エンタープライズ・セキュリティ管理
ポリシー管理の
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
Policy Management

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_pm_v1.4.pdf

2012 年 5 月 23 日

バージョン 1.4

平成 25 年 2 月 27 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7月15日	最初の完全なバージョン
1.1	2012年2月24～28日	(1.1) ESMアクセス制御PPからの変更内容を取り入れるため更新。 (1.1D1) Justinが確認したマッピングを一部修正するため更新。
1.2	2012年4月16日～5月2日	これまでに受け取ったコメントを挿入するため更新。 ESM PP Teleconからのコメントを挿入するため更新。 FIA_UAU/UIDに関する追加的課題に対処するため更新。 受動送信（passive transmission）を包含するため、FAU_STG_EXT.1内の「transmit（送信する）」という概念を明確化。
1.3	2012年5月4日	2012年5月4日Telecon以降のバージョン
1.4	2012年5月23日	ESM ICM PP開発中に見つけたフォーマッティングに関するマイナーバグ（minor nit）を修正。ESM_ACT.1の保証アクティビティの欠落を確認。 ESM_ACT.1の保証アクティビティを追加。

目次

1 プロテクションプロファイル（PP）序論 7

1.1 はじめに 7

1.2 概要 7

1.3 ESM ポリシー管理プロテクションプロファイルの概要 9

1.4 適合評価対象 12

1.5 共通機能 13

1.6 関連するプロテクションプロファイル 14

1.7 文書構成 14

2 適合主張 16

2.1 CC 適合主張 16

2.2 PP 適合主張 16

2.3 パッケージ適合主張 16

2.4 ST 適合要件 16

3 脅威 17

3.1 管理者によるミス 17

3.2 ポリシーと ESM データの漏洩 17

3.3 未認可のポリシーの作成（Unauthorized Policy Creation） 17

3.4 脆弱なポリシー（Weak Policies） 18

3.5 相矛盾するポリシー・データ 18

3.6 不正な更新 18

3.7 脆弱な認証機能 19

4 セキュリティ対策方針 20

4.1 システム・モニタリング 20

4.2 万全な TOE アクセス（Robust TOE Access） 20

4.3 管理者権限 20

4.4 ポリシーの定義 21

4.5 依存する製品設定 21

4.6 ポリシーのセキュアな配付 22

4.7 アクセス・バナー表示（Access Bannering） 22

5 拡張コンポーネント定義 23

5.1 クラス ESM: エンタープライズ・セキュリティ管理 23

5.1.1 ESM_ACD A アクセス制御ポリシー定義 23

5.1.2 ESM_ACT アクセス制御ポリシーの送信 24

5.1.3 ESM_ATD 属性定義 26

5.2 クラス FAU:セキュリティ監査 28
5.2.1 FAU_SEL_EXT.1 外部選択的監査 28
5.2.2 FAU_STG_EXT.1 外部監査証跡ストレージ 29
5.3 クラス FCS: 暗号化のサポート 30
5.3.1 FCS_CKM_EXT.4 暗号鍵のゼロ化 30
5.3.2 FCS_RBG_EXT.1 ランダムビット生成 31
5.4 クラス FMT:セキュリティ管理 32
5.4.1 FMT_MOF_EXT.1 機能のふるまいに対する外部管理 32
5.4.2 FMT_MSA_EXT.5 適合するセキュリティ属性 33
5.5 クラス FTA:TOE アクセス 34
5.5.1 FTA_SSL_EXT.1 TSF 起動セッション・ロック 34
6 セキュリティ要件 36
6.1 セキュリティ機能要件 37
6.1.1 PP 適用上の注意 39
6.1.2 クラス ESM: エンタープライズ・セキュリティ管理 40
6.1.3 クラス FAU: セキュリティ監査 43
6.1.4 クラス FCS: 暗号化のサポート 49
6.1.5 クラス FIA:識別及び認証 50
6.1.6 クラス FMT：セキュリティ管理 54
6.1.7 クラス FTA：TOE アクセス 62
6.1.8 クラス FTP: 高信頼パス/チャネル 63
6.1.9 未実現の依存性（Unfulfilled Dependencies） 67
6.2 セキュリティ保証要件 68
6.2.1 クラス ADV: 開発 69
6.2.2 クラス AGD: ガイダンス文書 71
6.2.3 クラス ALC: ライフサイクルサポート 74
6.2.4 クラス ASE: セキュリティターゲット評価 76
6.2.5 クラス ATE: テスト 81
6.2.6 クラス AVA: 脆弱性評定 83
6.3 セキュリティ保証要件根拠 85
7 セキュリティ課題定義根拠 86
8 セキュリティ課題定義 93
8.1 前提条件 93
8.1.1 接続性の前提条件 93
8.1.2 物理的な前提条件 93
8.1.3 人的な前提条件 93
8.2 脅威 93
8.3 組織のセキュリティ方針 95

8.4 セキュリティ対策方針 95
8.4.1 TOE のセキュリティ対策方針 95
8.4.2 運用環境のセキュリティ対策方針 97
附属書 A – サポート表と参考文献 98
A.1 参考文献 98
A.2 略語 101
附属書 B – NIST SP 800-53/CNSS 1253 マッピング 103
附属書 C – アーキテクチャのバリエーションと追加要件 113
C.1 属性定義 113
C.1.1 ESM_ATD.1 オブジェクトの属性定義 113
C.1.2 ESM_ATD.2 サブジェクトの属性定義 114
C.2 タイムスタンプ 115
C.2.1 FPT_STM.1 高信頼タイムスタンプ 115
C.3 セッション管理に関するオプションの SFR 115
C.3.1 FTA_TSE.1 TOE セッションの確立 115
C.3.2 FTA_SSL セッションのロック及び終了 116
C.4 暗号の機能要件 118
C.4.1 FCS_CKM.1 暗号鍵作成(非対称鍵用) 119
C.4.2 FCS_CKM_EXT.4 暗号鍵のゼロ化 121
C.4.3 FCS_COP.1(1) 暗号操作(データの暗号化/復号用) 122
C.4.4 FCS_COP.1(2) 暗号操作(暗号署名用) 123
C.4.5 FCS_COP.1(3) 暗号操作(暗号ハッシュ用) 124
C.4.6 FCS_COP.1(4) 暗号操作(鍵付ハッシュ・メッセージ認証用) 125
C.4.7 FCS_RBG_EXT.1 拡張:暗号操作(ランダムビット生成) 126
附属書 D – 文書の表記法 131
D.1 操作 131
D.2 拡張要件の表記法 131
D.3 適用上の注意 131
D.4 保証アクティビティ 132
附属書 E – 用語集 133
附属書 F – 識別 135

図一覧

図 1 プロテクションプロファイルの関係 12

表一覧

表 1 ESM プロテクションプロファイルスイートの要約 8
表 2 TOE 機能コンポーネント 37
表 3 監査対象事象 43
表 4 TOE の管理機能 60
表 5 TOE セキュリティ保証要件 68
表 6 前提条件、環境上の対策方針、根拠 86
表 7 ポリシー、脅威、対策方針、根拠 87
表 8 TOE の前提条件 93
表 9 TOE の前提条件 93
表 10 脅威 94
表 11 組織のセキュリティ方針 95
表 12 TOE のセキュリティ対策方針 95
表 13 運用環境のセキュリティ対策方針 97
表 14 略語と定義 101
表 15 NIST 800-53 要件との互換性 103
表 16 用語と定義 133

1 プロテクションプロファイル（PP）序論

1.1 はじめに

本節には、プロテクションプロファイル（PP）を、プロテクションプロファイル登録を通じて登録できるようにする際に必要となる文書管理及び概括的な情報が収録されている。識別情報は、PP の識別、分類（catalogue）、登録及び相互参照を行う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たものであり、その PP が興味を惹くものかどうか潜在的なユーザが判断するのに十分な情報を提供する。プロファイルの正式な識別については、「附属書 F – 識別」を参照されたい。

1.2 概要

エンタープライズ・セキュリティ管理（ESM）とは、ある組織[1]内の一連の IT 資産を集中的に管理するために使用される製品/製品に関するコンポーネント[2]一式を指す。ESM の機能には 2 つのタイプがある。1 つ目は*ポリシー定義*というタイプで、これは一連の 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る。2 つ目は*ポリシー利用*というタイプで、これはすでに定義してあるポリシーを利用してそれを実施する。この 2 種類の ESM 機能タイプは、ESM プロテクションプロファイルスイート全体において表わされる。

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

- **アクセス制御ポリシー**： 確定したオブジェクト（IT 資産又は IT 資源）に対する、確定したサブジェクト（行為者）に対して行われる特定のアクションを認可又は拒否するポリシー。
- **識別情報及びクレデンシャル情報に関するポリシー**： サブジェクトの識別情報、認証、認可（authorization）及び説明能力（accountability）のために使用される属性を定義し維持するポリシー。
- **オブジェクト属性ポリシー**： オブジェクトのために使用される属性を定義し維持するポリシー。
- **認証ポリシー（Authentication Policies）**： 利用者がエンタープライズ・システムから認証される環境を定義

[1] ESM の使用法では、「組織」という用語ではなく「エンタープライズ」という用語をよく使用する。これは、エンタープライズの総体が組織の境界線を越えているのではないかという事実を反映するためである。

[2] 技術的な意味では、「製品」という用語は正確ではない。しかしそれ以外の例えば「システム」というような用語も正確とは言い難く、過剰な表現である。ESM「システム」内の様々な「製品」は、他とは異質の製品であると言えよう（may）。また、それは、単に ST に記載される、比較的大型の製品内部で使用された半製品又は機能であると言えよう（may）。「製品」という用語を使用するのは単位に、セキュリティ・ターゲットが製品について説明するというだけの理由からであり、これ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システムとは対照的である。したがって、PP は通常特定のベンダの実装には依存しない方法で製品（又は製品のコンポーネント）について説明する。

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**: 監査データがエンタープライズ全体にわたって収集、集積、報告、及び維持される方法を定義するポリシー。

様々なポリシーを利用し、それを実施する ESM 製品/製品コンポーネントでは、以下のタイプのセキュリティが提供される。

- **予防的**: エンタープライズで定義された中心的なポリシーの侵害であると判明した場合、IT 資産に対して実行されるアクションは禁止される。
- **検知的**: 非セキュアな、悪意のある、又は、エンタープライズにまたがる不適当なふるまいのパターンを検知することができるよう、利用者及び IT 資産のふるまいは監査され集積される。
- **反応的**: IT 資産は組織で定義されたセキュアで中心的な定義と対比され、不一致が確認された場合には処置が講じられる。

ESM PP スイートは、6 種類のプロテクションプロファイルから成り、その特徴は以下のようなものと考えられる（may）。

表 1 ESM プロテクションプロファイルスイートの要約

プロテクションプロファイル	アクセス制御ポリシー	識別情報及びクレデンシャル情報に関するポリシー	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識別情報及び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)

プロテクションプロファイル	アクセス制御ポリシー	識別情報及びクレデンシャル情報に関するポリシー	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 = Consume（利用する）; D = Define（定義する）; E = Enforce（実施する）						

注： 1） TOE がどのよう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 で定義されるが、その両方で定義されるというわけではない。
3） 認証ポリシーは、許可された利用者が TOE から認証されなければならない（must）という意味で使用される。

1.3 ESM ポリシー管理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では、**アクセス制御ポリシーの定義と管理**を重点的に扱う。ESM ポリシーの管理者は、企業の中でどのようにしてオブジェクトを保護すべきかを決定するために、ESM ポリシー管理製品（PM）を使用することで、アクセス制御の製品を設定し、それを管理することができるようになる。この管理活動から生み出されるものが、アクセス制御製品に対するポリシーの生成と配付である。PM は、例えば、監査対象事象、監査対象事象データの格納先、PM との通信喪失の事象においてどのように運用すべきかについても、本製品の基本的なふるまいを制御できるべきである（should）。

ESM PM PP に準拠している TOE には、以下のふるまいを示すことが想定されている。

- TOE 自体と他のエンタープライズ・セキュリティ管理（ESM）製品との間に高信頼チャネルを確立する。
- 識別情報の証拠を他のエンタープライズ・セキュリティ管理製品に提供する。
- 識別情報の有効性確認を行い、ポリシー管理者の権限を決定するために、組織のサブジェクトと属性データを活用する。
- ポリシーの作成と配付を行うために、ポリシー管理者に、高信頼のリモート・インタフェース又はローカル・インタフェースを提供する。
- 同じアクティビティに対して認可と拒否の両方を与える規則のように、矛盾するデータが含まれる可能性のあ

るポリシーの競合を回避する。

- アクセス制御製品のポリシー実施のふるまいを設定する能力を提供する。
- 管理的なふるまいの監査証跡を生成する。

オプションとして、TOE は、後々ポリシー実施の際に使用されるサブジェクト又はオブジェクトの属性を定義する能力を提供することができる（may）。例えば、その TOE が、強制アクセス制御モデル（Mandatory Access Control: MAC）を利用するホストベースのアクセス制御製品を管理する場合には、機密レベルを明確に定義してオブジェクトに関連付け、クリアランスをサブジェクトに関連付ける必要がある。この機能は、TSF により実装されることができる（may）。アクセス制御の実施でサブジェクト又はオブジェクトの属性管理が必要であり、この管理が TSF によって実施されない場合、セキュリティターゲット（ST）作成者は、これらの属性がどのように定義され維持されるのかを指示しなければならない（must）。例えば、オブジェクト属性は、運用環境内のオペレーティング・システムで維持することができる（may）。

なお、これは ESM PP ファミリに属している多数のプロテクションプロファイルの 1 つである。本 PP は、1 つの ESM システムの 1 つのコンポーネントで利用されるよう意図されており、単独で機能するようには意図されていない。少なくとも互換性のあるアクセス制御製品は少なくとも 1 つ識別されていなければならない（must）。互換性は、TOE によって作成されるポリシーを利用するその製品の能力によって定義される。組織内でアクセス制御がどのように実装されるかによって、ID 管理、認証、及び監査のための ESM PP ソリューションが同様に実装される必要となることがある（may）。これらのコンポーネントのいずれかが、組織のベースラインとして活用されることが想定されている場合には、セキュアな構成管理ソリューションも活用される必要となることがある（may）。適用可能な ESM PP 評価済み製品をいずれも使用せずにソリューションが配備された場合、顧客は企業アーキテクチャの全般的なセキュリティを著しく侵害する可能性がある。

図 1 は、基本レベルで TOE が配置されると想定される状況を示したものである。TOE はシステム上にあり、サブジェクトとオブジェクト間のアクセス・ポリシーを定義する。サブジェクトの識別は、TOE の外部ソース（例えば『Standard Protection Profile for ESM Identity and Credential Management（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）』に適合しているもの）で定義されることになっている（is expected to）。TOE を運用する上で、監査ログ、設定情報、及びポリシー情報などのセキュリティ関連データをローカル保管する必要となることがある（may）。TOE によって定義されたポリシーは、『Standard Protection Profile for ESM Access Control（ESM アクセス制御標準プロテクションプロファイル）』に適合している製品に送信されて利用される。

また監査データも、『Standard Protection Profile for ESM Audit Management（ESM 監査管理の標準プロテクションプロファイル）』に適合している製品によってリモートのリポジトリに書き込まれることが可能で、そこで他のデータ・ストリームとともに情報を集約することができる。TOE は、システム内の設定項目に関する重要な ESM 規則を含むセキュアな構成管理製品によってモニターされると想定されている。この製品はまた、ポリシーが更新されなければならない（must）時に決定すべき、TOE とその接続先であるアクセス制御製品のポリシー・バージョンも監視することになる。

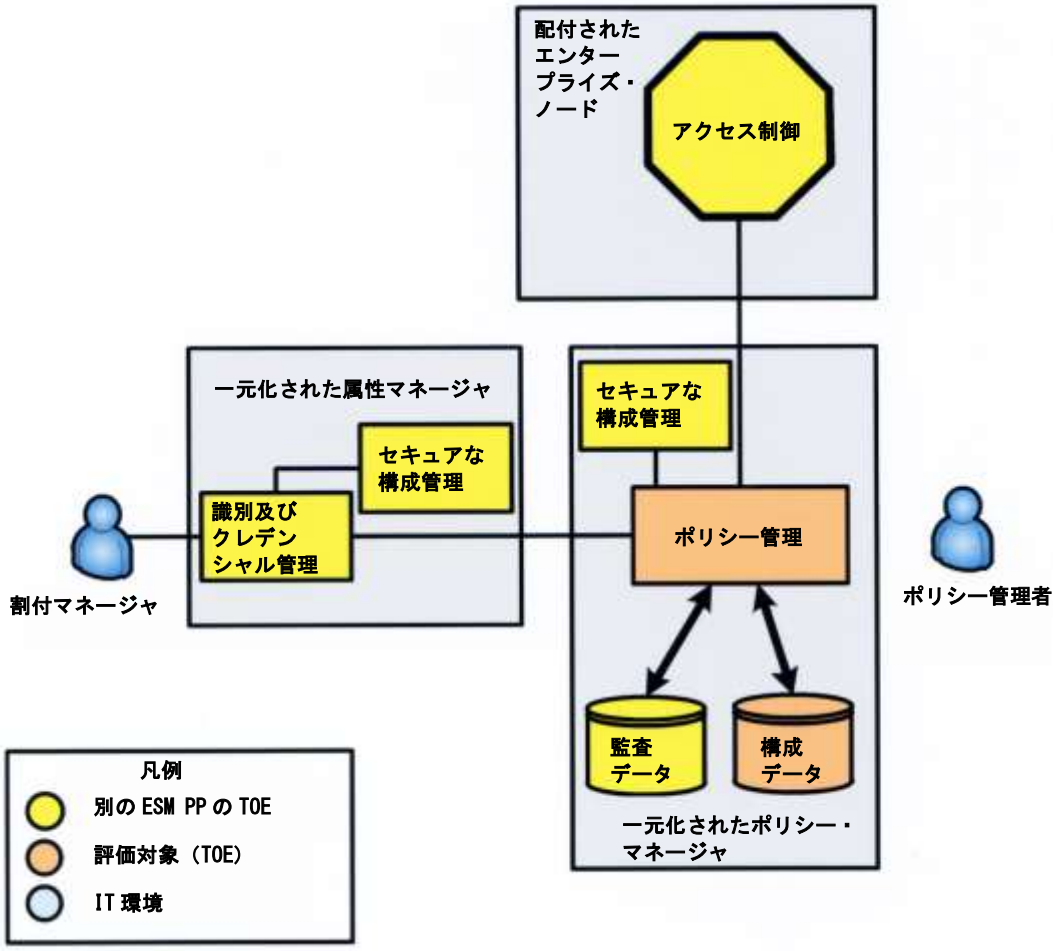

図 1 プロテクションプロファイルの関係

1.4 適合評価対象

ポリシー管理製品の目的は、1 つ以上のアクセス制御製品によって最終的に利用されるポリシー情報のための信頼できるソースとして役立つことである。このポリシーは、運用環境において保護を受けるべき資源はどれか、その資源にアクセスを許可されているのはどのサブジェクトか、及びこのアクセスに含まれることが許可されている操作一式にはどのようなものがあるのかを判断する。PP はアクセス制御で使用される何らかの特定な様式を規定することはない。望ましいアクセス制御メカニズムを実施できる場合には、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）をはじめとするポリシーを任意に定義することができる。

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するポリシーを定義できると思われる（may be able to）。どのような資源が保護されるのか、アクセス許可又はアクセス拒否の方法を判断する際にはどのような属性が使用されるのかということを明確に示すことは、セキュリティターゲット（ST）作成者の責務である。また ST は、TOE によって定義されたポリシーを利用できるアクセス制御製品をはじめとし、ポリシー定義の際に使用する組織データを TOE に提供する可能性がある ESM 製品も示されなければならない（must）。

TOE は、ハードウェア又はソフトウェアとして配置されることもあれば、冗長性を持つ配付型システムとして、あるいはサーバ又はネットワーク境界デバイス上に常駐する単一エージェントとして配置されることもある（may）。コンプライアンスは厳格であるという性質上、運用環境の目標は、TOE によって満たされているものであるとして主張されてはならない（may not be claimed）点に留意されたい。ESM ポリシー管理製品で運用環境の目標が達成される可能性のある一般的なケースについては、開発者は、CCEVS（NIAP Common Criteria Evaluation and Validation Scheme）用いて作業し、このプロファイルの将来のバージョンで、この SFR（セキュリティ機能要件）をオプション SFR として追加しなければならない（must）。

TOE は大規模な ESM システム内のサブシステムの 1 つになると予想されている（is expected）。ESM 製品全体は、適用可能な全ての ESM プロテクションプロファイルで評価されることになっている（is expected）。

1.5 共通機能

本プロテクションプロファイル（PP）は、ESM のセッティングでポリシー管理を実行することができるあらゆる製品によって満たされることになっている一連の要件を定義するものである。『Standard Protection Profile for ESM Access Control（ESM アクセス制御標準プロテクションプロファイル）』では、アクセス制御を実施できる技術タイプが多数定義されている。こうした技術タイプには、ポリシーによってアクセス制御ができるだけ詳しく定義できるよう、それぞれに対して最低限のオブジェクト一式が定義されている。本 PP への適合を主張するセキュリティターゲット（ST）は、それによってポリシーを定義できる該当の技術タイプを残らず識別すべきである（should）。そして、該当するアクセス制御製品に用いる要件がその内容でどのように満たさされているかを明示するために、このポリシーはできるだけ詳細に記述されるべきである（should）。

技術の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を主張する製品は、**組織的に定義されている**サブジェクトと属性を扱うことが必須となる。ESM 製品の目的は、サブジェクトと属性に関するデータに対して *一元的な（centralized）*定義を提示することである。ST 作成者は、TOE が活用することになる組織データ、データの受信元である高信頼ソース、及びこのデータが解釈されるメカニズム（SAML アサーションや X.509 証明書など）を定義しな

ければならない（must）。さらに、ポリシーを記述してアクセス制御製品を設定することができるのが許可されたサブジェクトのみとなるよう、ポリシー管理製品は、その製品独自の内部アクセス制御を実施することができなければならない（must）。

また、本 PP への適合を主張する製品には、その製品独自の識別情報をアクセス制御製品に送信し、その製品によって生成されるポリシー・データの受理を受信する機能を提供することが想定されている。これは必須機能であるため、これによって、アクセス制御製品は、真のソースからポリシー・データを受信していることが保証され、かつ、ポリシー管理製品は、指定したポリシーが、適切なアクセス制御製品によって受信されたことが保証される。

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）製品のために記載された一連のプロテクションプロファイルの一つである。以下は、本プロテクションプロファイルを補完するプロテクションプロファイルである。

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

本プロテクションプロファイルへの適合を主張する製品は、他のプロテクションプロファイルに適合しており互換性のある環境の製品を識別しなければならない（must）。多数のプロテクションプロファイルと互換性のある機能を TOE が実行する場合、該当するプロテクションプロファイルのいずれに対しても適合を主張しなければならない（must）。

1.7 文書構成

第 1 章では、プロテクションプロファイルの概要資料が提供されている。

第 2 章では、本プロテクションプロファイルに該当する適合主張が述べられている。

第 3 章では、ある TOE に対して生じる可能性のある脅威のタイプが定義されている。

第 4 章には、TOE が満たすことになっている対策方針が定義され、こうした対策方針へのコンプライアンスを明らかにしたセキュリティ機能要件がリストされている。

第 5 章では、本プロテクションプロファイルの中で使用される拡張コンポーネントが定義されている。

第 6 章では、TOE がプロテクションプロファイルに適合しているために主張されなければならない（must）セキュリティ機能要件とセキュリティ保証要件がリストされ、説明されている。

第 7 章では、プロテクションプロファイルの中で定義された前提条件、脅威、対策方針及び要件のあいだのマッピングが示されている。

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

この文書には、以下の附属書も含まれている。

- 附属書 A - 参考文献の一覧と、本書で使用されている略語が収録されている。
- 附属書 B - TOE の評価と認証の取り組みに対する適用可能性をすぐに確認できるようにプロテクションプロファイルと他の規格との関係が記述されている。
- 附属書 C – 適合したプロテクションプロファイルに採用することができる（may）オプション要件（暗号化の機能や、サブジェクト又はオブジェクトの属性管理のためのオプション要件をはじめとする要件）が定義されている。
- 附属書 D – 本書で使用している表記法について説明されている。
- 附属書 E – 本書で使用している用語の定義が記載されている。
- 附属書 F – 正式な PP 識別情報が示されている。

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 に適合している。

2.2 PP 適合主張

本プロテクションプロファイルは、他のプロテクションプロファイルへの適合を主張しない。

2.3 パッケージ適合主張

本プロテクションプロファイルは、追加された EAL1 のパッケージを主張する。

2.4 ST 適合要件

本プロテクションプロファイルへの適合を主張するセキュリティターゲットは、CC パート 1 の D.2 節で定義されている厳格な適合について最低限の基準を満たさなければならない（shall）。

厳格な PP 適合とは、PP で示されている要件が満たされ、ST が PP の具体化（instantiation）の 1 つであることを意味する。ST は PP よりも広範となる。ST は、運用環境が最大で PP と同じことを行うのに対して、TOE が最低限 PP と同じことを行うことを明記する。本 PP では、明記された要件の意図及びベンダがどのように要件を満たすかに関する期待をさらに明確にして説明するために、「適用上の注意」が示されている。ST の評価者は、ST とその ST で記述された TOE の中に、本 PP に記載されている全文（おそらくはそれ以上）が含まれているだけでなく、「適用上の注意」で述べられている期待が満たされると判断することによって、PP に対する厳格なコンプライアンスを確認することが期待されている。

保証について言えば、ST には、本 PP で述べられているものと同等又はそれよりも厳しい保証要件が含まれること、及び本 PP で述べられている全ての保証アクティビティが実行されることが期待されている。

3 脅威

以降の各節では、TOE に対して存在する脅威について列挙する。

3.1 管理者によるミス

悪意のある管理者又は不注意な管理者が、確定したセキュリティ要件に適合しない方法で TOE を設定したり、それを操作したりした場合、その TOE によって提供されたセキュリティ機能は、不適切なものになると考えられる（may）。例えば、そのセキュリティ機能は、暗号化通信を有効にすることができなくなったり、適切なパスワード・ポリシーを設定できなったりするか、必要のない利用者に必要以上の管理権限を割り当てる可能性がある（may）。TSF ではこうしたインシデントを防ぐことができないのに対し、明確な管理ガイダンスの配付により、過失が低減されることが期待されている。また、（利用規約に反する結果を明確に列挙した）利用規約（acceptable use）に関するバナーの表示は、何らかの悪意のあるアクティビティを抑制するのではないかと考えられる（may）。

[T.ADMIN_ERROR]

3.2 ポリシーと ESM データの漏洩

エンタープライズ・セキュリティ管理のアーキテクチャでは、遠隔装置間でデータ送信を行うことが、データが機能する（function）うえではほぼ確実に要求されることになる。TOE は、離れた場所にあるアクセス制御製品に対して、実施すべきポリシーを配付する（distribute）こともある（may）。TOE は、利用者属性又はセッション・データを、その環境内のどこか別の場所で受信することもあるし、離れた場所にある集中型のリポジトリに監査データを書き込むこともある（may）。このデータがセキュリティの程度が十分な高信頼チャネルによって保護されていなければ、不本意な漏洩が起こる可能性がある（may）。このデータにアクセスすることで攻撃者は、偵察目的にそれを使うか、正当な利用者又はエンティティになりすまそうとする場合には、既知の有効な情報を再現するためにそれを使うことができる。

[T.EAVES]

3.3 未認可のポリシーの作成（Unauthorized Policy Creation）

TSF がそれを使おうとしている人物を決定し、この識別データに基づいて認可を定義する十分な手段を提供しない場合、そのポリシーが完璧であり正確であるという保証はなくなる。認証機能に設計や実装上の不備があると、攻撃者に対して TSF への違法なアクセスを許してしまうことになり、管理機能を実行する試みを許してしまうことになる。データ保護機能に設計や実装上の不備があると、アクセス制御チェックがバイパスされ、権限昇格（privilege

escalation）が許可される。攻撃者がポリシー作成能力に対する違法アクセスを入手する方法がいかなるものであっても、その組織のアクセス制御ポリシーの完全性が危殆化する結果は同じである。

[T.UNAUTH]

3.4 脆弱なポリシー（Weak Policies）

『Standard Protection Profile for Enterprise Security Management Access Control（エンタープライズ・セキュリティ管理アクセス制御標準プロテクションプロファイル）』では、様々な技術タイプが規定され、各技術タイプに対して十分詳細なポリシーを定義できるよう、サブジェクト、オブジェクト、操作及び属性の最低限のセットが規定されている。ポリシー管理製品は、互換性を備えたアクセス制御製品が利用できるのと同程度の詳細さを備えたポリシーを作成できなければならない（must）。詳細さの不十分なポリシーは、意図しないアクティビティを許可するか、間違って正当な使用を制限するので、無効なアクセス制御メカニズムである。

[T.WEAKPOL]

3.5 相矛盾するポリシー・データ

アクセス制御ポリシーには潜在的に、様々なオブジェクトへのアクセスを許可したり禁止したりするいろいろの複雑な規則が数多く含まれている。この結果、1 つのポリシーの中に相矛盾する規則が含まれることがある。例えば、同じポリシー内で、特定の利用者に対して、特定のプログラムをホスト上で動かす能力を許可する規則もあれば、その利用者が属しているグループの全員がそれと同じプログラムを動かすことを禁じる規則が存在することもある（may）。こうした矛盾を抱えるポリシーがアクセス制御製品で利用された場合には、その製品からは予測できない結果が生じる可能性がある（may）。

[T.CONTRADICT]

3.6 不正な更新

アクセス制御製品が、更新されたポリシー情報と思われるものを TOE から受信したときは、そのアクセス制御製品は、そのポリシーの真正性（authenticity）と送信者の識別について同じ保証を確保しなければならない（must）。通信チャネルの保護が不十分な場合や、ポリシーの完全性を TOE が保証するメカニズムが万全でない場合、ポリシーを送信するときに使用する構文を把握している攻撃者は、偽の構文を勝手に捏造し、アクセス制御製品に利用させることができる可能性がある（may）。

こうしたことが起きた場合、アクセス制御製品は、未認可のアクセスを許可する許容的偽ポリシー（permissive fake policy）を実施したり、正当なアクティビティを実行できなくする制限的偽ポリシー（restrictive fake policy）を実行したり、フォーマットの正しくないポリシーを利用したり、アクセス制御製品が存在するシステム内のメモリ空間に対する攻撃者からのアクセスを終了させるか許可したりする設定にされる可能性がある（may）。

[T.FORGE]

3.7 脆弱な認証機能

TSF が管理者特権を定義する能力は、TSF の認証機能が総当たり攻撃による推測（brute force guessing）にさらされる恐れがある場合には、不正使用を予防しない。TSF は、総当たり方式によって攻撃者が TOE の認証を得る能力を限定するために、ログインを失敗させるメカニズム（login frustration mechanism）を提供しなければならない（must）。

[T.WEAKIA]

4　セキュリティ対策方針

4.1　システム・モニタリング

誤ったTOE設定や、保護されたオブジェクトに対して試みられた不正アクティビティを識別するために、TOEは、監査証跡を維持する能力を提供することになっている。この監査証跡では、TOE でどのポリシーが定義されているかを識別することで、システム操作に関する管理上の洞察の提供が可能になるべきである（should）。また、この監査証跡では、TSFで保護されているオブジェクトに対して今現在実行されているアクティビティがどのタイプであるかを識別することも可能である。

膨大な監査データで圧倒されているTOEのリスクを軽減し、ESM監査管理システムとの潜在的な適合を容易にするために、TOE は、外部の高信頼エンティティに対して監査データを送信することができるべきである（should）。こうすることで、監査データの可用性の可能性が高まっていくことになる。

本 PP は、この高信頼エンティティがアクセス不可の状態である場合でも、特定の措置を取ることを強制しない。この場合、ST作成者はTOEが示すふるまいを記録すべきである（should）。
(O.AUDIT: FAU_GEN.1、FAU_STG_EXT.1、FPT_STM.1 (オプション))

4.2　万全な TOE アクセス（Robust TOE Access）

無知な攻撃者が、繰り返された推測情報を使用してTOEに対して不正な認証を試みた場合、成功の可能性は、認証機能にアクセスできる時間内に攻撃者が試すことのできる認証試行の回数及び各試行の成功の可能性という2 つの要因に左右される。TOE は、こうした要因に関連するセキュリティを強化するメカニズムを提供することになっている。TOEはまた、（附属書 C.3で定義されているオプションの SFR により）セッション確立を拒否する機能と、確立後のセッションを中断又は終了する機能を提供してもよい（may）。

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

4.3　管理者権限

ポリシー管理者は、TSF により、TOE の管理とポリシーの作成に対して様々な責任を付与されるよう指名される。TSFは、もしサブジェクトが識別され、認証され、認可されない場合には、いかなるアクションも TSF に対して実行できないよう、制御されたアクセスの実施に関する独自の内部的な方法を持つ。
(O.AUTH: FIA_UAU.2、FIA_UID.2、FIA_USB.1、FMT_MSA.1(1)、FMT_SMR.1、FTP_TRP.1)

4.4 ポリシーの定義

TOE の第一の目的は、1 つ以上の技術タイプに対して万全なアクセス制御を実施するに足る詳細なポリシーを作成することである。したがって、TSF には少なくとも、該当する技術タイプ（これは『Standard Protection Profile for Enterprise Security Management Access Control（エンタープライズ・セキュリティ管理アクセス制御標準プロテクションプロファイル）』の利用者データ保護に関する要件で説明されている）と一致するポリシー属性の管理をできるようになることが求められている。さらに、TSF は、ポリシーが一義的に定義されているよう、ポリシー適用の際の不適合を検知し、それを回避することができるようになる。最終的には TOE もまた、リモート製品では今現在どのポリシーが実装されているのかを判断するのにそれを使用できるよう、作成するポリシーの一意的な識別もできるようにならなければならない（must）。TSF は、後々ポリシー定義の際に使用できるサブジェクトとオブジェクト（又はこのうちのいずれか）の属性を任意で定義し、（後々信頼できるソースとして役立て）てもよい（may）。例えば、必須となっているアクセス制御ポリシーの定義と併せて、TOE が、セキュリティラベルをオブジェクト属性として定義し、クリアランス（clearance）をサブジェクト属性として定義する機能を付与し、このラベルに基づいて認可されたアクセスを定義するポリシーを配付してもよい（may）。

(O.CONSISTENT、O.POLICY: ESM_ACD.1、ESM_ATD.1（optional）、ESM_ATD.2（オプション）、FMT_MSA.1(2)、FMT_MSA.3、FMT_MSA_EXT.5、FMT_SMF.1)

4.5 依存する製品設定

アクセス制御製品で利用されるポリシーの提供に責任を持つほかに、TOE は、これらの製品の機能のふるまいも設定できるようにしなければならない（must）。この中には、どんなイベントを監査するか、どんなポリシーを実施するか、失敗状態又は接続が失われた場合にどう対応するかという設定が含まれる。

(O.MANAGE: FAU_SEL_EXT.1、FMT_MOF_EXT.1、FMT_MSA.1(2)、FMT_SMF.1)

4.6 ポリシーのセキュアな配付

3.2 節で説明した理由から、ポリシーの漏洩防止は重要なことである。同様に、もしデータ送信中に攻撃者がポリシーや管理コマンドを修正できるならば、保護されている資産のセキュリティにリスクが及ぶことになる。その結果、TSF は、識別と認証を受けたエンドポイントへの高信頼チャネルを確立し、修正又は漏洩から守られているポリシーを配付することが求められている。また TSF は、こうした高信頼チャネルのセキュアな確立の際に使用する自身の識別の証拠も提示すべきである（should）。

(O.ACCESSID、O.AUTH、O.DISTRIB、O.EAVES、O.INTEGRITY、O.SELFID: ESM_ACT.1、FCS_CKM.1（オプション)、FCS_CKM_EXT.4（オプション)、FCS_COP.1(1)（オプション)、FCS_COP.1(2)（オプション)、FCS_COP.1(3)（オプション)、FCS_COP.1(4)（オプション)、FCS_RBG_EXT.1（オプション)、FIA_UID.2、FIA_UAU.2、FTP_ITC.1(1)、FTP_ITC.1(2)、FTP_TRP.1)

4.7 アクセス・バナー表示（Access Bannering）

TOE の適切な利用に関するガイダンスを順守する可能性を高めるために、TOE には、その利用規約（acceptable use）を規定する認証に先立って、バナー表示することが求められている。このバナーには、法的な調査が必要になった場合に監査データが適格となる監視に関する法律上の注意事項も記載される。

(O.BANNER: FTA_TAB.1)

5　拡張コンポーネント定義

ここでは、本 PP で説明しているすべての拡張コンポーネントに関する定義を紹介する。6.1 節で規定されている必須コンポーネント及び「附属書 C」に規定されているオプションのコンポーネントの両方が含まれる。

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、認可、説明能力及びコンプライアンスというアクティビティの集中的管理をサポートするふるまいに関係している。このクラスは、データ保護及び認証というアクティビティで使用されるデータを示すよう TSF に要求することで、クラス FDP 及び FIA をサポートする機能的なアクティビティを規定する。

5.1.1　ESM_ACD A アクセス制御ポリシー定義

ファミリのふるまい

このファミリの要件により、TSF は、ESM 配置で使用する際のアクセス制御ポリシーを明確に定義する能力を確実に確保する。

コンポーネントのレベル付け

このファミリのコンポーネントは ESM_ACD.1 の 1 つのみである。アクセス制御ポリシー定義 ESM_ACD.1 は、外部のアクセス制御製品が利用するためのアクセス制御ポリシーを定義できるよう TSF に要求する。

5.1.1.1　ESM_ACD.1 アクセス制御ポリシー定義

ESM_ACD ファミリは、アクセス制御ポリシーを定義するための要件を定義する。これにより、TSF で定義された属性データを活用することで、他の ESM 製品も独自のセキュリティ機能を実行することができる。ESM_ACD.1 要件が追加されたのは、TOE から見て外部にある製品のふるまいを管理するポリシーを定義する、TSF の能力に関する要件の記載が CC のパート 2 にないためである。

下位階層:	なし
依存性:	なし
ESM_ACD.1.1	TSF は、互換性を備えた 1 つ以上のアクセス制御製品が利用するためのアクセス制御ポリシーを定義する能力を提供しなければならない（shall）。

ESM_ACD.1.2　TSF で定義されるアクセス制御ポリシーには、以下の内容を盛り込まなければならない（must）。

a. サブジェクト：**[割付：アクセス制御決定のために使用できるサブジェクト及びそのサブジェクトが導出されるソースのリスト]** 及び

b. オブジェクト：**[割付：アクセス制御決定のために使用できるオブジェクト及びそのオブジェクトが導出されるソースのリスト]** 及び

c. 操作：**[割付：アクセス制御を決定するために使用できる操作及びその操作が導出されるソースのリスト]** 及び

d. 属性：**[割付：アクセス制御を決定するために使用できる属性、及びその属性が導出されるソースのリスト]**

ESM_ACD.1.3　TSF は、各ポリシーに一意の識別を関連付けなければならない（shall）。

管理:ESM_ACD.1

FMT の管理機能については、以下のアクションを考慮できる可能性がある（could）。

a）ポリシーの作成と修正。

監査:ESM_ACD.1

PP/ST に、ESM_ACD.1 識別情報及びクレデンシャル情報に関する定義が含まれている場合には、以下のアクションを監査対象にするべきである（should）。

a）最小：ポリシーの作成と修正。

5.1.2　ESM_ACT アクセス制御ポリシーの送信

ファミリのふるまい

このファミリの要件により、TSF は、定義されたアクセス制御ポリシーを他の ESM 製品に送信する能力を確実に確保する。

コンポーネントのレベル付け

このファミリのコンポーネントは ESM_ACT.1 の 1 つのみである。アクセス制御ポリシーの送信を意味する ESM_ACT.1 は TOE に対し、この ST 作成者が定義した条件下では TSF の外部に位置する互換性を備えかつ許可された ESM 製品宛てに、ESM_ACD.1 で定義されたアクセス制御ポリシー・データを送信することを要求している（require）。

5.1.2.1 ESM_ACT.1 アクセス制御ポリシーの送信

ESM_ACT ファミリは、エンタープライズ・ポリシーの属性の要件を定義する。これにより、他の ESM 製品は TSF で定義された属性データを活用することで、独自のセキュリティ機能を実施できる。ESM_ACT.1 要件が追加されたのは、TSF がアクセス制御ポリシー・データを外部エンティティに配付する能力に関する要件の記載が CC のパート 2 にないためである。

下位階層:	なし
依存性:	ESM_ACD.1 アクセス制御ポリシー定義
ESM_ACT.1.1	TSF は、以下の環境下では、互換性を備えかつ許可されたアクセス制御製品に対してポリシーを送信しなければならない（shall）。[選択：1 つ以上選択：新たにポリシーを作成した直後又は更新されたポリシーの作成直後、定期的、互換性を備えたセキュアな構成管理製品からの要求があり次第、**[割付：他の環境]**]。

管理:ESM_ACT.1

FMT の管理機能については、以下のアクションを考慮できる可能性がある（could）。

a) 送信対象となっているアクセス制御ポリシー・データの仕様。

b) このデータの送信が行われる環境の仕様。

c) このデータの送信先の仕様。

監査:ESM_ACT.1

PP/ST に、ESM ACT.1 アクセス制御ポリシーの送信が含まれている場合には、以下のアクションを監査対象にしておくべきである（should）。

a) 最小: 外部のプロセス又はリポジトリへの識別情報とクレデンシャル情報の送信。

5.1.3 ESM_ATD 属性定義

ファミリのふるまい

このファミリの要件により、TSF は、後々アクセス制御ポリシーの定義と実施の際に使用できる運用環境の属性を明確に定義する能力を確実に確保する。

コンポーネントのレベル付け

このファミリには、ESM_ATD.1 及び ESM_ATD.2 という 2 つのコンポーネントがある。この 2 つのコンポーネント間に階層はない。オブジェクト属性定義 ESM_ATD.1 は、TSF に対して、ポリシー関連のオブジェクト属性のセットを定義できるよう要求する。サブジェクト属性定義 ESM_ATD.2 は、TSF に対して、ポリシー関連のオブジェクト属性[3]のセットを定義できるよう要求する。いずれの場合も、この属性は、アクセス制御に対処する場合に使用するために、運用環境にある制御されたエンティティに後々関連付けられることになっている（are expected to）。オブジェクト属性の例には、強制アクセス制御（MAC）環境で使用するセキュリティラベルや、組織のイントラネット内にあるウェブ・ページと関連付けることのできる保護レベルなどが挙げられる。サブジェクト属性の例には、定義された識別に関連付けられるクリアランスや MAC 範囲（MAC range）などが挙げられる。

5.1.3.1 ESM_ATD.1 オブジェクト属性定義

ESM_ATD.1 コンポーネントは、オブジェクト属性の仕様要件を定義する。これにより、他の ESM 製品は TSF で定義された属性データを活用することで、独自のセキュリティ機能を実行できる。ESM_ATD.1 要件が追加されたのは、運用環境にあるオブジェクトに関連付けられている属性を定義する、TSF の能力に関する要件の記載が CC のパート 2 にないためである。

下位階層:	なし
依存性:	なし
ESM_ATD.1.1	TSF は、以下に示した各オブジェクトに属しているセキュリティ属性のリストを維持しなければならない（shall）。[割付：セキュリティ属性のリスト]
ESM_ATD.1.2	TSF は、セキュリティ属性を各オブジェクトに関連付けることができなければならない（shall）。

[3] 言い換えれば、アクセス制御コンポーネントにより実施されるポリシーに関連した属性。サブジェクトは、識別情報とクレデンシャル情報に関連した追加属性を持つことができる（may）。ポリシー管理コンポーネントでは、サブジェクト属性の管理能力はオプションである。システム設計者は、識別情報とクレデンシャル情報管理コンポーネント内の機能を提供するほうを選択することができる（may）。

管理:ESM_ATD.1

FMT の管理機能については、以下のアクションを考慮できる可能性がある（could）。

a）オブジェクト属性の定義。
b）属性とオブジェクトとの関連付け。

監査:ESM_ATD.1

PP/ST に、ESM_ATD.1 オブジェクト属性定義が含まれている場合には、以下のアクションを監査対象にしておくべきである（should）。

a）最小: オブジェクト属性の定義。
b）最小: 属性とオブジェクトとの関連付け。

5.1.3.2 ESM_ATD.2 サブジェクト属性定義

ESM_ATD.2 コンポーネントは、サブジェクト属性の仕様要件を定義する。これにより、他の ESM 製品は TSF で定義された属性データを活用することで、独自のセキュリティ機能を実施できる。特に、サブジェクト属性は、識別管理コンポーネントにより維持され、アクセス制御コンポーネントにより利用される可能性がある（might）。ESM_ATD.2 要件が追加されたのは、運用環境にあるサブジェクトに関連付けられている属性を定義する、TSF の能力に関する要件の記載が CC のパート 2 にないためである。

下位階層:	なし
依存性:	なし
ESM_ATD.2.1	TSF は、次に示した各サブジェクト属しているセキュリティ属性のリストを維持しなければならない（shall）: [**割付: *セキュリティ属性のリスト***]
ESM_ATD.2.2	TSF は、セキュリティ属性を各サブジェクトに関連付けることができなければならない（shall）。

管理: ESM_ATD.2

FMT の管理機能については、以下のアクションを考慮できる可能性がある（could）。

a）サブジェクト属性の定義。
b）属性とサブジェクトとの関連付け。

監査:ESM_ATD.2

PP/ST に、ESM_ATD.2 サブジェクト属性定義が含まれている場合には、以下のアクションを監査対象にしておくべきである（should）。

a）最小: サブジェクト属性の定義。
b）最小: 属性とサブジェクトとの関連付け。

5.2 クラス FAU:セキュリティ監査

5.2.1 FAU_SEL_EXT.1 外部選択的監査

FAU_SEL_EXT.1 ファミリは、外部 IT エンティティでの監査対象事象を定義するための要件を定義する。監査対象事象とは、FAU_GEN.1 で定義された監査データとして書き込まれる監査データを生じさせる状況を指す。FAU_SEL_EXT.1 要件が追加されたのは、所定の外部エンティティに対する監査対象事象を定義する、TSF の能力を明示する選択的監査要件の記載が CC のパート 2 にないためである。

下位階層: なし。

依存性: FAU_GEN.1 監査データの生成
FMT_MTD.1 TSF データの管理

FAU_SEL_EXT.1.1 TSFは、以下の属性に基づいて、ESMアクセス制御製品の監査対象である事象一式を監査対象事象の全一式から選択できなければならない（shall）。

a. [選択:オブジェクト識別、利用者識別、サブジェクト識別、ホスト識別、事象種別]、及び

b. **[割付:監査選択度が基準にしている追加的な属性のリスト]**

管理: FAU_SEL_EXT.1

FMT の管理機能については、以下のアクションを考慮できる可能性がある（could）。

a) TSF によって設定されることになる外部 IT エンティティの仕様。
b）外部 IT エンティティ用の監査対象事象の仕様。

監査:FAU_SEL_EXT.1

PP/ST に、FAU_STG_EXT.1 外部選択的監査が含まれている場合には、以下のアクションを監査対象にしておくべきである（should）。

a）最小: 外部エンティティにより監査可能なものとして定義されている事象のセットに対する変更。

5.2.2 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という理由から、セキュリティ監査に関係する。FAU_STG_EXT.1 要件が追加されたのは、ローカルの一時ストレージ[4]のポテンシャルを支援するのみならず、所定のセキュアな方法で所定の外部リポジトリの 1 つ以上に監査データを書き込む、TSF の能力を明示する監査記録要件の記載が CC のパート 2 にないためである。

下位階層: なし

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

FAU_STG_EXT.1.1 TSF は、生成された監査データを［***割付: 外部 IT エンティティに関する空でないリスト及び「TOE 内部ストレージ」(又はこのうちのいずれか)***］に送信（transmit）できなければならない（shall）。

適用上の注意: *「送信する（transmit）」という用語は、情報の転送を TOE が開始する場合と、外部 IT エンティティからの要求に応答して TOE が情報を転送する場合の両方を意図している。*

適用上の注意: *外部 IT の例としては、外部マシンにある監査管理 ESM コンポーネントやプラットフォームを TOE と共有する評価済みオペレーティング・システム、一元化されたロギング・コンポーネントが挙げられる。多数のソースへの送信が許可されている。*

FAU_STG_EXT.1.2 TSF は、生成された監査データをいずれの外部 IT エンティティに送信する場合にも、FTP_ITC.1 で定義されている高信頼チャネルを使用することを確実にしなければならない（shall）。

FAU_STG_EXT.1.3 TSF は、生成された監査データのいずれの TOE 内部ストレージも、以下のようになることを確実にしなければならない（shall）。

[4] FAU_STG.1 は、「附属書 C –アーキテクチャのバリエーションと追加要件」ではオプション要件として扱われた可能性がある。しかし、ローカル・ストレージしか持たないシステムが存在していたのかもしれないため、FAU_STG_EXT.1 もオプションにしておく必要があるという意味であったと思われる。この両方を1つの非オプション要件に統合。SFR は、ESM 機能を統合する一体型製品を今もサポートしているが、監査記録が保護されていること、及び送信を義務付けている（mandate）。

a. TOE 内部監査証跡に保管されている監査記録を未認可の削除から保護すること。及び

b. TOE 内部監査証跡に保管されている監査記録に対して行われる未認可修正を [選択、次から 1 つ選択: 防止する、検知する]

管理:FAU_STG_EXT.1

FMT の管理機能については、以下のアクションを考慮できる可能性がある(could)。

a) 生成された監査データを受信することになる外部 IT エンティティの仕様。

監査:FAU_STG_EXT.1

PP/ST に、FAU_STG_EXT.1 外部監査証跡ストレージが含まれている場合には、以下のアクションを監査対象にしておくべきである(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る外部 IT エンティティとの通信の確立及びその解除。

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、暗号鍵の削除に関する要件を定義する。FCS_CKM_EXT.4 要件は、CC パート 2 で規定されている対応の要件より高い特異性を鍵生成に対して付与するために追加されたものである。

下位階層: なし

依存性: なし

FCS_CKM_EXT.4.1 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・パラメータが不要になった場合には、それらをすべてゼロ化しなければならない(shall)。

管理:FCS_CKM_EXT.4

想定される管理アクティビティは存在しない。

監査:FCS_CKM_EXT.4

PP/ST に、FCS_CKM_EXT.4 暗号鍵ゼロ化が含まれている場合には、以下のアクションを監査対象にしておくべ

きである（should）。

a）基本: 鍵ゼロ化プロセスの失敗。

5.3.2 FCS_RBG_EXT.1 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により、TSF は確実に認定暗号化標準に従って乱数表を生成する。

コンポーネントのレベル付け

このファミリのコンポーネントは FCS_RBG_EXT.1 の 1 つのみである。暗号操作（ランダムビット生成）FCS_RBG_EXT.1は、定義済みの標準に従ってランダムビット生成を実行するようTOEに求めている（require）。

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、[選択: 次から 1 つ選択: (1) 1 つ以上の独立したハードウェアベースのノイズ源（noise source）、(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のノイズ源とソフトウェアベースのノイズ源の組み合わせ。] からエントロピーを集積するエントロピー源でシードした[選択、次から 1 つ選択: [選択: Hash_DRBG（任意）、HMAC_DRBG（任意）、CTR_DRBG (AES)、Dual EC DRBG（任意）] を使用する NIST Special Publication 800-90; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] に従って、すべてのランダムビットの生成（RBG）サービスを実行しなければならない（shall）。

FCS_RBG_EXT.1.2 決定論的（deterministic）RBGは、少なくともその鍵の最大ビット長に等しいエントロピーの少なくとも [選択、次から 1 つ選択: 128 ビット、256 ビット] でシードされなければならない（shall）。

管理:FCS_RBG_EXT.1

想定される管理アクティビティは存在しない。

監査:FCS_RBG_EXT.1

PP/ST に、FCS_RBG_EXT.1 暗号操作(ランダムビット生成)が含まれている場合には、以下のアクションを監査対象にしておくべきである(should)。

a) 基本: ランダム化プロセスの失敗。

5.4 クラス FMT:セキュリティ管理

5.4.1 FMT_MOF_EXT.1 機能のふるまいに対する外部管理

FMT_MOF ファミリは、TSF が TSF 自体の機能のふるまいを管理する能力を定義する。FMT_MOF_EXT は、外部 IT エンティティの機能のふるまいの管理に関する要件定義を行うことで、この機能を拡張する。この場合、管理対象となる外部 IT エンティティは、ESM アクセス制御製品である。FMT_MOF_EXT.1 要件が追加されたのは、TSF から見て外部のエンティティの機能を管理する、TSF の能力を明示する要件の記載が CC のパート 2 にないためである。

下位階層:	なし。
依存性:	FMT_SMF.1 管理機能の仕様 FMT_SMR.1 セキュリティ役割
FMT_MOF_EXT.1.1	TSF は、アクセス制御製品の諸機能である、監査済みの事象、リモートにある監査記録用のリポジトリ、アクセス制御 SFP、現在実装されているポリシーのバージョン、万一の通信障害(communications outage)の際に、**[割付: *認可と識別の済んだ役割*]** に対して **[割付: *他の機能*]** を実施するアクセス制御 SFP のふるまいについて、こうしたふるまいを問い合わせ、その機能を修正する能力を制限しなければならない(shall)。

管理:FMT_MOF_EXT.1

FMT の管理機能については、以下のアクションを考慮できる可能性がある(could)。

a) TSF によって設定されることになる外部 IT エンティティの仕様。

b) 指定された外部エンティティの機能の設定。

監査:FMT_MOF_EXT.1

想定される管理アクティビティは存在しない。この要件によって定義されるアクティビティは、FMT_SMF.1 で指定されている管理機能のサブセットである。このため、FMT_SMF.1 で規定されているすべての管理機能の監査は、FMT_MOF_EXT.1 の監査を扱うのに十分である。

5.4.2 FMT_MSA_EXT.5 適合するセキュリティ属性

FMT_MSA ファミリは、TSF のセキュリティ属性管理能力を定義する。FMT_MSA_EXT は、この属性を管理可能にする方法についての追加要件を定義することで、この機能を拡張する。FMT_MSA_EXT.5 は、TSF に対して、適合属性(consistent attribute)という概念を実施することを要求する。ST 作成者は、不適合属性(inconsistent attribute)を構成するのは何か、この不適合が検知されたとき TSF はどのようなふるまいを示したかを定義しなければならない(must)。単に不適合を検知するのみではなく、その不適合を回避するような形で TSF が実装されている場合には、そのことを示すこともできる(can)。FMT_MSA_EXT.5 要件が追加されたのは、不適合属性を定義してこの不適合属性の使用の回避又は検知を TSF がどのように行うかに関する要件の記載が CC のパート 2 にないためである。

下位階層: なし。

依存性: FMT_MOF_EXT.1 機能のふるまいの外部管理

FMT_MSA_EXT.5.1 TSF は、[選択: 配付の前に、次に示したポリシー内の内部不適合を識別: **[*割付: 不適合に関する空でないリスト*]; 不確定なポリシーの定義のみ許可]** しなければならない(shall)。

FMT_MSA_EXT.5.2 不適合が検知された場合、TSF は以下のアクションを講じなければならない(shall):[選択:管理者が手作業で不適合箇所を解決するプロンプトを発行する, [*割付: 他のアクション*]]。

管理:FMT_MSA_EXT.5

FMT の管理機能については、以下を考慮できる可能性がある(could)。

a) TSF による検知又は回避の対象となっている不適合データの仕様。

b) 不適合データが検知されたとき TSF が取ることになっているアクションの仕様。

監査:FMT_MSA_EXT.5

想定される監査対象事象は存在しない。この要件によって定義されるアクティビティは、FMT_SMF.1 で指定されている管理機能のサブセットである。このため、FMT_SMF.1 で規定されているすべての管理機能の監査は、FMT_MSA_EXT.5 の監査を扱うのに十分である。

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 がセッション・ロックを開始しなければならない場合、この SFR 自体が TOE のふるまいについて説明する。適用範囲を絞るため、及びロック・アクションを規定するために、明示的な要件が 1 つ要求されたが、これはコモンクライテリアの基本要件で解決された。

下位階層: なし。

FTA_SSL_EXT.1.1 TSF は、ローカルの対話セッションについて［選択:

- o セッションをロックする – 最新の内容を読込み不可にして、表示装置を消去するか上書きし、セッションのロックを解除せずに利用者のデータ・アクセス/表示装置に関するアクティビティを無効にし、その利用者に対してセッションのロック解除前に TSF に対する再認証を要求する:
- o セッションを終了する

］ことを認可された管理者が非活動時間を指定した後にしなければならない(shall)。

依存性: なし。

管理:FTA_SSL_EXT.1

FMT の管理機能については、以下のアクションを考慮できる可能性がある(could)。

a) 各利用者についてロックアウトが生じる前の利用者非活動時間の仕様。

b) ロックアウトが生じる前の利用者非活動デフォルト時間の仕様。

c) セッションのロック解除前に起こるべき事象の管理。

監査:FTA_SSL_EXT.1

PP/ST に、FTA_SSL_EXT.1 が含まれている場合には、以下のアクションを監査対象にしておくべきである（should）。

a）最小: 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）最小: 対話セッションの適切なロック解除。

c）基本: 対話セッション・ロック解除の試行。

6　セキュリティ要件

本書に記載されている要件は、機能要件と保証要件という 2 種類のセットに分割される。1 つ目の機能要件のセットは、コモンクライテリア（CC）から導出されたもので、監査及びポリシー実施に関する中心的要件を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 から導出されたもので、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）は通常 PP に盛り込まれるもので、SFR とは別に記載される。その後で、選択された SAR に基づく評価の段階で 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と、TOE であると確認された特定の技術の性質を考え合わせて、本 PP では特化した（tailored）手法が採用されている。前後関係と完全性を考慮して SAR は 6.2 節に記載しておくが、各 SFR と各 SFR についてこの TOE に対して評価者が実行する際に必要となる大多数のアクティビティについては、「*保証アクティビティ*」の段落で詳述している。保証アクティビティとは、評価が完結しているために行われなければならないアクティビティに関する規範的な説明を指す。保証アクティビティについては本 PP の 2 箇所に記載があり、特定の SFR に関係する保証アクティビティについては対応する SFR と一緒に記載されている。これに対し、SFR に関連のないものについては 6.2 節で詳述している。なお、保証アクティビティは、実際には特化した評価方法の 1 つであり、読みやすさ、理解、便宜を考慮してインライン表示で示されている。

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、保証アクティビティが 1 つ以上記載され、適合デバイスに対して要求された保証達成のために実行すべきアクティビティが詳述されている。

SFR と関係のないアクティビティを必要とする SAR については、6.2 節の中で、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 のポインタ付きで、達成すべき追加保証アクティビティが記載されている。

今後プロテクションプロファイル（PP）の繰り返しを重ねていけば、実際の製品評価から学んだ教訓に基づく緻密な保証アクティビティが提供されていくと考えられる。

6.1 セキュリティ機能要件

PP の機能上のセキュリティ要件は、以下のコンポーネントから成り、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_ACD.1	アクセス制御ポリシー定義
ESM_ACT.1	アクセス制御ポリシーの送信
ESM_ATD.1 (オプション)	オブジェクト属性定義 (附属書C.1.1節で定義されているとおり)
ESM_ATD.2 (オプション)	サブジェクト属性定義 (附属書C.1.2節で定義されているとおり)
FAU_GEN.1	監査データの生成
FAU_SEL_EXT.1	外部の選択的監査
FAU_STG_EXT.1	外部監査証跡ストレージ
FCS_CKM.1 (オプション)	暗号鍵生成(非対称鍵用) TOEが暗号機能を提供する場合は附属書C.4.1節で定義されているとおり)
FCS_CKM_EXT.4 (オプション)	暗号鍵ゼロ化 TOEが暗号機能を提供する場合は附属書C.4.2節で定義されているとおり)
FCS_COP.1(1) (オプション)	暗号操作(データの暗号化/復号用) TOEが暗号機能を提供する場合は附属書C.4.3節で定義されているとおり)
FCS_COP.1(2) (オプション)	暗号操作(暗号署名用) TOEが暗号機能を提供する場合は附属書C.4.4節で定義されているとおり)
FCS_COP.1(3) (オプション)	暗号操作(暗号ハッシュ法用) (TOEが暗号機能を提供する場合は附属書C.4.5節で定義されているとおり)

機能コンポーネント	
FCS_COP.1(4) (オプション)	暗号操作(鍵付ハッシュ・メッセージ認証用) (TOEが暗号機能を提供する場合は附属書C.4.6節で定義されているとおり)
FCS_RBG_EXT.1 (オプション)	拡張:暗号操作(ランダムビット生成) (TOEが暗号機能を提供する場合は附属書C.4.7節で定義されているとおり)
FIA_AFL.1	認証失敗時の取り扱い
FIA_SOS.1	秘密の検証
FIA_UAU.2	任意のアクションの前の利用者認証
FIA_UID.2	任意のアクションの前の利用者識別
FIA_USB.1	利用者とサブジェクトの結合
FMT_MOF_EXT.1	機能のふるまいの外部管理
FMT_MSA.1(1)	セキュリティ属性(内部属性)の管理
FMT_MSA.1(2)	セキュリティ属性(外部属性)の管理
FMT_MSA.3	静的属性の初期化
FMT_MSA_EXT.5	適合するセキュリティ属性
FMT_SMF.1	管理機能の仕様
FMT_SMR.1	セキュリティ管理の役割
FPT_STM.1 (オプション)	高信頼タイムスタンプ(Reliable Time Stamp) (附属書C2.1節で定義されているとおり)
FTA_SSL_EXT.1 (オプション)	TSF起動セッション・ロックと終了 (オプション – 附属書C.3節で定義)
FTA_SSL.3 (オプション)	TSF起動による終了 (オプション – 附属書C.3節で定義)

機能コンポーネント	
FTA_SSL.4 (オプション)	利用者起動による終了 (オプション – 附属書C.3節で定義)
FTA_TAB.1	TOEアクセス・バナー
FTA_TSE.1 (オプション)	TOEセッションの確立 (オプション – 附属書C.3節で定義)
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)
FTP_TRP.1	高信頼パス

6.1.1 PP 適用上の注意

6.1.1.1 使用

「適用上の注意」は、各要件の背後にある目的を読者が確認するために、PP に記載された多数の要件の後に示されている。ST 作成者は、ST に記載されたこの「適用上の注意」のいずれも複製すべきではない(should not)。

6.1.1.2 作成方針(Composition Philosophy)

ESM PP とは、変貌していく ESM 製品機能を網羅するために記載された関連プロテクションプロファイルのファミリを表す。ESM PP ファミリ内の多数の PP に対する適合を主張する ST については、ST 作成者は、「適用上の注意」を活用し、ESM コンポーネントの相互関連性を明確にすることが望ましい。そうすれば、評価対象となっている製品のパーツと、別の ESM 機能について規定した CC の概念との対応がどのようになっているのかを読者が判断するのに役立つ。

例えば、ESM の多数のパーツは、単一アプライアンスとして配置される場合がある。また、一連の冗長サーバとして配置され、この中にポリシー実施メカニズムも組み込まれる場合もある。あるいは、単一サーバに報告を行う各クライアント・システム上に実施地点が存在するクライアント・サーバ配置に配置されることもある。「適用上の注意」を活用すると、ESM システムのアーキテクチャに基づいて主張をする必要のない要件を判断しやすくなる。

6.1.2 クラス ESM: エンタープライズ・セキュリティ管理

ESM_ACD.1 アクセス制御ポリシー定義

下位階層: なし。

ESM_ACD.1.1 TSF は、互換性を備えた 1 つ以上のアクセス制御製品が利用するためのアクセス制御ポリシーを定義する能力を提供しなければならない(shall)。

ESM_ACD.1.2 TSF で定義されるアクセス制御ポリシーには、以下の内容を入れなければならない(must)。

サブジェクト:**[*割付:アクセス制御決定のために使用できるサブジェクト及びそのサブジェクトが導出されるソースの一覧*]** 及び

適用上の注意: *サブジェクトのソースの例には、互換性のある識別情報及びクレデンシャル情報管理製品が挙げられる。*

*オブジェクト:[**割付:アクセス制御決定のために使用できるオブジェクト及びそのオブジェクトが導出されるソースの一覧**] 及び*

適用上の注意: *オブジェクトに関するホストベースのソースの例としては、このオブジェクトが常駐するホストのオペレーティング・システムが挙げられる。*

*操作:[**割付:アクセス制御決定のために使用できる操作及びその操作が導出されるソースのリスト**] 及び*

適用上の注意: *操作に関するホストベースのソースの例としては、このオブジェクトが常駐するホストのオペレーティング・システムが挙げられる。*

*属性:[**割付:アクセス制御決定のために使用できる属性及びその属性が導出されるソースのリスト**]*

適用上の注意: *属性データのソースの例としては、互換性のある識別情報とクレデンシャル情報管理製品、あるいは TOE 自体が挙げられる。オブジェクト及びサブジェクト(又はこのうちのいずれか)の属性を定義するオプション SFR の記載については、附属書 C.1. 節を参照されたい。*

適用上の注意: *この要件の目的な、あるアクセス制御製品とその TSF の互換性があるならば、その*

TSF はその製品に備わるあらゆる種類の機能を活用するポリシーを作成できなければならないということを確実にすることである。例えば、そのTSFが、あるホストベースのアクセス制御製品と互換性があると主張しても、ファイル・アクセスを制御するポリシーしか書き込むことができなければ、そのTSFは、そのアクセス制御製品の特長を十分に活用することはできない。

ESM_ACD.1.3　TSF は、各ポリシーに一意の識別を関連付けなければならない（shall）。

適用上の注意:　*この要件は、TOE が作成するポリシーを利用するアクセス制御製品による実装が行われているポリシーがどのようなものであるかを、TOE が後々判断することができるよう準備されたものである。*

依存性:　なし

保証アクティビティ:

評価者は以下の項目を実施しなければならない（must）。

- *互換性のあるアクセス制御製品の識別をSTが行っているかどうかの検証*
- *ポリシー・セットを定義するエンティティの適用範囲と詳細さのレベル（granularity）についての説明をSTが行っているかどうかの検証*
- *互換性のあるアクセス制御製品の ST の見直し、及び TOE が作成できるポリシー及びアクセス制御製品が利用できるポリシーの間に対応関係があるかどうかの検証*
- *設計文書にポリシーの識別方法が示されているかどうかの検証*

評価者はこれができているかどうかを、TOEを使用してあらゆる種類のサブジェクト、オブジェクト、操作及び属性の完全一式を活用するポリシーを作成し、それを、互換性のあるアクセス制御製品に送信し利用することでテストすることになる。次に、評価者は、そのポリシーが適切に適用されたことを確認するために、アクセス制御製品が介在する（mediate）アクションを実行することになる。また、評価者は、アクセス制御製品によって実装中のポリシーを問い合わせることで、送信されたポリシーにポリシー識別子が関連付けられていることも検証することになる。

ESM_ACT.1 アクセス制御ポリシーの送信

下位階層:　なし。

ESM_ACT.1.1　TSF は、以下の環境下では、互換性のあるアクセス制御認可製品に対してポリシーを送信しなければならない（shall）。[選択：1 つ以上選択：新たにポリシーを作成した直後又は更新されたポリシーの作成直後、定期的、互換性を備えたセキュアな設定製品からの要求があり次第、**[割付：他の環境]**]。他の環境]].

適用上の注意：　*この要件の存在意義は、最新のポリシーが実装される保証を提供することである。*

適用上の注意：　*「at the request of a compatible Secure Configuration Management product（互換性を備えたセキュアな構成管理製品からの要求があり次第）」を選択する場合、ST 作成者は互換性のある製品を示さなければならない（must）。*

依存性：　ESM_ACD.1 アクセス制御ポリシー定義

保証アクティビティ：

評価者は、ポリシーの作成と更新の方法を決定するための操作ガイダンスと、利用する側である ESM 製品に新規ポリシー又は更新後のポリシーを送信する環境（及び適用可能な場合には、この環境の管理のされ方も）を見直さなければならない（shall）。評価者は、互換性のあるアクセス制御製品を入手し、ポリシー・マネージャ（Policy Manager）とアクセス制御製品のいずれにも対応する操作ガイダンスに定められた手順に従って新たにポリシーを作成し、そのポリシー・マネージャ内に定義されたその新規ポリシーが、SFR で定義されている環境に応じて、そのアクセス制御製品に適切に送信されインストールされていることを確認しなければならない

つまり、もし新規ポリシー作成後に送信するという選択をしたのなら、評価者は新規ポリシーを作成して、送信のための適切な画面が終了した後、その新規ポリシーがインストールされていることを確認しなければならない（shall）。また、もし定期的に送信する選択をしたのなら、評価者は、新規ポリシーを作成し、一定の期間が過ぎるまで待ってから、作成した新規ポリシーがアクセス制御製品内にあるということを確認しなければならない（shall）。また、もし互換性のあるセキュアな設定構成管理コンポーネントからの要求があり次第送信する選択をしたのなら、評価者は、ポリシーを作成し、セキュアな構成管理コンポーネントを使用して送信要求を行い、アクセス制御製品コンポーネントがそのポリシーを受信してインストールを完了したことを確認しなければならない（shall）。ST 作成者が「他の環境」を指定した場合、当該環境下における送信を確認するためには同様のテストが実施されなければならない（shall）。

次に、評価者は以前に作成したポリシーに変更を加え、それが済んだら、SFR 指定の環境に従って更新後のポリシーがアクセス制御製品に送信されていることを確認するために、以前の手続きを繰り返さなければならない（shall）。最後に、ポリシー更新はポリシーの遅延を引き起こすので、評価者は、そのプロセスを 3 回繰り返し、このときそのポリ

シーを削除し、アクティブ状態のポリシーとしてアクセス制御製品からそれが消去されていることを確認しなければならない(shall)。

注:このテストは、ESM_ACD.1 のテストと併せて実施される可能性もある。

6.1.3 クラス FAU: セキュリティ監査

FAU_GEN.1 監査データの生成

下位階層: なし。

FAU_GEN.1.1 TSF は、以下に示した監査対象事象に関する監査記録を生成できなければならない(shall)。

a) 監査機能の起動とシャットダウン、及び

b) [未指定] レベルの監査のために、表 3 で識別した監査対象事象全般、及び

c) [割付:他の属性事象]

表 3 監査対象事象

コンポーネント	事象	追加情報
ESM_ACD.1	ポリシーの作成又は修正	一意のポリシー識別子
ESM_ACT.1	アクセス制御製品へのポリシーの送信	ポリシーの定義
ESM_ATD.1 (オプション)	オブジェクト属性の定義	定義された属性の識別
ESM_ATD.1 (オプション)	属性とオブジェクトとの関連付け	オブジェクト及び属性の識別
ESM_ATD.2 (オプション)	サブジェクト属性の定義	定義された属性の識別
ESM_ATD.2 (オプション)	属性とサブジェクトとの関連付け	サブジェクト及び属性の識別

コンポーネント	事象	追加情報
FAU_SEL_EXT.1	設定を監査するためのすべての修正	なし
FAU_STG_EXT.1	監査サーバとの通信の確立及び確立の解除	監査サーバの識別
FCS_CKM.1(1) (オプション)	鍵ゼロ化アクティビティの失敗	なし
FCS_CKM_EXT.4 (オプション)	鍵ゼロ化プロセスの失敗	ゼロ化を要求しているか、ゼロ化を引き起こしているサブジェクトの識別、消去中のオブジェクト又はエンティティの識別
FCS_COP.1(1) (オプション)	暗号化又は復号の失敗	操作の暗号モード、現在暗号化/復号中のオブジェクトの名称/識別子
FCS_COP.1(2) (オプション)	暗号署名の失敗	操作の暗号モード、現在署名中/確認中のオブジェクトの名称/識別子
FCS_COP.1(3) (オプション)	ハッシュ機能の失敗	操作の暗号モード、現在ハッシュ化が行われているオブジェクト名称/識別子
FCS_COP.1(4) (オプション)	非データの完全性に関する暗号ハッシュ化中の障害	操作の暗号モード、現在ハッシュ化が行われているオブジェクトの名称/識別子
FCS_RBG_EXT.1 (オプション)	ランダム化プロセスの失敗	なし
FIA_AFL.1	認証試行の失敗閾値の到達、その閾値が到達したときに取られたアクション、及びノーマルな状態に復元するために取られたアクション	閾値に到達したときに取られたアクション
FIA_SOS.1	テストされた任意の秘密に対するTSFによる拒否又は受諾（acceptance）	なし
FIA_SOS.1	定義されている品質基準に加えられた任意の変更の識別	品質基準に加えられた変更
FIA_UAU.2	認証メカニズムの全使用	なし

コンポーネント	事象	追加情報
FIA_UID.2	識別メカニズムの全使用	提供された利用者識別
FIA_USB.1	サブジェクトへの利用者属性の結合の成功及び失敗	なし
FMT_MSA.1	セキュリティ属性の全修正	なし
FMT_MSA.3	セキュリティ属性の初期値の全修正	修正された属性、修正された値
FMT_SMF.1	管理機能の使用	実行された管理機能
FMT_SMR.1	管理役割メンバーの修正	なし
FTP_ITC.1(1)	高信頼機能の全使用	高信頼チャネルのイニシエータ及びターゲットの識別
FTP_ITC.1(2)	高信頼機能の全使用	高信頼チャネルのイニシエータ及びターゲットの識別
FTP_TRP.1	高信頼パス機能のすべての使用試行	高信頼パス機能と関連付けられた利用者の識別（利用可能な場合）

FAU_GEN.1.2　TSF は、各監査記録の中に少なくとも以下の情報を記録しなければならない（shall）。

a) その事象の日付と時刻、事象種別、サブジェクト識別（適用可能な場合）、及びその事象の結果（成功又は失敗）、及び

b) 各監査事象種別について、PP/ST に含まれている機能コンポーネントの監査対象事象定義に基づく［***割付:他の監査関連情報***］。

適用上の注意:　*「他の監査関連情報」には、責任者及びその人物によって取られる特定のアクションを識別するために十分な情報が盛り込まれなければならない（must）。*

依存性:　FPT_STM.1 高信頼タイムスタンプ

適用上の注意:　*『Standard Protection Profile for ESM Audit Management（ESM 監査*

管理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ストレージと処理を扱っている。

TOE での事象の監査は、成功したものも不成功のものも事象はすべて捕捉され、ログ記録がとられていることを確実にすることで、悪意のある利用者によるアクションの隠ぺい(masking)に対処する(mitigate)ことに役立つ。

保証アクティビティ:

評価者は、操作ガイダンスをチェックして、その中に監査対象事象のすべてがリストされており、かつ、各監査記録種別の内容の説明も示されていることを確認しなければならない(shall)。各監査記録の書式タイプ(format type)が網羅されていなければならず、かつ、各欄(field)の簡単な説明も含まれていなければならない(must)。評価者は、本 PP で義務付けられている(mandated)各監査事象種別がいずれも説明されていること、及び欄の説明の中に FAU_GEN 1.2 によって必須とされている(required)情報と表 3 で規定されている追加情報が盛り込まれていることを確認するためのチェックを行わなければならない(shall)。

評価者は、本 PP で規定された要件を実施するために必要であり TOE に実装されたメカニズムについて有効化(enabling)又は無効化(disabling)をはじめとする設定を許可する管理インタフェース(サブコマンド、スクリプト、設定ファイルなど)を決定するために、操作ガイダンス及び入手可能な任意の文書について見直しを行わなければならない(shall)。評価者はこれを行うための方法論と手法を文書にしなければならない(shall)。評価者は、このアクティビティを、この要件を満たす AGD_OPE ガイダンスの保証に関連するアクティビティの一環として実施することができる(may)。評価ではこのリストを使用して、セキュリティ関連の管理インタフェースのそれぞれに対応する、その事象についての適切な情報が記録される監査事象が備わっていることが確認されなければならない(shall)。

評価者は、ST で定義されており、かつ前述の 2 つのアクティビティで識別された(又はこのうちのいずれかの)全事象についての監査記録を TOE に生成させる方法を用いて、TOE の監査機能をテストしなければならない(shall)。このテストが済んだ後、評価者は、監査記録がそのリポジトリに書き込まれたこと、及びこの監査記録の中に ST で定義されたような属性が入っていることを確定するために、ST で定義された監査リポジトリ、操作ガイダンス、又は(入手可能な場合には)開発上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実行と併せて行なうことができる(may)。例えば、間違った認証用の秘密(authentication secret)が入力されたときは監査記録が生成されるように指定しておけば、識別と認証をテストした結果、監査記録が生成されることになる。評価者はまた、ログの内容が TOE で実行されたアクティビティと一致して

いるかどうか確認するためのチェックも行わなければならない(shall)。例えば、ポリシーの定義が行われているというようなテストが実行される場合には、これに対応する監査記録に、ポリシーの定義が正しく示されているべきである(should)。

FAU_SEL_EXT.1 外部選択的監査

下位階層: なし。

FAU_SEL_EXT.1.1 TSFは、以下の属性に基づいて、ESMアクセス制御製品の監査対象である事象一式をすべての監査対象事象の一式から選択できなければならない(shall)。

a) [選択:オブジェクト識別、利用者識別、サブジェクト識別、ホスト識別、事象種別]、及び

b) [***割付:監査選択度が基準にしている追加的な属性のリスト***]

適用上の注意: *この要件は、アクセス制御製品の監査機能を TOE が設定する能力に関するものである。『Access Control Protection Profile(エンタープライズ・セキュリティ管理アクセス制御標準プロテクションプロファイル)』に収録されている FAU_SEL.1 要件を補完する要件である。*

依存性: FAU_GEN.1 監査データの生成
FMT_MTD.1 TSF データの管理

保証アクティビティ:

評価者は、監査対象事象の一式に対して作成されることが可能である選択項目(selection)を決定するために、操作ガイダンスをチェックしなければならない(shall)。また、その中に、セキュリティターゲットで識別された選択項目が全部盛り込まれていることも確認しなければならない(shall)。

評価者は、以下を備えた互換性のあるアクセス制御製品を設定することで、この機能をテストしなければならない(shall)。

- *有効となっているすべての選択可能な監査対象事象*
- *無効となっているすべての選択可能な監査対象事象*
- *有効となっている選択可能な監査対象事象の一部*

評価者は、この設定のそれぞれに対して、すべての選択可能な監査対象事象を実行し、各設定でアクセス制御製

品によって記録されるのは有効となっている事象のみであることを監査データの見直しによって決定しなければならない（shall）。

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、生成された監査データを［***割付: 外部 IT エンティティに関する空でないリスト及び「TOE 内部ストレージ（又はこのうちのいずれか）」***］に送信できなければならない（shall）。

適用上の注意: *「送信する（transmit）」という用語は、情報の転送を TOE が開始する場合と、外部 IT エンティティからの要求に応答して TOE が情報を転送する場合の両方を意図している。*

適用上の注意: *外部 IT の例としては、外部マシンにある監査管理 ESM コンポーネントやプラットフォームを TOE と共有する評価済みオペレーティング・システム、一元化されたロギング・コンポーネントが挙げられる。多数のソースへの送信が許可されている。*

FAU_STG_EXT.1.2 TSF は、生成された監査データをいずれの外部 IT エンティティに送信する場合にも、FTP_ITC.1 で定義されている高信頼チャネルを使用することを確実にしなければならない（shall）。

FAU_STG_EXT.1.3 TSF は、生成された監査データの TOE 内部ストレージのいずれについても、以下のようになることを確実にしなければならない（shall：企画要求事項 http://sys-assist.co.jp/archives/233 を参照）。

a. TOE 内部監査証跡に保管されている監査記録を未認可の削除から保護すること。及び

b. TOE 内部監査証跡に保管されている監査記録に対して行われる未認可の修正を［選択、次から 1 つ選択: 防止する、検知する］。

依存性: FAU_GEN.1 監査データの生成

FTP_ITC.1 TSF 間高信頼チャネル

適用上の注意: この要件は、1 つ以上の外部 IT エンティティ又は製品に対して、生成された監査データを送信する能力を提供する。また、この要件は、ローカル・ストレージと、生成された監査データの保護もサポートする（おそらくは、外部 IT エンティティとの通信が利用できないときの一時的な手段として）。ST 作成者は、この要件で指定された外部 IT エンティティが利用できないときの監査データの記録方法と、通信の再確立時に同期化を有効にする方法を指示しなければならない（must）。

保証アクティビティ:

評価者は、監査記録で使用する外部リポジトリの設定及び使用に関する方法の記述が盛り込まれているかどうかを判断するために、操作と準備のガイダンスをチェックしなければならない。また評価者は、そのリポジトリまでの通信がどのように確立されているのか、データはそのリポジトリにどのように受け渡されているのか、そのリポジトリへの接続が失われた後に接続を確立し直すときに何が起きるのかということをはじめとした、このリポジトリのインタフェースに関する説明が盛り込まれているかどうかを判断するために、操作ガイダンスもチェックしなければならない（shall）。

評価者は、この機能（capability）を設定し、監査対象事象を実行し、ローカル監査記録と外部監査記録の中に同一データが収められていることを検証することで、この機能（function）をテストしなければならない（shall）。また評価者は、外部監査記録までの通信を利用できないようにし、TOE 上で監査された事象を実行し、通信を再確立し、外部監査証跡ストレージがローカル・ストレージと同期していることも確認しなければならない（shall）。FAU_GEN.1 のテストと同じように、このテストも他の機能の演習と併せて行うことが可能である（can）。最後になるが、この要件は特に、FTP_ITC.1 によって確立された高信頼チャネル経由で送信される監査記録を要求するという理由から、そうした要件の検証はこの要件のこの箇所を明らかにするのに十分である。

6.1.4 クラス FCS: 暗号化のサポート

TOE の暗号要件は、TSF で実装されるか、非 ESM 運用環境コンポーネント依存で実装されるかのいずれかで可能である。独自の一意で冗長な暗号機能の実装をベンダが強いるのではなく、TSF が、すでに妥当性が確認されている暗号アルゴリズム一式を活用することができることが期待される。 ST は、TSF ではどのような暗号機能が使用されるのかを明確に示すべきである。（should）暗号機能がどこにあるかに関わらず、期待される機能は同じである。

TOE.の暗号要件については、附属書 C.4 節を参照されたい。

6.1.5 クラス FIA:識別及び認証

FIA_AFL.1 認証失敗の取り扱い

下位階層: なし

FIA_AFL.1.1 TSF は、[割付: 認証事象のリスト] に関して、[選択: **[割付: 正の整数値]、[割付: 許容可能な値の範囲]** 内における管理者による設定の可能な正の整数値] 回の不成功認証試行が生じたときを検出しなければならない(shall)。

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

依存性: FIA_UAU.1 認証のタイミング

保証アクティビティ:

評価者は、認証失敗の取り扱いの検討が操作ガイダンスに存在し、かつ、それがセキュリティターゲット内の表現と適合していることを検証するために、その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、TSF の認証機能を使用して不正なクレデンシャルを故意に入力することで、この機能をテストしなければならない(shall)。評価者は、不正な認証試行の回数を十分に重ねた後、適正なアクションが生じることを確認すべきである(should)。また評価者は、閾値の変更が可能であることを検証するために、操作ガイダンスに適合した方法で、TSF を使用して閾値の再設定も行うべきである(should)。

FIA_SOS.1 V 秘密の検証

下位階層: なし。

FIA_SOS.1.1 TSF は、以下の項目を満たす秘密を検証するメカニズムを提供しなければならない。

a) パスワードを使用する認証については、以下の規則を適用する。

1. ***パスワードは、以下の文字セットのサブセットで構成できるものでなければならない(shall) [割付:TSF がパスワード入力用としてサポートしている文字セットのリストで、リスト内に次の値 [割付: サポート対象となっている各文字セットに対するサポート対象文字のリスト] が含まれているもの。及び***

適用上の注意: *英文字のセットの文字種には、大文字が 26 文字、小文字が 26 文字、英数字が 10 個、特殊文字は「!」、「@」、「#」、「$」、「%」、「^」、「&」、「*」、「(」及び「)」の 10 文字が含まれることになっている。TOE で英文字セット以外がサポートされている場合、ST 作成者は、そのセットの各サブカテゴリについて許される文字スペースとともに、サポート対象となる文字セットを指定しなければならない(shall)。*

2. ***最小パスワード長は、管理者が設定可能なものでなければならず、かつ、16 文字以上から成るパスワードをサポートしなければならない(shall)。及び***

適用上の注意: *パスワードの最小パスワード長及び文字空白に基づくパスワードの組み合わせ数は、10^{14} を上回るものでなければならない(shall)。これは、最低 8 文字の長さを持つ 72 の文字セットを使用する英語のパスワードで満たすことが可能であると思われる。*

3. ***パスワードの構成に必要となる文字種と文字数を指定するパスワード作成規則(password composition rule)は、管理者が設定可能なものでなければならない(shall)。及び***
4. ***パスワードには、管理者が設定できる最上限の存続時間(lifetime)を提供しなければならない(shall)。及び***
5. ***新しいパスワードには、少なくとも管理者が指定した文字数分の古いパスワードからの変更が含まれていなければならない(must)。及び***
6. ***パスワードは、その利用者が使用するパスワードについて管理者が指定できる直近の数の範囲内では再使用されてはならない(must not)。***

b) ***パスワードを使用しない認証については、以下の規則を適用する。***

1. ***秘密の存続時間中に攻撃者によって秘密が入手されうる確率は 2^{-20} 未満である。***

依存性: なし。

保証アクティビティ:

評価者は、使用される認証がパスワードに基づくのか、パスワードに基づかないのかを識別するために、ST 及び操作ガイダンスを検査しなければならない(shall)。

a. *パスワードに基づく認証について、評価者は、ST で規定されているパスワードの作成、設定、および有効期限に関するいずれの要件も TSS 及び AGD の中で検討されていることを特定し、例えば、最低パスワード長を 6 に設定し、7 文字のパスワードと 16 文字のパスワードがいずれも受け入れられることを確認したた後、最低パスワード長を 8 に変更した場合には 7 文字のパスワードは拒否されるが 16 文字のパスワードは受け入れられることを確認することなどを行って、この機能を 1 つずつテストしなければならない(shall)。*

b. *パスワードに基づかない認証について、評価者は、認証メカニズムの解空間(solution space)及びパスワード試行可能回数を決定するために、基本的な機能強度分析(strength of function analysis)を実施しなければならない(shall)。例えば、もしその認証が、1 時間に 1 回試行可能な 4 桁の PIN 認証であるとするならば、この要件は合格しないことになる。認証メカニズムの強度が、バイオメトリクス認証メカニズムが使用されている場合のように額面どおりの機能強度メトリクスで決定できない場合には、ベンダは機能強度に関する何らかの証拠を示すべきである(should)。*

FIA_UAU.2 アクション前の利用者認証

下位階層:	FIA_UAU.1 認証のタイミング
FIA_UAU.2.1	TSF は、ほかに各利用者を代行する TSF 調停アクション(TSF-mediated action)を許可する前に、その利用者が認証されることを要求しなければならない(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、ある TOE に対してアクセスを要求する対話的利用者がすでに認証済みで、その TOE による認証クレデンシャルの妥当性確認の方法、又はその TOE が受信するアサーションの識別方法を決定するために、操作ガイダンスをチェックしなければならない(shall)。評価者は、有効な認証情報が提供されていない状態で TOE にアクセスすることでこの機能をテストして、TSF へのアクセスが後々拒否されることを確認しなければならない(shall)。

この SFR は、TOE と情報のやり取りを行う認可済みの IT エンティティ(認可済みのアクセス制御コンポーネントなど)にも適用される。こうしたことに対処するために、評価者は、操作ガイダンス及び TSS の見直しを行って、IT エンティテ

ィとの通信を認可する際に使用されるメカニズムを決定し、かつ、そのメカニズムによって、少なくとも 1 つの IT エンティティが TOE との通信を行うことができる設定にしなければならない(shall)。その後で、評価者は、その IT エンティティとの通信を試して、その通信が適切に認証され識別されていることを確認しなければならない(shall)。また評価者は、未確認(unidentified)のエンティティ又は非認証(unauthenticated)のエンティティとの通信も試して、この接続が失敗することも確認しなければならない(shall)。

FIA_UID.2 アクション前の利用者識別

下位階層:	FIA_UID.1 識別のタイミング
FIA_UID.2.1	TSF は、ほかに各利用者を代行する TSF 調停アクションを許可する前に、その利用者が識別されることを要求しなければならない(shall)。
依存性:	なし。

保証アクティビティ:

この機能は、対話的利用者(interactive user)、及び許可された IT エンティティの両方に対するものであり、FIA_UAU.2 で同時に検証されている。

FIA_USB.1 利用者サブジェクト結合(User-subject binding)

下位階層:	なし。
FIA_USB.1.1	TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない(shall)。[***割付:利用者セキュリティ属性のリスト***]
FIA_USB.1.2	TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない(shall)。[***割付:属性の最初の関連付けの規則***]
FIA_USB.1.3	TSFは、その利用者を代行して動作するサブジェクトに関連付けられている利用者セキュリティ属性への変更を管理する以下の規則を実施しなければならない(shall)。[***割付:属性の変更に関する規則***]
依存性:	FIA_ATD.1 利用者属性定義

保証アクティビティ:

評価者は、外部のデータソースが呼び出され、TSF が制御している利用者データにそれがマッピングされるメカニズムが操作ガイダンスで説明されていることを検証するために、その操作ガイダンスをチェックしなければならない(shall)。

評価者は、ST で定義した外部ソースからの利用者情報を TSF が受け入れるという設定にすることで、この機能をテストしなければならない(shall)。次に評価者は、この方法を使用して認証アクティビティを実施し、いずれの例においても認証が成功したことの妥当性を確認しなければならない(shall)。次に評価者は、利用者権限付与(user authorization)と、外部で定義された認可属性及び TSF のアクセス制御ポリシーの設定との間に矛盾がないと判定するために、各サブジェクトに割り当てられている定義済みの権限に基づいて様々な管理テストを実施しなければならない(shall)。例えば、LDAP リポジトリに定義されている 1 人の利用者が、あるグループに属しており、TSF の設定ではポリシー情報の読み取り専用アクセス権がそのグループのメンバーだけに付与されるようになっている場合では、評価者は TSF からこの利用者として認証を受けて、そのグループのメンバーにはポリシー情報への書き込みアクセス権はないという TSF 制御下のサブジェクトとしてそのことを検証しなければならない(shall)。これにより、この利用者が実行できることは何かを決定するために、この利用者に対する TSF の対処法に関係する多面的な利用者識別データが外部ソースから適切に取得され活用されるということが検証される。

6.1.6 クラス FMT:セキュリティ管理

FMT_MOF_EXT.1 機能のふるまいの外部管理

下位階層: なし。

FMT_MOF_EXT.1.1 TSF は、***監査済みの事象、リモートにある監査記録用のリポジトリ、アクセス制御 SFP、現在実装されているポリシーのバージョン、万一の通信障害(communications outage)の際に、[割付: 他の機能]を[割付: 認可と識別の済んだ役割]に実施するアクセス制御 SFP のふるまい***について、アクセス制御製品のふるまいを問い合わせ、その機能を改変する能力を制限しなければならない(shall)。

適用上の注意: *この要件は主にアクセス制御製品を管理する TSF の能力に関係している。『Access Control Protection Profile(エンタープライズ・セキュリティ管理アクセス制御標準プロテクションプロファイル)』に収録されている FMT_MOF.1 要件を補完す*

る要件である。

依存性: FMT_SMF.1 管理機能の仕様

FMT_SMR.1 セキュリティ役割

保証アクティビティ:

評価者は、この機能(capability)とやり取りを行うことのできるアクセス制御コンポーネントが用意されている環境に評価対象(TOE) を配置することで、この能力をテストしなければならない(shall)。評価者は、この環境を設定するにあたり、評価対象(TOE) に命令を発するための認可がこのポリシー管理製品に付与されているようにしなければならない(must)。この設定が済んだ後、評価者は、上記要件に定めた機能のふるまいを改変するのにポリシー管理製品を使用しなければならない(must)。評価者は、ポリシー管理製品を使用して改変目的のふるまいと改変後のふるまいを問い合わせることで、その改変が適切に適用されたことを各機能について検証しなければならない(must)。

また評価者は、その改変のとおりにTOEに応答させるアクティビティも実施しなければならない(must)。このアクションには、各機能について以下のアクティビティが含まれる。

- *監査済みの事象:機能のふるまいの改変前にすでに監査を受けた(又は監査を受けていない)事象を実施し、監査リポジトリが今、改変後のふるまいに基づいてこの事象のログ記録を取っている(又は取っていない)ことを確認する。*
- *リモートにある監査記録用のリポジトリ:監査済みの事象が所定のリポジトリに書き込まれたことを確認し、TOE による監査済み事象の書き込み先となるリポジトリを改変し、監査対象事象を実行し、それがもはや元のリポジトリに書き込まれなくなったことを確認する。*
- *アクセス制御 SFP:現在のアクセス制御 SFP が許可している(又は許可していない)アクションを実行し、アクションを今許可しない(又は許可する)よう実装したSFPを改変し、同じアクションを実行し、SFPの当初の繰返し(original iteration)と異なる認可であることを確認する。*
- *現在実装されているポリシーのバージョン:特定のアクセス制御ポリシーによって許可されている(又はされていない)アクションを実行し、現在そのアクションを許可していない(又は許可している)TSF ポリシーを提供し、同じアクションを実行し、SFP の当初の繰返しと異なる認可であることを確認する。*
- *通信障害が生じたときに実装すべきアクセス制御 SFP のふるまい:(適用可能な場合には)万一の通信障害の際に所与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との間の通信を再確立し、万*

一の通信障害が発生した場合に TOE が実装すべき SFP のふるまいを変更し、TOE とポリシー管理製品との間の通信を切断し、当初実行されたものと同じアクションを実行し、改変後のアクション処理方法が正しく適用されたことを確認する。

これが済み次第、評価者は、評価対象(TOE)とポリシー管理製品を再設定し、そのポリシー管理製品にはその評価対象(TOE)を設定する許可がもはや付与されていないようにしなければならない(shall)。再設定後、評価者は、そのポリシー管理製品を使用して評価対象(TOE)の設定を試みて、この試行が拒否されているのか、そのオプションが存在すらしていないのかを確認しなければならない(shall)。

FMT_MSA.1(1) セキュリティ属性の管理(内部属性)

下位階層: なし。

FMT_MSA.1.1(1) TOE セキュリティ機能(TSF)は、セキュリティ属性 ***[割付:セキュリティ属性のリスト]*** に対して [選択:デフォルト値変更、問合せ、改変、削除、***[割付:他の操作]***] を行う能力を ***[割付:認可を受け、かつ、識別された役割]*** に制限しなければならない(shall)。

適用上の注意: *この繰返しには、少なくとも以下の属性を入れなければならない(must)。*

- *TSF 自体のアクセス制御ポリシーを定義する属性、及び*
- *他の ESM 製品及び環境リポジトリへの TSF の接続を定義する属性*

保証アクティビティ:

評価者は、ST と操作ガイダンスを見直して、TSF が内部的にはそれ自体のアクセス制御をどのように維持するのか(つまり、「もし私が PM TOE の管理者ならば、私が担当する利用者になるのは誰なのか、その利用者はどのようなアクセス制御製品を制御できるのか、及びその利用者はそのアクセス制御製品をどの程度制御できるのかについて私はどのように言及するのか」)ということがそこに説明されていると判定しなければならない(shall)。評価者は、説明されているふるまいが、文書にまとめられている意味(semantics)を表している(exhibit)ことを確認するために、テストを実施しなければならない(つまり、新規利用者を設定し、その利用者に権限を付与してログインし、その権限が付与されていることを確認し、その権限に影響を与えることになる属性を一部変更し、もう一度ログインしてその権限が変更されたことを確認する)。

また評価者は、STと操作ガイダンスを見直して、TOE が ESM アクセス制御製品にどのように関連付けられているの

かについても判定しなければならない(shall)。評価者は、TOEが運用環境の中でアクセス制御製品をどのように見出すのか、及びTOEがアクセス制御製品の有効なコントローラとしてどのように認識されるのかを検証しなければならない(shall)。評価者は、このふるまいをテストを実施することで確認しなければならない(shall)。これを行う1つの切り口としては、TOEおよび互換性のある2台のアクセス制御製品を同じネットワーク上に配置することである。評価者は、そのアクセス制御製品のうちの1台がTOEに関連付けられているというように文書化された設定手順に従わなければならない(shall)。次に評価者は、現時点でそれが管理できるのはそのアクセス制御製品のみであることを確認しなければならない(shall)。評価者は、トラフィックを捕捉して、もう1台のアクセス制御製品に対してそれを再現し、そのトラフィックが無効であることを確認しなければならない(shall)。

評価者は、STと操作ガイダンスを見直して、定義済みの内部セキュリティ属性がほかにないかどうか決定しなければならない(shall)。もしあった場合には、評価者は、その属性を証拠で規定されているような方法で設定できること、及びその設定に証拠で定義した効果があることを検証しなければならない(shall)。

FMT_MSA.1(2) セキュリティ属性の管理(外部属性)

FMT_MSA.1.1(2) TOE セキュリティ機能(TSF)は、セキュリティ属性 ***[割付:セキュリティ属性のリスト]*** に対して [選択:デフォルト値変更、問合せ、改変、削除、***[割付:他の操作]***] を行う能力を ***[割付:認可を受け、かつ、識別された役割]*** に制限しなければならない(shall)。

適用上の注意: *この繰返しには、少なくとも以下の属性を入れなければならない(must)。*

- *他のESMアクセス制御製品にエクスポートされるポリシーを定義する属性*

適用上の注意: *分かりやすくするために、SFRは2つの繰返しに分けられている。1つ目の繰返しは、TSFが管理し、かつ後々TSFが使用するセキュリティ属性を定義する。2つ目の繰返しは、TSFが管理するセキュリティ属性で、外部のアクセス制御製品に送信されるアクセス制御ポリシーに関係しているセキュリティ属性を定義する。*

依存性: [FDP_ACC.1 サブセット・アクセス制御、又は
FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の仕様

保証アクティビティ:

評価者は、TSFによる管理可能な操作がSTに規定されていると判定するために、このSTを見直さなければならない(shall)。例えば、TSFはポリシーを作成する能力がなければならない(must)。このポリシーを構成できるデータはSTの中で定義されているべきである(should)。次に評価者は、この属性を扱うことのできるSTおよびTSFのメカニズムとの間に矛盾がなく、かつ管理されている一連の属性が操作ガイダンスの中で定義してあると判定するために、この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、定義された属性と操作のそれぞれについて、この属性を扱うTSF上で操作を実行することで、この機能をテストしなければならない(shall)。また評価者は、集められた外部の識別と認証情報をTSFに提供する利用者に対してTSF操作の権限がいかにして割り当てられるようになるかが理解されるようにセッション確立のメカニズムが定義されているかどうかも検証すべきである(also)。

FMT_MSA.3 静的属性初期化

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値を提供するため、***[割付: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ときにデフォルト値を上書きする代替の初期値を指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 セキュリティ役割

保証アクティビティ:

評価者は、管理されている属性のデフォルト値は何であるのか定義されていると判定するために、操作ガイダンスを見直さなければならない(shall)。評価者は、新たなセキュリティ属性のインスタンス化を引き起こすTSFに対抗するアクティビティを実行し、かつ、ガイダンスの記述とデフォルト値が一致していること及びこのデフォルト値をSTの定義した方法で一括して説明できることを確認することで、この機能をテストしなければならない(shall)。

FMT_MSA_EXT.5 適合するセキュリティ属性

下位階層:	なし。

FMT_MSA_EXT.5.1 TSF は、[選択: 配付の前に、次に示したポリシー内の内部不適合を識別: ***[割付: 不適合に関する空でないリスト]***; 明確なポリシーの定義のみ許可] しなければならない(shall)。

適用上の注意: *予想される最も一般的な不適合は、ポリシー内のある箇所でサブジェクトのオブジェクトへのアクセスが許可され、別の箇所では同じサブジェクトの同じオブジェクトへのアクセスが拒否されるケースである。*

適用上の注意: *TOE のポリシー管理エンジンが、矛盾が生じないようなポリシーの実装という明確な階層化法を定義する場合には、ST 作成者は、不明確なポリシーを拒否することができるということを示す。この場合には、TSS 又は操作ガイダンスで、相矛盾するポリシーを TOE がどのように回避するかについての概要が提供されることになっている(is expected that)。*

FMT_MSA_EXT.5.2 不適合が検知された場合、TSF は以下のアクションを講じなければならない(shall) [選択:管理者が手作業で不適合箇所を解決するプロンプトを発行する、***[割付: 他のアクション]***]。

適用上の注意: *TOE のポリシー管理エンジンが、矛盾が生じないようなポリシーの実装という明確な階層化法を定義する場合には、FMT_MSA_EXT.5.2 は、検知すべき不適合を持つことは不可能であるため、無意味ではあるが条件を満たしている(vacuously satisfied)。*

依存性: FMT_MOF_EXT.1 機能のふるまいの外部管理

保証アクティビティ:

評価者は、ポリシー・データに存在すると考えられる矛盾が当該操作ガイダンスで説明されていると判定するために、当該操作ガイダンスをチェックしなければならない(shall)。例えば、ポリシーには潜在的に、同じサブジェクトが同じオブジェクトにアクセスすることを許可し、禁止する 2 つの規則が含まれている可能性がある。代案として、矛盾の発生を不可能にする明確な階層化を TOE が定義することができる(may)。

評価者は、操作ガイダンスで示された矛盾を含むポリシーを定義し、次に、TSF がこの矛盾を検知して ST で規定された方法で対処して応答するかどうかを確認することで、この機能(capability)をテストしなければならない(shall)。TSF が、矛盾が起きないようにふるまうのであれば、評価者は、矛盾を回避するメカニズムの説明がされているかどう

か、及びこの特長(feature)が管理者に伝えられているかどうか判断するために、操作ガイダンスを見直さなければならない(shall)。この特長は、互換性のあるアクセス制御製品とともにテストされるべきである(should)。つまり、もしその TOE に矛盾を回避するメカニズムが備わっているのであれば(例えば、拒否規則が許可規則に常に優先されるのであれば)、互換性のあるアクセス制御製品がこのポリシーを適正に実施することが、このメカニズムの有効性を実証するための必要かつ十分な条件となる。

FMT_SMF.1 管理機能の特定

下位階層: なし。

FMT_SMF.1.1 TSF は、管理機能【*割付: TSF が提供する管理機能のリスト*】を実行できなければならない(shall)。

適用上の注意: *以下の表 4 にリストアップした管理機能が摘要できる場合、ST 作成者はこれを主張しなければならない(must)。*

適用上の注意: *ST 作成者は、追加的なセキュリ関連の操作、オブジェクト及びセキュリティ属性をこの表に加えることができ(may)、そうすることが推奨される。追加オブジェクトは既存の操作に追加することができ(may)、追加セキュリティ属性は既存のオブジェクトに追加することができる(may)。*

依存性: なし。

表 4 TOE の管理機能

要件	管理アクティビティ
ESM_ACD.1	ポリシーの作成
ESM_ACT.1	ポリシーの送信
ESM_ATD.1 (オプション)	オブジェクト属性の定義 属性とオブジェクトとの関連付け
ESM_ATD.2 (オプション)	サブジェクト属性の定義 属性とサブジェクトとの関連付け
FAU_SEL_EXT.1	定義した外部エンティティに対する監査対象事象の設定

要件	管理アクティビティ
FAU_STG_EXT.1	外部監査記録場所（external audit storage location）の設定
FIA_AFL.1	認証失敗の閾値の設定、閾値に達したときに取るべきアクションの設定、閾値アクション後の通常の状態への復旧の実行（適用可能な場合）
FIA_SOS.1	秘密を検証するために使用される測定基準の管理
FIA_UAU.2	対話的利用者及び認可されたITエンティティの両方に対する認証データの管理
FIA_UID.2	対話的利用者及び認可されたITエンティティの両方に対する利用者識別の管理
FIA_USB.1	サブジェクト・セキュリティ属性デフォルト値の定義（default subject security attributes）、サブジェクト・セキュリティ属性の改変
FMT_MOF_EXT.1	他のESM製品のふるまいの設定
FMT_MSA.1	セキュリティ属性と情報をやり取りする一連のサブジェクトの管理、指定された値をセキュリティ属性が継承するときに使用する規則の管理
FMT_MSA.3	初期値を指定できるサブジェクトの管理、指定されたアクセス制御SFPに対する、許容可能又は限定的なデフォルト値の設定、セキュリティ属性が値を継承する場合に準拠する規則の管理
FMT_MSA_EXT.5	TSFが識別すべきポリシー不一致にはどのようなものがあるか、及び何らかの矛盾が検出された場合にTSFが対処すべき方法の設定（適用可能な場合）
FMT_SMR.1	特定の役割に帰属する利用者の管理
FTA_TAB.1	バナーの維持
FTP_ITC.1(1)	高信頼チャネルを要求するアクションの設定（適用可能な場合）
FTP_ITC.1(2)	高信頼チャネルを要求するアクションの設定（適用可能な場合）
FTP_TRP.1	高信頼パスを要求するアクションの設定（適用可能な場合）

保証アクティビティ：

評価者は、TSF に対して実行されうる管理機能全般、その実行方法、及びその機能から達成されることが操作ガイダンスで定義されていると判定するために、当該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、ま

ずTOEにアクセスし、定義した管理機能がいずれも存在すること、それが規定どおりに実行されうること、及び文書に記載されている機能(capability)をそれが達成できることを検証することで、この機能(capability)をテストしなければならない(shall)。

FMT_SMR.1 セキュリティ管理の役割

下位階層: なし。

FMT_SMR.1.1 TSF は役割［*割付:許可・識別された役割*］を維持しなければならない(shall)。

適用上の注意: *本プロテクションプロファイルでは、アクセス制御ポリシーの書き込み及びその配付の許可された個人を指すときに「ポリシー管理者(Policy Administrator)」という用語を使用する。これは、個人はこの権限を付与されるべきである(should)ということを反映するための1つの論理的構成として解釈されるべきものであり(should)、当該権限を持つ者であれば TSF はいかなる人物をも「ポリシー管理者」という用語で呼称しなければならないという明示的な命令として解釈されるべきものではない。*

FMT_SMR.1.2 TSF は利用者と役割を関連付けることができなければならない(shall)。

依存性: FIA_UID.1 認証のタイミング

保証アクティビティ:

評価者は、TOE に対して定義されている役割を決定するために、ST 及び操作ガイダンスを見直さなければならない(shall)。評価者は、異なる利用者を異なる役割に関連付けるのに TOE を使用しなければならない(shall)。ある役割に割り当てられることで、利用者と TSFとの情報のやり取り(interact with)の方法に影響が生じるのであれば、このアクティビティは他の要件と同時にテストすることができる(may)。例えば、TSF の内部アクセス制御メカニズムは、(スーパー・ユーザだけが新規利用者の作成を行うことができ、監査者はポリシーの閲覧を行うことはできるが変更することはできないなど)、異なるレベルの権限を異なる役割を持つ利用者に付与することができる(may)ため、利用者の役割属性の変更が与える影響は FMT_MSA.1(1) によってすでにテスト済みであると思われる。

6.1.7 クラス FTA:TOE アクセス

FTA_TAB.1 TOE アクセス・バナー

下位階層: なし。

FTA_TAB.1.1 利用者セッションを確立する前に、TSF は TOE の未認可使用について注意を促すメッセージ(advisory warning message)を表示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、TOE バナーの表示と設定がどのようになされているのか判断するために、操作ガイダンスを見直さなければならない(shall)。デフォルトでバナーが表示されていなければ、評価者はバナー表示を有効にするために、操作ガイダンスに従って TOE を設定しなければならない(shall)。この設定が済んだ後、評価者は TOE へのアクセスを試みて、TOE のバナーが存在することを検証しなければならない(shall)。適用できる場合、評価者は、FMT_SMF.1 で定義した標準のとおりに TOE のアクセス・バナーを改変する機能を使用してみて、TOE のアクセス・バナーが適切に更新されていることも検証することになる。

6.1.8 クラス FTP: 高信頼パス/チャネル

FTP_ITC.1(1) TSF 間高信頼チャネル(漏洩の防止)

下位階層: なし。

FTP_ITC.1.1(1) **詳細化**:TSF は、***許可された IT エンティティ***と TSF 自体との間に、他の通信チャネルとは論理的に異なり、かつ、TSF エンドポイントの確実な識別を提供し、チャネル・データを漏洩から保護する***高信頼***通信チャネルを提供する**ために、*[割付: FCS 指定サービス(FCS-specified service)]* を***使用***しなければならない(shall)。

適用上の注意: *ST 作成者は、FCS サービスが TSF にとって内部的なものか、運用環境により提供されるのか示さなければならない(must)。*

適用上の注意: *IT エンティティが認可されているかどうかの判断は、FIA_UID.2 及び FIA_UAU.2 によって実施される、そのエンティティの識別と認証のメカニズムに基づく。*

FTP_ITC.1.2(1) **詳細化**:TSF は、***TSF 又は許可された IT エンティティ***が、高信頼チャネル経由の通信を開始す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・データの送信［割付: 他の機能］***のために、高信頼チャネル経由で通信を開始しなければならない(shall)。

適用上の注意: *ST 作成者は、この割付に、TOE に備わる ESM 他製品との保護付き通信(protected communications the TOE has with other ESM products)(監査データの送信、識別データの要求、認証サーバへの通信など)*をすべて記入すべきである(should)。

依存性: なし。

保証アクティビティ:

評価者は、セキュアな通信が有効となるメカニズムを決定するために、操作ガイダンスをチェックしなければならない(shall)。また評価者は、セキュアな通信が促進される手段を決定するために、TSS 及び操作ガイダンスをはじめとして提供された証拠のチェックも行わなければならない(shall)。こうしたことに基づいて、以下の分析が必要になる。

- *暗号が TOE にとって内部的なものである場合、評価者は、製品の妥当性が FIPS 140-2(米国又はカナダで評価する場合)により確認済みであるか、評価実施国でこの要件に相当する国内基準により確認済みであることを検証しなければならない(shall)。*
- *暗号が運用環境によって提供される場合、評価者は、暗号がどのように利用されるかを確認し、かつ使用された機能の妥当性が FIPS 140-2(米国又はカナダで評価する場合)により確認済みであるか、評価実施国でこの要件に相当する国内基準により確認済みであることを検証するために、操作ガイダンス及び ST をはじめとし入手可能な設計文書であればいかなるものも見直さなければならない(shall)。*

評価者は、TOE でのセキュアな通信を有効にし、かつ、ローカル・ネットワークにパケット・スニファを置くことで、この機能をテストしなければならない(shall)。次に評価者は TOE を使用して、TOE の通信相手である高信頼 IT 製品全般との通信を要求するアクションを実行し、TOE を宛先とする捕捉されたパケット通信量又は TOE を起点とする捕捉されたパケット通信量を確認し、その内容が難読化されていることを確認しなければならない(shall)。

FTP_ITC.1(2) TSF 間高信頼チャネル(改変の検知)

下位階層: なし。

FTP_ITC.1.1(2) **詳細化**:TSF は、***許可された IT エンティティ***と TSF 自体との間に、他の通信チャネルとは論理的に異なり、かつ、TSF エンドポイントの確実な識別を提供し、***データ***

改変を検知する高信頼通信チャネルを***提供するときには［割付：FCS 指定サービス（FCS-specified service）］を使用***しなければならない（shall）。

適用上の注意： *ST 作成者は、FCS サービスが TSF にとって内部的なものか、運用環境により提供されるのか示さなければならない（must）。*

適用上の注意： *IT エンティティが認可されているかどうかの判断は、FIA_UID.2 及び FIA_UAU.2 によって実施される、そのエンティティの識別と認証のメカニズムに基づく。*

FTP_ITC.1.2(2) **詳細化**：TSF は、***TSF 又は許可された IT エンティティ***が、高信頼チャネル経由の通信を開始す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・データの送信［割付：他の機能］***のために、高信頼チャネル経由で通信を開始しなければならない（shall）。

適用上の注意： *ST 作成者は、この割付に、TOE に備わる ESM 他製品との保護付き通信（protected communications the TOE has with other ESM products）（監査データの送信、識別データの要求、認証サーバへの通信など）をすべて記入すべきである（should）。*

依存性： なし。

保証アクティビティ：

評価者は、セキュアな通信が有効になるメカニズムを決定するために、操作ガイダンスをチェックしなければならない（shall）。また評価者は、セキュアな通信が促進される手段を決定するために、TSS、操作ガイダンスをはじめとする入手可能な証拠のチェックも行わなければならない（shall）。こうしたことに基づいて、以下の分析が必要になる。

- *暗号が TOE にとって内部的なものである場合、評価者は、製品の妥当性が FIPS 140-2（米国又はカナダで評価する場合）により確認済みか、評価実施国でこの要件に相当する国内基準により確認済みであることを検証しなければならない（shall）。*
- *暗号が運用環境によって提供される場合、評価者は、暗号がどのように利用されるかを確認し、かつ使用された機能の妥当性が FIPS 140-2（米国又はカナダで評価する場合）により確認済みであるか、評価実施国でこの要件に相当する国内基準により確認済みであることを検証するために、操作ガイダンス、ST 及び入手*

可能ないかなる設計文書も見直さなければならない(shall)。

評価者は、TOE でのセキュアな通信を有効にし、かつ、ローカル・ネットワークにパケット・スニファを置くことで、この機能をテストしなければならない (shall)。次に評価者は TOE を使用して、TOE の通信相手である高信頼 IT 製品全般との通信を要求するアクションを実行し、TOE を宛先とするか TOE を起点とする捕捉されたパケット通信量を確認し、その内容が難読化されていることを確認しなければならない (shall)。

FTP_TRP.1 高信頼パス

下位階層: なし。

FTP_TRP.1.1 **詳細化**:TSF は、TSF 自体とリモートの利用者との間に、他の通信路とは論的に異なり、かつ、TSF エンドポイントの確実な識別を提供し、かつ、通信後のデータを[選択: 改変、漏洩、[***割付: 他種別の完全性違反又は機密性違反 (other types of integrity or confidentiality violation)***]] から保護する通信路を提供するために、***[選択: 内部の、サードパーティ製の] 暗号スイート*を*活用***(*leverage*)しなければならない(shall)。

FTP_TRP.1.2 TSF は、リモートの利用者が高信頼パス経由で通信を開始することを許可しなければならない(shall)。

FTP_TRP.1.3 TSF は、初期利用者認証、管理機能実行のために高信頼パスの使用を要求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、利用者が HTTPS 経由のウェブ・アプリケーションのような TOE と情報をやりとりする方法が当該操作ガイダンスに説明されていることを検証するために、操作ガイダンスをチェックしなければならない(shall)。評価者は、TOE への高信頼パスが確立されるメカニズムが説明されているかどうか、及びこの確立を支援するために TSF が信頼する環境コンポーネントがもしあるとすればそれはどのようなものであるか説明されているかどうか判断するために、当該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、この機能を FTP_ITC.1 の保証アクティビティと同じような方法でテストしなければならない(shall)。利用者と TOE との間で送信されたデータが難読化されていれ

ば、高信頼パスが確立されたと推定できる。

6.1.9 未実現の依存性（Unfulfilled Dependencies）

ここでは、本 PP のために選択された要件に対する依存性として記載されたにもかかわらず未だに主張されていないセキュリティ機能要件（SFR）を詳述する。こうした依存性のそれぞれに対して、除外の根拠が提供されている。

FDP_ACC.1	この SFR は FMT_MSA.1 に対する未実現の依存性である。これは、管理者権限決定のための正式なアクセス制御 SFP がまだ PP によって要求されていないため、除外されてきたものである。FMT_MSA.1 は、FMT_MOF.1 と同じように適用されるべきである（should）。本 PP では、セキュリティ属性の管理権限を定義する際に特定のアクセス制御 SFP を適用するのではなく、すでに割り当てられた役割のみにそれを制限するか、他に利用者を論理的に分類するので十分である。
FIA_ATD.1	この SFR は FIA_USB.1 に対する未実現の依存性である。これは、ESM ポリシー管理製品が利用者のセキュリティ属性を*定義する*のではなく利用することになっていることから除外されてきた SFR である。ポリシーを定義する際に使用されうる属性はどのような属性であっても、互換性のある識別情報及びクレデンシャル情報管理製品により定義済みにしておくべきである（should）。そうでなければ、こうした属性は、ESM_ATD コンポーネントによって定義される可能性がある（may）。
FPT_STM.1	この SFR は FAU_GEN.1 に対する未実現の依存性である。これは、TOE には必ずしもそれ自体のシステム・クロックを組み込むことになっていないことから除外されてきた SFR である。ST 作成者は、システム・クロックの開始点を決定するために、評価段階で ESM の全体を検査すべきである（should）。評価境界（evaluation boundary）が、内部システム・クロックを使用する ESM 機器（appliance）の総体である場合には、FPT_STM.1 を主張すべきである（should）。しかし、ESM が、ホストのオペレーティング・システムや NTP サーバのような環境コンポーネントに依存する場合には、これは環境目標として正確なシステム時刻を表すのに許容可能な選択肢である。

6.2 セキュリティ保証要件

第 8.4.1 節の TOE に関するセキュリティ対策方針は第 8.2 節で識別した脅威に対処するために構成された。第 6.1 節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規のインスタンス化である。プロテクションプロファイル（PP）は、評価者が評価に適用可能な文書を査定して独立テストを実施する範囲の基本的な詳細を決めるために EAL1 セキュリティ保証要件（SAR）から得られたものである。

第 6.1 節の冒頭部で述べたように、本節にはコモンクライテリア（CC）に由来する SAR の一式が完全に盛り込まれている。これに対し、評価者が実施すべき保証アクティビティは「附属書 C –アーキテクチャのバリエーションと追加要件」及び本節で詳述されている。

本 PP に適合するために記載された ST に対して TOE を評価するための一般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、コモンクライテリア評価機関（CCTL : Common Criteria Testing Laboratory）は TOE を入手し、IT 環境及び TOE の管理ガイドを支援することになる。ST に記載された（ST 又は別文書の中で TOE 固有のものとして CCTL が詳細化することになる）保証アクティビティは、その後 CCTL によって実施されることになる。また CCTL は、EAL1 共通評価方法（CEM：Common Evaluation Methodology）で義務付けられたアクションもすべて実施することになっている（is expected to）。このアクティビティの結果は、妥当性確認のために（使用された管理者ガイダンスと併せて）文書にまとめられて提供されることになる。

開発者が追加的に提供すべき文書及びアクティビティ（又はこのうちのいずれか）があるとすれば、それはどのようなものかを明確にするために、各ファミリの開発者アクションエレメントに「開発者向け注意事項」が示されている。内容/記述及び評価者のアクティビティに関するエレメントは、追加的な保証アクティビティ（第 6.1 節に既出）がエレメント別ではなくファミリ全体として説明されている。また、本節で説明されている保証アクティビティは、第 6.1 節に規定されているものを補完する。

表 5 に要約した TOE セキュリティ保証要件は、本 PP の第 8.2 章で識別されている脅威に対処するために必要となる管理アクティビティと評価アクティビティを識別している。第 6.3 節では、本節のセキュリティ保証要件を選択する正当な理由を簡潔に示している。

表 5 TOE セキュリティ保証要件

保証クラス	保証コンポーネント	保証コンポーネントの説明

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 – 適合
脆弱性評定	AVA_VAN.1	脆弱性分析
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 の適合については、TOE の情報は、最終利用者が入手可能なガイダンス文書、及び ST の TOE 要約仕様(TSS)部分に収録されているものと予想される(注)。TOE 開発者は TSS を書くことは要求されないが、TSS に含まれている製品の説明は機能要件と関連があるため、この製品説明には同意しなければならない(must)。各 SFR に関連付けられている保証アクティビティは、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 ST 作成者に提供するべきである(should)。

注: 所有権にかかわる詳細情報が要求される場合、開発者は追加文書提供の選択権を保有するが、一般に公開された文書中に膨大な量の情報を記載しておくべきである(should)。

6.2.1.1 基本機能仕様(ADV_FSP.1)

機能仕様とは TSFI について記述したものである。必ずしも、このインタフェースの正式な仕様又は完全な仕様を用意する必要はない。また、本 PP に適合する TOE には、TOE 利用者が直接には呼び出さない運用環境に対するインタフェースが必ず用意されることになることから、あえて当該インタフェースを独自に記述するよう定めるのはほとんど無意味であり、あるとすれば当該インタフェースの間接的なテストのみと考えられる。本 PP では、このファミリのアクティビティは、機能要件を受けてTSSに記載されたインタフェースの理解と、AGD 文書に記載されたインタフェースの理解を重点的に扱うべきである(should)。指定された保証アクティビティを満たすために追加する「機能仕様」文書は不要とすべきである(should)。

評価対象となるべきインタフェースは、リストアップした保証アクティビティを実施するのに必要な情報を通じて明らかに

される。

開発者アクションエレメント

ADV_FSP.1.1D　開発者は、機能仕様を提示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 までの追跡を示さなければならない（shall）。

開発者向け注意事項: この節の最初の部分で述べたように、機能仕様は、ST の TSS で提供される情報と、AGD_OPR 及び AGD_PRE 文書に収録されている情報で構成されている。機能要件の中の保証アクティビティは、AGD_OPR 及び AGD_PRE 文書及び TSS セクション内に存続すべき証拠を挙げている。これは SFR と直接関連付けられているため、ADV_FSP.1.2D エレメントの追跡は暗黙的に実施済みであり、証拠文書を追加する必要はない。

内容及びプレゼンテーションエレメント

ADV_FSP.1.1C　機能仕様は、SFR 実施（SFR-enforcing）及び SFR 支援（SFR-supporting）TSFI のそれぞれについて使用目的と使用方法を記述しなければならない（shall）。

ADV_FSP.1.2C　機能仕様は、SFR 実施及び SFR 支援 TSFI のそれぞれに関連付けられているパラメータをすべて識別しなければならない（shall）。

ADV_FSP.1.3C　機能仕様は、インタフェースが SFR 不干渉（SFR-non-interfering）として暗黙的に分類されるための根拠を示さなければならない（shall）。

ADV_FSP.1.4C　追跡では、機能仕様において SFR が TSFI まで遡ることを実証しなければならない（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関する要件をすべて満たしていることを確認しなければならない（shall）。

ADV_ FSP.1.2E　評価者は、機能仕様が SFR の正確で完全なインスタンス化であると判定しなければならない（shall）。

保証アクティビティ:

このSARに関連付けられてい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 で説明されている評価アクティビティを支援するだけでなく、ほかに AGD、ATE 及び AVA の SAR で説明されているアクティビティのためにも提供されている。機能仕様の情報の内容についての要件は、実施されている他の保証アクティビティにより暗黙的に評価されている。インタフェース情報が十分でないために評価者がアクティビティを実行することができないとするならば、適切な機能仕様が提供されていなかったことになる。例えば、TOE が暗号アルゴリズム用の鍵の長さを設定する機能を提供しても、この機能を実行するインタフェースを指定していなければ、FMT_SMF に関連付けられた保証アクティビティは失敗することになる。

評価者は、TOE が遮断するか動作するときに使用する一連のインタフェースが TOE の機能仕様で説明されていることを検証しなければならない(shall)。評価者は、このインタフェースの説明を吟味して、このインタフェースの呼び出しについて十分な説明が尽くされていることを検証すべきである(should)。

また評価者は、TOE が無効データを受け入れる可能性にどのように対処するかに関する説明が TOE 機能仕様にあることも検証しなければならない(shall)。適切に保護されなければ、無効データを受け入れる可能性によって、アクセス制御の判断が翻され、許可されていない利用者にアクセス権が付与されるか許可された利用者へのアクセスが拒否されるという可能性が生じる。

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併せて提供されることになる。ガイダンスには、運用環境がセキュリティ機能に対してそれ自体の役割を果たすことができるという点について、許可された利用者がそれをどのように検証するのかについての説明を盛り込まれなければならない(must)。文書のスタイルは堅苦しくならず、許可された利用者が読みやすいものにすべきである(should)。

ST で主張されているように、ガイダンスは製品がサポートする運用環境ごとに提供されなければならない(must)。このガイダンスには以下の内容が盛り込まれる。

- その環境で、TOE を適切にインストールするための指示。及び
- 製品の1つ及び大規模な運用環境のコンポーネントの1つとして TOE のセキュリティを管理するための指示。

また、システム起動の最中に設定を改変することも、システム起動シーケンスからその設定を完全に消去することもできないように、ホスト側オペレーティング・システム上のセキュアな設定で TOE を起動する方法に関するガイダンスも提供しなければならない(must)。また、信頼されていないサブジェクトによって製品が使用不可(例えば、シャットダウ

ン)にならないような製品設定方法もガイダンスで説明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。こうしたガイダンスの要件は、各 SFR に定めた保証アクティビティに収録されている。

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: 開発者は、ここで情報を繰り返すのではなく、これから評価者がチェックすることになるガイダンスの詳細を確かめるために、このコンポーネントの保証アクティビティを見直すべきである(should)。そうすることで、条件を満たしたガイダンスを準備するのに必要な情報が得られる。

内容及びプレゼンテーションエレメント

AGD_OPE.1.1C 利用者操作ガイダンスには、利用者がアクセスすることができ、かつ、適切な警告をはじめとするセキュアな処理環境において制御しておくべき機能と権限が利用者役割別に記述されなければならない(shall)。

適用上の注意: *評価チームは、管理要件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施すべきである(should)。*

AGD_OPE.1.2C 利用者操作ガイダンスには、TOE によって提供された利用可能なインタフェースをセキュアに使用する方法が、利用者の役割ごとに記述されなければならない(shall)。

AGD_OPE.1.3C 利用者操作ガイダンスには、利用可能な機能とインタフェース(特に利用者の管理下にあるすべてのセキュリティ・パラメータ)が、利用者の役割ごとに記述されており、必要に応じてセキュアな値が示されていなければならない(shall)。

AGD_OPE.1.4C 利用者操作ガイダンスには、TSF の管理下にあるエンティティのセキュリティ特性の変更をはじめとする、実施の必要があり利用者がアクセスすることのできる機能に関連したセキュリティ関連事象の各種別が、利用者の役割ごとに明確に示されなければならない(shall)。

AGD_OPE.1.5C　利用者操作ガイダンスでは、TOE の(障害又は操作ミスの後の操作をはじめとする)操作について考えられうるモードがすべて識別され、かつ、セキュアな操作を維持した場合の結果と影響も識別されなければならない(shall)。

AGD_OPE.1.6C　利用者操作ガイダンスには、ST に記載の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が利用者の役割ごとに記述されなければならない(shall)。

AGD_OPE.1.7C　利用者操作ガイダンスは、明確かつ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関する要件をすべて満たしていることを確認しなければならない(shall)。

保証アクティビティ:

操作ガイダンスの内容によっては、各 SFR と併せて保証アクティビティで検証されるものもある。以下の追加情報も必要である。

操作ガイダンスには、評価を受けた TOE 設定に関連付けられた暗号エンジン設定のための指針を盛り込まなければならない(shall)。操作ガイダンスは、TOE に関する CC 評価の段階では他の暗号エンジンの使用に関する評価及びテストはいずれも行われなかったという警告を管理者に示さなければならない(shall)。

6.2.2.2　準備手順(AGD_PRE.1)

開発者アクションエレメント

AGD_PRE.1.1D　開発者は、準備手順込みで 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、開発者は準備手順についても必要となる内容を決定するために、保証アクティビティに目を向けるべきである(should)。

内容及びプレゼンテーションエレメント

AGD_ PRE.1.1C　準備手順には、開発者の引渡手順(delivery procedure)に従って引渡された TOE のセキュアな受入れ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　準備手続きには、TOE のセキュアな設置、及び ST に記述された運用環境のセキュリティ対策方針に従った運用環境のセキュアな準備に必要なすべての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関する要件をすべて満たしていることを確認しなければならない（shall）。

AGD_ PRE.1.2E　評価者は、TOE が運用を目的としてセキュアに準備されうることを確認するために、準備手順を適用しなければならない（shall）。

保証アクティビティ：

最初の部分で説明したように、特に TOE 機能要件をサポートするように運用環境の設定をするときには、ドキュメントに寄せられる期待が大きい。評価者は念のために、TOE のために ST が要求したすべてのプラットフォーム（（つまり、ハードウェアとオペレーティング・システムの組み合わせ）が TOE に対して提供されたガイダンスの中で適切に扱われていることを確認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 に対して提供された保証レベルでのライフサイクルサポートは、TOE ベンダの開発及び構成管理プロセスの検査ではなく、むしろ末端の利用者が目にすることの多い（end-user-visible aspects of）ライフサイクルに限定される。これは、製品全体の信頼性に貢献する際に開発者の実践が果たす重要な役割が損なわれるということではなく、むしろ、この保証レベルの評価において入手可能にすべき情報を反映したものである。

6.2.3.1　TOE のラベル付け（ALC_CMC.1）

このコンポーネントは、同じベンダの別製品又は別バージョンとの区別ができるよう、かつ、最終利用者が入手する場合に特定がしやすいよう TOE を識別することを目標としている。

開発者アクションエレメント

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

内容及びプレゼンテーションエレメント

ALC_CMC.1.1C　TOE には、一意の参照でラベル付けしなければならない（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関する要件をすべて満たしていることを確認しなければならない（shall）。

保証アクティビティ：

評価者は、ST をチェックして、ST の要件を満たすバージョンを特に識別する（製品名／バージョン番号のような）識別子が含まれていることを確認しなければならない（shall）。さらに、評価者は、テスト用に受け取った AGD ガイダンス及び TOE のサンプルをチェックして、バージョン番号が ST の中のバージョン番号と一致していることを確認しなければならない（shall）。ベンダが TOE を宣伝するウェブサイトを維持している場合、評価者はウェブサイトの情報を検査して、ST 内の情報が製品を識別するのに十分であることを確認しなければならない（shall）。

6.2.3.2　TOE の CM 範囲（ALC_CMS.1）

TOE の適用範囲及びそれに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 に記載した保証アクティビティで網羅される。

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）。

内容及びプレゼンテーションエレメント

ALC_CMS.1.1C　構成リストには、TOE 自体、及び SAR により必要とされる評価証拠を入れなければならない（shall）。

ALC_CMS.1.2C　構成リスト（configuration list）は、構成項目（configuration item）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関する要件をすべて満たしていることを確認しなければならない（shall）。

保証アクティビティ：

本 PP の中の「SAR によって要求される評価証拠」は、AGD 要件の下で情報管理者及び利用者に提供されるガイダンスとともに ST 内の情報に限定される。TOE が明確に識別されていること及びこの識別が ST と AGD ガイダンスと一致していることを(ALC_CMC.1 の保証アクティビティで行われるとおり)保証することで、評価者はこのコンポーネントに必要な情報を暗黙的に確認する。

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、適合主張を提示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示しなければならない(shall)。

内容及びプレゼンテーションエレメント

ASE_CCL.1.1C 適合主張には、ST 及び TOE が適合を主張する CC のバージョンを識別する CC 適合主張が盛り込まれなければならない(shall)。

ASE_CCL.1.2C CC 適合主張には、ST の CC パート 2 への適合が、CC パート 2 適合(CC Part 2 conformant)又は CC パート 2 拡張(CC Part 2 extended)として記述されなければならない(shall)。

ASE_CCL.1.3C CC 適合主張には、ST の CC パート 3 への適合が、CC パート 3 適合(CC Part 3 conformant)又は CC パート 2 拡張(CC Part 2 extended)として記述されなければならない(shall)。

ASE_CCL.1.4C CC 適合主張は、拡張コンポーネント定義(extended components definition)と一致していなければならない(shall)。

ASE_CCL.1.5C 適合主張には、ST が適合を表示する PP 及びセキュリティ要件パッケージがすべて識別されなければならない(shall)。

ASE_CCL.1.6C 適合主張には、ST のパッケージに対するいかなる適合も、パッケージ-適合又はパッケージ-追加(package-augmented)として記述されなければならない(shall)。

ASE_CCL.1.7C 適合主張の根拠では、その TOE 種別(TOE type)が、適合を主張している PP 内の

TOE 種別と一致しているということが実証されなければならない（shall）。

ASE_CCL.1.8C　適合主張の根拠は、そのセキュリティ課題定義が、適合を主張している PP 内のセキュリティ課題定義と一致していることを実証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関する要件をすべて満たしている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、セキュリティ要件に関する記述（statement）を示さなければならない（shall）。

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

内容及びプレゼンテーションエレメント

ASE_ECD.1.1C　セキュリティ要件に関する記述は、拡張セキュリティ要件をすべて識別しなければならない（shall）。

ASE_ECD.1.2C　拡張コンポーネントの定義では、拡張コンポーネントが拡張セキュリティ要件別に定義されなければならない（shall）。

ASE_ECD.1.3C　拡張コンポーネントの定義では、各拡張コンポーネントが、CC の既存のコンポーネント、ファミリ及びクラスにどのように関連しているのかが説明されなければならない（shall）。

ASE_ECD.1.4C　拡張コンポーネントの定義では、CC の既存のコンポーネント、ファミリ、クラス及び方法論が記述モデルとして使用されなければならない（shall）。

ASE_ECD.1.5C　拡張コンポーネントは、測定可能なエレメントと目標エレメントの適合又は不適合を実証できるようなエレメントで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関する要件をすべて満たしていること

を確認しなければならない(shall)。

ASE_ECD.1.2E　評価者は、拡張コンポーネントが既存のコンポーネントを使用して明確に説明される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 概説を提示しなければならない(shall)。

内容及びプレゼンテーションエレメント

ASE_INT.1.1C　ST 概説には、ST 参照、TOE 参照、TOE 概要及び TOE 説明を盛り込まなければならない(shall)。

ASE_INT.1.2C　ST 参照は、ST を一意に識別しなければならない(shall)。

ASE_INT.1.3C　TOE 参照は、TOE を一意に識別しなければならない(shall)

ASE_INT.1.4C　TOE 概要は、TOE の使用法及び主なセキュリティの特長を要約しなければならない(shall)。

ASE_INT.1.5C　TOE 概要は TOE 種別を識別しなければならない(shall)

ASE_INT.1.6C　TOE 概要は、TOE が必要とする任意の非 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 の物理的な適用範囲を記述しなければならない(shall)。

ASE_INT.1.8C　TOE 説明は、TOE の論理的な適用範囲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_INT.1.1E　評価者は、提供された情報が証拠の内容と記述に関する要件をすべて満たしている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 説明が相互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に関する記述を提示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示しなければならない（shall）。

内容及びプレゼンテーションエレメント

ASE_OBJ.2.1C セキュリティ対策方針に関する記述では、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説明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立ち向かった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）まで遡及して TOE の各セキュリティ対策方針を追跡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立ち向かった脅威、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遡及して、運用環境の各セキュリティ対策方針を追跡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すべての脅威に対抗するということを実証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すべての OSP（組織のセキュリティ方針）に立ち向かうということを実証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、運用環境のセキュリティ対策方針がいずれの想定も支持するということを実証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関する要件をすべて満たしている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、セキュリティ要件に関する記述を提示さなければならない（shall）。

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

内容及びプレゼンテーションエレメント

ASE_REQ.2.1C　セキュリティ要件の記述は、SFR 及び SAR を説明しなければならない（shall）。

ASE_REQ.2.2C　SFR 及び SAR で使用される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その他の用語は定義されなければならない（shall）。

ASE_REQ.2.3C　セキュリティ要件に関する記述は、セキュリティ要件のすべての操作を識別しなければならない（shall）。

ASE_REQ.2.4C　いずれも操作も正しく実行されなければならない（shall）。

ASE_REQ.2.5C　セキュリティ要件の依存性はそれぞれ満たされていなければならない。又は、満たされていない依存性がセキュリティ要件の根拠により正当化されなければならない（shall）。

ASE_REQ.2.6C　セキュリティ要件の根拠は、TOE のセキュリティ対策方針まで遡及して各 SFR を追跡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、TOE のセキュリティ対策方針をすべて満たしていることを実証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 が選択さ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記述は、内部的に一致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関する要件をすべて満たしている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、セキュリティ課題定義を提示しなければならない（shall）。

内容及びプレゼンテーションエレメント

ASE_SPD.1.1C　セキュリティ課題定義は脅威について説明しなければならない（shall）。

ASE_SPD.1.2C　いずれの脅威も、脅威エージェント、資産及び有害なアクションの観点から説明されなければならない（shall）。

ASE_SPD.1.3C　セキュリティ課題定義は OSP について説明しなければならない（shall）。

ASE_SPD.1.4C　セキュリティ課題定義は、TOE の運用環境に関する想定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_SPD.1.1E　評価者は、提供された情報が証拠の内容と記述に関する要件をすべて満たしていることを確認しなければならない（shall）。

6.2.4.7　TOE 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 要約仕様を提供しなければならない（shall）。

ASE_TSS.1.1C　TOE 要約仕様は、TOE が各 SFR をどのように満たしているのか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関する要件をすべて満たしていることを確認しなければならない（shall）。

ASE_TSS.1.2E　評価者は、TOE 要約仕様が TOE 概要及び TOE 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

設計又は実装上の弱点を利用する面とシステムの機能面のテストが指定されている。システムの機能的側面に関するテストは、ATE_IND ファミリで実施されるのに対し、設計又は実装上の弱点を利用する側面のテストは AVA_VAN ファミリで実施される。本 PP で規定した保証レベルでは、テストは、宣伝された機能及びインタフェースに基づいて行われるが、それと同時に設計情報の入手可能性にも依存する。評価プロセスの主な収穫の 1 つは、以下

の要件で規定したテスト報告書である。

6.2.5.1 独立テスト – 適合(ATE_IND.1)

TSS で説明されている機能と、提供された(設定及び操作をはじめとする)管理的な資料を確認するためにテストが実施される。6.1 節に SAR のための追加テストがいくつか指定されているが、このテストの焦点は、各 SFR で指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では、このコンポーネントに関連付けられている最低限のテスト・アクティビティが識別される。評価者は、テスト計画及びその結果を文書化するテスト報告書と、本 PP への適合を主張しているプラットフォーム/TOE の組み合わせに焦点を当てたカバレージに関する論証(coverage arguments)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、テスト用の TOE を提供しなければならない(shalll)。

内容及びプレゼンテーションエレメント

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関する要件をすべて満たしていることを確認しなければならない(shall)。

ATE_IND.1.2E 評価者は、TSF が指定されたとおりに操作することを確認するために、TSF のサブセットをテストしなければならない(shall)。

保証アクティビティ:

評価者は、システムのテスト実行という側面を文書にまとめたテスト計画と報告書を用意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文中に収録されているテスト・アクションをすべて網羅する。保証アクティビティに記載されている各テストに対してテストケースを 1 つずつ用意する必要ははないが、評価者は、ST に記載された該当するテスト要件がそれぞれ網羅されていることをテスト計画に文書化しなければならない(must)。

テスト計画はテストの対象となるプラットフォームを識別する。テスト計画には含まれていないが ST に含まれているプラットフォームについては、プラットフォームのテストを実施しない正当な理由(justification)をテスト計画で提示する。

正当な理由では、テストを実施したプラットフォームとテストを実施しなかったプラットフォームの違いを検討し、この違いが、実施対象となっているテストに影響を与えないという論拠を示さなければならない(must)。単に、この違いが何ら影響を与えないと断言するだけでは不十分で、根拠を示さなければならない(must)。ST で主張したプラットフォームがすべてテストされていれば、根拠は不要である。

テスト計画は、テストの対象となる各プラットフォームの構成、及び AGD 文書に収録されているもの以上に必要なセットアップについて説明する。評価者がテストの一環又は標準的な予備テスト条件として各プラットフォームのインストールとセットアップを行う場合には、AGD 文書に従うことになっている(are expected to)点に留意されたい。これには、特殊なテストドライバ又はツールが含まれる場合がある(may)。このドライバ又はツールは機能の性能に悪影響を及ぼさないであろうという論証(argument)(断言(assertion)ではない)が TOE とそのプラットフォームによって各ドライバ又はツールごとに示される。これには、使用される暗号エンジンの設定も含まれる。このエンジンによって実装された暗号アルゴリズムは本 PP で規定されており、現在評価を受けている最中の暗号プロトコル(Ipsec、TLS/HTTPS、SSH)で使用される。

テスト計画は、高度なテスト目的と、この目的を達成するために従うべきテスト手順を識別する。この手順には起こり得る結果が盛り込まれる。テスト報告書(単にテスト計画の注釈付き版になる可能性もある)には、テスト手順が実行されたときに起きたアクティビティが詳述され、実際のテスト結果が盛り込まれる。この記載は累積的な報告でなければならない(shall)。したがって、もし結果的に失敗に終わったテスト実行であれば、改変プログラムをインストールしてから、テストの再実行を適切に行い、報告書には、「合格」の結果のみを記載するのではなく、「不合格(fail)」及び「合格(pass)」という結果を(それを補う詳細と併せて)記載することになる。

6.2.6 クラス AVA: 脆弱性評定

評価機関は本プロテクションプロファイルの初回生成時に、このタイプの製品に対してこれまでどのような脆弱性が発見されているのかを見出すためにオープンソースを調査することになっている(is expected to)。この脆弱性には、初級攻撃者の脆弱性を上回る高度な知識が要求されることが多い。評価者は、侵入ツールが作成されてそれが評価機関にくまなく配布されてはじめて、TOE 内で見つかったこの脆弱性のテストを行うことになっている。ベンダ提供の文書があれば、評価機関はこの脆弱性の可能性についてコメントすることになっている。この情報は、侵入テストツールの開発や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ことになる。

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、テスト用の TOE を提供しなければならない(shalll)。

内容及びプレゼンテーションエレメント

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関する要件をすべて満たしていることを確認しなければならない(shall)。

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

AVA_VAN.1.3E 評価者は、その TOE が基本的な攻撃能力を持つと思われる攻撃者によって実行される攻撃に対して耐性があると判定するために、すでに識別されている潜在的な脆弱性に基づいて、侵入テストを実施しなければならない(shall)。

保証アクティビティ:

ATE_IND と同様、評価者はこの要件についても、得られた結果を文書にまとめた(document)報告書を作成しなければならない(shall)。この報告書は、実際には ATE_IND の中で言及されている包括的なテスト報告書に組み込まれるか、別文書になる可能性がある。評価者は、総じて ESM アプリケーションの分野で発見されてきた脆弱性と、特定の TOE に関係している脆弱性を決定するため、公開情報の検索を実施する。評価者は、調べたソース及び報告書の中で見出した脆弱性を文書にまとめる。評価者は、発見した脆弱性のそれぞれについて、その非適用性について理論的根拠を示すか、適正であれば、この脆弱性を確認するために、(ATE_IND で提供されるガイドラインを使用して)テストを策定する。適合性(suitability)は、脆弱性を悪用する際に必要となる攻撃ベクトル(attack vector)を評価することで決定される。例えば、起動時にキーの組み合わせを押すことで脆弱性を検出することができるのであれば、テストは本 PP の保証レベルに適している。また、脆弱性を悪用するために電子顕微鏡と液体窒素のタンクが必要になるとするならば、テストは適正なものではなく、適切な正当化が策定されることになろう。

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、この技術にとって初めての米国政府のプロテクションプロファイルであるからである。これらのタイプの製品に脆弱性が見つかった場合には、実際にベンダで行われている慣行に基づいて、一層厳しいセキュリティ保証要件が義務付けられることになる。

7 セキュリティ課題定義根拠

本節では、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。更に、マッピングが適切であることがわかるよう、リストされた対策方針を満たす際に使用されるセキュリティ機能要件（SFR）に基づく根拠も提供される。PP 適合実証のために、これらのマッピングがなければならないことが必ずしも要求されていない状況では、ST 作成者に役立つよう、根拠の末尾に太字の文字を追加した。

表 6 前提条件、環境上の対策方針、根拠

前提条件	対策方針	根拠
A.ESM – セキュリティデータを共有するために、TOEは他のESM製品との接続性を確立できるようになる。	**OE.AUDIT** – 運用環境が、遠隔にある監査データ保管用の場所を提供する。	運用環境は、FAU_STG_EXT.1を満たすために、遠隔にある監査データ用のリポジトリを提供しなければならない。これは、ESM監査管理製品が管理することが前提である。
	OE.PROTECT – 組織の資産を保護するために、アクセス制御製品が運用環境に1つ以上配置される。	TOEが、少なくとも1つのアクセス制御製品にポリシー・データを提供しない場合には、配置に目的があるわけではない。
A.MANAGE – TOEのインストール、設定及び操作を行うよう任命された有資格者が1人以上存在する。	**OE.ADMIN** – TOE内でサブジェクト識別子から属性へのマッピングを担う運用環境の管理者が1人以上存在する。	セキュリティ機能（TSF） は、新規のサブジェクト・データを企業に導入することを目的として用意されたものではないため、ESMが使用することになる識別データを定義する行為は、運用環境に帰属するアクティビティである。
	OE.INSTAL – TOE担当者は、TOEの配付、インストール、管理、及び操作がセキュアな形で行われていることを保証しなければならない（must）。	管理者が、TOEのセキュアな設定及び操作を保証できる場合には、その管理者が有資格であることが前提である。
	OE.PERSON – TOE管理者として従事する者は、注意深く選定され、TOEの適切な運用のための研修を	管理者の選定及び研修に対して適切な配慮がなされる場合は、以降も同じ管理者が義務を遂行すると期待される。

前提条件	対策方針	根拠
	受けなければならない（shall）。	
A.USERID – TOEが識別データを運用環境にから受け取る。	**OE.USERID** – 運用環境は、TOEへのアクセスを要求する利用者を識別できなければならない。	ESM製品が期待していることは、組織的に維持されている識別データをこの製品が利用できることである。

表 7 ポリシー、脅威、対策方針、根拠

ポリシー/脅威	対策方針	根拠
P.BANNER – TOEは、使用に関する禁止事項、法的取り決めをはじめとし、利用者がシステムへのアクセスによって同意する適切な情報を説明した初期バナー表示しなければならない（shall）。	**O.BANNER** – TOEは、TOEの使用について注意を促すメッセージを表示する。	**FTA_TAB.1**TOEがバナーを表示するための要件は、このポリシーが実装されることを保証するのに十分である。
T.ADMIN_ERROR – 管理者がTOEのインストール又は設定を不適切に行うと、結果的にセキュリティの仕組みが無効になる可能性がある。	**OE.ADMIN** – TOE内でサブジェクト識別子から属性へのマッピングを担う運用環境の管理者が1人以上存在する。	この対策方針では、TOEの設定を行う管理者を指名しておくようTOEに要求しており、これによってTOEには、一貫した管理と設定を受けるようになるという何らかの保証が提供される。
	OE.INSTAL – TOE担当者は、TOEの配付、インストール、管理、及び操作が、ITセキュリティと一致した形で行われていることを保証しなければならない（must）。	この対策方針は、担当者に対し、ITセキュリティが最上位の状態である形でセットアップされるようTOEをインストールし、構成をすることを要求する。これにより、TOEが適切かつセキュアな形でインストールされることが保証される。
	OE.PERSON – TOE管理者として従事する者は、注意深く選定され、TOEの適切な運用のための研修を受けなければならない（shall）。	この対策方針では、TOEのインストール、設定及び管理を行う者は、TOEを購入して活用しようと意図する組織によって厳しく検査されることが要求されている。これにより、この人物が怠慢ではなく、悪意もない

ポリシー/脅威	対策方針	根拠
		という何らかの保証が提供される。
T.CONTRADICT – 不注意な管理者が、アクセス制御実施について相矛盾する規則が含まれたポリシーを作成し、結果的に、明確なポリシー規則を持たないセキュリティポリシーが生成される可能性がある。	**O.CONSISTENT** – TSFが、相矛盾するポリシー・データを識別して修正する仕組みを提供する。	**FMT_MSA_EXT.5** 不適合データを検知して、検知した不適合箇所を修正する能力を提供するTSFの能力によって、アクセス制御製品には適合ポリシーのみが送信されて利用される。
T.EAVES – 悪意のある利用者が、TOEデータに対する未認可のアクセス権を得て、ネットワーク・トラフィック上で盗聴する可能性がある。	**O.DISTRIB** – TOEは、セキュアなチャネルを使用して高信頼IT製品にポリシーを配付する能力を提供する。	**ESM_ACT.1** **FTP_ITC.1(1)** TOEは、ある製品内及びその製品のセンシティブな接続に使用するクリティカル・セキュリティ・パラメータ（CSP）を生成するために、サードパーティ製の暗号ツールを活用する。TOEは、高信頼チャネルを介して外部製品宛てに送信されたデータ、及びマルチプルボックス配置（multiple-box deployment）の場合はTOEコンポーネント間で送信されたデータの暗号化、ハッシュ、及び認証の際に適切なCSPを使用することが期待される。
	O.EAVES – TOEがサードパーティ製の暗号一式を利用することになるか、TOEの中に、TOEを宛先とする通信チャネル及びTOEを起点とする通信チャネルのセキュリティを確保する暗号アルゴリズムを活用する能力が組み込まれる。	**FTP_ITC.1(1)** **FCS_CKM.1 (オプション)** **FCS_CKM_EXT.4 (オプション)** **FCS_COP.1(1) (オプション)** **FCS_COP.1(2) (オプション)** **FCS_COP.1(3) (オプション)** **FCS_COP.1(4) (オプション)** **FCS_RBG_EXT.1 (オプション)** **FTP_TRP.1** 送信時にデータを保護する暗号機能を使

ポリシー/脅威	対策方針	根拠
		用すると、未認可の第三者にデータが漏洩することも、その第三者によってデータが改変されることもなくなるという合理的な保証がTOEに付与される。
T.FORGE – 悪意のある利用者は、TOEの脆弱な能力又は存在していない能力を悪用して、アクセス制御製品に偽造ポリシーを送信するために、自らの識別の証拠を提供する可能性がある。	**O.ACCESSID** – 他のESM製品にデータを配付する前に、その製品の識別の妥当性を確認する能力がTOEに組み込まれる。	**FTP_ITC.1(1)** TOEからの高信頼チャネルを確立する前に識別の証拠を提供するようアクセス制御製品に要求すると、TOEによる不正なソースへの認証ポリシーの漏洩の危険性が低減される。これにより、ポリシーが調査目的で分析される危険性が低減する。
	O.AUTH – TOEは、運用環境からと人間及びITエンティティの利用者識別データを検査する仕組みを提供し、主張されている識別が、TSF管理機能をどの程度実行できる必要があるかを判断する。	**FIA_UAU.2** **FIA_UID.2** ポリシー管理製品は、認可と識別の済んだ外部のITエンティティとだけポリシー情報を交換することになっている（is expected to）。
	O.INTEGRITY – ポリシー・データの完全性を断言する能力がTOEに組み込まれる。	**FTP_ITC.1(2)** アクセス制御製品に送信されるポリシー・データの完全性を保証することにより、アクセス制御製品が受信するポリシーがそのためのポリシーであるという保証が考慮される。
	O.SELFID – TOEは、ESM配置内の他のプロセスにデータを送信した時点で、ESM配置に対して識別を確認できるようになる。	**FTP_ITC.1(1)** アクセス制御製品を使用して高信頼チャネルを確立する前に、TOEに対して識別の証拠を提供するよう要求すると、偽造ポリシーを使用するアクセス制御製品の危険性を軽減するのに役立つ。

ポリシー/脅威	対策方針	根拠
T.UNAUTH – 悪意のある利用者が、TOEの管理機能を利用するために、TOEの識別、認証、及び認可の仕組みを回避する可能性がある。	**O.AUDIT** – TOEは、TOEで保護された資源に対して行われる利用者のアクセス試行を検知するセキュリティ関連事象を生成する手段を提供する。	**FAU_GEN.1** **FAU_STG_EXT.1** **FPT_STM.1 (オプション)** ポリシー管理製品は、適切に識別された利用者に対してのみ、アクションの実行を許可する。ポリシー管理製品には、TOEの利用者が実行した監査ログを各セキュリティ関連アクションに対して生成することも要求されている。このほかに、TOEは、ローカルで監査を受けた事象を見直すために、悪意のあるアクションを検知できるような何らかの機能も提供しなければならない（must）。また、TOEは、監査後の事象データを監査マネージャESMコンポーネント又は外部リポジトリに解放（offload）する機能も提供しなければならない（must）。TOE上で実行されるアクションに対して適切な説明能力は、未認可アクションの検知に役立つことができるとともに、その影響を軽減することもできる。
	O.AUTH – TOEは、運用環境からと人間及びITエンティティの利用者識別データを検査する仕組みを提供し、主張されている識別が、TSF管理機能をどの程度実行できる必要があるかを判断する。	**FIA_UAU.2** **FIA_UID.2** **FIA_USB.1** **FMT_MSA.1(1)** **FMT_SMR.1** **FTP_TRP.1** ポリシー管理製品には、製品に組み込まれた固有の管理機能を、許可された利用者には許可し、未認可利用者には許可しないようにその製品独自のアクセス制御ポリシーを定義することが要求されている。これを行うために、利用者には、適切な識別と認証を受けることが求められ、例えば利用者セッション中に適用可能なサブジェクトが含まれるような、確立されたセッショ

ポリシー/脅威	対策方針	根拠
		ンを持つことが求められる。
	TOEは、セキュアなチャネルを使用して高信頼IT製品のふるまいを管理する能力を提供する。	**FAU_SEL_EXT.1** **FMT_MOF_EXT.1** **FMT_MSA.1(2)** **FMT_SMF.1** TSFには、少なくとも互換性のあるアクセス制御製品用に監査対象事象を設定する能力を組み込むことが要求されている。これにより、関連する監査データがESM配置全体で記録されていることが保証される。
T.WEAKIA - 悪意のある利用者が、総当たり攻撃によって認証資格情報を推測することで、TSFから不正に認証される可能性がある、	**O.ROBUST** - TOEは、攻撃者が正当な利用者になりすます能力をできるだけ食い止める仕組みを提供する。	**FIA_AFL.1** **FIA_SOS.1 FTA_TSE.1 (オプション)** **FTA_SSL_EXT.1 (オプション)** **FTA_SSL.3 (オプション)** **FTA_SSL.4 (オプション)** TOEが利用者のパスワードに対して、秘密の強度に関するポリシー（strength of secrets policy）を適用した場合には、個々のパスワードの特定に成功する確率が低くなる。 TOEが認証失敗の処理を適用した場合は、攻撃者が行うことのできる個々の推測数が少なくなる。
T.WEAKPOL – ポリシー管理者が、TOEを使用して、アクセス制御を容易にするために十分詳しい定義付けを行うことができなくなり、結果的に、アクセス制御製品のふるまいが、違法なアクティビティを行うことができるようになるか、適法なアクティビティを禁止するようになる可能性がある。	**O.POLICY** – TOEは、「Standard Protection Profile for Enterprise Security Management Access Control（エンタープライズ・セキュリティ管理アクセス制御標準プロテクションプロファイル）」に記載された技術タイプのうち、その1つ以上のデータ保護要件を十分満たすほど詳しく説明されているポリシーを生成する能力を提供する。	**ESM_ACD.1** **ESM_ATD.1 (オプション)** **ESM_ATD.2 (オプション)** **FMT_MSA.1(2)** **FMT_MSA.3 FMT_SMF.1** ポリシー管理製品は、ポリシーを定義する能力を提供しなければならない（must ）。この製品は、万全（robust）でなければならず、デフォルトでは必ず限定された状態でなければならない。これにより、互換性を備えた製品のアクセス制御機能の全一式を活用できる信頼すべきポリシーを作成す

ポリシー/脅威	対策方針	根拠
		ることが保証される。

8 セキュリティ課題定義

次節では、本 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

以下にリストアップした特定の条件が、TOE の運用環境に存在するものと想定されている。これらの前提条件には、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が含まれている。

8.1.1 接続性の前提条件

表 8 TOE の前提条件

前提条件の名称	前提条件の定義
A.ESM	セキュリティデータを共有するために、TOEが他のESM製品との接続性を確立できるようになる。
A.USERID	TOEが、識別データを運用環境にから受け取ることになる。

8.1.2 物理的な前提条件

本プロテクションプロファイルでは、TOE のアーキテクチャが変わる可能性があるという理由から、物理的な前提条件を規定していない。ST 作成者は、予想される TOE の使用法に適合する前提条件を加えるべきである（should）。

8.1.3 人的な前提条件

表 9 TOE の前提条件

前提条件の名称	前提条件の定義
A.MANAGE	TOEのインストール、設定及び操作を任命された有資格者が1人以上存在する。

8.2 脅威

以下は、TOE に対して適用可能な脅威のリストである。この脅威は、TOE が不正に機能する原因となる可能性の

ある攻撃、又は TOE セキュリティ機能（TSF）データを許可なくして入手する攻撃に関するものである。

表 10 脅威

表名	脅威の定義
T.ADMIN_ERROR	管理者がTOEのインストール又は設定を不適切に行うと、結果的にセキュリティの仕組みが無効になる可能性がある。
T.CONDTRADICT	不注意な管理者が、アクセス制御実施に関して相矛盾する規則が含まれたポリシーを作成する可能性がある。
T.EAVES	悪意のある利用者が、TOEデータに対する未認可のアクセス権を得て、ネットワーク・トラフィック上で盗聴する可能性がある。
T.FORGE	悪意のある利用者が、TOEの脆弱な能力又は存在していない能力を悪用して、アクセス制御製品に偽造ポリシーを送信するために、自らの識別の証拠を提供する可能性がある。
T.UNAUTH	悪意のある利用者が、TOEの管理機能を不正利用するために、TOEの識別、認証、又は認可の仕組みを回避する可能性がある。
T.WEAKPOL	ポリシー管理者が、TOEを使用して、万全なアクセス制御を容易にするために十分詳細な定義付けを行うことができなくなり、結果的に、アクセス制御製品のふるまいが、違法なアクティビティを行うことができるようになるか、適法なアクティビティを禁止するようになる可能性がある。
T.WEAKIA	悪意のある利用者が、認証資格情報を総当たり攻撃によって推測することで、TSFから不正に認証される可能性がある。

8.3 組織のセキュリティ方針

以下は、TOE に対して適用可能な組織のセキュリティ方針のリストである。

表 11 組織のセキュリティ方針

前提条件の名称	前提条件の定義
P.BANNER(注)	TOEは、使用に関する禁止事項、法的取り決めをはじめとし、利用者がシステムへのアクセスによって同意する適切な情報を説明した初期バナーを表示しなければならない（shall）。

注：このポリシーは、NIST SP 800-53 の管理番号 AC-8（control AC-8 in NIST SP 800-53）に基づくものである。

8.4 セキュリティ対策方針

本 PP に定義された脅威に適切に対処することを確実にするために、TOE 及び運用環境の両方に対するセキュリティ対策方針を満たさなければならない（must）。このセキュリティ対策方針については、以降の節にリストしている。

8.4.1 TOE のセキュリティ対策方針

以下に示したセキュリティ対策方針は、予想される TOE の特性である。この対策方針と、本 PP で定義しているセキュリティ機能要件との関連性については第 7 節で説明している。

表 12 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.ACCESSID	他のESM製品にデータを配付する前に、その製品の識別の妥当性を確認する能力がTOEに組み込まれる。
O.AUDIT	TOEは、TOEで保護された資源に対して行われる利用者のアクセス試行を検知するセキュリティ関連事象を生成する手段を提供する。
O.AUTH	TOEは、運用環境からと人間及びITエンティティの利用者識別データを検査する仕組みを提供し、主張されている識別が、TSF管理機能をどの程度実行できる必要があるかを判断する。

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.BANNER	TOEは、TOEの使用について注意を促すメッセージを表示する。
O.CONSISTENT	TSFが、相矛盾するポリシー・データを識別して修正する仕組みを提供する。
O.DISTRIB	TOEは、セキュアなチャネルを使用する高信頼IT製品にポリシーを配付する能力を提供する。
O.MANAGE	TOEは、セキュアなチャネルを使用して高信頼IT製品のふるまいを管理する能力を提供する。
O.EAVES	TOEがサードパーティ製の暗号一式を利用することになるか、TOEの中に、TOEを宛先とする通信チャネル及びTOEを起点とする通信チャネルのセキュリティを確保する暗号アルゴリズムを活用する能力が組み込まれる。
O.INTEGRITY	ポリシー・データの完全性を断言する能力がTOEに組み込まれる。
O.POLICY	TOEは、「Standard Protection Profile for Enterprise Security Management Access Control（エンタープライズ・セキュリティ管理アクセス制御標準プロテクションプロファイル）」に記載された技術タイプのうち、その1つ以上のデータ保護要件を十分満たすほど詳しく説明されているポリシーを生成する能力を提供する。
O.ROBUST	OEは、攻撃者が正当な利用者になりすます能力をできるだけ食い止める仕組みを提供する。
O.SELFID	TOEは、ESM配置内の他のプロセスにデータを送信した時点で、ESM配置に対して識別を確認できるようになる。

8.4.2 運用環境のセキュリティ対策方針

以下のセキュリティ対策方針は、TOE を配置される運用環境に対して予想される特性である。

表 13 運用環境のセキュリティ対策方針

環境セキュリティ対策方針	環境のセキュリティ対策方針の定義
OE.ADMIN	TOE内でサブジェクト識別子から属性へのマッピングを担う運用環境の管理者が1人以上存在する。
OE.AUDIT	運用環境が、監査データ保管用としてリモートの場所を提供する。
OE.INSTAL	TOE担当者は、TOEの配付、インストール、管理、及び操作がセキュアな形で行われていることを保証しなければならない（must）。
OE.PERSON	TOE管理者として従事する者は、注意深く選定され、TOEの適切な運用のための研修を受けなければならない（shall）。
OE.PROTECT	組織の資産を保護するために、アクセス制御製品が運用環境に1つ以上配置される。
OE.USERID	運用環境は、TOEへのアクセスを要求する利用者を識別できなければならない。

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 Identity and Credential Management, version 1.*x*, forthcoming

(2) Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Access Control, version 2.0, March 14, 2012

(3) Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Secure Configuration Management, version *TBD*, forthcoming

(4) Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Audit Management, version *TBD*, forthcoming

(5) Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Authentication Server, version *TBD*, 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

(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, The Advanced Encryption Standard Algorithm Validation Suite (AESAVS), November 2002

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

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

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

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

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

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

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

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

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

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

(28) National Institute of Standards and Technology, NIST Special Publication 800-90 Recommendation for Random Number Generation, March 2007

(29) National Institute of Standards and Technology, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001

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

(31) 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 略語

表 14 略語と定義

略語	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）
DAC	Discretionary Access Control（任意アクセス制御）
ESM	Enterprise Security Management（エンタープライズ・セキュリティ管理）
IT	Information Technology（情報通信技術）
LDAP	Lightweight Directory Access Protocol（ライトウェイト・ディレクトリ・アクセス・プロトコル）
MAC	Mandatory Access Control（強制アクセス制御）
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（オペレーティング・システム）
OSP	Organizational Security Policy（組織のセキュリティ方針）
PM	Policy Management（ポリシー管理）
PP	Protection Profile（プロテクションプロファイル）
RBAC	Role-Based Access Control（役割ベースのアクセス制御）
SAR	Security Assurance Requirement（セキュリティ保証要件）
SCM	Secure Configuration Management（セキュアな構成管理）
SFP	Security Function Policy（セキュリティ機能方針）
SFR	Security Functional Requirement（セキュリティ機能要件）

略語	定義
ST	Security Target（セキュリティターゲット）
TSF	TOE Security Function（TOEセキュリティ機能）
TFSI	TOE Security Function Interface（TOEセキュリティ機能インタフェース）

附属書 B - NIST SP 800-53/CNSS 1253 マッピング

ここでは、要求を満たすために TOE が使用できる他の関連基準の要件を示すデータを記載する。この情報はコモンクライテリア（CC）の観点から見れば必ずしも必要というわけではないが、この情報をセキュリティターゲットに盛り込むことは、配置の際に多数の基準への適合の必要が生じたとき省くことのできる冗長作業を特定するのに役立つと考える。

以下の表は、本 PP の一部として定義された機能要件と保証要件、及びこの要件に適用する NIST 800-53 セキュリティ管理をリストアップしたものである。CC パート 2 及び CC パート 3 に定義した機能要件と保証要件の対応表は、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」から導出された。

なお、以下に掲載したガイドラインは、本 PP に対する厳格な適合が主張されているという想定に基づくものである。もし ST 作成者が、多数の PP に対する適合を主張することで TOE を強化している場合には、ここには詳細に記録されていない追加的な管理が適用される可能性がある。

表 15 NIST 800-53 要件との互換性

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
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_ACD.1	**アクセス制御ポリシー定義** アクセス制御ポリシー定義	AC-2	アカウント管理 | アクセス権の指定	部分的。 ESM_ACD.1は、後々アクセス制御製品が実施することのできるアクセス制御ポリシーを定義する能力をTOEに提供する。これにより、AC-2のアクセス権（access privilege）に関する仕様の側面が提供される。
		AC-3	アクセス実施 | システム実施認可	部分的。AC-3は実施に焦点を当てているが、実施に極めて重要なものは、実施対象のポリシーを定義する能力である。
		AC-3(3)	**アクセス実施** | 非任意アクセス制御	**部分的。**この管理策（control）は、このポリシーの管理を受けるサブジェクト、オブジェクト、及び操作を定義する。
		AC-3(4)	**アクセス実施** | 任意アクセス制御	**部分的。**この管理策は、このポリシーの管理を受けるサブジェクト、オブジェクト、及び操作を定義する。
		注: 推理によれば、ESM_ACDは、他で実施されるポリシーを定義するという点で、FDP_ACC及びFDP_IFC管理にほぼ類似している。		

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
ESM_ACT.1	**アクセス制御ポリシー送信** アクセス制御ポリシー定義	AC-2	**アカウント管理** | アクセス権の指定	**部分的。** ESM_ACD.1は、後々アクセス制御製品が実施することのできるアクセス制御ポリシーを送信する能力をTOEに提供する。これにより、AC-2のアクセス権に関する仕様の側面が提供される。
ESM_ATD.1 (オプション)	**属性定義** オブジェクト属性定義	AC-3	**アクセス実施** | システムが認可を実施する	**部分的。**この管理策は、ポリシーの実施に極めて重要なオブジェクト属性を定義する。
		AC-3(3)	**アクセス実施** | 非任意アクセス制御	**部分的。**この管理策は、ポリシーの実施に極めて重要なオブジェクト属性を定義する。
		AC-3(4)	**アクセス実施** | 任意アクセス制御	**部分的。**この管理策は、ポリシーの実施に極めて重要なオブジェクト属性を定義する。
ESM_ATD.2 (オプション)	**属性定義** サブジェクト属性定義	AC-2	**アカウント管理** | アクセス権の指定	**部分的。**この管理策は、ポリシーの実施に極めて重要なサブジェクト属性を定義する。
		AC-3	**アクセス実施** | システムが認可を実施する	**部分的。**この管理策は、ポリシーの実施に極めて重要なサブジェクト属性を定義する。
		AC-3(3)	**アクセス実施** | 非任意アクセス制御	**部分的。**この管理策は、ポリシーの実施に極めて重要なサブジェクト属性を定義する。
		AC-3(4)	**アクセス実施** | 任意アクセス制御	**部分的。**この管理策は、ポリシーの実施に極めて重要なサブジェクト属性を定義する。
FAU_GEN.1	**セキュリティ監査データの生成** 監査データの生成	AU-2	**監査対象事象** | [監査対象事象]、根拠、及び調整	**部分的。**FAU_GEN.1.1は、監査すべき事象の定義を行う(この管理策の大半に対処する)が、そのセットが対応しているかどうか確認するには割付を比較する必要がある。FAU_GENには、監査可能及び監査済みという両方の意味がある。また、これは800-53では2つの明確な管理策であることにも留意されたい。
		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の生成の側面は、AU-12の生成の側面を提供する。
		AC-17(1)	**リモート・アクセス** | 自動化監査/管理	**部分的。**FAU_GEN.1での割付に、リモート・アクセスの監査が含まれてい

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
				ない場合には、この制御は部分的に満たされている（監査の面）。
		AU-3	**監査記録の内容** | 最小の監査記録情報	**部分的。** FAU_GEN.1.2は各監査記録に含まれていなければならない内容のリストを詳述する。AU-3/AU-3(1)を満たしてどうか確認するために、割付を制御と比較しなければならない（must）。
		AU-3(1)	**監査記録の内容** | 追加詳細情報:[リスト]	**部分的。** FAU_GEN.1.2は各監査記録に含まれていなければならない内容のリストを詳述する。AU-3/AU-3(1)を満たしてどうか確認するために、割付を制御と比較しなければならない（must）。
		注: このSFRは、監査対象事象を、セキュリティターゲットに盛り込まれている他のSFRと、目的とする情報レベル(最小限、基本など)に基づかせている。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の割付の間に、義務付けられた相関性はない。		
FAU_SEL_EXT.1	**セキュリティ監査事象の選択** 外部選択監査	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管理策の項目bに移動する。
FAU_STG_EXT.1	**セキュリティ監査事象ストレージ** リモート監査証跡ストレージ	AU-9	**監査情報の保護** | 未認可アクセスから情報/ツールを保護する	**部分的。** SFRは基本的な管理策の基本的な目的に取り組むが、監査データの書き込み先となるリポジトリ/エンティティは、未認可での監査データの改変をできないようにしなければならない（must）。しかし、この管理策は、監査証跡を保護するのみならず、（SFRの対象外となっている）監査ツールも保護する。
FCS_CKM.1 (オプション)	**暗号鍵管理** 暗号鍵作成	SC-12	**暗号鍵の確立と管理** | 組織が暗号鍵を確立/管理する	**部分的。** このSFRは、800-53管理策の側面の1つを取り扱う。標準及びプロトコルの割付は、必要とされる拡張と突き合わせて比較する必要がある。
		注: NIST 800-53管理では、様々な角度から見た管理(生成、配付、アクセス及び破棄)を区別していない。		
FCS_CKM_EXT.4 (オプション)	**暗号鍵管理** 暗号鍵破棄	SC-12	**暗号鍵の確立と管理** | 組織が暗号鍵を確立/管理する	**部分的。** このSFRは、800-53管理策の側面の1つを取り扱う。標準及びプロトコルの割付は、必要とされる拡張と付き合わせて比較する

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
				必要がある。
		注: NIST 800-53管理では、様々な角度から見た管理(生成、配付、アクセス及び破棄)を区別していない。		
FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) (オプション)	**暗号操作** 暗号操作	SC-13	**暗号の使用** | 要件を満たすモジュールによる暗号の実装	**部分的。** SFRがその管理策を満たす程度は、割付がどのように仕上がったかによって異なる。
		注: SFRはきわめて広範であり、全種類の暗号操作を網羅するために完了することができる(may)。その多くは、NIST800-53のSFRでは網羅されていない。NISTで取り上げられていない領域の例には、セキュアな暗号ハッシュとそれを必ず使用するタイミング、及び使用された乱数生成器の品質に関する標準などがある。		
FCS_RBG_EXT.1 (オプション)	**ランダムビット生成** ランダムビット生成			**マッピングはなし。** これに対応する管理策は見当たらない。SFRは、予想される乱数生成の特徴を定義する。
FIA_AFL.1	**認証失敗** 認証失敗処理	AC-7	**失敗に終わったログイン試行** | 制限及びロック	**完全。** このSFRは、この管理策のあらゆる面を対象にするようである。
FIA_SOS.1	**秘密の仕様** 秘密の確認	IA-5(1)	**認証者管理** | パスワード複雑化(Password complexity)、ライフタイム、再使用	**部分的。** 割付内の複雑化の仕組みは、利用者が作成したパスード(秘密鍵)に対する強度の検証を扱う。
FIA_UAU.2	**利用者の認証** アクション前の利用者の認証	IA-2	**識別及び認証 (組織の利用者) |** 組織の利用者に対する一意の I&A	**部分的。** これは、組織の利用者の認証を扱う。
		IA-8	**識別及び認証 (組織外利用者) |** 組織外利用者に対する一意の I&A	**部分的。** これは、組織外利用者の認証を扱う。
FIA_UID.2	**利用者の識別** アクション前の利用者の識別	IA-2	**識別及び認証 (組織の利用者) |** 組織の利用者に対する一意の I&A	**部分的。** これは、組織の利用者の識別を扱う。
		IA-8	**識別及び認証 (組織外の利用者) |** 組織外利用者に対する一意の I&A	**部分的。** これは、組織外利用者の識別を扱う。
FIA_USB.1	**利用者・サブジェクト結合** 利用者・サブジェクト			**マッピングはなし。** このSFRは、TSFが特定の利用者属性とサブジェクトとを関連付けて、初期割付時又はその属性を変更する時に一連の規則を実施することを要求してい

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
	結合			る。AC-16は、情報と属性の結合を扱う。ただし、明確に、FIA_USB.1で同義のサブジェクトに対してということではない。
FMT_MOF_EXT.1	TSF内のセキュリティの管理 外部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** | 非任意アクセス制御	**部分的。**管理機能を特定の役割に制限することは、少なくともRBACの部分的な実装である。
FMT_MSA.1(1)	セキュリティ属性の管理 セキュリティ属性の管理（内部属性）	SI-9	**情報入力に関する禁止事項** | 情報を入力できるのは、許可された人物に限られる	**部分的。**SFRは、この管理策を暗示しているようではあるが、SFRのほうがはるかに具体的である。
FMT_MSA.1(2)	セキュリティ属性の管理 セキュリティ属性の管理（外部属性）	SI-9	**情報入力に関する禁止事項** | 情報を入力できるのは、許可された人物に限られる	**部分的。**SFRは、この管理策を暗示しているようではあるが、SFRのほうがはるかに具体的である。
FMT_MSA.3	セキュリティ属性の管理 静的属性の初期化			**マッピングはなし。**このSFRに対応する管理策は見当たらない。SFRは、TOEに対し、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1つを選択する: RESTRICTIVE（限定的な）、PERMISSIVE（許容的）［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し、オブジェクト又は情報が作成される場合は、[割付: 認可を受け、かつ識別された役割] が、そのデフォルト値を無効にする別の初期値を指定することを許可することを要求する。
FMT_MSA_EXT.5	セキュリティ属性の管理 適合するセキュリティ属性			**マッピングはなし。**このSFRはTSFに対し、アクセス制御製品に適合するセキュリティ属性を定義して、不適合が検知された場合には対策を取るよう要求する。適合している定義済みの属性を要求する特定の管理策はない。
FMT_SMF.1	管理機能の仕様 管理機能の仕様			**マッピングはなし。**このSFRは、他の場所で捕捉されていない管理機能を指定するための制約なしのSFR（open ended SFR）である。割付に応じて、ほぼすべての管理策に対応することが可能と思われる。

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
FMT_SMR.1	**セキュリティ管理役割** セキュリティ役割	AC-2(7)	**アカウントの管理** | 役割に基づくスキーム	**部分的。**このSFRは、情報システムに関するものであり、管理策は組織に関するものであるが、利用者全員が役割に割り当てられると言っているようであり、これはFMT_SMRと一致する。
		AC-5	**職務分掌（Separation of Duties）** | 組織レベル	**部分的。**システムが明らかな役割を提供する場合、それは職務分掌規定及び最小特権原則の適用を支援するのはほぼ間違いない。
		AC-6	**最小特権（Least Privilege）** | 最小特権の概念を採用する	**部分的。**システムが明らかな役割を提供する場合、それは職務分掌規定及び最小特権原則の適用を支援するのはほぼ間違いない。
FPT_STM.1 (オプション)	**タイムスタンプ** 高信頼タイムスタンプ	AU-8	**タイムスタンプ** | 内部クロック	**完全。**このSFRは、信頼できるタイムスタンプの提供について言及している。おそらくは監査目的である。大半のプロファイルは、（AU-8(1)を提供する）環境でNTPと統合するために、これを改変している。ただしこれは、基本SFRから義務付けられたものではない。
FTA_SSL_EXT.1 (オプション)	**セッション・ロックと終了** 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はシステム起動のセッション・ロックを提供する。FTA_SSL.1.2は、適切な割付があれば、ロック解除のために必要となるアクションを扱う。
		AC-11(1)	**セッション・ロック** |スクリーン・セーバーあり（With screen saver）	**完全。**FTA_SSL.1.1は、システム起動による画面のクリア又は上書きを提供する。
FTA_SSL.3 (オプション)	**セッション・ロックと終了** TSF起動による終了	SC-10	**ネットワークの切断** | セッション終了時又は [時刻] にネットワーク接続を終了	**完全。**旧AC-10はAC-10に統合されなかった点に留意されたい。これにより、このことがネットワークの切断であるだけでなく、セッションの終了も意味することが明らかになった。
FTA_SSL.4 (オプション)	**セッション・ロックと終了** 利用者起動による終了	SC-23(2)	**セッションの真正性** | 容易に観測可能なセッション・ログアウト機能を提供	**完全。**このSFRは、ウェブ・セッションのログアウト機能があるということを暗示しているようである。
		注: ウェブ以外のセッションについては利用者が見ることができるログアウト機能があることを義務付ける管理はない模様である。		
FTA_TAB.1	**TOEアクセス・バナー表示** TOEアクセス・	AC-8	**システムの利用に関する通知** | バナー	**完全。**この管理策は、この管理策のあらゆる面に対処するようである。この管理策には、メッセージを消去するための積極的なアクションを要

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
	バナー（デフォルト値）（Default TOE Access Banners）			求するなどの追加要件があることに留意されたい。
FTA_TSE.1 (オプション)	TOEセッション確立 TOEセッション確立			**マッピングはなし。**このSFRは、TOEが [割付: 属性] に基づいて、セッションの確立を拒否できることを要求する。これは、「NIST SP 800-53 Revision 3 control（NIST SP 800-53改訂3版管理策）」とのマッピングを行うには広範過ぎる。
FTP_ITC.1(1) FTP_ITC.1(2)	TSF間高信頼チャネル TSF間高信頼チャネル	IA-3(1)	**デバイスの識別及び認証** | 双方向暗号に基づく認証によるリモート/無線接続の前	**部分的。**このSFRは、他の通信チャネルとは論理的に異なり、そのエンドポイントについて確実な識別を提供し、かつ、チャネル・データを改変又は漏洩から保護する、それ自体と別の高信頼IT製品との間にある通信チャネルの供給について説明する。この管理策は、エンドポイントの識別を提供する。
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] 間の高信頼パス	**部分的。**SFRが管理策を提供するかどうかは、割付によって異なる。
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			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	適合主張 適合主張			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6	セキュリティ課題定義 セキュリティ課題定義			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
EAL7				
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			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
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			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**拡張コンポーネント定義** 拡張コンポーネント定義			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
ASE_REQ.1 EAL1	**セキュリティ要件** 言明されているセキュリティ要件			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
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			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
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			**マッピングはなし。**このSARは、セキュリティターゲットの書式及び構造、評価対象となっている製品の機能要件及び保証要件の説明を扱う。
ASE_TSS.1 EAL1 EAL2 EAL3 EAL4	**TOE要約仕様** TOE要約仕様	SA-4(1)	**取得** | 取得文書は、分析/テストをサポートするセキュリティ管理の機能特性を説明する	**部分的。**ST内のTSSは、製品が*どのように*してセキュリティ機能要件を実装するかを説明し、以降に行われるあらゆる分析及びテストのための高水準の基盤を提供する。

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
EAL5 EAL6 EAL7		SA-5(1)	**情報システム証拠文書** | 組織は、セキュリティ関連の機能特性に関するベンダ証拠文書を入手する	**部分的。**ST内のTSSは、STで主張されてい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を説明する。
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)	**取得** | 取得文書は、分析/テストをサポートするセキュリティ管理の設計/実装を説明する。	**部分的。**ADV_FSPファミリは、機能インタフェースに関する情報を提供する。
		SA-5(2)	**情報システム証拠文書** | 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を説明する	**部分的。**ADV_FSPファミリは、機能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	**利用者操作ガイダンス** 利用者操作ガイダンス	SA-5	**情報システム証拠文書** | SFUG + TFM	**完全。**AGD_OPEは、管理者及び利用者証拠文書の統合要件である。
		注: NIST 800-53はCC v2の手法と類似しており、管理者と利用者の証拠文書(AGD_USR、AGD_ADM)とを区別した。CC v3はこの2つを結合して1つのSARにし、管理者以外の利用者を持たない製品も中にはあるという状況を反映した。		
AGD_PRE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**準備手順** 準備手順	SA-5	**情報システム証拠文書** | SFUG + TFM	**完全。**このSFRは、セキュアな受け入れとセキュアな配付に必要となるすべての手順の説明を要求している。この管理策は、セキュアな設定及びインストールのための証拠文書を要求している。
注: 800-53での構成管理(CM)とコモンクライテリアでの構成管理(CM)との違いに関する一般的な見解。コモンクライテリアの構成管理(CM)とは、製品開発の構成管理(CM)を意味するものであり、システム内で構成管理が行うフィールディングのことではない。NIST 800-53ではフィールディング後のシステムの管理の制御に焦点が当てられており、開発者構成管理(CM)にはそれほど焦点が当てられていない。				
ALC_CMC.1 EAL1	**構成管理（CM ）の機能** **TOEのラベル付け**	CM-9	**構成管理計画** | 必要な情報とともに構成管理(CM)計画を有する	**部分的。**これは、設定項目の定義を扱う。ALC_CMは、*製品*に焦点を当てているのに対し、CM-9は*システム*に焦点を当てている点に留意されたい。
		SA-10	**開発者構成管理** | 開発段階では開発者が構成管理を有する; 欠陥の追跡	**部分的。**ALC_CMCは、CMプロセスの持つ開発者の側面をいくつか捕捉する。
ALC_CMS.1 EAL1	**CM適用範囲** **TOE CM 範囲（Coverage）**	CM-9	**構成管理計画** | 必要な情報とともに構成管理(CM)計画を有する	**部分的。**これは、設定項目の定義及び設定項目を特定する方法の定義を扱う。ALC_CMは、*製品*に焦点を当てているのに対し、CM-9は

CC SFR/SAR		NIST 800-53管理策		コメント及び見解
				*システム*に焦点を当てている点に留意されたい。
		SA-10	**開発者構成管理** | 開発段階では開発者が構成管理を有する; 欠陥の追跡	**部分的。**ALC_CMSは、CMプロセスの持つ開発者の側面をいくつか捕捉する。
ATE_IND.1 EAL1	**独立テスト** **独立テスト – 適合**	CA-2	**セキュリティ評価** | 開発計画、評価、報告書の作成	**部分的。**この管理策は、セキュリティ機能に対する独立テスト計画の開発の側面及びその機能の評価の側面を扱う。
		CA-2(1)	**セキュリティ評価** | 独立した評価者とともに…	**部分的。**これは、評価がベンダではなく、CCTLによって実施されるという事実を扱う。
		SA-11(3)	**開発者セキュリティ・テスト** | 独立した妥当性確認及び検証の下でのST&Eの実装	**部分的。**ATE_INDは、テスト一式の全体又は一部の再実行など、評価者によって実施される独立テストを要求する。
		注: ATE_INDとSA-11(3)には大きな違いがある。ATE_INDは独立評価者がテストを実施することを求めている。SA-11(3) は、独立評価者の監視の下で開発者にテストを実施させる。そもそもテスト手順と反復について実際の品質を評価するという点で、この手法には大きな違いがある。 **注:** テスト一式の一部に対して独立的に監視できるのはATE_IND.1のみである。		
AVA_VAN.1 EAL1	**脆弱性分析** **脆弱性調査**	CA-2(2)	**セキュリティ・アセスメント** | [告知された/ 告知されていない] セキュリティのテスト（例: 侵入テスト）	**部分的。**これは、侵入テストを実施するための要件を扱う。
		RA-3	**リスク評価** | リスク・アセスメントの実施/詳細記録化/見直し	**部分的。**考えられる限りでは、リスク評価の一部で、脆弱性に関する調査を実施中である。CCは、正式な脆弱性の走査を暗示していない点に留意されたい。それに該当するのはRA-5である。
		SA-11(2)	開発者脆弱性分析	**部分的。**AVA_VAN は、実施された脆弱性分析があることを要求する。
		注: 別のAVA_VANコンポーネントは、脆弱性の深さと範囲の点で異なる。NIST SP 800-53改訂第3版では、脆弱性評価の品質について指示（dictate）することはどうにもならないようである。		

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 属性定義

本プロテクションプロファイルは少なくとも、適合 TOE はアクセス制御ポリシーを定義して配付できなければならないということを要求している。企業に対して十分きめ細かいアクセス制御を円滑に進めるために、ポリシーはサブジェクト属性及びオブジェクト属性（又はこのうちのいずれか）を要求することができる（may）。したがって、エンタープライズ・セキュリティ管理（ESM）には、サブジェクト及びオブジェクト（又はこのうちのいずれか）の属性データを定義する機能を組み込まなければならない（must）。属性の定義は、ポリシー管理コンポーネントで扱うか、「Standard Protection Profile for ESM Identity and Credential Management（ESM 識別情報及びクレデンシャル情報管理標準プロテクションプロファイル）」で扱うことができる（may）。サブジェクト又はオブジェクトの属性定義機能が、ポリシー管理コンポーネントに組み込まれることになっている場合には、本節のセキュリティ機能要件（SFR）を使用すべきである（should）。本 PP への TOE の適合主張にこの機能が含まれていない場合には、実施する識別情報管理及びクレデンシャル情報管理製品との互換性がなければならない（must）。

C.1.1 ESM_ATD.1 オブジェクトの属性定義

下位階層: なし。

ESM_ATD.1.1 TSF は、次に示した各オブジェクトに属しているセキュリティ属性のリストを維持しなければならない（shall）: [**割付: *セキュリティ属性のリスト***]。

ESM_ATD.1.2 TSF は、セキュリティ属性を各オブジェクトに関連付けることができなければならない（shall）。

適用上の注意: オブジェクト・セキュリティ属性（object security attribute）とは、最終的にはアクセス制御の決定を考慮してもよいが（factor into）、利用者及びポリシーのいずれにも関連付けられていない属性を意味する。

依存性: なし。

保証アクティビティ:

評価チームは、TOE 内のオブジェクト・データの生成と活用がどれほど正確であるかについては、設計文書の評価を

通して決定しなければならない(must)。次に評価チームは、目的とするオブジェクト又はオブジェクトのセットにデータを適用することになる通常の TOE 機能を介してこの情報を生成しなければならない(must)。次に評価チームは、アクセス制御決定の際に適用されたこの属性データを使用するポリシーを書き込むために、ポリシー管理製品を使用しなければならない(must)。このポリシーがアクセス制御製品によって利用された時点で、評価チームは、予想される肯定的な結果と否定的な結果の両方について、そのオブジェクトに対するアクションを試すべきである(should)。

この追加(inclusion)のほかに、現在 PP によって記述されている既存の SFR に対して以下の要件追加(augmentation)を行うべきである(should)。

- FMT_MSA.1 は、サブジェクト属性のほかにオブジェクト・セキュリティ属性にも適用されると想定されていなければならない(must)。

C.1.2 ESM_ATD.2 サブジェクトの属性定義

下位階層: なし。

ESM_ATD.2.1 TSF は、次に示した各サブジェクト属しているセキュリティ属性のリストを維持しなければならない(shall):[割付:***セキュリティ属性のリスト***]。

ESM_ATD.2.2 TSF は、セキュリティ属性を各サブジェクトに関連付けることができなければならない(shall)。

適用上の注意: サブジェクト・セキュリティ属性とは、最終的にはアクセス制御の決定を考慮してもよく、かつ、アクセス制御ポリシーの下でアクティブになっているエンティティと関連付けられている属性を指す。

依存性:なし。

保証アクティビティ:

評価チームは、TOE 内のサブジェクト・データの生成と活用がどれほど正確であるかについては、設計文書の評価を通して決定しなければならない(must)。次に評価チームは、目的とするサブジェクトにデータを適用することになる通常の TOE 機能を介してこの情報を生成しなければならない(must)。次に評価チームは、アクセス制御決定の際に適用されたこの属性データを使用するポリシーを書き込むために、ポリシー管理製品を使用しなければならない(must)。このポリシーがアクセス制御製品によって利用された時点で、評価チームは、予想される肯定的な結果と否定的な結果の両方について、定義されたオブジェクトに対して行われるサブジェクトによるアクションを試すべきである

(should)。

この追加のほかに、現在PPによって記述されている既存のSFRに対して、以下の要件追加を行うべきである(should)。
FMT_MSA.1は、オブジェクト属性のほかにサブジェクト・セキュリティ属性にも適用されると想定されていなければならない(must)。

C.2 タイムスタンプ

本プロテクションプロファイルは、タイムスタンプが運用環境により提供されるという前提で執筆されている。TOE が 1 つのアプライアンスとして実装されている場合には、タイムスタンプ機能は TOE から見て内部的であってもよい(may)。その場合には、次の SFR を組み込むべきである(SFR)。

C.2.1 FPT_STM.1 高信頼タイムスタンプ

下位階層:	なし。
FPT_STM.1.1	TSF は、それ自身の使用のために高信頼タイムスタンプを提供できなければならない(shall)。
依存性:	なし

保証アクティビティ:

評価チームは、TOE がクロックを初期化して起動する方法については、操作ガイダンスの評価を通して決定しなければならない(must)。次に評価チームは、その指示に従って、クロックを既知の値にセットし、信頼できる形でそのクロックが単調増分(monotomically increment)することを確認しなければならない(must)。評価チームは他の TOE 機能の実行を通して、タイムスタンプの値が適切に使用されていることを確認しなければならない(must)。

C.3 セッション管理に関するオプションの SFR

C.3.1 FTA_TSE.1 TOE セッションの確立

下位階層:	なし
FTA_TSE.1.1	TSF は、[***選択: 日付、時刻、[割付: 他の属性***] に基いてくセッションの確立を拒否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。この要件は、時刻、曜日又は地理的場所のように、認証資格情報が有効である状況を決定することで、TSF がホストの認証機能に対するアクセス制御を行うメカニズムを提供するために組み込まれている。*

適用上の注意: *この SFR が主張されている場合には、ST 作成者は、監査対象事象としてセッション確立の成功又は拒否を含めなければならない(must)。成功の監査はすべてのレベルの監査の操作中に無効化される可能性がある。*

保証アクティビティ:

評価者は TSS を検査して、セッションを拒否できる属性がいずれも明確に定義されていると判断しなければならない(shall)。評価者は操作ガイダンスを検査して、TSS 内で識別された各属性を設定するためのガイダンスがその中に盛り込まれていると判断しなければならない(shall)。評価者はこのほかに、各属性について以下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、TOE へのセッション確立に成功する。次に評価者は、操作ガイダンスに従って、当該アクセスがその属性の固有の値に基づいて拒否されるよう TOE を設定する。次に評価者は、属性のセッティングに違反したセッション(例えば、ある場所が時刻に基づいて拒否されるなど)の確立を試さなければならない(shall)。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)。*

C.3.2 FTA_SSL セッションのロック及び終了

C.3.2.1 FTA_SSL_EXT.1 TSF 起動セッション・ロック

下位階層: なし

FTA_SSL_EXT.1.1 TSF は、ローカルの対話セッションについて [選択:

- ○ セッションをロックする – 最新の内容を読込み不可にして、表示装置を消去するか上書きし、セッションのロックを解除せずに利用者のデータ・アクセス/表示装置に関するアクティビティを無効にし、その利用者に対してセッションのロック解除前に TSF に対する再認証を要求する:
- ○ セッションを終了する

] ことを認可された管理者が非活動時間を指定した後に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、以下のテストを実施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って、コンポーネント中で参照される無活動時間周期(inactivity time period)に、異なる値をいくつか設定する。設定した各周期に対して、評価者は TOE とのローカル対話セッションを確立する。次に評価者は、設定した時間周期の後でセッションがロックされるのか終了されるのかを確認する。コンポーネントから「ロック」を選択した場合、評価者はセッションのロックを解除しようとするときに再認証が必要になることを確認する。*

C.3.2.2 FTA_SSL.3 TSF 起動による終了

下位階層: なし

FTA_SSL.3.1 TSF は、許可された管理者が設定できる無活動セッションの時間間隔が過ぎてから、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、以下のテストを実施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って、コンポーネントで参照される無活動の時間間隔に対して、異なる値をいくつか設定する。これは少なくとも、操作ガイダンスで指定した最大許容値と最小許容値及び他の1 つの値で構成されなければならない (shall)。設定した各周期に対して、評価者は TOE とのリモート対話セッションを確立する。次に評価者は、設定した時間周期の後でセッションが終了されることを確認する。*

C.3.2.3 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、管理者起動による管理者自身の対話セッションの終了を許可し

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、以下のテストを実施しなければならない(shall)。

- *テスト1:評価者は、TOE とのローカル対話セッションを開始する。評価者は、操作ガイダンスに従って、セッションを終了するかログオフし、その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 とのリモート対話セッションを開始する。評価者は、操作ガイダンスに従って、セッションを終了するかログオフし、そのセッションが終了したことを確認する。*

C.4 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、それを奨励するために書かれている。TOE が、それ自体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には、次の要件も考慮に入れなければならない(must)。

適用できる要件

1. ST 作成者は、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(must)。
2. 評価チームは、ST 内のこの附属書に要件を主張しなければならない(must)。
3. 開発者は、この附属書の要件が適切に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、この附属書の中で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(must)。

この要件は、TOEがそれ自体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主張されるべきである(should)。これらの要件は、IPsec 仮想プライベート・ネットワーク(VPN)ゲートウェイのためのセキュリティ要件から採用されたものである。この機能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留意されたい。それ以外の国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 作成者によって使用されなければならない(shall)。

C.4.1 FCS_CKM.1 暗号鍵作成(非対称鍵用)

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(shall)。

[選択:

- 有限体ベース鍵確立スキーム(finite field-based key establishment scheme)については、NIST Special Publication 800-56A の「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」・ 楕円曲線ベース鍵確立スキーム(elliptic curve-based key establishment scheme)、及び「NIST curves」P-256、P-384、[選択: P-521、他の曲線なし] の実装については NIST SP 800－56A の「Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography」(FIPS PUB186-3「Digital Signature Standard」で定義)
- RSA ベース鍵確立スキーム(RSA-based key establishment scheme)については NIST Special Publication 800-56B の「Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography」

及び指定された暗号鍵サイズは、112 ビットの**セキュリティと同等又はそれ以上**であること。

適用上の注意: *このコンポーネントは、例えば IPsec のような TOE で使用される様々な暗号プロトコルに使用される公開/プライベート鍵のペアを生成するよう TOE に要求する。多数のスキームがサポートされている場合には、ST 作成者は、この機能を捕捉するために、この要件を繰り返し記述すべきである(should)。使用されるスキームは、ST*

作成者によって選択肢から選択されることになる。

使用することになるドメイン・パラメータは本 PP のプロトコルの要件で指定されているため、TOE がドメイン・パラメータを生成することは期待されていない。したがって、本 PP で指定したプロトコルに TOE が順守しているときは、ドメイン・パラメータの妥当性確認をさらに行う必要はない。

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又はそれ以上である必要がある。同等な鍵強度については、NIST SP800-57 の「Recommendation for Key Management(鍵管理に関する勧告)」を参照されたい。

依存性: [FCS_CKM.2 暗号鍵配付、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 作成者が実施する選択肢に応じて、「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)」の鍵ペアの生成に関する部分を使用しなければならない(shall)。 したがって評価者には、テスト段階での検証が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備えていることが要求される。

TSF の実装が、選択した内容に応じて 800-56A 及び 800-56B(又はこのうちのいずれか)に適合していることを示すために、評価者は、TSS に以下の情報が盛り込まれていることを確認しなければならない(shall)。

- *TSS は、TOE が準拠する 800-56 規格の該当するセクションをすべて記載しなければならない(shall)*
- *TSS に記載する各該当節で、「しなければならない(shall)」ではないすべての陳述(つまり、「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、もし TOE がこうしたオプションを実装するのなら、そのことを TSS の中で説明しなければならない(shall)。組み込まれた機能性が、規格の中で「しないものとする(shall not)」又は「すべきではない(should not)」で示される場合には、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についての根拠を提示しなければならない(shall)。

- *800－56A 及び 800－56B(選択に従う)の各該当節について、「しなければならない(shall)」又は「すべきである(should)」という陳述に関連する機能性の省略はいかなるものも説明されなければならない(shall)。*
- *TOE 固有の拡張、文書に記載されていない処理、又は TOE が実施することになっているセキュリティ要件に影響を与える可能性のある文書が許可した別の実装は説明されなければならない(shall)。*

C.4.2 FCS_CKM_EXT.4 暗号鍵のゼロ化

下位階層: なし

FCS_CKM_EXT.4.1 TSF は、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・パラメータがすべて不要になった場合には、それをすべてゼロ化しなければならない(shall)。

適用上の注意: *セキュリティに関連する情報(鍵、認証データ及びパスワードなど)は、セキュリティ上重要なデータの漏洩又は改変を防ぐために、使用の必要がなくなったときにはゼロ化しなければならない(must)。*

上記のゼロ化は、鍵/暗号クリティカル・セキュリティ・パラメータを他の場所に移動させる際に、平文の鍵/暗号クリティカル・セキュリティ・パラメータを格納する中間的なストレージ・エリア(すなわち、このようなデータのパスに含まれる、例えばメモリ・バッファのような記憶域)にそれぞれ適用される。

依存性: なし

保証アクティビティ:

評価者は、TTS をチェックして、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、及び鍵生成のために使用されるクリティカル・セキュリティ・パラメータのそれぞれについて、いつそれがゼロ化されるのか(例えば、使用後直ちに、システムのシャットダウン時など)、及び実行されるゼロ化処理の種別(ゼロで上書き、ランダムなパターンで 3 回上書きなど)が TSS で説明されていることを確認しなければならない(shall)。保護対象を保管するために各種のメモリを利用している場合、評価者は TSS をチェックして、データが格納されるメモリに関してゼロ化手順(例えば、flash に

格納された秘密鍵はゼロで 1 回上書きされるのに対し、内蔵ハード・ドライブに格納された秘密鍵は、各書き込み動作前に変更されるランダム・パターンを使って 3 回上書きされる)が TSS で説明されていることを確認しなければならない(shall)。

C.4.3 FCS_COP.1(1) 暗号操作(データの暗号化/復号用)

下位階層: なし

FCS_COP.1.1(1) **詳細化**:SF は、指定された暗号アルゴリズム [***[割付:1 つ以上のモード]での AES 操作]*** と、暗号鍵サイズ **128 ビット、256 ビット、**及び以下を満たす[選択: 192 ビット、鍵サイズは他になし] に従って、[***暗号化と復号***] を実行しなければならない。

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

適用上の注意: *割付について、ST 作成者は AES が操作するモードを 1 つ又は複数選択すべきである(should)。1 番目の選択について、ST 作成者は、この機能でサポートしている鍵を選択すべきである(should)。2 番目の選択に関して、ST 作成者は割付で指定されているモードについて説明する規格を選択すべきである(should)。*

依存性: [FDP_ITC.1 セキュリティ属性を持たない利用者データのインポート、又は
[FDP_ITC.2 セキュリティ属性を持つ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指針として「The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)」、「The XTS-AES Validation System (XTSVS)」「The CMAC Validation System (CMACVS)」、「The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)」及び「The Galois/Counter Mode (GCM) and GMAC Validation

System (GCMVS)」(いずれの文書も http://csrc.nist.gov/groups/STM/cavp/index.html から入手可能) から選択した上記の要件のモードに該当するテストを使用しなければならない(shall)。したがって評価者には、テスト段階での検証が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備えていることが要求される。

C.4.4 FCS_COP.1(2) 暗号操作(暗号署名用)

下位階層: なし

FCS_COP.1.1(2) 詳細化:TSF は、以下の各項目に従って暗号署名サービスを実施しなければならない(shall)。[選択:

(1) 2048 ビット以上の鍵サイズ(係数)のデジタル署名アルゴリズム(DSA)

(2) 2048 ビット以上の鍵サイズ(係数)の RSA デジタル署名アルゴリズム(rDSA)、

又は

(3) 256 ビット以上の鍵サイズの楕円曲線デジタル署名アルゴリズム(ECDSA)]

であって、以下に準拠するものとして、

デジタル署名アルゴリズム(DSA)の場合:

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

RSA デジタル署名アルゴリズム(rDSA)の場合:

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

楕円曲線デジタル署名アルゴリズム(ECDSA)の場合:

- ***FIPS PUB 186-3「Digital Signature Standard」、及び***
- ***TSF は、(FIPS PUB 186-3、「Digital Signature Standard」に定義されているとおり)「NIST curves」P-256、P-384、及び[選択:P-521、他の曲線なし]を実装しなければならない。***

適用上の注意: *暗号署名の推奨手法として、本 PP の将来のバージョンでは楕円曲線が必要となる予定である。*

適用上の注意: *ST 作成者は、デジタル署名を実行するように実装されるアルゴリズムを選択すべきである(should)。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、機能を特定するために繰り返し記述されるべきである(should)。選択したアルゴリズムについて、ST 作成者は、適切な割付/選択を行って、そのアルゴリズムに実装するパラメータを特定すべきである(should)。*

楕円曲線ベースのスキームでは、鍵サイズは、基点の位数の log_2 をとった値を意味する。暗号署名の推奨手法として、本 PP の将来のバージョンでは楕円曲線が要求されるであろう。

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

[FDP_ITC.2 セキュリティ属性を持つ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指針として「The FIPS 186-3 Digital Signature Algorithm Validation System (DSAVS)」、「The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)」、及び「The RSA Validation System (RSAVS)」の署名の生成と署名の検証に関する部分を使用しなければならない(shall)。したがって評価者には、テスト段階での検証が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備えていることが要求される。

C.4.5 FCS_COP.1(3) 暗号操作(暗号ハッシュ用)

下位階層: なし

FCS_COP.1.1(3) **詳細化**:TSF は、FIPS Pub 180-3***「Secure Hash Standard」***を満たす、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・サイズ [選択:160、256、384] ビットに従って、***暗号ハッシュサービス***を実行しなければならない(shall)。

適用上の注意: *本 PP のバージョンでは、TLS の使用が許可されるのは、後方互換性という理由があるときに限られる。次回のバージョンでは、SHA-1 の使用は完全に除外される可能性が高い。*

適用上の注意: *ハッシュ・アルゴリズムの選択肢は、メッセージ・ダイジェスト・サイズの選択肢に対応していなければならない(must)。例えば、SHA-1 を選択していれば、メッセージ・ダイジェスト・サイズで唯一有効な選択肢は 160 ビットになる。*

依存性: [FDP_ITC.1 セキュリティ属性を持たない利用者データのインポート、又は
[FDP_ITC.2 セキュリティ属性を持つ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指針として「The Secure Hash Algorithm Validation System (SHAVS)」を使用しなければならない(shall)。したがって評価者には、テスト段階での検証が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備えていることが要求される。

C.4.6 FCS_COP.1(4) 暗号操作(鍵付ハッシュ・メッセージ認証用)

下位階層: なし

FCS_COP.1.1(4) **詳細化**: TSF は、***FIPS Pub 198-1「The Keyed-Hash Message Authentication Code」*** と FIPS Pub 180-3 ***「Secure Hash Standard」*** を満たす、指定された暗号アルゴリズム HMAC-[選択: SHA-1、SHA-256、SHA-384]、鍵サイズ [**割当**: ***HMAC で使用される鍵サイズ(ビット単位)***]、及びメッセージ・ダイジェスト・サイズ [選択: 160、256、384] ビットに従って、***鍵付きハッシュ・メッセージ認証***を実行しなければならない(shall)。

適用上の注意: *本 PP のバージョンでは、TLS の使用が許可されるのは、後方互換性という理由があるときに限られる。次回のバージョンでは、SHA-1 の使用は完全に除外される可*

能性が高い。

適用上の注意: *ハッシュ・アルゴリズムの選択肢は、メッセージ・ダイジェスト・サイズの選択肢に対応していなければならない(must)。例えば、HMAC-SHA-256 を選択していれば、メッセージ・ダイジェスト・サイズで唯一有効な選択肢は 256 ビットになる。*

上記のメッセージ・ダイジェスト・サイズは、使用された基盤となる基本ハッシュ・アルゴリズムに対応する。ハッシュ・アルゴリズムの後で HMAC の出力データを切り捨てることは、様々なアプリケーションの適切な 1 つのステップであることに留意されたい。これによって、この要件との適合の妥当性を欠くことにはならないが、ST は、この切捨てが実施されたこと、最終出力サイズ、及びこの切捨てが準拠する規格について陳述すべきである(should)。

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

[FDP_ITC.2 セキュリティ属性を持つ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指針として「The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)」を使用しなければならない(shall)。したがって評価者には、テスト段階での検証が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備えていることが要求される。

C.4.7 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、[選択: 次から 1 つ選択: (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のノイズ源とソフトウェアベースのノイズ源の組み合わせ。] からエントロピーを集積するエントロピー源でシードした [選択、次から 1 つ選択: [選択: Hash_DRBG (任

意)、HMAC_DRBG (任意)、CTR_DRBG (AES)、Dual_EC_DRBG (任意)] を使用する NIST Special Publication 800-90; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] に従って、すべてのランダムビットの生成(RBG)サービスを実行しなければならない。

FCS_RBG_EXT.1.2 決定論的 RBG は、少なくともその鍵の最大ビット長に等しいエントロピーの少なくとも [選択、次から 1 つ選択: 128 ビット、256 ビット] でシードされなければならない(shall)。

適用上の注意: *NISTSP800-90 附属書 C は、FIPS-140 の将来のバージョンで要求される可能性のある最小限のエントロピー測定について説明している。可能であれば、直ちにこれを使用すべきであり、本 PP の将来のバージョンではこれが要求されるだろう。*

FCS_RBG_(EXT).1.1 の最初の節について、ST 作成者は、RBG サービスが適合する規格(800-90 及び 140-2 附属書 C のいずれか)を選択すべきである(should)。

SP800-90 には、乱数表を生成する 4 種類の方法が含まれている。この方法は基盤となる暗号プリミティブ(ハッシュ関数/暗号)に依存する。ST 作成者は、使用される関数を選択し(800-90 を選択した場合)、要件又は TSS の中で使用される特定の基盤となる暗号プリミティブを含める。Hash_DRBG 又は HMAC_DRBG に関しては、識別されたハッシュ関数(SHA-1、SHA-224、SHA-256、SHA-384、SHA-512)のいずれが許可されるが、CT_DRBG に関しては AES に基づく実装のみが許可される。Dual_EC_DRBG に関しては 800-90 で定義されたすべての曲線が許可されるが、ST 作成者は選択した曲線だけでなく使用されるハッシュ・アルゴリズムも含めなければならない(must)。

FIPS Pub 140-2 附属書 C については現在、「NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms」の第 3 節で説明した方法のみが有効であることに留意されたい。ここで使用される AES 実装の鍵長が、利用者データを暗号化するために使用するものと異なる場合、FCS_COP.1 は異なる鍵長を反映するように調節するか、繰返し記述することが必要になる可能性がある(may

have to)。FCS_RBG_EXT.1.2 における選択について、ST 作成者は RBG をシード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 作成者はこのほかに、TOE のベースライン要件に基本的な関数がすべて盛り込まれることも保証する。

将来的には、「A Method for Entropy Source Testing: Requirements and Test Suite Description」に記述されている要件の大部分が本 PP で要求されることになる。以下の保証アクティビティは、現在、要求されるアクティビティのサブセットのみ反映している。

依存性: なし

保証アクティビティ:

評価者は、TSS 節を見直して、TOE で使用される RBG(1 つ又は複数)を含んでいる製品のバージョン番号を確定しなければならない(shall)。評価者は、エントロピーを収集するハードウェアベースのノイズ源が TSS に記述されていることも確認しなければならない(shall)。さらに、評価者は、RBG で使用される基本的なすべての関数及びパラメータが TSS にリストされていることも検証する。

評価者は、エントロピー入力を取得する方法に加えて、使用されるエントロピー源の識別、各エントロピー源からどれだけのエントロピーが生成されるのかをはじめとする RBG モデルの記述が TSS に含まれていることを検証しなければならない(shall)。また、評価者は、エントロピー源故障の既知のモードについても TSSに記述されていることを確認しなければならない。最後に、評価者は、時間条件及び環境条件(又はこのうちのいずれか)による出力と分散の独立性の観点で RBG 出力の記述が TSS に含まれていることを確認しなければならない(shall)。RBG が適合を主張している基準に関係なく、評価者は以下のテストを実施しなければならない。

- *テスト1:評価者は、エントロピー源テスト一式を使用して、各エントロピー源についてエントロピーの推量を決定しなければならない(shall)。評価者は、すべてのエントロピー源から取得されたすべての結果の最小値であるエントロピー推定量が TSS に含まれることを確実にしなければならない(shall)。*

評価者は、RBG が適合する基準に従って、以下のテストも実施しなければならない(shall)。

FIPS 140-2 附属書 C に適合する実装

この節に含まれるテストについての参考文献は、「The Random Number Generator Validation System (RNGVS)」[RNGVS]である。評価者は、以下のテストを実施しなければならない(shall)。「期待値」は、正しいことが知られているアルゴリズムの参照実装により生成されることに留意されたい。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(Variable Seed Test)を実施しなければならない(shall)。評価者は、TSF RBG 関数に 128(シード、DT)ペアのセットをそれぞれ 128 ビットで提供しなければならない。また、評価者は、すべての 128(シード、DT)ペアに一定の(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)。DT の値は、セットごとに 1 ずつ増加される。シードの値は、セット内で反復してはならない。評価者は、TSF から返される値が期待値と一致していることを確認する。

評価者は、モンテカルロ・テスト(Monte Carlo Test)を実施しなければならない。(shall)。このテストでは、TSF RBG 関数に初期シードと DT の値をそれぞれ 128 ビットで提供する。また、評価者は、テストを通して一定の(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)。評価者は、DT の値を毎回 1 ずつ増加させ、「NIST -Recommended Random Number Generator Based on 「ANSI X9.31Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms」の第 3 節の指定に従って生成された後続の新しいシードを使用して、TSF RBG を 10000 回呼び出す。

NIST Special Publication 800-90 に適合する実装

評価者は、RNG 実装について 15 回試行しなければならない(shall)。もし RNG が設定可能であれば、評価者はそれぞれの設定について 15 回試行しなければならない(shall)。また、評価者は、RNG 機能を設定するための適切な指示が操作ガイダンスに含まれていることも確認しなければならない(shall)。

もし RNG の予測耐性が有効化されて(have prediction resistance enabled)いれば、それぞれの試行は (1) drbg のインスタンス化、(2) ランダムビットの 1 番目のブロックの生成、(3) ランダムビットの 2 番目のブロックの生成、(4) アンインスタンス化(終了処理、内部状態のゼロ化)(uninstantiate)から成る。評価者は、ランダムビットの 2 番目のブロックが期待値であることを検証する。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、生成の初回呼び出しのための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 回目の呼び出しのための追加入力とエントロピー入力である。この値はランダムに生成される。「ランダムビットの 1 ブロックを生成する」とは、返されるビット長が(NIST SP 800-90 で定義された)出力ブロック長と等しくなる

ランダムビットを生成するという意味である。

もしRNGが予測耐性を備えていなければ、それぞれの試行は（1）drbgのインスタンス化、(2) ランダムビットの1番目のブロックの生成、(3) ランダムビットの 2 番目のブロックの生成、(4) アンインスタンス化（終了処理、内部状態のゼロ化）から成る。評価者は、ランダムビットの 2 番目のブロックが期待値であることを検証する。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のための追加入力である。6番目と7番目は、初期化の呼び出しのための追加入力とエントロピー入力である。最後の値は、生成の2回目の呼び出しのための追加入力である。

以下に、評価者が生成及び選択すべき（又はこのうちのいずれか）入力値のいくつかに関して詳しい情報を示す。

***エントロピー入力（Entropy input）**：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（Nonce）**：ナンスがサポートされている（df なしの CTR_DRBG がナンスを使用しない）場合、ナンス・ビット長はシード長の半分である。*

***個別化文字列（Personalization string）**：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）。もし実装が 1 つの個別化文字列のみサポートするなら、両方の値について同じ長さが利用可能である。もし複数の文字列の長さをサポートするなら、評価者は 2 つの異なる長さの個別文字列を使用しなければならない。実装が個別文字列を使用しない場合は、値を提供する必要はない。*

***追加入力**：追加入力のビット長は、個別化文字列長と同じデフォルト値及び制約条件を持つ。*

附属書 D – 文書の表記法

本 PP の中で使用される表記法、書式及び表記規則は、英国式綴りを米国式綴りに置換すること以外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。本 PP の読者に役立つよう、ここでは選定された記述の選択肢について説明する。

D.1 操作

CC は、機能要件に基づいて実行されるべき機能コンポーネントの操作として、割付、詳細化、選択、及び繰返しの 4 つを許可している。本 PP では、この 4 つの操作を以下の方法で強調する。

- **割付**: 識別されたパラメータの仕様を許可する。ST 作成者によってさらに操作が必要な場合には、「割付」というプロンプトが含まれた角括弧内に***太字でイタリック体***の文字で示される。
- **詳細化**: 詳細情報の追加を許可する。イタリック体の文字で示される。
- **選択**: リストから 1 つ以上のエレメントの仕様を許可する。「選択」というプロンプトが含まれている角括弧内のアンダーライン付きの文字で示される。
- **繰返し**: 様々な操作と共にコンポーネントが 2 度以上使用されることを許可する。SFR のエレメント番号の後ろの括弧内に連番で示される。

CC パート 2 から採用された要件については、***太字でイタリック体***の文字は、この要件が 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箇所を示している。

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には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(must)、要件を明瞭に表現するときには 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(are required)。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

適用上の注意には、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があるか有用であると考えられる追加的な補足情報が盛り込まれている。適用上の注意にはこのほかに、コンポーネントについて許可されている操作に関連する助言も盛り込まれている。

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の共通評価方法として役立つ。このアクティビティには、評価者が TSS で文書化されている TOE の特定の側面を分析するための指示が含まれているため、この情報を TSS の節に盛り込むよう ST 作成者に対して暗に要求している。将来のバージョンはこの要件を別の附属書又は文書に移動させる可能性があるが、PP のこのバージョンでは、保証アクティビティは、機能及び保証コンポーネントに直接関連付けられている。

附属書 E – 用語集

表 16 用語と定義

用語	定義
アクセス制御（Access Control）	明確なサブジェクトからリクエストされ、かつ、明確なオブジェクトに対して実行されるべき明確な操作の実行を許可又は拒否するために導入された仕組み。又は、明確なサブジェクトからリクエストされ、かつ、この仕組みを採用することで達成される結果に対して実行されるべき明確な操作の実行を許可又は拒否するために導入された仕組み。
属性ベースのアクセス制御（Attribute-Based Access Control） Attribute-Based Access Control）	利用者の権利ではなく利用者の属性に基づくアクセス制御の手段。一例として、同じ利用者でもその人物が技術者であれば特定の資源へのアクセスが許可されるが、請負人であればアクセスが拒否されるシステムを挙げることができる。
許可された管理者（Authorized Administrator）	コモンクライテリアのSFRでは固有の用語を採用していることから使用される管理者と同義の用語。
利用する（Consume）	ポリシーを受信して構文解析し、アクセス制御を実施する際に使用できるような形で保管するアクセス制御製品の行為。
任意アクセス制御（DAC：Discretionary Access Control）	それらの識別又はグループのメンバーシップによって、サブジェクトに対して出された権限に基づくアクセス制御の手段。
エンタープライズ・セキュリティ管理	セキュリティ管理に関する管理策を指示、生成、普及、改変、停止及び終了するために必要とされるシステム及び人材。
識別情報及びクレデンシャル情報管理製品（Identity and Credential Management Product）	ESM配置内の識別情報及びクレデンシャル情報を識別及び認証を目的として保管・管理するための主要機能が搭載されているESM製品。
強制アクセス制御（MAC：Mandatory Access Control）	企業内のあらゆるサブジェクト及びオブジェクトは、1つ以上の階層的ラベルに関連付けら得ているという考え方に基づくアクセス制御の手段。こ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。

用語	定義
運用環境（Operational Environment）	TOEの境界内に存在していない企業内のハードウェア及びソフトウェア資源の集合。TOEが操作を要求するサードパーティ製のソフトウェア・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などがこの中に含まれる。
ポリシー（Policy）	アクセス制御SFPのインスタンス化の方法を決定する規則の集合。この規則は、明確なオブジェクトに対して明確な操作を実行することを明確なサブジェクトに許可する条件を定義する。
ポリシー管理者（Policy Administrator）	本PPの文脈では、これは、TOE使用してポリシーの生成と配付を担う1人以上の個人を意味する。
ポリシー実施点（Policy Enforcement Point）	ある企業における関連するあらゆるふるまいへのアクセス制御SFPの適用を担うエンタープライズ・セキュリティ管理のコンポーネントの1つ。本PPで言及しているアクセス制御製品と同義。
ポリシー管理製品（Policy Management product）	ポリシー実施点により使用されるポリシーの生成を担うアプリケーション。このポリシーは、自動化された仕組みを使用するか、管理者が手作業で入力するか、あるいはこの2つを組み合わせた何らかの方法により作成される。これが本PPで定義されているTOEである。
役割ベースのアクセス制御（Role-Based Access Control）	割り当てられる役割及びその役割に関連付けられている権限に基づいて、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（Secure Configuration Management）	ESMコンポーネントの設定及び運用環境内にあるシステムのプロビジョニングを行う（provision）能力（又はこのうちのいずれか）を変更する機能を搭載した製品。
TOE管理者（TOE Administrator）	本PPの文脈では、この用語は、TOEのセットアップ、TOEが利用するポリシーを定義する際のポリシー管理製品の使用、及びTOEが生成する監査データの検証を担当する1人以上の個人を意味する。
利用者（User）	TOEの一般利用者の総称。ポリシー管理製品から識別され認証されている任意のエンティティ。

附属書 F – 識別

タイトル:エンタープライズ・セキュリティ管理ポリシー管理　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・コミュニティの承認を受けた代表として)

コモンクライテリア識別技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、2009 年 7 月

バージョン: PP バージョン 1.4

キーワード:エンタープライズ・セキュリティ、エンタープライズ・セキュリティ管理、ポリシー管理、セキュリティ管理

評価保証レベル(EAL):EAL 1 要件追加