エンタープライズセキュリティ管理とアクセス制御の標準プロテクションプロファイル

原文タイトル：

Standard Protection Profile for Enterprise Security Management Access Control

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。

http://www.niap-ccevs.org/pp/pp_esm_ac_v2.pdf

2012 年 2 月 22 日

バージョン 2.0

平成 24 年 9 月 18 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	備考
1.0	2011 年 10 月 21 日	ESM テクニカルコミュニティからの最初の完全なバージョン
1.x	2011 年 11 月～2012 年 2 月	CCEVS の懸念に対処し、かつその他の CCEVS PP と標準化するための更新。
2.0	2012 年 2 月 22 日	最初の公表バージョン

目次

図一覧

表一覧

1 プロテクションプロファイル（PP）序論

1.1 序論

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登録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含んでいる。識別情報は、PP を識別し、カタログし、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。

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。ESM の機能には 2 つのタイプがある。最初のタイプ、*ポリシー定義*、は一連の IT 資産のふるまいを管理するために使用される中心的な組織のポリシーを定義するために使用されている。第 2 のタイプ、*ポリシー利用*、は定義されたポリシーを使い、それを実施する。これらの 2 つのタイプの 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において表わされる。

現行の 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：

- **アクセス制御方針**：定義されたオブジェクト（IT 資産又は資源）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認可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情報、認証、権限付与及び説明責任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**： オブジェクトの権限付与のために使用される属性を定義し維持するポリシー。

---

1 注：技術的な意味では、「製品」という用語は正確ではないが、（「システム」のような）その他の用語は同様に不十分で、荷が重すぎる。ESM「システム」内の様々な「製品」は別個の製品かもしれない。又は、それらは、単に ST に記載される、より大型の製品内部の半製品又は機能かもしれない。「製品」という用語の使用は、*システム*（それらは特定の任務に対して設計された製品の統合された集積である）とは対照的なものとして、単に、セキュリティターゲットが*製品*を説明するというだけの理由である。したがって、PP は通常特定のベンダーの実装から独立した方法で製品（又は製品のコンポーネント）について説明する。

2 注：ESM の使用では、全体的な企業（エンタープライズ）が組織の境界を超えるという事実を反映して、「組織」の代わりに、「企業（エンタープライズ）」という用語がよく使用される。

- **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。
- **セキュアな構成ポリシー**: 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た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**: 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**: 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当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**: 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 PP スイートは、以下のように特徴づけられることもある 6 つのプロテクションプロファイルから構成される:

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	アクセス制御方針	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	セキュアな構成ポリシー	監査ポリシー
ESM アクセス制御プロテクションプロファイル	C/E	C	C	C(3)	C	C(1)
ESM ポリシー管理プロテクションプロファイル	D	C	D/C(2)	C(3)	C	C(1)/D
ESM 識別情報とクレデンシャル情報管理	C	D	C/D(2)	D/C(3)	C	C(1)
ESM 認証サーバ	C	C/E		C/E	C	C(1)
ESM 監査管理		C		C(3)	C	C(1)/E
ESM セキュアな構成管理				C(3)	D/C/E	C(1)
C=使う;D=定義する;E=実行する						
注: (1) TOE がどんな事象を監査するか決めるとともに、監査ポリシーは利用される。 (2) オブジェクト属性は、識別情報及びクレデンシャル情報管理 PP、又はポリシー管理 PP のいずれかで定義されるが、そ						

の両方で定義されるわけではない。
(3) 認証ポリシーは、許可された利用者が TOE に認証しなければならないという意味で使われる。

1.3 ESM アクセス制御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**アクセス制御の判断及び実施**に焦点を置く。本プロテクションプロファイルに適合する製品/製品コンポーネント[3]は、中心に定義されたアクセス制御方針を使い、それを実施する。そうする際に、それは一貫した方法でエンタープライズに予防的セキュリティを提供する。本プロテクションプロファイルに適合する製品は、(ワークステーション上のファイルシステムオブジェクト又は組織のイントラネット上のウェブサイトのような)あるタイプの定義された資源に対する要求を傍受し、要求が許可されるべきかどうか判断することが期待されている。ESM 環境では、この機能は*ポリシー決定ポイント*、又は *PDP* と呼ばれる。その後、それは、この判断の結果を実施するか、又は実施自体を行う信頼されるエンティティに決定を送る。ESM 環境では、この第 2 の機能は*ポリシー実施ポイント*、又は *PEP* と呼ばれる。本文書に定義されたプロファイルに適合する製品は、ポリシー決定及びポリシー実施の両方を提供する。いくつかの ESM 製品は、単にポリシー決定を提供し、運用環境への実施を延期するのみである; そのような場合には、本プロファイルに対してそのような製品を評価する唯一の方法は、運用環境実施コンポーネントが TOE コンポーネントとして再分類されるように、TOE の境界を引くことである。

運用システムで一般に見られるアクセス制御と ESM アクセス制御がどのように異なるか理解することが重要である:

- **ESM アクセス制御は中心に規定される**: ESM アクセス制御が*中心に定義されたポリシー*を実施する一方で、運用システムは*ローカルに定義されたポリシー*(つまりローカルに、及び、その運用システムに固有のポリシー)を実行する。中心的なアクセス制御方針を定義し、所定の一連の利用者及び/又は IT 資産に組織全体にわたってそれを一様に適用させる能力は、組織のセキュリティ方針の一貫した適用を可能にする。

3 以後、単に「製品」と表す。

- **ESM アクセス制御は組織的に定義されたオブジェクト上で作動する**: ESM アクセス制御方針は、しばしば運用システムとは異なる粒状度のオブジェクト上で作動する。運用システムは、ファイル及び IPC インタフェースのような基本的なオブジェクトに焦点を置くが、ESM 製品は、基本的なオブジェクトの組合せ（例えば、複数のファイルの組合せかもしれない「命令」）として実装されることもある、上位の抽象的概念上で操作する能力を持っている。したがって、ESM 製品は、ウェブトランザクションを媒介するか又はメール・ゲートウェイでデータの流出を防ぐ機能を提供する。運用システム上のエージェントとして機能する ESM アクセス制御製品は、信頼されたベンダーによって創造されるアプリケーションをホワイトリストに載せるような、本来の OS の機能への補足的な役割を実行するために配置される。（そして、更に重要なのは、それは中心に定義されたポリシーを実施することができる。）

- **ESM アクセス制御は組織の識別情報に基づいている**: 運用システム固有の利用者・ベースと対照的に、ESM アクセス制御の製品は集中化された識別データを使用して作動する。これは、アクセス制御が、レガシー利用者及びグループ特性によって分類されることを強制するポリシーに代わって、組織が重要と認める、組織の属性及び関係を使用して設定されることを可能にする。

上に注記されるように、アクセス制御コンポーネントは、ESM コンポーネントの全体的なパッケージプログラムの一部である。アクセス制御コンポーネントは、他の ESM コンポーネントによって提供される次の能力を利用する:

- **集中化されたポリシー定義**: 個別のポリシー管理能力は、アクセス制御製品のポリシー決定の指標となる一連の規則を定義すると期待されている。これらの規則は、関心のある活動、及びこれらの活動が検知される場合、製品はどのように対応すべきかを定義するサブジェクト － オブジェクト － 操作の組合せを含むだろう。サブジェクトとオブジェクトは、（利用者の利用者名、その地理的位置、保護された資源の URL 及び時刻のような）組織的に優位な属性によって定義される。

- **集中化されたサブジェクトの定義**: 個別の識別情報とクレデンシャル情報管理能力は、利用者の中心的な定義を提供し、利用者と、組織がセキュリティ関連とみなす属性を持つプログラム及びワークステーションのような非人格エンティティ（NPE）を恐らく関連させると期待されている。アクセス制御製品は、どのように要求を処理すべきかを決定するために、あるアクションを実行するサブジェクトのセキュリティ属性を検査する。

- **オブジェクトの定義**: ほとんどの場合、アクセス制御製品によって検査されたオブジェクトの属性は、運用環境におけるオブジェクトの定義の本質的な部分であろうと期待されている。例えば、ウェブアクセス管理者は、アクセスが適切かどうか判断するためにウェブページの URL、又はそれがアクセスされた時刻を検査 する。しかしながら、ある状況においては、望ましい方法でアクセスを管理するために、個別の属性管理能力が必要なこともある。例えば、強制アクセス制御(MAC)を使用することができるように、運用システムは第三者製品を機密保護ラベルでそのオブジェクトと関連させることもある。

- **サブジェクト識別情報の集中化された保証**: 個別の認証サーバ製品は、それらの要求された識別情報が有効であることを決定するため、サブジェクトを認証すると期待されている。アクセス制御製品によって検査されたアクションは、認証されたサブジェクトによって起動される。

- **集中化された監査に対する支援**: 個別の監査管理能力は、集中化された報告及びインシデント処理のため監査データを収集すると期待されている。アクセス制御製品は、サブジェクト説明責任を実施することができるように、この能力に関係しているか、この能力によって問い合わすことができる位置にその監査データを書き込むことができなければならない。

- **構成管理に対する支援**: 組織のセキュリティ方針と一致する方法で作動することを保証するために、個別のセキュアな構成管理がアクセス制御製品の設定を検査すると期待されている。これには、それが完全にパッチされているか、最新のポリシーを使用しているか、又は、その設定が適切であることを保証するような、製品の設定の様々な面を含んでいることもある。

図 1 は、これらの依存性がアクセス制御製品に関連してどのように配置してよいかの視覚的なアウトラインを提供する。これらの依存性は、個別の製品によって、又は複雑な製品の追加的側面として満たされることもある。ESM 製品が複数の能力を提供する場合、満たすことができる ESM プロテクションプロファイルのすべてについて評価されなければならない。

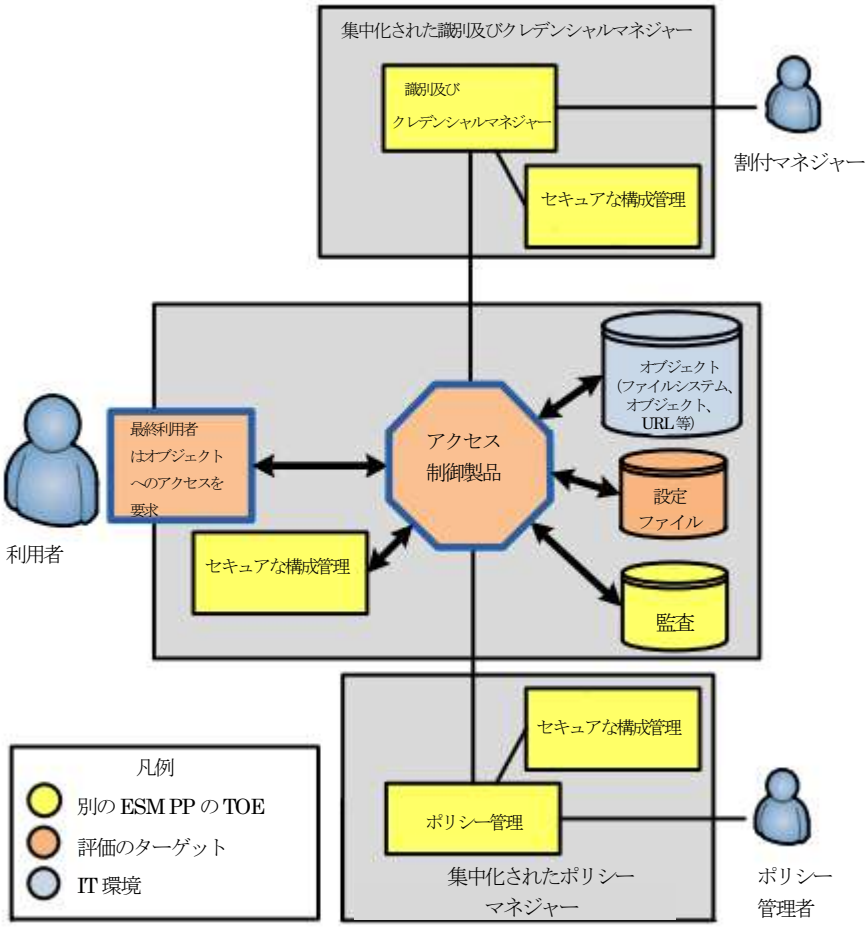

図 1 プロテクションプロファイルの関係

1.4 適合評価対象

アクセス制御製品の目的は信頼されたポリシーを使うことである。これらのポリシーは、運用環境においてどのオブジェクトが保護されるべきか、どのサブジェクトがこれらのオブジェクトへのアクセスを与えられているか、及びどのような一連の操作をこのアクセスは包含することを許されているかを判断する。PP は何らかの特定のタイプのアクセス制御を規定することはない;それらが望ましいアクセス制御メカニズムを実施することができる場合、強制アクセス制御(MAC)、任意アクセス制御(DAC)、役割ベースのアクセス制御(RBAC)、属性ベースのアクセス制御(ABAC)又はその他のポリシーを配置することができる。

本 PP に適合する TOE は、多様な資源のいずれかへのアクセスを制御していることもある。保護されるオブジェクト、及びポリシーに基づいて、アクセスがどのように許可され又は拒否されるかを判断するために使用される属性を明瞭に示すことは、セキュリティターゲット(ST)執筆者の責任である。

TOE は、ハードウェア又はソフトウェア、冗長性を持つ分散型システム、クライアントエンドポイントの集合の 1 つ、又はサーバもしくはネットワーク境界デバイス上に存在する単一のエージェントとして配置する。運用環境の目標

は、厳格なコンプライアンスの性質により、TOE によって適合されるよう表示してはならないということに留意すべきである。運用環境の目標が ESM アクセス制御製品によって達成されることもある共通の場合については、本プロファイルの将来のバージョンにおけるオプションの SFR としてそれらの SFR を追加するため、開発者は CCEVS を用いて作業しなければならない。

1.5 一般的な機能

本プロテクションプロファイルは、ESM のセッティングでアクセス制御を実行することができるすべての製品によって、満たされるべき一連の要件を定義する。アクセスが制御することができるオブジェクトが広汎なため、TOE セキュリティ方針（TSP）によって保護することができる最小限のオブジェクトのセットを考え出すことは不可能である。しかしながら、このことは、セキュリティ機能の最低限度を表示することにより、本プロテクションプロファイルへの適合性を表示する TSP の課題を提起する。本節の意図は、アクセス制御技術のタイプの概要を提供し、その技術に係る TSP の下で定義可能な最小限のオブジェクト及び運用のベースラインを規定することである。

本プロテクションプロファイルに準拠するセキュリティターゲットを記述する場合、ST 執筆者は TOE に適用される技術のタイプを明瞭に識別しなければならない。TOE が何らかの該当するタイプに係るベースラインを十分に適合することを示すために、それらは利用者・データプロテクションの要件に適切な対応する情報を含まなければならない。技術タイプがより明瞭に示されるようになるとともに、プロテクションプロファイルの本節が、より多様なアクセス制御ソリューションを適合するために改良されるであろうと期待されていることに留意すること。

技術タイプにかかわらず、ESM プロテクションプロファイルへの適合性を表示する製品が、**組織的に定義される**サブジェクトと属性を取扱うことは必須である。言いかえれば、TOE は、可能な場合は常に、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。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 執筆者は、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 アサーション又は 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。その他の ESM コンポーネントは、これらの組織の属性を維持する責任を負うだろうと期待されている。

1.5.1 ホストアクセス制御

標準的な運用システム及びアプリケーションは、ローカルの運用システム及びアプリケーションのネイティブな資源にアクセス制御を提供するよう設計されている。しかしながら、1 つ又はそれ以上のネイティブな運用システム又はアプリケーション資源から構成される、より高次レベルの組織の抽象的概念によって実施されることをアクセス制御に要求する、多くの潜在的な能力がある。ホストアクセス制御の ESM 製品は、これらの組織の抽象的概念によってアクセス制御を実施するよう設計されている。ESM ホストアクセス制御製品が、組織の要求を取扱うのに十分な汎用性があるためには、最小限、次のオブジェクト及び操作が必要とされる:

- ファイルに対する操作の読取、書込、修正、削除、実行
- 実行可能なプロセスに対する操作の読取、書込、修正、削除、実行
- システム構成パラメタに対する挿入、修正の操作
- TOE を要素とするシステムに対する終了、再起動の操作

これらのオブジェクトは、ポリシー内で任意に定義可能であると期待されていることに留意すること。ポリシーはネイティブ・オブジェクトを直接制御することができることもあり、又はオブジェクトの集合である抽象的概念を扱うこともある。単一の静的に定義された実行可能ファイル（例えば Windows Solitaire へのアクセスを制限するためだけに存在する製品）にアクセス制御を提供する製品は、評価について検討されるべき十分な組織の価値を提供しない。

ホストアクセス制御 TOE は、運用環境（例えば運用システムルートアカウント）においてシステム管理者の許可を制限するのに使用されることもある。例えば、下図 2 において、Linux"ルート"アカウント利用者は、ローカルの運用システムへの構成設定に変更を加えようとしている。変更の実施が許可される前に、TOE は利用者がローカル運用システムの構成に変更を加える、適切な権限を持っていることを保証する。TOE によって実施されるポリシーが、当該利用者が運用システムに提案された変更を加えることを許可しない場合、TOE は変更が行なわれることを防ぎ、事象を監査する。

さらに、ホストアクセス制御 TOE は、運用が始められた日時に基づき、ポリシーを随意に実施する。

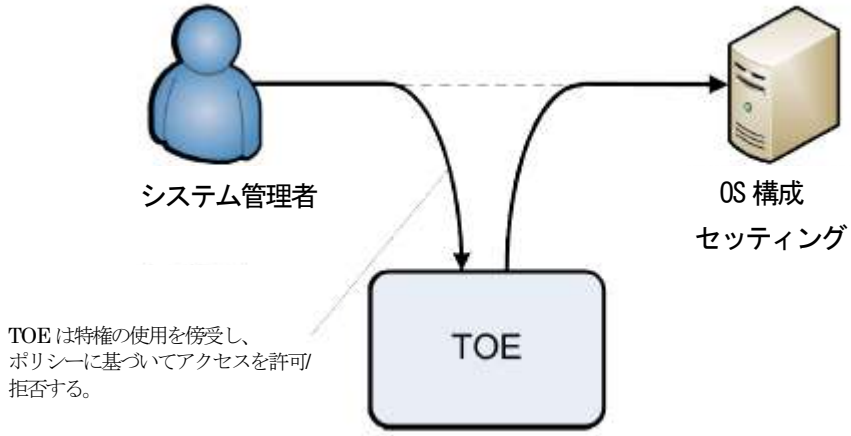

図 2　管理者アクセスの中の TOE の仲介

上記の図 2 に示されるような TOE の使用は、その環境におけるスーパー利用者に対して制限を課すことにより、職務の分離を実施するのに役立つことがある。

1.5.2 ウェブアクセス制御

ウェブアクセス制御 TOE は、ウェブベースの内容と双方向通信するためのサブジェクトの要求を検査し、これらの要求が許可されるか又は拒否されるかを判断するポリシーを実施するアプリケーションである。それは、通常、サブジェクトの要求が経由する中央サーバ上に存在する。ESM ウェブアクセス制御製品が、組織の要求を取扱うのに十分な汎用性があるためには、最小限、次のオブジェクト及び運用が必要とされる:

- ウェブオブジェクトに対する HTTP GET、HEAD、POST 操作
- ウェブオブジェクトに埋め込まれているスクリプトに対する操作を実行する。

これらのオブジェクトは、ポリシー内で便宜的に定義可能であると期待されていることに留意すること。単一の静的に定義された HTTP オブジェクト（例えば単一の静的な URL）にアクセス制御を提供する製品は、評価について検討されるべき十分な組織の価値を提供しない。さらに、ウェブアクセス制御 TOE は、運用が始められた日と時刻に基づき、ポリシーを随意に実施する。

1.5.3 データ喪失防止

データ喪失防止デバイスの主要な目的は、不正な漏洩のリスクを削減しつつ、組織内の機密情報の存在を識別し、そのアクセスとリリースの権利を実施することである。今日のデータ喪失防止（DLP）ソリューションは、一般的にネットワーク、エンドポイント及びエンタープライズディスカバリープロテクションを提供する。データ喪失防止デバイスとの重要な区別は、コンテナ自体へのアクセスと対照的に、コンテナ内の情報（コンテンツ）に焦点が置かれている

ということである。データ喪失防止デバイスのよい例は、クロスドメインガード内に共通して見られる「ダーティワードチェッカー」であろう。

ネットワークベースの DLP ソリューションは、ファイアウォールと同様の方法でネットワーク内に位置する。ネットワーク DLP ソリューションは、データの流出を検知し、修復する、通常、ハードウェア、ソフトウェアのみ、又はバーチャル・マシン・アプライアンスである。代表的な例には電子メール、ウェブトラフィック及びファイル交換を含む。ネットワークコンテンツ-認識 DLP ソリューションは、インラインか、ルーター又はネットワーク・スイッチ上のスパンポートへ付けられたものとして、配置することができる。

エンドポイント DLP ソリューションは、利用者のコンピュータ又はネットワーク・サーバ上に保管され運用される機密情報を識別し、監査し、修復するための OS 内に、ローカルに作動するホストエージェントである。エンドポイント DLP ソリューションは、しばしば、カット/ペースト、印刷、ファイル操作(コピー、保存、削除、開く)、CD/DVD への焼き付け及び USB デバイス制御のような能力による情報のアクセス及びリリースを制御する。

エンタープライズディスカバリーDLP ソリューションは、データベース、ストレージエリアネットワーク(SAN)/ネットワーク接続ストレージ(NAS)、シェアポイント、文書管理システムそしてさらに発見するべきデスクトップエンドポイントなどのようなデータストア、カタログ、及び機密データを含む修復データオブジェクトをクロールする能力を提供する。これは、通常アプライアンス(ハードウェア又はバーチャルマシン)、又は資源自体にインストールされたエージェントベースのソフトウェアとして可能になる。エンタープライズディスカバリーDLP ソリューションは、ポリシーの実施とは対照的に、設定を見つけることにより焦点を置いているので、セキュアな構成管理 ESM PP によってカバーされている。

TOE は、IT 以外の方法による漏洩、計画的な混乱又は秘密チャネルからは保護しない。

ESM データ喪失防止製品が、組織の要求を取扱うのに十分な汎用性があるためには、最小限、次のオブジェクト及び運用が必要とされる:

- 印刷スプールに対する書込み操作
- リムーバブルデバイスに対する読書き操作
- アプリケーション内の、及びアプリケーション間のコピーとペーストの操作

- メールサービスに対する送信操作
- ウェブコンテンツに対する HTTP POST 操作

さらに、データ喪失防止 TOE によって使われるポリシーは、データ喪失から保護されるべきデータのタイプを定義し、識別し、カタログすることができなければならない。これらの属性は、ポリシー内で任意的に定義可能であると期待されていることに留意すること。静的重要度に基づきあるセキュリティドメインに属すると定義されるデータの喪失を防ぐ製品は、同じ重要度定義を使用しない組織にとって無益である。

最後に、データ喪失防止 TOE はまた、TSS に定義されたレベルに、それらが非表示フィールドとメタデータにあるものを含む機密情報を含むかどうか判断するために、データベース、PDF 及びワード文書のようなデータファイルを点検することができなければならない。更に、DLP TOE は、また直接点検することができないコンテンツに対して、パタン、署名又はハッシュに基づいたデータオブジェクトを識別すべきである（should）。最後に、DLP ソリューションは、暗号化されたオブジェクトの存在を識別し、それらが暗号化されるかどうかに基づき、それらの送信を許可するか、拒否すべきである。これは、機密データを含む文書又はリポジトリを信頼されない論理ドライブに送信することはできず、ウェブ形式に掲示することはできず、あるいは、電子メールの添付ファイルとして送信することができないことを保証することにより、データ漏洩に対する追加的なプロテクションを提供する。

このタイプのアクセス制御の意図は、悪意のある内部的な「漏洩」に対する包括的な防衛手段を完全に独力で提供することではないことに注意すること。その脅威の緩和が望ましい場合、固く決心した敵を阻止するために、十分に強力な物理的セキュリティ、人的セキュリティ及びネットワーク境界フロー制御デバイスも使用する必要がある。

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）製品に対する書面による一連のプロテクションプロファイルの 1 つである。次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 ポリシー管理の標準プロテクションプロファイル
- ESM 識別情報及び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
- ESM 監査管理の標準プロテクションプロファイル
- ESM セキュアな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性を表示する製品は、他のプロテクションプロファイルに適合する互換性を持つ環境の製品を識別しなければならない（must）。TOE が複数のプロテクションプロファイルと互換性をもつ機能を実行する場合、すべての該当するプロテクションプロファイルへの適合性が表示されなければならない。

1.7 文書の構成

第 1 章は、プロテクションプロファイルの序論的な資料を提供する。

第 2 章は、プロテクションプロファイルに該当する適合主張について述べる。

第 3 章は、TOE に対して生じる可能性のある 脅威のタイプを定義する。

第 4 章は、TOE が果たすと期待される目標を定義し、これらの目標へのコンプライアンスを説明するセキュリティ機能要件をリストする。

第 5 章は、本プロテクションプロファイルにおいて使用される拡張コンポーネントを定義する。

第 6 章は、TOE がプロテクションプロファイルと適合性があるために表示されなければならないセキュリティ機能要件及びセキュリティ保証要件を列挙し説明する。

第 7 章は、プロテクションプロファイルにおいて定義される想定、脅威、目標及び要件の間のマッピングを提供する。

第 8 章は、プロテクションプロファイルに適用される想定、脅威及び目標を定義する。

文書はまた次の附属書を含んでいる：

- 附属書 A－この附属書は、参考文献のリストを提供し、本文書において使用されている頭字語を定義する。
- 附属書 B－TOE の証明と認可の活動への適用可能性を迅速に確認することができるように、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－PP 適合製品が示すかもしれない潜在的なアーキテクチャ上の変動を定義し、別の技術タイプに係る利用者・データプロテクションの要件をリストする。また、それは承認されたオプションの要件を提供する。
- 附属書 D－文書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*、CCMB-2009-07-004、バージョン 3.1 改訂 2009 年 7 月 3 日に適合している。

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 適合である。

2.2 PP 適合主張

本プロテクションプロファイルは、他のどんなプロテクションプロファイルへの適合性も表示しない。

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、増強された EAL1 のパッケージを表示する。

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性を表示するセキュリティターゲットは、CC パート 1 の D.2 節で定義されるような厳密な適合性の最小限の標準を満たさなければならない（shall）。

厳密な PP の適合性とは、PP の中の要件が満たされ、ST が PP のインスタンス化であることを意味する。ST は PP より広範囲になりえる 。ST は、TOE が少なくとも PP と同じことを遂行し、その一方で運用環境はよくても PP と同じであることを明記する。本 PP では、明記された要件の意図及びベンダーがどのように要件に適合するかに関する期待をさらに明確にし説明するために、適用上の注意が提供されている。ST の評価者は、ST 及びその記述された TOE が本PP 内のすべての説明（及び恐らくより多く）を含むだけでなく、適用上の注意によって説明される期待値にも適合したと判断することにより、厳密な PP のコンプライアンスを保証するであろうと期待されている。

保証に関しては、ST が PP 内にあるものと少なくとも等しいか、より強力な保証要件を含み、PP 内で説明されたすべての保証活動が実行されることが期待されている。

3 脅威

次の節は、TOE 又は運用環境に悪影響を及ぼすために用いられる可能性のある脅威をリストする。

3.1 環境資源への不正なアクセス

TOE を配置する主要な目的は、運用環境に存在するオブジェクトに対してアクセス制御を実施することである。それは、オブジェクトに対する操作を実行するというサブジェクトの要求を傍受し、かつ定義されたアクセス制御方針が、要求が生じるのを許可するべきかどうか判断するメカニズムを提供することにより遂行される。これらの活動が覆されるか回避される場合、又は TOE が期待されるレベルの粒状度へのアクセスを制御することができない場合には、運用環境のすべて又は一部は、あたかも TOE が存在しないかのように機能する。この状況は、適切な権限なくアクセスされているオブジェクトを考慮に入れている。

[T.UNAUTH]

3.2 TOE の無力化

オブジェクトに対するアクセス制御を実施するために、TOE は、それが要求を傍受することを可能にする論理的な位置に存在しなければならない（must）。アクセスが制御されている資源のタイプは、TOE に対し、これらの資源にローカルに存在するよう要求する。

TOE がエンドポイントシステムに位置する場合、TOE が無力化される脅威が増大する。これは、エンドポイントシステムが制御されたアクセス環境に永久に留まる可能性はより低いという事実による。物理的なアクセス制御の保証が減少する時、システムにアクセスを試みる攻撃者のリスクは増加する。

TOE が終了することができるプロセスとして実行する場合、又は、そのファイルが運用システムの起動シーケンスから移動されるか、変更されるか、除去されることができる場合、利用者は、アクセス制御の実施を回避する能力を持つだろう。

[T.DISABLE]

3.3 ポリシーデータアクセスの不連続

TOE が他の ESM コンポーネントから遠く離れて位置する場合、リスクが存在することもある。TOE と遠隔資源の間の結合が中断される場合、TOE はそのセキュリティ機能を適切に実施することができないかもしれない（may not）。さらに悪いことには、不連続の脅威は、サービスの拒否によって、又は単にケーブルのプラグを抜くことによって現実になりうる。またそれは、不注意にかつ TOE 自体の運用から遠くに隔たった個人によって、大変容易に実行することができる。このため、TOE は、事実上避けられないサービス停止が起きた場合に、運用の継続性を維持する何らかの方法を持たなければならない（must）。

[T.NOROUTE]

3.4 ポリシーと ESM データの漏洩

運用環境は、データが機能するために遠隔装置間で送信されることを、ほぼ間違いなく必要とする。TOE は、離れたソースから実施すべきポリシーを受信することもある。それは、利用者属性又はセッション・データを環境のどこか他のところから受信する、そして、離れた位置にある集中型のリポジトリに監査データを書き込むだろう。このデータが移送中に、十分にセキュアな信頼されたチャンネルによって保護されない場合、それには強制的な漏洩が起こりやすいこともある。このデータへのアクセスを持つ攻撃者は、それを偵察のために、又は正当な利用者もしくはエンティティを装うことを試みる際に既知の有効情報をリプレイするために使うことができる。

[T.EAVES]

3.5 偽りの実施保証

ポリシー管理製品は、TOE が実施に責任を負うポリシーを分散するために、TOE と通信しなければならない（must）。ポリシーが受信されており実施されることを保証するために、TOE は、ポリシー管理製品にポリシーの受信と利用の何らかの証拠を提供すべきである（should）。しかしながら、この受領のフォーマットが十分に包括的か、又は通信チャンネルが漏洩に対して十分に保護されない場合、攻撃者は、ポリシーの分散を傍受し、ポリシー管理製品に偽りの受領を報告することもある。この結果は、TOE が正しいポリシーを実施せず、及び、管理者側の視点から何も誤ったように見えないということであり、また、セキュリティ違反を検知することがより困難になる可能性がある。

[T.FALSIFY]

3.6 偽りの更新

TOE が最新のポリシー情報であるように見えるものを受信する場合、TOE はポリシーの真正性及び送信元の識別情報について何らかの保証を持たなければならない（must）。通信チャンネルが十分に保護されていないか、TOE がポリシーのソースの識別情報を確認するメカニズムが、十分に確固としていない場合、ポリシーを送信するのに使用されたシンタックスを認識している攻撃者は、任意に偽のシンタックスを偽造し、TOE にそれを使わせることができるかもしれない。これが起きる場合、TOE は不正アクセスを許可する任意の偽のポリシーを実施するか、正当な活動が実行されるのを妨げる限定的な偽のポリシーを実施するか、あるいは不正確にフォーマットされたポリシーを使うように設定されるかもしれない。

[T.FORGE]

3.7 潜在的アクション

ある組織内部に ESM ソリューションを実装する理由の一部は、透明度と説明責任を提供するためである。このために、TOE がそのアクセス制御方針の実施を監視し監査する能力を提供すると期待されている。攻撃者が以前に議論された攻撃ベクタを搾取することにより、監査データを混乱させることができる場合（TOE の監査能力を再設定するためにセキュアな構成管理を装う、データを転用するか書き直すために任意の遠隔の監査リポジトリへの信頼さ

れたチャンネルを危険にさらす、監査の責任を負うTOEの一部を無能力にする、ローカルの監査ログを削除するか修正する)、その後、彼らは、見つかるリスクが減少することで、ポリシーの弱点についてシステムを探査し始めることができる。同様に、TOE がそれ自体に対して講じられた変則的な又は悪意のあるアクションを識別せず、監査しない場合、そのふるまいが検知されないで変更される可能性が存在する。万一これが発生するとしたら、そのアクセス制御の実施が適切に機能していたという保証はない。

[T.MASK]

3.8 無効なポリシーの受諾

TOE は、潜在的にいろいろのソースからのインプットを受諾する責任を負う。攻撃者がポリシーデータをリプレイするか、移送中の正当なポリシーデータを修正することができる場合、TSF は正しくないポリシーを実施していることもある。これは攻撃者に権限のないデータへアクセスする機会をもたらす。

[T.OFLOWS]

4 セキュリティ対策方針

4.1 データ保護

アクセス制御 TOE の目的は、TOE が配置されなければ許可されない操作の実行を防ぐことである。この結果は、資産の保護、又はそれらが適切な方法で運用されていることの保証である。この結果を達成するために、TOE は、ポリシーに従ってアクセスが求められているオブジェクトの重要度に対して、アクセスを求めるエンティティの許可の比較(エンティティの運用環境の属性を含む)に基づいてアクセスを制御すべきである。このポリシーデータは、互換性をもつポリシー管理製品によって TOE に分散され、TOE のセキュリティ態勢を監視し、設定することができるように、互換性を持つセキュアな構成管理製品によって問い合わせすることができる。

(O.DATAPROT:FDP_ACC.1、FDP_ACF.1、FMT_MOF.1、FMT_MOF.1、FMT_MSA.1、FMT_MSA.3、FMT_SMF.1、FMT_SMR.1(2)(1);ESM_DSC.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);FTA_TSE.1(オプション))

4.2 無効なポリシーの拒否

TOE は、それが受信するあらゆるポリシーデータの完全性を確認し、あらゆる無効の又はリプレイされたデータも拒絶することができなければならない(must)。TOE が無効データを受理することができるとしたら、それは正しくないポリシーの実装を引き起こす可能性がある 。また、それは不正確にフォーマットされたポリシーの受理により、バッファオーバーフローを引き起こす可能性もある 。

(O.OFLOWS:FPT_RPL.1、FTP_ITC.1(2))

4.3 保証された完全性

TOE はポリシー、識別情報、クレデンシャル情報、属性、及び他の ESM 能力から得られたその他のセキュリティ情報の、ローカルに保有されたコピーの完全性を保護するために、停止中のローカルのデータを保護するための、十分に強力で信頼されるメカニズムを使用しなければならない(must)。万一そうすることに失敗したら、TOE を多くのレベルでのセキュリティ侵害又は効果がないポリシー管理にさらす恐れがある 。

(O.INTEGRITY:FTP_ITC.1(2)、FCS_CKM.1.1、FCS_CKM_EXT.4、FCS_COP.1、FCS_COP.1、FCS_COP.1(3)、FCS_COP.1(4)、FCS_RBG_EXT.1(オプション)(オプション)(オプション)(2)(オプション)(1)(オプション)(オプション)(オプション))

4.4 自己防衛

1.4.1 節で議論されたように、ホストベースのアクセス制御 TOE は運用システム上にあるオブジェクトへのアクセスを制御するために配置されることもある。この場合、操作上の任務を達成するためには、その運用システムの利用者がその能力の完全なスイートへのアクセスを要求しないという暗黙の想定がある。したがって、TOE の行動に影響を与えるオブジェクトを保護するよう TSF に要求することは、論理上一貫している。利用者は、彼らの指定された役割を達成するのに必要な運用システムの特徴に対してのみアクセスを与えられるべきであり（should）、彼ら自身の許可を変更する手段を与えられてはならない（must）。

（O.RESILIENT:FDP_ACC.1、FDP_ACF.1、FPT_FLS.1（オプション））

4.5 システムモニタリング

保護されたオブジェクトに対する、正しくない TOE 設定及び悪意のある活動の試みを識別するために、TOE がそのふるまいに関する監査データを生成する能力を提供すると期待されている。大量の監査データで圧倒されている TOE のリスクを削減し、かつ ESM 監査管理システムへの潜在的なコンプライアンスを容易にするために、TOE は外部の高信頼エンティティにこの監査情報を送信することができなければならない。これは、監査データの可用性の可能性が高くなる。

本 PP は、この高信頼エンティティにアクセスできない場合に、執られるべき特定のアクションを命じない。ST 執筆者は、この場合に TOE が示すふるまいを文書化すべきである。

（O.MONITOR:FAU_GEN.1、FAU_SEL.1、FAU_STG.1、FAU_STG_EXT.1）

4.6 実施の継続

ESM 能力の分散された性質により、ネットワーク攻撃、システム攻撃、又は偶発的な保守の誤りのような状況は、システム間の接続を切断する原因となることもある。この理由で、TOE は、それにアクセス制御の決定情報を提供することを、遠隔のポリシー管理製品に完全には依存するべきではない。TOE が、ネットワーク・サービスの混乱の場合に、ある種のポリシーを実施する能力が存在しなければならない（must）。

（O.MAINTAIN:FPT_FLS_EXT.1、FRU_FLT.1）

4.7 ESM コンポーネント確認

ポリシーを確認する能力に加えて、TOE は、ポリシーの起点の識別情報を確認する能力を持つべきである（should）。同様に、ポリシー、識別情報及び監査データが高信頼エンティティだけに送信されるように、TOE は、他の ESM コンポーネントにそれ自体を識別すべきである（should）。それに失敗する場合は、その後の攻撃に対する基礎を提供

することができるはずの組織のセキュリティデータの侵害をもたらす可能性がある 。

（O.SELFID、O.MNGRID:FCO_NRR.2、FTP_ITC.1（1）、FTP_ITC.1（2））

5 拡張コンポーネント定義

本節は、本 PP 内に記述されたすべての拡張コンポーネントに定義を提供する。これには、第 6 節に規定された必要なコンポーネント及び附属書で規定されたオプションのコンポーネントの両方を含んでいる。

5.1 クラス ESM：エンタープライズセキュリティ管理

ESM 機能要件は、組織における認証、権限付与、説明責任及びコンプライアンス活動の集中的管理をサポートするふるまいに関係する。このクラスは、データ保護と認証活動に対して使用されるデータを提出するよう TSF に要求することにより、クラス FDP 及び FIA をサポートする機能的な活動を規定する。

5.1.1 ESM_DSC オブジェクト発見

ファミリのふるまい

このファミリの要件は、TSF が運用環境のオブジェクトを識別する能力を持ち、かつ、この識別情報に基づいたある措置を講じることを保証する。

コンポーネントのレベル付け

このファミリ、ESM_DSC.1 にはただ 1 つのコンポーネントがある。ESM_DSC.1、オブジェクト発見は、ある基準を満たすデータに係る運用環境をサーチし、そのデータの発見に基づく措置を講じることを TSF に要求する。この要件の主要な目的は、TSF がその関連する属性によって許可された位置にないデータを識別し、引き続いて、これに基づきある形式の修正措置を講じることができるように、強制アクセス制御（MAC）又は同様の環境で使用することである。

5.1.1.1 ESM_DSC.1 オブジェクト発見

ESM_DSC ファミリは、ある特性を示す運用環境においてオブジェクトのインベントリーをとり、ある方法でそれらのオブジェクトに作用するための要件を定義する。このアクションを実行する TSF の能力は、ESM TOE の主要な機能（この場合、アクセス制御）をサポートするので、これは ESM に関係する。CC パート 2 は、TSF が運用環境でなされた確認を検査しそれに従って行動する能力に係る要件を欠くので、ESM_DSC.1 要件が追加された。

下位階層: なし

依存性: なし

ESM_DSC.1.1 TSF は、次の条件を満たす運用環境においてオブジェクトを発見することができなければならない（shall）:[選択:ポリシーが暗号化することを要求する復号されたデータ、データの定義された重要度属性と一致しない領域に存在するデータ、[*割付:運用環境に存在するデータは TSF によってカタログされるべきであることを示すその他の条件*]]。

ESM_DSC.1.2 TSF は、ESM_DSC.1.1 によって定義されるオブジェクトの発見に従って次の措置を講じなければならない（shall）:[選択:オブジェクトを暗号化する、その重要度属性と一致する位置にオブジェクトを移動させる、オブジェクトを削除する、[*割付:その他のアクション*]]。

管理:ESM_DSC.1

次のアクションは FMT における管理機能とみなされる可能性がある :

a） 検知基準の仕様。

b） 検知基準を満たすオブジェクトの発見に従って講じられた措置の仕様。

監査:ESM_DSC.1

ESM_DSC.1 オブジェクト発見が PP/ST に含まれている場合、次のアクションが監査可能であるべきである（should）:

a） 最少: 検知基準を満たすオブジェクトの発見。

b）最少: 発見されたオブジェクトに対して講じられた措置。

5.2 クラス FAU：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、外部IT エンティティに対し監査データを記録するための要件を定義する。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指す。これは、どのように監査データを取扱うべきかを検討するので、セキュリティ監査に関係する。CC パート 2 は、TSF が特定のセキュアな方法で特定の外部リポジトリに監査データを書き込む能力を説明する監査ストレージ要件を欠くので、FAU_STG_EXT.1 要件が追加された。

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FTP_ITC.1TSF 間の高信頼チャンネル

FAU_STG_EXT.1.1 TSF は、FTP_ITC.1 に定義された、高信頼チャンネル経由で、外部 IT エンティティに対して生成された監査データを送信することができなければならない（shall）。

管理: FAU_STG_EXT.1

次のアクションは FMT における管理機能とみなされる可能性がある :

a） 生成された監査データを受信する外部 IT エンティティの仕様。

監査:FAU_STG_EXT.1

FAU_STG_EXT.1 外部監査証跡ストレージが PP/ST に含まれている場合、次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使用されている外部 IT エンティティとの通信の設定及び廃止。

5.3 クラス FCS：暗号化のサポート

5.3.1 FCS_CKM_EXT.4 暗号鍵のゼロ化

FCS_CKM_EXT ファミリは、暗号鍵の削除に係る要件を定義する。FCS_CKM_EXT.4 要件は、CC パート 2 の対応する要件より、重要な削除に対してより高度の特異性を提供するために付け加えられた。

下位階層: なし

依存性: なし

FCS_CKM_EXT.4.1 もはや必要でない場合、TSF はすべての平文の秘密及びプライベート暗号鍵と暗号化によるセキュリティパラメタをすべてゼロ化しなければならない。

管理: FCS_CKM_EXT.4

予見される管理アクティビティはない。

監査: FCS_CKM_EXT.4

FCS_CKM_EXT.4 外部監査証跡ストレージが PP/ST に含まれている場合、次のアクションが監査可能であるべきである(should):

a) 基本: 重要なゼロ化プロセスの失敗。

5.3.2 FCS_RBG_EXT ランダムビット生成

ファミリのふるまい

このファミリの要件は、TSF が承認された暗号化標準に従って乱数表を生成するということを保証する。

コンポーネントのレベル付け

このファミリ、FCS_RBG_EXT.1 にはただ 1 つのコンポーネントがある。FCS_RBG_EXT.1(暗号操作(ランダムビット生成))は、定義された標準に従ってランダムビット生成を実行することを TOE に要求する。

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

下位階層: なし

依存性: なし

FCS_RBG_EXT.1.1 TSF はランダムビット生成(RBG)サービスを、[選択:次から一つを選択:(1)1 つ以上の独立したハードウェアベースのノイズ源(2)1 つ以上の独立したソフトウェアベースのノイズ源(3)(ハードウェアベースとソフトウェアベースのノイズ源の組合せ)]からエントロピーを蓄積するエントロピー源によって初期化されたシード(seed)として与えられた;[選択、次から一つを選択:[選択:Hash_DRBG(いずれか)(CTR_DRBG、HMAC_DRBG(いずれか)(AES))、Dual_EC_DRBG](いずれか)]を使用する NISTSpecial Publication800-90;FIPS Pub140-2 付属書 C:AES を使用する X9.31 付属書 2.4]に従ってすべて行わなければならない(shall)。

FCS_RBG_EXT.1.2 決定論的 RBG は、少なくとも(その RBG が)生成する鍵及び権限付与の要素の最大長以上、及び、最低限[選択、次から1つを選択:128 ビット、256 ビット]のエントロピーによって初期化しなければならない(shall)。

管理:FCS_RBG_EXT.1

予見される管理アクティビティはない。

監査:FCS_RBG_EXT.1

FCS_RBG_EXT.1 外部監査証跡ストレージが PP/ST に含まれている場合、次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。

5.4 クラス FPT:TSF の保護

5.4.1 FPT_FLS_EXT.1 通信の失敗

この SFR は、ポリシー管理製品と TOE の相互の通信に障害がある場合における TOE のふるまいについて記述する。

下位階層: なし

FPT_FLS_EXT.1.1 TSF とポリシー管理製品の間の通信が失敗状態に遭遇する場合、TSF は次の方法でポリシー実施を維持しなければならない(shall):[選択:要求をすべて拒否する、受信された最新のポリシーを実施する、[*割付:失敗ポリシー*]]。

適用上の注意: *詳細化された上記の要件は、ポリシー管理製品と TOE の相互の通信に障害がある場合の TOE のふるまいについて記述するため、ST 執筆者によって使用されている。この要件は、TOE がある種のポリシーを継続的に実施するため、「セキュアな状態」の概念が定義されることを示すために詳細化された。この状況で実施されるポリシーの特定の性質は、ST 執筆者によって完成されるべきである。*

依存性: なし

管理:FPT_FLS_EXT.1

次のアクションは FMT における管理機能とみなされる可能性がある :

a) 通信失敗が発生する場合に執るべきふるまいの定義。

監査:FPT_FLS_EXT.1

FPT_FLS_EXT.1 通信障害が PP/ST に含まれている場合、次のアクションが監査可能であるべきである(should):

a) TOE とポリシー管理製品の間の通信失敗

5.5 クラス FTA：TOE アクセス

5.5.1 FTA_SSL_EXT.1 TSF 起動セッションロック

この SFR は、TOE がセッションロックを起動しなければならない場合の、TOE のふるまいについて記述する。範囲を狭くし、かつロックのアクションを規定するために、明示的な要件が必要だった。それはコモンクライテリアの基本要件に固定された。

下位階層: なし

FTA_SSL_EXT.1.1 TSF は、ローカルな対話セッションについて、セキュリティ管理者指定の非アクティブである時間間隔後に、以下を実施しなければならない[選択:

- セッションをロックする－現在の内容を読取り不能にし、セッションのアンロック以外の利用者のデータへのアクセス/デバイスの表示等のあらゆるアクティビティを無効にすることで、ディスプレイデバイスをクリア又は上書きする、そして利用者がセッションのアンロック前に TSF に再認証することを要求する;
- セッションを終了する]

依存性: なし

管理: FTA_SSL_EXT.1

次のアクションは FMT における管理機能とみなされる可能性がある :

a) 個々の利用者についてロックアウトが発生する後の、利用者の非アクティブな時間の仕様;

b) ロックアウトが発生する後の、利用者の非アクティブなデフォルトの時間の仕様;

c) セッションのアンロックの前に発生するはずの事象の管理。

監査: FTA_SSL_EXT.1

FPT_FLS_EXT.1 が PP/ST に含まれている場合、次のアクションが監査可能であるべきである（should）:

a)最少: セッションロックメカニズムによる対話セッションのロック。

b)最少: 対話セッションをうまくアンロックすること。

c) 基本: 対話セッションをアンロックするあらゆる試み。

6 セキュリティ要件

本文書の要件は機能要件と保証要件の2つに分割されている。最初の機能要件のセットは、コモンクライテリアから導出され、監査及びポリシー実施に係る中核要件を取扱うよう設計されている。本 PP の中の機能要件は、CC のパート 2 から導出され、セキュリティ対策方針の正式のインスタンス化である。これらの要件は TOE のセキュアな操作のサポートに関連している。

セキュリティ保証要件（SAR）は、PP に通常挿入され、SFR とは別々に列挙される：その後、選ばれた SAR に基づく評価の間に CEM が調べられる。コモンクライテリアセキュリティ保証要件の性質及び TOE と確認された特定の技術のために、より適合するアプローチが本 PP 内でなされる。SAR は、前後関係と完全性のため 6..2 節になお列挙されるが、評価者が各 SFR 及び SAR に関してこの TOE に対して実行する必要のある大多数のアクティビティは、「*保証アクティビティ*」パラグラフで詳述される。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アクティビティの標準的な説明である。保証アクティビティは本 PP 内の 2 か所にある：特定の SFR に関係するものはそれらの SFR とともにあり、一方、SFR と無関係のものは、6..2 節に詳述されている。保証アクティビティは、実際には、理解及び便宜のため、インラインで示された、調整された評価方法であることに注意すること。

SFR に直接関連した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、適合するデバイスに必要な保証を達成するために実行される必要のあるアクティビティを詳述して、列挙される。

SFR と無関係のアクティビティを必要とする SAR については、6..2 節は、SAR に関連する特定の保証アクティビティが記載された SFR へのポインターとともに、達成される必要のある追加の保証アクティビティを表示する。

プロテクションプロファイルの今後の反復は、実際の製品評価から学習された教訓に基づき、より詳細な保証アクティビティを提供することもある。

6.1 セキュリティ機能要件

PP の機能的なセキュリティ要件は、次のコンポーネントから構成され、表 2 に要約されている。

表 2 -TOE 機能コンポーネント

機能コンポーネント	
ESM_DSC.1 (optional)	オブジェクト発見 (附属書 C.1.5 で特定の技術タイプに対して定義される)
FAU_GEN.1	監査データ生成
FAU_SEL.1	選択的監査
FAU_STG.1	保護された監査証跡ストレージ(ローカルストレージ)
FAU_STG_EXT.1	外部監査証跡ストレージ
FCO_NRR.2	受領の実施された証拠
FCS_CKM.1.1 (optional)	暗号鍵生成(非対称暗号鍵) (TOE が暗号化機能を提供する場合、附属書 C.3.1 で定義される)
FCS_CKM_EXT.4 (optional)	暗号鍵ゼロ化 (TOE が暗号化機能を提供する場合、附属書 C.3.2 で定義される)
FCS_COP.1 (1) (optional)	暗号操作(データの暗号化/復号) (TOE が暗号化機能を提供する場合、附属書 C.3.3 で定義される)
FCS_COP.1 (2) (optional)	暗号操作(暗号署名) (TOE が暗号化機能を提供する場合、附属書 C.3.4 で定義される)
FCS_COP.1 (3) (optional)	暗号操作(暗号ハッシュ) (TOE が暗号化機能を提供する場合、附属書 C.3.5 で定義される)
FCS_COP.1 (4) (optional)	暗号操作(鍵付ハッシュメッセージ認証に関して)(TOE が暗号化機能を提供する場合、附属書 C.3.6 で定義される)
FCS_RBG_EXT.1	拡張:暗号操作(ランダムビット生成) (TOE が暗号化機能を提供する場合、附属書 C.3.7 で定義される)

(optional)	
機能コンポーネント	
FDP_ACC.1 FDP_ACC.1 (1) FDP_ACC.1 (2)	アクセス制御方針 (附属書 C.1 で特定の技術タイプに対して定義される)
FDP_ACF.1 FDP_ACF.1 (1) FDP_ACF.1 (2)	アクセス制御機能 (附属書 C.1 で特定の技術タイプに対して定義される)
FMT_MOF.1 (1)	機能のふるまい管理
FMT_MOF.1 (2)	機能のふるまい管理
FMT_MSA.1	セキュリティ属性の管理
FMT_MSA.3	静的属性の初期化
FMT_SMF.1	管理機能の仕様
FMT_SMR.1	セキュリティの役割
FPT_FLS.1 (optional)	セキュアな状態を保った失敗 (オプション－附属書 C.2.2 で定義される)
FPT_FLS_EXT.1	通信の失敗
FPT_RPL.1	リプレイ検知
FRU_FLT.1	フォールトトレランスの低下
FTA_SSL_EXT.1 (optional)	TSF 起動セッションロックと終了 (オプション－附属書 C.2.1 で定義される)
FTA_SSL.3 (optional)	TSF 起動による終了 (オプション－附属書 C.2.1 で定義される)
FTA_SSL.4 (optional)	利用者起動による終了 (オプション－附属書 C.2.1 で定義される)
FTA_TSE.1 (optional)	TOE セッションの確立 (オプション－附属書 C.2.1 で定義される)
FTP_ITC.1 (1)	TSF 間高信頼チャネル(漏洩の防止)

FTP_ITC.1 (2)	TSF 間高信頼チャネル(修正の検知)

6.1.1 PP 適用上の注意

6.1.1.1 使用

適用上の注意は、読者が各要件の後ろの意図を識別するために、PP の中の多くの要件の後に提供されている。ST 執筆者は、ST の中のこれらの適用上の注意のうちのどれも再現すべきではない（should not）。

6.1.1.2 作成原理

ESM PP は、ESM 製品の変動する能力を包含するために書かれた、関連するプロテクションプロファイルのファミリを表わす。ESM PP ファミリ内の多数の PP への適合性を表示する ST については、ST 執筆者は、適用上の注意の使用を通じて、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確にすることが推奨される。これは、読者が、評価されるべき製品の部分が別の ESM 能力についての CC の概念とどのように対応するか判断するのを支援する。

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また含んでいる一連の冗長性を持つサーバとして、又は単一のサーバに報告する個々のクライアント・システムに実施地点が存在するクライアントサーバの配置として配置する。適用上の注意を使用することで、ESM システムのアーキテクチャに基づいて表示することが不要な要件の判断が簡単になる。特定の要件は、特定のアーキテクチャに基づいて除外してもよい。除外の可能性に関する一層の詳細に関しては、附属書 C.1 を参照すること。

6.1.2 クラス FAU：セキュリティ監査

FAU_GEN.1 監査データ生成

下位階層: なし

FAU_GEN.1.1 TSF は、次の監査対象事象の監査記録を生成することができなければならない（shall）:

a) 監査機能の起動及び終了; *そして*

b) [指定なし]レベルの監査として*表 3 に識別された*すべての監査対象事象; *そして*

c) [*割付:その他の監査対象事象*]。

表 3 –監査対象事象

コンポーネント	事象	追加情報
FAU_SEL.1	監査設定へのすべての修正	なし
FAU_STG_EXT.1	監査サーバとの通信の設定及び廃止	監査サーバの識別情報
FCO_NRR.2	否認サービスの呼び出し	情報、宛先及び提供される証拠のコピーの識別情報
FCS_CKM.1 (1) (optional)	重要な生成アクティビティの失敗。	なし
FCS_CKM_EXT.4 (optional)	重要なゼロ化プロセスの失敗。	ゼロ化を要求するか引き起こすサブジェクトの識別情報、オブジェクトの識別情報又はクリアされているエンティティ。
FCS_COP.1 (1) (optional)	暗号又は復号の失敗。	操作の暗号モード、暗号化/復号されたオブジェクトの名称/識別子。
FCS_COP.1 (2) (optional)	暗号署名の失敗。	操作の暗号モード、署名された/確認されたオブジェクトの名称/識別子。
FCS_COP.1 (3) (optional)	ハッシュ機能の失敗。	操作の暗号モード、ハッシュ化されたオブジェクトの名称/識別子)。
FCS_COP.1 (4) (optional)	非データの完全性に係る暗号ハッシュ化中の障害。	操作の暗号モード、ハッシュ化されたオブジェクトの名称/識別子)。

FCS_RBG_EXT.1 (optional)	ランダム化プロセスの失敗。	なし
コンポーネント	**事象**	**追加情報**
FDP_ACC.1	実施されたポリシーへのあらゆる変更	変更しているポリシー管理製品の識別情報
FDP_ACF.1	SFP によってカバーされたオブジェクト上で操作を実行するためのすべての要求	サブジェクト識別情報、オブジェクト識別情報、要求された操作。
FMT_MOF.1	TSF のふるまいへのすべての修正	なし
FPT_FLS_EXT.1	TOE とポリシー管理製品の間の通信失敗	ポリシー管理製品の識別情報、失敗の理由
FPT_RPL.1	リプレイの検知	特定のアクションに基づいて講じられる措置
FTP_ITC.1 (1)	高信頼チャネル機能のすべての使用	高信頼チャンネルのイニシエーター及びターゲットの識別情報
FTP_ITC.1 (2)	高信頼チャネル機能のすべての使用	高信頼チャンネルのイニシエーター及びターゲットの識別情報

FAU_GEN.1.2　TSF は各監査記録内に少なくとも次の情報を記録しなければならない(shall):

a) 事象の日付と時間、事象のタイプ、サブジェクト識別情報(該当する場合)及び事象の成果(成功又は失敗);そして

b) 各監査事象種別について、PP/ST に含まれた機能コンポーネントの監査可能な事象定義に基づき、[表 3 の中の情報[そして割付:その他の監査関連情報]。

適用上の注意: 「その他の監査関連情報」は、責任のある個人及び個人によって講じられた特定の措置を識別するために十分な情報を含んでいなければならない(must)。

依存性: FPT_STM.1 高信頼タイムスタンプ

適用上の注意: ESM 監査管理の標準プロテクションプロファイルは、TOE によって生成された監査事象の保管及び処理に責任を負う。

TOE に関する事象の監査は、うまく行ったもの及び行かなかったもの両方のすべての事象が取り込まれ、記録されることを保証することにより、悪意のある利用者が彼らのアクションを覆うのを緩和するのに役立つ。

***保証アクティビティ**:*

評価者は、管理者ガイダンスをチェックし、すべての監査対象事象がリスト化され、監査記録の各タイプの内容の記述が提供されていることを確実にしなければならない(shall)。各監査記録フォーマットタイプが網羅され、各フィールドの簡潔な説明が含まれていなければならない(must)。評価者は、PP で強制された各監査事象種別が記述されており、フィールドの記述が FAU_GEN.1.2 で要求されている情報及び表 3 に規定された追加の情報を含んでいることを確実にするためにチェックしなければならない(shall)。

評価者は、PP で指定された要件の実施に必要で、TOE に実装されているメカニズムの設定(有効又は無効を含む)を許可する管理者インタフェース(サブコマンド、スクリプト、及び設定ファイルを含む)を判断するために、管理者及び利用者ガイダンス、及びすべての利用可能なインタフェースの文書を検証しなければならない(shall)。評価者は、これをするために執った方法又はアプローチ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を確実にする際に付随したアクティビティの一部として実行してもよい。このリストを使用して、評価は各セキュリティ関連の管理者インタフェースが事象に適切な情報を記録する、対応する監査事象を有することを確認しなければならない(shall)。

評価者は、TOE に対して、ST で定義されており、及び/又は、先の 2 つのアクティビティで識別された、すべての事象についての監査記録を生成させることによって、TOE の監査機能をテストしなければならない(shall)。評価者はその後、監査記録がリポジトリに書き込まれ、ST によって定義された属性を含んでいることを判断するために(可能なら)ST によって定義された監査リポジトリ又は実験用の証拠をチェックすべきである(should)。

このテストは他の機能の演習と共に行なってもよい。例えば、アクセス要求が FDP_ACF.1 で規定されたポリシーによって拒否されるときには、監査記録が生成されるだろうということを ST が規定すれば、監査記録がポリシーの有効性をテストする結果として生成されると期待されるだろう。評価者はまた、ログの内容が TOE 上で実行されたアクティビティと一致していることを確実にするためにチェックしなければならない(shall)。例えば、アクセス要求がポリシーによって拒否されるように、テストが実行される場合、対応する監査記録は正確に障害を示すべきである。

FAU_SEL.1 選択的監査

下位階層: なし

FAU_SEL.1.1 TSF は、次の属性に基づき一連のすべての監査対象事象から、監査されるべき一連の事象を選ぶことができなければならない（shall）:

a) [選択:オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、事象種別]; そして

b) [*割付:監査選択度が基づく追加の属性のリスト*]。

適用上の注意: 直接 TOE にアクセスする利用者によってではなく互換性をもつポリシー管理製品によって、選択的監査能力が行使されると期待されている。

依存性: FAU_GEN.1 監査データ生成

FMT_MTD.1TSF データ保証アクティビティの管理:

保証アクティビティ:

評価者は、一連の監査対象事象になることができる選択を判断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）、それがセキュリティターゲットで識別される選択をすべて含むことを確認しなければならない（shall）。

評価者は、次の方法で TOE を設定するために互換性をもつポリシー管理製品を使用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）:

- *有効なすべての選択できる監査対象事象*
- *無効なすべての選択できる監査対象事象*
- *有効ないくつかの選択できる監査対象事象*

これらの設定の各々については、評価者は選択できる監査対象事象をすべて実行し、各設定では、有効な事象のみが記録されることを監査データの検証によって判断しなければならない（shall）。

FAU_STG.1 保護された監査証跡ストレージ(ローカルストレージ)

下位階層: なし

FAU_STG.1.1 TSF は、無許可の削除から、監査証跡にローカルに保管された監査記録 [**割付:ストレージの容量**] を保護しなければならない(shall)。

FAU_STG.1.2 TSF は、監査証跡に保管された監査記録への無許可の修正を防がなければならない(shall)。

適用上の注意: 監査情報をエクスポートする能力に加えて、TOE はある容量のローカルストレージを持つように要求される。ST 執筆者は、監査記録に利用可能なローカルストレージの容量について割り当てを完了する;これにはメガバイトで、監査記録の平均値などがある。

依存性: FAU_GEN.1 監査データ生成

保証アクティビティ:

評価者は、それがローカルに保管される監査データの量を記述すること;ローカルの監査データストアが満杯の場合何が起きるか;及びこれらの記録が不正アクセスに対してどのように保護されているかを確実にするために TSS を検査しなければならない(shall)。評価者はまた、それがローカルの監査データと、監査ログサーバへ送信される監査データの関係について記述することを判断するため、操作ガイダンスを検査しなければならない(shall)。例えば、監査事象が生成される場合、それは外部サーバとローカルストアに同時に送られたか、又は、ローカルストアはバッファーとして使用され、そして監査サーバへデータを送信することにより定期的に「クリア」されているか。

FAU_STG_EXT.1 外部監査証跡ストレージ

下位階層: なし

FAU_STG_EXT.1.1 TSF は、FTP_ITC.1 に定義された、高信頼チャンネル経由で、外部 IT エンティティに対して生成された監査データを送信することができなければならない。(shall)。

依存性: FAU_GEN.1 監査データ生成

FTP_ITC.1 TSF 間高信頼チャンネル

保証アクティビティ:

評価者は、管理者ガイダンスが管理者に対してどのように監査サーバとの通信を確立するかを指示していることを確実にするため、管理者ガイダンスを検査しなければならない(shall)。ガイダンスは、このチャネルがどのようにセキュアな方法(例えば、IPsec、TLS)で確立されるかを指示しなければならない(must)。評価者は、監査サーバへのリンクを確立し、生成された監査記録が当該サーバに送信されたことを確認することにより管理者ガイダンスをテストしなければならない(shall)。これが FAU_GEN.1 の下で規定された保証アクティビティを実行するために行われる必要があることに留意すること。

6.1.3 クラス FCO : 通信

FCO_NRR.2、受領の実施の証拠:

下位階層: FCO_NRR.1 受領の選択的な証拠

FCO_NRR.2. TSF は、常に受信した[ポリシー]に係る受領の証拠の生成を実施しなければならない（shall）。

適用上の注意: この要件の意図は、ポリシーがうまく受信される場合、TSF がポリシー管理製品に受領書を提供することができるということである。

FCO_NRR.2.2 TSF は、情報の発信者の[ソフトウェア名、バージョン、[割付:その他の識別する情報]]、及び証拠が適用される情報の[許容できるポリシー管理製品を識別する、保管された内部データ]関連づけることができなければならない。（shall）。

FCO_NRR.2.3 TSF は、所定の[割付:TSF が元のポリシー管理製品にポリシーデータの受領書を提供すると期待される時間間隔]で[ポリシー管理製品]へ、情報の受領書の証拠を確かめる能力を提供するものとする。

適用上の注意: ST 執筆者は、TSF が元のポリシー管理製品にポリシーデータの受領書を提供すると期待される時間間隔を定義しなければならない（must）。これは、理想的にできる限り即時性に近くなければならない（should）。

依存性: FIA_UID.1 識別のタイミング:

保証アクティビティ:

評価者は、TOE が、当該ポリシーデータを本来送ったポリシー管理製品に、受信したポリシーデータを戻した証拠をどのように確認するか判断するために開発の証拠をチェックしなければならない（shall）。これは、受領書のコンテンツ及びフォーマットを、それを構成するデータが証明可能なように含むべきである。

評価者は、TOE が、一定のソースからポリシーを受理することを許されるような環境を設定すること、そのソースからポリシーをそれに送信すること、ポリシーは引き続いて使われ、そして正確な受領書は、ST に規定された時間間隔内にポリシー管理製品に返信されることを確認することにより、この能力をテストしなければならない（shall）。評価者は、受領書を調べ、その内容が既知のデータと一致していることを確実にするため、ポリシー管理製品を使用することにより精度を確認する。

6.1.4 クラス FCS：暗号サポート

TOE の暗号要件は、TSF、又は非 ESM 運用環境コンポーネントに対する信頼によって実装することができる。TSF が、彼ら自身の固有の冗長性を持つ暗号化機能を実装するようベンダーに強いることではなく、以前に確認された暗号アルゴリズムのスイートを利用することができることが期待される。ST は、どの暗号化機能が TSF によって使用されているか明瞭に示すべきである。

TOE に係る暗号要件に関しては附属書 C.3 を参照すること。

6.1.5 クラス FDP：利用者データ保護

PP は、アクセス制御が必要な異なる状況に関する 3 つのタイプのデータ保護メカニズムを含んでいる。必要に応じてアクセス制御の追加の手段を含めるため、そのメカニズムのリストが時とともに修正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には現在 FDP_ACC.1 と FDP_ACF.1 の要件の 3 つの別個のセットがある。評価内に表示された TOE に適用されるデータ保護メカニズムによって、セキュリティターゲット執筆者はセキュリティターゲットに対して対応する FDP 要件を選ばなければならない（must）。FDP 要件の各々のセットは、選ばれたメカニズムに関する特定の機能を表示する。FDP 要件は附属書 C.1 に記載されており、TOE が適合するべき 4 つの現行のメカニズムは次の通りである：ホストベースのアクセス制御、ウェブベースのアクセス制御及びデータ喪失防止アクセス制御。

FDP_ACC.1 アクセス制御方針

附属書 C.1 を参照。

FDP_ACF.1 アクセス制御機能

附属書 C.1 を参照。

保証アクティビティ:

特定の保証アクティビティは附属書 C.1 の各技術タイプについて定義される。

6.1.6 クラス FMT：セキュリティ管理

FMT_MOF.1(1) 機能のふるまい管理

下位階層: なし

FMT_MOF.1(1) TSF は、以下の機能の*ふるまいを問い合わせ*、*修正する*能力を制限するものとする(shall):*監査された事象*、*遠隔の監査ストレージのリポジトリ*、*アクセス制御 SFP*、*TSF によって実装されるポリシー*、*通信機能停止の場合に実施されるべきアクセス制御 SFP のふるまい*、*認可され互換性をもつポリシー管理製品に対する[割付:その他の機能]*。

依存性: FMT_SMF.1 管理機能の仕様

FMT_SMR.1 セキュリティの役割

適用上の注意: ST 執筆者は、TSF がどのようにポリシー管理製品を信頼することができるか定義しなければならない(must)。例えば、TSF は、それらの鍵を使用して、高信頼チャンネルが設定される場合は、そのチャンネルのもう一つの端から生じるポリシーデータを信頼するべきことを TSF が知るように、内部的にそのポリシー管理製品に一定の鍵を関連させてもよい。

適用上の注意: 問い合わせする能力に関しては、これは、ポリシーのバージョンに関する問い合わせ、又はポリシーの詳細に関する問い合わせのいずれでもありえる 。これについては TSS 内で明らかにされなければならない(must)。

保証アクティビティ:

評価者は、それと通信することができるポリシー管理製品がある環境において、TOE を配置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、ポリシー管理製品が TOE へのコマンドを発することを認可されるように、この環境を設定しなければならない(must)。一旦これが行われた場合、評価者は、上記の要件で規定された機能のふるまいを修正するために、ポリシー管理製品を使わなければならない(must)。各機能について、評価者は、修正に係るふるまい及びその修正後のふるまいを問い合わせするためにポリシー管理製品を使うことにより、修正が適切に適用されたことを確かめなければならない(must)。

評価者はまた、修正が指図する方法で TOE の反応を引き起こすアクティビティを実行しなければならない(must)。これらのアクションには、各機能について、次のアクティビティを含む:

- *監査された事象:以前に機能の行動の修正前に監査された(又は監査されなかった)事象を実行し、監査リポジトリが、現在修正される行動に基づきこの事象をログする(又はログしない)ことを確認する。*
- *遠隔の監査ストレージのリポジトリ:監査された事象が特別のリポジトリに書き込まれていることを確認し、TOE が監査された事象を書き込むべきリポジトリを修正し、監査可能な事象を実行し、それらが当初のリポジトリにもはや書き込まれないことを確認する。*
- *アクセス制御 SFP:現行のアクセス制御 SFP によって許可されている(又は却下された)アクションを実行し、そのアクションが今却下される(又は許可された)ように実装された SFP を修正し、同じアクションを実行し、権限付与が SFP の当初の反復と異なることを確認する。*
- *TSF によって実装されているポリシー:特定のアクセス制御方針によって許可されている(又は却下された)アクションを実行し、今そのアクションを却下する(又は許可する)TSF ポリシーを提供し、同じアクションを実行し、権限付与が FSP の当初の反復と異なることを確認する。*
- *通信機能停止の場合に実装するべきアクセス制御SFP のふるまい:通信機能停止(該当する場合)の場合に、一定の方法で処理されるアクションを実行し、TOE とポリシー管理製品の間の通信を再設定し、TOE が通信機能停止の場合に実装するべき SFP のふるまいを変更し、TOE とポリシー管理製品の間の接続を切断し、本来実行されたのと同じアクションを実行し、アクションを取扱う修正された方法が正しく適用されていることを確認する。*

一旦これが行われたならば、ポリシー管理製品がもはや TOE を設定することを認可されないように、評価者は TOE とポリシー管理製品を再設定しなければならない(shall)。評価者は、その後、TOE を設定するためにポリシー管理製品を使用しようとし、かつそれが却下されるか、オプションが存在すらしないということを確認する。

FMT_MOF.1(2) 機能のふるまいの管理

下位階層: なし

FMT_MOF.1(1)　TSF は、以下の機能の*ふるまいを問い合わせる*能力を制限しなければならない(shall):
TSF によって実装されているポリシー、認可され互換性をもつエンタープライズセキュリティ管理製品への[割付:その他の機能]。

依存性:　FMT_SMF.1 管理機能の仕様

FMT_SMR.1 セキュリティの役割

保証アクティビティ:

評価者は、それと通信することができるポリシー管理製品がある環境において、TOE を配置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、ポリシー管理製品が TOE へのコマンドを発することを認可されるように、この環境を設定しなければならない(must)。一旦これが行われたならば、評価者は、TOE によって実装されているポリシーを問い合わせするためにポリシー管理製品を使用しなければならない(must)。

一旦これが行われたならば、ポリシー管理製品がもはや TOE を設定することを認可されないように、評価者は TOE とポリシー管理製品を再設定しなければならない(shall)。評価者は、その後、TOE を設定するためにポリシー管理製品を使用しようとし、かつそれが却下されるか、オプションが存在すらしないということを確認する。

FMT_MSA.1　セキュリティ属性の管理

下位階層:　なし

FMT_MSA.1.1　TSF は、セキュリティ属性[*割付:セキュリティ属性のリスト*]を、[*割付:認可された識別された役割*]に[選択:デフォルトを変更し、問い合わせ、修正し、削除し、[*割付:その他の操作*]]する能力を制限するために[*割付:アクセス制御 SFP*]を実施しなければならない(shall)。

適用上の注意:　最小限、定義されたセキュリティ属性は、アクセス制御方針、それらを構成する属性、及びそれらが有効かどうかを含む。

適用上の注意:　指定された SFP(s)は、表示された FDP_ACC.1 要件から導かれるはずである(should)。TOE のアクセス制御技術タイプに基づく、該当する SFP については、附属書 C を参照すること。

適用上の注意: 認可された役割は、ポリシー定義コンポーネントである外部IT機関に 関係していると予想されている。

依存性: FDP_ACC.1 サブセットアクセス制御

FMT_SMF.1 管理機能の仕様

FMT_SMR.1 セキュリティの役割

保証アクティビティ:

評価者は、示された属性がTOEによって維持されることを確認するため、TSS及びガイダンス文書を検証しなければならない(shall)。評価はまた、表示された操作を実行する能力が識別された役割(ESMポリシー定義PPに適合するコンポーネントによって提供される機能を予想している)に制限されていると文書が表示することを確認しなければならない(shall)。評価者は、示された属性に対して各々の識別された操作が実行され、そして、TOEインタフェースは、示された属性に対する操作を実行する能力をその他のどんな役割に対しても提供しないということを確認するため、関連するポリシー定義製品を使用しなければならない(shall)。

FMT_MSA.3 静的属性の初期化

下位階層: なし

FMT_MSA.3.1 TSFは、SFPを実施するのに使用されるセキュリティ属性に[限定的な]デフォルトの値を提供するため、[*アクセス制御SFP*]を実施しなければならない(shall)。

FMT_MSA.3.2 TSFは、[*割付:認可された識別された役割*]に、オブジェクト又は情報が作成される場合に、デフォルトの値に優先する代替の初期値を規定することを許可しなければならない(shall)。

依存性: FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティの役割

適用上の注意: 認可された役割はポリシー定義コンポーネントである外部IT機関に関係しているだろうと予想されている。

保証アクティビティ:

1. *評価者は、デフォルト値がTOEによってどの程度限定的に設定されるか(例えば、アクセス制御方針は、アクセス制御規則がなくても操作を必ず制限するように、デフォルトで拒否するモードで作動すべきである)をTSSとガイダンス文書が記述することを確認するため、それらを検証しなければなりません(shall)。評価者は、各々の識別されたセキュリティ属性と限定的な初期状態について、TOEが正しい限定的な値を実装することを確認するため、関連するポリシー定義製品を使用しなければならない(shall)。*

FMT_SMF.1 管理機能の仕様

下位階層: なし

FMT_SMF.1.1 TSF は次の管理機能を実行することができなければならない（shall）::[*監査された事象の設定、遠隔の監査ストレージに係るリポジトリの設定、アクセス制御 SFP の設定、TSF によって実装されているポリシーの問い合わせ、通信機能停止の場合に実施するべきアクセス制御 SFP のふるまいの管理、[割付:TSF によって提供されるその他の管理機能]*。

適用上の注意: この要件の予想は、直接の管理上のアクションによってではなく、むしろ別の ESM 製品によってこれらの管理機能が制御されるであろうということである。

依存性: なし

保証アクティビティ:

評価者は、どのポリシー管理及びセキュアな構成管理製品が TOE と互換性を持つか決めるために、TOE の簡略な仕様をチェックしなければならない（shall）。評価者は、これらの互換性をもつ製品と設定された TOE を配置し、セキュリティターゲット及び操作ガイダンスで定義された機能を実行するためにこれらの製品を使用しなければならない（shall）。ST と操作ガイダンスの中の広告された各々の管理機能については、評価者は、この管理機能を実行するためにポリシー管理製品を使用しなければならない（shall）。その後、各管理機能については、評価者はこのふるまいを試みて、観察されたふるまいが実行された管理機能の期待と一致していることを確かめなければならない（shall）。

FMT_SMR.1 セキュリティの役割

下位階層: なし

FMT_SMR.1.1 TSF は、役割[*割付:TOE への接続の設定について認可されたポリシー　管理製品に関連する役割*]を維持しなければならない（shall）。

FMT_SMR.1.2 TSF は、役割に利用者を関連させることができなければならない（shall）。

依存性: FIA_UID.1 識別のタイミング:

保証アクティビティ:

評価者は、経営権が 1 つ以上の役割によってどのように委任されるか、また、認可されたポリシー定義製品がどのようにそれらの役割に関係しているかを、TSS とガイダンス文書が記述することを確認するため、それらを検証しなければならない（shall）。評価者は、TOE に接続するために関連するポリシー定義製品を使用し、かつそれが指定された役割内で作動していることを確認するものとする。評価はまた、示された役割について認可されていない利用者又はその他の外部エンティティが、示された役割を引き受けることができないことを確認しなければならない（shall）。クラス FPT: TSF の保護

FPT_FLS_EXT.1 通信の障害

下位階層: なし

FPT_FLS_EXT.1.1 *TSF とポリシー管理製品の間の通信が障害状態に遭遇する場合、TSF は次の方法でポリシー実施を維持しなければならない（shall）:[選択:要求をすべて拒否する、受信された最新のポリシーを実施する、[割付:実施されたポリシーの障害状態の特徴]]。*

適用上の注意: 詳細化された上記の要件は、ポリシー管理製品と TOE の相互の通信 に障害がある場合の、TOE のふるまいについて記述するため、ST 執筆者によって使用されている。この状況で実施されるポリシーの特定の性質は、ST 執筆者によって完成されるべきである。

依存性: なし

保証アクティビティ:

評価者は、TOE が他の ESM 製品に関連してどのように配置されるか議論することを判断するため、操作ガイダンス（及び、利用できる場合は、実験的な証拠）をチェックしなければならない（shall）。TOE がそれに伴うポリシー管理製品と対話することができない場合、評価者が期待されるふるまいを判断できるように、これは遂行される。

評価者は、TOE にポリシーを分散する製品を終了することにより、及びまた、該当する場合に TOE とこの製品の間のネットワーク接続を切断することにより、この能力をテストしなければならない（shall）。その後、評価者は、TOE と対話する。一方、この状態でそれが示すふるまいが期待されるふるまいと一致していることを判断するため、これらの通信は停止されている。

FPT_RPL.1 リプレイ検知

下位階層: なし

FPT_RPL.1.1 TSF は、次のエンティティのリプレイを探知しなければならない（shall）:[*割付: 識別されたエンティティのリスト*]。

FPT_RPL.1.2 TSF は、リプレイが検知される場合、[*割付: 特定のアクションのリスト*]を実行しなければならない（shall）。

適用上の注意: 識別されたエンティティのリストが空又は「なし」であることは受けいれられない。また、特定のアクションが空又は「なし」であることも受け入れられない。

依存性: なし

保証アクティビティ:

評価者は、TSF がリプレイされたデータを検知する方法について記述することを判断するために、管理者ガイダンスと TSS（及び利用できる場合は、実験的な証拠）をチェックしなければならない（shall）。例えば、ポリシーがある予期される図表と一致していることを確かめるために、TSF によって有効確認することができる証明書又はその他の値を提供してもよい。あるいは、TOE は、リプレイの脅威からそれを免疫にするデータを送信するために、SSL のようなプロトコルを利用してもよい。

評価者は、TOE とローカルネットワーク上の（Wire shark のような）パケット・スニファー・アプリケーションの起動、それへの有効なポリシーの送信、及びこのポリシーを含むパケットの確認により、この能力をテストしなければならない（shall）。その後、評価者は、これらのパケットを取り、TOE にそれらを再送信することができる。一旦これが行われたならば、評価者は、実施されたポリシーが送信された最初のポリシーであろうという期待をもって、利用者データ保護テストの適切なサブセットを実行するものとする。期待される結果が達成される場合、TOE は初歩的なポリシー偽造に対して十分に対応できる。

6.1.7 クラス FRU：資源利用

FRU_FLT.1 フォールトトレランスの低下

下位階層: なし

FRU_FLT.1.1 TSF は、次の障害が発生する場合[*最近のポリシーを実施する*]操作を確実にしなければならない（shall）:[*停電の後のポリシー管理製品との通信の障害。*]。

依存性: FPT_FLS.1 セキュアな状態の保存の失敗:

保証アクティビティ:

評価者は、TOE とポリシー管理製品の間のネットワーク接続の切断と最新のポリシーの定義により、この能力をテストしなければならない（shall）。また、接続の再設定は、TOE が FCO_NRR.2.3 で規定された時間間隔内で新しいポリシーデータを適切に受信するかどうかを決定する。評価者は、古いポリシーが特定のアクションを許可し、新しいポリシーがその同じアクションを拒否するように、シナリオを考案しなければならない（shall）。その後、評価者はそのアクションを実施し、それが許可されることを確認し、ポリシー管理製品との接続を切断し、その停電中に新しいポリシーを定義し、接続を再設定し、FCO_NRR.2.3 によって定義された間隔を待ち、再び同じアクションを実施し、それがもはや許可されないことを確認する。

6.1.8 クラス FTP：高信頼パス/チャンネル

FTP_ITC.1（1） TSF 間高信頼チャンネル（漏洩の防止）

下位階層: なし

FTP_ITC.1.1（1） **詳細化:** TSF は、それ自体と、他の通信チャンネルとは論理上異なり、そのエンドポイントの確かな識別情報と漏洩からのチャンネル・データの保護を提供する、*認可された IT エンティティとの間の高信頼*通信チャンネルを提供するために、*[割付:FCS に規定されたサービス]を使用しなければならない*（shall）。

適用上の注意: ST 執筆者は、FCS サービスが TSF にとって内部的なものか又は運用環境によって提供されるものかを示さなければならない(must)。

FTP_ITC.1.2(1) **詳細化**:TSF は、*TSF 又は認可された IT エンティティ*が高信頼チャンネル経由で通信を始めることを許可しなければならない(shall)。

FTP_ITC.1.3(1) TSFは、*ポリシーデータの転送、[割付:その他の機能*のために高信 頼チャンネル経由で通信を始めるものとする。

適用上の注意: ST 執筆者は、TOE がその他の ESM 製品と持っているすべての保護された通信(監査データの転送、識別データの要請、認証サーバなどへの通信)で割付を一杯にするべきである。

依存性: なし

保証アクティビティ:

評価者は、セキュアな通信が可能になるメカニズムを判断するために、管理者ガイダンスをチェックしなければならない(shall)。保証証拠が実験的な証拠を含んでいる場合、評価者はまた、セキュアな通信が容易になる手段について議論がなされることを確実にするために、その証拠をチェックしなければならない(shall)。これに基づいて、次の分析が必要である:

- *暗号が TOE にとって内部的なものである場合、評価者は、製品が FIPS 140-2(米国又はカナダで評価する場合)又は評価が行なわれている国家の同等な国内標準によって有効確認されたことを確かめなければならない(shall)。*
- *暗号が運用環境によって提供される場合、評価者は、暗号作成法がどのように利用されるかを見て、かつ使用された機能が FIPS 140-2(米国又はカナダで評価する場合)又は評価が行なわれている国家の同等な国内標準によって有効確認されたことを確かめるために設計文書を検証しなければならない(shall)。*

評価者は、TOE に対するセキュアな通信を可能にし、ローカルネットワークにパケットスニファを置くことにより、この能力をテストしなければならない(shall)。彼らはその後、TOE が通信するすべての高信頼 IT 製品との通信を必要とするアクションを実行するため、TOE を使用し、及び、それらの内容が不明瞭にされていることを確実にするため、TOE に向かう、又は TOE から向けられるパケットのトラフィックが取り込まれていることを確認する。評価者はまた、暗号のネゴセッションハンドシェイクが、通信を保護するために使用される表示された暗号アルゴリズムと一致していることを確かめるために、これらの通信の設定の間パケットスニファを実行しなければならない(shall)。

FTP_ITC.1(2) TSF 間高信頼チャンネル(修正の検知)

下位階層: なし

FTP_ITC.1.1(2) **詳細化:**TSF は、それ自体と他の通信チャンネルとは論理的に異なり、そのエンドポイントの確かな識別情報及び *データの修正の検知*を提供する、*認可された IT エンティティ*との間の *高信頼*通信チャンネルを *提供する際に[割付:FCS に規定されたサービス]*を *使用*しなければならない(shall)。

適用上の注意: ST 執筆者は、FCS サービスが TSF にとって内部的なものか又は運用環境によって提供されるものかを示さなければならない(must)。

FTP_ITC.1.2(2) **詳細化:**TSF は、*TSF 又は認可された IT エンティティ*が高信頼チャンネル経由で通信を始めることを許可しなければならない(shall)。

FTP_ITC.1.3(2) TSF は、*ポリシーデータの転送、[割付:その他の機能]* のために高信頼チャンネル経由で通信を始めるものとする。

適用上の注意: ST 執筆者は、TOE がその他の ESM 製品と持っているすべての保護された通信(監査データの転送、識別データの要請、認証サーバなどへの通信)で割付を一杯にするべきである。

依存性: なし

保証アクティビティ:

評価者は、セキュアな通信が可能になるメカニズムを判断するために、管理者ガイダンスをチェックしなければならない(shall)。保証の証拠が実験的な証拠を含んでいる場合、評価者はまた、セキュアな通信が容易になる手段について議論がなされることを確実にするために、その証拠をチェックしなければならない(shall)。これに基づいて、次の分析が必要であろう:

- *暗号が TOE にとって内部的なものである場合、評価者は、製品が FIPS 140-2(米国又はカナダで評価する場合)又は評価が行なわれている国家の同等な国内標準によって有効確認されたことを確かめなければならない(shall)。*
- *暗号が運用環境によって提供される場合、評価者は、暗号作成法がどのように利用されるかを見て、かつ使用された機能が FIPS 140-2(米国又はカナダで評価する場合)又は評価が行なわれている国家の同等な国内標準によって有効確認されたことを確かめるために設計文書を検証しなければならない(shall)。*

評価者は、TOE が、認可された IT エンティティと言われているところから受信されたデータに対するどんな修正も検知することができることを実証しなければならない(shall)。この能力をテストする望ましいアプローチは、評価者が TOE と互換性をもち認可されたポリシー管理製品との間のネットワークリンクにノイズを人為的に導入することである。その後、評価者は、TOE に分散されるべきポリシー管理製品上で、管理アクティビティを実行し、かつデータの修正を引き起こす、導入されたノイズによりそれらが効果を現わさないことを確認しなければならない(shall)。この確認は、その機能がそれに対して修正されるデータを送信する試みの前の状態と同じであることを示すために、TOE に問い合わせするため、ノイズを止め、ポリシー管理製品を使用することによるか、又は、TOE の機能の前/

後の比較を実行することによるかのいずれかで実行することができる。そしてポリシー管理製品から受け取る修正されたデータの結果としてそれらが変更されなかったことを確認することができる。

注:使用される技術及びインタフェースへのアクセスによっては、代替アプローチは、TOE の適切な「メッセージ」を(恐らく PM 製品によって)「生成する」こと、その「メッセージ」を取って 1 つのビットを変更すること、通常のインタフェースを通じて TOE へ「メッセージ」を提出し、次に、修正が TOE の何らかのアクションによって検知されるか、又は「メッセージ」に対して TOE の応答はないことを確認する。

6.1.9 満たされていない依存性

本節は、本 PP に対して選択された要件への依存性としてリストされたが主張されていないセキュリティ機能要件(SFR)を詳述する。そのような要件ごとに、その除外の根拠が提供される。

FIA_UID.1　この SFR は、FCO_NRR.2 に対する満たされていない依存性である。適用上の注意及び FCO_NRR.2 の定義された割付は、ポリシーの起源の識別情報が、ポリシー送付機能を起動するいずれかの利用者の利用者識別情報ではなく、ソフトウェア/ハードウェア情報に限定されていることを述べているため、含まれていなかった。この SFR はまた、FMT_SMR.1 に対する依存性である。管理者の役割は、識別されたポリシー管理製品に関係しているので、この依存性を満たすことは含まれていなかった。したがって、O.MNGRID にマップされた SFR は、サブジェクトの識別情報を促進するのに十分であるとみなされる。

FMT_MTD.1　この SFR は、FAU_SEL.1 に対する満たされていない依存性である。依存性の意図は、監査機能の設定を管理する TSF データが設定可能であると期待されているということであるため、含まれていなかった。監査するふるまいは、TSF データの集合ではなくむしろ TSF の機能であると考えられるので、この依存性は FMT_MOF.1(1)によって満たされている。

FPT_STM.1　この SFR は、FAU_GEN.1 に対する満たされていない依存性である。TOE は、自身のシステムクロックを含むと必ずしも期待されないため、含まれていなかった。ST 執筆者は、システム時刻の起点を決定するため、評価中の全 ESM を検査すべきである(should)。評価の境界が内部システムクロックを使用する ESM アプライアンス全体である場合、FPT_STM.1 が表示されるべきである。しかしながら、ESM がホスト運用システム又は NTP サーバのような環境上のコンポーネントに依存する場合、それは、環境上の目標として正確なシステム時刻を表わす、受入可能な選択肢である。

FPT_FLS.1　この依存性は、がそうである代わりの明確な要件 FPT_FLS_EXT.1 を通じて満たされている。注:FPS_FLS.1 はオプションの要件として含まれている。しかし、FPT_FLS.1 のオプションの使用は、FPT_FLS.1 の依存性(FPT_FLS_EXT.1 はそれに対する正しい充足である)について SFR で使用することとは異なる方法で完了している。

6.2 セキュリティ保証要件

第 4 章の TOE に係るセキュリティ対策方針は第 3 章で識別された脅威に対処するために構成された。第 6 章のセキュリティ機能要件（SFR）は、セキュリティ対策方針の正式なインスタンス化である。PP は、評価者が評価に適用できる文書を査定し、独立したテストを実行する範囲を枠組みするために、EAL1 からセキュリティ保証要件（SAR）を引き出す。

第 6 章の前文で示されたように、本節が CC からすべての SAR を含む一方、評価者によって実行される保証アクティビティは本節と同様に第 6 節でも詳述される。

本 PP に適合するために書かれた ST に対する TOE を評価するための一般的なモデルは、以下のとおりである：

ST が評価について承認された後、評価機関（CCTL）は、TOE を入手し、IT 環境や TOE に対する管理者ガイダンスをサポートする。ST にリストされた保証アクティビティ（ST 内に、又は別の文書において TOE 特有のものとして、CCTL によって詳細化されるだろう）は、その後、CCTL によって実行されるだろう。CCTL はまた、EAL1 に係る共通評価方法（CEM）によって義務付けられたすべてのアクションを実行すると期待される。これらの活動の結果は、有効性確認のため、（使用された管理者ガイダンスと共に）文書化され提示されるだろう。

各ファミリに対して、開発者にとってもしあるとすればどのような追加の文書/活動が必要かを明確にするため、開発者アクションエレメントに「開発者向け注意事項」が提供される。その内容/記述及び評価者アクティビティエレメントに対して、追加の保証アクティビティ（第 6 節に既に含まれている）は各エレメントではなくむしろ、ファミリ全体として説明されている。さらに、本節に説明されている保証アクティビティは、第 6 節に規定されているものを補完する。

TOE セキュリティ保証要件は、表 4 に要約されているが、本 PP の第 3 章で識別された脅威に対処するために必要な管理・評価活動を識別する。6.3 節は、本節の中のセキュリティ保証要件を選ぶことの簡潔な正当化の理由を提供する。

表 4 -TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネント記述
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
テスト	ATE_IND.1	独立テストー適合
脆弱性評定	AVA_VAN.1	脆弱性調査
ライフサイクルサポート	ALC_CMC.1	TOE のラベル付け
	ALC_CMS.1	TOE の CM 範囲

6.2.1 クラス ADV:開発

本 PP への TOE の適合性については、TOE の情報は、最終利用者が利用可能なガイダンス文書や、ST の TOE 要約仕様(TSS)部分に含まれていると予想されている[4]。TOE 開発者が TSS を書く必要はない一方で、TOE 開発者は機能要件に関して TSS に含まれている製品の説明に同意しなければならない(must)。各 SFR と関連する保証アクティビティは、ST 執筆者が TSS セクションの適切な内容を決定するのに十分な情報を提供するべきである(should)。

6.2.1.1 ADV_FSP.1　基本機能仕様

機能仕様は TSFI を記述している。これらのインタフェースの正式な又は完全な仕様を持つ必要はない。さらに、本 PP に適合する TOE は TOE 利用者によって直接呼び出し可能でない運用環境とのインタフェースが必要であり、そのようなインタフェースの間接的なテストのみが可能であろうから、そのようなインタフェース自体について内外を説明するような明細を記す意味はほとんどない。本 PP については、このファミリの活動は、機能要件に対する TSS に示されたインタフェースと、AGD 文書に示されたインタフェースを理解することに焦点を置くべきである(should)。特定の保証アクティビティを満たすための、追加の「機能仕様」文書は不要であるべきである(should)。

評価される必要のあるインタフェースは、独立した、抽象的なリストよりはむしろ、リストされた保証アクティビティを実行するために必要な情報を通じて特徴を述べられる。

4 開発者は、独占的な詳細が必要な場合、追加文書を供給するオプションを持っている。しかし、莫大な量の情報は大衆に公開された文書にあるべきである(should)。

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 までのトレーシングを提供しなければならない（shall）。

開発者向け注意事項: 本章の前文で示されたように、機能仕様は、ST の TSS で提供される情報と相まって、AGD_OPR 及び AGD_PRE 文書に含まれる情報から構成される。機能要件における保証アクティビティは、証拠文書とTSS セクションに存在すべき証拠を指している。これらは SFR と直接関連しているので、エレメント ADV_FSP.1.2D のトレーシングは既に暗黙裡になされており、追加の証拠文書は必要ない。

内容と記述エレメント:

ADV_FSP.1.1C　機能仕様は、SFR を実施し及び SFR を支援する各 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 を強化し、SFR を支援する各 TSFI に関連するすべてのパラメタを識別するものとする（shall）。

ADV_FSP.1.3C　機能仕様は、SFR−非干渉としてのインタフェースの暗黙のカテゴリー分類に根拠を提供しなければならない（shall）。

ADV_FSP.1.4C　トレーシングは、機能仕様での TSFI への SFR の追跡を実際に明らかにするもの　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と記述に係るすべての要件を満たす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 の正確で完全なインスタンス化であることを判断しなければならない（shall）。

保証アクティビティ:

これらの SAR に関連する特定の保証アクティビティはない。機能仕様文書は各 SFR について記述された評価アクティビティを支援するため、及び AGD、ATE 及び AVA の SAR に記述されたその他のアクティビティのために提供されている。機能仕様の情報の内容についての要件は、実行されているその他の保証アクティビティのおかげで暗黙裡に評価されている;インタフェース情報が不十分なために評価者があるアクティビティを実行することができない場合には、適切な機能仕様は提供されていなかった。例えば、TOE が暗号アルゴリズムに係る鍵の長さを設定する能力を提供するが、この機能を実行するインタフェースを規定しそこなう場合は、FMT_SMF に関連する保証アクティビティは失敗する。

評価者は、TOE 機能仕様が、TOE が傍受するか、共に作業する一連のインタフェースについて記述していることを確かめなければならない(shall)。評価者は、これらのインタフェースの説明を吟味し、それらの呼び出しについて満足な説明を含んでいることを確かめるべきである(should)。

評価者はまた、TOE が無効データの受入の可能性にどのように対処するか、TOE 機能仕様が説明していることを確認しなければならない(shall)。適切に保護されなければ、無効データの受入の可能性は、無許可の利用者にアクセス権を与えるか又は認可された利用者へのアクセスを拒否する、アクセス制御の判断を変更する可能性もある。

6.2.2 クラス AGD: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ともに提供されるだろう。ガイダンスは、運用環境がセキュリティ機能に係るその役割を果たすことができることを、認可された利用者がどのように確かめるかの説明を含まなければならない(must)。文書は非公式な形で、認可された利用者が読みやすいものであるべきである(should)。

ガイダンスは、ST に表示されているとおり、製品がサポートするすべての運用環境について提供されなければならない(must)。このガイダンスは以下を含む。

- その環境において、TOE をうまくインストールするための指示;及び、
- 製品として、及び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。

ガイダンスはまた、システム起動の間にそれを修正することができないか、システム起動シーケンスから完全に取り除くことはできないように、ホスト運用システム上のセキュアな設定へ TOE をブートする方法に関して定めなければならない(must)。また、それは、製品が信頼されていないサブジェクトによって無効にされる(例えば、終了)のを防ぐように、製品を設定する方法について記述しなければならない(must)。

特定のセキュリティ機能に関係するガイダンスも提供される:そのようなガイダンスについての要件は、各 SFR で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）。

開発者向け注意事項: ここで情報を繰り返すより、開発者は、評価者がチェックするガイダンスの詳細を確かめるために、このコンポーネントの保証アクティビティを検証するべきである（should）。このことは、受入可能なガイダンスの準備に必要な情報を提供する。

内容と記述エレメント:

AGD_OPE.1.1C 利用者操作ガイダンスは、適切な警告を含むセキュアな処理環境で制御されるべき利用者がアクセス可能な機能及び特権を、各利用者の役割について、記述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の TOE には必要な管理機能がないので、AGD_OPE.1 の証拠と分析は、主として TOE の他の ESM 製品との関係の管理に焦点を置くべきである（should）。さらに、TOE に接続されたポリシー管理製品に対する AGD_OPE の評価によって、TOE のふるまい（例えばポリシーの実施）の定義が取り扱われると期待される。TOE が特に管理機能を含んでいる場合には、評価チームは AGD_OPE.1 の要件の本来の意図を使用し、それらが適切に満たされていることを確実にするために評価アクティビティを実行するべきである（should）。*

AGD_OPE.1.2C　利用者操作ガイダンスは、TOE によって提供される利用可能なインタフェースをセキュアなやり方で利用する方法を、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、利用可能な機能及びインタフェース、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、適宜セキュアな値を示しつつ、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 の管理下にあるエンティティのセキュリティ特性を変更することを含む、実行される必要のある、利用者がアクセス可能な機能に関連する各タイプのセキュリティ関連事象を、利用者の役割ごとに明確に示さなければならない（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（障害又は操作ミスの後の操作を含む）、セキュアな操作を維持することへのそれらの結果及び影響について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履行するために、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と記述に係るすべての要件を満たす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あるものは、各 SFR と保証アクティビティによって確かめられるだろう。次の追加情報も必要である。

操作ガイダンスは、TOE の評価された設定に関連する暗号エンジンを設定するための指示を含まなければならない（shall）。それは、TOE の CC 評価の間に、他の暗号エンジンの使用が評価されず、テストもされなかったということについて、管理者に対する警告を提供しなければならない（shall）。

6.2.2.2 準備手続 (AGD_PRE.1)

開発者アクションエレメント:

AGD_PRE.1.1D 開発者は、その準備手続を含む TOE を提供しなければならない(shall)。

開発者向け注意事項: 操作ガイダンスと同様に、開発者は準備手続に関して必要な内容を判断するために、保証アクティビティに目を向けるべきである(should)。

内容と記述エレメント:

AGD_PRE.1.1C 準備手続は、開発者の引渡手順に従って引渡された TOE のセキュアな受入に必要なすべての段階を記述しなければならない(shall)。

AGD_PRE.1.2C 準備手続は、TOE のセキュアなインストール、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段階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の内容と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

AGD_PRE.1.2E 評価者は、TOE が操作のために安全に準備できることを確認するため、準備手続を適用しなければならない(shall)。

保証アクティビティ:

上記の前文で示されるように、特にTOE機能要件をサポートするために運用環境を設定する場合、文書化に関して著しい期待がある。評価者は、TOE用に提供されるガイダンスが、STにTOEを要求するすべてのプラットフォーム(すなわちハードウェアと運用システムの組合せ)に適切に対処することを確実にするためチェックしなければならない(shall)。

6.2.3 クラス ALC: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、ライフサイクルサポートは、TOEベンダーの開発及び構成管理プロセスの検討ではなく、ライフサイクルの最終利用者に見える側面に限定される。これは、製品の全体的な信頼性に寄与する際に、開発者の実践が果たす重要な役割を減少するつもりではない;むしろ、それは、この保証レベルでの評価に利用できる情報に対する反映である。

6.2.3.1 TOE のラベル付け（ALC_CMC.1）

このコンポーネントは、同じベンダーの他の製品又はバージョンとそれを区別できるようにTOEを識別することを目標としており、最終利用者が獲得する場合、容易に特定することができる。

開発者アクションエレメント:

ALC_CMC.1.1D 開発者は TOE と TOE の参照を提供しなければならない（shall）。

内容と記述エレメント:

ALC_CMC.1.1C TOE は、その一意の参照でラベル付けされなければならない（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と記述に係るすべての要件を満たす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 の要件を満たすバージョンを特に識別する（製品名/バージョン番号のような）識別子を含むことを確実にするためにSTをチェックしなければならない（shall）。さらに、評価者は、バージョン番号がSTの中のそれと一致していることを確実にするため、テストのために受信したAGDガイダンス及びTOEのサンプルをチェックしなければならない（shall）。ベンダーがTOEを広告するウェブサイトを維持する場合、評価者は、STの中の情報が製品を識別するのに十分であることを確実にするため、ウェブサイトについての情報を検査しなければならない（shall）。

6.2.3.2 TOE の CM カバレージ（ALC_CMS.1）

TOE の範囲とその関連する評価証拠要件を考慮すると、このコンポーネントの保証アクティビティは、ALC_CMC.1 に記載された保証アクティビティによってカバーされる。

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）。

内容と記述エレメント:

ALC_CMS.1.1C　構成リストは下記を含んでいなければならない（shall）:TOE 自体;及び SAR によって必要とされる評価証拠。

ALC_CMS.1.2C　構成リストは構成項目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と記述に係るすべての要件を満たす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 の中の「SAR によって要求される評価証拠」とは、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結び付けられた ST の情報に限定されている。TOE が特に識別され、この識別が、（ALC_CMC.1 に対する保証アクティビティにおいてそうであるように） ST 及び AGD ガイダンスにおいて一貫していることを確実にすることによって、評価者は、このコンポーネントによって必要とされる情報を暗黙裡に確認する。

6.2.4 クラス ASE：セキュリティターゲット評価

6.2.4.1 適合主張（ASE_CCL.1）

開発者アクションエレメント:

ASE_CCL.1.1D　開発者は適合主張を提供しなければならない（shall）。

ASE_CCL.1.2D　開発者は適合主張の根拠を提供しなければならない（shall）。

内容と記述エレメント:

ASE_CCL.1.1C　適合主張には、ST と TOE が適合性を表示する CC のバージョンを識別する CC 適合主張を含むものとする。

ASE_CCL.1.2C　CC 適合主張は、CC パート 2 適合又は CC パート 2 拡張のいずれかとして、ST の CC パート 2 への適合性を記述しなければならない（shall）。

ASE_CCL.1.3C　CC 適合主張は CC パート 3　適合又は CC パート 3 拡張のいずれかとして、ST の CC パート 3 への適合性を記述しなければならない（shall）。

ASE_CCL.1.4C　CC 適合主張は、拡張されたコンポーネントの定義と一致していなければならない（shall）。

ASE_CCL.1.5C　適合主張は、ST が適合性を表示するすべての PP 及びセキュリティ要件パッケージを識別しなければならない（shall）。

ASE_CCL.1.6C　適合主張は、パッケージ-適合又はパッケージ－増加のいずれかとしてパッケージへの ST の任意の適合性を記述しなければならない（shall）。

ASE_CCL.1.7C　適合主張の根拠は、TOE のタイプが、適合性が表示されている PP の中の TOE タイプと一致していることを説明しなければならない（shall）。

ASE_CCL.1.8C　適合主張の根拠は、セキュリティ問題の定義の説明は、適合性が表示されている PP の中のセキュリティ問題の定義の説明と一致していることを説明しなければならない（shall）。

評価者アクションエレメント:

ASE_CCL.1.1E　評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない（shall）。

6.2.4.2 拡張コンポーネント定義 (ASE_ECD.1)

開発者アクションエレメント:

ASE_ECD.1.1D　開発者は、セキュリティ要件の説明を提供しなければならない（shall）。

ASE_ECD.1.2D　開発者は、拡張コンポーネントの定義を提供しなければならない（shall）。

内容と記述エレメント:

ASE_ECD.1.1C　セキュリティ要件の説明は、拡張セキュリティ要件をすべて識別するものとする。

ASE_ECD.1.2C　拡張コンポーネントの定義は拡張されたセキュリティ要件ごとに、拡張されたコンポーネントを定義しなければならない（shall）。

ASE_ECD.1.3C　拡張コンポーネントの定義は、各拡張コンポーネントが、既存の CC コンポーネント、ファミリ及びクラスとどのように関連しているかを記述しなければならない（shall）。

ASE_ECD.1.4C　拡張コンポーネント定義は、既存のCCコンポーネント、ファミリ、クラス、及び記述のモデルとしての方法を使用するものとする。

ASE_ECD.1.5C　拡張コンポーネントは、測定可能な要素と目標要素への適合性又は不適合が説明することができるようなこれらの要素から構成されなければならない（shall）。

評価者アクションエレメント:

ASE_ECD.1.1E　評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない（shall）。

ASE_ECD.1.2E　評価者は、既存のコンポーネントを使用して、どんな拡張コンポーネントも明確に表現することができないことを確認しなければならない（shall）。

6.2.4.3　ST 概説 (ASE_INT.1)

開発者アクションエレメント:

ASE_INT.1.1D　開発者は ST 概説を提供するものとする。

内容と記述エレメント:

ASE_INT.1.1C　ST 概説は、ST 参照、TOE 参照、TOE 概要及び TOE 説明を含まなければならない（shall）。

ASE_INT.1.2C　ST 参照は一意に ST を識別しなければならない（shall）。

ASE_INT.1.3C　TOE 参照は TOE を識別するものとする。

ASE_INT.1.4C　TOE 概要は、TOE の使用及び主要なセキュリティの特徴を要約しなければならない（shall）。

ASE_INT.1.5C　TOE 概要は TOE のタイプを識別するものとする。

ASE_INT.1.6C　TOE 概要は、TOE によって必要とされる任意の非 TOE ハードウェア/ソフトウェア/ファームウェアを識別しなければならない（shall）。

ASE_INT.1.7C　TOE 説明は、TOE の物理的な範囲について記述しなければならない（shall）。

ASE_INT.1.8C　TOE 説明は、TOE の論理的な範囲について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:

ASE_INT.1.1E　評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

ASE_INT.1.2E　評価者は、TOE 参照、TOE 概要及び TOE 説明が互いに一致していることを確認しなければならない(shall)。

6.2.4.4 セキュリティ対策方針 (ASE_OBJ.2)

開発者アクションエレメント:

ASE_OBJ.2.1D　開発者は、セキュリティ対策方針の説明を提供しなければならない(shall)。

ASE_OBJ.2.2D　開発者は、セキュリティ対策方針の根拠を提供しなければならない(shall)。

内容と記述エレメント:

ASE_OBJ.2.1C　セキュリティ対策方針の説明は、TOE のセキュリティ対策方針及び運用環境のセキュリティ対策方針を記述しなければならない(shall)。

ASE_OBJ.2.2C　セキュリティ対策方針の根拠は、当該セキュリティ対策方針が遭遇する脅威及び当該セキュリティ対策方針によって実施された OSP(組織のセキュリティ方針)まで、TOE の各セキュリティ対策方針をトレースしなければならない(shall)。

ASE_OBJ.2.3C　セキュリティ対策方針の根拠は、当該セキュリティ対策方針が遭遇する脅威、当該セキュリティ対策方針によって実施された OSP(組織のセキュリティ方針)及び当該セキュリティ対策方針によって支持される想定まで、運用環境の各セキュリティ対策方針をトレースしなければならない(shall)。

ASE_OBJ.2.4C　セキュリティ対策方針の根拠は、セキュリティ対策方針が遭遇するすべての脅威を説明するものとしなければならない(shall)。

ASE_OBJ.2.5C　セキュリティ対策方針の根拠は、セキュリティ対策方針が実行するすべての OSP を説明しなければならない(shall)。

ASE_OBJ.2.6C　セキュリティ対策方針の根拠は、セキュリティ対策方針が実行するすべての OSP を説明しなければならない(shall)。

評価者アクションエレメント:

ASE_OBJ.2.1E　評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

6.2.4.5 派生したセキュリティ要件 (ASE_REQ.2)

開発者アクションエレメント::

ASE_REQ.2.1D 開発者は、セキュリティ要件の説明を提供しなければならない(shall)。

ASE_REQ.2.2D 開発者はセキュリティ要件の根拠を提供しなければならない(shall)。

内容と記述エレメント:

ASE_REQ.2.1C セキュリティ要件の説明は SFR と SAR について記述するものとします。

ASE_REQ.2.2C すべてのサブジェクト、オブジェクト、操作、セキュリティ属性、外部エンティティ及び SFR と SAR において使用されたその他の用語がすべて定義されなければならない(shall)。

ASE_REQ.2.3C セキュリティ要件の説明は、セキュリティ要件についてのすべての操作を識別するものとする。

ASE_REQ.2.4C すべての操作は正しく実行されるものとする。

ASE_REQ.2.5C セキュリティ要件の各々の依存性は、満たされるか、又は、セキュリティ要件の根拠は、満たされていない依存性を正当化するものとする。

ASE_REQ.2.6C セキュリティ要件の根拠は、各 SFR を TOE のセキュリティ対策方針までトレースしなければならない(shall)。

ASE_REQ.2.7C セキュリティ要件の根拠は、SFR が、TOE のセキュリティ対策方針にすべて適合することを説明しなければならない(shall)。

ASE_REQ.2.8C セキュリティ要件の根拠は、SAR が選ばれた理由を説明しなければならない(shall)。

ASE_REQ.2.9C セキュリティ要件の説明は内部的に一貫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:

ASE_REQ.2.1E 評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

6.2.4.6 セキュリティ課題の定義 (ASE_SPD.1)

開発者アクションエレメント:

ASE_SPD.1.1D 開発者は、セキュリティ課題の定義を提供しなければならない(shall)。

内容と記述エレメント:

ASE_SPD.1.1C セキュリティ課題の定義は、脅威について記述しなければならない(shall)。

ASE_SPD.1.2C すべての脅威は、脅威のエージェント、資産及び有害なアクションの用語で記述しなければならない(shall)。

ASE_SPD.1.3C セキュリティ課題の定義は、OSP について記述しなければならない(shall)。

ASE_SPD.1.4C セキュリティ課題の定義は、TOE の運用環境に関する想定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:

ASE_SPD.1.1E 評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

6.2.4.7 TOE の要約仕様 (ASE_TSS.1)

開発者アクションエレメント:

ASE_TSS.1.1D 開発者は、TOE の要約仕様を提供しなければならない(shall)。

ASE_TSS.1.1C TOE の要約仕様は、TOE が各 SFR にどのように適合するか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:

ASE_TSS.1.1E 評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

ASE_TSS.1.2E 評価者は、TOE の要約仕様が TOE の概要及び TOE の説明と一致していることを確認しなければならない(shall)。

6.2.5 クラス ATE : テスト

テストは、設計又は実装の弱さを利用する観点だけでなく、システムの機能的な観点に対しても規定される。前者は ATE_IND ファミリを通じて行なわれ、一方後者は AVA_VAN ファミリを通じて行なわれる。本 PP で規定される保証レベルでは、テストは設計情報の利用可能性に依存して、広告された機能性及びインタフェースに基づく。評価プロセスの主要なアウトプットの一つは、次の要件の中で特定されるテスト報告である。

6.2.5.1 独立テスト-適合性 (ATE_IND.1)

テストは、提出された管理上の(設定と運用を含む)文書だけでなく、TSS に記載された機能性も確認するために実行される。テストの焦点は、ある追加のテストが 6.2 の SAR として特定されているが、各 SFR で特定された要件が満たされていることを確認することである。保証アクティビティは、これらのコンポーネントに関連する最小限のテスト・アクティビティを識別する。評価者は、テストの計画と結果を文書で証明するテスト報告書、並びに、本PP への適合性を表示しているプラットフォーム/TOE コンビネーションに焦点を置くカバレージ論証を作成する。

開発者アクションエレメント:

ATE_IND.1.1D 開発者はテストに対する TOE を提供しなければならない(shall)。

内容と記述エレメント:

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と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

ATE_IND.1.2E 評価者は、指定されたように TSF が作動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、システムのテスト側面を文書で証明するテスト計画及び報告書を準備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テストアクションをすべてカバーする。保証アクティビティにリストされているテストごとにテストケースがある必要はない一方、評価者は、ST の適切なテスト要件がカバーされていることをテスト計画の中で文書で証明しなければならない。

テスト計画は、テストされるプラットフォームを識別する。また、テスト計画に含まれないが、ST に含まれるプラットフォームについては、テスト計画は、プラットフォームをテストしないことの正当化の理由を提供する。この正当化は、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の間の相違を取扱い、その相違が実行されるテストに影響しないことを議論しなければならない。その相違による影響はないと単に断言するだけでは十分ではない; 根拠が提供されなければならない。ST 内で表示されるすべてのプラットフォームがテストされる場合、根拠は必要ではない。

テスト計画は、テストされる各プラットフォームの構成、及び AGD 文書に含まれているもの以外に必要なあらゆるセットアップについて記述する。評価者は、各プラットフォームのインストール及びセットアップについて、テストの一部、又は標準プレテスト条件として、AGD 文書に従うと期待されていることに注意すべきである(should)。これは特別なテストドライバー又はツールを含むかもしれない。各ドライバー又はツールに関して、ドライバー又はツールが TOE とそのプラットフォームによる機能性のパフォーマンスに悪影響を及ぼさないことの論証(単なる主張ではない)が提供される。これはまた、使用される暗号エンジンの設定を含む。このエンジンに実装される暗号アルゴリズムは、本PPによって特定されたもので、評価されている暗号プロトコル(IPsec、TLS/HTTPS、SSH)によって使用されてい

る。

テスト計画はハイレベルのテスト目標と、それらの目標を達成するために従うテスト手順を識別する。これらの手順は期待される結果を含む。テスト報告書(単にテスト計画の注釈付きバージョンの可能性もある)は、テスト手順が実行された際に行なわれたアクティビティを詳述し、検査の実際の結果を含む。これは累積的な計算であるものとする。したがって、実行されたテストが不合格に終わり;プログラムの改修が行なわれ、テストが成功裡に再試行される場合、報告書は、単なる「合格」結果だけでなく、「不合格」と「合格」の結果(そしてそれをサポートする詳細)を表示する 。

6.2.6 クラス AVA：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、評価機関は、これらのタイプの製品にどの脆弱性が発見されてきたかを発見するため、オープンソースを調査することが期待される。ほとんどの場合、これらの脆弱性は、最低レベルの攻撃者を越える複雑さを必要とする。侵入ツールが作成され、一様に評価機関に配布されるまで、評価者は、TOE の中のこれらの脆弱性に対するテストをしないよう求められる。ベンダーから提供される文書に載っているこれらの脆弱性の可能性に関して評価機関がコメントすると期待されるだろう。この情報は、侵入テストツールの開発において、及び将来のプロテクションプロファイルの開発のために使用される。

6.2.6.1 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 開発者はテストに対する TOE を提供しなければならない(shall)。

内容と記述エレメント:

AVA_VAN.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:

AVA_VAN.1.1E 評価者は、提供された情報が証拠の内容と記述に係るすべての要件を満たすことを確認しなければならない(shall)。

AVA_VAN.1.2E 評価者は、TOE の潜在的な脆弱性を識別するためにパブリックドメインソースのサーチを実行しなければならない(shall)

AVA_VAN.1.3E 評価者は、識別された潜在的な脆弱性に基づいて、TOE が最低レベルの攻撃の可能性を持つ攻撃者によって実行される攻撃に耐性があるかどうかを判断するため、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、この要件に関して、彼らの調査結果を文書で証明するために報告書を作成しなければならない(shall)。この報告書は、実体的に ATE_IND で言及された全体的なテスト報告書の一部、又は個別の文書でありえる。評価者は、特定の TOE に関係する脆弱性だけでなく、一般的に ESM アプリケーションのこのカテゴリー内で見つかった脆弱性を判断するために、公開情報のサーチを実行する。評価者は、調べた情報源及び報告書で見つかった脆弱性を文書で証明する。見つかった各脆弱性については、評価者は、非適用範囲に関して根拠を提供するか、又は、脆弱性を確認するために、適切であれば、(ATE_IND 内で提供されるガイドラインを使用して)テストを考案する。適合性は、脆弱性を利用するために必要とされる攻撃のベクトルを査定することにより判断される。例えば、ブートアップのキーコンビネーションを押すことで脆弱性を検知することができれば、テストは本 PP の保証レベルで適切だろう。脆弱性の活用が、例えば、電子顕微鏡と液体窒素を必要とすれば、テストは適切ではないし、また、適切な正当化が考案される 。

6.3 セキュリティ保証要件根拠

これらのセキュリティ保証要件を選択する根拠は、これがこの技術の最初の米国政府プロテクションプロファイルであるということである。これらのタイプの製品において脆弱性が見つかる場合は、より厳格なセキュリティ保証要件が、実際のベンダーの慣行に基づいて義務付けられる。

7 セキュリティ課題定義根拠

本節は、前提条件と環境上の対策方針との間のマッピングだけでなく、セキュリティ課題の定義で定義された脅威と対策方針との間のマッピングも識別する。さらに、マッピングが適切であると理解できるように、リストされた対策方針を満たすのに使用される SFR に基づいて、根拠が提供される。これらのマッピングが PP の適合性を説明するために必ずしも存在する必要のない状況では、ST 執筆者に役立つよう、太字のテキストが根拠の終わりに追加された。

表 5 – 前提条件、環境上の対策方針及び根拠

前提条件	対策方針	根拠
A.AUDIT –TOE は、セキュリティデータを共有するため、他の ESM 製品への接続を設定することができるだろう。	OE.AUDIT－運用環境は監査データのストレージのため、離れた場所を提供する。	監査データの保存のために離れた場所を提供するよう OE に求めることは、FAU_STG_EXT.1 が満たされることを可能にする。
A.POLICY– TOE は運用環境からポリシーデータを受信する。	OE.POLICY－運用環境は、TOE が実施するポリシーを提供する。	TOE にポリシーを提供するよう OE に求めることは、TOE がその中核機能性によって機能することを可能にする。
A. USERID－TOE は運用環境から有効な識別・データを受信する。	OE. USERID－運用環境は、利用者を識別し、TOE にこの確認を伝えることができなければならない（must）。	どの利用者がアクセス制御機能性についてのデータへのアクセスを要求するかについての情報を TOE が持つように、TOE に対し確認された利用者識別を確認し、提供することが必要である。

脅威	対策方針	根拠
A. INSTAL－TOE をインストールするために提供されたガイダンスに従う、適任で高信頼の管理者がいるだろう。	OE. INSTAL－TOE に責任を負う者は、TOE が管理ガイダンスと一致する方法で提供され、インストールされることを確実にしなければならない（must）。	TOE をセットアップするために 1 人以上の管理者を提供することは、それが適任の個人によってインストールされるだろうという想定を満たすのに役立つ。
A. TIMESTAMP－TOE は、運用環境から、高信頼タイムスタンプを受信する。	OE. TIME- 運用環境は TOE に高信頼タイムスタンプを提供しなければならない。	高信頼タイムスタンプの提供は、正確な監査記録を確実にする。

表 6 －脅威、対策方針及び根拠

脅威	対策方針	根拠
T.DISABLE –悪意のある利用者又は不注意な利用者は、TOE の操作を停止又は終了し、したがって、環境又は TOE の保護されたデータへのアクセス制御を実施できなくする。	O. RESILIENT－TOE が操作システム上の資源に対して利用者によって実行されるアクションを補正する場合、当該利用者は、TOE のふるまいを無効にし、さもなければ修正する資源を変更することは決してできないものとする。	FDP_ACC.1 FDP_ACF.1 FPT_FLS.1 (optional) TOE が操作システムのオブジェクトを保護することができる場合、本 PP 内で規定される FDP の要件は、TOE のふるまいを構成するかふるまいに影響するオブジェクトを保護することを TOE に要求する。 TOE がこのようにそれ自体を保護しない場合、ST 執筆者はこのマッピングを除去することができる。 O.RESILIENT 又は OE.PROTECT の少なくとも 1 つはこの脅威の緩和のためにマップされるべきである。

脅威	対策方針	根拠
	OE. PROTECT –運用環境は、TOE をその機能及びデータに対する無許可の修正及びアクセスから保護する。	運用環境は、環境上のリポジトリ又はランタイムメモリに保存される TSF データを保護するために使用してもよい。 例えば、監査又はポリシーのデータは環境上の SQL データベースに保存してもよい。 TOE がこのようにそれ自体を保護しない場合、ST 執筆者はこのマッピングを除去することができる。 O.RESILIENT 又は OE.PROTECT の少なくとも 1 つはこの脅威の緩和のためにマップされるべきである。
T.EAVES –TOE データへの不正アクセスを獲得するために、悪意のある利用者はネットワークのトラフィックを盗み聞きすることができる可能性がある。	**O. MNGRID** –TOE は、それからポリシー・データを受ける前にポリシー管理製品を識別し、認可することができる。	**FTP_ITC.1(1)** **FTP_ITC.1.3(2)** 高信頼チャンネルの確立を通じて、各々の ESM コンポーネントは、それに接続する他のあらゆるコンポーネントの識別を保証しているだろう。 したがって、高信頼チャンネルが TOE とそのポリシー管理製品の間で確立されれば、それらのコンポーネントの各々は、その他の真正性を保証する。

脅威	対策方針	根拠
T.FALSIFY –悪意のある利用者は、ポリシー管理製品にTOEがポリシーを実施しているという偽りの保証をすることで、TOE の識別を変造することができる。	O. SELFID –TOE は、新しいポリシー到着の受領書を送信する間に、ポリシー管理製品への識別を確認することができる。	FCO_NRR.2 ポリシー管理製品にポリシー受領書の証明可能な証拠を提供することによって、TSF は、それが正しいポリシーを実装しているという保証をすることができる。
T.FORGE –悪意のある利用者は、偽りのポリシーを作成し、そのふるまいを悪い方に変更して使うように、TOE にそれを送信する。	O. INTEGRITY –TOE は、ハッシュ法及び鍵付き メッセージ認証モードの中でセキュアなハッシュアルゴリズムを使用して、運用環境コンポーネントからの転送データの完全性を確認する能力を含む。	FTP_ITC.1.3(2) FCS_CKM.1.1 (optional) FCS_CKM_EXT.4 (optional) FCS_COP.1(1)(optional) FCS_COP.1(2) (optional) FCS_COP.1(3)(optional) FCS_COP.1(4) (optional) FCS_RBG_EXT.1(optional) 他の ESM 製品からの送信データ上でハッシュ値の算出又は電子署名を実行するよう TOE に要求することによって、TOE は、転送データは ESM 製品によって転送されるよう意図されたデータであり、第三者によって傍受されたり変更されたりすることはなかったことについて合理的な保証を得ることができる。

脅威	対策方針	根拠
	O. MNGRID –TOE は、それからポリシー・データを受ける前にポリシー管理製品を識別し、認可することができる。	FTP_ITC.1(1) FTP_ITC.1.3(2) 高信頼チャンネルの確立を通じて、各々の ESM コンポーネントは、それに接続する他のあらゆるコンポーネントの識別を保証する。 したがって、高信頼チャンネルが TOE とそのポリシー管理製品の間で確立されれば、それらのコンポーネントの各々はその他のものの真正性を保証する。
T. MASK –悪意のある利用者は、彼らのアクションを隠そうとする、それによって、監査データは不正確に記録されたり、記録されなかったりする。	O. MONITOR –TOE は、自身のふるまいの、変則的なアクティビティを監視する（例えば、利用者による TOE の保護された資源へのアクセスの試みを検知する、セキュリティ関連事象を生成するための手段を提供する）。	FAU_GEN.1 FAU_SEL.1 FAU_STG.1 FAU_STG_EXT.1 TOE の監視生成能力が適切に機能すれば、それらのアクションを隠そうとする悪意のある利用者によるどんな試みも失敗する。

脅威	対策方針	根拠
T.NOROUTE –悪意があるか不注意な利用者は、TOE に、そのポリシーを実施する源への接続を失わせ、アクセス制御のふるまいに悪い影響を与えることもある。	O.MAINTAIN –もしポリシー管理から分離されれば、TOE はポリシー実施を維持することができる。	FPT_FLS_EXT.1 FRU_FLT.1 TOE のフォールトトレランス要件は、ポリシー管理製品と通信することができないときに、TOE が講ずるべき措置を定義する。これは、接続の問題が TOE のアクセス制御 SFP の実施を妨害しないだろうと保証する。また、それらは、通信が再確立された時、TSF は、2 つのコンポーネントが接続されない間に最近のポリシーデータが生成されたとしても、直ちにそれを実施するということを確実にする。
T.OFLOWS –悪意のある利用者は、そのアクセス制御方針実施のふるまいを変更するために、TOE に正しくないポリシー管理データを提供しようとする。	O.OFLOWS –TOE は利用者による無効か悪意のあるインプットを認識し、廃棄することができる。	FTP_ITC.1.3(2) FPT_RPL.1 この対策方針の意図は、ポリシーデータが既知の高信頼のソースから生じたもので、情報のリプレイを表わすものではないことを確実にすることである。

脅威	対策方針	根拠
T.OFLOWS –悪意のある利用者は、そのアクセス制御方針実施のふるまいを変更するために、TOE に正しくないポリシー管理データを提供しようとする。	O.MNGRID –TOE は、それからポリシーデータを受ける前にポリシー管理製品を識別し、認可することができる。	FTP_ITC.1(1) ESM コンポーネントの保証された識別を要求することによって、ポリシーデータの有効なソースとして、攻撃者は、彼らの識別を確かめられることができないので、TOE に正しくないポリシー管理データを提供することはできない。
T.UNAUTH –悪意があるか不注意な利用者は、機密データの漏洩を引き起こしたり、システムのふるまいに悪影響を与えたりする運用環境内のオブジェクトにアクセスする。	O.DATAPROT –TOE は、ポリシー管理製品によって作りだされたアクセス制御方針の実施により、無許可の修正からデータを保護する。	ESM_DSC.1(optional) FDP_ACC.1 FDP_ACF.1 FMT_MOF.1(1) FMT_MOF.1(2) FMT_MSA.1 FMT_MSA.3 FMT_SMF.1 FMT_SMR.1 FTA_SSL_EXT.1(optional) FTA_SSL.3(optional) FTA_SSL.4(optional) FTA_TSE.1(optional) TOE の主要な目的はサブジェクトとオブジェクトの間のアクセスを制限することである。 運用環境内のオブジェクトに対するアクセス制御方針を実施する TOE の能力は、この目的が果たされることを可能にする。 アクセス制御方針を実施するために、TOE は、そのようなポリシーの能力が設定されることを必要とする。 ポリシーが実施されているという保証をするために、TOE は、問い合わせされるポリシーの能力を必要とす

		る。
P.UPDATEPOL –組織は、TOE が関連するポリシーデータで更新されることを確実にするため、デューディリジェンスを行なう。	**O.SELFID** –TOE は、新しいポリシー到着の受領書を送信する間に、ポリシー管理製品への識別を確認することができる。	**FCO_NRR.2** 最新のポリシーデータが受信されている証拠を提供するTOEの能力は、組織が、ポリシーデータが最新のものに維持されていることを確かめることを助ける。

8 セキュリティ課題定義

次節は、PP の前提条件、脅威及び対策方針をリストアップする。

8.1 前提条件

次の小節にリストアップされた特定の条件が TOE の運用環境に存在することが想定されている。これらの前提条件は、TOE セキュリティ要件の策定において、現実的に実現するもの、及び TOE の使用の際の必須の環境条件の両方を含んでいる。

8.1.1 接続性の前提条件

表 7 –TOE の前提条件

前提条件の名称	前提条件の定義
A. AUDIT	保護されたリポジトリは、監査データが書面になりうる運用環境に存在する。
A.POLICY	TOE は運用環境からポリシーデータを受信する。
A.USERID	TOE は運用環境から有効な識別・データを受信する。
A.TIMESTAMP	TOE は運用環境から高信頼タイムスタンプを受信する。

8.1.2 物理的な前提条件

TOE のアーキテクチャが変わる可能性があるので、物理的な前提条件は本プロテクションプロファイル内では規定されない。ST 執筆者は、TOE の期待される用法と一致している前提条件を加えるべきである。

8.1.3 人的な前提条件

表 8 –TOE の前提条件

前提条件の名称	前提条件の定義
A.INSTAL	TOE をインストールするために提供されたガイダンスに従う、適任で高信頼の管理者がいる。

8.2 脅威

TOE は、可能性として別々に獲得されたデバイスなので、何らかの直接利用者と接するインタフェースを持つとは期待されていない。TOE に唯一期待されるインタフェースは、設定ファイル、TOE を管理するために使用された ESM 製品への論理インタフェース(ポリシー管理製品)、監査コンポーネントへの論理インタフェース、及び ESM を貫通する要求されたアクセスを傍受するインタフェースである 。TOE は、それが PM から受信するデータは真正であるという保証を必要とするので、PM と TOE の間のリンクは保護するべき重要なインタフェースである。同等に重要なのは、TOEとその関連する設定ファイルの間のリンクである。TOE が既知の状態で作用できるように、TOE は、これらのファイルにおける設定データの完全性について保証を得る必要がある。PM は、ポリシーが信頼されたエンティティのみに送信されるように、TOE と、それが実装されているポリシーのバージョンの真正性を確かめるメカニズムを必要とする。TOE に対してあてはまる脅威は以下にリストアップされている。これらの脅威は、TOE に不正確な機能を引き起こす、又は攻撃者が許可なく TOE セキュリティ機能(TSF)のデータを得る可能性のある攻撃に関係する。

表 9 –脅威

脅威の名称	脅威の定義
T.DISABLE	悪意のある利用者又は不注意な利用者は、TOE の操作を停止又は終了し、したがって、環境又は TOE の保護されたデータへのアクセス制御を実施できなくなる。
T.EAVES	TOE データへの不正アクセスを獲得するために、悪意のある利用者はネットワークのトラフィックを盗み聞きすることができる。
T.FALSIFY	悪意のある利用者は、ポリシー管理製品に TOE がポリシーを実施しているという偽りの保証をすることで、TOE の識別を変造することができる。
T.FORGE	悪意のある利用者は、偽りのポリシーを作成し、そのふるまいを悪い方に変更して使うように、TOE にそれを送信する。
T.MASK	悪意のある利用者は、彼らのアクションを隠そうとする、それによって、監査データは不正確に記録されたり、記録されなかったりする。
T.NOROUTE	悪意があるか不注意な利用者は、TOE に、そのポリシーを実施する源への接続を失わせ、アクセス制御のふるまいに悪い影響を与えることもある。
T.OFLOWS	悪意のある利用者は、そのアクセス制御方針実施のふるまいを変更するために、TOE に正しくないポリシー管理データを提供しようとする
T.UNAUTH	悪意があるか不注意な利用者は、機密データの漏洩を引き起こしたり、システムのふるまいに悪影響を与えたりする運用環境内のオブジェクトにアクセスする。

8.3 組織のセキュリティ方針

次の組織のセキュリティ方針は TOE を配置する組織で使用されると予想される。

表 10 –組織のセキュリティ方針

方針の名称	方針の定義
P.UPDATEPOL	組織は、TOE が関連するポリシーデータで更新されることを確実にするため、相当な注意を払う。

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緩和されることを確実にするために、TOE と運用環境の両方についてセキュリティ対策方針を満たさなければならない。それらは以下の節でリストアップされている。

8.4.1 TOE のセキュリティ対策方針

次のセキュリティ対策方針は TOE の期待される特性である。

表 11 –TOE のセキュリティ対策方針

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針の定義
O.MONITOR	TOE は、自身のふるまいの変則的なアクティビティを監視する(例えば、利用者による TOE の保護された資源へのアクセスの試みを検知する、セキュリティ関連の事象を生成するための手段を提供する)。
O.DATAPROT	TOE は、ポリシー管理製品によって作りだされたアクセス制御方針の実施により、無許可の修正からデータを保護する。
O.INTEGRITY	TOE は、ハッシュ法及び鍵付きのメッセージ認証モードの中でセキュアなハッシュアルゴリズムを使用して、運用環境コンポーネントからの転送データの完全性を確認する能力を含むでしょう。
O.RESILIENT	TOE が操作システム上の資源に対して利用者によって実行されるアクションを補正する場合、システム管理者又は利用者は、TOE のふるまいを無効にし、さもなければ修正する運用環境において操作を実行することは認められないものとする。

O.MAINTAIN	もしポリシー管理製品から分離されれば、TOE はポリシー実施を維持することができるだろう。
O.OFLOWS	TOE は利用者による無効か悪意のあるインプットを認識し、廃棄することができるだろう。
O.SELFID	TOE は、新しいポリシー到着の受領書を送信する間に、ポリシー管理製品への識別を確認することができるだろう。
O.MNGRID	TOE は、それからポリシーデータを受ける前にポリシー管理製品を識別し、認可することができるだろう。

8.4.2 運用環境のセキュリティ対策方針

次のセキュリティ対策方針は、TOE が配置される運用環境の期待する特性である。

表 12－ 運用環境のセキュリティ対策方針

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針の定義
OE. AUDIT	運用環境は監査データのストレージのため、離れた場所を提供する。
OE.INSTAL	TOE に責任を負う者は、TOE が IT セキュリティと一致する方法で提供され、インストールされ、管理され、操作されることを確実にしなければならない(must)。
OE.POLICY	運用環境は、TOE が実施するポリシーを提供する。
OE.PROTECT	運用環境は、TOE をその機能及びデータに対する無許可の修正及びアクセスから保護する。
OE.USERID	運用環境は、利用者を識別し、TOE にこの確認を伝えることができなければならない(must)。
OE.TIME	運用環境は TOE に高信頼タイムスタンプを提供しなければならない(must)。

附属書 A　サポート表と参考文献

A.1　参考文献

[1] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Policy Management, version 1.0, forthcoming

[2] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Authentication Server, version 1.0, forthcoming

[3] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Secure Configuration Management, version 1.0, forthcoming

[4] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Audit Management, version 1.0, forthcoming

[5] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Authentication Server, version 1.0, forthcoming

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

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

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

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

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

[11] National Institute of Standards and Technology, FIPS PUB 197 Advanced Encryption Standard, November 2001

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

2001　Standard Protection Profile for Enterprise Security Management Access Control

[13] 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

[14] 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

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

[16] 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

[17] National Institute of Standards and Technology. "Recommended Security Controls for Federal Information Systems and Organizations". NIST SP 800-53 Revision 3 Errata 1. May 1, 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 Standard Protection Profile for Enterprise Security Management Access Control

[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

A.2 頭字語

表 13- 頭字語と定義

頭字語	定 義
ABAC	Attribute-Based Access Control(属性ベースのアクセス制御)
CC	Common Criteria(コモンクライテリア)
CM	Configuration Management(構成管理)
COI	Communities of Interest(利益共同体)
DAC	Discretionary Access Control(自由裁量のアクセス制御)
ESM	Enterprise Security Management(エンタープライズセキュリティ管理)
IT	Information Technology(情報技術)

頭字語	定 義
MAC	Mandatory Access Control（強制アクセス制御）
NAC	Network Access Control（ネットワークアクセス制御）
NIST	National Institute of Standards and Technology（米国国立標準技術局）
OE	Operational Environment（運用環境）
OS	Operating System（運用システム）
OSP	Organizational Security Policy（組織のセキュリティ方針）
PII	Personally Identifiable Information（個人識別情報）
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）
RBAC	Role-Based Access Control（役割ベースのアクセス制御）
SAC	System Access Control（システムアクセス制御）
SAR	Security Assurance Requirement（セキュリティ保証要件）
SFP	Security Function Policy（セキュリティ機能ポリシー）
SFR	Security Functional Requirement（セキュリティ機能要件）
SQL	Structured Query Language（構造化照会言語）
ST	Security Target（セキュリティターゲット）
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）
TSP	TOE Security Policy（TOE セキュリティポリシー）

附属書 B -NIST SP 800-53/CNSS 1253 マッピング

本節は、履行するために TOE が使用することができる他の関連する標準からの要件を示すデータをリストアップする。この情報は CC の観点からは必要ではないが、セキュリティターゲットにそれを含めることは、複数の基準への適合性がその配置には必要な場合に減らすことができる余分な作業を識別する際、読者の助けになるだろう。

下記の表は、本 PP の一部として定義された機能的な及び保証の要件、そしてそれらに適用される NIST 800-53 セキュリティ管理をリストアップしている。CC パート 2 及び CC パート 3 で定義された、機能的な及び保証の要件のためのマッピングは、航空宇宙技術運用報告書 TOR-2012(8506)-5「Exploding 800-53:An Analysis of NIST SP 800-53 Revision 3 as Completed by CNSSI 1253″」から導かれた。

以下にリストアップされたガイドラインは、本 PP との厳密な適合性が表示されているという前提条件に基づいていることに注意すること。ST 執筆者が、複数の PP への適合性の表示を通じて TOE を強化している場合、ここで文書化されていない新たな管理が該当する。

表 14 -NIST 800-53 の要件の互換性

CC SFR/SAR		NIST 800-53 管理		コメントと確認
コモンクライテリアバージョン 3 x セキュリティ機能要件(SFR)及び PP 拡張 SFR				
ESM_DSC.1	**オブジェクトインベントリー** オブジェクトインベントリー	AU-13	**情報公開に対する監視**|無許可の流出の検知	**完全。**この制御は、SFR によって完全に履行されているように見える。
		AC-4	**アクセス実施**|承認された認可の実施	**部分的。**この制御は、オブジェクトが承認された状態にない場合に検知することにより、アクセス実施を維持するのに役立つために使用することができる。
FAU_GEN.1	**セキュリティ監査データ生成** 監査データ生成	AU-2	**監査対象事象**| [監査対象事象]、根拠と調整	**部分的。**FAU_GEN.1.1 は、(この制御の大部分を取り扱って)どんな事象を監査しなければならないかを定義する。しかし、セットが同等かどうか確かめるために割付を比較する必要がある。また FAU_GEN が監査可能であり、監査された CC SFR/SAR NIST

CC SFR/SAR		NIST 800-53 管理		コメントと確認
				800-53 制御コメント及び確認を意味し、それは 800-53 の下で 2 つの別個の制御であることに注意すること。
		AU-12	**監査生成** | [コンポーネント]上で作成しあらかじめ選択する。	部分的。FAU_GEN の生成面は、AU-12 の生成面を提供する。
		AC-17(1)	**リモートアクセス**| 自動監視/制御	**部分的。**FAU_GEN.1 の割付がリモートアクセスの監査を含んでいる場合、この制御は部分的に適合される(監視側面)。
		AU-3	**監査記録の内容** |最小限の監査記録情報	**部分的。**FAU_GEN.1.2 は、各監査記録に含まれているに違いないもののリストを詳述する。 AU-3/AU-3(1)が満たされるかを確かめるために割付を制御と比較しなければならない。
		AU-3(1)	**監査記録の内容** |付加的な詳細な情報:[リスト]	**部分的。**FAU_GEN.1.2 は、各監査記録に含まれているに違いないもののリストを詳述する。 AU-3/AU-3(1)が満たされるかを確かめるために割付を制御と比較しなければならない。
		注:SFR は、監査対象事象を、情報の望ましいレベル(最小限、基礎的、など)だけでなく、セキュリティターゲットに含まれるその他の SFR に基づかせる。CNSS は NSS に定義を提供するが、NIST は定義済みのセットを持っていない。SFR と NIST の割付間に義務付けられた相関性はない。		

CC SFR/SAR		NIST 800-53 管理		コメントと確認
FAU_SEL.1	**セキュリティ監査事象選択** 選択的監査	AU-12	**監査生成** [コンポーネント]上で作成しあらかじめ選択する。	**部分的。**FAU_SEL.1 は AU-12 制御の項目 b に行く。FAU_SEL.1 SFR は、選択のために必要なものの用語の点で、AU-12 の制御よりはるかに弾力的である。
FAU_STG.1	**保護された監査証跡ストレージ(ローカルストレージ)**	AU-9	**監査情報の保護** 不正アクセスから情報/ツールを保護する。	**部分的。**FAU_STG.1.2 は、CC SFR/SAR NIST 800-53 制御コメントと確認「防ぐ」で完成する必要がありうるが、SFR は制御の基本的な意図に対処する。しかしながら、その制御は証跡だけでなく、(SFR によってカバーされない)監査用具も保護する。
FAU_STG_EXT.1				**部分的。**監査データが書き込まれるリポジトリ/エンティティは次にそのデータの無許可の修正を防がなければならないが、SFR は制御の基本的な意図に対処する。しかしながら、その制御は証跡だけでなく、(SFR によってカバーされない)監査用具も保護する。
FCO_NRR.2	**受領の非否認 受領の実施された証拠**	AU-10	**非否認**否認に対する保護	**部分的。**この SFR は、特定のアクションの領収書の非否認について論じる; 受領書の非否認は制御で言及される行為のうちの 1 つである。フレーズ「特定

CC SFR/SAR		NIST 800-53 管理		コメントと確認
				のアクション」は曖昧なので、SFR の中の割付に十分一致できる。
		AU-10(1)	**非否認|** 情報と情報製作者の識別を関連させる。	**部分的。**受領書の証拠については、これは、FCO_NRR.2.2 に一致するように見える。
		AU-10(2)	**非否認|** 識別及び情報結合を確認する。	**部分的。**受領書の証拠については、これは、FCO_NRR.2.3 に一致するように見える。
FCS_CKM.1	**暗号鍵管理** **暗号鍵生成**	SC-12	**暗号鍵設定及び管理 |** 組織は暗号鍵を設定/管理する。	**部分的。**SFR は、800-53 制御の側面のうちの 1 つに対処する。標準とプロトコルの割付を必要とされた機能強化と比較する必要がある。
		注:NIST 800-53 の制御は、鍵管理(生成、分散、アクセス及び破棄)の多様な側面を区別しない。		
FCS_CKM_EXT.4	**暗号鍵管理** 暗号鍵破棄	SC-12	**暗号鍵設定及び管理|** 組織は暗号鍵を設定/管理する。	**部分的。**SFR は、800-53 制御の側面のうちの 1 つに対処する。標準とプロトコルの割付を必要とされた機能強化と比較する必要がある。
		注:NIST 800-53 の制御は、鍵管理(生成、分散、アクセス及び破棄)の多様な側面を区別しない。		
FCS_COP.1	**暗号操作** 暗号操作	SC-13	**暗号の使用|** 規制を満たすモジュールを通じた暗号の実装	**部分的。**SFR がその制御を満たす範囲は、割付がどのように完成したかに依存する。
		注:SFR は非常に広範で、暗号操作の種類をすべてカバーするために完成してもよい。それらの多くは、NIST800-53 の SFR ではカバーされない。NIST		

CC SFR/SAR		NIST 800-53 管理		コメントと確認
		でカバーされないエリアの例には、セキュアな暗号ハッシュの標準及びそれらがいつ使用されねばならないか、そして、使用される乱数生成器の品質の標準を含む		
FCS_RBG_EXT.1	**ランダムビット生成** ランダムビット生成			**マッピングなし。**これに対応する制御はないように見える。SFR は、乱数生成の期待される特性を定義する。
FDP_ACC.1	**アクセス制御方針** サブセットアクセス制御	AC-3	**アクセス実施** システム実施の権限	**部分的。**アクセス制御は、ポリシーによって制御されたオブジェクトの仕様を意味する。しかし、NIST はサブセットと完全なアクセス制御を区別しない。
		AC-3(3)	**アクセス実施** 非自由裁量アクセス制御	**部分的。**役割についてのオブジェクトに対してカバーされる操作を特定するために、適切な割付が必要とされるだろう。
		AC-3(4)	**アクセス実施** 自由裁量のアクセス制御	**部分的。**サブジェクトのために指定されたオブジェクトに対して、カバーされる操作を特定するために、適切な割付が必要とされるだろう。
		SC-7	**境界保護** システムモニターと境界での通信の制御	**部分的。**TOE がデータ喪失防止アクセス制御を実行する場合、それはデータの流出に関係する通信を制御することができる。TOE がウェブアクセス制御を実行する場合、それは内部か外部のウェブサーバを巻きこむ通信を制

CC SFR/SAR		NIST 800-53 管理		コメントと確認
				御することができる。
		注: サブジェクト、オブジェクト及び対象の属性を定義する FDP_ACC ファミリ並びに、サブジェクトがそれらの属性に基づいてどのようにオブジェクトにアクセスするかを定義するアクセス制御規則を定義する FDP_ACF ファミリとともに、CC はアクセス制御について異なるアプローチをする。		
FDP_ACF.1	**アクセス制御機能** セキュリティ属性ベースのアクセス制御	AC-3	**アクセス実施** システム実施の権限	**部分的。**これはアクセス実施の一般的な考え方を把握する。何らかのポリシーの点では特定されていない。これを明確にする補足のガイダンスは、DAC と同様に MAC にも使用できる可能性があり、したがって、FDP_ACF 又は FDP_IFF のいずれかはこれを適合することができる可能性がある。
		AC-3(3)	**アクセス実施** 非自由裁量アクセス制御	**部分的。**FDP_ACF が RBAC ポリシーを特定するために使用されれば、それは AC-3(3)の下での適切な割付になるだろう。
		AC-3(4)	**アクセス実施** 自由裁量のアクセス制御	**部分的。**FDP_ACF が旧来の DAC ポリシーを特定するために使用されれば、それは AC-3(4)の下での適切な割付になるだろう。
		SC-7	**境界保護** システムモニターと境界での通信の制御	**部分的。**TOE がデータ喪失防止アクセス制御を実行する場合それはデータの流出に関係する通信を制御することができる。TOE がウェブアクセス制御を実行する場合、それ

CC SFR/SAR		NIST 800-53 管理		コメントと確認
				は内部か外部のウェブサーバを巻きこむ通信を制御することができる。
		注: FDP_ACF の一般的な柔軟性により、広範な情報の流れのポリシーが特定されることを可能にする。実際には、FDP_ACFを使用して、AC-3 の多くのポリシーを書き込むことができ、したがって、人は割付を入念に見る必要がある。		
FMT_MOF.1	**TSF における機能の管理** セキュリティ機能のふるまいの管理	AC-3(3)	**アクセス実施** 非自由裁量アクセス制御	**部分的。**特別の役割への管理機能の制限は、少なくとも RBAC の部分的な実装である。
FMT_MSA.1	**セキュリティ属性の管理** セキュリティ属性の管理	SI-9	**情報入力の制限** 情報を入力することができるのは権限のある人に限られる。	**部分的。** SFR ははるかにより特定のものであるが、SFR はこの制御を意味するように見えるだろう。

CC SFR/SAR		NIST 800-53 管理		コメントと確認
FMT_MSA.3	**セキュリティ属性の管理** 静的属性の初期化			**マッピングなし。**この SFR に対応する制御はないように見える。SFR は、TOE に対し、オブジェクト又は情報が作成される場合に、[割付:認可され、識別された役割]が、デフォルト値を無効にする代替の初期値を特定することを許可するだけでなく、セキュリティポリシーを実施するために使用されるセキュリティ属性に、[選択、次の一つを選択する:限定的な、任意の[割付:他のプロパティ]]デフォルト値を提供することを要求する。
FMT_SMF.1	**管理機能の仕様** 管理機能の仕様			**マッピングなし。**この SFR は、他では把握されない管理機能を特定するための、終端を開いた SFR である。それは割付により、ほとんどあらゆる制御に対応できる可能性がある。
		AC-5	**任務のセパレーション** 組織レベル	**部分的。**ほぼ間違いなく、システムが別の役割を提供する場合、それは任務のセパレーションの提供及び最小特権の原則の適用をサポートする。
		AC-6	**最小特権** 最小特権の概念の使用	**部分的。**ほぼ間違いなく、システムが別の役割を提供する場合、それは任務のセパレーションの提供

CC SFR/SAR		NIST 800-53 管理		コメントと確認
				及び最小特権の原則の適用をサポートする。
FPT_FLS_EXT.1	**フェールセキュア** 通信の障害	SC-7(6)	**境界保護** 境界保護メカニズムが故障する場合、組織は情報又は通信が無許可で境界を越えてリリースされることを防ぐ。	**部分的。**この制御は、境界保護デバイスのセキュアな条件に障害が起きる特別な例である。
		SC-7(18)	**境界保護** 境界保護メカニズムが故障する場合のフェールセキュア	**部分的。**この制御は、境界保護デバイスのセキュアな条件に障害が起きる特別な例である。
		SC-24	**既知の状態での障害** [情報]を保存する[既知の状態]に対する障害	**部分的。**SFR は、既知のセキュアな状態に対する障害を必要とする。それは、SC-24 に適合するように見える。
FPT_FLS.1	**フェールセキュア** セキュアな状態の保存と障害	SC-7(6)	**境界保護** 境界保護メカニズムが故障する場合、組織は情報又は通信が無許可で境界を越えてリリースされることを防ぐ。	**部分的。**この制御は、境界保護デバイスのセキュアな条件に障害が起きる特別な例である。
		SC-7(18)	**境界保護** 境界保護メカニズムが故障する場合のフェールセキュア	**部分的。**この制御は、境界保護デバイスのセキュアな条件に障害が起きる特別な例である。
		SC-24	**既知の状態での障害** [情報]を保存する[既知の状態]に対する障害	**部分的。**SFR は、既知のセキュアな状態に対する障害を必要とする。それは、SC-24 に適合するように見える。
FPT_RPL.1	**リプレイ検知** リプレイ検知	SC-23	**セッションの真正性** 通信セッションの真正性を保護するメカニズム	**部分的。**割付に応じて、リプレイ検知メカニズムはセッション真正性を提供し、中間者攻撃に対処する。

CC SFR/SAR		NIST 800-53 管理		コメントと確認
FRU_FLT.1	**フォールトトレランス** フォールトトレランスの低下			**マッピングなし。**この SFR は、通信の回復の際に、操作がポリシーを訂正することを、TSF が確認することを要求する。特定の障害(それらは、監査障害のように、他の SFR によって実際にはカバーされる)の場合に、NIST 800-53 の制御が継続に対処する場合が多少あるが、一般的なフォールトトレランス要件はない。
FTA_SSL_EXT.1	**セッションのロック及び終了** TSF 起動セッションロック	AC-11	**セッションロック|** 再識別され認証されるまでタイムアウト・ロック	**部分的。**FTA_SSL.1.1 はシステム起動セッションロックを提供する。 FTA_SSL.1.2 は、適切な割付で、アンロックが必要なアクションに対処する。
		AC-11(1)	**セッションロック|** スクリーンセーバーで	**完全。**FTA_SSL.1.1 は、システム起動の,画面の清掃又は上書きを提供する。
		注:FTA_SSL.1 は、利用者起動ロッキングの能力を必要としないので、独力で AC-11 を満たさない。FTA_SSL.1 と FTA_SSL.2 はともに、AC-11 を満たすように要求される。		
FTA_SSL.2	**セッションのロック及び終了** 利用者起動ロッキング	AC-11	**セッションロック|** 再識別され認証されるまでタイムアウト・ロック	**部分的。**FTA_SSL.2.1 は利用者起動セッションロックを提供する。FTA_SSL.2.2 は、適切な割付で、アンロックが必要なアクションに対処する。
		AC-11(1)	**セッションロック|** スクリーンセーバーで	**完全。**FTA_SSL.2.1 は、利用者起動の、画面の清掃又は上書きを提供する。

CC SFR/SAR		NIST 800-53 管理		コメントと確認
		注: FTA_SSL.2 は、利用者起動ロッキングの能力を必要としないので、独力で AC-11 を満たさない。FTA_SSL.1 と FTA_SSL.2 はともに、AC-11 を満たすように要求される。		
FTA_SSL.3	**セッションのロック及び終了** TSF 起動による終了	SC-10	**ネットワーク切断** セッション終了又は[時間]でネットワーク接続を終了する。	**完全。**前の AC-10 は、これがネットワーク終了だけでなくセッション終了を指すことを明確にして、SC-10 に組み入れられたことに留意すること。
FTA_SSL.4	**セッションのロック及び終了** 利用者起動による終了	SC-23(2)	**セッションの真正性** 容易に識別できるセッションログアウト能力を提供する。	**完全。**SFR は、ウェブセッションに係るログアウトの能力があることを意味する。
		注: ウェブ以外のセッションについて、利用者が見ることができるログアウト能力があることを義務づける制御はないように見える。		
FTA_TSE.1	**TOE セッション確立** TOE セッション確立			**マッピングなし。**この SFR は、TOE が[割付:属性]に基づいたセッション確立を拒否することができるよう要求する。これは広範すぎるので、NIST の制御にマップすることができない。
FTP_ITC.1	**TSF 間高信頼チャンネル** TSF 間高信頼チャンネル	IA-3(1)	**デバイスの識別と認証** 双方向の暗号に基づく認証による、遠隔/ワイヤレス接続の前に	**部分的。**SFR は、それ自体と、他の通信チャンネルとは論理上異なる、別の高信頼 IT 製品との間の通信チャンネルの提供について議論し、そのエンドポイントの確実な識別と修正又は漏洩からのチャンネル・データの保護を提供する。この制御は、エンドポイントの識別を提供す

CC SFR/SAR		NIST 800-53 管理		コメントと確認
				る。
FTP_TRP.1	**高信頼パス** 高信頼パス	SC-11	**高信頼パス** 利用者と[機能]の間の高信頼パス	**部分的。**SFR が制御を提供するかどうかは割付に左右される。
コモンクライテリアバージョン 3.x セキュリティターゲット保証要件				
ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**ST 概説** ST 概説			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**適合主張** 適合主張			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**セキュリティ課題定義** セキュリティ課題の定義			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。
ASE_OBJ.1 EAL1	**セキュリティ対策方針** 運用環境のセキュリティ対策方針			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。

CC SFR/SAR		NIST 800-53 管理		コメントと確認
ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**セキュリティ対策方針** セキュリティ対策方針			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**拡張コンポーネントの定義** 拡張コンポーネントの定義			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。
ASE_REQ.1 EAL1	**セキュリティ要件** 述べられたセキュリティ要件			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。
ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**セキュリティ要件** 派生したセキュリティ要件			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。
ASE_SPD.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**セキュリティ課題定義** セキュリティ課題定義			**マッピングなし。**この SAR は、セキュリティターゲットのフォーマットと構造、評価される製品の機能的な保証要件の説明を取扱う。

CC SFR/SAR		NIST 800-53 管理		コメントと確認
ASE_TSS.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**TOE の要約仕様** TOE 要約仕様	SA-4(1)	**獲得 |** 獲得文書は、分析/テストをサポートするためのセキュリティ制御の機能特性について記述する。	**部分的。**ST の中の TSS は、製品がどのようにセキュリティ機能要件を実装するかを記述し、すべてのその後の分析及びテストに対するハイレベルな基礎を提供する。
		SA-5(1)	**情報システム証拠資料|** 組織は、セキュリティ関連の機能特性についてのベンダーの文書を入手する。	**部分的。**ST の中の TSS は、ST で要求されるセキュリティのふるまいに対するセキュリティ関連の機能特性について記述する。
コモンクライテリアバージョン 3.x セキュリティ保証要件				
ADV_FSP.1 EAL1	**機能仕様** 基本機能仕様	SA-4(2)	**獲得|** 獲得文書は、分析/テストをサポートするためのセキュリティ制御の設計/実装について記述する。	**部分的。**ADV_FSP ファミリは、機能的なインタフェースに関する情報を提供する。
		SA-5(2)	**情報システム文書|** 文書は、分析/テストをサポートするセキュリティ関連の外部インタフェースについて記述する。	**部分的。**ADV_FSP ファミリは、機能的なインタフェースに関する情報を提供する。
AGD_OPE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**利用者向け操作ガイダンス** 利用者向け操作ガイダンス	SA-5	**情報システム文書|** SFUG+TFM	**完全。**AGD_OPE は管理者と利用者の文書に対する組み合わせた要件である。
		注: NIST 800-53 は CC v2 アプローチに平行する。それは管理者と利用者の文書(AGD_USR、AGD_ADM)を区別した。CC v3 はこれらを単一の SAR へ結び付けた。その SAR は、一部の製品は管理者以外の利用者を持たないという状況を反映している。		
AGD_PRE.1 EAL1 EAL2 EAL3	**準備手続** 準備手続	SA-5	**情報システム文書|** SFUG+TFM	**完全。**SFR は、セキュアな受入及びセキュアな提供に必要なすべての段階について記述することを要

CC SFR/SAR		NIST 800-53 管理		コメントと確認
EAL4 EAL5 EAL6 EAL7				求する。管理は、文書又はセキュアな設定及びインストールを要求する。
注:800-53 の下の CM と共通の基準の下の CM の間の相違に関する一般的な意見。共通の基準の CM は、システム内の配置ではなく、製品の開発の CM を指す。NIST 800-53 は配置されたシステムの設定を管理することに焦点を置き、開発者の CM についてはそれほど焦点を置かない。				
ALC_CMC.1 EAL1	CM の能力 TOE のラベリング	CM-9	**構成管理計画** 必要な情報を備えた CM 計画を持つ。	**部分的。**これは構成項目の定義に対処する。 ALC_CMC が製品に焦点を置く一方で、CM-9 はシステムに焦点を置いていることに留意すること。
		SA-10	**開発者の構成管理** 開発者は開発の間の構成管理を持つ; 欠点のトラッキング	**部分的。**ALC_CMC は、CM プロセスの開発者の側面のうちの一部をキャプチャーする。
ALC_CMS.1 EAL1	CM の範囲 TOE CM のカバレージ	CM-9	**構成管理計画** 必要な情報を備えた CM 計画を持つ。	**部分的。**これは、設定項目を定義すること及び設定項目の識別の方法に対処する。 ALC_CMC が製品に焦点を置く一方で、CM-9 はシステムに焦点を置いていることに留意すること。
		SA-10	**開発者の構成管理** 開発者は開発の間の構成管理を持つ; 欠点のトラッキング	**部分的。**ALC_CMS は、CM プロセスの開発者の側面のうちの一部をキャプチャーする。
ATE_IND.1 EAL1	独立したテスト 独立したテスト-適合性	CA-2	**セキュリティ評価** 計画を策定、評価、作成、報告。	**部分的。**この制御は、セキュリティ機能に係る独立したテスト計画の開発の側面及びそれらの機能の評価に対処する。

CC SFR/SAR		NIST 800-53 管理		コメントと確認
		CA-2(1)	**セキュリティ評価|** ・・・独立した評価者による	**部分的。**これは、評価がベンダーではなくCCTLによって行われるという事実に対処する。
		SA-11(3)	**開発者のセキュリティ・テスト|** 独立した確認と検証の下にST&Eを実装する。	**部分的。**ATE_INDは、テストスイートの全部又は一部の再実行を含む、確認者による独立したテストを必要とする。
		注: ATE_INDとSA- 11(3)の間に重要な相違がある。ATE_INDは、テストを実行することを独立した評価者に要求する。SA-11(3)には独立した評価者の監督の下にテストを実行する開発者がある。主としてテスト手順の実際の品質と反復性の評価において、このアプローチには重要な相違がある。 **注:** ATE_IND.1のみが、テストスイートの一部に対する独立した監督がある。		
AVA_VAN.1 EAL1	**脆弱性分析** **脆弱性調査**	CA-2(2)	**セキュリティ評価|** [発表された/未発表の]セキュリティ・テスト(例えばペネトレーションテスト)	**部分的。**これは、浸透試験を実施するための要件を取扱う。
		RA-3	**リスク評価|** リスク評価の実施/文書/再検証	**部分的。**考えられる限りでは、リスク評価の一部は、脆弱性に関する調査を行っている。CCは、正式の脆弱性走査を意味しないことに留意すること。それはRA-5である。
		SA-11(2)	**開発者セキュリティ・テスト|** 開発者脆弱性分析	**部分的。**AVA_VANは、実行された脆弱性分析があることを求める。
		注: 別のAVA_VANコンポーネントは、脆弱性分析の深さ及び広がりの点で異なる。NIST SP 800-53改訂3は、脆弱性評価の品質を規定することを制御しないように見える。		

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 アーキテクチャのバリエーション

次のシナリオは、本プロテクションプロファイルを満たす TOE によって実施されるかもしれない、多様なタイプのアクセス制御を取扱う。これらはオプションのコンポーネントではない;それらは、データ保護SFRがどのようにして完成されるべきか、そして、以下に識別されるような機能性を特にサポートするアーキテクチャだけに利用できるかを明確にする。

C.1.1 ホストベースのアクセス制御

ホストベースのアクセス制御は、サブジェクトが特別のシステム上で何を行うことができるかを判断するために使用されている。この技術の意図は、サブジェクトが破損したり、さもなければホストシステムに対して、無許可のソフトウェアを実行するか、その設定を修正するような、不適当な動作をしたりすることを防ぐことにある。これには次の不適当な行動を含むが、それに限られるわけではない:

- プログラムへのアクセス:合法の組織機能に貢献しないプログラムを実行すること、合法の組織機能に貢献するプログラムを除去すること、又は、合法の組織機能(例:監査)に貢献する実行中のプログラム又はプロセスを終了すること。
- ファイルへのアクセス:無効の位置にファイルを作ること、サブジェクトはアクセスを許可されるべきでないデータを含むファイルを読み取ること、重要な情報を含む又は合法のプログラムのふるまいに影響するファイルを修正又は削除すること、又は信頼されていないサブジェクトがそれにアクセスすることを許可するようにファイルの許可を変更すること
- ホストの設定:合法のプログラム又はシステム全体のふるまいを変更しようとする際に、ウィンドゥズのレジストリのようなホストの機能性を定義する値を読み取り、修正し又は削除すること。

持続的なアクセス制御を実施するために、この技術タイプの TOE は、それがアクセスを制御するシステムにローカルに存在すると期待される。このために、TSF は、信頼されていないサブジェクトがそれを終了したり、それを再設定したり、又はそれを実行するのを妨げたりするのを防止するため、それ自体に対するアクセス管理を自動的に用いると期待されている。そのようなアクセス管理は、ポリシー管理製品から受信されるあらゆるポリシーと無関係に使用されるべきである。そのような自己防衛メカニズムがどのように使用されるか、また、どのデータがこの方法で保護されるかを示すことは ST 執筆者の責任である。例えば、ウィンドウズシステム上でエンドポイントエージェントとして実行するプログラムは、それがインストールされたディレクトリ、ウィンドウズスタートアップディレクトリ、そのふるまいを制御するレジストリ値、及び実行可能なプロセス自体へのアクセスを制限する(might)。このように、それらのふるまいに対して実施したアクセス制御方針を持つサブジェクトは、それらのポリシーの実施をバイパスすることはできない。

FDP_ACC.1(1) アクセス制御方針

下位階層: なし

FDP_ACC.1(1) TSF は、[*アクセス制御セキュリティ機能ポリシー(SFP)*]を以下について実施しなければならない(shall)[

- *サブジェクト:組織のデータストアからの利用者のサブセット[割付:追加のサブジェクト];及び、*
- *オブジェクト:プログラム、ファイル、ホスト設定、認証機能、[割付:追加のオブジェクト];及び、*
- *操作:オブジェクトの許可を作成し、読み取り、修正し、実行し、削除し、終了し、又は変更する能力、認証機能を利用する能力、[割付:追加の操作]]*

適用上の注意: *サブジェクト、オブジェクト及び操作は、組織のポリシー管理者に見られるような組織の抽象的概念の観点から定義されなければならない。TOE の内部では、それらの抽象的概念からプラットフォームレベルの特定のサブジェクト、オブジェクト及び操作までマッピングがある。*

適用上の注意: *ST 執筆者は、TOE がこの SFP を適用する特定のメカニズムを示さなければならない(must)。例えば、TOE が包括的なファイルシステムオブジェクトの便宜的に定義されたコンテナに基づいたポリシーを実施する場合、ST 執筆者は表 15 で議論されたこれらの表とエレメントの対応を明瞭に示すべきである。*

適用上の注意: *認証機能を利用する能力の制御は、さらに FTA_TSE.1 を表示することを ST 執筆者に要求する。附属書 C.2.1 を参照。*

依存性: FDP_ACF.1 セキュリティ属性ベースのアクセス制御

FDP_ACF.1(1) アクセス制御機能

下位階層: なし

FDP_ACF.1.1(1) TSF は、次に基づきオブジェクトへの[*アクセス制御 SFP*]を実施しなければならない(shall):[*数セットの組織属性に基づいて、下記の表 15 で定義されたサブジェクトとオブジェクトの間のすべての操作*]。

適用上の注意: *TSF は、サブジェクトとオブジェクト属性を定義することを期待されてはいない:代わりに、それが受信するサブジェクトとオブジェクトの属性データに依存すると期待されている。*

FDP_ACF.1.2(1) TSF は、制御されたサブジェクト及び制御されたオブジェクトの間の操作が許可されるかどうか判断するため、次の規則を実施しなければならない(shall):[*認可され互換性を持つポリシー管理製品から受信された規則*]。

FDP_ACF.1.3(1)　TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に認可しなければならない（shall）:[割付:他の追加の規則]

適用上の注意:　*ST 執筆者は、TSF がこの能力を与える場合に、アクセス制御 SFP への他の明示的なオーバーライドを特定することを検討するべきである。例えば、ホストベースのアクセス制御製品は、信頼された出版者という考え、又はそれら自身への更新を実行することを許可されるかもしれない特定の信頼されたプログラムに基づく、デフォルトで拒否するポリシーに対して適用除外をする。追加の規則のもう一つの例は、利用者がオブジェクトの所有者の場合、そのオブジェクトに対するあらゆる操作は利用者によって許可される。*

FDP_ACF.1.4(1)　TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に拒否しなければならない(shall):[*なし*]。

適用上の注意:　*ST 執筆者は、明確な拒否のプロセスによって保護された特定のオブジェクトを指定しなければならない（must)。この明確な拒否のプロセスは、TSF によって使われた任意のポリシーと無関係に実装されるべきである。*

依存性:　FDP_ACC.1　サブセットアクセス制御

FMT_MSA.3　静的属性の初期化

サブジェクト	オブジェクト	操作
利用者	プロセス	実行｜削除｜終了
		許可の変更
	ファイル	作成｜読取｜修正｜削除
		許可の変更
	ホスト設定	読取｜修正｜削除
	認証機能	ログイン

表 15－ホストベースアクセス制御のための FDP 要件テーブル

保証アクティビティ:

評価者は、TOE が上記の表 15 に定義されるアクティビティを補正することができることを確かめるために、ST 及び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、その後、これらのアクティビティの補正に係る規則を含むポリシーを定義するため、認可され互換性をもつポリシー管理製品を使用しなければならない（shall)。サブジェクト/オブジェクト/操作/属性のコンビネーションの

各々については、評価者は、TSF がこれらのアクティビティを適切に補正することができることを示すために、少なくとも 1 回の陽性テスト及び 1 回の陰性テストを実行するものとする。

例えば、ポリシーは、ある利用者があるプロセスを実行することを許可する規則を定め、異なる利用者が同じプロセスを実行することを禁止するもう一つの規則を定めるかもしれない。一旦このポリシーが実装されると、評価者は、これらの利用者の各々としてシステムにアクセスし、指定されたプロセスを実行する能力が適切に許可されるか拒否されるかを確認する。さらに、サポートされる各条件属性については、要求された操作が許可されても許可されなくても、評価者は、条件属性が影響することを証明する陽性及び陰性テストを考案する。その後、このアクティビティは、他の個々のサブジェクト/オブジェクト/操作/属性の組に対して繰り返される。

FDP_ACC.1(2) アクセス制御方針

下位階層: なし

FDP_ACC.1.1(2) TSF は以下について、[***自己防衛セキュリティ機能ポリシー(SFP)***]を実施するものとする[

- ***サブジェクト:組織データストアからの利用者のサブセット、[割付:追加のサブジェクト];そして、***
- ***オブジェクト:TOE データを構成するか含んでいるプログラム、ファイル及び設定値[割付:追加のオブジェクト];そして、***
- ***操作:オブジェクトの許可を作成し、読み取り、修正し、実行し、削除し、終了し、又は変更する能力、[割付:追加の操作]***

適用上の注意: このポリシーの目的は、ポリシー管理製品の要求で実装されているあらゆるポリシーと無関係の、無許可の修正又は終了から、TSF がそれ自体を保護することである。これには以下のものを含むが、必ずしもそれに限られるわけではない:

- TOE を構成する 1 つ以上の実行可能なファイル
- TOE のふるまいを定義するレジストリ又はその他のシステムの設定 値
- システム・ブーツで実行されるプログラムを定義するファイル又はディレクトリ

ST 執筆者は、このように保護される特定のオブジェクトを指定しなければならない。複数の操作システムが TOE にサポートされる場合、この要件の複数の反復は操作システム間の違いにより必要かもしれない。

依存性: FDP_ACF.1 セキュリティ属性ベースのアクセス制御

FDP_ACF.1(2) アクセス制御機能

下位階層: なし

FDP_ACC.1.1(2) TSF は、次に基づきオブジェクトへの[***自己防衛 SFP***]を実施しなければならない(shall):[***数セットの組織属性に基づくサブジェクトとオブジェクトの間のすべての操作***]。

適用上の注意: *TSF は、サブジェクトとオブジェクト属性を定義することを期待されてはいない;代わりに、それが受信するサブジェクトとオブジェクトの属性データに依存すると期待されている。*

FDP_ACF.1.2(2) TSF は、制御されたサブジェクト及び制御されたオブジェクトの間の操作が許可されるかどうか判断するため、次の規則を実施しなければならない(shall):[***TOE は保護されるべきであると定義されるオブジェクトに対して、要求された操作を許可しない、ただし、行為するサブジェクトが、TOE のインストール及び初期設定に責任を負った個人である場合を除く***]。

FDP_ACF.1.3(2) TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に認可しなければならない(shall):[***なし***]。

FDP_ACF.1.4(2) TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に拒否しなければならない(shall):[***なし***]。

依存性: FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性の初期化

保証アクティビティ:

評価者は、開発文書を、それがレジストリ値、実行可能なプロセス又は設定ファイルのような、TOE のふるまいに影響を与える運用環境に存在するオブジェクトを識別することを確かめるためにチェックしなければならない。(shall)。評価者は、自己防衛メカニズムが十分であることを、次のアクションの実行により確認しなければならない(shall):

- TOE を構成するプロセスを終了しようとすること
- 定義された設定ファイル又はレジストリ値を削除又は任意の修正をしようとすること

- TOE の関連するプロセスが、システム起動から除外されるように、システムの起動シーケンスを修正しようとすること。

この全体にわたって、評価者は、TOE が決して実行を中止しないこと、TOE はそれを構成する部分の移動、変更、及び/又は除去を適切に防ぐこと、及び上記の 3 番目の事例で、TOE は、システムブート中にまだ始められることを確認する。

C.1.2 オプション・ホストベースのアクセス制御 SFR –システム管理者からの保護

このオプションのシナリオでは、TOE が、運用環境のシステム管理者の許可を制限することができる。例えば、TOE は、管理者アカウント利用者がそのシステム上で実行できることを制約する、運用システム上で配置されるアプリケーションかもしれない。この利用者のアクセスが限られているという事実によって、それらは信頼されたとは考えられない。したがって、それらは、TOE を修正又は無効にする権限を持ってはならない。さもないと、それらのアクティビティの制限に目的はない。

該当する要件

1. ST 執筆者は、このシナリオがこの製品に対して存在すると確信しなければならない。

2. FDP_ACC.1 と FDP_ACF.1 の要件は、そのふるまいに影響を与える TSF によって自動的に保護されるオブジェクトを、文書で証明しなければならない(附属書 C.1.1 を参照)(must)。これには、該当する場合、以下を含む:

   a. 環境システム上に存在する TOE の実装の任意の部分

   b. 任意の設定ファイル又は TOE によって使用されたローカルの監査データ・ストアのようなリポジトリ

   c. システムクロック

3. TOE の資源をマニュアルで保護しなければならない場合、AGD_PRE.1 のための証拠は、保護されねばならないオブジェクト、及びこれがどのようにして遂行されることになっているかを識別しなければならない。

C.1.3 ウェブベースのアクセス制御

ウェブベースのアクセス制御は、サブジェクトが特別のシステムにアクセスすることができるオンラインの資源を判断するために使用されている。この技術の意図は、サブジェクトが、他の場合には許容できるアプリケーションのコンテキスト内で、無許可のオンラインの内容と対話するのを妨げることである。例えば、組織は、遠隔の参加者に訓練セッションを表示するためにストリーミングメディアアプリケーションを利用したいと思う一方、この同じアプリケーションを、生のスポーツイベントを見るために使用されることを防ぐことがある。より一般的には、これは次のふるまいを含んでいるが、必ずしもそれに限定しない:

- URL へのアクセス：悪意があるか不適当な内容を含んでいるかもしれない URL によって識別された、オンラインの内容へのアクセス

- ファイルへのアクセス：ウェブコンテンツを開いたり、又はオンラインでホストされ、悪意があるか不適当な内容を含んでいるかもしれない文書、画像、実行可能なバイナリ及びその他のファイルをダウンロードしたりすること

- 実行可能なスクリプトへのアクセス：ウェブページ内に含まれている JSP 又は ActiveX のような実行可能なスクリプトを実行すること、又は、これらを実行する自分自身の能力を制御する(有効にする/無効にする)こと

- フォームへのアクセス：ソーシャルネットワーキングサイトあるいは一般的関心のある伝言板のような、有効な組織目的に貢献しないウェブページへ、HTTP 操作(GET、POST)によりファイル又は投稿データをアップロードすること

HTTP 操作の実装に関する詳細な情報に関しては、RFC2616、ハイパーテキスト転送プロトコル –http://www.ietf.org/rfc/rfc2616.txt の HTTP/1.1 を参照すること。

FDP_ACC.1 アクセス制御方針

下位階層: なし

FDP_ACC.1.1 TSF は、[***アクセス制御セキュリティ機能ポリシー(SFP)***]を以下について実施しなければならない(shall) [

- **サブジェクト：組織のデータストアからの利用者のサブセット；そして**
- **オブジェクト：URL、ファイル、実行可能なスクリプト、フォーム；そして、**
- **操作：アクセス、開く、ダウンロードする、実行する、有効にする、無効にする、HTTP 操作]**

適用上の注意: 節 1.4 に概説されたデバイスのタイプに基づくアクセス制御 SFP の例は、以下にリストアップされている。これらの例は、この要件の割付を終える場合に使用される可能性のある、サブジェクト、オブジェクト及び操作のタイプを単に代表しているものにすぎないことに注意すること。ST 執筆者は、これらの例のうちのどれかを逐語的に使用するのではなく、TSF のふるまいに基づく自分の割当データを開発すべきである。TOE の複数の例が 1 つの ESM システムにあることもありえるかもしれない。その場合には、各々の固有の TOE ポリシーは、この要件を新しく反復する中で取りこまれるべきである。

依存性: FDP_ACF.1 セキュリティ属性ベースのアクセス制御

FDP_ACF.1 アクセス制御機能

下位階層: なし

FDP_ACF.1.1 TSF は、次に基づきオブジェクトへの[***アクセス制御 SFP***]を実施しなければならない(shall):[***下記の表 16 で定義された属性に基づく利用者とオブジェクトの間のすべての操作***]。

適用上の注意: *ESM の意図と一致しているので、サブジェクトを定義する SFP 関連のセキュリティ属性は、運用環境に存在すると期待されている。TOE は、それを配置する組織によってグローバルに定義される、レガシーサブジェクトに基づいたポリシーを実施すべきである(should)。*

FDP_ACF.1.2 TSF は、制御されたサブジェクト及び制御されたオブジェクトの間の操作が許可されるかどうか判断するため、次の規則を実施しなければならない(shall):[***認可され互換性を持つポリシー管理製品から受信された規則***]。

FDP_ACF.1.3 TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に認可しなければならない(shall):[***割付:追加の規則***]

適用上の注意: *ここの意図は、匿名のアクセスをサポートすることである。そのようなアクセスは、アドレスのソースに基づき、(つまり、内部の要求は認証を必要としない)、「ウェブコンテンツが組織のウェブドメインにある場合は、それが認証を必要としない場合に、TOE のすべての利用者がデータを読むことを可能にしてください。」のような表現を使用して、許可されるかもしれない(might)。*

FDP_ACF.1.4 TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に拒否しなければならない(shall):[

- ***要求されたオブジェクトがポリシーによって明確に許可されない場合、要求されたオブジェクトへのアクセスはデフォルトで拒否される。]***

適用上の注意: *ST 執筆者は、附属書 C にある要件 FTA_TSE.1 及び FTA_SSL を組込むことを検討すべきである。管理者でない利用者に対するウェブサーバのセッションの確立に対して、セッションがいつ/どのように管理者に対して確立されるかを制御する能力を TOE が提供する場合、ST 執筆者は FTA_TSE.1 の要件を繰り返したいと思うかもしれない。TOE がセッションをロックするか終了する能力を提供する場合、FTA_SSL 要件が使用されるべきである(should)。*

依存性: FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性の初期化

サブジェクト	オブジェクト	操作
利用者	URL	HTTP の操作によるアクセス
	ファイル	開く｜ダウンロード
	実行可能なスクリプト	実行
		有効｜無効
	フォーム	HTTP GET| HTTP POST

表 16 ウェブベースのアクセス制御のための FDP 要件テーブル

***保証アクティビティ**:*

評価者は、TOE が上記の表 16 に定義されるアクティビティを補正することができることを確かめるために、ST 及び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、その後、これらのアクティビティの補正に係る規則を含むポリシーを定義するため、認可され互換性をもつポリシー管理製品を使用しなければならない(shall)。サブジェクト/オブジェクト/操作/属性のコンビネーションの各々については、評価者は、TSF がこれらのアクティビティを適切に補正することができることを示すために、少なくとも 1 回の陽性テスト及び 1 回の陰性テストを実行するものとする。

例えば、ポリシーは、ある利用者がある URL を訪問することを許可する規則を定め、異なる利用者が同じ URL を訪問することを禁止するもう一つの規則を定めるかもしれない。一旦このポリシーが実装されると、評価者は、これらの利用者の各々としてシステムにアクセスし、指定された URL を訪問する能力が適切に許可されるか拒否されるかを確認する。さらに、(時刻制限のような)各条件属性については、要求された操作が許可されても許可されなくても、評価者は、条件属性が影響することを証明する陽性及び陰性テストを考案する。その後、このアクティビティ

は、他の個々のサブジェクト/オブジェクト/操作/属性の組に対して繰り返される。

C.1.4 データ喪失防止アクセス制御

データ喪失防止アクセス制御は、異なるセキュリティドメイン間の不注意によるデータ漏洩のリスクを削減するために使用される。これは漏洩から独占的な又は機密情報を保護するために使用される可能性もある。例えば、ある「下品な」単語、フレーズ又は一般的な表現は、独占的、機密的、又は米国社会保障番号の標準フォーマットである###-##-####のような又は個人的に識別可能なデータを示すこともある。データ喪失防止アクセス制御 TOE は、これらのタイプのデータが外部ドメイン(又はそれほど機密的でない内部ドメイン)へ送られている可能性がある場合に、識別し、アクションを禁止すべきである(should)。これには次のタイプの漏洩を含むが、必ずしもそれに限られるわけではない:

- プリントスプールの漏洩:機密データを権限のない位置に物理的に移動させる可能性がある、そのようなデータをプリントスプールに置いて印刷すること
- アプリケーション層プロトコルの漏洩:機密データを含む電子メールを送信するか、ウェブ形式によってそれを含むファイルをアップロードするようなアプリケーションによって、機密データを送信すること
- ファイルの漏洩:サブジェクトには見る権限がない機密データを含むファイルを見たり、別のハードドライブのようなより安全性の低いドメインへそれを移動させたり、コピーしたりすること
- クリップボードの漏洩:開いたファイル内の機密データを、その後、より安全性の低いドメインに貼り付けられるように、コピーすること
- 取り外し可能なデバイスの漏洩:権限のない位置に物理的に移動されるかもしれない取り外し可能なデバイスに、機密データを含むファイルを書き込むこと

このタイプのアクセス制御の意図は、悪意のある内部的な「漏洩」に対する包括的な防衛手段を完全に独力で提供することではないことに注意すること。その脅威の緩和が望ましい場合、固く決心した敵を阻止するために、十分に強力な物理的セキュリティ、人的セキュリティ及びネットワーク境界フロー制御デバイスもまた使用する必要がある。

FDP_ACC.1 アクセス制御方針

下位階層: なし

FDP_ACC.1.1　TSF は、[***アクセス制御セキュリティ機能ポリシー(SFP)***]を以下について実施しなければならない(shall)[

- ***サブジェクト:組織のデータストアからの利用者のサブセット;そして***
- ***オブジェクト:受信されたデータを受け、その後に保管し、さもなければ作用することができるローカルの、そして離れた場所;そして***
- ***操作:実行依頼する、送信する、見る、移動する、コピーする、貼り付ける、書き込む;そして、***
- ***属性:機密データの文字列と確かめられる重要度レベル(例えば PII)があるようなデータを含むファイル又はリポジトリ]。***

適用上の注意:　このポリシーの意図は、独占的か機密的として定義されたデータが、数　セットの共通の手段によって、コンピュータから離れることはできないはずであるということを確実にすることである。例えば、TSF は、そのようなデータが電子メールによって送信されたり、又は異なる論理ドライブにエクスポートされたりするのを妨げるべきである。ただし、明らかに許可された場合を除く。

適用上の注意:　データ喪失防止製品は、復号された又は置き違えられた機密データについて、運用環境を検査し、矛盾を正す能力を含んでいるかもしれない。この能力は、本 PP に含まれるオプションの要件 ESM_DSC.1 によって表わされる。

依存性:　FDP_ACF.1 セキュリティ属性ベースのアクセス制御

FDP_ACF.1 アクセス制御機能

下位階層:　なし

FDP_ACF.1.1　TSF は、次に基づきオブジェクトへの[***アクセス制御 SFP***]**を実施しなければならない**(shall):[***下記の表 17 で定義された属性に基づく利用者とオブジェクトの間のすべての操作***]。

適用上の注意:　ESM の意図と一致しているので、サブジェクトを定義する SFP 関連のセキュリティ属性は、運用環境に存在すると期待されている。TOE は、それを配置する組織によってグローバルに定義される、レガシーサブジェクトに基づいたポリシーを実施すべきである(should)。

FDP_ACF.1.2　TSF は、制御されたサブジェクト及び制御されたオブジェクトの間の操作が　許可されるかどうか判断するため、次の規則を実施しなければならない(shall):[***認可され互換性を持ち、次の考え方を包含するポリシー管理製品から受信された規則***:

- ***統計情報の属性は、機密的、独占的のようなセキュリティ属性で示されるかもしれない、又は、それ以外には開示を許されない(例えば PII、機密扱いされたデータ); そして***
- ***このデータを含むオブジェクトは、システムを離れることは禁止される、ただし、意図された送信先が明確に信頼される位置の場合を除く; そして、***
- ***システムを離れるメカニズムは最小限、他の論理デバイスへの転送、印刷、電子メール及びクリップボードへのコピーを構成する]。***

適用上の注意:　*ST 執筆者は、TSF が機密的であると考えるデータの一定のタイプと値、それらがこの機密データを含むかどうか判断するために検査することができるファイルとメタデータの一定のタイプを特定すると期待されている。*

FDP_ACF.1.3　TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に認可しなければならない(shall):[***オブジェクトが、信頼されるとしてフラグが明示的に立てられるメールの受信者又は論理ドライブのような送信先に移動しているか、さもなければ組織に対して完全に内部的な場合には、操作は許可される***]。

適用上の注意:　*ST 執筆者は、論理デバイスが信頼されるとしてフラグが立てられるかどうか、TOE が判断する能力に対する要件を定義すると期待される。*

FDP_ACF.1.4　TSF は、次の追加の規則に基づいた、オブジェクトへのサブジェクトのアクセスを明白に拒否しなければならない(shall):[***なし***]。

依存性:　FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性の初期化

サブジェクト	オブジェクト	操　作
	プリントスプール	提出する（セキュリティドメインの外部に転送する）

利用者	アプリケーション層のプロトコル	送信する（セキュリティドメインの外部に転送する）
	ファイル	見る｜移動する｜コピーする（別のセキュリティドメインへ）
	クリップボード	コピーする｜貼り付ける（別のセキュリティドメインへ）
	取り外し可能なデバイス	書き込む（セキュリティドメインの外部へ転送する）

表 17－　データ喪失防止アクセス制御のための FDP 要件テーブル

保証アクティビティ:

評価者は、TOE が上記の表 17 に定義されるアクティビティを補正することができることを確かめるために、ST 及び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、その後、これらのアクティビティの補正に係る規則を含むポリシーを定義するため、認可され互換性をもつポリシー管理製品を使用しなければならない(shall)。サブジェクト/オブジェクト/操作/属性のコンビネーションの各々については、評価者は、TSF がこれらのアクティビティを適切に補正することができることを示すために、少なくとも 1 回の陽性テスト及び 1 回の陰性テストを実行するものとする。

例えば、ポリシーは、ある特定の機密データ値を含んでいない文書のみを印刷することを利用者に許可するという規則を定義する。一旦このポリシーが実装されれば、評価者はシステムにアクセスし、機密データを含む文書を印刷することができず、機密データを含まない別の文書を印刷することができるということを確認する。さらに、(時刻制限のような)各条件属性については、要求された操作が許可されても許可されなくても、評価者は、条件属性が影響することを証明する陽性及び陰性テストを考案する。その後、このアクティビティは、他の個々のサブジェクト/オブジェクト/操作/属性の組に対して繰り返される。

C.1.5 オプションのデータ喪失防止 SFR:コンテンツディスカバリー

オブジェクトインベントリー

下位階層:　　なし

ESM_DSC.1.1　TSF は、次の条件を満たす運用環境においてオブジェクトを発見することができなければならない(shall):[選択:ポリシーが暗号化することを要求する復号されたデータ、データの定義された重要度の属性と一致しない領域に存在するデータ、[***割付:運用環境に存在するデータは TSF によってカタログされるべきであることを示すその他の条件***]]。

適用上の注意:　*本プロテクションプロファイルの中のオブジェクト発見の特定の目的は、TSF が、それらがその中に存在することを許されるべきではないドメインに入ったり、存在したりしているオブジェクトを検知することである。*

ESM_DSC.1.2　TSF は、ESM_DSC.1.1 によって定義されるオブジェクトの発見に従って次の措置を講じなければならない(shall):[選択:オブジェクトを暗号化する、その重要度属性と一致する位置にオブジェクトを移動させる、オブジェクトを削除する、[***割付:その他のアクション***]]。

適用上の注意:　*割付が選択される場合、執られた特定のアクションは、発見されたオブジェクトに対して執られた修正措置に関連すべきである。*

適用上の注意:　*この SFR が含まれている場合、監査事象は発見された内容及び執られた措置を含む、オブジェクトの監査を含めるように調節されるべきである(should)。*

依存性:　なし

保証アクティビティ:

注:この SFR に対する保証アクティビティはまだ開発中である。本プロテクションプロファイルの利用者は、この SFR を確かめるために、それらが使用するプロセスと手順を文書で証明し、本 PP の次のバージョンに含まれる一般化保証アクティビティへ入力するように、CCEVS にそれらのプロセスと手順のコピーを提供すべきである(should)。

C.2 追加のオプション SFR

C.2.1 セッション管理に係るオプションの SFR

TOE セッション確立

下位階層: なし

FTA_TSE.1.1 TSF は、[***選択:日、時間、[割付:その他の属性]に基づくセッションの確立を 拒否することができなければならない*** *(shall)*。]

依存性: なし

適用上の注意: *セッション確立は、TSF によって管理されるホストに対するものである。この要件には、時刻、曜日又は地理的位置のように認証クレデンシャル情報が有効な状況を判断することにより、TSF がホストの認証機能に関するアクセス管理を行使するためのメカニズムを提供することが含まれている。*

適用上の注意: *この SFR が表示される場合、ST 執筆者は監査対象事象としてセッション確立の正常終了又は拒否を含めなければならない(must):正常終了の監査はすべてのレベルの監査の操作中に無効になるかもしれない。*

保証アクティビティ:

評価者は、セッションが拒否されうる属性のすべてが特に定義されることを判断するために TSS を検査しなければならない(shall)。評価者は、TSS 内で識別された属性の各々を設定するためのガイダンスをそれが含むことを判断するため、操作ガイダンスを検査しなければならない(shall)。評価者は、また各属性について次のテストを行なわなければならない(shall):

- *テスト 1:評価者は、成功裡に TOE へのセッションを確立する。その後、評価者は、当該アクセスが属性の特定の値に基づいて拒否されるように、TOE を設定するための操作ガイダンスに従う。その後、評価者は、属性のセッティングに抵触するセッションを確立するよう試みなければならない(shall)。(例えば、位置は時刻に基づいて拒否される。) 評価者は、セッション確立の試みが失敗することを確認しなければならない(shall)。*

TSF 起動セッションのロックと終了(FTA_SSL)

下位階層: なし

FTA_SSL_EXT.1 TSF 起動セッションロック

FTA_SSL_EXT.1.1 TSF は、ローカルな対話セッションについて、セキュリティ管理者指定の非アクティブである時間間隔後に、以下を実施しなければならない[選択:

- セッションをロックする-現在の内容を読取り不能にし、セッションのアンロック以外の利用者のデータへのアクセス/デバイスの表示等のあらゆるアクティビティを無効にすることで、ディスプレイデバイスをクリア又は上書きする、そして利用者がセッションのアンロック前に TSF に再認証することを要求する;
- セッションを終了する]

依存性: なし

保証アクティビティ:

評価者は次のテストを実行しなければならない(shall):

- *テスト 1:評価者は、操作ガイダンスに従い、コンポーネント中で参照される非アクティブである時間間隔にいくつかの異なる値を設定する。それぞれの設定された時間間隔について、評価者は TOE とのローカルな対話セッションを確立する。その後、評価者は、設定された時間間隔後に、セッションがロック又は終了されることを確認する。ロックがコンポーネントから選択される場合、評価者はセッションをアンロックしようとするときに再認証が必要であることを確実にする。*

FTA_SSL.3 TSF 起動による終了

下位階層: なし

FTA_SSL.3.1 TSF は、権限のある管理者が設定可能なセッション非アクティブである時間間隔の後に、遠隔の対話セッションを終了しなければならない(shall)。

依存性: なし

保証アクティビティ:

評価者は次のテストを実行しなければならない(shall):

- *テスト 1:評価者は、操作ガイダンスに従い、コンポーネント中で参照される非アクティブである時間間隔にいくつかの異なる値を設定する。これらは、互いの値だけでなく、少なくとも操作ガイダンスで指定されるような最小限及び最大限の許容値から構成されなければならない(shall)。それぞれの設定された時間間隔について、評価者は TOE との遠隔な対話セッションを確立する。その後、評価者は、設定された時間間隔後に、セッションが終了されることを確認する。*

FTA_SSL.4　利用者起動による終了

下位階層:　　なし

FTA_SSL.4.1　TSF は、管理者自身の対話セッションの管理者起動による終了を許可しなければならない(shall)。

依存性:　　なし

保証アクティビティ:

評価者は次のテストを実行しなければならない(shall):

- *テスト 1:評価者は、TOE とローカルの対話セッションを起動する。その後、評価者は、操作ガイダンスに従い、セッションを終了するか又はログオフし、セッションが終了したことを確認する。*

- *テスト 2:評価者は TOE と遠隔の対話セッションを起動する。その後、評価者は、操作ガイダンスに従い、セッションを終了するか又はログオフし、セッションが終了したことを確認する。*

C.2.2 継続的なアクセス実施を確実にするオプションの SFR

セキュアな状態の保存と障害

下位階層:　　なし

FPT_FLS.1　TSF は、次のタイプの障害が発生する場合、[詳細化:***次のアクションを実行する:[選択:1 つ又はそれ以上の事象のログ、コンポーネントの再起動、管理者へのアラーム送信***]しなければならない(shall)。[***割付:TOE コンポーネント及び可能性のある誤作動状態のリスト***]。

適用上の注意:　*この要件の例は、TSF が 3 つの実行プロセスで構成される状況で、他のものがまだ実行中であることを確実にするために、その各々は継続的にポーリングする。利用者が TSF の*

アクセス制御を、それを構成するプロセスの 1 つを終了することで回避しようとする場合、その他のプロセスの一つは終了したものを再起動し、アクセス制御の実施における混乱を防ぐだろう。また、管理者が、可能性のある悪意のあるアクティビティが起きていることに気づくように、それはある種の通知を作成する。

適用上の注意: *そのコンポーネントの監視を実行する TOE の要件は、システム上の無許可のアクティビティに対して保護する他の機能性と協力して、監査を無効にできないことを確実にすることにより、利用者が彼らのアクションを隠してはならないことを確実にする。この SFR が ST に含まれていれば、それは対策方針 O.RESILIENT を満たすためにマップされるだろう。*

依存性: なし

保証アクティビティ:

注:この SFR に対する保証アクティビティはまだ開発中である。本プロテクションプロファイルの利用者は、この SFR を確かめるために、それらが使用するプロセスと手順を文書で証明し、本 PP の次のバージョンに含まれる一般化保証アクティビティへ入力するように、CCEVS にそれらのプロセスと手順のコピーを提供できるはずである (should)。

C.3 内部的な暗号の機能要件

本プロテクションプロファイルは、TOE 開発者が、運用システム又は暗号ライブラリのような、TOE を保護するために暗号化機能性を提供する第三者の技術を使用することを許可し、奨励するために書かれている。TOE が、それ自身の内部的な暗号の機能性を提供し、第三者の技術に依存しない場合、次の要件も考慮に入れなければならない(must)。

該当する要件

1. ST 執筆者は、このシナリオがこの製品に対して存在すると確信しなければならない。

2. 評価チームは、ST 内のこの附属書に要件を表示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取り扱われるという保証の証拠を提供しなければならない(must)。

4. 評価チームは、これらの要件内に参照される機能性をテストするため、テストを考案し実行しなければならない。

これらの要件は、TOE がそれ自身の暗号の機能性を実行し、機能性を実行するために OS 又は暗号ライブラリに依存しない場合にのみ表示されるべきである(should)。これらの要件は、IPsec 仮想プライベート・ネットワーク(VPN)ゲートウェイに対するセキュリティ要件から得られた。これらの能力を定義するために使用される暗号の規格は、米国固有のものであることに注意すること:その他の国々によって監視されるべき評価については、該当する同等の国内規格が ST 執筆者によって使用されなければならない(shall)。

C.3.1 FCS_CKM.1 暗号鍵生成(非対称暗号鍵用)

下位階層: なし

FCS_CKM.1.1 TSF は、以下に従って**鍵確立**に使用される**非対称**暗号鍵を生成**しなければならない**。:

[選択:

- NIST の SP800－56A、有限体に基づく鍵確立スキームについての「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」;

- NIST の SP 版 800－56A、楕円曲線に基づく鍵確立スキームについての「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」 P-256、P-384 そして[選択:P-521、他の曲線なし](FIPS

PUB186-3「Digital Signature Standard」に定義された)を実装する。

- NIST の SP800－56B、RSA に基づく鍵確立スキームについての「Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography」]及び特定の暗号鍵サイズは 112 ビットの**セキュリティと同等もしくはそれ以上**であること。

適用上の注意: *このコンポーネントは、TOE が TOE によって使用される多様な暗号プロトコル(例えば IPsec)の鍵確立に使用される公開/秘密鍵ペアを生成することができることを要求している。複数のスキームがサポートされている場合、ST 執筆者は、この能力を示すために、この要件を繰り返すべきである。使用されるスキームは、選択肢から ST 執筆者によって選ばれるだろう。*

使用されるドメインパラメタが本 PP 内のプロトコルの要件によって指定されるので、TOE がドメインパラメタを生成することは期待されていない。したがって、TOE が本 PP 内で特定されるプロトコルに適合する場合に、追加ドメインパラメタの確認は必要とされない。

生成された 2048 ビットの DSA 鍵及び rDSA 鍵の鍵強度は、112 ビットのセキュリティと同等もしくはそれ以上である必要がある。同等な鍵強度に関する情報として、NIST の SP800-57 の「鍵管理に関する勧告」を参照すること。

依存性: [FCS_CKM.2 暗号鍵の分散、又は

FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

保証アクティビティ:

評価者は、ST 執筆者によって実行される選択により、上記の要件をテスト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使用しなければならない(shall)。これは、評価者が、テストにおいて検証可能なテストベクタを生成できるアルゴリズムの高信頼参照実装を持っていることを必要とする。

TSF の実装が、なされた選択によって 800－56A 及び/又は 800－56B に適合することを示すために、評価者は、TSS が次の情報を含むことを確実にしなければならない (shall) ;

- *TSS は、TOE が適合する適切な 800-56 規格のすべてのセクションをリストアップしなければならない*

(shall)；

- *TSS にリストアップされた個々の該当する節について、「しなければならない」(shall)でないすべての説明(すなわち、「してはならない」(shall not)、「すべきである」(should)、「すべきではない」(should not))については、TOE がそのようなオプションを実装する場合、それは TSS に記載されるものとする。含まれる機能性が規格では「しないものとする」(shall not)又は「すべきではない」(should not)として示される場合、TSS は、なぜこれが TOE によって実装されたセキュリティポリシーに悪影響を及ぼさないかの根拠を提供するものとする；*

- *800－56A 及び 800－56B(選択に従う)の個々の該当する節について、「しなければならない」(shall)又は、「すべきである」(should)という記述に関連する機能性の何らかの省略は、記載されるものとする；*

- *何らかの TOE に特有の拡張、文書に含まれていないプロセッシング、又は、TOE が実施すべきセキュリティ要件に影響を与える文書によって許可される代替の実装は、記載されるものとする。*

C.3.2 FCS_CKM_EXT.4　暗号鍵ゼロ化

下位階層:　　なし

FCS_CKM_EXT.4.1　もはや必要でない場合、TSF はすべての平文の秘密及びプライベート暗号鍵と暗号化によるセキュリティパラメタをすべてゼロ化しなければならない。

適用上の注意:　*(鍵、認証データ及びパスワードのような)何らかのセキュリティに関する情報は、セキュリティの重要なデータの漏洩又は修正を防ぐために、それ以上使用されない場合はゼロ化しなければならない。*

上に示されたゼロ化は、鍵/クリティカルセキュリティパラメタを他の場所に移動させる際に、平文の鍵及び/又はクリティカルセキュリティパラメタのための中間格納領域(すなわち、このようなデータの経路に含まれる、メモリバッファーのようなあらゆるストレージ)に適用される。

依存性:　　なし

保証アクティビティ:

評価者は、TSS が、秘密鍵(対称暗号化のために使用される鍵)、プライベート鍵及び鍵の生成に使用されるクリティカルセキュリティパラメタの各々について記述することを確実にするためチェックするものとする:それらはいつゼロ化されるか(例えば使用後直ちに、システム終了時、等);及び実行されるゼロ化処理のタイプ(ゼロで上書き、ラン

ダムパタンで 3 回上書き等)。もし、保護すべきものを格納するために様々な種類のメモリが利用されている場合、評価者は TSS において、データが格納されているメモリを単位としてゼロ化処理(たとえば、フラッシュに格納されている秘密鍵はゼロで 1 回上書きされ、一方、内部ハードドライブに格納された秘密鍵は、各書き込み前に変更されるランダムパタンを使って 3 回上書きされる)が記述されていることを確実にするためにチェックしなければならない。

C.3.3 FCS_COP.1(1)　暗号操作(データ暗号化/復号に関して)

下位階層:　　なし

FCS_COP.1(1)　**詳細化**:TSF は、指定された暗号アルゴリズム[*[**割付:一つ以上の利用モード**]*での***AES 操作***]及び以下に合致する ***128 ビット、256 ビット、及び***[*選択:192 ビット、他の鍵サイズなし*]の暗号鍵サイズに従って、[*暗号化及び復号*]を実施しなければならない(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 執筆者は、AES の 1 つ又は複数の利用モードを選択すべきである(should)。最初の選択については、ST 執筆者は、この機能性によりサポートされる鍵サイズを選択するべきである。第 2 の選択については、ST 執筆者は、割付で指定された利用モードを記述する規格を選択すべきである。*

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

FDP_ITC.2　セキュリティ属性のある利用者データのインポート、又は

FCS_CKM.1　暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

保証アクティビティ:

評価者は、上記要件をテストする際のガイドとして、以下の文書から上記の要件で選択した利用モードに適切なテストを使用しなければならない(shall)。「The Advanced Encryption Standard Algorithm Validation Suite」(AESAVS)、「The XTS-AES Validation System」(XTSVS)、CMAC 確認システム(CMACVS)。」「The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)」、「The Galois/Counter Mode (GCM) and GMAC Validation ystem (GCMVS)」(これらの文書は

http://csrc.nist.gov/groups/STM/cavp/index.htmlh から利用可能）これは、評価者が、テストにおいて検証可能なテストベクタを生成できるアルゴリズムの基準実装を持っていることを必要とする。

C.3.4 FCS_COP.1(2)　暗号操作(暗号署名に関して)

下位階層:　　なし

FCS_COP.1.1(2)　**詳細化**:TSF は、以下に従って***暗号署名サービス***を実行しなければならない（shall)。[選択:

(1):2048 ビット以上の鍵サイズ(法)の電子署名アルゴリズム(DSA)

(2)2048 ビット以上の鍵サイズ(法)の RSA 電子署名アルゴリズム(rDSA)、又は

(3)256 ビット以上の鍵サイズの楕円曲線電子署名アルゴリズム(ECDSA):

*であって、**以下に準拠するもの***

電子署名アルゴリズムの場合:

- ***FIPS PUB 186-3,「Digital　Signature　Standard」;又は***

RSA 電子署名アルゴリズムの場合:

- ***FIPS PUB 186-3,「Digital　Signature　Standard」;又は***

楕円曲線電子署名アルゴリズムの場合:

- ***FIPS PUB 186-3,「Digital　Signature　Standard」;そして***
- ***TSF は、(FIPS PUB、「Digital　Signature　Standard」186-3 に定義されている通り)「NIST 曲線」P-256、P-384[そして選択:P-521、その他の曲線なし]を実装しなければならない（shall)。***

適用上の注意:　暗号署名のための好ましいアプローチとして、楕円曲線が本 PP の将来のバージョンで要求される。

適用上の注意:　ST 執筆者は、電子署名を実行するよう実装されるアルゴリズムを選択するべきである;もし複数のアルゴリズムが利用可能であれば、この要件(及び対応する FCS_CKM.1 要件)は、機能性を特定するために繰り返されるべきである。選択されたアルゴリズムについて、ST

執筆者は、適切な割付/選択を行ない、そのアルゴリズムについて実装されるパラメタを特定すべきである(should)。

楕円曲線に基づくスキームに関して、鍵サイズは、小数点の位数の log2 を取った値を意味する。電子署名の好ましいアプローチとして、ECDSA は本 PP の将来のバージョンで要求される。

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

FDP_ITC.2 セキュリティ属性のある利用者データのインポート、又は

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

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 FIPS 186-3 Digital Signature Algorithm Validation System (DSAVS)」、「The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation Systemn (ECDSA2VS)」、and 「The RSA Validation System (RSAVS)」の署名生成部分と署名検証部分を使用しなければならない(shall)。これは、評価者が、テストにおいて検証可能なテストベクタを生成できるアルゴリズムの基準実装を持っていることを必要とする。

C.3.5 FCS_COP.1(3) 暗号操作(暗号ハッシュ法に関して)

下位階層: なし

FCS_COP.1.1(3) **詳細化**: TSF は、以下に合致する、指定された暗号アルゴリズム[選択:SHA-1(SHA-256)、SHA-384]及び***メッセージダイジェスト***のサイズ[選択:160、256、384]に従って***暗号ハッシュサービス***を実行しなければならない(shall): ***FIPS Pub 180-3、「Secure Hash Standard」***

適用上の注意: *PP の本バージョンについては、SHA-1 の使用は、後方互換性の理由での TLS に対する場合のみ許可される。PP の次のバージョンは、完全に SHA-1 の使用を除外する。*

適用上の注意: *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のサイズの選択と合致しなければならない(must);例えば、SHA-1 が選択された場合、有効なメッセージダイジェストのサイズの選択は 160 ビットのみとなる。*

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

FDP_ITC.2 セキュリティ属性のある利用者データのインポート、又は

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

保証アクティビティ:

評価者は上記の要件をテストするガイドとして「The Secure Hash Algorithm Validation System (SHAVS)」を使用しなければならない(shall)。これは、評価者が、テストにおいて検証可能なテストベクタを生成できるアルゴリズムの基準実装を持っていることを必要とする。

C.3.6 FCS_COP.1(4) 暗号操作(鍵付ハッシュメッセージ認証に関して)

下位階層: なし

FCS_COP.1.1(4) **詳細化**:TSF は、以下に合致する指定された**暗号アルゴリズム** HMAC－[選択:SHA-1(SHA-256)、SHA-384]、***鍵のサイズ[割付:HMAC の中で使用される鍵のサイズ(ビット)]***及び***メッセージダイジェスト***のサイズ*[選択:160、256、384]***ビット***に従って鍵付ハッシュメッセージ認証を実行しなければならない(shall):***FIPS Pub 198-1,「鍵付ハッシュメッセージ認証コード及び FIPS Pub 180-3、「セキュアなハッシュ規格」***

適用上の注意: *PP の本バージョンについては、SHA-1 の使用は、後方互換性の理由での TLS に対する場合のみ許可される。PP の次のバージョンは、完全に SHA-1 の使用を除外する。*

適用上の注意: *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のサイズの選択と合致しなければならない(must):例えば、HMAC-SHA-256 が選択された場合、有効なメッセージダイジェストのサイズの選択は 256 ビットのみとなる。*

上記のメッセージダイジェストのサイズは、使用される、内在するハッシュアルゴリズムに対応する。ハッシュ計算の後でHMACのアウトプットを切り捨てることは、様々なアプリケーションの適切な段階であることに注意すること。これは、この要件の適合性を無効にしない、しかしながら、ST は、切り捨てが実行されること、最終アウトプットのサイズ、そしてこの切り捨てが適合する規格を述べなければならない(shall)。

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

FDP_ITC.2 セキュリティ属性のある利用者データのインポート、又は

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4 暗号鍵破棄

保証アクティビティ:

評価者は上記の要件をテストするガイドとして「The Secure Hash Algorithm Validation System (SHAVS)」を使用しなければならない(shall)。これは、評価者が、テストにおいて検証可能なテストベクタを生成できるアルゴリズムの参照実装を持っていることを必要とする。

C.3.7 FCS_RBG_EXT.1 拡張： 暗号操作(ランダムビット生成)

下位階層: なし

FCS_RBG_EXT.1.1 TSF はランダムビット生成(RBG)サービスを、[選択:次から一つを選択:(1)1 つ以上の独立したハードウェアベースのノイズ源(2)1 つ以上の独立したソフトウェアベースのノイズ源(3)(ハードウェアベースとソフトウェアベースのノイズ源の組合せ)]からエントロピーを蓄積するエントロピー源によって初期化されたシード(seed)として与えられた;[選択、次から一つを選択:[選択:Hash_DRBG(いずれか)、HMAC_DRBG(いずれか)、CTR_DRBG (AES))、Dual_EC_DRBG(いずれか)]を使用する NISTSpecial Publication800-90;FIPS Pub140-2 付属書 C:AES を使用する X9.31 付属書 2.4]に従ってすべて行わなければならない(shall)。

FCS_RBG_EXT.1.2 決定論的RBG は、少なくとも(その RBG が)生成する鍵及び認証要素の最大長以上、及び、最低限[選択、次から 1 つを選択:128 ビット、256 ビット]のエントロピーによって初期化されなければならない(shall)。

適用上の注意: *NISTSP800-90、(附属書 C)は、恐らくFIPS-140 の将来のバージョンを要求する最小限のエントロピー測定について記述する。可能であれば、これは直ちに使用されるべきであり、本 PP の将来のバージョンでは要求されるだろう。*

FCS_RBG_(EXT).1.1 の最初の選択について、ST 執筆者は、RBG サービスが適合する規格(800-90 又は 140-2 付属書 C のいずれか)を選ぶべきである。

SP800-90 は、乱数表を生成する 4 つの異なる方法を含んでいる;これらの各々は、今度は、内在する暗号プリミティブ(基関数)(ハッシュ関数/暗号に依存している。ST 執筆者は、(800-90 が選択される場合)使用される関数を選び、要件又は TSS の中で使用される特定の内在する暗号プリミティブを含めるだろう。識別されたハッシュ関数(SHA-1、SHA-224、SHA-256、SHA-384、SHA-512)のいずれかが、Hash_DRBG 又は

HMAC_DRBG に関して許容され、CT_DRBG に対して AES に基づく実装のみが許可される。800-90 で定義された曲線カーブのうちのいずれかが Dual_EC_DRBG に対して許可されるが、ST 執筆者は選択した曲線を含めなければならないだけでなく、使用されるハッシュアルゴリズムをふくめなければならない(must)。

FIPS Pub 140-2 付属書 C に関して、3-Key Triple DES 及び AES アルゴリズム第 3 節を使用した ANSI X9.31 付属書 A.2.4 に基づく、NIST 推奨乱数生成器に記載される方法のみが現在有効であることに注意すること。ここで使用される AES の実装に係る鍵の長さが、利用者データを暗号化するために使用されるものと異なる場合、FCS_COP.1 は異なる鍵の長さを反映するために調節されるか、又は繰り返されなければならないかもしれない。FCS_RBG_EXT.1.2 の選択について、ST 執筆者は、RBG を初期化するために使用されるエントロピーの最小ビット数を選択する。

ST 執筆者はまた、TOE のベースライン要件にあらゆる内在する関数が含まれることを確実にする。

将来、ほとんどの要件はエントロピー源テストの方法に記述される:要件及びテストスイートの説明が、本 PP によって必要とされるだろう。次の保証アクティビティは、現在、必要なアクティビティのサブセットのみを反映している。

依存性: なし

保証アクティビティ:

評価者は、TOE で使用される RBG を含む製品のバージョンを決定するため、TSS 節を検証しなければならない(shall)。評価者はまた、TSS が、エントロピーが収集されるノイズ源について記述していることを確認し、さらに、このノイズ源の位置を確認しなければならない(shall)。評価者はさらに、RBG で使用されるすべての内在する関数及びパラメタが TSS にリストアップされていることを確かめる。

評価者は、使用されるエントロピー源の識別、どれだけのエントロピーが各エントロピー源によって生成されるかだけでなく、エントロピー入力を獲得する方法を含む、RBG モデルの説明を TSS が含んでいることを、確かめなければならない(shall)。評価者はまた、TSS がエントロピー源障害の既知のモードを記述していることも確実にしなければならない(shall)。最後に、評価者は、アウトプットの独立性及び時間及び/又は環境条件による分散の観点で、TSS が RBG アウトプットの説明を含んでいることを確実にしなければならない(shall)。RBG が適合性を表示している規格にかかわらず、評価者は次のテストを実行する:

- テスト 1:評価者は、エントロピー源テストスイートの使用により各エントロピー源のエントロピー推定値を判断しなければならない(shall)。評価者は、TSS が、すべてのエントロピー源から得られたすべての結果の最小限のものであるエントロピー推定値を含むことを確実にしなければならない(shall)。

評価者はまた、RBG が適合する規格に応じて次のテストを行わなければならない(shall)。

FIPS 140-2、Annex C に適合する実装

本節に含まれるテストの参考文献は The Random Number Generator Validation System [RNGVS]である。評価者は次の 2 つのテストを実施するものとする。正しいと知られているアルゴリズムの参照実装によって、「期待値」が生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ている。

評価者は可変シードテストを実行しなければならない(shall)。評価者は、TSF RBG 関数に対し、各 128 ビットで 128 ペア(シード、DT)のセットを提供しなければならない(shall)。評価者はまた、すべての 128 ペア(シード、DT)に対して一定の値の(AES アルゴリズムに対して適切な長さの)鍵を提供しなければならない(shall)。DT の値は、各セットに対して 1 ずつ増加される。シードの値はセットの中で反復があってはならない(shall not)。評価者は、TSF から返される値が期待値と一致することを確実にする。

評価者はモンテカルロ・テストを行なわなければならない(shall)。このテストについては、初期シードと DT 値を、各 128 ビットずつ、TSF RBG 関数に対して供給する。評価者はまた、テストの全体にわたって一定の値の(AES アルゴリズムに適切な長さの)鍵を提供しなければならない(shall)。その後、評価者は、各々の繰り返しごとに DT 値を 1 ずつ増加させつつ、TSF RBG を 10,000 回呼び出す。そして次の繰り返しのための新しいシードは、3-Key Triple DES 及び AES アルゴリズム第 3 節を使用した ANSI X9.31 属書 A.2.4 に基づく、NIST 推奨乱数生成器で指定されるように生成される。評価者は、10,000 回目に生成された値が期待値と一致することを確認する。

NIST SP800-90 に適合する実装

評価者は、RNG 実装について 15 回の試行を実行しなければならない(shall)。RNG が設定変更可能な場合、評価者は、それぞれの設定条件につき 15 回の試行を行なわなければならない(shall)。評価者はまた、操作ガイダンスが RNG 機能性を設定変更するための適切な指示を含んでいることを確認しなければならない(shall)。

RNG が予測耐性を有効にできる場合、それぞれの試行は、(1)drbg のインスタンス化、(2)ランダムビット列の 1 番目のブロックの生成、(3)ランダムビット列の 2 番目のブロックの生成、(4)インスタンスの終了(ゼロ化)から構成される。評価者は、ランダムビット列の 2 番目のブロックが期待値であることを確かめる。評価者は、それぞれの試行について、8 つの入力値を生成しなければならない(shall)。1 番目は整数カウンタ(0 -14)である。次の 3 つは、インスタンス化操作のためのエントロピー入力、ナンス及び個別化文字列である。次の 2 つは、生成の初回の呼び出しに対する追加入力とエントロピー入力である。最後の 2 つは、生成の 2 回目の呼び出しに対する追加入力とエントロピー入力である。これらの値はランダムに生成される。「ランダムビット列の 1 ブロックを生成する」とは、返送されたビット数が、(NIST SP800-90 で定義された)出力ブロック長と等しいようなランダムビット列を生成すると言う意味である。

RNG に予測耐性がない場合、それぞれの試行は、(1)drbg のインスタンス化、(2)ランダムビット列の 1 番目のブロックの生成、(3)再シード、(4)ランダムビット列の 2 番目のブロックの生成、(4)インスタンスの終了(ゼロ化)から構成される。評価者は、ランダムビット列の 2 番目のブロックが期待値であることを確かめる。評価者は、それぞれの試行

について、8 つの入力値を生成しなければならない(shall)。1 番目は整数カウンタ(0 −14)である。次の 3 つは、インスタンス化操作のためのエントロピー入力、ナンス及び個別化文字列である。5 番目の値は、生成の初回の呼び出しに対する追加入力である。6 番目と 7 番目は、再シードの呼び出しに対する追加入力とエントロピー入力である。最後の値は、2 回目の生成の呼び出しに対する追加入力である。

次のパラグラフは、評価者によって生成/選択される入力値のいくつかについてのより多くの情報を含んでいる。

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

***ナンス**:ナンスがサポートされる(df のない CTR_DRBG がナンスを使用しない)場合、ナンスのビット長はシード長の 2 分の 1 である。*

***個別化文字列**:個別化文字列の長さは、シード長以下でなければならない(must)。実装が1つの個別化文字列の長さのみをサポートする場合、両方の値について同じ長さを使用することができる。2つ以上の文字列の長さがサポートされる場合、評価者は、2 つの異なる長さの個別化文字列を使用しなければならない(shall)。実装が個別化文字列を使用しない場合、値を供給する必要はない。*

***追加入力**:追加入力文字列のビット長は、個別化文字列長と同じデフォルト値及び制約条件がある。*

附属書 D -文書の表記法

英国式の綴りをアメリカ式の綴りに置き換えることを除いて、本 PP の中で使用される表記法、フォーマット及び表記規則はコモンクライテリア(CC)のバージョン3.1と一致している。選択された記述の選択はPPの読者を助けるため、ここで議論される。

D.1 操作

CC は、機能要件上で実行されるように、4 つの機能コンポーネントの操作ー割付、詳細化、選択及び繰返しーを許可する。本 PP は、次の方法で 4 つの操作を強調する:

- **割付**:識別されたパラメタの仕様を許可する。ST 執筆者によって一層の操作が必要な場合、プロンプト「割付」を含む角括弧の内部に*太文字でイタリック体のテキスト*で表示される;
- **詳細化**:詳細の追加を許可する。イタリック体のテキストで表示される。
- **選択**:リストから 1 つ以上の要素の仕様を許可する。プロンプト「選択」を含んでいる角括弧の内側のアンダーラインを引かれたテキストで表示される。
- **繰返し**:コンポーネントが、異なる操作と共に2度以上使用されることを許可する。SFR の要素番号に続く括弧内に、シーケンシャル番号で表示される。

CC パート 2 から取られた要件に関して、*太文字でイタリック体のテキスト*は、これらの要件が PP に適用されることを保証するために、割付の操作が既に完了した場所を表示する。

D.2 拡張要件の表記法

CC が、作成者のニーズを満たすために適切な要件を提示しない場合、拡張要件が許可される。拡張要件は、識別されなければならず、要件を明瞭に表現する際に、CC のクラス/ファミリ/コンポーネントモデルを使用するように要求される。拡張要件は、コンポーネント内に挿入された「EXT」で表示される。

D.3 適用上の注意

適用上の注意は、開発者、評価者及びISSEに対する一般的な情報だけでなく、適合するTOEのセキュリティターゲットの構成にとって関連するか有用であると考えられる、新たな補足情報を含んでいる。適用上の注意はまた、コン

ポーネントの許可された操作に関する助言を含んでいる。

D.4 保証アクティビティ

保証アクティビティは、脅威を緩和するためにTOEに課された機能要件に係る共通評価方法として役立つ。アクティビティは、評価者が、TSSで文書化されるTOEの特定の側面を分析するという指示を含んでおり、従って、TSSの節にこの情報を含めるよう、ST執筆者に暗黙の要件を課す。将来のバージョンはこれらの要件を個別の附属書又は文書に移動させるかもしれないが、PPの本バージョンでは、これらのアクティビティは、直接に、機能上の及び保証コンポーネントに関係している。

附属書 E -用語集

表 18ー用語と定義

用　語	定　義
アクセス制御(Access Control)	定義されるサブジェクトによって、定義されるオブジェクトに対して実行されるよう要求される、定義される操作の実行を許可し又は拒否するために機能するメカニズム又はそのメカニズムを使用することにより達成される結果。
アクセス制御 SFP(Access Control SFP)	アクセス制御を実行するために TOE がどんな属性を使用するかの定義。これはポリシーとは異なる。なぜならポリシーは、これらの値が表わす抽象的な属性を定義するというよりはむしろ、アクセス制御のために使われる特定の値に関連するアクセス制御 SFP の例であるからである。
属性ベースのアクセス制御 (Attribute-Based Access Control)	静的な許可とアクセス制御のリストというよりはむしろ、利用者の属性に基づくアクセス制御の手段。利用者が技術者の場合に特定の資源へのアクセスを許可し、利用者が請負人の場合に同じ資源へのアクセスを拒否するシステムが一つの例である。
使用(consume)	ポリシーを受信し、それを構文解析し、アクセス制御の決定を実行するために使用できるような方法でそれを保管する、TOE の行為
自由裁量のアクセス制御 (Discretionary Access Control)	それらの識別又はグループメンバーシップによって、サブジェクトに発給された権限に基づくアクセス制御の手段。
最終利用者(End User)	TOE によって保護される資源へアクセスしようとする個人。アクセス制御において、サブジェクトとして定義される。
エンタープライズセキュリティ管理(Enterprise Security Management)	企業全体の情報保証サービス、プロセス及びデバイスを提供し操作するための管理監督を指示し、生成し、行きわたらせ、修正し、停止し及び終了するために必要とされるシステムと資源

用　語	定　義
強制アクセス制御(Mandatory Access Control)	企業内のすべてのサブジェクトとオブジェクトは、一つ以上の階層的ラベルに関係しているという考え方に基づくアクセス制御の手段。これらのラベルに割り当てられた支配関係が、アクセスが許可されるかどうかを決定する。
ネットワークのアクセス制御（Network Access Control）	サブジェクトがネットワークトラフィックの集合である場合の、アクセス制御の形式。
環境(Environment)	TOE の境界内にない企業におけるハードウェアとソフトウェア資源の集合。これには、TOE が操作を要求する第三者のソフトウェア・コンポーネント、TOE によって保護される資源及び TOE がインストールされるハードウェアを含んでいるかもしれないが、それらに限られるわけではない。
ポリシー(Policy)	アクセス制御 SFP がどのようにインスタンス化されるか決める規則の集合。これらの規則は、定義されたサブジェクトが定義されたオブジェクトに対して定義された操作を実行することを許可されている条件を定義する。
ポリシー決定ポイント(Policy Decision Point)	アクセス制御方針を使い、それらの有効性を判断するために、該当する規則に対して確認される環境上のふるまいを裁く責任を負う ESM ソリューションのコンポーネント。
ポリシー実施ポイント(Policy Enforcement Point)	ポリシー決定ポイントによって到達された決定に従って行動する責任を負う ESM ソリューションのコンポーネント。
ポリシー管理製品(Policy Management Product)	ポリシー決定ポイントによって使われるポリシーを生成する責任を負うアプリケーション。これらのポリシーは、自動的なメカニズムによって、マニュアルの管理上の入力によって、又は 2 つの何らかのコンビネーションによって生成される。

用　語	定　義
役割ベースのアクセス制御 (Role-Based Access Control)	それらが割り当てられる役割及びそれらの役割に関係する権限に基づき、サブジェクトの要求を認可するアクセス制御の手段。
セキュアな構成管理製品(Secure Configuration Management Product)	ESM の安全構成管理の標準プロテクションプロファイルに適合する製品。そのような製品は、運用環境において配置したシステム及び/又はアプリケーションの状態を判断し、この現状を定義された組織のセキュリティベースラインと比較し、配置がベースラインと一致しない場合、訂正又は通知するアクションを実行することができる。
システムのアクセス制御(System Access Control)	オブジェクトが、コンピュータ・システム上のバイナリ又は資源である場合のアクセス制御の形式。
システム管理者(System Administrator)	運用環境において、オブジェクトに対し管理者権限を持つ個人。
TOE 管理者(TOE Administrator)	PP の関係内では、これは、TOE をセットアップし、TOE が使うポリシーを定義するためにポリシー管理製品を使用し、TOE が生成する監査データを検証する責任を負う 1 人以上の個人を指す。
利用者(User)	最終利用者の項を参照。

附属書 F -PP 識別

F.1 識別

タイトル: エンタープライズセキュリティ管理アクセス制御の標準プロテクションプロファイル

作成者: Booz Allen Hamilton、ESM プロテクションプロファイルベンダーコミュニティを代表し、その承認により

コモンクライテリア識別:: 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、2009 年 7 月 1 日

バージョン: PP バージョン 2.0

キーワード: エンタープライズセキュリティ、アクセス制御、方針実施、データ保護

評価保証レベル(EAL): **EAL 1 追加**

F.2 謝辞

本プロテクションプロファイルは、2008 年 9 月に韓国のチェジュで開催された国際コモンクライテリア会議において、Booz |Allen |Hamilton (BAH)の Winterton 及び CA テクノロジーの Joshua Brickman によって当初提案された。それは、業界、政府/スキーム入力、コモンクライテリアコンサルタント及び評価機関とともに、Booz |Allen |Hamilton によって著された。作成者は、エンタープライズセキュリティ管理プロテクションプロファイル専門委員会のメンバーに、本文書の作成への大変な作業及びコミットメントを感謝したい。