価者は、FCS_IPSEC_EXT.1.1 に規定されたパラメタのそれぞれを用いて、IPsec 接続を構成し確立しなければならない (shall)。すべてのパラメタのすべての組み合わせを用いて接続を行うことは必要とされない一方で、どの組み合わせがテストされたか、また選ばれたそのサブセットが代表的なものである理由は明確にされなければならない (must)。テストの意図を満たすには、暗号スイートのネゴシエーションが成功することを (通信路上で) 確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビット AES であって256 ビットAES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。ネゴシエーションがあいまい化され得る場合 (例えば、フェーズ 2 ネゴシエーション)、要求されるパラメタが使われていることを示す代替的な手段は許容可能である (例えば、特定の確立された接続に対して用いられているパラメタを示すよう設計された管理コマンド)。*

- *テスト 2 : 評価者は操作ガイダンスの指示により TOE を構成し、アグレッシブモードで IKEv1 フェーズ 1 接続を使用した接続の確立を試行しなければならない (shall)。この試行は失敗するはずである (should)。評価者は次に、メインモードの交換がサポートされていることを示すべきである (should)。*

- *テスト 3 : 評価者は操作ガイダンスの指示により TOE を構成し、ESP を「機密性のみ」モードで使用した接続の確立を試行しなければならない (shall)。この試行は失敗するはずである (should)。次に評価者は、ESP を機密性及び完全性モードで使用した接続を確立しなければならない (shall)。*

- *テスト 4 : 評価者は、フェーズ 1 SA が確立され、再ネゴシエーションまでに 24 時間を超えて維持が試行されるようにテストを構築しなければならない (shall)。評価者は、24 時間以内にこの SA がクローズされるか、再ネゴシエーションされることを確認しなければならない (shall)。そのようなアクションのために TOE が特定の構成を必要とする場合、評価者は TOE の構成機能が操作ガイダンスに*

文書化されたように動作することを例証するテストを実施しなければならない (shall)。

- *テスト5:評価者は、ライフタイムが24 時間ではなく8 時間であることを除いて、テスト1 と同様のテストをフェーズ2 SA に対して行わなければならない (shall)。*
- *テスト6 : 評価者は、フェーズ2 SA が確立され、その接続上で上記の割付に規定されたものよりも大量のデータが流れる間維持が試行されるようにテストを構築しなければならない (shall)。評価者は、規定されたデータの量を超える前にこの SA がクローズされるか、再ネゴシエーションされることを確認しなければならない (shall)。そのようなアクションのために TOE が特定の構成を必要とする場合、評価者は TOE の構成機能が操作ガイダンスに文書化されたように動作することを例証するテストを実施しなければならない (shall)。*
- *テスト7 : サポートされる DH グループのそれぞれについて、評価者はその特定の DH グループを用いてすべての IKE プロトコルの完了が成功することをテストし保証しなければならない (shall)。*
- *テスト 8 : 評価者は、操作ガイダンスに示されるように事前共有鍵を生成して使用し、2 つのピアの間の IPsec 接続を確立させなければならない (shall)。TOE が事前共有鍵の生成をサポートしている場合、鍵を生成する TOE のインスタンスだけではなく、単に鍵を受け取り利用するだけの TOE のインスタンスについても、鍵の確立が行われることを評価者は保証しなければならない (shall)。*
- *テスト9 : 評価者は、上記の構成要件を満たす 22 文字の長さの事前共有鍵を生成しなければならない (shall)。次に評価者はこの鍵を使用して、IPsec 接続の確立を成功させなければならない (shall)。評価者には要件に列挙されたすべての特殊文字または長さがサポートされていることをテストすることは要求されない一方で、テストのために選ばれたこれらの文字のサブセットを正当化することが要求される (実際にサブセットが用いられた場合)。*

C.8.9 FCS_RBG_EXT.1 暗号操作 (ランダムビット生成)

下位階層： 他のコンポーネントなし。

FCS_RBG_EXT.1.1 TSF は、 [選択、1 つを選択 : [選択 : Hash_DRBG (任意) 、HMAC_DRBG (任意) 、CTR_DRBG (AES) 、Dual_EC_DRBG (任意)] を用いる NIST Special Publication 800-90、FIPS Pub 140-2 附属書 C : AES を用いる X9.31 附属書 2.4] であって、[選択、1 つを選択 : (1) 1 つ以上の独立したハードウェアベース

の雑音源、(2) 1 つ以上の独立したソフトウェアベースの雑音源、(3) ハードウェアベースとソフトウェアベースの雑音源の組み合わせ] からエントロピーを蓄積するエントロピー源によりシードを供給されるものに従って、すべてのランダムビット生成 (RBG) サービスを行わなければならない (shall) 。

FCS_RBG_EXT.1.2 決定論的 RBG は、鍵とそれが生成するハッシュの中で最もセキュリティ強度の高いものと少なくとも等しい、最小で [選択、1 つを選択 : 128 ビット、256 ビット] のエントロピーによりシードが供給されなければならない (shall)。

適用上の注意： *NIST Special Pub 800-90 の附属書 C には、FIPS-140 の将来のバージョンでおそらく必要とされることになる最小エントロピー量が記述されている。可能であれば直ちにこれを用いるべきであり (should)、また本 PP の将来のバージョンでは要求されることになる。*

FCS_RBG_(EXT).1.1 の最初の選択に関しては、ST 作成者は RBG サービスが適合する規格 (800-90 または 140-2 附属書 C のいずれか) を選択しなければならない (must)。

SP 800-90 には、4 つの異なる乱数生成手法が含まれる。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 (800-90 が選択される場合)、要件または TSS に用いられる具体的な基盤となる暗号プリミティブを取り込む。識別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 に許可されるが、CT_DRBG には AES ベースの実装のみが許可される。800-90 に定義された任意の曲線が Dual_EC_DRBG に許可される一方で、ST 作成者は選択された曲線だけではなく、利用されるハッシュアルゴリズムも取り込まなければならない (must)。

FIPS Pub 140-2 の附属書 C については、現在のところ NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms の節 3 に記述される手法のみが有効であることに注意すること。ここで用いられる AES 実装の鍵の長さが利用

者データの暗号化に用いられるものと異なる場合、FCS_COP.1 を調整するか繰り返して異なる鍵の長さを反映する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。

また ST 作成者は、任意の基盤となる機能が TOE のベースライン要件に保証含まれるようにする。

FCS_RBG_EXT.1.2 の選択については、ST 作成者は ST に含まれるアルゴリズムの中で最も大きなセキュリティ強度に対応するエントロピーの適切なビット数を選択する。セキュリティ強度は、NIST SP 800-57A の表 2 及び 3 に定義されている。例えば、実装に 2048 ビット RSA (セキュリティ強度 112 ビット)、AES 128 (セキュリティ強度128 ビット)、そしてHMAC-512 (セキュリティ強度 256 ビット) が含まれている場合、ST 作成者は 256 を選択することになる。

依存性： 依存性なし。

保証アクティビティ：

評価者は TSS 節をレビューして、TOE に用いられる RBG を含む製品のバージョン番号を決定しなければならない (shall)。また評価者は TSS をレビューして、附属書 C.9 エントロピーの文書かと評定に記述された要件に十分対応する議論が含まれていることを決定しなければならない (shall)。本文書は、セキュリティターゲットの補遺として取り込まれてもよい。

RBG がどの規格への適合を主張しているかに関わらず、評価者は以下のテストを行う：

テスト 1：評価者は、エントロピー源テストスイート (Entropy Source Test Suite) を用いることにより、各エントロピー源のエントロピーの推定値を決定しなければならない (shall)。評価者は、全エントロピー源から得られたすべての結果の最小値であるエントロピーの推定値が TSS に含まれていることを保証しなければならない (shall)。

FIPS 140-2 の附属書 C に準拠する実装

本節に含まれるテストの参照情報は、The Random Number Generator Validation System (RNGVS) [RNGVS] である。評価者は、以下の 2 つのテストを実施しなければならない (shall)。「期待値」は、正しいことが知られているアルゴリズムの参照実装により作成され

ることに注意すること。正しさの証明は、各スキームに任される。

評価者は、可変シードテストを行わなければならない (shall)。評価者は (Seed, DT) ペアの 128 個のセット (それぞれ 128 ビット) をTSF のRBG 機能に提供しなければならない (shall)。また評価者は、128 ペアの (Seed, DT) すべてについて一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。DT の値は、各セットについて1 ずつ増やされる。シードの値は、セットの中で繰り返されてはならない (shall not)。評価者は、TSF により返される値が期待値と一致することを保証する。

評価者は、モンテカルロテストを行わなければならない (shall)。このテストについては、評価者がシード及びDT の初期値 (それぞれ128 ビット) をTSF のRBG 機能に提供する。また評価者は、テストを通して一定である (AES アルゴリズムに適切な長さの) 鍵も提供しなければならない (shall)。次に評価者はTSF のRBG を、繰返しのたびにDT の値を1 ずつ増やしながら、そして NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms の節3 に指定されるように次回の繰返しの際の新たなシードを作成して、10,000 回呼び出す。評価者は、得られた 10,000 番目の値が期待値と一致することを保証する。

NIST Special Publication 800-90 に準拠する実装

評価者は、RNG 実装の 15 回の試行を行わなければならない (shall)。RNG が構成可能な場合、評価者は各構成について 15 回の試行を行わなければならない (shall)。また評価者は、RNG 機能を構成するための適切な指示が操作ガイダンスに含まれていることも確認しなければならない (shall)。

RNG が有効な予測困難性を持つ場合、各回の試行は (1) drbg をインスタンス化し、(2) ランダムなビットの最初のブロックを生成し、(3) ランダムなビットの2 番目のブロックを生成し、(4) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして個別化文字列である。次の 2 つは、最初の生成呼び出しへの追加的入力とエントロピー入力である。最後の 2 つは、2 番目の生成呼出しへの追加的入力とエントロピー入力である。これらの値は、ランダムに生成される。「ランダムなビットのひとつのブロックを生成」とは、返されるビット数が (NIST SP 800-90 に定義される) Output Block Length と等しいランダムなビットを生成することを意味する。

RNG が予測困難性を持たない場合、各回の試行は (1) drbg をインスタンス化し、(2) ランダムなビットの最初のブロックを生成し、(3) シードを再供給し、(4) ランダムなビッ

トの 2 番目のブロックを生成し、 (5) 非インスタンス化する、という手順になる。評価者は、ランダムなビットの 2 番目のブロックが期待された値であることを検証する。評価者は、各試行に 8 つの入力値を生成しなければならない (shall)。最初はカウント (0～14) である。次の 3 つはインスタンス化操作のエントロピー入力とノンス、そして個別化文字列である。5 番目の値は、最初の生成呼出しへの追加的入力である。6 番目と 7 番目は、シードを再供給する呼出しへの追加的入力とエントロピー入力である。最後の値は、2 回目の生成呼出しへの追加的入力である。

以下のパラグラフには、評価者により生成／選択されるべき入力値のいくつかについて、より多くの情報が含まれている。

***エントロピー入力**：エントロピー入力値の長さは、シードの長さと等しくなければならない (must)。*

***ノンス**：ノンスがサポートされている場合 (導出関数 (df) なしの CTR_DRBG はノンスを利用しない)、ノンスのビット長はシードの長さの半分となる。*

***個別化文字列**：個別化文字列の長さは、シードの長さ以下でなければならない (must)。実装が 1 とおりの個別化文字列の長さしかサポートしていない場合、両方の値に同一の長さが使用できる。2 とおり以上の文字列の長さがサポートされている場合、評価者は 2 つの異なる長さの個別化文字列を用いなければならない (shall)。実装が個別化文字列を用いない場合、値を供給する必要はない。*

***追加的入力**：追加的入力のビット長は、個別化文字列の長さと同一のデフォルトと制約を持つ。*

C.8.10 FCS_SSH_EXT.1 SSH

下位階層： 他のコンポーネントなし。

FCS_SSH_EXT.1.1 TSF は、RFC 4251、4252、4253、及び 4254 に準拠する SSH プロトコルを実装しなければならない (shall)。

適用上の注意： *ST 作成者は、識別された 1 つまたは複数の規格に実装がどのように準拠しているかを決定するために十分な詳細を提供しなければならない (must)。これは、このコンポーネントへエレメントを追加することにより、または TSS 中の追加的詳細により、達成できる。本 PP の将来のバージョンでは、鍵更新に関して要件が追加されることになる。この要件は、「TSF は、その鍵を用いて 2^{28} 以下のパケットが通過した後に SSH 接続が鍵更新*

されることを保証しなければならない (shall)」となる。

FCS_SSH_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手法をサポートすることを保証しなければならない (shall)：公開鍵に基づくもの、パスワードに基づくもの。

FCS_SSH_EXT.1.3 TSF は、RFC 4253 に記述されるように、SSH トランスポート中の [***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 (shall)。

適用上の注意： *RFC 4253 は、「大きなパケット (large packets)」の受け入れを、そのパケットが「合理的な長さ (reasonable length)」でなければ破棄されるべき (should) という注意と共に規定している。割付には受け入れられる最大のパケットサイズが ST 作成者により記入され、これにより TOE の「合理的な長さ (reasonable length)」が定義されるべきである (should)。*

FCS_SSH_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用いることを保証しなければならない (shall)：AES-CBC-128、AES-CBC-256、[選択：AEAD_AES_128_GCM、AEAD_AES_256_GCM、その他のアルゴリズムなし]。

適用上の注意： *割付の中で、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「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 中に存在すべきである (should)。2010 年 12 月に NDPP v1.0 が公開されて以降、商用ネットワークデバイスにおける AES-GCM のサポートの普及に関してかなりの進歩が見られた。将来に公開される本 PP の更新されたバージョンでは、AES-GCM が要求される一方で AES-CBC がオプションとなることは十分にあり得る。*

FCS_SSH_EXT.1.5 TSF は、SSH トランスポートの実装がその 1 つまたは複数の公開鍵アルゴリズムとして SSH_RSA 及び [選択：PGP-SIGN-RSA、PGP-SIGN-DSS、その他の公開鍵アルゴリズムなし] を用いることを保証しなければならない (shall)。

適用上の注意： *RFC 4253 は、要求される (required) 公開鍵アルゴリズムと許可できる (allowable) 公開鍵アルゴリズムを規定している。こ*

の要件により SSH-RSA は「要求される (required)」ものとなり、またその他2 つがST 中で主張できるようになる。ST 作成者は、SSH_RSA のみが実装される場合「その他の公開鍵アルゴリズムなし」を選択して、適切な選択を行うべきである (should)。

FCS_SSH_EXT.1.6 TSF は、SSH トランスポート接続に用いられるデータ完全性アルゴリズムが [選択 : hmac-sha1、hmac-sha1-96、hmac-md5、hmac-md5-96] であることを保証しなければならない (shall)。

FCS_SSH_EXT.1.7 TSF は、diffie-hellman-group14-sha1 が SSH プロトコルに用いられる唯一の許可される鍵交換手法であることを保証しなければならない (shall)。

依存性： FCS_COP.1 暗号操作

保証アクティビティ：

評価者は、以下を検証するため、TSS を検査しなければならない (shall)：

1. *認証への使用に受容可能な公開鍵アルゴリズムの記述が含まれること、このリストが FCS_SSH_EXT.1.5 に適合すること、そしてパスワードに基づく認証手法もまた許可されること。*
2. *RFC 4253 の意味での「大きなパケット (large packets)」がどのように検出され取り扱われるか記述されていること。*
3. *任意の暗号アルゴリズム及びオプションの特徴が規定されていること、そしてこの情報がSFR と一貫していること。*
4. *サポートされるデータ完全性アルゴリズムが列挙されていること、またそのリストがこのSFR 中のリストと対応していること。*
5. *このプロトコルと関連付けられた FCS 要件中の暗号機能 (FCS_COP.1(1) など) が暗号機能の実行に用いられる方法が記述されていること。運用環境により提供される暗号機能については、評価者は以下のアクティビティを行わなければならない (shall)。*
    a. *運用環境を構成する代表的なプラットフォームのリスト (ハードウェア及びソフトウェア) がST に含まれることを保証する。*
    b. *TSS をチェックして、(ST 中に識別されるプラットフォームのそれぞれにつ*

いて) この機能を呼び出すためにTOE により使われるインタフェースが記述されていることを保証する。

c. *ST 中に識別されたプラットフォームのそれぞれについて、OE 文書をチェックして前のステップで識別することンタフェースが存在することを保証する。*

評価者は、以下を検証するため、操作ガイダンスを検査しなければならない (shall) :

1. *SSH がTSS 中の記述に適合するようにTOE を構成するための指示 (例えば、TOE により通知されるアルゴリズムのセットが、要件に合うよう制限されなければならない (have to) かもしれない) が含まれていること。*
2. *許可されたデータ完全性アルゴリズムのみがTOE とのSSH 接続に用いられる (特に、MAC アルゴリズム「なし (none)」が許可されない) ことを保証する方法に関する管理者への指示が含まれていること。*
3. *SSH のすべての鍵交換がDH グループ14 を用いて行われるようにセキュリティ管理者が TOE を構成できるような構成情報が含まれていること。この機能が TOE に「ハードコーディング」されている場合、評価者はTSS をチェックしてSSH プロトコルの議論の中でこれが言明されていることを保証しなければならない (shall)。*

評価者は、以下のテストを行うことにより、この機能をテストしなければならない (shall)。

- *テスト 1 : 評価者は、サポートされる公開鍵アルゴリズムのそれぞれについて、その公開鍵アルゴリズムを用いた利用者接続の認証を TOE がサポートすることを示さなければならない (shall)。このテストをサポートするために要求される構成アクティビティが存在する場合、それは操作ガイダンス中の指示に従って行われなければならない (shall)。*
- *テスト 2 : 操作ガイダンスを用いて、評価者はパスワードに基づく認証を受け入れるようにTOE を構成し、認証子としてパスワードを用いたSSH 上でTOE への利用者の認証が成功することを例証しなければならない (shall)。*
- *テスト 3 : 評価者は、FCS_SSH_EXT.1.3 に規定されたものよりも大きなパケットを TOE が受信すると、そのパケットが破棄されることを例証しなければならない (shall)。*
- *テスト 4 : 評価者は、FCS_SSH_EXT.1.4 及びFCS_SSH_EXT.1.6 に規定された暗号化及び完全性アルゴリズムのそれぞれを用いて、SSH 接続を確立しなければならない (shall)。テストの意図を満たすには、アルゴリズムのネゴシエーション*

成功を (通信路上で) 確認すれば十分である。

- *テスト 5：評価者は、diffie-hellman-group1-sha1 鍵交換の実行を試行して、この試行が失敗することを確認しなければならない (shall)。次に評価者は、diffie-hellman-group14-sha1 鍵交換の実行を試行して、この試行が成功することを確認しなければならない (shall)。*

C.8.11 FCS_TLS_EXT.1 TLS

下位階層： 他のコンポーネントなし。

FCS_TLS_EXT.1.1 TSF は、以下の暗号スイートをサポートする以下の 1 つ以上のプロトコル [選択 : TLS 1.0 (RFC 2246)、TLS 1.1 (RFC 4346)、TLS 1.2 (RFC 5246)] を実装しなければならない (shall)：

必須暗号スイート：

TLS_RSA_WITH_AES_128_CBC_SHA

オプションの暗号スイート：

[選択：
なし
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
]。

適用上の注意： *ST 作成者は、TLS の実装を反映した適切な選択及び割付を行わなければならない (must)。ST 作成者は、識別された 1 つまたは複数の規格に実装がどのように準拠しているかを決定するために十分な詳細を提供しなければならない (must)。これは、*

このコンポーネントへエレメントを追加することにより、または TSS 中の追加的詳細により、達成できる。

評価される構成に用いられる暗号スイートは、この要件により制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである (should)。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、「なし」が選択されるべきである (should)。実装によりネゴシエーションされるスイートをこの要件中のものに制限するために管理手順が取られる必要がある場合、AGD_OPE により要求されるガイダンス中にその適切な指示が含まれる必要がある。上に列挙した Suite B アルゴリズム (RFC 5430) は、実装に望ましいアルゴリズムである。2010 年 12 月に NDPP v1.0 が公開されて以降、商用デバイスにおける TLS 1.2 の普及に関してあまり進歩が見られない。本 PP の将来の版では TLS 1.2 (RFC 5246) のサポートが要求されることになる；しかし、本 PP の次のバージョンには TLS 1.2 のサポート要件が含まれないが、SSL 2.0 または SSL 3.0 を用いたすべての接続試行を拒否する手段を TOE が提供することが要求されることは十分にあり得る。

依存性： FCS_COP.1 暗号操作

保証アクティビティ：

評価者は TSS 中のこのプロトコルの実装の記述をチェックして、オプションの特徴 (例えば、サポートされる拡張、サポートされるクライアント認証) が規定され、またサポートされる暗号スイートも規定されていることを保証しなければならない (shall)。評価者は TSS をチェックして、規定された暗号スイートがこのコンポーネントに列挙されたものと同一であることを保証しなければならない (shall)。評価者は TSS をチェックして、このプロトコルと関連付けられた FCS 要件中の暗号機能 (FCS_COP.1(1) など) が暗号機能の実行に用いられる方法が記述されていることを検証しなければならない (shall)。運用環境により提供される暗号機能については、評価者は以下のアクティビティを行わなければならない (shall)。

a. *運用環境を構成する代表的なプラットフォームのリスト (ハードウェア及びソフトウェア) が ST に含まれることを保証する。*

b. *TSS をチェックして、(ST 中に識別されるプラットフォームのそれぞれについて) この機能を呼び出すために TOE により使われるインタフェースが記述*

されていることを保証する。

c. *ST 中に識別されたプラットフォームのそれぞれについて、OE 文書をチェックして前のステップで識別することンタフェースが存在することを保証する。*

評価者は操作ガイダンスをチェックして、TLS がTSS 中の記述に適合するようにTOE を構成するための指示 (例えば、TOE により通知される暗号スイートのセットが、要件に合うよう制限されなければならない (have to) かもしれない) が含まれていることを保証しなければならない (shall)。

評価者は、要件に規定された暗号スイートのそれぞれを用いてTLS 接続を確立することにより、この機能をテストしなければならない (shall)。この接続は、より高位のプロトコルの確立の一部として確立されてもよい (例えば、HTTPS セションの一部として)。テストの意図を満たすには、暗号スイートのネゴシエーションが成功することを (通信路上で) 確認すれば十分であり、利用されている暗号スイート (例えば、暗号アルゴリズムが 128 ビットAES であって256 ビットAES でないこと) を識別するために暗号化されたトラフィックの特徴を検査する必要はない。

C.9 エントロピーの文書化と評定

エントロピー源の文書は、それを読んだ後の評価者が完全にエントロピー源を理解し、それがエントロピーを供給すると信頼できる理由を理解できるように、十分に詳細であるべきである (should)。本文書には、設計の記述、エントロピーの正当化、運用条件及びヘルステストという、複数の詳細な節が含まれるべきである (should)。本文書は、TSS の一部である必要はない。

設計の記述

文書には、すべてのエントロピー源コンポーネントの相互作用を含めた、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 (shall)。これにはエントロピー源の動作が記述され、どのように動作するのか、どのようにエントロピーが作り出されるのか、そしてどのように未処理 (生の) データをエントロピー源の内部からテスト目的で取り出すことができるのか、などが含まれることになる。本文書では、エントロピー源の設計の概略が説明され、ランダム性がどこから由来し、次にどこへ渡されるのか、任意の生の出力の後処理 (ハッシュ、XOR など)、保存されるのか (保存されるとすればどこに)、そして最後に、どのようにしてエントロピー源から出力されるのかが示されるべきである (should)。処理に課される条件があれば (例えば、ブロッキング)、それもエントロピー源の設計の中で記述されるべきである (should)。図や例の利用が推奨される。また、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説明と、境界外部の敵対者がエントロピー量に影響を

与えられないことがどのようにしてセキュリティ境界により確実とされるのかという説明が含まれなければならない (must)。

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、エントロピー源が確率的な挙動を示すことがなぜ確信できるのか (確率分布の説明と、その分布が特定のエントロピー源により得られるという正当化を行うことは、これを記述する方法のひとつである) という、技術的な議論が存在すべきである (should)。この議論には、期待されるエントロピー量の記述と、十分なエントロピーが TOE のランダム化シード供給プロセスへ与えられると確信できる理由の説明が含まれることになる。この議論は、エントロピー源がエントロピーを含むビットを作り出すと信頼できる理由の正当化の一部となる。

運用条件

また文書には、エントロピー源がランダムデータを生成すると期待される運用条件の範囲も含まれることになる。これには、これらの条件の下でエントロピー源が動作し続けることを保証するために、システムの設計に取り入れられた対策が明確に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故障または一貫しない動作となることがわかっている条件も記述されなければならない (shall)。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手法が、含まれなければならない (shall)。

ヘルステスト

さらに具体的に、すべてのエントロピー源ヘルステストとその根拠が文書化されることになる。これには、ヘルステストの記述、各ヘルステストが実行される頻度及び条件 (例えば、起動時、連続、またはオンデマンド)、各ヘルステストに期待される結果、そしてそれぞれのテストがエントロピー源の 1 つ以上の故障を検出するために適切であると信じられる理由を示す根拠が含まれることになる。

附属書D： 文書の表記

英国式つづりを米国式つづりに置き換えた以外には、本 PP に用いられる記法、様式、及び表記はコモンクライテリア (CC) のバージョン 3.1 と一貫している。PP の読者を助けるため、選択された表記法についての議論をここで行う。

D.1 操作

CC では、割付、詳細化、選択、及び繰返しという 4 つのコンポーネント操作を機能要件に対して行うことを許可している。本 PP では、これら 4 つの操作を以下のように明示する。

- **割付**：識別されたパラメタの規定を許可する。さらなる操作がセキュリティターゲット作成者により必要とされる場合、「割付：」というプロンプトを含む大括弧の内側の***太字かつイタリック体のテキスト***により示される。
- **詳細化**：詳細の追加を許可する。イタリック体のテキストにより示される。また詳細化を持つ SFR には、それが編集上の詳細化 (すなわち機能的詳細化のみがこのようにラベル付けされている) のみである場合を除いて、「*詳細化：*」が前に置かれる。
- **選択**：リストから 1 つ以上のエレメントの規定を許可する。「選択：」というプロンプトを含む大括弧の内側の<u>下線付きテキスト</u>により示される。
- **繰返し**：様々な操作と共に二回以上コンポーネントが用いられることを許可する。繰り返される SFR のエレメント番号に引き続く括弧の中の連番により示される。

CC パート 2 から取り込まれた要件であって PP に適用するために選択及び割付が既に記入されている場合、「選択：」及び「割付：」プロンプトが存在しないことを除き、表記は通常の操作と同一である。

D.2 拡張要件の表記

拡張要件は、作成者のニーズを満たす適切な要件を CC が提供していない場合に許可される。拡張要件は識別されなければならず (must)、またその要件を関連付けるにあたって CC のクラス／ファミリ／コンポーネントモデルを利用することが要求される。CC パート 2 クラスまたはファミリに基づく拡張要件は、コンポーネント中に「EXT」を挿入することにより示される。エンタープライズセキュリティ管理機能に関して特に定義された拡張要件は、「ESM」クラス名により示される。

D.3 適用上の注意

適用上の注意には、適合 TOE のセキュリティターゲットの構築に関連する、または役立つと考えられる追加のサポート情報に加えて、開発者、評価者、及び ISSE の方への一般的な情報が含まれる。適用上の注意には、コンポーネントの許可された操作に関するアドバイスも含んでいる。

D.4 保証アクティビティ

保証アクティビティは、脅威を低減するため TOE に課された機能要件の共通評価方法としての役割を果たす。このアクティビティには、TSS に文書化された TOE の特定の側面を評価者が分析するための指示が含まれているため、ST 作成者にはこの情報を TSS 節へ取り込むという暗黙の要求が課されている。PP の本バージョンにおいては、これらのアクティビティは、機能と保証コンポーネントに直接関連付けられているが、将来のバージョンでは、これらの要件を別々の附属書または文書へ移すかもしれない。

附属書E： 用語集

表 16. 用語と定義

用語	定義
アクセス制御製品 (Access Control Product)	エンタープライズセキュリティ管理製品であって、定義されたアクセス制御ポリシーの実施を担当するもの。
割付管理者 (Assignment Manager)	TSF を用いてサブジェクトの識別情報とクレデンシャル情報データの定義と維持を行う権限を持つ個人。
クレデンシャル情報 (Credential)	識別情報と関連付けられた 1 件以上の情報の集合であって、アイデンティティの主張に用いることができるもの。
エンドユーザ (End User)	権限を明確にし、アカウント情報により活動を明確に記録するため、ESM システムにより管理される個人。
登録 (Enrollment)	ESM システムでの新たな利用者を定義する行為。
エンタープライズセキュリティ管理 (Enterprise Security Management)	セキュリティ管理策を指示、作成、配備、改変、一時停止、終了するために必要なシステムと要員。
フェデレーション (Fedefation)	あるドメインで認証されたサブジェクトが他のドメインでも同様に有効であることを相互に保証する複数のドメイン。
識別情報 (Identity)	個人に割り当てられる一意の識別子であって、利用者のライフサイクルの期間、固定であり続けるもの。
管理リポジトリ (Managed Repository)	識別情報とクレデンシャル情報属性データが保存するためのデータストア。管理リポジトリは TSF の一部である必要はないが、TSF がその内容の変更を許可された唯一のサブジェクトであるべきである (should)。
人間以外のエンティティ (Non-Person Entity)	ハードウェアやソフトウェア等の人間の利用者以外の、組織の運用環境で何らかの機能を果たす、識別されたサブジェクト。
運用環境 (Operational Environment)	TOE 境界の外の、エンタープライズにおけるハードウェア及びソフトウェア資源の集合。TOE の動作に必要なサードパーティのソフトウェア部品、TOE が保護する資源、及び TOE をインストールするハードウェアが含まれるかもしれないが、これらに限定されない。
ポリシー管理者 (Policy Administrator)	ESM のアクセス制御ポリシーを定義するためにポリシー管理製品を使用する個人。
ポリシー管理製品 (Policy Management Product)	アクセス制御製品が実行するための、アクセス制御ポリシーの定義と送信の責任を負う、エンタープライズセキュリティ管理製品。
利用者 (User)	エンドユーザを参照すること。

附属書F： 識別情報

タイトル：エンタープライズセキュリティ管理識別情報とクレデンシャル情報管理のプロテクションプロファイル

作成者：ESM プロテクションプロファイル技術コミュニティ

コモンクライテリア識別情報: 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、バージョン 3.1、2012 年 9 月

バージョン：PP バージョン 2.1

キーワード：エンタープライズセキュリティ、エンタープライズセキュリティ管理、識別情報管理、クレデンシャル情報管理、利用者の登録、ミッション管理、属性管理

評価保証レベル (EAL)：EAL 1 追加