U.S. Government Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness

Version 1.68

中位の頑強性が要求される環境下のマルチレベルOS用

米国政府プロテクション・プロファイル 1.68版

第5章セキュリティ機能要件 翻訳 0.9版

2006年8月24日
日本セキュリティ・マネージメント学会
セキュアOS研究会　WG2

5. Security Functional Requirements

5. セキュリティ機能要件

This section contains detailed security functional requirements for the operating systems' trusted security functions (TSF) supporting single-level systems in medium robustness environments. The requirements are applied against the operating system in conjunction with the underlying hardware that supports it. The requirements contained in this section are either selected from Part2 of the CC or have been explicitly stated (with short names in bold and ending in "_EXP"). Table 5.1 lists the explicit functional requirements in this section.

本章では、中位信頼性を求める環境でシングルレベルシステムをサポートする、オペレーティングシステムのTOEセキュリティ機能（TSF）向けの、詳細なセキュリティ機能要件を述べる。これらの要件は、要件をサポートするハードウェアと併せて、オペレーティングシステムに適用される。本章で述べられる要件は、CCのPart2から抜粋されたものか、明示的に（太字の_EXPで終わる短い名称で）示されたものである。表5.1は、本章における明示的な機能要件のリストである。

The cryptographic module plays an important role in the enforcement of the TOE security policies. For this reason, the cryptographic related requirements contain more detail than other requirements, in terms of refinements, iterations, and explicitly stated requirements. Refer to section 1.3 to see the notation and formatting used in this profile.

暗号モジュールは、TOEのセキュリティ方針を施行する中で重要な役割を果たす。そのため、暗号に関する要件については、詳細化や繰返しという表現で、そして明示的に述べられる要件で、他の要件より詳細な情報を含んでいる。このプロファイルで用いられる表記法や表記形式は、1.3章を参照すること。

Table 5.1 - Explicit Functional Requirements

Explicit Component	Component Behavior Name
FCS_BCM_EXP.1	Baseline Cryptographic Module
FCS_CKM_EXP.1	Key Validation and Packaging
FCS_CKM_EXP.2	Cryptographic Key Handling and Storage
FCS_COA_EXP.1	Cryptographic Operations Availability
FCS_COP_EXP.1	Random Number Generation
FDP_IFF_EXP.2(1)	Hierarchical Security Attributes (for Mandatory Access Control)
FDP_IFF_EXP.2(2)	Hierarchical Security Attributes (for Mandatory Integrity Control)
FPT_TRC_EXP.1 Internal	TSF Data Consistency
FPT_TST_EXP.1	TSF Testing
FTP_TRP_EXP.1	Trusted Path

表 5.1 – 明示的な機能要件

明示的コンポーネント	コンポーネントビヘイビア名
FCS_BCM_EXP.1	基本暗号モジュール
FCS_CKM_EXP.1	鍵の検証と梱包
FCS_CKM_EXP.2	暗号鍵の取り扱いと保管
FCS_COA_EXP.1	暗号処理の利便性
FCS_COP_EXP.1	乱数生成
FDP_IFF_EXP.2(1)	階層的セキュリティ属性 (for Mandatory Access Control)
FDP_IFF_EXP.2(2)	階層的セキュリティ属性 (for Mandatory Integrity Control)
FPT_TRC_EXP.1 Internal	TSF のデータ一貫性
FPT_TST_EXP.1	TSF のテスト
FTP_TRP_EXP.1	高信頼パス

5.1 Security Audit (FAU)

5.1 セキュリティ監査（FAU）

5.1.1 Security Audit Automatic Response (FAU_ARP)

5.1.1 セキュリティ監査自動応答（FAU_ARP）

5.1.1.1 Security Alarms (FAU_ARP.1)

5.1.1.1 セキュリティアラーム

FAU_ARP.1.1 **Refinement:** Upon detection of a potential security violation, the TSF shall **generate a warning message to the authorized administrator that requires explicit acknowledgement by the administrator**.1

FAU_ARP.1.1 詳細化:セキュリティ侵害の可能性が検出された場合、TSFは、許可管理者に向けて、管理者による明示的な確認を求める警告メッセージを生成しなくてはならない。

Application Note: "Potential security violation" is an activity that, if continued unchecked, would lead to a security violation (e.g. repeated failed authentication attempts).

適用上の注釈："セキュリティ侵害の可能性"とは、もし放置され続けた場合、セキュリティ侵害につながる行為である。（例えば、連続的な認証試行の失敗）

5.1.2 Security Audit Data Generation (FAU_GEN)

5.1.2 セキュリティ監査データ生成(FAU_GEN)

5.1.2.1 Audit Data Generation (FAU_GEN.1)

5.1.2.1 **監査データ生成**（FAU_GEN.1）
FAU_GEN.1.1 **Refinement:** The TSF shall be able to generate an audit record of the following auditable events: FAU_GEN.1.1
詳細化：TSFは下記の監査可能な事象に対して、監査記録を生成できなければならない。

a) Start-up and shutdown of the audit functions;
a) **監査機能の開始と停止；**
b) Start-up and shutdown of the TOE;
b) TOE**の開始と停止；**
c) Uses of special permissions that circumvent the access control policies;
c) **アクセス制御ポリシーを回避する特別な許可の使用；**

Application Note: These special permissions are typically those often used by authorized administrators.

適用上の注釈： 特別許可は権限を与えられた管理者によってしばしば使われる許可である。

d) All auditable events **listed in Table 5.2**; **and**
d) **表**5.2**に掲載されている全ての監査可能事象；および**
e) All other security relevant auditable events for the minimal level of audit.
e) **監査の最小のレベル対する他の全てのセキュリティ関連監査可能事象。**

Application Note: For other security relevant functions that are not included in this PP, the ST author defines a minimal level of audit.

適用上の注釈：このPPに含まれていない他のセキュリティ関連機能については、STの著者が監査の最小レベルを定義する。

Table 5.2 - Auditable Events[11]

Requirement	**Audit events prompted by requirement**
Security Alarms (FAU_ARP.1)	• Actions taken to address potential security violations.
Audit Data Generation (FAU_GEN.1)	(none)
User Identity Association (FAU_GEN.2)	(none)
Potential Violation Analysis (FAU_SAA.1)	• Enabling and disabling of any of the analysis mechanisms. • Automated responses provided by the security audit analysis mechanism.
Audit Review (FAU_SAR.1)	• Opening the audit records.
Restricted Audit Review (FAU_SAR.2)	• Unsuccessful attempts to read information from the audit records.
Selectable Audit Review (FAU_SAR.3)	(none)
Selective Audit (FAU_SEL.1)	• All modifications to the audit configuration that occur while the audit collection functions are operating.

Protected Audit Trail Storage (FAU_STG.1)	(none)
Prevention of Audit Data Loss (FAU_STG.4)	• Actions taken due to the audit storage failure.
Explicit: Baseline Cryptographic Module (FCS_BCM_EXP.1)	(none)
Cryptographic Key Generation (for symmetric keys) (FCS_CKM.1(1))	• Failure of the symmetric key generation process12. • The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1(2))	• Failure of the asymmetric key generation process9. • The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
Cryptographic Key Distribution (FCS_CKM.2)	• Failure to properly complete the key distribution process9. • The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
Cryptographic Key Destruction (FCS_CKM.4)	• Failure of the key zeroization process9. • The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
Explicit: Cryptographic Key Validation and Packaging (FCS_CKM_EXP.1)	• Failure of a key validation technique9. • The object attribute(s), and object value(s) excluding any sensitive information (e.g. keys).
Explicit: Cryptographic Key Handling and Storage (FCS_CKM_EXP.2)	• Failure in key handling or storage9. • The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).
Cryptographic Operations Availability (FCS_COA_EXP.1)	(none)
Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))	• Failure in encryption or decryption9. • Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information.
Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))	• Failure in cryptographic signature9. • Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information.
Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))	• Failure in hashing function9. • Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information.
Cryptographic Operation (for cryptographic key agreement) (FCS_COP.1(4))	• Failure in cryptographic key exchange9. • Any applicable cryptographic mode(s) of operation, subject attributes and object attributes, excluding any sensitive information.
Explicit: Random Number Generation (FCS_COP_EXP.1)	• Failure in the randomization process9.

Complete Access Control (FDP_ACC.2)	(none)
Security Attribute Based Access Control (FDP_ACF.1)	• All requests to perform an operation on an object covered by the SFP.
Export of User Data With Security Attributes (FDP_ETC.2)	• All attempts to export information.
Complete Information flow control (for Mandatory Access Control Policy) (FDP_IFC.2(1))	(none)
Complete Information flow control (for Mandatory Integrity Control Policy) (FDP_IFC.2(2))	(none)
Hierarchical Security Attributes (for Mandatory Access Control) (FDP_IFF_EXP.2(1))	• All decisions on requests for information flow.
Hierarchical Security Attributes (for Mandatory Integrity Control) (FDP_IFF_EXP.2(2))	• All decisions on requests for information flow.
Limited Illicit information Flows (FDP_IFF.3)	• All decisions on requests for information flow. • The use of identified illicit information flow channels.
Import of User Data Without Security Attributes (FDP_ITC.1)	• All attempts to import user data.
Import of User Data With Security Attributes (FDP_ITC.2)	• All attempts to import user data, including any security attributes.
Full Residual Information Protection (FDP_RIP.2)	(none)
Authentication Failure Handling (FIA_AFL.1)	• The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
User Attribute Definition (FIA_ATD.1)	(none)
Verification of Secrets (FIA_SOS.1)	• Rejection or acceptance by the TSF of any tested secret.
Timing of Authentication (FIA_UAU.1)	• All use of the authentication mechanism.
Re-authenticating (FIA_UAU.6)	• All re-authentication attempts.
Protected Authentication Feedback (FIA_UAU.7)	(none)
Timing of Identification (FIA_UID.1)	• All use of the user identification mechanism, including the user identity provided.

User-Subject Binding (FIA_USB.1)	• Success and failure of binding of user security attributes to a subject (e.g. success and failure to create of a subject).
Management of Security Functions Behavior (for specification of auditable events) (FMT_MOF.1(1))	• All modifications in the behavior of the functions in the TSF.
Management of Security Functions Behavior (for authentication data) (FMT_MOF.1(2))	• All modifications in the behavior of the functions in the TSF.
Management of Security Attributes (for Discretionary Access Control) (FMT_MSA.1(1))	• All modifications of the values of security attributes.
Management of Security Attributes (for Mandatory Access Control) (FMT_MSA.1(2))	• All modifications of the values of security attributes.
Management of Security Attributes (for Mandatory Integrity Control) (FMT_MSA.1(3))	• All modifications of the values of security attributes.
Secure Security Attributes (FMT_MSA.2)	• All offered and rejected values for a security attribute.
Static Attributes Initialization (FMT_MSA.3)	• Modifications of the default setting of permissive or restrictive rules. • All modifications of the initial values of security attributes.
Management of TSF Data (for general TSF data) (FMT_MTD.1(1))	• All modifications of the values of TSF data.
Management of TSF Data (for audit data) (FMT_MTD.1(2))	• All modifications of the values of audit data.
Management of TSF Data (for previously written audit records) (FMT_MTD.1(3))	(none)
Management of TSF Data (for initialization of user security attributes) (FMT_MTD.1(4))	• All initializations of the values of user security attributes.
Management of TSF Data (for modification of user security attributes, other than authentication data) (FMT_MTD.1(5))	• All modifications of the values of user security attributes.
Management of TSF Data (for modification of authentication data) (FMT_MTD.1(6))	• All actions associated with modifications of the values of authentication data.

Management of TSF Data (for reading of authentication data) (FMT_MTD.1(7))	(none)
Management of TSF Data (for critical cryptographic security parameters) (FMT_MTD.1(8))	• All actions associated with modifications of the values of critical cryptographic security parameters.
Revocation (to authorized administrators) (FMT_REV.1(1))	• All attempts to revoke security attributes.
Revocation (to owners and authorized administrators) (FMT_REV.1(2))	• All attempts to revoke security attributes.
Time-Limited Authorization (FMT_SAE.1)	• Specification of the expiration time for an attribute. • Action taken due to attribute expiration.
Security Roles (FMT_SMR.2)	• Modifications to the group of users that are part of a role.
Assuming Roles (FMT_SMR.3)	• Explicit requests to assume a role. • Use of any function restricted to an authorized administrator role (identified in FMT_SMR.2).
Abstract Machine Testing (FPT_AMT.1)	• Execution of the tests of the underlying machine and the results of the tests.
Basic Internal TSF Data Transfer Protection (FPT_ITT.1)	(none)
TSF Data Integrity Monitoring (FPT_ITT.3)	• Detection of modification of TSF data.
Manual Recovery (FPT_RCV.1)	• The fact that a failure or service discontinuity occurred. • Resumption of the regular operation. • Type of failure or service discontinuity
Replay Detection (FPT_RPL.1)	• Detected replay
Non-Bypassability of the TSF (FPT_RVM.1)	(none)
SFP Domain Separation (FPT_SEP.2)	(none)
Reliable Time Stamps (FPT_STM.1)	• Changes to the time.
Internal TSF Data Consistency (FPT_TRC_EXP.1)	• Any detection of inconsistency between TSF data.
TSF Testing (FPT_TST_EXP.1)	• Execution of the TSF self tests and the results of the tests.
TSF Testing (for cryptography) (FPT_TST.1(1))	• Execution of the cryptography self tests and the results of the tests.

TSF Testing (for key generation components) (FPT_TST.1(2))	• Execution of the key generation component self tests and the results of the tests.
Maximum Quotas (for persistent storage) (FRU_RSA.1(1))	• Rejection of allocation operation due to persistent storage limits.
Maximum Quotas (for system memory) (FRU_RSA.1(2))	• Rejection of allocation operation due to percentage of system memory limits.
Maximum Quotas (for processing time) (FRU_RSA.1(3))	• Rejection of allocation operation due to processing time limits.
Limitation on scope of selectable attributes (FTA_LSA.1)	• All attempts at selecting a session security attribute.
Basic limitation on multiple concurrent sessions (FTA_MCS.1)	• Rejection of a new session based on the limitation of multiple concurrent sessions.
TSF-Initiated Session Locking (FTA_SSL.1)	• Locking of an interactive session by the session locking mechanism. • Any attempts at unlocking of an interactive session.
User-Initiated Locking (FTA_SSL.2)	• Locking of an interactive session by the session locking mechanism. • Any attempts at unlocking of an interactive session.
Default TOE Access Banners (FTA_TAB.1)	(none)
TOE Access History (FTA_TAH.1)	(none)
TOE Session Establishment (FTA_TSE.1)	• All attempts at establishment of a user session.
Trusted Path (FTP_TRP_EXP.1)	• All attempted uses of the trusted path functions. • Identification of the user associated with all trusted path failures, if available.

表 5.2 - 監査可能な事象[11]

要件	**要件によって引起される監査事象**
セキュリティ警報(FAU_ARP.1)	• **潜在的なセキュリティ違反を指すために採られる行動.**
監査データ生成(FAU_GEN.1)	(**なし**)
ユーザ識別子の結合 (FAU_GEN.2)	(**なし**)
潜在的違反分析(FAU_SAA.1)	• **分析メカニズムの任意のものの操作および操作停止** • **セキュリティ監査分析メカニズムによって提供される自動応答**
監査再検討 (FAU_SAR.1)	• **監査記録を開く**

制限された監査再検討 (FAU_SAR.2)	• 監査記録から情報を読む不成功の試み
選択可能な監査再検討 (FAU_SAR.3)	(なし)
選択的監査(FAU_SEL.1)	• 監査収集機能の操作中に起きる監査構成への全ての変更。
保護された監査証跡記憶 (FAU_STG.1)	(なし)
監査データ損失の防止 (FAU_STG.4)	• 監査記憶故障のために採られる行動
明示的要件：基礎暗号モジュール (FCS_BCM_EXP.1)	(なし)
暗号鍵生成（対称鍵について） (FCS_CKM.1(1))	• 対称鍵生成処理の失敗[12] • 客体属性、および機微な情報（例えば秘密鍵または個人鍵）を除く客体の値
暗号鍵生成(非対称鍵について) (FCS_CKM.1(2))	• 非対称鍵生成処理の失敗[9] • 客体属性、および機微な情報（例えば秘密鍵または個人鍵）を除く客体の値
暗号鍵配布(FCS_CKM.2)	• 鍵配布処理を適切に完了しなかったこと[9] • 客体属性、および機微な情報（例えば秘密鍵または個人鍵）を除く客体の値
暗号鍵破壊(FCS_CKM.4)	• 鍵のゼロ化処理の失敗[9] • 客体属性、および機微な情報（例えば秘密鍵または個人鍵）を除く客体の値
明示的要件：暗号鍵確認と梱包 (FCS_CKM_EXP.1)	• 鍵確認技法の失敗[9] • 客体属性、および機微な情報（例えば秘密鍵または個人鍵）を除く客体の値
明示的要件：暗号鍵取り扱いと記憶(FCS_CKM_EXP.2)	• 鍵取り扱いまたは記憶の失敗 • 客体属性、および機微な情報（例えば秘密鍵または個人鍵）を除く客体の値
暗号操作の可用性 (FCS_COA_EXP.1)	(なし)
暗号操作（データ暗号化／復号のための）(FCS_COP.1(1))	• 暗号化または復号の失敗[9] • 適用可能な暗号操作モード、主体の属性および客体の属性、機微な情報を除く
暗号操作(暗号的署名のための)	• 暗号的署名の失敗[9]

(FCS_COP.1(2))	• 適用可能な暗号操作モード、主体の属性および客体の属性、機微な情報を除く
暗号操作（暗号的ハッシュのための）(FCS_COP.1(3))	• ハッシュ機能の失敗[9] • 適用可能な暗号操作モード、主体の属性および客体の属性、機微な情報を除く
暗号操作（暗号的鍵共有のための）(FCS_COP.1(4))	• 暗号的鍵共有の失敗[9] • 適用可能な暗号操作モード、主体の属性および客体の属性、機微な情報を除く
明示的要件：乱数生成 (FCS_COP_EXP.1)	• ランダム化処理の失敗[9]
完全アクセス制御(FDP_ACC.2)	(なし)
セキュリティ属性に基づくアクセス制御 (FDP_ACF.1)	• SFPによってカバーされる客体に操作を行う全ての要求
セキュリティ属性を持つユーザデータのエクスポート (FDP_ETC.2)	• 情報をエクスポートしようとする全ての試み
完全情報フロー制御（強制アクセス制御ポリシーに対する） (FDP_IFC.2(1))	(なし)
完全情報フロー制御（強制完全性制御ポリシーに対する） (FDP_IFC.2(2))	(なし)
階層的セキュリティ属性（強制アクセス制御に対する） (FDP_IFF_EXP.2(1))	• 情報フローに対する要求についての全ての決定
階層的セキュリティ属性（強制完全性制御に対する） (FDP_IFF_EXP.2(2))	• 情報フローに対する要求についての全ての決定
限定された不正情報フロー (FDP_IFF.3)	• 情報フローに対する要求についての全ての決定 • 識別された不正情報フローチャネルの使用
セキュリティ属性のないユーザデータのインポート (FDP_ITC.1)	• ユーザデータをインポートしようとする全ての試み
Import of User Data With Security Attributesセキュリティ属性付ユーザデータのインポート (FDP_ITC.2)	• セキュリティ属性を含むユーザデータをインポートしようとする全ての試み

全ての残留情報の保護 (FDP_RIP.2)	**(なし)**
認証失敗処理(FIA_AFL.1)	**• 不成功認証の試みに対する閾値の到達と取られた行動（例えば、端末の非活性化）および適切であれば、それに続く正常状態への回復（例えば、端末利用の再活性化）**
ユーザ属性定義(FIA_ATD.1)	**(なし)**
秘密の検証(FIA_SOS.1)	**• テストされた秘密のTSFによる拒絶または受容**
認証の時刻(FIA_UAU.1)	**• 認証メカニズムの全ての使用**
再認証(FIA_UAU.6)	**• 全ての再認証の試み**
保護された認証フィードバック (FIA_UAU.7)	**(なし)**
本人確認の時刻(FIA_UID.1)	**• ユーザ本人確認メカニズムの全ての使用、提供されたユーザ識別情報を含む**
ユーザ主体結合(FIA_USB.1)	**• ユーザセキュリティ属性の主体への結合の成功と失敗（例えば、主体について作り出すことの成功および失敗）**
セキュリティ機能の振舞いの管理（監査可能事象の仕様に対する）(FMT_MOF.1(1))	**• TSFにおける機能の振舞いの全ての変更**
セキュリティ機能の振舞いの管理（認証データに対する） (FMT_MOF.1(2))	**• TSFにおける機能の振舞いの全ての変更**
セキュリティ機能の振舞いの管理（任意アクセス制御に対する） (FMT_MSA.1(1))	**• セキュリティ属性の値の全ての変更**
セキュリティ属性の管理（強制アクセス制御に対する） (FMT_MSA.1(2))	**• セキュリティ属性の値の全ての変更**
セキュリティ属性の管理（強制完全性制御に対する） (FMT_MSA.1(3))	**• セキュリティ属性の値の全ての変更**
セキュアなセキュリティ属性 (FMT_MSA.2)	**• セキュリティ属性に対する全ての提供されたおよび拒絶された値**
静的属性初期化(FMT_MSA.3)	**• 許可または制限規則 のデフォルト設定の変更** **• セキュリティ属性の初期値の全ての変更**

TSFデータの管理（一般TSFデータに対する）(FMT_MTD.1(1))	• TSFデータの値の全ての変更
TSFデータの管理（監査データに対する）(FMT_MTD.1(2))	• 監査データの値の全ての変更
TSFデータの管理（以前に書かれた監査記録に対する）(FMT_MTD.1(3))	(なし)
TSFデータの管理（ユーザセキュリティ属性の初期化に対する）(FMT_MTD.1(4))	• ユーザセキュリティ属性の値の全ての初期化
TSFデータの管理（認証データ以外のユーザセキュリティ属性の変更に対する）(FMT_MTD.1(5))	• ユーザセキュリティ属性の値の全ての変更
TSFデータの管理（認証データの変更に対する）(FMT_MTD.1(6))	• 認証データの値の変更に関係する全ての行動
TSFデータの管理（認証データの読み取りに対する）(FMT_MTD.1(7))	(なし)
TSFデータの管理（重要な暗号セキュリティパラメータに対する） (FMT_MTD.1(8))	• 重要な暗号セキュリティパラメータの値の変更に関連する全ての行動
無効化（権限を与えられた管理者への） (FMT_REV.1(1))	• セキュリティ属性を無効にする全ての試み
無効化（所有者および権限を与えられた管理者への）(FMT_REV.1(2))	• セキュリティ属性を無効にする全ての試み
時限認証(FMT_SAE.1)	• 属性に対する有効期限の指定 • 有効期限切れによって取られた行動
セキュリティ規則 (FMT_SMR.2)	• 役割に参加しているユーザのグループの変更
役割の引き受け (FMT_SMR.3)	• 役割を引き受ける明示的な要求 •権限を与えられた管理者の役割に限定された機能の使用（FMT_SMR.2に確認されている）
抽象マシンデスト(FPT_AMT.1)	• 下位のマシンのテストの実行とテストの結果

基礎的内部TSFデータ転送保護 (FPT_ITT.1)	(なし)
TSFデータ完全性監視 (FPT_ITT.3)	• TSFデータの変更の検知
手作業による回復(FPT_RCV.1)	• 故障またはサービス中断が起きた事実 • 正規の操作の再開 • 故障またはサービス中断のタイプ
リプレイ検出(FPT_RPL.1)	• 検出されたリプレイ
TSFのバイパス不能性 (FPT_RVM.1)	(なし)
SFP領域隔離(FPT_SEP.2)	(なし)
信頼できるタイムスタンプ (FPT_STM.1)	• 時刻への変更
内部TSFデータ一貫性 (FPT_TRC_EXP.1)	• TSFデータの間のくい違いの検出
TSFテスト (FPT_TST_EXP.1)	• TSF自己テストの実行とテストの結果
TSFテスト（暗号に対する） (FPT_TST.1(1))	• 暗号自己テストの実行とテストの結果
TSFテスト（鍵生成部品に対する） (FPT_TST.1(2))	• 鍵生成部品自己テストの実行とテストの結果
最大割り当て（永続性記憶に対する）(FRU_RSA.1(1))	• 永続性記憶限度によるアロケーション操作の拒絶
最大割り当て（システム記憶に対する） (FRU_RSA.1(2))	• システム記憶のパーセンテージ限度によるアロケーション操作の拒絶
最大割り当て（処理時間に対する） (FRU_RSA.1(3))	• 処理時間限度によるアロケーション操作の拒絶
選択可能な属性の範囲についての限度 (FTA_LSA.1)	• セッションセキュリティ属性を選択するときの全ての試み
多重同時操作セッションについての基本的限度(FTA_MCS.1)	• 多重同時操作セッションについての限度に基づく新しいセッションの拒否
TSFによって開始されたセッションのロック(FTA_SSL.1)	• セッションロックメカニズムによるインタラクティブセッションのロック. • インタラクティブセッションのロックを外す試み
ユーザによって開始されたロッ	• セッションロックメカニズムによるインタラクティブセッショ

ク(FTA_SSL.2)	ンのロック. • インタラクティブセッションのロックを外す試み
デフォルトのTOEアクセスバナー(FTA_TAB.1)	(なし)
TOEアクセス履歴(FTA_TAH.1)	(なし)
TOEセッション確立 (FTA_TSE.1)	• ユーザセッションの確立の全ての試み
トラステッドパス (FTP_TRP_EXP.1)	• トラステッドパス機能の全ての試みられた使用 • 入手可能な場合には、全てのトラステッドパスの失敗に関連するユーザの識別

[11] Not all listed events must be captured in separate audit records but the capability must exist to query the audit data based on any individual event.

[11]掲載されている全ての事象が監査記録に捕捉されなければならなくはないが、個々の事象に基づく監査データを質問する能力は存在しなければならない。

[12] Typically, upon detection of a crypto-related failure, a system indication should be generated, and the system should transition to a known safe (secure) state. The generation of an audit log can provide a mechanism for capturing more information about a failed event. The exact content of the crypto-related audit log is implementation-dependent. However, the log should include information that could help pinpoint the part of the crypto-related process that failed, but without compromising the value of any critical cryptographic security parameters. In addition, the audit record requirements specified in FAU_GEN.1.2 should be considered and included where appropriate. As a simple example, detection of a key checkword error during an internal transfer of key might be implemented as follows: Generate a “Bad Key” error message to the system, prevent use of the bad key and zeroize it, and generate an audit record that includes the date of the event, the time of the event, “key checkword error”, bad key ID tag or subject/user associated with the bad key, and “failed key transfer during internal handling”.

[12] 典型的に暗号関連の失敗を検知したときに、システム表示が生成されるべきであり、システムは分かった安全な（セキュアな）状態に移行すべきである。監査ログの生成は、失敗事象についてのより多くの情報を捕捉するためのメカニズムを提供することができる。暗号関連の監査ログの正確な内容は、実装依存である。しかし、ログは、失敗した暗号関連処理の部分をピンポイントするのに役立つ情報を含むべきであるが、重要な暗号セキュリティパラメータのいかなる値も暴露してはならない。更に、FAU_GEN.1.2に指定された監査記録要件は考慮され、適切な場合には含まれるべきである。簡単な例として、鍵の内部転送の間の鍵チェックワード誤りの検出は、次のように実装され得る：システムへの「Bad Key」誤りメッセージを生成し、誤りのある鍵の使用を防止し、それをゼロ化する、そして事象の日付、事象の時刻、「鍵チェックワード誤り」、誤りのある鍵のIDタグまたは誤りのある鍵に関連する主体／ユーザ、および「内部処理中の鍵転送失敗」を含む監査記録を生成する。

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

FAU_GEN.1.2 TSFは、監査記録の中に、少なくとも次の情報を記録しなければならない：

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

a) 事象の日付と時刻、事象のタイプ、主体の識別、および事象の結果（成功または失敗）、および

Application Note: "Subject identity" means user identity associated with the subject.

適用上の注釈：「主体の識別」は主体に関連するユーザの識別を意味する。

Application Note: For alarms, type of event refers to the cause of what triggered the alarm (not merely the fact that an alarm was triggered).

適用上の注釈：警報については、事象のタイプはその警報を起こした原因を意味する（単に、警報が起こされたという事実だけでなく）

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST,

• the name, sensitivity label, and integrity label of the object;

• the sensitivity label and integrity label of the subject;

• for changes to TSF data (except for authentication data and critical cryptographic security parameters), the new and old values of the data;

• for authentication attempts, the origin of the attempt (e.g., terminal identifier);

• for assuming a role, the type of role, and the location of the request;

b) 各監査事象タイプについては、PP/STに含まれる機能コンポーネントの監査可能定義に基づいて

- 客体の名前、機密ラベル、および完全性ラベル；
- 主体の機密ラベルおよび完全性ラベル；
- TSFデータ（認証データおよび重要な暗号セキュリティパラメータについてを除く）への変更については、データの新しい値と旧い値；
- 認証の試みについては、試みの発信元（例えば、端末識別子）；
- 役割の引き受けについては、役割のタイプ、および要求の場所；

Application Note: TSF data includes access control attributes, user security attributes, definition of roles, and user authorizations.

適用上の注釈：TSFデータは、アクセス制御属性、ユーザセキュリティ属性、役割の定義、およびユーザの権限付与を含む。

Application Note: Other audit relevant information associated with security-relevant functions not included in this PP should be included within the audit records.

適用上の注釈：このPPに含まれていないセキュリティ関連機能に関する他の監査関連情報は、監査記録の中に含まれなければならない。

5.1.2.2 User Identity Association (FAU_GEN.2)

5.1.2.2 **ユーザ識別情報結合(FAU_GEN.2)**

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_GEN.2.1 TSF**は、監査可能事象をその事象の原因となったユーザの識別情報に結び付けることができなければならない。**

Application Note: For failed login attempts no user association is required because the user is not under TSF control until after a successful identification/authentication.

適用上の注釈： ユーザは識別／認証が成功した後にならないとTSF**の管理下にないので、失敗したログインの試みについては、ユーザ結合は必要ない。**

5.1.3 Security Audit Analysis (FAU_SAA)

5.1.3 **セキュリティ監査分析**(FAU_SAA)

5.1.3.1 Potential Violation Analysis (FAU_SAA.1)

5.1.3.1 潜在的侵害分析(FAU_SAA.1)

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.
FAU_SAA.1.1 TSF**は、監査事象の監視において規則セットを適用可能でなければならず、かつこれらの規則にもとづいて**TSP**の潜在的侵害を示さなければならない。**

FAU_SAA.1.2 **Refinement:** The TSF shall **monitor the** accumulation or combination of **the following events** known to indicate a potential security violation:2
FAU_SAA.1.2 **詳細化：**TSF**は潜在的セキュリティ侵害を示すことで知らされる次の事象の累積もしくは組合せを監視しなければならない。**

a) an administrator specified number of user authentication failures within an administrator specified time period,
a) **管理者が指定した時間内で、ユーザ認証失敗回数を特定した、**

b) an administrator specified number of Discretionary Access Control policy violation attempts by an individual user within an administrator specified time period,
b) **管理者が指定した時間内で個々のユーザによる任意アクセス制御ポリシー侵害の攻撃の回数を特定した、**

c) any failure of the cryptographic self-tests,
c) **あらゆる暗号自己ストの失敗、**

d) any failure of the TSF self-tests,

d) あらゆるTSF自己テストの失敗、

e) *[assignment:* additional events from the set *of defined auditable events].*
e) [割付：定義済みの監査可能事象セットからの追加事象]。

5.1.4 Security Audit Review (FAU_SAR)
5.1.4 セキュリティ監査レビュー(FAU_SAR)

5.1.4.1 Audit Review (FAU_SAR.1)
5.1.4.1 監査レビュー (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **authorized administrators** with the capability to read **all audit information** from the audit records.
FAU_SAR.1.1 TSFは、認可された管理者が監査記録からすべての監査情報を読み取ることを可能にしなければならない。

Application Note: For a distributed system, the authorized administrator should be able to read all audit information within the TOE.
運用上の注釈：分散システムでは、認可された管理者は、TOE内のすべての監査情報を読み取とれるようにしなければならない。

FAU_SAR.1.2 **Refinement:** The TSF shall provide the audit records in a manner suitable for the **authorized administrator** to interpret the information **using a tool to access the audit records**.3
FAU_SAR.1.2 詳細化：TSFは、監査記録へのアクセスツールを使って情報を解釈するために、認可された管理者に対して適切な方法で監査記録を提供しなければならない。3

Application Note: The tool provides a means to easily and efficiently review the audit records. It is expected (yet not necessary) that the tool satisfying this requirement will also satisfy the FAU_SAR.3 and FAU_SEL.1 requirements.
適用上の注釈：このツールは、監査記録を容易かつ十分にレビューするための手段を提供する。この要件を満たすツールは、FAU_SAR.3およびFAU_SEL.1の要件も満たすことが期待される（だが必須ではない）。

5.1.4.2 Restricted Audit Review (FAU_SAR.2)
5.1.4.2 限定監査レビュー (FAU_SAR.2)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.
FAU_SAR.2.1 TSFは、明示的にリードアクセスが許可されているユーザを除いて、すべてのユーザに監査記録へのリードアクセスを禁止しなければならない。

5.1.4.3 Selectable Audit Review (FAU_SAR.3)
5.1.4.3 選択可能監査レビュー (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data based on **the following attributes:**
FAU_SAR.3.1 TSFは、**次の属性に基づく監査データの検索と分類の実行能力を提供しなければならない**。

a) user identity,
a) **ユーザ識別、**

b) object identity,
b) **オブジェクト識別、**

c) date of the event,
c) **事象の日付、**

d) time of the event,
d) **事象の時刻、**

e) type of event,
e) **事象の種別、**

f) subject sensitivity label,
f) **サブジェクト機密ラベル、**

g) object sensitivity label,
g) **オブジェクト機密ラベル、**

h) subject integrity label,
h) **サブジェクト完全性ラベル、**

i) object integrity label,
i) **オブジェクト完全性ラベル、**

j) success of auditable security events, and
j) **監査可能セキュリティ事象の成功、および**

k) failure of auditable security events.
k) **監査可能セキュリティ事象の失敗。**

5.1.5 Security Audit Event Selection (FAU_SEL)
5.1.5 **セキュリティ監査事象選択**(FAU_SEL)

5.1.5.1 Selective Audit (FAU_SEL.1)
5.1.5.1 **選択的監査** (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
FAU_SEL.1.1 TSFは、次の属性に基づく監査事象のセットから、監査可能事象を含めたり含めなかったりできなければならない。

a) object identity、
a) オブジェクト識別、

b) user identity、
b) ユーザ識別、

c) host identity、
c) ホスト識別、

d) event type、
d) 事象種別、

e) subject sensitivity label;
e) **サブジェクト機密ラベル**;

f) object sensitivity label;
f) **オブジェクト機密ラベル**;

g) subject integrity label;
g) **サブジェクト完全性ラベル**;

h) object integrity label
h) **オブジェクト完全性ラベル**

i) success of auditable security events, and
i) **監査可能セキュリティ事象の成功、および**

j) failure of auditable security events.
j) **監査可能セキュリティ事象の失敗**。

5.1.6 Security Audit Event Storage (FAU_STG)
5.1.6 **セキュリティ監査事象格納**(FAU_STG)

5.1.6.1 Protected Audit Trail Storage (FAU_STG.1)
5.1.6.1 **保護された監査事象格納** (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.1 TSFは、許可されない消去から、格納された監査記録を保護しなければならない。

FAU_STG.1.2 The TSF shall be able to prevent modifications to the audit records.
FAU_STG.1.2 TSFは、監査記録の変更を防ぐことができ来なければならない。

Application Note: In order to reduce the performance impact of audit generation, audit records are often temporarily buffered in memory before being written to the disk. In such implementations, these buffered records will be lost if the operation of the TOE is interrupted by hardware or power failures. The developer should document the expected loss in such circumstances and show that it has been minimized.
適用上の注釈：監査生成による性能への影響を低減するために、監査記録はディスクに書き込まれる前に、頻繁にメモリに一時記憶される。こうした実装では、ハードウェアもしくは電源障害によってTOEのオペレーションが中断された場合、これら一時記憶された記録は失われるであろう。開発者は、こうした環境における期待損失を文書化して、それが最小限に抑えられていることを示すべきである。

5.1.6.2 Prevention of Audit Data Loss (FAU_STG.4)
5.1.6.2 監査データの消失防止(FAU_STG.4)

FAU_STG.4.1 **Refinement: When the audit trail becomes full,** the TSF shall **provide the authorized administrator the capability to** prevent auditable events, except those taken by the authorized **administrator (in the context of performing TOE maintenance)** and **generate an alarm to the authorized administrator**.4
FAU_STG.4.1 詳細化：監査証跡が満杯になったときには、TSFは認可された管理者に対し，認可された管理者によって得られる（TOEの保守との関連で）以外の監査可能事象を抑制する機能、および認可された管理者に警告を発する機能を提供しなければならない。4

5.2 Cryptographic Support (FCS)[13]
5.2 暗号サポート(FCS)13

5.2.1 Explicit: Baseline Cryptographic Module (FCS_BCM_EXP)
5.2.1 明示的: 基本暗号モジュール(FCS_BCM_EXP)

5.2.1.1 Explicit: Baseline Cryptographic Module (FCS_BCM_EXP.1)
5.2.1.1 明示的：基本暗号モジュール (FCS_BCM_EXP.1)

FCS_BCM_EXP.1.1 All cryptographic modules shall comply with FIPS PUB 140-2 when performing FIPS-approved cryptographic functions in FIPS approved cryptographic modes of operation.
FCS_BCM_EXP.1.1 すべての暗号モジュールは、FIPS認可の暗号オペレーションモードでFIPS認可の暗号機能を実行する場合には、FIPS PUB140-2に準拠しなければならない。

13 In drafting specific requirements for this section for general-purpose operating systems, experts were consulted and their input was incorporated. The result is a very minimal set of crypto-related requirements chosen to be consistent with the other requirements of this CC-based protection profile. These crypto

requirements are expected to be achievable in commercial products in the near term, and to gradually mature over time. Evolving public standards on cryptographic functions and related areas have required the following interim approach to writing these cryptographic requirements for general purpose operating systems. This approach uses a variety of footnotes and application notes in an attempt to fill gaps, forewarn of future plans, and/or qualify interpretation of the existing referenced standards (sometimes specific draft versions). As a result, in many instances the presentation of the crypto requirements here is more cumbersome than desired. Still, today these requirements represent a step in the direction of helping to improve the security in COTS products. Over time the approach and presentation will be expanded upon and refined. Correspondingly, the PP will be updated as the underlying public standards and the body of related special publications mature.
13 汎用 OS に関する本セクションへの特定要件の草稿段階で、専門家の相談に預かり、そのアドバイスが盛り込まれた。その結果が正に、この CC ベースのプロテクションプロファイルの他の要件と一致するように選択された暗号関連の要件の最小セットである。これらの暗号要件は、近々のうちに商用製品として完成され、やがて徐々に成熟していくものと期待される。暗号機能とその関連分野についての進化する公的標準は、汎用 OS に対するこれらの暗号要件を記述するため，次のような暫定的なアプローチを必要とする。このアプローチは、ギャップを埋めようとして、将来計画について予め警告しようとして、および／あるいは既存の参照基準（場合によっては特定の草稿バージョン）の解釈を修正しようとして、種々の脚注や適用上の注釈を利用する。結果として多くの場合、暗号要件のここでのプレゼンテーションは、望んだよりも厄介なものになる。なお、今日これらの要件提示は、COTS 製品におけるセキュリティ改善の支援に向けての一歩となる。このアプローチやプレゼンテーションは、やがて発展し洗練されるであろう。相応して、PP も基盤をなす公的標準として、また完成した関連の専門出版物の本文として最新のものに更新されるであろう。

FCS_BCM_EXP.1.2 Cryptographic functions and cryptographic modes of operation as identified in this PP shall be NSA-validated.
FCS_BCM_EXP.1.2 このPPにおいて識別される暗号機能および暗号モードオペレーションは、NSAに承認されていなければならない。

Application Note: In time, OS PP cryptographic requirements are expected to evolve such that NSA-validated cryptographic modules shall only contain cryptographic functions, cryptographic modes of operation, and other types of cryptographic processing that are compliant with this protection profile.
適用上の注釈：OSのPP暗号要件は、やがてNSA承認の暗号モジュールが、このプロテクションプロファイルに準拠した暗号機能、暗号モードオペレーションおよび他の形式の暗号処理を包含することのみ義務付けられるようになるまで進化することが期待される。

FCS_BCM_EXP.1.3 All cryptographic modules implemented in the TSF ***[selection:***
FCS_BCM_EXP.1.3 TSFに実装されるすべての暗号モジュール ***[選択:***

(1) Entirely in hardware shall have a minimum overall rating of FIPS PUB 140-2, Level 3;
(1) もっぱらハードウェア内部においては、FIPS PUB 140-2、 Level 3の最小総合評価を得なければならない；

(2) Entirely in software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2,Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles, Services and authentication; Cryptographic

Key Management; Design Assurance; and FIPS PUB 140-2,Level 4 Self Tests [14] ***as defined by this Protection Profile;***

(2) もっぱらソフトウェアの内部においては、以下に対して、FIPS PUB 140-2、Level 1の最小総合評価を得るとともに、FIPS PUB 140-2、Level 3もまた満たさなければならない：
暗号モジュールおよびインターフェース；役割、サービスおよび認証；暗号科学技術管理；設計上の保証;およびこのプロテクションプロファイルで定義されるようなFIPS PUB 140-2、レベル4 自己テスト 14 ;

(3) As a combination of hardware and software shall have a minimum overall rating of FIPS PUB 140-2, Level 1 and also meet FIPS PUB 140-2, Level 3 for the following: Cryptographic Module Ports and Interfaces; Roles,Services and Authentication; Cryptographic Key Management; Design Assurance; and FIPS PUB 140-2，Level 4 Self Tests[15] ***as defined by this Protection Profile.]***

(3) ハードウェアとソフトウェアの組み合わせとしては、FIPS PUB 140-2のレベル 1の最小総合評価を得なければならないと同時に、以下に対してFIPS PUB 140-2のレベル 3も満たさなければならない。：
暗号モジュールポートおよびインターフェース；役割；サービスと認証；暗号鍵管理；設計上の保証;およこのプロテククションプロファイルで定義されるようなFIPS PUB 140-2のレベル4自己テスト 15

Application Note: "Combination of hardware and software" means that some part of the cryptographic functionality will be implemented as a software component of the TSF. The combination of a cryptographic hardware module and a software device driver whose sole purpose is to communicate with the hardware module is considered a hardware module rather than a "combination of hardware and software".
適用上の注釈：" ハードウェアとソフトウェアの組み合わせ "は、暗号機能の一部がTSFのソフトウェア部品として実装されることを意味する。ハードウェアと単に通信することだけを目的とする暗号ハードウェアモジュールとソフトウェアデバイスドライバの組み合わせは、ハードウェアとソフトウェアの組み合わせというよりはむしろハードウェアモジュールと考えられる。

14 Security Level 4 Self Tests comprise the Security Level 1 Self Tests in FIPS PUB 140-2 and the Statistical RNG Tests in Appendix C of this protection profile. These Statistical RNG Tests are the same as those included in the 25 May 2001 version of FIPS PUB 140-2.
14 セキュリティレベル 4 の自己テストは、FIPS PUB 140-2におけるセキュリティレベル 1 の自己テストおよびこのプロテクションプロファイルの附録Cにある統計的RNGテストを包含する。これらのRNGテストは、2001年5月25日版 FIPS PUB 140-2.に含まれるものと同じである。

15 See previous footnote.
15 前掲脚注を見よ

16 This requirement applies strictly to **generation** of symmetric keys. **Validation** techniques for generated symmetric keys are discussed in FCS_CKM_EXP.1.1.
16 この要件は対称鍵の生成に厳密に適用する。生成された対称鍵の検証技術は、FCS_CKM_EXP.1.1において論じられる。

5.2.2 Cryptographic Key Management (FCS_CKM)

5.2.2 暗号鍵管理 (FCS_CKM)

5.2.2.1 Cryptographic Key Generation (for symmetric keys) (FCS_CKM.1(1))

5.2.2.1 暗号鍵生成 (対称鍵) (FCS_CKM.1(1))

FCS_CKM.1.1(1) **Refinement:** The TSF shall generate[16] **symmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm **as follows:** 5 ***[selection:***

FCS_CKM.1.1(1) 詳細化: TSF は、以下の[選択: 以下のリスト] 指定された暗号鍵生成アルゴリズムに従って、対称暗号鍵を生成 16 しなければならない。

(1) a hardware random number generator (RNG) as specified in FCS_COP_EXP.1, but with a NIST-approved hashing function required for mixing, and/or

(1) FCS_COP_EXP.1 で指定されたハードウェア乱数生成器 (RNG) であって混合用に要求される NIST 承認のハッシュ関数を備えるもの、及び/または

(2) a software RNG as specified in FCS_COP_EXP.1, and/or

(2) FCS_COP_EXP.1 に指定されたソフトウェア RNG、及び/または

(3) a key establishment scheme as specified in FCS_COP.1(4) based upon public key cryptography using a software RNG as specified in FCS_COP_EXP.1, and/or a hardware RNG as specified in FCS_COP_EXP.1, but with a NIST-approved hashing function required for mixing].

(3) FCS_COP_EXP.1 に指定されたソフトウェア RNG、及び/または FCS_COP_EXP.1 で指定されたハードウェア RNG であって混合用に要求される NIST 承認のハッシュ関数を備えるものに基づく FCS_COP.1(4)で指定された鍵確立スキーム。

that meets the following:

上記は、以下を満たす:

a) All cases: (i.e., any of the above)

a) 全ての場合: (すなわち、上記のいずれの場合も)

- **FIPS PUB 180-2, Secure Hash Algorithm;**
- FIPS PUB 180-2、セキュアハッシュアルゴリズム;

b) Case: Finite field-based key establishment schemes

b) 有限体ベース鍵確立スキームの場合:

- **ANSI X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography;** [17]
- ANSI X9.42-2001、金融サービス産業向け公開鍵暗号: 離散対数暗号を用いた対称鍵交換;17

Application Note: For example, "Classic" Diffie-Hellman-based schemes

適用上の注釈: 例えば、「典型的な」ディフィー-ヘルマンベースのスキーム

c) Case: RSA-based key establishment schemes (with odd e)

c) RSA ベースの鍵確立スキーム (奇数 e) の場合:

▪ **ANSI X9.31-1998 (May 1998), Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) for generation of the RSA;**[18] **and**

▪ ANSI X9.31-1998 (1998/5)、RSA18 の生成のための金融サービス産業向け双方向 (reversible) 公開鍵を用いたデジタル署名 (rDSA) ; 及び

Application Note: Although ANSI X9.31 is a standard intended for digital signatures, it is being used here for its coverage of the generation of RSA parameters since ANSI X9.44 is still under development. Once ANSI X9.44 is approved it will be referenced here.

適用上の注釈: ANSI X.9.31 は署名用の標準であるが、ここでは、RSA パラメタ生成を含むものであるために使用している。ANSI X9.44 が開発中であるが、これが承認されれば、この部分に反映される。

d) Case: Elliptic curve-based key establishment schemes

d) 楕円曲線ベースの鍵確立スキームの場合:

▪ **ANSI X9.63-200x (1 Oct 2000), Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography.** [19]

▪ ANSI X9.63-200x (2000/10/1) 、金融サービス産業向け公開鍵暗号: 楕円曲線暗号 19 を用いた鍵交換及び鍵転送。

5.2.2.2 Cryptographic Key Generation (for asymmetric keys) (FCS_CKM.1(2))

5.2.2.2 暗号鍵生成 (非対称鍵) (FCS_CKM.1(2))

FCS_CKM.1.1(2) **Refinement:** The TSF shall generate[20] **asymmetric**[21] cryptographic keys in accordance with a **domain parameter generator** and ***[selection:***

FCS_CKM.1.1(2) 詳細化: TSF は、ドメインパラメタ生成器及び以下の[選択: 以下のリスト] に従って非対称 21 暗号鍵を生成 20 しなければならない。

(1) a random number generator and/or

(1) 乱数生成器及び/または

(2) a prime number generator].

(2) 素数生成器。

that meet the following: 6

上記は、以下を満たす: 6

a) Generated key strength shall be equivalent to, or greater than, a symmetric key

strength of 128 bits using conservative estimates;

a) 生成された鍵長は、控えめに見積もっても、128 ビットの対称鍵強度と同等かそれ以上でなければならない;

b) ANSI X9.80 (3 January 2000), Prime Number Generation, Primality Testing, and Primality Certificates using random integers with deterministic tests, or constructive generation methods;

b) ANSI X9.80 (2000/1/3) 、素数生成、素数テスト、及び決定論的テストによるランダムな整数、あるいは構成的生成方法を用いた素数性の証明

c) Case: For domain parameters used in finite field-based key establishment schemes

c) 有限体ベースの鍵確立スキームで用いられるドメインパラメタに対する場合:

▪ **ANSI X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography;** [22]

▪ ANSI X9.42-2001、金融サービス産業向け公開鍵暗号: 離散対数暗号を用いた対称鍵交換; 22

Application Note: For example, "Classic" Diffie-Hellman-based schemes

適用上の注釈: 例えば、「典型的な」ディフィー-ヘルマンベースのスキーム

d) Case: For domain parameters used in RSA-based key establishment schemes (with odd e)

d) RSA ベースの鍵確立スキーム (奇数 e) で用いられるドメインパラメタに対する場合:

▪ **ANSI X9.31-1998 (May 1998), Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) for the generation of the RSA parameters**[23]**; and**

▪ ANSI X9.31-1998 (1998/5)、RSA パラメタ 23 の生成のための金融サービス産業向け双方向 (reversible) 公開鍵を用いたデジタル署名 (rDSA) ; 及び

Application Note: Although ANSI X9.31 is a standard intended for digital signatures, it is being used here for its coverage of the generation of RSA parameters since ANSI X9.44 is still under development. Once ANSI X9.44 is approved it will be referenced here.

適用上の注釈: ANSI X.9.31 は署名用の標準であるが、ここでは、RSA パラメタ生成を含むものであるために使用している。ANSI X9.44 が開発中であるが、これが承認されれば、この部分に反映される。

e) Case: For domain parameters used in elliptic curve-based key establishment schemes

e) 楕円曲線鍵確立スキームで用いられるドメインパラメタに対する場合:

▪ **ANSI X9.63-200x (1 Oct 2000), Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography.**[24]

▪ ANSI X9.63-200x (2000/10/1) 、金融サービス産業向け公開鍵暗号: 楕円曲線暗号 24 を用いた鍵交換及び鍵転送。

5.2.2.3 Cryptographic Key Distribution[25] (FCS_CKM.2)

5.2.2.3 暗号鍵配付 25 (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method ***[selection: Manual (Physical) Method, Automated (Electronic) Method, Manual Method and Automated Method]*** that meets the following:

FCS_CKM.2.1 TSF は、以下に合致する、指定された暗号鍵配付方法[選択: 手動 (物理的) 方法、自動 (電子的) 方法、手動方法及び自動方法] に従って、暗号鍵を配付しなければならない:

a) Manual (Physical) Methods:

a) 手動 (物理的) 方法:

• The TSF shall support manual distribution of symmetric key in accordance with FIPS PUB 171 (Key Management Using ANSI X9.17).[26]

・TSF は、FIPS PUB 171 (ANSI X9.17 を用いた鍵管理) に従った対称鍵の手動配付をサポートしなければならない。26

• The TSF shall support manual distribution of private asymmetric key material (certificates and/or keys) in accordance with NSA-certified DOD PKI for public key distribution using NSA-approved certificate schemes[27] **with hardware tokens for protection of private keys that meet the following:**

・ TSF は、以下を満たす秘密鍵の保護のためのハードウェアトークンを持つ NSA 承認の証明書スキーム 27 を使った NSA 認証の DOD PKI に従った秘密非対称鍵データ (証明書及び/または鍵) の手動配付をサポートしなければならない:

1) PKI Roadmap for the DoD,

1) DoD のための PKI ロードマップ、

2) DoD X.509 Certificate Policy,

2) DoD X.509 証明書ポリシー、

3) PKCS #8 v1.2 (Private-Key Information Syntax Standard),

3) PKCS #8 v1.2 (秘密鍵情報シンタックス標準)、

4) PKCS #12 v1.0 (Personal Information Exchange Syntax),

4) PKCS #12 v1.0 (個人情報交換シンタックス)

5) PKCS #5 v2.0 (Password-Based Encryption Standard, 25 Mar 1999 - Final), and

5) PKCS #5 v2.0 (パスワードベース暗号化標準、1999/3/25 最終版)、及び

6) PKCS #11 v2.11 (Cryptographic Token Interface Standard).

6) PKCS #11 v2.11 (暗号トークンインタフェース標準) 。

• The TSF shall support manual distribution of public asymmetric key material (certificates and/or keys) in accordance with NSA-certified DOD PKI for public key

distribution using NSA-approved certificate schemes[28] for protection of public keys that meet the following:

・TSF は、以下を満たす公開鍵の保護のために、NSA 承認の証明書スキーム 28 を使った公開鍵配付のための NSA 認証の DOD PKI に従った公開非対称鍵データ (証明書及び/または鍵) 手動配付をサポートしなければならない。

1. PKI Roadmap for the DoD,

1. DoD のための PKI ロードマップ、

2. DoD X.509 Certificate Policy,

2. DoD X.509 証明書ポリシー、

3. PKCS#12 v1.0 (Personal Information Exchange Syntax),

3. PKCS #12 v1.0 (個人情報交換シンタックス)

b) Automated (Electronic) Methods:

b) 自動 (電子的) 方法:

• The TSF shall automatically distribute symmetric keys in accordance with FIPS PUB 171 (Key Management Using ANSI X9.17).[29].

・TSF は、FIPS PUB 171 (ANSI X9.17 を用いた鍵管理) に従った対称鍵の自動配付をサポートしなければならない。29

• The TSF shall automatically distribute public asymmetric key material (certificates and/or keys) in accordance with NSA-certified DoD PKI for public key distribution using NSA-approved certificate schemes[30] that meet the following:

・TSF は、以下を満たす NSA 承認の証明書スキーム 30 を使った公開鍵配付のための NSA 認証の DoD PKI に従った公開非対称鍵データ (証明書及び/または鍵) を自動的に配付しなければならない:

1. PKI Roadmap for the DoD,

1. DoD のための PKI ロードマップ、

2. DoD X.509 Certificate Policy,

2. DoD X.509 証明書ポリシー、

3. PKCS#12 v1.0 (Personal Information Exchange Syntax),

3. PKCS #12 v1.0 (個人情報交換シンタックス)

• The TSF shall only support manual distribution of private asymmetric key material (certificates and/or keys) in accordance with NSA-certified DOD PKI for public key distribution using NSA-approved certificate schemes[31] with hardware tokens for protection of private keys that meet the following:

・ TSF は、以下を満たす秘密鍵の保護のためのハードウェアトークンを持つ NSA 承認の証明書スキーム 31 を使った公開鍵配付のための NSA 認証の DOD PKI に従った秘密非対称鍵デー

タ (証明書及び/または鍵) の手動配付だけをサポートしなければならない。

1) PKI Roadmap for the DoD,

1) DoD のための PKI ロードマップ、

2) DoD X.509 Certificate Policy,

2) DoD X.509 証明書ポリシー、

3) PKCS #8 v1.2 (Private-Key Information Syntax Standard)

3) PKCS #8 v1.2 (秘密鍵情報シンタックス標準)、

4) PKCS #12 v1.0 (Personal Information Exchange Syntax Standard)

4) PKCS #12 v1.0 (個人情報交換シンタックス)

5) PKCS #5 v2.0 (Password-Based Encryption Standard, 25 Mar 99--Final) and,

5) PKCS #5 V2.0 (パスワードベース暗号化標準、1999/3/25 最終版)、及び

6) PKCS #11 v2.11 (Cryptographic Token Interface Standard).

6) PKCS #11 v2.11 (暗号トークンインタフェース標準) 。

5.2.2.4 Cryptographic Key Destruction (FCS_CKM.4)

5.2.2.4 暗号鍵破棄 (FCS_CKM.4)

FCS_CKM.4.1 **Refinement:** The TSF shall destroy cryptographic keys in accordance with a **cryptographic key zeroization method** that meets the following:7

FCS_CKM.4.1 詳細化: TSF は、以下に合致する暗号鍵ゼロ化方法に従って、暗号鍵を破棄しなければならない。

a) FIPS PUB 140-2;

a) FIPS PUB 140-2;

b) Zeroization of all plaintext cryptographic keys and all other critical cryptographic security parameters shall be immediate and complete; and

b) すべての平文の暗号鍵と他のすべての機密上重要な暗号セキュリティパラメタのゼロ化が迅速かつ完全になされねばならない; 及び

c) For embedded cryptographic modules, the zeroization shall be executed by overwriting the key/critical cryptographic security parameter storage area three or more times using a different alternating data pattern each time.

c) 埋め込まれた暗号モジュールに対し、鍵/機密上重要な暗号セキュリティパラメタの格納領域は、3 回以上の上書きによってゼロ化されねばならず、その際、各回ごとに異なる交互データパターンが使用されねばならない。

Application Note: Although verification of this zeroization of a plaintext key/critical cryptographic security parameter is desired here (by checking for the final known alternating data pattern), it is not required at this time. However, vendors are highly encouraged to incorporate this verification whenever possible into their

implementations.

適用上の注釈: 平文の鍵/重要な暗号セキュリティパラメタのゼロ化の検証 (最後に得られる既知の交互データパターンをチェックする) が本来望ましいのであるが、ここでは、そこまで要求しない。しかしながら、ベンダは、この要件の実装において、可能な限り検証機能を組み込むことが強く望まれる。

Application Note: Zeroization of any storage, such as memory buffers, that is included in the path of a plaintext key/critical cryptographic security parameter is addressed in FCS_CKM_EXP.2 (Cryptographic Key Handling and Storage).

適用上の注釈: 平文の暗号/重要な暗号セキュリティパラメタのパスに含まれるあらゆる格納領域のゼロ化 (メモリバッファなど) は、FCS_CKM_EXP.2 (暗号鍵の扱いと格納) で対応される。

5.2.2.5 Explicit: Cryptographic Key Validation and Packaging (FCS_CKM_EXP.1)

5.2.2.5 **明示的要件: 暗号鍵確認とパッケージ化** (FCS_CKM.EXP.1)

FCS_CKM_EXP.1.1: The TSF shall apply validation techniques (e.g., parity bits or checkwords) to generated **symmetric** keys in accordance with:

FCS_CKM_EXP.1.1: TSF **は、以下に従って、生成された対称鍵に対する確認技術 (例えば、パリティビットやチェックワード) を適用しなくてはならない**:

a) FIPS PUB 46-3 (Data Encryption Standard (DES)), and

a) FIPS PUB 46-3 (**データ暗号標準** (DES))**、及び**

b) FIPS PUB 171[32] (Key Management Using ANSI X9.17).

b) FIPS PUB 17132 (ANSI X9.17 **を用いた鍵管理**)

FCS_CKM_EXP.1.2: The TSF shall apply validation techniques to generated **asymmetric** keys in accordance with the standards corresponding to the generation technique as called out in FCS_CKM.1.1(2).

FCS_CKM_EXP.1.2: TSF **は、**FCS_CKM.1.1(2)**で呼び出される生成技術に対応する標準に従って生成された非対称鍵に対する確認技術を適用しなければならない。**

FCS_CKM_EXP.1.3: Any public key certificates generated by the TSF shall be in accordance with NSA-certified NSA-approved certificate schemes[33].

FCS_CKM_EXP.1.3: TSF **によって生成されるいかなる公開鍵証明書も、**NSA **に認証された** NSA **承認の証明書スキーム** 33 **に従ったものでなければならない。**

5.2.2.6 Explicit: Cryptographic Key Handling and Storage (FCS_CKM_EXP.2)

5.2.2.6 **明示的要件: 暗号鍵の扱いと格納** (FCS_CKM_EXP.2)

FCS_CKM_EXP.2.1: The TSF shall perform key entry and output in accordance with FIPS PUB 140-2, Level 3.

FCS_CKM_EXP.2.1: TSF は、FIPS PUB 140-2、レベル 3 に従って鍵の入力と出力を実行しなくてはならない。

FCS_CKM_EXP.2.2: The TSF shall provide a means to ensure that keys are associated with the correct entities (i.e., person, group, or process) to which the keys are assigned.

FCS_CKM.EXP.2.2: TSF は、鍵が、その鍵が割り付けられる正しいエンティティ (すなわち、人、グループ、あるいはプロセス)と組み合わされていることを保証する手段を提供しなくてはならない。

FCS_CKM_EXP.2.3: The TSF shall perform a key error detection check on each transfer of key (internal, intermediate transfers).

FCS_CKM_EXP.2.3: TSF は、鍵の各転送 (内部転送、他への転送) ごとに誤り検出チェックを実施しなくてはならない

Application Note: A parity check is an example of a key error detection check.

適用上の注釈: 鍵誤り検出チェックの例として、パリティチェックがある。

FCS_CKM_EXP.2.4: The TSF shall encrypt or split persistent secret and private keys when not in use.

FCS_CKM_EXP.2.4: TSF は、永続的な共通鍵及び秘密鍵が使用されないとき、それを暗号化するか分割しなくてはならない。

Application Note: A persistent key, such as a file encryption key, is one that must be available in the system over long periods of time. A non-persistent key, such as a key used to encrypt or decrypt a single message or a session, is one that is ephemeral in the system.

適用上の注釈: ファイル暗号化鍵などの永続的鍵は、長い期間にわたってそのシステム内で使用できなくてはならない。単一メッセージや一つのセッションなどを暗号化あるいは復号するために使用される非永続的鍵は、そのシステム内で、短時間しか存在しない。

Application Note: "When not in use" shall be interpreted in the strictest sense so that persistent keys only exist in plaintext form during intervals of operational necessity. For example, a file encryption key shall exist in plaintext form only during actual encryption and/or decryption processing of a file. Once the file is decrypted or encrypted the file encryption key shall be immediately covered for protection.

適用上の注釈: 永続的鍵が運用上必要な間だけ平文形式で存在しなければならないよう、「使用されないとき」の表現を最大限厳密な意味で解釈しなくてはならない。例えば、ファイル暗号化鍵は、ファイルを実際に暗号化及び/または復号処理する間だけ平文形式で存在しなくてはならない。ファイルが復号あるいは暗号化されたら、そのファイル暗号化鍵は、ただちに保護のためにカバーされなくてはならない。

FCS_CKM_EXP_2.5 The TSF shall destroy non-persistent cryptographic keys after an administrator-defined period of time of inactivity.

FCS_EXP_2.5: TSF は、管理者が定義した非活性状態の時間の後、非永続的暗号鍵を破壊しなくてはならない。

FCS_CKM_EXP.2.6: The TSF shall overwrite each intermediate storage area for plaintext key/critical cryptographic security parameter (i.e., any storage, such as

memory buffers, that is included in the path of such data). This overwriting shall be executed three or more times using a different alternating data pattern each time upon the transfer of the key/critical cryptographic security parameter to another location.

FCS_EXP_2.6: TSF は、平文鍵/機密上重要な暗号セキュリティパラメタ (すなわち、そのデータの経路中に含まれる、メモリバッファなどのあらゆる格納領域) に対する各中間的格納領域を上書きしなくてはならない。この上書きは、鍵/機密上重要な暗号セキュリティパラメタの他の場所への転送のたびに、異なる交互データパターンを使って 3 回以上実行しなくてはならない。

Application Note: This is related to the elimination of internal, temporary copies of plaintext keys created during processing, not to the total destruction of a key from the TOE which is discussed under Key Destruction. Although verification of the zeroization of each intermediate location of a plaintext key/critical cryptographic security parameter is desired here (by checking for the final known alternating data pattern), it is not required at this time. However, vendors are highly encouraged to incorporate this verification whenever possible into their implementations.

適用上の注釈: これは、処理中に生成された、内部の一時的な平文鍵のコピーの削除に関わるものであり、鍵の破棄で議論された、TOE からの鍵の完全な破棄に関わるものではない。平文鍵/機密上重要な暗号セキュリティパラメタの各々の中間的な場所のゼロ化の検証が望ましいのであるが、ここでは、それは要求されない。しかしながら、ベンダは、実装が可能なときには必ずこの検証を組み込むことが強く推奨される。

FCS_CKM_EXP.2.7: The TSF shall prevent archiving of expired (private) signature keys.

FVS_CKM_EXP.2.7: TSF は、有効期限が切れた (秘密の) 署名鍵が保管 (archive) されるのを防がなくてはならない。

Application Note: This requirement is orthogonal to typical system back-up procedures. Therefore, it does not address the problem of archiving an active (private) signature key during a system back-up and saving the key beyond its intended life span.

適用上の注釈: この要件は、典型的なシステムバックアップ手続と直交するものである。それゆえに、これは、有効な (秘密の) 署名鍵がシステムバックアップ中に保管 (archive) され、本来意図するその鍵の寿命を超えて保存されてしまう問題には対応しない。

---

16 This requirement applies strictly to generation of symmetric keys. Validation techniques for generated symmetric keys are discussed in FCS_CKM_EXP.1.1.

16 この要件は、対称鍵の生成に厳密に適用される。生成された対称鍵の確認技術は、FCS_CKM_EXP.1.1 で議論される。

17 Any pseudorandom RNG used in these schemes for generating private values shall be seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP).

17 秘密の値を生成するためのこれらの枠組みで使用されるあらゆる擬似ランダム RNG (この PP での RNG 要件を満たす両タイプの RNG) は、非決定論的 RNG によって種を与えられなくてはならない。

18 A pseudorandom RNG seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP) shall be used in the generation of these primes.

18 非決定論的 RNG (この PP での RNG 要件を満たす両タイプの RNG) によって種を与えられる擬似ランダム RNG は、これらの素数の生成において使用されなくてはならない。

19 Any pseudorandom RNG used in these schemes for generating private values shall be seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP).

19 秘密の値を生成するためのこれらの枠組みで使用されるあらゆる擬似ランダム RNG は、非決定論的 RNG (この PP での RNG 要件を満たす両タイプの RNG) によって種を与えられなくてはならない。

20 This requirement applies strictly to generation of asymmetric keys. Validation techniques for generated asymmetric keys are discussed in FCS_CKM_EXP.1.2.

20 この要件は、非対称鍵の生成に厳密に適用される。生成された非対称鍵の確認技術は、FCS_CKM_EXP.1.2 で議論される。

21 These are the keys/parameters (e.g., the public/private key pairs) underlying a public key-based key establishment scheme, not the session keys established by such schemes.

21 これらは、公開鍵ベースの鍵確立スキームの基礎をなす鍵/パラメタ (例えば、公開/秘密鍵ペア) であり、そのようなスキームによって確立されるセション鍵ではない。

22 Any pseudorandom RNG used in these schemes for generating private values shall be seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP).

22 秘密の値を生成するためのこれらの枠組みで使用されるあらゆる擬似ランダム RNG は、非決定論的 RNG (この PP での RNG 要件を満たす両タイプの RNG) によって種を与えられなくてはならない。

23 A pseudorandom RNG seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP) shall be used in the generation of these primes.

23 非決定論的 RNG (この PP での RNG 要件を満たす両タイプの RNG) によって種を与えられる擬似ランダム RNG は、これらの素数の生成において使用されなくてはならない。

24 Any pseudorandom RNG used in these schemes for generating private values shall be seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP).

24 秘密の値を生成するためのこれらの枠組みで使用されるあらゆる擬似ランダム RNG は、非決定論的 RNG (この PP での RNG 要件を満たす両タイプの RNG) によって種を与えられなくてはならない。

25 Key Distribution (and key establishment) is typically addressed in terms of key transport methods or key agreement methods. Key transport methods are discussed in this section. Key agreement methods are addressed in FCS_COP.1(4) (Cryptographic Operation (for cryptographic key agreement)).

25 鍵配付 (及び鍵確立) は、一般的に、鍵転送法あるいは鍵交換法の観点で対応される。鍵転送法は、このセクションで議論される。鍵交換法は、FCS_COP.1(4) (暗号操作 (暗号鍵交換用)) で対応される。

26 Until NIST identifies approved methods for manually distributing symmetric key, FIPS PUB 171 (Key Management Using ANSI X9.17) shall be used. For purposes of interpreting FIPS PUB 171,

only the Triple Data Encryption Algorithm (TDEA) with 168 bits of key shall be applied. (DES is not acceptable for meeting this requirement. Eventual migration to AES is expected.)

26 NIST が手動の対称鍵配付に対する承認済みの方法を提示するまで、FIPS PUB 171 (ANSI X9.17 を用いる鍵管理) を使わなくてはならない。FIPS PUB 171 の解釈のため、168 ビット鍵を持つトリプルデータ暗号アルゴリズム (TDEA) だけが適用されなくてはならない。(DES は、この要件を満たすためには適用不可。その結果、AES への移行が期待される。)。

27 DoD multilevel applications require Class 5 PKI to address worst case environments, but currently this class is just a concept. In the interim, NSA-approved certificate schemes with hardware tokens for protection of private key are approved under the added requirement that stronger protection mechanisms must be applied at the boundaries of the protected environment as stated earlier in this PP. When Class 5 certificates are fully established, they will be required.

27 DoD マルチレベルアプリケーションは、最悪ケースの環境に対応するためにクラス 5 の PKI を要求するが、現時点では、このクラスはコンセプトにすぎない。暫定措置として、本 PP の前半で述べられた、より強力な保護メカニズムが保護された環境の境界に適用されなくてはならないという付加的要件の元で、秘密鍵の保護にハードウェアトークンを使う NSA 承認の認証スキームが承認される。クラス 5 認証が完全に確立されれば、それが必要となる。

28 See previous footnote.

28 前の注釈を参照。

29 Until NIST identifies approved methods for automatically distributing symmetric key, FIPS PUB 171 (Key Management Using ANSI X9.17) is being used here. For purposes of interpreting FIPS PUB 171, only TDEA with 168 bits of key shall be applied. (DES is not acceptable for meeting this requirement. Eventual migration to AES is expected.) Where public key schemes are used in key transport methods, NIST Special Publication 800-56 (“Recommendation on Key Establishment Schemes”; DRAFT 2.0, January 2003) shall also be used.

29 NIST が自動的対称鍵配付に対する承認済みの方法を提示するまで、FIPS PUB 171 (ANSI X9.17 を用いる鍵管理) を使わなくてはならない。FIPS PUB 171 の解釈のため、168 ビット鍵を持つトリプルデータ暗号アルゴリズム (TDEA) だけが適用されなくてはならない。(DES は、この要件を満たすには受け入れられない。その結果、AES への移行が期待される。) 鍵の転送法に公開鍵スキームが使われる場合、NIST 特別出版 800-56 (「鍵確立スキームにおける勧告」; ドラフト 2.0、2003/1) も使われなくてはならない。

30 DoD multilevel applications require Class 5 PKI to address worst case environments, but currently this class is just a concept. In the interim, NSA-approved certificate schemes with hardware tokens for protection of private key are approved under the added requirement that stronger protection mechanisms must be applied at the boundaries of the protected environment as stated earlier in this PP. When Class 5 certificates are fully established, they will be required.

30 DoD マルチレベルアプリケーションは、最悪ケースの環境に対応するためにクラス 5 の PKI を要求するが、現時点では、このクラスはコンセプトにすぎない。本 PP の前半で述べられた、より強力な保護メカニズムが保護された環境の境界に適用されなくてはならないという付加的要件の元で、秘密鍵の保護にハードウェアトークンを使う NSA 承認の認証スキームが暫定的に承認される。クラス 5 認証が完全に確立されたら、それが必要とされる。

31 See previous footnote.

31 前の注釈を参照。

32 For purposes of interpreting this standard, only TDEA with 168 bits of key shall be applied (DES is not acceptable for meeting this requirement. Eventual migration to AES is expected.).

32 この標準の解釈として、168 ビット鍵の TDEA だけが適用されなくてはならない(DES は、この要件を満たすためには適用不可。結果的に、AES への移行が期待される。)。

33 DoD multilevel applications require Class 5 PKI to address worst case environments, but currently this class is just a concept. In the interim, NSA-approved certificate schemes with hardware tokens for protection of private keys are approved under the added requirement that stronger protection mechanisms must be applied at the boundaries of the protected environment as stated earlier in this PP. When Class 5 certificates are fully established, they will be required.

33 DoD マルチレベルアプリケーションは、最悪ケースの環境に対応するためにクラス 5 の PKI を要求するが、現時点では、このクラスはコンセプトにすぎない。本 PP の前半で述べられた、より強力な保護メカニズムが保護された環境の境界に適用されなくてはならないという付加的要件の元で、秘密鍵の保護にハードウェアトークンを使う NSA 承認の認証スキームが暫定的に承認される。クラス 5 認証が完全に確立されたら、それが必要とされる。

5.2.3 Explicit: Cryptographic Operations Availability (FCS_COA_EXP)

5.2.3 明示的要件：暗号操作の可用性（FCS_COA_EXP）

5.2.3.1 Explicit: Cryptographic Operations Availability (FCS_COA_EXP.1)

5.2.3.1 明示的要件：暗号操作の可用性（FCS_COA_EXP.1）

FCS_COA_EXP.1 The TSF shall provide the following cryptographic operations to applications:
FCS_COA_EXP.1 TSF は、以下の暗号技術アプリケーションに対する操作に対して提供されなければならない。

a) encryption
a)暗号化
b) decryption
b)復号化
c) digital signature
c)デジタル署名
d) secure hashing
d)セキュア・ハッシュ
e) [assignment: any other cryptographic operations provided to applications].
e)[割付]その他のいかなる暗号技術を用いた操作を提供するアプリケーション

5.2.4 Cryptographic Operation (FCS_COP)

5.2.4 暗号操作（FCS_COP）

5.2.4.1 Cryptographic Operation (for data encryption/decryption) FCS_COP.1(1))

5.2.4.1（データ暗号／復号の）暗号操作（FCS_COP.1(1)）

FCS_COP.1.1(1) **Refinement:** The TSF shall perform **data encryption/decryption services** in accordance with a **NIST-approved implementation of the** cryptographic algorithm **Triple Data Encryption Algorithm[34] (TDEA) used in NIST-approved modes of operation** and cryptographic key size **of 168 bits (three independent keys)** that meets the following*:*
FCS_COP.1.1(1) **詳細化：**TSF **は、以下に合致する** NIST **認可の暗号アルゴリズム** Triple Data Encryption Algorithm[34] (TDEA)**と暗号鍵長** 168 **ビット（３つの独立した鍵）に従ってデータの暗号化／複合化サービスを実行しなければならない：**

a) FIPS PUB 140-2, Security Requirements for Cryptographic Modules,
a)FIPS PUB 140-2、**暗号モジュールのセキュリティ要件**

b) FIPS PUB 46-3, Data Encryption Standard, and
b)FIPS PUB 46-3、**データ暗号化規格　そして**

c) ANSI X9.52-1998, Triple Data Encryption Algorithm Modes of Operation.
c)ANSI X9.52-1998 **三重データ暗号化アルゴリズムモードの操作**

5.2.4.2 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

5.2.4.2　（暗号署名の）暗号操作（FCS_COP.1(2)）

FCS_COP.1.1(2) **Refinement:** The TSF shall perform **cryptographic signature services** in accordance with the **NIST-approved digital signature** algorithm ***[selection:***
FCS_COP.1.1(2) **詳細化：**TSF **は、以下に合致する** NIST **認可のデジタル署名アルゴリズム**［**選択**

(1) Digital Signature Algorithm (DSA) with a key size (modulus)of 2048[35] bits or greater,
1)**鍵長（絶対値）が**2048[35]**ビットより長いデジタル署名アルゴリズム**（DSA）、

(2) RSA Digital Signature Algorithm (rDSA with odd e) with a key size (modulus) of 2048[36] bits or greater, or
2)**鍵長（絶対値）が** 2048[36] **ビットより長い** RSA **デジタル署名アルゴリズム**（rDSA）、**もしくは**

(3) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater]

3)鍵長が 256 ビット以上の楕円曲線デジタル署名アルゴリズム（ECDSA)］

Application Note: For elliptic curve-based schemes the key size refers to the log2 of the order of the base point. As the preferred approach for cryptographic signature, elliptic curves will be required within a TBD time frame after all the necessary standards and other supporting information are fully established.
適用上の注釈：楕円曲線スキームのために、キー・サイズは、基点の命令の記録を参照します。暗号の署名のための好ましいアプローチとして、必要な標準および他の支援する情報がすべて完全に確立された後、楕円のカーブは TBD 時間枠内に要求されます。

a) Case: Digital Signature Algorithm
FIPS PUB 186-2[37], Digital Signature Standard, for signature creation and verification processing; and ANSI Standard X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography for generation of the domain parameters[38];

a)デジタル署名アルゴリズム利用時には
FIPS PUB 186-2[37], 署名の生成と検証に関するデジタル署名標準,
ANSI標準 X9.42-2001, 金融業界向け公開鍵暗号:
領域パラメーター[38]の生成のために個別の離散対数暗号を使った対称なキーの合意

b) Case: RSA Digital Signature Algorithm (with odd e)
ANSI X 9.31-1998 (May 1998), Digital Signatures Using Reversible Public Key Cryptography For The Financial Services Industry (rDSA)[39];
b)RSA デジタル署名アルゴリズム利用時には
ANSI X.31, 金融業界向け逆公開鍵を用いたデジタル署名(rDSA)[39]；

c) Case: Elliptic Curve Digital Signature Algorithm
ANSI X9.62-1-xxxx (10 Oct 1999), Public Key Cryptography for the Financial Services Industry: Elliptic Curve Digital Signature Algorithm (ECDSA) [40].
c)楕円曲線デジタル署名アルゴリズム利用時には
ANSI X9.62, 署名の生成と検証に関するデジタル署名標準: 楕円曲線デジタル署名アルゴリズム(ECDSA)[40]。

5.2.4.3 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))
5.2.4.3 (暗号ハッシュの) 暗号操作 (FCS_COP.1(3))

FCS_COP.1.1(3) **Refinement:** The TSF shall perform **cryptographic hashing services** in accordance with a **NIST-approved hash implementation of the Secure Hash** algorithm and **message digest size of at least 256 bits** that meets the following**: FIPS PUB 180-2.**
FCS_COP.1.1(3) 詳細化：TSF は、FIPS PUB 180-2 に合致する NIST 認可のハッシュ実装である

セキュアハッシュアルゴリズムと少なくとも 256 ビットのメッセージダイジェスト長の暗号ハッシュサービスを提供しなければならない：
Application Note: The message digest size should correspond to double the system encryption key strength.
適用上の注釈：メッセージ・ダイジェストのサイズは、システムの暗号化鍵の 2 倍の強度相当でなければなりません。

5.2.4.4 Cryptographic Operation (for cryptographic key agreement) (FCS_COP.1(4))

5.2.4.4 （暗号鍵交換の）暗号操作（FCS_COP.1(4)）

FCS_COP.1.1(4) **Refinement:** The TSF shall perform **cryptographic key agreement services** in accordance with a **NIST-approved implementation of a key agreement** [41] algorithm ***[selection:***
FCS_COP.1.1(4) 詳細化：TSF は、以下に合致する NIST 認可の鍵交換 [41] アルゴリズム［選択：

(1) Finite Field-based key agreement algorithm and cryptographic key sizes(modulus) of 2048 bits or greater,
1)有限体に基づいたアルゴリズムと暗号化された暗号鍵長が 2048 ビットよりも大きい、

(2) Elliptic Curve-based key agreement algorithm and cryptographic key size of 256 bits or greater]
2)楕円曲線鍵交換アルゴリズム (ECKEA)と暗号鍵長が 256 ビット以上］

Application Note: For elliptic curve-based schemes the key size refers to the $\log_2$ of the order of the base point. As the preferred approach for key exchange, elliptic curves will be required within a TBD time frame after all the necessary standards and other supporting information are fully established.
適用上の注釈：楕円曲線スキームのために、キー・サイズは、基点の命令の記録を参照します。キー交換のための好ましいアプローチとして、必要な標準および他の支援する情報がすべて完全に確立された後、楕円曲線 TBD 時間枠内に要求されるでしょう。

a) Case: Finite field-based key agreement schemes
ANSI X9.42-2001, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography[42]**;**
a)有限体に基づいたスキーム利用時には、ANSI X9.42, 金融業界向け公開鍵暗号:離散対数暗号 [42] を使った対象鍵の合意；

Application Note: For example, "Classic" Diffie-Hellman-based schemes
注釈：たとえば、Diffie-Hellmanに基づいたスキーム

b) Case: Elliptic curve -based key agreement schemes
ANSI X9.63-200x (1 Oct 2000), Public Key Cryptography for the Financial

Services Industry: Key Agreement and Key Transport using Elliptic Curve Cryptography. [43]
b)楕円曲線に基づいたスキーム利用時には、
ANSI 9.63, 金融業界向け公開鍵暗号: 楕円暗号 [43] の鍵の合意と鍵配送；そして

Application Note: Some authentication mechanism on the keying material is recommended. In addition, repeated generation of the same shared secrets should be avoided. As an example, the MQV schemes described in the above standards address these issues.
適用上の注釈：鍵構成物に対する認証メカニズムが推奨されます。追加措置として、同一の共有鍵は共有秘密情報の繰り返しの生成は避けるべきです。たとえば上記標準で説明している MQV スキームがこれらの問題を解決します。

5.2.4.5 Explicit: Random Number Generation (FCS_COP_EXP.1)
5.2.4.5 明示:乱数生成(FCS_COP_EXP.1)

FCS_COP_EXP.1.1 The TSF shall perform all random number generation (RNG) services in accordance with [selection:
FCS_COP.EXP.1.1 TSF は、以下に合致する［選択：

(1) multiple independent hardware-generated inputs combined with a mixing function, or
1)混合機能（mixing function）と組み合わせた、複数の独立ハードウェアで生成されたインプット、または

Application Note: A NIST-approved hashing function is recommended for the mixing function in hardware based RNGs. If the length of the needed random number exceeds the length of the hash's message digest, then multiple hashes can be used to provide the needed random quantity.
適用上の注釈：ハードウェアを利用した RNG に於ける混合機能には、NIST 認可のハッシュ関数が推奨される。必要とされる乱数の長さがハッシュのメッセージ・ダイジェストの長さを超過する場合、多数のハッシュは必要とされるランダム量を提供するために使用することができる。

(2) multiple independent software-generated inputs combined with a NIST-approved hashing function, or
2)NIST 認可のハッシュ関数と組み合わされた、複数の独立したソフトウェアで生成されたインプット、または

Application Note: A NIST-approved hashing function is required for the mixing function in software based RNGs. If the length of the needed random number exceeds the length of the hash's message digest, then multiple hashes can be used to provide the needed random quantity.
適用上の注釈：ハードウェアを利用した RNG に於ける混合機能には、NIST 認可のハッシュ機能が推奨される。必要とされる乱数の長さがハッシュのメッセージのダイジェスト長さを超過する場合、多数のハッシュは必要とされるランダム量を提供するために使用することができる。

(3) a combination of multiple independent hardware-generated inputs combined with a mixing function and multiple independent software-generated inputs combined with a NIST-approved hashing function.]
3)NIST 認可のハッシュ関数と組み合わされた、複数の独立したソフトウェアで生成されたインプット、または

a) FIPS PUB 180-2, when using a NIST-approved hashing function as the mixing function,
a)混交機能として NIST 認可のハッシュ関数を利用する場合、FIPS PUB 180-2、

b) Documents listed in Appendix D and NIST Special Publication 800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications;
b)付録 D および NIST800-22 にリストされたドキュメント：暗号適用用ランダムおよび擬似乱数的な数ジェネレーター用の統計的検査方法；

Application Note: This publication includes some discussion and guidance on randomness and RNG seeding. Successful completion and documentation of these tests during the TOE development helps to demonstrate the random number generator design is rigorous. There exists a NIST toolbox for running these tests. Requirements for acceptable thresholds and sample sizes for use in applying NIST Special Publication 800-22 in the context of this protection profile can be found in Appendix D of this profile.
適用上の注釈：この出版は、任意および RNG に関する、議論およびガイダンスを含んでいます。乱数生成を実証する TOE 開発支援中のこれらのテストの無事完了およびドキュメンテーションは正確です。これらのテストを実行するためのツールボックスが存在します。この保護プロフィールの中の NIST の特別の出版 800-22 の適用で使用される受理可能なしきい値およびサンプル・サイズのための必要条件は、このプロフィールの付録 D で見つけることができます。

c) All the RNG/PRNG self-tests of FIPS PUB 140-2,
c)FIPS PUB-2, 140-24 の全 RNT/PRNG 自己テスト
d) All statistical RNG tests (as specified in Appendix C) upon demand and upon powerup
d) すべての統計的な RNG の要求に応じて段階的にでテストします(Appendix C で指定されるように)。
e) The augmented tests, and self-test requirements from this PP: TSF Self Testing, and
e)当 PP が規定する拡張テストと自己テスト要件：TSF 自己テスト、そして
f) RNG/PRNG design and test documentation consistent with that required in this PP for other subsystems: Development Documentation (ADV)
f)当 PP による他のサブシステムに対する要求と合致した RNG/PRNG デザインとテストドキュメント：ドキュメントの作成（セクション６．３）

FCS_COP_EXP.1.2 The TSF shall defend against tampering of the random number generation (RNG)/ pseudorandom number generation (PRNG) sources.

FCS_COP.EXP.1.2 TSF は、乱数生成（RNG）／疑似乱数生成（PRNG）のソースの改ざんを防止しなくてはならない。

Application Note: The RNG/PRNG should be resistant to manipulation or analysis of its sources,or any attempts to predictably influence its states. Three examples of very different approaches the TSF might pursue to address this include: a) identifying the fact that physical security must be applied to the product, b) applying checksums over the sources, or c) designing and implementing the TSF RNG with a concept similar to a keyed hash (e.g.,
where periodically, the initial state of the hash is changed unpredictably and each change is protected as when provided on a tamper-protected token, or in a secure area of memory.
適用上の注釈：PNG/PRNG は、外部からの操作、そのソースの分析、または予想されるその状態への外部からの影響から防御されていなくてはなりません。この問題を解決する為に TSF が行える、異なった方法の例が３つあります： a)物理的セキュリティは、その OS を搭載している製品によって適用されているという事実を明確にする（すなわち、要件を保留する）、または b)ソースに対してチェックサムを適用する、または c)鍵付きハッシュと似たコンセプトで TSF RNG をデザインして実装する（たとえば、定期的にハッシュの初期状態が予知不能で変更され、各変更は改ざん不能なトークンや、メモリー内の保護エリアを与えられることによって保護されている場合など）。

---

34 The Advanced Encryption Standard (AES) employing key lengths of 128 bits or greater and meeting NISTapproved AES standards will be required when AES is fully established. With the approval of FIPS PUB 197 and NIST Special Publication 800-38A, progress is being made to fully establish AES, but establishment is not yet complete. Other approved public standards or NIST special publications are still needed for AES. (An example of this is key distribution for AES.)

34 拡張暗号標準Advanced Encryption Standard (AES)が完全に確立された後には、AESが採用する鍵長128ビット以上で、NIST認可のAES標準が必要になります。 FIPS PUB197とNIST Special Publication800-38Aの承認をもって、AESを完全に確立されると見られていますが、まだ完全ではありません。 他の承認された公共の規格かNISTの特別な刊行物がまだAESに必要です。(この例はAESに、主要な分配です。)

35 A 2048-bit or greater modulus is required to provide the desired 128-bit equivalent symmetric key strength. The 2048-bit modulus is compatible with (1.) operationally practical digital signature key sizes in pending IPSEC commercial products, and (2.) the current direction of digital signatures in the DoD PKI. This smaller modulus reduces the equivalent symmetric key strength to 112 bits. Certificate signatures based on a 2048-bit or greater modulus or the elliptic curve approach is recommended as soon as the DoD PKI can support it. The elliptic curve approach is preferred. *{"Nearterm applications" means products designed and validated against this specific version of the OS PP.}*

35 2048ビットか、より大きい係数が必要な128ビットの同等な左右対称の主要な強さを提供するのに必要です。 2048年のビットの係数はDoD PKIで未定のIPSEC商品の中の(1)操作上実用的なデジタル署名主要なサイズ、およびデジタル署名の(2)現在の指示と互換性があります。 このより小さい係数は同等な左右対称の主要な強さを112ビットまで減少させます。 DoD PKIがそれを支持することができるとすぐに、署名が基礎づけた証明書は2048ビットの、または、より大きい係数か楕円曲線接近のときに推薦されます。 楕円曲線アプローチは好まれます。 {「Nearterm アプリケーション」

はOS PPのこの特定のバージョンに対して設計されて、有効にされた製品を意味します。}

[36] See previous footnote.

[36] 前掲の脚注を見てください。

[37] FIPS PUB 186-3 is under development. It will incorporate the signature creation and verification processing of FIPS PUB 186-2, and the generation of domain parameters of ANSI X9.42. FIPS PUB 186-3 shall be used here when it is finalized and approved.

[37] FIPS PUB186-3は作成中です。それはFIPS PUB186-2の署名創造と検証処理、およびANSI X9.42のドメインパラメタの世代を取り入れるでしょう。これが確立させられて承認されるとき、FIPS PUB186-3はここで使用されるでしょう。

[38] Any pseudorandom RNG used in these schemes for generating private values shall be seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP).

[38] プライベートな値を発生させるのにこれらの計画に使用されるどんな擬似ランダムRNGも非決定性RNG(このPPの両方のタイプのRNGミーティングRNG要件)によって種を蒔かれるものとします。

[39] See previous footnote.

[39] 前掲の脚注を見てください。

[40] See previous footnote.

[40] 前掲の脚注を見てください。

[41] Until FIPS PUB 140-2 identifies approved key agreement schemes, NIST Special Publication 800-56 (“Recommendation on Key Establishment Schemes”, DRAFT 2.0, Jan 2003) shall be used here.

[41] FIPS PUB140-2が承認された主要な協定計画を特定するまで、NIST Special Publication800-56はここで使用されるものとします(「主要な設立の推薦状は計画されます」、DRAFT2.0、2003年1月)。

[42] Any pseudorandom RNG used in these schemes for generating private values shall be seeded by a nondeterministic RNG (both types of RNGs meeting RNG requirements in this PP).

[42] プライベートな値を発生させるのにこれらの計画に使用されるどんな擬似ランダムRNGも非決定性RNG（このPPの両方のタイプのRNGミーティングRNG要件)によって種を蒔かれるものとします。

[43] See previous footnote.

[43] 前掲の脚注を見てください。

5.3 User Data Protection (FDP)
5.3 ユーザデータ保護（FDP）

5.3.1 Access Control Policy (FDP_ACC)
5.3.1 アクセス制御方針（FDP_ACC）

5.3.1.1 Complete Access Control (FDP_ACC.2)
5.3.1.1完全アクセス制御 (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the **Discretionary Access Control policy** on ***all subjects and all named objects*** and all operations among them.
FDP_ACC.2.1 TSF は、任意アクセス制御方針を全てのサブジェクトと全ての名前付きオブジェクトとそれら間の全ての操作に対して実施しなければならない。

Application Note: The DAC policy does not cover local public objects.
適用上の注釈：DAC 方針はローカルな公開オブジェクトには適用されません。

FDP_ACC.2.2 **Refinement:** The TSF shall ensure that all operations between any subject and any **named** object are covered by **the Discretionary Access Control policy**.10
FDP_ACC.2.2 詳細化：TSF は、任意のサブジェクトと任意の名前付きオブジェクト間の全ての操作に任意アクセス制御方針が適用されていることを保証しなければならない。10

5.3.2 Access Control Functions (FDP_ACF)
5.3.2 アクセス制御機能 (FDP_ACF)

5.3.2.1 Security Attribute Based Access Control (FDP_ACF.1)
5.3.2.1 セキュリティ属性に基づいたアクセス制御 (FDP_ACF.1)

FDP_ACF.1.1 **Refinement:** The TSF shall enforce the **Discretionary Access Control policy** to **named** objects based on the following types of subject and object security attributes **:**
FDP_ACF.1.1 詳細化：TSF は、以下に述べるサブジェクトの種類とオブジェクトのセキュリティ属性に基づき、名前付きオブジェクト対する任意アクセス制御を実施しなければならない：

a) the authorized user identity and group membership(s) associated with a subject and
a) サブジェクトに関連する許可ユーザの識別情報とグループメンバーシップ属性

b) the [authorized user (or group) identity, access operations] pairs associated with a named object.
b) 名前付きオブジェクトに割り当てられた[許可ユーザ（グループ）、操作]の対

Application Note: This requirement is worded to include only implementations where access control attributes are associated with objects rather than subjects. This implementation becomes critical when satisfying FMT_MTD.1.1(3) and FMT_REV.1.1(1).
適用上の注釈：当要件は、サブジェクトではなくオブジェクトに関連するアクセス制御属性を実装するために言及しています。この実装は、FMT_MTD.1.1(3)**と** FMT_REV.1.1(1)**の要件を満たすうえで重要になってきます。**

FDP_ACF.1.2 **Refinement:** The TSF shall enforce the following rules to determine if an operation among subjects and **named** objects is allowed:11
FDP_ACF.1.2 **詳細化：**TSF **は、サブジェクトと名前付きオブジェクト間の操作が許可されているかを決定するために、以下の規則を実施しなければならない：**11

• The Discretionary Access Control policy mechanism shall, either by explicit authorized user action or by default, provide that named objects are protected from unauthorized access according to the following ordered rules:
- **任意アクセス制御は、明示的なユーザ操作又は標準の操作に対して、名前付きオブジェクトを権限の無いアクセスから以下の順序付き規則に従って保護するものでなければならない。**

1) If the requested mode of access is denied to that authorized user, deny access.
1）要求されたアクセスモードが許可ユーザに対して不許可になっている場合、アクセスを不許可とする。

2) If the requested mode of access is permitted to that authorized user, permit access.
2）要求されたアクセスモードが許可ユーザに対して認められている場合、アクセスを許可する。

3) If the requested mode of access is denied to every group of which the authorized user is a member, deny access
3）要求されたアクセスモードが許可ユーザの所属する全てのグループに対して不許可になっている場合、アクセスを不許可とする。

4) If the requested mode of access is permitted to any group of which the authorized user is a member, grant access
4）要求されたアクセスモードが許可ユーザの所属する何れかのグループに対して許可になっている場合、アクセスを許可する。

5) Else deny access.
5）それ以外、アクセスを不許可とする。

FDP_ACF.1.3 **Refinement:** The TSF shall explicitly authorize access of subjects to **named** objects based on the following additional rules:

FDP_ACF.1.3 **詳細化：TSF は、以下の追加規則に基づいて、名前付きオブジェクトに対するサブジェクトのアクセスを明示的に許可できなければならない：**

a) Authorized administrators must follow the above -stated Discretionary Access Control policy, except after taking the following specific actions: *[assignment: list of specific actions]*.
ａ）許可管理者は、上述の任意アクセス制御方針に従う必要があるが、以下の特定アクションを行った後にはその限りではない：[割付：特定アクションのリスト]。

b) The enforcement mechanism (i.e., access control lists) shall allow authorized users to specify and control sharing of named objects by individual user ide ntities and group identities and shall provide controls to limit propagation of access rights.
b) **執行メカニズム（たとえば、アクセス制御リスト）により、許可ユーザが、名前付き共有オブジェクトの指定及び制御を単一ユーザ及びグループ単位で行う事を認め、かつアクセス権限の伝搬を制限できなければならない。**

c) [assignment: other rules, based on security attributes, that explicitly authorize access of subjects to **named** *objects].*
c) **[割付：セキュリティ属性に基づく名前付きオブジェクトに対するサブジェクトのアクセスを明示的に許可するその他の規則]。**

Application Note: This element allows specifications of additional rules for authorized administrators to bypass the Discretionary Access Control policy for system management or maintenance (e.g., system backup).
適用上の注釈：このエレメントは、許可管理者に対して、システム管理やメンテナンス（たとえばシステムバックアップ）の任意アクセス制御方針をバイパスする追加規則の指定を可能にします。

FDP_ACF.1.4 **Refinement:** The TSF shall explicitly deny access of subjects to **named** objects based on the following rules:
FDP_ACF.1.4 **詳細化：TSF は、以下の追加規則に基づいて、名前付きオブジェクトに対するサブジェクトのアクセスを明示的に拒否できなければならない：**

a) If the requested mode of access is denied to that authorized user, deny access.
ａ）要求されたアクセスモードが許可ユーザに対して不許可になっている場合、アクセスを不許可とする。

b) If the requested mode of access is denied to every group of which the authorized user is a member, deny access
ｂ）要求されたアクセスモードが許可ユーザの所属する全てのグループに対して不許可になっている場合、アクセスを不許可とする。

c) These access controls shall be capable of specifically excluding access to the granularity of a single user.

c）これらのアクセス制御は、単一ユーザの粒度でアクセス不許可の指定が出来るものでなければならない。

5.3.3 Export to Outside TSF Control (FDP_ETC)
5.3.3 TSF **制御外へのエクスポート** (FDP_ETC)

5.3.3.1 Export of User Data with Security Attributes (FDP_ETC.2)
5.3.3.1 **セキュリティ属性付きユーザデータのエクスポート** (FDP_ETC.2)

FDP_ETC.2.1 The TSF shall enforce the **Mandatory Access Control and Mandatory Integrity Control policies** when exporting user data, controlled under the SFPs, outside of the TSC.
FDP_ETC.2.1 **TSF は、SPFs 制御下にあるユーザデータを TSC 外にエクスポートするとき、必須アクセス制御と必須完全制御方針を実施しなければならない。**

Application Note: For this family (FDP_ETC) the term "security attributes" refers only to the sensitivity and integrity labels of subject and objects.
適用上の注釈：当ファミリー（FDP_ETC）に於いて"セキュリティ属性"という用語は、サブジェクトとオブジェクトの機密と完全ラベルのみを指します。

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.
FDP_ETC.2.2 **TSF は、ユーザデータのエクスポート時には、ユーザデータに関係したセキュリティ属性を付けてエクスポートしなければならない。**

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.
FDP_ETC.2.3 **TSF は、セキュリティ属性が TSC の外部にエクスポートされるとき、それがエクスポートされるユーザデータに曖昧さなく関連づけられることを保証しなければならない。**

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC:
FDP_ETC.2.4 **TSF は、ユーザデータが TSC からエクスポートされるとき、以下の規則を実施しなければならない：**

a) When data is exported in hardcopy form each page shall be marked with a printed representation of the "least upper bound" sensitivity label of all data exported to the page. By default this marking shall appear on both the top and bottom of each printed page.
a) **データが印刷物としてエクスポートされる場合、そのページにエクスポートされる全データの "最小上限"機密ラベルを示す印を各ページに付けなければならない。デフォルトで、この印は各印刷ページの上部と下部の両方に記されなければならない。**

b) If a device is capable of maintaining data security attributes, the security

attributes shall be exported with the data.
b) **デバイスがデータのセキュリティ属性を保持できる場合、データと一緒にセキュリティ属性はエクスポートされなければならない。**

Application Note: Devices may include external storage devices such as disks, tapes, CDs, DVDs, flash memory as well as wired or wireless networks.
適用上の注釈：デバイスは、テープ、ＣＤ、ＤＶＤ、フラッシュメモリなどが有線で又は無線ネットワークで接続された外部記憶を含んでよい。

c) ***[Assignment: Any additional rules that control the export of information from the TSC and their corresponding security attributes. In all cases the TOE must export the security attributes with the corresponding information]***
c) **［割付：TSC からの情報エクスポートを制御するその他の規則と、それらに関連するセキュリティ属性。全ての場合に於いて、TOE は関連情報と共にセキュリティ属性をエクスポートしなければならない。］**

5.3.4 Information Flow Control Policy (FDP_IFC)
5.3.4 **情報フロー制御方針** (FDP_IFC)

5.3.4.1 Complete Information flow control (for Mandatory Access Control Policy) (FDP_IFC.2(1))
5.3.4.1**必須アクセス制御方針の）完全情報フロー制御** (FDP_IFC.2(1))

FDP_IFC.2.1(1) **Refinement:** The TSF shall enforce the **Mandatory Access Control policy** on ***[assignment: list of all subjects and all objects]***, and all operations that cause information to flow **among them**.12
FDP_IFC.2.1(1) **詳細化：TSF は、［割付：全サブジェクトと全オブジェクトのリスト］及びそれらの間に情報の流れを引き起こす全ての操作に対して必須アクセス制御を実施しなければならない。**12

Application Note: In most systems there is only one type of subject, usually called a process or task, which needs to be specified in the ST. The ST author must also explicitly list the objects that exist in the TOE; this list must include storage objects (data storage resources, input/output devices, etc.) as well as named objects, which may be used to sh are information among subjects acting on the behalf of different users, and for which access to the object can be specified by a name or other identity (such as files or their equivalents). The operations, listed in the ST, among subjects and objects must explicitly define all relationships between subjects and objects in the TOE, and must be consistent with the list of objects defined in the earlier assignment.
適用上の注釈：大半のシステムに於いては、通常プロセス、またはタスクと呼ばれる１種類のサブジェクトしか存在しない。それは、ST に定義されてなければならない。ST の作者は、TOE に存在するオブジェクトも明示的にリストしなければならない；このリストには、名前付きオブジェクトのほかに保管オブジェクト（データ保管リソース、入力／出力デバイスなど）もリストされる必要がある。それは、他のユーザの代理で操作を行うサブジェクト間の情報共有のためであり、そのようなアクセスは名前、またはその他の識別情報（たとえばファイルやそれらと同等のもの）によって指定される。ST にリストされる操作は、ＴＯＥにおけるサブジェク

トおよびオブジェクト間のすべての関係を明示的に定義したものであり、以前の設定で定義されたオブジェクトのリストと矛盾のないものでなければならない。

Application Note: The MAC policy covers all subjects and all objects. The list of objects must include object attributes that are themselves objects (such as filenames) because they can be manipulated by a user.
適用上の注釈：MAC 方針は、全てのサブジェクトと全てのオブジェクトに適用されます。オブジェクトのリストにはオブジェクトの属性も含まれている必要があり、ユーザが操作できることからオブジェクト属性自体がオブジェクトになります（たとえばファイル名）。

FDP_IFC.2.2(1) **Refinement:** The TSF shall ensure that all operations that cause any information in the TSC to flow **among subjects and objects** in the TSC are covered by the **MAC** SFP.13
FDP_IFC.2.2(1) 詳細化：TSF は、TSC 内の情報を TSC 内のサブジェクトとオブジェクト間に情報の流れを引き起こす全ての操作が、MAC SFP によって取り扱われることを保証しなければならない。13

5.3.4.2 Complete Information flow control (for Mandatory Integrity Control Policy) (FDP_IFC.2(2))
5.3.4.2 （必須完全性制御の）完全情報フロー制御 (FDP_IFC.2(2))

FDP_IFC.2.1(2) **Refinement:** The TSF shall enforce the **Mandatory Integrity Control policy** on ***[assignment: list of all subjects and objects]***, and all operations that cause that information to flow **among them**.14
FDP_IFC.2.1(2) 詳細化：TSF は、［割付：全サブジェクトと全オブジェクトのリスト］及びそれらの間に情報の流れを引き起こす全ての操作に対して必須完全性制御を実施しなければならない。14

Application Note: The Mandatory Integrity Control policy is based upon trustworthiness: subjects with a low degree of trustworthiness cannot change data of a higher degree of trustworthiness. A subject with a high degree of trustworthiness can not be forced to rely on data of a low degree of trustworthiness.
適用上の注釈：必須完全制御は、信頼性に基づいています：信頼性の度合いが低いサブジェクトは、それよりも高い度合いの信頼性を持ったデータに変更を加えることはできません。信頼性の度外が高いサブジェクトを、信頼度の度合いが低いデータに依存させることを強制することはできません。

FDP_IFC.2.2(2) **Refinement:** The TSF shall ensure that all operations that cause any information in the TSC to flow **among subjects and objects** in the TSC are covered by the **MIC** SFP.15
FDP_IFC.2.2(2) 詳細化：TSF は、TSC 内の情報を TSC 内のサブジェクトとオブジェクト間に情報の流れを引き起こす全ての操作が、MIC SFP によって取り扱われることを保証しなければならない。15

5.3.5 Information Flow Control Functions (FDP_IFF)
5.3.5 情報フロー制御機能（FDP_IFF）

5.3.5.1 Explicit: Hierarchical Security Attributes (for Mandatory Access Control) (FDP_IFF_EXP.2(1))
5.3.5.1 明示的要件：（必須アクセス制御の）階層的セキュリティ属性（FDP_IFF_EXP.2(1)）

FDP_IFF_EXP.2.1(1) The TSF shall enforce the **Mandatory Access Control policy** based on the following types of subjects, **objects,** and security attributes:
FDP_IFF_EXP.2.1(1) TSF は、以下のサブジェクト、オブジェクト、セキュリティ属性の種別に基づいて必須アクセス制御方針を実施しなければならない。

a) ***[Assignment: list of all subjects]***
a) ［割付：全てのサブジェクトのリスト］

b) the sensitivity label of the subject consisting of at least 8 site definable hierarchical levels and a set of 60 site definable non-hierarchical categories;
b) 最低、８サイトの定義可能な階層的レベルと６０サイトの定義可能な非階層的カテゴリーのセットから成るサブジェクトの機密ラベル；

Application Note: The implementation of sensitivity labels does not need to store labels in a format that has the components of the label explicitly instantiated, but may use some form of tag which maps to a level and category set.
適用上の注釈：機密ラベルの実装に於いては、明示的に具現化するラベルのコンポーネントを保持した形式でラベルを保管する必要はありませんが、レベルやカテゴリーのセットに紐付けするタグのようなものを利用することはあります。

c) ***[Assignment: list of all objects]***
c)［割付：全てのオブジェクトのリスト］

d) the sensitivity label of the object consisting of at least 8 site definable hierarchical levels and a set of 60 site definable non-hierarchical categories;
d) 最低、８サイトの定義可能な階層的レベルと６０サイトの定義可能な非階層的カテゴリーのセットから成るオブジェクトの機密ラベル；

e) ***[Assignment: list of any additional security attributes]*****.**
e)［割付：追加のセキュリティ属性のリスト］

Application Note: For this family (FDP_IFF) the term "security attributes" refers only to the sensitivity labels of subject and objects.
適用上の注釈：当ファミリー（FDP_IFF）に於いて“セキュリティ属性”という用語は、サブジェクトとオブジェクトの機密ラベルのみを指します。

FDP_IFF_EXP.2.2(1) The TSF shall permit an information flow **among subjects**

and objects based on the following rules:
FDP_IFF_EXP.2.2(1) TSF **は、サブジェクトとオブジェクト間の以下の規則に基づいて、情報フローを許可しなければならない：**

a) If the sensitivity label of the subject is greater than (see FDP_IFF_EXP.2.7) or equal to the sensitivity label of the object, then the flow of information from the object to the subject is permitted (a read operation);
a) **サブジェクトの機密ラベルがオブジェクトの機密ラベルを上回っている（FDP_IFF_EXP.2.7 参照）または同等な場合、オブジェクトからサブジェクトへの情報フローは許可される（読み込み操作）；**

b) If the sensitivity label of the object is greater than or equal to the sensitivity label of the subject; then the flow of information from the subject to the object is permitted (a write operation);
b) **オブジェクトの機密ラベルがサブジェクトの機密ラベルを上回っているまたは同等な場合、サブジェクトからオブジェクトへの情報フローは許可される（書き込み操作）；**

Application Note: where the label of the object is greater than the label of the subject, this is a blind append (i.e., write does not imply a read).
適用上の注釈：オブジェクトのラベルがサブジェクトのラベルを上回っている場合、これは無条件アペンドになります（すなわち書き込みは無条件での読み込みを意味しません）。

c) If the information flow is between objects, the sensitivity label of the destination object must be greater than (see FDP_IFF_EXP.2.7) or equal to the sensitivity label of the source object.
c) **情報フローがオブジェクト間で起きる場合、送信先オブジェクトの機密ラベルは送信元オブジェクトの機密ラベルを上回っているか（FDP_IFF_EXP.2.7 参照）同等でなくてはならない。**

FDP_IFF_EXP.2.3(1) The TSF shall **provide authorized administrators with a MAC-exempt capability by *[assignment: list of means of invoking MAC-exempt rules]***.
FDP_IFF_EXP.2.3(1) TSF **は、［割付：MAC を免除される規則を行使する手段のリスト］によって、許可管理者が** MAC **を免除される操作を行なう能力を提供しなければならない。**

FDP_IFF_EXP.2.4(1) The TSF shall provide the following administrator actions requiring MAC-exemption:
FDP_IFF_EXP.2.4(1) TSF **は、管理者に、以下の** MAC **の免除を必要とするアクションを提供しなければならない：**

a) Change a MAC label to another valid MAC label.
a) MAC **ラベルを他の適切な** MAC **ラベルへの変更**

b) *[assignment: list of additional administrator actions requiring MAC-exemption]*.
b) **［割付：追加の** MAC **免除を必要とする管理者のアクションのリスト］**

Application Note: These rules regulate the behavior for each of the roles identified under FMT_SMR.
適用上の注釈：これらの規則は、FMT_SMR で定義された各役割の動作を規制する。

FDP_IFF_EXP.2.5(1) The TSF shall explicitly authorize an information flow based on the following rules:
FDP_IFF_EXP.2.5(1) TSF **は、以下の規則に基づいて情報フローを明示的に承認しなければならない：**

a) A authorized user with an administrator assigned privilege may change a MAC label to another valid MAC label.
a) **管理者によって権限を与えられ、許可された利用者が** MAC **ラベルを他の適切な** MAC **ラベルに変更する。**

b) [*assignment: list of additional privileges that may be assigned by an administrator*].
b) **［管理者によって与えられた追加の権限のリスト］**

FDP_IFF_EXP.2.6(1) The TSF shall explicitly deny an information flow based on the following rules*: [assignment: rules based on security attributes that explicitly deny information flows]*.
FDP_IFF_EXP.2.6(1) TSF **は、以下の規則に基づいて情報フローを明示的に拒否しなければならない：［割付：情報フローを明示的に拒否するセキュリティ属性に基づいた規則］**

FDP_IFF_EXP.2.7(1) The TSF shall enforce the following relationships for any two valid **MAC** security attributes:
FDP_IFF_EXP.2.7(1) TSF **は、以下の関係を任意の２つの有効な** MAC **セキュリティ属性に対して実施しなければならない：**

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable;
a) **２つの有効なセキュリティ属性が与えられたとき、セキュリティ属性が同等か、一方のセキュリティ属性が他方より上か、またはセキュリティ属性が比較不能であるかどうかを判別する順序付け機能が存在する；**

4. 1. Sensitivity labels are equal if the hierarchical level of both labels are equal and the non-hierarchically category sets are identical;
4. 1. **両ラベルの階層的レベルが同等で、非階層的カテゴリーのセットが同等である場合、機密ラベルは同等；**

5. 2. Sensitivity label A is greater than sensitivity label B if the hierarchical level of A is greater than or equal to the hierarchical level of B, and the non-hierarchical category set of A is equal to or a superset of the nonhierarchical category set of B.

5. 2. A の階層的レベルが B の階層的レベルを上回っているもしくは同じで、A の非階層的カテゴリーセットが B の非階層的カテゴリーセットと同等もしくは上位集合となっている場合、機密ラベル A は機密ラベル B を上回っている；

6. 3. Sensitivity labels are incomparable if they are not equal and neither label is greater than the other as defined in 1 and 2 above.
6. 3. ラベルが同等でなく、かつ上の 1,2 で定義したようにいずれも一方を上回っていない場合、機密ラベルは比較不能

b) There exists a "least upper bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
b) ２つの有効なセキュリティ属性があり、いずれの有効なセキュリティ属性と同等、もしくは上回る有効なセキュリティ属性が存在する場合、セキュリティ属性のセットに " 最小上限 " が存在する。

c) There exists a "greatest lower bound" in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.
c) ２つの有効なセキュリティ属性があり、いずれの有効なセキュリティ属性をも上回らない有効なセキュリティ属性が存在する場合、セキュリティ属性のセットに" 最大下限 "が存在する。

5.3.5.2 Explicit: Hierarchical Security Attributes (for Mandatory Integrity Control) (FDP_IFF_EXP.2(2))

5.3.5.2 明示的要件：（必須完全制御の）階層的セキュリティ属性（FDP_IFF_EXP.2(2)）

FDP_IFF_EXP.2.1(2) The TSF shall enforce the **Mandatory Integrity Control policy** based on the following types of subjects, **objects,** and integrity attributes:
FDP_IFF_EXP.2.1(2) TSF は、以下のサブジェクト、オブジェクト、完全属性の種別に基づいて必須完全制御方針を実施しなければならない：

a) ***[Assignment: list of all subjects];***
a) ［割付：全てのサブジェクトのリスト］

b) the integrity attribute of each subject;
b) 各サブジェクトの完全属性；

c) ***[Assignment: list of all objects];***
c) ［割付：全てのオブジェクトのリスト］

d) the integrity attribute of each object;
d) 各オブジェクトの完全属性；

e) ***[Assignment: any additional security attributes].***

e) ［割付：追加のセキュリティ属性］

Application Note: An example of such integrity attributes is labels cited in the Biba Integrity policy.
適用上の注釈：このような完全属性の例は、Biba Integrity ポリシーで前述したラベルです。

FDP_IFF_EXP.2.2(2) The TSF shall permit an information flow **among subjects and objects** based on the following rules:
FDP_IFF_USEXP.2.2(2) TSF は、サブジェクトとオブジェクト間の以下の規則に基づいて、情報フローを許可しなければならない：

[Selection:
• For Hierarchical integrity attributes schemes:
［選択：
・階層的な完全属性の場合：

a) If the integrity label of the subject is greater than or equal to the integrity label of the object, then a write (the flow of information from the subject to the object) is permitted;
a) サブジェクトの完全ラベルがオブジェクトの完全ラベルを上回っている、または同等な場合、書き込み（サブジェクトからオブジェクトへの情報フロー）は許可される；

b) If the integrity label of the object is greater than or equal to the integrity label of the subject; then a read (the flow of information from the object to the subject) is permitted;
b) オブジェクトの完全ラベルがサブジェクトの完全ラベルを上回っている、または同等な場合、読み込み（オブジェクトからサブジェクトへの情報フロー）は許可される；

c) If the information flow is between objects, the integrity label of the source object must be greater than or equal to the integrity label of the destination object.
c) 情報フローがオブジェクト間で起きる場合、送信元オブジェクトの完全ラベルは送信先オブジェクトの完全ラベルを上回っているか同等でなくてはならない。

• For Non-hierarchical integrity attributes schemes:
・非階層的な完全属性の場合：

[*Assignment: Mandatory integrity rules that determine access based upon subject and object integrity attributes.*]]
［割付：サブジェクトとオブジェクトの完全属性に基づきアクセスを決定する必須完全規則］

Application note: The mandatory integrity rules are to enforce the mandatory integrity control policy for the system. Integrity focuses on controlling what data can be read into a subject's address space as well as what data can be modified by a subject. Examples of hierarchical controls include: preventing a high-integrity subject from reading or executing a low-integrity object, and a low-integrity subject from modifying a high-integrity object. An example of

non-hierarchical controls include: a rule must exist to that explicitly allows a subject to read, modify, or execute an object based on their integrity attributes.
適用上の注釈：必須完全規則は、システムの必須完全制御を実施します。完全性は、サブジェクトのアドレス空間にどのデータを読み込むか、やサブジェクトによってどのデータを書き換えるか、を制御することに焦点を当てます。階層的な制御の例には、完全性の上位のサブジェクトによる、下位のオブジェクトの読み込みや実行を防止することを含みます。非階層的な制御の例には、サブジェクトが、完全属性に基づいて、オブジェクトを読み込む、書き換える、または実行することを明示的に許可する規則が存在しなければならないことを含みます。

FDP_IFF_EXP.2.3(2) The TSF shall **provide authorized administrators with a MIC-exempt capability by *[assignment: list of means of invoking MIC-exempt rules]***.
FDP_IFF_EXP.2.3(2) TSF **は、［割付：MIC を免除される規則を行使する手段のリスト］によって、許可管理者が** MIC **を免除される操作を行う能力を提供しなければならない。**

FDP_IFF_EXP.2.4(2) The TSF shall provide the following administrator actions requiring MIC-exemption:
FDP_IFF_EXP.2.4(2) TSF **は、管理者に、以下の** MIC **の免除を必要とするアクションを提供しなければならない：**

a) Change a MIC label to another valid MIC label.
a) MIC **ラベルを他の適切な** MIC **ラベルへの変更**

*b) [*assignment: list of additional administrator actions requiring MIC-exemption*]*
b) ［**割付：追加の** MIC **免除を必要とする管理者のアクションのリスト**］

.ApplicationNote: These rules regulate the behavior for each of the roles identified under FMT_SMR.
適用上の注釈：これらの規則は、FMT_SMR **で定義された各役割の動作を規制する。**

FDP_IFF_EXP.2.5(2) The TSF shall explicitly authorize an information flow based on the following rules:
FDP_IFF_EXP.2.5(2) TSF **は、以下の規則に基づいて情報フローを明示的に承認しなければならない：**

a) A authorized user with an administrator assigned privilege may change a MIC label to another valid MIC label.
a) **管理者によって権限を与えられ、許可された利用者が** MIC **ラベルを他の適切な** MIC **ラベルに変更する。**

b) [*assignment: list of additional privileges that may be assigned by an administrator*].
b) ［**管理者によって与えられた追加の権限のリスト**］

FDP_IFF_EXP.2.6(2) The TSF shall explicitly deny an information flow based on the

following rules*: [assignment: rules, based on security attributes, that explicitly deny information flows].*
FDP_IFF_EXP.2.6(2) TSF は、以下の規則に基づいて情報フローを明示的に拒否しなければならない：[割付：情報フローを明示的に拒否するセキュリティ属性に基づいた規則]

FDP_IFF_EXP.2.7(2) The TSF shall enforce the following relationships for any two valid **MIC** security attributes:
FDP_IFF_EXP.2.7(2) TSF は、以下の関係を任意の２つの有効な MIC セキュリティ属性に対して実施しなければならない：

[Selection:
• For Hierarchical integrity attributes schemes:
[選択：
・階層的な完全属性の場合：

a) There exists an ordering function that, given two valid security attributes, determines if the security attributes are equal, if one security attribute is greater than the other, or if the security attributes are incomparable; and
a) ２つの有効なセキュリティ属性が与えられたとき、セキュリティ属性が同等か、一方のセキュリティ属性は他方を上回るか、またはそれらセキュリティ属性が比較不能であるかどうかを判別する順序付け機能が存在する；

b) There exists a “least upper bound” in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is greater than or equal to the two valid security attributes; and
b) どのような２つの有効なセキュリティ属性が与えられたときでも、いずれの有効なセキュリティ属性と同等か、もしくは上回る有効なセキュリティ属性が存在する場合、セキュリティ属性のセットに“最小上限”が存在する；そして

c) There exists a “greatest lower bound” in the set of security attributes, such that, given any two valid security attributes, there is a valid security attribute that is not greater than the two valid security attributes.
c) どのような２つの有効なセキュリティ属性が与えられたときでも、いずれの有効なセキュリティ属性をも上回らない有効なセキュリティ属性が存在する場合、セキュリティ属性のセットに“最大下限”が存在する。

• For Non-hierarchical integrity attributes schemes:
・非階層的な完全属性の場合：

There shall be only one applicable rule per subject/object attribute pair.]
サブジェクト/オブジェクト属性のペア毎にただ一つの適用可能な規則がなければならない。

5.3.5.3 Limited Illicit Information Flows (FDP_IFF.3)
5.3.5.3 制限付き不正情報フロー（FDP_IFF.3）

FDP_IFF.3.1 **Refinement**: The TSF shall enforce the **Mandatory Access Control policy** to **ensure that no illicit information flows exist which cross any cryptographic boundary**.
FDP_IFF.3.1 **詳細化：TSF は、暗号領域を越すような不正情報フローが発生しないようにするために、必須アクセス制御方針を実施しなければならない。**

Application Note: The analysis need not be performed on data other than that composing cryptographic keys and other critical cryptographic security parameters. The analysis for such flows is also covered by the AVA_CCA requirements.
適用上の注釈：暗号鍵や他の重要セキュリティパラメータを構成するデータ以外のデータに対しては分析を実施する必要はありません。このようなフローの分析は、AVA_CCA 要件でもカバーされています。

5.3.6 Import From Outside TSF Control (FDP_ITC)
5.3.6 TSF **制御外からのインポート**（FDP_ITC）

5.3.6.1 Import of User Data without Security Attributes (FDP_ITC.1)
5.3.6.1 **セキュリティ属性なしユーザデータのインポート**（FDP_ITC.1）

FDP_ITC.1.1 **Refinement:** The TSF shall enforce the **Mandatory Access Control and Mandatory Integrity Control policies** when importing **any unlabeled** user data, **or non-validated labeled user data** controlled under the SFP, from outside the TSC.
FDP_ITC.1.**1** **詳細化：TSF は、SFP に従って制御されているラベル無しユーザデータや有効でないラベルが付いているユーザデータを TSC 外からインポートするときは、必須アクセス制御と必須完全制御方針を実施しなければならない。**

Application Note: The "label" is the security attributes associated with the data. Validated labels are recognized labels that are cryptographically verified and originate from a source deemed trustworthy (e.g., by the authorized administrator).
適用上の注釈：" ラベル " はデータと結びつくセキュリティ属性である。有効なラベルとは、認可されたラベルのことで、信頼できると判断できるソース（たとえば許可管理者）によって生成され、暗号的に照合されている。

Application Note: For this family (FDP_ITC) the term "security attributes" refers only to the sensitivity labels of subject and objects.
適用上の注釈：当ファミリー（FDP_ITC）に於いて、" セキュリティ属性 " という用語は、サブジェクトとオブジェクトの機密ラベルのみを指す。

FDP_ITC.1.2 **Refinement:** The TSF shall ignore any security attributes associated with the **non-validated** user data when imported from outside the TSC.
FDP_ITC.1.**2** **詳細化：TSF は、TSC 外からインポートされるとき、有効でないユーザデータに関連づけられたいかなるセキュリティ属性も無視しなければならない。**

FDP_ITC.1.3 **Refinement:** The TSF shall enforce the following rules when importing

unlabeled or non-validated user data controlled under the SFP from outside the TSC:
FDP_ITC.1.3　詳細化：TSF は、SFP に従って制御されるラベル無し、または有効でないユーザデータを TSC 外からインポートするとき、以下の規則を実施しなければならない。

a) When importing data that has no validated MAC label (see FDP_ITC.2.5), the TSF shall allow the authorized administrator to specify that the data is to be labeled with (1) the label of the subject importing the data, (2) the label of the device by which the data is imported, or (3) the highest MAC label of data processed by the TOE;
a) 有効な MAC ラベル（FDP_ITC.2.5 参照）を持たないデータをインポートするとき、TSF は許可管理者が次のどのラベルをデータ付与するかを指定することを許可しなければならない。（1） データをインポートするサブジェクトのラベル（2） データをインポートするデバイスのラベル、（3） TOE で処理されるデータの最高 MAC ラベル；

Application Note: The authorized administrator must recognize that options 1 and 2 could result in data being improperly labeled. The most secure option is 3 followed by a manual review and appropriate labeling of the data. A complete discussion of the issues and the procedures for addressing them is expected to be included in the administrative guidance documents.
適用上の注釈：オプション（1）および（2）はデータにラベルが誤って付けられることがあることを許可管理者は認識しておく必要がある。最も安全なものはオプション（3）で、これはマニュアルレビューと適切なラベル付けでフォローされる。この項目とアドレッシングの手順についてはアドミニストラティブガイダンスに記載するのがよい。

b) When importing data that has no validated integrity label (see FDP_ITC.2.5), the TSF shall allow the authorized administrator to specify that the data is to be labeled with (1) the label of the subject importing the data, (2) the label of the device by which the data is imported, or (3) the lowest integrity label of data processed by the TOE;
b) 有効な完全ラベル（FDP_ITC.2.5 参照）を持たないデータをインポートするとき、TSF は許可管理者が次のどのラベルをデータ付与するかを指定することを許可しなければならない。（1） データをインポートするサブジェクトのラベル（2） データをインポートするデバイスのラベル、（3） TOE で処理されるデータの最低完全ラベル；

Application Note: The authorized administrator must recognize that options 1 and 2 could result in data being improperly labeled. The most secure option is 3 followed by a manual review and appropriate labeling of the data. A complete discussion of the issues and the procedures for addressing them is expected to be included in the administrative guidance documents.
適用上の注釈：オプション（1）および（2）はデータにラベルが誤って付けられることがあることを許可管理者は認識しておく必要がある。最も安全なものはオプション（3）で、これはマニュアルレビューと適切なラベル付けでフォローされる。この項目とアドレッシングの手順についてはアドミニストラティブガイダンスに記載するのがよい。

c) When importing data, the data is given restrictive Discretionary Access Control attributes limiting access to only the importer of the data;
c) データをインポートする時、データのインポーターに限定した限定的任意アクセス制御属性

が与えられる。;

d) *[Assignment: any additional importation control rules].*
d) [**割付：その他のインポート制御規則**]

Application Note: The ST author must explicitly state the rules under which authorized users can designate the security attributes of the mechanisms, or devices, used to import data without security attributes; and any attribute change must be audited. The ST author must also make it clear that mechanisms, or devices, used to import data without security attributes cannot also be used to import data with security attributes unless this change in state can only be done manually and is audited.
適用上の注釈：ST 作者は、セキュリティ属性を持たないデータをインポートするのに利用するメカニズムやデバイスセキュリティ属性を、許可ユーザーが指定できる規則を明確に記載しなければならない。属性の変更は全て監査されていなければならない。ST 作者は、セキュリティ属性を持たないデータをインポートするのに利用するメカニズムやデバイスを利用してセキュリティ属性を持つデータをインポートすることができないことも明確にしなければならないが、この状態が手動で変更され、かつ監査されている場合はその限りではない。

5.3.6.2 Import of User Data with Security Attributes (FDP_ITC.2)
5.3.6.2　セキュリティ属性付きユーザデータのインポート（FDP_ITC.２）

FDP_ITC.2.1 **Refinement:** The TSF shall enforce the **Mandatory Access Control and Mandatory Integrity Control policies,** when importing **validated labeled** user data, controlled under the SFP, from outside the TSC.
FDP_ITC.２.1　**詳細化：TSF は、SFP に従って制御されている有効ラベル付きユーザデータを TSC 外からインポートするときは、必須アクセス制御と必須完全制御方針を実施しなければならない。**

Application Note: The "label" is the security attributes associated with the data. Validated labels are recognized labels that are cryptographically verified and originate from a source deemed trustworthy (e.g., by the authorized administrator).
適用上の注釈：" ラベル "はデータと結びつくセキュリティ属性である。有効なラベルとは、認可されたラベルのことで、信頼できると判断できるソース（たとえば許可管理者）によって生成され、暗号的に照合されている。

FDP_ITC.2.2 **Refinement:** The TSF shall use the security attributes associated with the imported **validated labeled** user data.
FDP_ITC.２.２　**詳細化：TSF は、インポートされる有効ラベル付きユーザデータに関連付けられたセキュリティ属性を使用しなければならない。**

FDP_ITC.2.3 **Refinement:** The TSF shall ensure that the protocol used provides for the **correct** unambiguous association between the **imported security attributes** and the **imported** user data.[16]
FDP_ITC.２.３　**詳細化：TSF は、使用されるプロトコルが、インポートされた有効ラベルとインポートされたユーザデータ間で正確な曖昧さのない関連性を備えていることを保証しなけ**

ればならない。16

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.２.４　TSF は、インポートされるユーザデータのセキュリティ属性の解釈が、ユーザデータの生成元によって意図されたとおりであることを保証しなければならない。

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC:
FDP_ITC.２.５　TSF は、SFP によって制御されているユーザデータを TSC 外からインポートするときは、以下の規則を実施しなければならない。

a) A cryptographic mechanism (e.g., cryptographic signature) shall be used to validate the security attributes.
a) セキュリティ属性の確認をするために暗号メカニズム（たとえば暗号署名）を利用しなければならない。

b) If the validation mechanism fails, the data shall be treated as if it had no security attributes.
b) 確認メカニズムが失敗したとき、データは全くセキュリティ属性を持たないものとして取り扱わなくてはならない。

Application Note: The process for treating data with no security attributes is defined in FDP_ITC.1.
適用上の注釈：セキュリティ属性を持たないデータの取り扱いは FDP_ITC.１にて定義されている。

c) If the data contains security attributes that are not recognized by the TOE, yet the TOE has a means of obtaining the security attributes' scheme used by the origin of the data, then the TOE must assign the data its own representation of the equivalent security attributes.
c)　TOE によって確認できないセキュリティ属性を含むデータがあるが、TOE はデータの送信元で利用されているセキュリティ属性スキームを手に入れる手段を持つ場合、TOE はデータに対してそのセキュリティ属性と同等な属性を付与しなければならない。

d) If the data contains any security attributes that are not recognized by the TOE, and the TOE does not have a means of obtaining the security attributes' scheme used by the origin of the data, then those security attributes must be rejected, while recognized security attributes may still be accepted;
d) TOE によって確認できないセキュリティ属性を含むデータがあり、かつ TOE がデータの送信元で利用されているセキュリティ属性スキームを手に入れる手段を持たない場合、このセキュリティ属性は拒否されなければならないが、認められているセキュリティ属性に関しては許可される。

Application Note: The process for treating data with no security attributes is defined in FDP_ITC.1.

適用上の注釈：セキュリティ属性を持たないデータの取り扱いは FDP_ITC.1 にて定義されている。

e) If the source of the imported data is not considered trustworthy according to the Organizational Security Policy (e.g., via a certificate mechanism), then the data must be treated as if it had no security attributes.
e) インポートしたデータの起点が組織セキュリティ方針（たとえば証明書メカニズム経由で）により信用できないと判断された場合は、データはセキュリティ属性を持たないものとして取り扱わなければならない。

Application Note: The process for treating data with no security attributes is defined in FDP_ITC.1.
適用上の注釈：セキュリティ属性を持たないデータの取り扱いは FDP_ITC.1 にて定義されている。

f) *[Assignment: any additional importation control rules].*
f) [割付：その他のインポート制御規則]

Application Note: The ST must describe the labeling system that is used by the TOE, so that integrators can avoid interconnecting TOEs whose bit-pattern representations for labels are in conflict. If the TOE includes a mechanism for countering such potential conflicts (e.g., a label representation translator, a means of accepting labels only from certain locations, etc), the rules enforced by such a mechanism should be included in the rules of FDP_ITC.2.5.
適用上の注釈：ラベルを示すビットパターンが異なる TOE をインテグレータが相互接続してしまうことを防ぐために、ST は TOE にて利用されるラベル付けシステムに関して説明しなければならない。TOE 自体がそのような違いを克服するメカニズムを備えている場合（たとえばラベル代表変換、特定場所のみからのラベルを受け入れる手段、etc）、そのようなメカニズムによって施行される規則は、FDP_ITC.2.5 の規則に含めなければならない。

5.3.7 Internal TOE Transfer (FDP_ITT)
5.3.7 TOE 内転送（FDP_ITT）

5.3.7.1 Basic Internal Transfer Protection (FDP_ITT.1)
5.3.7.1 基本内部転送保護（FDP_ITT.1）

FDP_ITT.1.1 **Refinement:** The TSF shall prevent the disclosure **and** modification of user data when it is transmitted between physically-separated parts of the TOE **through the use of TSF-provided cryptographic services**.17

FDP_ITT.1.1 詳細化：TSF は TSF の暗号サービスを使って、TOE の物理的分離されたパーツ間を転送される時、暴露や改変を未然に防がなければならない。17

Application Note: This requirement applies to transmissions between physically-separated parts of the TOE whose intercommunication is not protected by the environment. It does not apply to transmissions between the TOE and another IT system.

適用上の注釈：この要件は物理的に離れたパーツ間で通信が保護されてない場合の TOE 間通信に適用され、TOE と他の IT システム間の通信には適用されない。

5.3.8 Residual Information Protection (FDP_RIP)

5.3.8 残存情報保護（FDP_RIP）

5.3.8.1 Full Residual Information Protection (FDP_RIP.2)

5.3.8.1 全残存情報保護（FDP_RIP.２）

FDP_RIP.2.1 **Refinement:** The TSF shall ensure that any previous information content of a resource is made unavailable upon the *[selection: allocation of the resource to, deallocation of the resource from]* all objects **other than those associated with cryptographic keys and critical cryptographic security parameters as described in FCS_CKM.4.1 and FCS_CKM_EXP.2.5**.

FDP_RIP.２.１ 詳細化：TSF は、暗号鍵や、FCS_CKM.4.1 や FCS_CKM_EXP.2.5 で説明している重要な暗号セキュリティパラメータに関するものを除いて全てのオブジェクト[選択：への資源の割り当て、からの資源の割り当て解除]に於いて、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

Application Note: This requirement applies to all resources except for cryptographic keys and critical cryptographic security parameters governed by or used by the TSF; it includes resources used to store data and attributes. It also includes the encrypted representation of information. Residual information protection for cryptographic data is covered in class FCS.

適用上の注釈：この要件は暗号鍵や重要な暗号セキュリティパラメータを除いて、TSF によって管理されまたは利用される全ての資源に対して適用される。データや属性を保管するのに利用する資源も含まれる。データの暗号化されたものも含まれる。暗号データの残存情報の保護は FCS でカバーされている。

Application Note: Clearing the content of resources on deallocation is sufficient to satisfy this requirement, provided that unallocated resources will not accumulate new information until they are allocated again.

適用上の注釈：割当て解除された資源が再度割当てされるまで新たな情報を蓄積しないと言う条件のもと、割当て解除時に資源の内容をクリアすることで十分この要件を満たす。

16 の注 セキュリティ属性を特定するため 有効ラベルに変更した
17 の注 詳細化をはっきり書いたので、割付を削除した

5.4 Identification and Authentication (FIA)

5.4. 識別と認証（FIA）

5.4.1 Authentication Failures (FIA_AFL)

5.4.1 認証失敗（FIA_AFL）

5.4.1.1 Authentication Failure Handling (FIA_AFL.1)

5.4.1.1 認証失敗時の取り扱い(FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when **an authorized administrator configurable positive integer of consecutive** unsuccessful authentication attempts occur related to **any authorized user authentication process**.

FIA_AFL.1.1 TSF は、全ての許可された利用者の認証過程に関して、許可管理者が定義可能な正の整数回の連続した不成功認証試行が生じたことを検出しなければならない。

FIA_AFL.1.2 **Refinement:** When the defined number of **consecutive** unsuccessful authentication attempts has been met or surpassed, the TSF shall:

FIA_AFL.1.2 詳細化:連続した不成功の認証試行が定義した回数に達するか上回ったとき、TSF は以下を実施しなければならない：

a) For all administrator accounts, disable the account for an authorized administrator configurable time period;

a) 全ての管理者アカウントに対しては、許可管理者の設定可能期間アカウントを無効にする；

b) For all other accounts, disable the user logon account until it is re-enabled by the authorized administrator.

b) その他のアカウントに対しては、許可管理者によって再度有効にされるまでユーザログオンアカウントを無効にする

c) For all disabled accounts, respond with an "account disabled" message without attempting any type of authentication.

c) 全ての無効なアカウントに対しては、いずれの認証も認めずに" このアカウントは無効にされました（account disabled）" とメッセージを返す。

Application Note: "Consecutive unsuccessful authentication attempts" is the total number of unsuccessful attempts that occur, in order, prior to a successful authentication attempt. For distributed systems, the TOE must reconcile unsuccessful attempts across nodes in accordance with FPT_TRC_EXP.1.

適用上の注釈:" 連続した不成功の認証試行 " とは、順番に、成功した認証試行より前に発生した不成功認証試行の合計数のことである。分散システムのために、TOE は、FPT_TRC_EXP.1 に従ってノード間の不成功試行を調整しなければならない。

5.4.2 User Attribute Definition (FIA_ATD)

5.4.2 ユーザ属性定義（FIA_ATD）

5.4.2.1 User Attribute Definition (FIA_ATD.1)

5.4.2.1 ユーザ属性定義（FIA_ATD.1）

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

FIA_ATD.1.1 TSF は、個々のユーザに属する以下のセキュリティ属性のリストを維持しなければならない：

a) unique identifier;

a) 一意の識別子；

b) group memberships;

b) グループメンバーシップ；

c) authentication data;

c) 認証データ；

d) sensitivity level;

d) 機密レベル

e) integrity level;

e) 完全レベル；

f) security-relevant roles (see FMT_SMR.2);

f) セキュリティ関連役割（FMT_SMR.2 参照）；

g) ***[Assignment: Any security attributes related to cryptographic function (e.g., certificate used to represent the user)]*****; and**

g) ［割付：暗号機能に関連する任意のセキュリティ属性（たとえばユーザを代表するのに利用する証明書)］そして

h) ***[Assignment: Any other security-relevant authorizations or attributes (e.g., privilege)].***

h)［割付：その他のセキュリティ関連の許可又は属性（たとえば特権)］

Application Note: Group membership may be expressed in a number of ways: a list per user specifying to which groups the user belongs, a list per group which includes which users are members, or implicit association between certain user identities and certain groups.

適用上の注釈:グループメンバーシップは様々な形式で表現されることがある：ユーザがどのグループに所属するかを示すユーザ毎のリスト;どのユーザが所属しているかを示すグループ毎のリスト;または特定のユーザ識別情報と特定のグループ間での関連性。

Application Note: A TOE may have two forms of user and group identities which have a unique mapping between the representations.

適用上の注釈:TOE では、ユーザ識別とグループ識別の 2 形式を保持していることもあり、それらの表現と一意に紐付けられている。

Application Note: It is possible that the notion of privilege is tied to the security-relevant roles (item f).

適用上の注釈:特権の概念は、セキュリティ関連役割と結びつけることも可能である。

5.4.3 Specification of Secrets (FIA_SOS)

5.4.3 **秘密についての仕様**（FIA_SOS）

5.4.3.1 Verification of Secrets (FIA_SOS.1)

5.4.3.1 **秘密の検証**（FIA_SOS.1）

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **the following:**

FIA_SOS.1.1 TSF **は、秘密が以下に合致することを検証するメカニズムを提供しなければならない**:

a) For each attempt to use the authentication mechanism, the probability that a random attempt will succeed is less than one in 5 x 10_{15};

a) **認証メカニズムを使用するそれぞれの試みで、無作為の試みが成功する確率は** 1/**5** x1015 **よりも少ない；**

Application Note: This can be achieved with a password of eight characters, assuming an alphabet of 92 characters.

適用上の注釈:これは、92 種類の文字セットを想定して８文字以上のパスワードを設定することによって達成できる。

b) The authentication mechanism must provide the capability for an administrator to specify the conditions that need to be met before an individual user can reuse a secret;

b) 認証メカニズムは、個々のユーザが秘密を再利用できる前に、満たされる必要がある条件を指定する能力を管理者に供給しなければならない。

c) The authentication mechanism must provide a delay such that there can be no more than ten attempts per minute; and

c) 認証メカニズムは、1 分で 10 回以上の試みができないように、遅延時間を提供しなければならない；そして

d) Any feedback given during an attempt to use the authentication mechanism will not reduce the probability below the above metrics.

d) 認証メカニズム試行時のフィードバックによって、上述のメトリックを下回る確率になることはない。

Application Note: The ST specifies the method of authentication.
Where authentication is provided by a password mechanism, the ST shows that the restrictions upon passwords (length, alphabet, conditions for reuse (e.g., time period, number of intermediate secrets), and other characteristics) result in a password space conforming to items (a) and (b) above, as well as characterize the delay to show conformance to item (c) above. Where authentication is provided by a mechanism other than passwords, the ST shows the authentication method has a low probability equivalent to item (a) above that authentication data can be forged or guessed.

適用上の注釈:ST は認証の方式を明確にしなければならない。パスワードメカニズムによって認証が提供される場合、ST はパスワードに於ける制限（長さ、アルファベット、そして他の特性）により、パスワードスペースは上記項目 a)に適合し、延滞時間が上記項目 b)に適合することを示さなければならない。パスワード以外のメカニズムで認証が提供される場合、ST はその認証メカニズムの認証データが偽造されたり、推定される確率が低いことを示さなければならない。

5.4.4 User Authentication (FIA_UAU)

5.4.4 ユーザ認証（FIA_UAU）

5.4.4.1 Timing of Authentication (FIA_UAU.1)

5.4.4.1 認証のタイミング（FIA_UAU.1）

FIA_UAU.1.1 **Refinement:** The TSF shall allow **read access to *public objects*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.1 **詳細化：TSF は、ユーザが認証される前にユーザに代わって行われる［割付：公開オブジェクトのリスト］への読み込みアクセスを許可しなければならない。**

FIA_UAU.1.2 **Refinement:** The TSF shall require each user to be successfully authenticated **(i.e., an exact match between the user's entered data and the stored TSF authentication data)** before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1.2 **詳細化：TSF は、そのユーザを代行する他の TSF 仲介アクションを許可する前に、各ユーザに認証が成功（すなわちユーザの入力データと保管 TSF 認証データの完全な一致）することを要求しなければならない。**

Application Note: The entire entered user's authentication data must exactly match the entire stored data. No other parameters such as length of password should be used to short-circuit the authentication verification.

適用上の注釈:入力されたユーザの認証データ全ては保管されたデータ全てと完全に一致しなければならない。パスワード長といったその他のパラメータによって認証照合が短絡化されてはならない。

5.4.4.2 Re-authenticating (FIA_UAU.6)

5.4.4.2 再認証(FIA_UAU.6)

FIA_UAU.6.1 **Refinement:** The TSF shall re-authenticate the user **when changing authentication data**.[18]

FIA_UAU.6.1 **詳細化：認証データ 18 を変更する時、TSF はユーザを再認証する。**

5.4.4.3 Protected Authentication Feedback (FIA_UAU.7)

5.4.4.3 保護された認証フィードバック（FIA_UAU.7）

FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the user while the authentication is in progress.

FIA_UAU.7.1 **詳細化：TSF は、認証を行っている間、重要事項が解らないフィードバックだけをユーザに提供しなければならない。**

Application Note: "Obscured feedback" implies the TSF does not produce a visible display of any authentication data entered by a user (such as the echoing of a password), although an obscured indication of progress may be provided (such as an asterisk for each character). It also implies that the TSF does not return any information during the authentication process to the user, which may provide any indication of the authentication data.

適用上の注釈:" 重要事項が解らないフィードバック " とは、TSF がユーザによって入力された認証データの可視表示を生成しないこと（たとえばパスワードを繰り返す）を意味するが、

進行状況があいまいに表示されることもある（たとえば各文字毎にアスタリスクを表示）。それはまた、TSF がユーザの認証中には、いかなる認証データの表示を生成しないことを意味する。

5.4.5 User Identification (FIA_UID)

5.4.5 ユーザ識別（FIA_UID）

5.4.5.1 Timing of Identification (FIA_UID.1)

5.4.5.1 識別のタイミング（FIA_UID.1））

FIA_UID.1.1 The TSF shall allow **read access to *public objects*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.1 TSF は、ユーザが識別される前にユーザに代わって実行される公開オブジェクトへの読み込みアクセスを許可しなければならない。

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID.1.2 TSF は、そのユーザを代行する他の TSF 仲介アクションを許可する前に、各ユーザの識別が成功することを要求しなければならない。

5.4.6 User-Subject Binding (FIA_USB)

5.4.6 ユーザ・サブジェクト結合（FIA_USB）

5.4.6.1 User-Subject Binding (FIA_USB.1)

5.4.6.1 ユーザ・サブジェクト結合（FIA_USB.1）

FIA_USB.1.1 **Refinement:** The TSF shall associate the **following** user security attributes with subjects acting on behalf of that user:19

FIA_USB.1.1 詳細化：TSF は、以下のユーザセキュリティ属性を、そのユーザ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：19

a) The unique user identity that is associated with auditable events;

a) 監査対象事象に関連するユーザの一意識別子；

b) The user identity or identities that are used to enforce the Discretionary Access Control Policy;

b) 任意アクセス制御方針を執行するのに利用する１つ、または複数のユーザ識別子；

Application Note: The DAC and audit policies require that each subject acting on behalf of a user has a user identity associated with the subject. While this identity is typically the one used at the time of identification to the system, the DAC policy enforced by the TSF may include provisions for making access decisions based upon a different user identity, such as the "set user ID (su)" command in UNIX.

適用上の注釈:ユーザを代行して行動する各サブジェクトが、そのサブジェクトに関連付けられたユーザ識別子を含むことを DAC と監査方針は要求します。この識別子は典型的にはシステムで識別される時に利用されるものである一方、TSF によって実施される DAC 方針では UNIX の" set user ID (su) "といった異なるユーザ識別子をもとにアクセスの判断する規定を含むことができる。

c) The group identity or identities that are used to enforce the Discretionary Access Control Policy; and

c) 任意アクセス制御方針を執行するのに利用する１つ、または複数のグループ識別子；そして

d) The user sensitivity level that is used to enforce the Mandatory Access Control policy;

d) 必須アクセス制御方針を執行するのに利用するユーザ機密レベル；

e) The user integrity level that is used to enforce the Mandatory Integrity Control policy;

e) 必須完全制御方針を執行するのに利用するユーザ完全レベル；

f) The user's authorized roles;

f) ユーザの認可された役割

g) *[Assignment: other list of user security attributes related to cryptographic function (e.g., certificate used to represent the user, key used to encrypt data on behalf of the user)].*

g) ［割付：暗号機能に関連するユーザセキュリティ属性の他のリスト（たとえばユーザを代表するのに利用する証明書、ユーザに代わりデータを暗号化するのに利用する鍵)］；

Application Note: The attributes listed in FIA_USB.1 should be comparable to those listed in FIA_ATD.1. For example, the user's current sensitivity level (FIA_USB.1 item d) should be within the set of the user's clearances (FIA_ATD.1 item d).

適用上の注釈:FIA_USB_US_INTERP_EXP.1 における属性リストは FIA_ATD.1.でのリストに相当する。(例えば、ユーザーの最新機密レベル (FIA_USB_US_INTERP_EXP.1 項目 d)は (FIA_ATD.1 i 項目 d)のユーザークリアランスのセットにあるべきである).

5.5 Security Management (FMT)

5.5 セキュリティ管理 (FMT)

5.5.1 Management of Functions in TSF (FMT_MOF)

5.5.1 TSFにおける機能の管理 (FMT_MOF)

5.5.1.1 Management of Security Functions Behavior (for specification of auditable events) (FMT_MOF.1(1))

5.5.1.1 セキュリティ機能のふるまいの管理 (監査可能なイベントの仕様について) (FMT_MOF.1(1))

FMT_MOF.1.1(1) **Refinement:** The TSF shall restrict the ability to disable and enable the **audit** functions **and to specify which events are to be audited (see FAU_SEL.1.1)** to **the authorized administrators.**

FMT_MOF.1.1(1) 詳細化: TSFは、監査機能の有効化/無効化、および、監査対象となるイベントを特定する(FAU_SEL.1.1参照)能力を許可管理者に制限しなければならない。

Application Note: To "specify" means the ability to select what events will be audited.

適用上の注釈：「特定する」とは、どのイベントが監査されるかを選ぶことを意味する。

5.5.1.2 Management of Security Functions Behavior (for authentication data) (FMT_MOF.1(2))

5.5.1.2 セキュリティ機能のふるまいの管理 (認証データについて) (FMT_MOF.1(2))

FMT_MOF.1.1(2) **Refinement:** The TSF shall restrict the ability to **manage** the **values** of security attributes **associated with user authentication data** to **authorized administrators.** 20

FMT_MOF.1.1(2) 詳細化: TSFは、利用者認証データに関連したセキュリティ属性値を管理する能力を許可管理者に制限しなければならない。20

Application Note: The word "manage" includes but is not limited to create, initialize, change default, modify, delete, clear, append, and query. Security attributes associated with user authentication data include password length, expiration, history, etc.

適用上の注釈：「管理」とは、生成、初期化、デフォルト値の変更、改変、削除、クリア、追加、問い合わせを含むが、それらに限定されるものではない。利用者認証データに関連づけられたセキュリティ属性はパスワードの長さ、有効期限、履歴、その他を含む。

5.5.2 Management of Security Attributes (FMT_MSA)

5.5.2 セキュリティ属性の管理 (FMT_MSA)

5.5.2.1 Management of Security Attributes (for Discretionary Access Control) (FMT_MSA.1(1))

5.5.2.1 セキュリティ属性の管理(任意アクセス制御について) (FMT_MSA.1(1))

FMT_MSA.1.1(1) The TSF shall enforce the **Discretionary Access Control policy** to restrict the ability to **change** the **value of object** security attributes **to authorized administrators and owners of the object.** 21

FMT_MSA.1.1(1) TSFは、オブジェクトセキュリティ属性値を変更する能力を許可管理者およびオブジェクト所有者に制限するために任意アクセス制御ポリシを実施しなければならない。21

5.5.2.2 Management of Security Attributes (for Mandatory Access Control) (FMT_MSA.1(2))

5.5.2.2 セキュリティ属性の管理(強制アクセス制御について) (FMT_MSA.1(2))

FMT_MSA.1.1(2) The TSF shall enforce the **Mandatory Access Control policy** to restrict the ability to **change** the **value of the sensitivity label associated with an object** to **authorized administrators**. 22

FMT_MSA.1.1(2) TSFは、オブジェクトに関連した機密ラベルの値を変更する能力を許可管理者に制限するために強制アクセス制御のポリシを実施しなければならない。22

5.5.2.3 Management of Security Attributes (for Mandatory Integrity Control) (FMT_MSA.1(3))

5.5.2.3 セキュリティ属性の管理 (強制完全制御について) (FMT_MSA.1(3))

FMT_MSA.1.1(3) The TSF shall enforce the **Mandatory Integrity Control policy** to restrict the ability to **change** the **value of the integrity label associated with an object** to **authorized administrators**. 23

FMT_MSA.1.1(3) TSFは、オブジェクトに関連した整合性ラベルの値を変更する能力を許可管理者に制限するために強制完全制御のポリシを実施しなければならない。23

5.5.2.4 Secure Security Attributes (FMT_MSA.2)

5.5.2.4 セキュアなセキュリティ属性 (FMT_MSA.2)

FMT_MSA.2.1 **Refinement:** The TSF shall ensure that only valid values are accepted for security attributes. 24

FMT_MSA.2.1 詳細化: TSFは有効な値だけがセキュリティ属性として受け入れられることを保証しなければならない。24

Application Note: Valid implies that the values fall within an appropriate range for that attribute (e.g., the password length attribute must be a non-negative integer).

適用上の注釈：「有効」とは属性が適当な範囲の間におさまることを意味する。（例：パスワードの長さの属性は非負の整数でなければならない）

5.5.2.5 Static Attributes Initialization (FMT_MSA.3)

5.5.2.5 静的属性初期化 (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **Discretionary Access Control policy** to provide restrictive default values for security attributes that are used to enforce the SPS.

FMT_MSA.3.1 TSFは、SFPで使用されるセキュリティ属性について制限されたデフォルト値を提供するために任意アクセス制御ポリシを実施しなければならない。

Application Note: The TOE must provide protection by default for all objects at creation time. This may allow authorized users to explicitly specify the desired access controls upon the object at its creation, provided that there is no window of vulnerability through which unauthorized access may be gained to newly-created objects.

適用上の注釈：TOEは全てのオブジェクトについてその生成時にデフォルトによる防御を提供しなければならない。これにより、新しく生成されたオブジェクトに対して認可されていないアクセスが可能となるような脆弱性が生じないことを前提とした上で、認可された利用者はオブジェクトの生成時に明確に希望するアクセス権限を特定することができる。

FMT_MSA.3.2 The TSF shall allow the **authorized administrator** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3.2 TSFは、オブジェクトや情報が生成されるとき、許可管理者がデフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

5.5.3 Management of TSF Data (FMT_MTD)

5.5.3 TSFデータの管理 (FMT_MTD)

5.5.3.1 Management of TSF Data (for general TSF data) (FMT_MTD.1(1))

5.5.3.1 TSFデータの管理 (一般的なTSFデータについて) (FMT_MTD.1(1))

FMT_MTD.1.1(1) The TSF shall restrict the ability to **manage** the **security-relevant TSF data except for audit records, user security attributes, authentication data,**

and critical cryptographic security parameters to **authorized administrators**.

FMT_MTD.1.1(1) TSFは、監査記録、利用者セキュリティ属性、認証データおよび重要な暗号セキュリティパラメータを除くセキュリティ関連のTSFデータを管理する能力を許可管理者に制限しなければならない。

Application Note: The word "manage" includes but is not limited to create, initialize, change default, modify, delete, clear, append, and query. Security attributes associated with user authentication data include password length, password expiration, password history, etc. The restrictions for audit records, user security attributes, authentication data, and critical cryptographic security parameters are specified below.

適用上の注釈：「管理(manage)」とは、生成、初期化、デフォルト値の変更、改変、削除、クリア、追加、問い合わせを含むが、それらに限定されるものではない。利用者認証データに関連づけられたセキュリティ属性はパスワードの長さ、有効期限、履歴、その他を含む。監査記録、利用者セキュリティ属性、認証データ、重要な暗号セキュリティパラメータに対する管理の制限について以下に示す。

5.5.3.2 Management of TSF Data (for audit data) (FMT_MTD.1(2))

5.5.3.2 TSFデータの管理 (監査データについて) (FMT_MTD.1(2))

FMT_MTD.1.1(2) The TSF shall restrict the ability to query, delete, and clear the **audit records** to **authorized administrators**.

FMT_MTD.1.1(2) TSFは、監査記録の問い合わせ、削除、クリアする権限を許可管理者に制限しなければならない。

5.5.3.3 Management of TSF Data (for previously written audit records) FMT_MTD.1(3))

5.5.3.3 TSFデータの管理 (より以前に作成された監査データについて) (FMT_MTD.1(3))

FMT_MTD.1.1(3) **Refinement:** The TSF shall **prevent** modification of **previously written audit records**.

FMT_MTD.1.1(3) 詳細化: TSFは、前回の監査記録が改変されないよう防止しなければならない。

5.5.3.4 Management of TSF Data (for initialization of user security attributes) (FMT_MTD.1(4))

5.5.3.4 TSFデータの管理 (利用者セキュリティ属性の初期化について) (FMT_MTD.1(4))

FMT_MTD.1.1(4) The TSF shall restrict the ability to **initialize user security attributes** to **authorized administrators**.

FMT_MTD.1.1(4) TSFは、利用者セキュリティ属性を初期化する能力を許可管理者に制限しな

ければならない。

5.5.3.5 Management of TSF Data (for modification of user security attributes, other than authentication data) (FMT_MTD.1(5))

5.5.3.5 TSF**データの管理 (認証データ以外の利用者セキュリティ属性について)** (FMT_MTD.1(5))

FMT_MTD.1.1(5) The TSF shall restrict the ability to modify **user security attributes, other than authentication data,** to **authorized administrators.**

FMT_MTD.1.1(5) TSF**は、認証データ以外については利用者セキュリティ属性の改変を行う能力を許可管理者に制限しなければならない。**

5.5.3.6 Management of TSF Data (for modification of authentication data) (FMT_MTD.1(6))

5.5.3.6 TSF**データの管理 (認証データの改変について)** (FMT_MTD.1(6))

FMT_MTD.1.1(6) The TSF shall restrict the ability to modify **authentication data** to **authorized administrators and users authorized to modify their own authentication data.**

FMT_MTD.1.1(6) TSF**は、認証データを改変する能力を許可管理者および自身の認証データ改変を許可された利用者に制限しなければならない。**

5.5.3.7 Management of TSF Data (for reading of authentication data)(FMT_MTD.1(7))

5.5.3.7 TSF**データの管理 (認証データの読み込みについて)** (FMT_MTD.1(7))

FMT_MTD.1.1(7) **Refinement:** The TSF shall **prevent reading of authentication data**.26

FMT_MTD.1.1(7) **詳細化**: TSF**は、認証データの読み込みを防止しなければならない。**26

5.5.3.8 Management of TSF Data (for critical cryptographic security parameters) (FMT_MTD.1(8))

5.5.3.8 TSF**データの管理 (重要なセキュリティ暗号パラメータについて)** (FMT_MTD.1(8))

FMT_MTD.1.1(8) The TSF shall restrict the ability to **manage** the **critical cryptographic security parameters and data related to cryptographic configuration** to **cryptographic administrators**.

FMT_MTD.1.1(8) TSF**は、重要な暗号セキュリティパラメータと暗号化設定に関する設定を管理する能力を暗号管理者に制限しなければならない。**

Application Note: The word "manage" includes but is not limited to create, initialize, change default, modify, delete, clear, append, and query. Critical cryptographic security parameters are defined in the glossary where examples are also provided. Examples of data related to cryptographic configuration include, but are not limited to: setting of the cryptographic algorithm, setting the cryptographic mode of operation, setting the key length, setting a hash digest size, etc."

適用上の注釈：「管理(manage)」とは、生成、初期化、デフォルト値の変更、改変、削除、クリア、追加、問い合わせを含むが、それらに限定されるものではない。重要な暗号セキュリティパラメータは実例と一緒に「語彙集」の中で定義される。暗号化設定に関するデータの例としては、暗号アルゴリズムと暗号操作のモードの設定、キーの長さの設定、ハッシュダイジェストの長さの設定などを含むが、それらに限定されるものではない。

5.5.4 Revocation (FMT_REV)

5.5.4 **取消し** (FMT_REV)

5.5.4.1 Revocation (to authorized administrators) (FMT_REV.1(1))

5.5.4.1 **取消し (許可管理者に対して)** (FMT_REV.1(1))

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to **authorized administrators**.

FMT_REV.1.1(1)TSF**は、**TSC**の範囲内で、利用者に関連したセキュリティ属性を取消す能力を許可管理者に制限しなければならない。**

Application Note: The phrase "revoke security attributes" means to change attributes so that access is revoked.

適用上の注釈：「セキュリティ属性を取消す(revoke security attributes)」とは、アクセスが取消されるような属性の変更を意味する。

FMT_REV.1.2(1) **Refinement:** The TSF shall enforce the **immediate revocation of security-relevant authorizations.**27

FMT_REV.1.2(1) **詳細化**: TSF**は、セキュリティに関連した許可の即時取消しを実施しなければならない。**27

Application Note: Security-relevant authorizations include the ability of authorized users to log in or perform privileged operations. An example of revoking a security-relevant authorization is the deletion of a user account upon which system access is immediately terminated.

適用上の注釈：「セキュリティに関連した認可」とは、認可された利用者がログインしたり特権操作を行ったりする権限を含む。セキュリティに関連した認可の即時取消しの例として、直ちにシステムへのアクセスが不可能になる「利用者アカウントの削除」が挙げられる。

5.5.4.2 Revocation (to owners and authorized administrators) (FMT_REV.1(2))

5.5.4.2 **取消し (所有者と許可管理者に対して)** (FMT_REV.1(2))

FMT_REV.1.1 (2) **Refinement:** The TSF shall restrict the ability to revoke security attributes **of named** objects within the TSC to **owners of the named object and authorized administrators.** 28

FMT_REV.1.1 (2) **詳細化**: TSFは、TSCに含まれている名前付きオブジェクトのセキュリティ属性を取消す能力を、許可管理者およびそのオブジェクトの所有者に制限しなければならない。28

Application Note: The term "revoke security attributes" means "change attributes so that access is revoked".

適用上の注釈：「セキュリティ属性を取消す(revoke security attributes)**」とは、アクセスが取消されるような属性の変更を意味する。**

FMT_REV.1.2 (2) **Refinement:** The TSF shall enforce the **revocation of access rights associated with named objects when an access check is made.** 29

FMT_REV.1.2 (2) **詳細化**: TSFは、アクセスのチェックが行われる際に名前付きオブジェクトに関連づけられたアクセス権限の取消しを実施しなければならない。29

Application Note: The state where access checks are made determines when the access control policy enforces revocation. The access control policy may include immediate or delayed revocation. The access rights are considered to have been revoked when all subsequent access control decisions made by the TSF use the new access control information. In cases where a previous access control decision was made to permit an operation, it is not required that every subsequent operation make an explicit access control decision.

適用上の注釈：アクセス制御ポリシがいつ取消しを実施するかはアクセス権限チェックが行われる状況により決定される。アクセス制御ポリシは即時的、あるいは遅延的な取消しを行う場合がある。アクセス権限はTSFによる一連の全てのアクセス制御の判断が新しいアクセス制御情報に基づき行われるようになった時点で、失効されたものとみなされる。古いアクセス制御情報に基づく判断で操作が許可された場合、それに続く一連の操作に対する明示的なアクセス制御の判断を伴うとは限らない。

5.5.5 Security Attribute Expiration (FMT_SAE)

5.5.5 **セキュリティ属性有効期限** (FMT_SAE)

5.5.5.1 Time-Limited Authorization (FMT_SAE.1)

5.5.5.1 **時限付き許可** (FMT_SAE.1)

FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for **authorized user authentication data** to **the authorized administrator**.

FMT_SAE.1.1 TSFは、許可利用者の認証データに対する有効期限の時間を特定する能力を許可管理者に制限しなければならない。

FMT_SAE.1.2 **Refinement:** The TSF shall be able to **lock out the associated authorized user account** after the expiration time has passed. 30

FMT_SAE.1.2 詳細化: TSFは、有効期間を経過後、関連した許可利用者アカウントをロックアウトできなければならない。30

5.5.6 Security Management Roles (FMT_SMR)

5.5.6 セキュリティ管理役割 (FMT_SMR)

5.5.6.1 Security Roles (FMT_SMR.2)

5.5.6.1 セキュリティ役割 (FMT_SMR.2)

FMT_SMR.2.1 The TSF shall maintain the roles:

FMT_SMR.2.1 TSFは、以下の役割を維持しなければならない:

a) authorized administrator;

a) 許可管理者;

Application Note: Any user that is authorized to modify the TOE such that any MAC, MIC, or DAC policy is bypassed is by definition, an authorized administrator. The TOE may provide multiple administrator roles (audit administrator, security administrator, etc).

適用上の注釈:定義によれば、MAC, MIC, DACポリシのようなTOEを変更することを許可された利用者、あるいは、それらのTOEが適用されない利用者が「許可管理者」となる。TOEは、複数の管理者の役割を提供する場合がある（監査管理者、セキュリティ管理者、その他）

b) cryptographic administrator

b) 暗号管理者 cryptographic administrator

Application Note: Any user authorized to perform functions that affect the operation of the cryptographic module(s) such as cryptographic initialization, setting of cryptographic algorithm modes, and selection of the algorithms is by definition, a cryptographic administrator.

適用上の注釈:定義によれば、暗号モジュールの初期化、暗号アルゴリズムのモードの設定、暗号アルゴリズの組み合わせなど暗号に関するモジュールに影響を与える機能の実行を認可されているのが暗号管理者である。

c) [assignment: any other roles].

c) [割付:その他の役割].

FMT_SMR.2.2 **Refinement:** The TSF shall be able to associate **authorized** users with roles.

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

FMT_SMR.2.3 **Refinement:** The TSF shall ensure that **roles are distinct and that no overlap of allowed operations exists between roles**. 31

FMT_SMR.2.3 詳細化: TSFは、それぞれの役割が識別可能であり、複数の役割の間で許可された操作の重複が発生しないことを保証しなければならない。31

5.5.6.2 Assuming Roles (FMT_SMR.3)

5.5.6.2 負わせる役割 (FMT_SMR.3)

FMT_SMR.3.1 **Refinement**: The TSF shall require an explicit request to assume **any role**.

FMT_SMR.3.1 詳細化: TSFは、任意の役割を負わせるために、明示的な要求を行わなければならない。

5.6 Protection of the TOE Security Functions (FPT)
5.6 TOEセキュリティ機能の保護（FPT）

5.6.1 Underlying Abstract Machine Test (FPT_AMT)
5.6.1 基礎を成す抽象マシンテスト（FPT_AMT）

5.6.1.1 Abstract Machine Testing (FPT_AMT.1)
5.6.1.1 抽象マシンテスト (FPT_AMT.1)

FPT_AMT.1.1 **Refinement:** The TSF shall run a suite of tests during the initial startup and also periodically during normal operation, or at the request of an authorized **administrator** to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the **software portions of the** TSF.
FPT_AMT.1.1 詳細化: TSF は、TSFのソフトウエア部分に従う抽象マシンが提供するセキュリティ設定条件が正しく動作することを実証するために、初期起動時及び通常運用時でも定期的に、あるいは許可管理者から要求されたとき、一群のテストを実行しなければならない。

Application Note: The test suite need only cover aspects of the underlying abstract machine on which the TSF relies to implement required functions, including domain separation.
適用上の注釈:一群のテストは、ドメイン分離を含み、TSFが要求機能を実装していることをあ

てにしている基本抽象マシンの解釈のみを対象とすれば良い。

5.6.2 Internal TOE TSF Data Transfer (FPT_ITT)
5.6.2 TOE 内 TSF データ転送 (FPT_ITT)

5.6.2.1 Basic Internal TSF Data Transfer Protection (FPT_ITT.1)
5.6.2.1 基本TSF 内データ転送保護 (FPT_ITT.1)

FPT_ITT.1.1 **Refinement:** The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE **through the use of the TSF-provided cryptographic services**.
FPT_ITT.1.1 詳細化: TSFは、TSFが提供する暗号サービスにより、TOE の分離したパーツ間で送信されるTSFデータが露呈されることがないよう保護しなければならない。

5.6.2.2 TSF Data Integrity Monitoring (FPT_ITT.3)
5.6.2.2 TSF データ完全性監視 (FPT_ITT.3)

FPT_ITT.3.1 **Refinement:** The TSF shall be able to detect modification, **insertion** and **replay** of TSF data transmitted between separate parts of the TOE **through the use of the TSF-provided cryptographic services**.
FPT_ITT.3.1 詳細化: TSFは、TSFが提供する暗号サービスにより、TOE の分離したパーツ間で送信されるTSFデータの改変、挿入及びリプレイを検出できなければならない。

Application Note: Use of a keyed hash function (e.g., HMAC) that is: (1.) calculated over the TSF data to be transmitted, (2.) appended to the transmitted TSF data, and (3.) checked by the receiving part of the TOE is an example of a cryptographic means that detects modification and substitution of such data. Another example is the use of a cryptographic signature over the transmitted TSF data.
適用上の注釈:鍵付きハッシュ機能の利用(たとえばHMAC)：【 (1)送信されるTSF データから算出、(2)送信されるTSF データに付与する、そして(3)受信元であるTOE のパーツで確認される】は、そのようなデータの改変やリプレイを検出する暗号の利用例です。その他の例としては、送信されるTSFデータに暗号署名を利用する方法があります。

FPT_ITT.3.2 Upon detection of a data integrity error, the TSF shall take the following actions:
a) reject data
b) audit event
c) [assignment: specify the action to be taken].
FPT_ITT.3.2データ完全性誤りを検出したとき、TSF は以下のアクションを取らねばならない:
a) データの拒否
b) 事象の監査
c) [割付:取られるアクションを指定].

Application Note: Additional actions ST author might consider are: retransmission of data and, an alarm after reaching a retransmission threshold.

適用上の注釈:ST 作者が検討するべきその他のアクション:データの再送信、そして再送信閾値に達した後の警告。

5.6.3 Trusted Recovery (FPT_RCV)
5.6.3 高信頼回復 (FPT_RCV)

5.6.3.1 Manual Recovery (FPT_RCV.1)
5.6.3.1 手動回復 (FPT_RCV.1)

FPT_RCV.1.1 **Refinement:** After a failure or service discontinuity **that may lead to a violation of the TSP**, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. **As part of the secure state, the cryptographic module shall be in a known and secure state such that all storage is empty of plaintext cryptographic keys and sensitive data and inaccessible to processes, and all security policies are enforced**.
FPT_RCV.1.1 詳細化: 障害発生あるいはサービス中断の後、TSF は、TOE をセキュアな状態に戻すことができるメンテナンスモードに移らなければならない。セキュアな状態では、暗号モジュールは、全てのストレージには平文の暗号鍵や重要データが存在せず、そこからプロセスにアクセスできない状態であり、また、全てのセキュリティ方針が実施されているという、既知でセキュアな状態でなければならない。

5.6.4 Replay Detection
5.6.4 リプレイ検出 (FPT_RPL)

5.6.4.1 Replay Detection (FPT_RPL.1)
5.6.4.1 リプレイ検出 (FPT_RPL.1)

FPT_RPL.1.1 **Refinement:** The TSF shall **be able to** detect **replay** of TSF data transmitted between separate parts of the TOE **through the use of the TSF-provided cryptographic services**.
FPT_RPL.1.1 詳細化: TSFは、TSFが提供する暗号サービスにより、TOE の分離したパーツ間で送信されるTSF データのリプレイを検出できなければならない。

Application Note: Use of a keyed hash function (e.g., HMAC) that is: (1.) calculated over the TSF data to be transmitted, (2.) appended to the transmitted TSF data, and (3.) checked by the receiving part of the TOE is an example of a cryptographic means that detects modification and substitution of such data. Another example is the use of a cryptographic signature over the transmitted TSF data.
適用上の注釈:鍵付きハッシュ機能の利用(たとえばHMAC):【(1)送信されるTSF データから算出、(2)送信されるTSF データに付与する、そして(3)受信元であるTOE のパーツで確認される】は、そのようなデータの改変やリプレイを検出する暗号の利用例です。その他の例としては、送信されるTSFデータに暗号署名を利用する方法があります。

FPT_RPL.1.2 **Refinement:** Upon detection of **TSF data** replay, the TSF shall take the following actions:32

d) reject data
e) audit event
f) [assignment: specify the action to be taken].
FPT_RPL.1.2 **詳細化**: TSF **データのリプレイを検出したとき、**TSF **は以下のアクションを取らねばならない**:32
d) **データの拒否**
e) **事象の監査**
f) [**割付:取られるアクションを指定**].

Application Note: Additional actions ST author might consider are: retransmission of data and, an alarm after reaching a retransmission threshold.
適用上の注釈:ST **作者が検討するべきその他のアクション**:**データの再送信、そして再送信閾値に達した後の警告**。

5.6.5 Reference Mediation (FPT_RVM)
5.6.5 **リファレンス調停** (FPT_RVM)

5.6.5.1 Non-Bypassability of the TSF (FPT_RVM.1)
5.6.5.1 TSP **の非バイパス性** (FPT_RVM.1)
[**訳注．情報処理推進機構** (IPA) **の**「CC Version 2.1」**日本語訳に従い、原文の**『TSF』**を**『TSP』**とした。**]

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.
FPT_RVM.1.1 TSF**は、**TSC**内の各機能の動作が許可される前に、**TSP**実施機能が呼び出され成功することを保証しなければならない**。

5.6.6 Domain Separation (FPT_SEP)
5.6.6 **ドメイン分離** (FPT_SEP)

5.6.6.1 SFP Domain Separation (FPT_SEP.2)
5.6.6.1 SFP **ドメイン分離** (FPT_SEP.2)

FPT_SEP.2.1 The unisolated portion of the TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.
FPT_SEP.2.1 TSF **の分離していない部分は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない**。

FPT_SEP.2.2 The TSF shall enforce separation between the security domains of subjects in the TSC.
FPT_SEP.2.2 TSF **は、**TSC **内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない**。

FPT_SEP.2.3 **Refinement:** The TSF shall maintain separation of the part of the TSF related to **cryptography**[44] that protects it from interference and tampering by the

remainder of the TSF and by subjects untrusted with respect to cryptography.[33]
FPT_SEP.2.3 詳細化: TSF は、TSFの他の部分及び暗号に関して信頼できないサブジェクトによる干渉や改ざんから保護する暗号(注)に関係するTSFのパートの分離を維持しなければならない。[33]

[44] At a minimum this separation must be maintained for the part of the TSF implementing the cryptoalgorithm and the management of persistent keys.
(注) 最低でも、TSFが暗号アルゴリズムと永続的な鍵管理を実装するパートに関し、この分離は維持されなければならない。

Application Note: Although not required at this time, establishing a separate address space for the cryptography for its own execution and that protects it from accidental interference and tampering by malicious untrusted subjects is the preferred approach for meeting this requirement in medium robustness products, and will be required in updated versions of the OS PP in the near future. For now, as an interim solution, other combinations of techniques that jointly support the overall protection and logical separation of the cryptography may be acceptable pending NSA review.
適用上の注釈：現状では要求されることではないが、自身の実行のためや、悪意のある信頼性できないサブジェクトによる不測の干渉や改ざんからそれを保護する暗号のため、アドレス空間を分離することは、中程度に堅固な製品において、この要件に合致する望ましい方法である。そして、近い将来、OS PP の更新版では要求されることになるであろう。今のところ、当面の解決法としては、全般的に保護や暗号の論理的な分離に連帯して対応する他の技術の組み合わせが、NSAのレビューまでは、容認されるであろう。

Application Note: Ideally, use of off board hardware or a third processor hardware state is the most preferred implementation supporting separation, because it would protect the cryptography from all other parts of the TSF, including malicious parts of the kernel. Migration to this most preferred implementation is anticipated eventually.
適用上の注釈：理想的には、ボードを分離したハードウェアあるいは3分割されたプロセッサーを持つハードウェア状態を使用することが最も望ましい分離をサポートする実装である。なぜなら、カーネルの悪意のある部分も含む、TSFの他の全ての部分から暗号を保護するからである。この最も望ましい実装への移行が、結局、期待されるものである。

5.6.7 Time Stamps (FPT_STM)
5.6.7 タイムスタンプ (FPT_STM)

5.6.7.1 Reliable Time Stamps (FPT_STM.1)
5.6.7.1 高信頼タイムスタンプ (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.
FPT_STM.1.1 TSF は、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。

Application Note: A time stamp includes the correct date and time such that the order of events can be determined.
適用上の注釈:タイムスタンプには、例えばイベントの順序が決定できるような、正しい日付と時間を含む。

5.6.8 Internal TOE TSF Data Replication Consistency (FPT_TRC)
5.6.8 TOE 内 TSF データ複製一貫性 (FPT_TRC)

5.6.8.1 Explicit: Internal TSF Data Consistency (FPT_TRC_EXP.1)
5.6.8.1 明示的要件：TSF 内データ一貫性(FPT_TRC_EXP.1)

FPT_TRC_EXP.1.1 The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state in a timely manner.
FPT_TRC_EXP.1.1 TSFは、首尾一貫していないTSFデータをタイムリーな方法により一貫性のある状態に導くメカニズムを提供することにより、TOE のパート間でTSFデータの一貫性を保証しなければならない。

Application Note: In general, it is impossible to achieve complete, constant consistency of TSF data that is distributed to remote portions of a TOE because distributed portions of the TSF may be active at different times or disconnected from one another. This requirement attempts to address this situation in a practical manner by acknowledging that there will be TSF data inconsistencies but that they will be corrected without undue delay. For example, a TSF could provide timely consistency through periodic broadcast of TSF data to all TSF nodes maintaining replicated TSF data. Another example approach is for the TSF to provide a mechanism to explicitly probe remote TSF nodes for inconsistencies and respond with action to correct the identified inconsistencies.
適用上の注釈：一般的に、TSFの分散部分は異なる時間に動いている、あるいは他と不連続であるため、TOEの遠隔部に分散しているTSFデータを完全に、絶えず一貫性を維持することは不可能である。この要件は、TSFデータの矛盾は存在するかもしれないが過度の遅れがなく訂正されることを認めることにより、実用的な方法でこの状態に向かうことを試みることである。例えば、複製されたTFSデータを保持している全てのTSFノードにTSFデータを定期的にばらまくことで、TSFはタイムリーに一貫性を提供できる。他の例では、TSFが、遠隔のTSFノードに矛盾がないかを明示的に調べ、矛盾が認められた場合には訂正するということで対応するメカニズムを提供する。

5.6.9 TSF Self Testing (FPT_TST)
5.6.9 TSF 自己テスト (FPT_TST)

5.6.9.1 Explicit: TSF Testing (FPT_TST_EXP.1)
5.6.9.1 明示的要件: TSF テスト (FPT_TST_EXP.1)

FPT_TST_EXP.1.1 The TSF shall run a suite of self tests during the initial start-up and also either periodically during normal operation, or at the request of an authorized administrator to demonstrate the correct operation of the TSF.
FPT_TST_EXP.1.1 TSF は、TSFが正しく動作することを実証するために、初期起動時及び通常運用時でも定期的に、あるいは許可管理者から要求されたとき、一群のテストを実行しなければならない。

FPT_TST_EXP.1.2 The TSF shall provide authorized administrators with the capability to verify the integrity of stored TSF executable code through the use of the TSF-provided cryptographic services.
FPT_TST_EXP.1.2 TSF は、許可管理者に、TSFが提供する暗号サービスを利用する格納されたTSF 実行コードの完全性を検証する能力を提供しなければならない。

5.6.9.2 TSF Testing (for cryptography) (FPT_TST.1(1))
5.6.9.2 (暗号システムの)TSF テスト (FPT_TST.1(1))

FPT_TST.1.1(1) **Refinement:** The TSF shall run a suite of self tests **in accordance with FIPS PUB 140-2, Level 4 and Appendix C (as identified in Table 5.3)** during initial start-up **(on power on)**, at the request of the **cryptographic administrator (on demand)**, **under various conditions defined in section 4.9 of FIPS 140-2,** and periodically **(at least once a day)** to demonstrate the correct operation of the **following:**34
a) key error detection;
b) software/firmware;
c) cryptographic algorithms;
d) RNG/PRNG;
e) other FIPS PUB 140-2 critical functions; and
f) ***[assignment: list of all critical security functions implemented in the TOE]***.
FPT_TST.1.1(1) 詳細化: TSF は、次に示す動作が正常に行われることを実証するため、初期起動時(電源投入時)、暗号システム管理者の要求時に(要求があり次第)、「FIPS 140-2, section 4.9」で定義されている様々な条件下で、また定期的に(最低1日一回)、一群の自己テストを「FIS PUB 140-2, Level 4」及び「付録 C」(表5.3 に示す)に従って実行しなければならない: 34
a) 鍵異常の検知;
b) ソフトウェア/ファームウェア;
c) 暗号アルゴリズム;
d) 乱数ジェネレータ(RNG)/疑似乱数ジェネレータ(PRNG);
e) 他の FIPS PUB 140-2 重要機能; そして
f) *[割付:TOEに実装されている全重要セキュリティ機能のリスト]*.

Table 5.3 - Interpretation of FIPS PUB 140-2 Self-tests

	FIPS-140 Security Level 4
Software/Firmware Integrity Tests	on power on on demand conditional
Cryptographic Algorithm Tests	on power on on demand conditional
Other FIPS PUB 140-2 critical functions tests and other tests as determined by FIPS PUB 140-2 (Appendix A)	on power on on demand conditional
Statistical RNG/PRNG tests (Appendix C)	on power on on demand

表5.3 - FIPS PUB 140-2 自己テストの解釈

	FIPS-140 Security Level 4
ソフトウェア/ファームウェア完全性テスト	電源投入時 要求があり次第 条件付
暗号アルゴリズムテスト	電源投入時 要求があり次第 条件付
他の FIPS PUB 140-2 重要機能テスト 及び FIPS PUB 140-2 (付録 A) が決定した他のテスト	電源投入時 要求があり次第 条件付
統計的な RNG/PRNG テスト (付録 C)	電源投入時 要求があり次第

FPT_TST.1.2(1) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of TSF data **related to the cryptography by using TSF-provided cryptographic functions**.35
FPT_TST.1.2(1) 詳細化: TSF は、許可暗号システム管理者に、TSFが提供する暗号機能を使用して暗号に関係するTSF データの完全性を検証する能力を提供しなければならない。35

FPT_TST.1.3(1) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of stored TSF executable code **related to the cryptography by using TSF-provided cryptographic functions**.36
FPT_TST.1.3(1) 詳細化: TSF は、許可暗号システム管理者に、TSFが提供する暗号機能を使用して暗号に関係する格納されたTSF 実行コードの完全性を検証する能力を提供しなければならない。36

5.6.9.3 TSF Testing (for key generation components) (FPT_TST.1(2))
5.6.9.3 (鍵生成コンポーネントの)TSF テスト (FPT_TST.1(2))

FPT_TST.1.1(2) **Refinement**: The TSF shall perform self tests **immediately after generation of a key** to demonstrate the correct operation **of each key generation component**. **If any of these tests fails, that generated key shall not be used, the cryptographic module shall react as required by FIPS PUB 140-2 for failing a self-test, and this event will be audited**.37
FPT_TST.1.1(2) 詳細化: TSFは、各鍵生成コンポーネントが正しく動作することを実証するため、鍵生成後、速やかに自己テストを実行しなければならない。もしこれらのテストのいずれかが失敗に終わった場合、そこで生成された鍵は使用してはならない、また、暗号モジュールは自己テスト失敗に関するFIPS PUB 140-2 の要求に対応しなければならない、そして、この事象は検査される。37

Application Note: Key generation components are those critical elements that compose the entire key generation process (e.g., any algorithms, any RNG/PRNGs, any key generation seeding processes, etc.).
適用上の注釈：鍵生成コンポーネントとは全ての鍵生成プロセスを構成する重要な要素である

（例えば、アルゴリズム、乱数ジェネレータ/疑似乱数ジェネレータ、鍵生成における種乱数の使用法、など）。

Application Note: These self-tests on the key generation components can be executed here as a subset of the full suite of self-tests run on the cryptography in FPT_TST.1(1) as long as all elements of the key generation process are tested.
適用上の注釈：全ての鍵生成プロセス要素がテストされている限り、完全な自己テスト群のサブセットが FPT_TST.1(1) の暗号で実行している時点で、鍵生成コンポーネントにおけるこれらの自己テストは実行可能である。

FPT_TST.1.2(2) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of TSF data **related to the key generation by using TSF-provided cryptographic functions**.38
FPT_TST.1.2(2) **詳細化**: TSF **は、許可暗号システム管理者に、TSFが提供する暗号機能を使用した鍵生成に関係するTSFデータの完全性を検証する能力を提供しなければならない。**38

FPT_TST.1.3(2) **Refinement:** The TSF shall provide authorized **cryptographic administrators** with the capability to verify the integrity of stored TSF executable code **related to the key generation by using TSF-provided cryptographic functions**.39
FPT_TST.1.3(2) **詳細化**: TSF **は、許可暗号システム管理者に、TSFが提供する暗号機能を使用した鍵生成に関係する格納されたTSF 実行コードの完全性を検証する能力を提供しなければならない。**39

Resource Utilization (FRU)

5.7 資源の利用(FRU)

5.7.1 Resource Allocation(FRU_RSA)

5.7.1 資源の割当(FRU_RSA)

5.7.1.1 Maximum Quotas (for shared persistent storage)(FRU_RSA.1(1))

5.7.1.1 最大割当（共有永久記憶装置に対して）(FRU_RSA.1(1))

FRU_RSA1.1(1) The TSF shall enforce maximum quotas of the following resources:**portion of shared persistent storage** that individual **authorized** users can use simultaneously.

FRU_RSA1.1(1) TSF(TOE Security Function)は以下の資源の最大割当てを実施しなければならない。すなわち、各認定ユーザが同時に共有の永久記憶装置を区分使用可能な最大量

Application Note: For persistent storage, simultaneously means that the shared media contains data belonging to more than one user.

適用上の注釈：永久記憶装置については、‘同時に’と言う言葉は‘共有している媒体’が複数のユーザデータを蓄積していることを意味する。

5.7.1.2 Maximum Quotas (for system memory)(FRU_RSA.1(2))

5.7.1.2 最大割当（システムメモリに対して）(FRU_RSA.1(2))

FRU_RSA1.1(2) The TSF shall enforce maximum quotas of the following resources:**portion of system memory** that individual **authorized** users can use simultaneously.

FRU_RSA1.1(2) TSFは以下の資源の最大割当てを実施しなければならない。すなわち、各認定ユーザが同時にシステムメモリを区分使用可能な最大量

5.7.1.3 Maximum Quotas (for processing time)(FRU_RSA.1(3))

5.7.1.3 最大割当（処理時間に対して） (FRU_RSA.1(3))

FRU_RSA1.1(3) The TSF shall enforce maximum quotas of the following resources:**portion of processing time** that subjects can use over a specified period of time.

FRU_RSA1.1(3) TSFは以下の資源割当を実施しなければならない。すなわち、主体（Subjects)が特定の時間の間利用可能な処理時間の割合

Application Note: The algorithm to determine percentages of time can be based on many factors(e.g. member of users, relative priority of users, availability of resources to users).

適用上の注釈：時間の割合を決定するアルゴリズムは、ユーザ数、ユーザの相対的優先順位、ユーザへの資源可用性など多くの要因を基にすることができる。

5.8 TOE Access (FTA)
5.8 TOEアクセス(FTA)

5.8.1 Limitation on scope of selectable attributes (FTA_LSA)
5.8.1 選択可能な属性の範囲の制限(FTA_LSA)

5.8.1.1 Limitation on scope of selectable attributes(FTA_LSA.1)
5.8.1.1 選択可能な属性の範囲の制限(FTA_LSA.1)

FTA_LSA.1.1 **Refinement**: The TSF shall restrict the scope of **roles, user sensitivity and integrity levels and user privileges** based on location, time, and day.
FTA_LSA.1.1 **詳細化：ＴＳＦは、場所や日付、時刻によってユーザの役割、ユーザ感度、完全性の水準、ユーザ特権の範囲を制限しなければならない。**

Application Note: The intent of this requirement is to allow or disallow the assumption of roles or the effectiveness of user privileges based on the location where the session was established or the date/time of session establishment.
適用上の注釈：この要求の意図は、セションが確立された場所、日時により、役割の受任、ユーザ特権の有効性を許可または不許可にすることである。

Application Note: 'Location' refers to what ever means the TOE users to identify a point of entry for interactive user session establishment. The adequacy of this means is determined by other requirements (e.g. FTP SEP, AVA_VLA).
適用上の注釈： Location（場所）はTOE（評価対象）のユーザが対話的なセションを確立するための登録場所を確認する手段のどんなものにも対応する。

5.8.2 Limitation on multiple concurrent sessions(FTA_MCS)
5.8.2 同時にセションを多数開くことの制限（FTA_MCS）

5.8.2.1 Basic limitation on multiple concurrent sessions(FTA_MCS.1)
5.8.2.1 多数の同時セションを開くことの基本的制限(FTA_MCS.1)

FTA_MCS.1.1 **Refinement:** The TSF shall **enforce a** maximum number of concurrent interactive sessions per user.
FTA_MCS.1.1 **詳細化**: TSFは**1**ユーザ当りの同時に開くことのできる対話セションの最大数を規定しなければならない。

FTA_MCS.1.2 **Refinement:** The TSF shall allow **an authorized administrator to set the maximum number of concurrent interactive** sessions per user.
FTA_MCS.1.2 **詳細化：**TSFは公式の管理者が1ユーザ当りの同時に開くことのできる対話セションの最大数を設定することを許可しなければならない。

Application Note: `Concurrent' refers to any specific synchronization as defined in the internal TSF data consistency requirement FRT_TRC_EXP.1.1. Enforcement of the requirement is at every synchronization.

適用上の注釈： `Concurrent（同時）'とは、内部TSFデータの一貫性の要求であるFRT_TRC_EXP.1.1で定義されたどのような特殊な同期にも対応する．要求の強制はどんな同期の時でも行われる。

5.8.3 Session Locking(FTA_SSL)
5.8.3 セションのロック(FTA_SSL)

5.8.3.1 TSF-Initiated Session Locking (FTA_SSL.1)
5.8.3.1 TSF起動のセションのロック(FTA_SSL.1)

FTA_SSL.1.1 The TSF shall lock an interactive session after **an authorized administrator specified time interval of user inactivity** by :
FTA_SSL1.1 TSFは公式の管理者が決めたユーザをアクティベイトしない時間間隔を指定した後、以下のことによって対話セションをロックしなければならない：

a) clearing or overwriting display devices, making the current contents unreadable.
a) 現在のコンテンツが読めないように表示デバイスをクリアまたは重ね書きする

b) disabling any activity of the user's data access/display devices other than unlocking the session.
b) そのセションのロック解除を行う以外はユーザのデータアクセス／表示デバイスのいかなる活動をも無効にする

FTA_SSL.1.2 **Refinement:** The TSF shall require the **user to re-authenticate** to unlock the session:
FTA_SSL.1.2 詳細化：TSFはセションのロック解除のために、ユーザに再認証を受けるよう要求しなければならない。

5.8.3.2 User-Initiated Session Locking (FTA_SSL.2)
5.8.3.2 ユーザ起動のセションのロック（FTA_SSL.2）

FTA_SSL.1.2 The TSF shall allow user-initiated locking of the user's own interactive session by :
FTA_SSL.1.2 TSFは 以下のことによって、ユーザ起動によるユーザ自身の対話セションのロックを許可しなければならない。

a) clearing or overwriting display devices, making the current contents unreadable.
a) 現在のコンテンツが読めないように表示デバイスをクリアまたは重ね書きする

b) disabling any activity of the user's data access/display devices other than unlocking the session.
b) そのセッションのロック解除を行う以外は、ユーザのデータアクセス/表示デバイスのいかなる活動も無効にする

FTA_SSL.2.2 **Refinement:** The TSF shall require the **user to re-authenticate** to unlock the session.
FTA_SSL.2.2 **詳細化：** TSF **はセションのロック解除のためには、ユーザに再認証を要求しなければならない。**

5.8.4 TOE Access Banners(FTA_TAB)
5.8.4 TOE**アクセスバナー**(FTA_TAB)

5.8.4.1 Default TOE Access Banners (FTA_TAB.1)
5.8.4.1 **デフォルトによる** TOE **アクセスバナー** (FTA_TAB.1)

FTA_TAB.1.1 **Refinement:** Before establishing a user session, the TSF shall display an **authorized-administrator specified** advisory **notice and consent** warning message regarding unauthorized use of the TOE.
FTA_TAB.1.1 **詳細化**: **ユーザセションの確立の前に、**TSF**は公式の管理者が 定めた**TOE**の不正使用に関する助言的通知と同意警告のメッセージを表示しなければならない。**

5.8.5 TOE Access History(FTA_TAH)
5.8.5 TOE**アクセス履歴**(FTA_TAH)

5.8.5.1 TOE Access History (FTA_TAH.1)
5.8.5.1 TOE **アクセス履歴** (FTA_TAH.1)

FTA_TAH.1.1 **Refinement:** Upon successful **interactive** session establishment, the TSF shall display **to the authorized user** the date and time of **that authorized user's** last successful **interactive** session establishment.
FTA_TAH.1.1 **詳細化**: **対話セションの確立の成功時に、**TSF**は許可されたユーザに、その許可ユーザが最後に対話セションの確立に成功した日時を表示しなければならない。**

FTA_TAH.1.2 Upon successful **interactive** session establishment, the TSF shall display **to the authorized user** the date and time of the last unsuccessful attempt and the number of unsuccessful attempts at **interactive** session establishment **for that user identifier** since the last successful **interactive** session establishment.
FTA_TAH.1.2 **対話セションの確立の成功時に、**TSF**は許可されたユーザの確認のために、前回最後に対話セションを確立して以降、成功しなかった対話セション確立の試みの最新日時とそのときまでの試行回数を表示しなければならない。**

Application Note: In both of the above elements, for distribution systems, date and time needs to be accurate to the degree required by FPT_TRC_EXP.1.
適用上の注釈：上述の二つの要素においては、配布システムのために、日付や時刻情報はFPT_TRC_EXP.1**により要求される程度の精度が必要になる。**

FTA_TAH.1.3 **Refinement:** the TSF shall not erase the access history information from the **authorized** user interface without giving the **authorized** user the opportunity to

review the information.
FTA_TAH.1.3 詳細化： TSF は許可されたユーザがアクセス履歴情報を吟味する機会を与えずに許可ユーザの画面からその情報を消去してはならない。

5.8.6 TOE Session Establishment(FTA_TSE)
5.8.6 TOEセションの確立(FTA_TSE)

5.8.6.1 TOE Session Establishment (FTA_TSE.1)
5.8.6.1 TOE セッションの確立 (FTA_TSE.1)

FTA_TSE.1.1 TSF shall be able to deny session establishment **based on location, time, day, and requested session security and integrity levels.**
FTA_TSE.1.1 TSFは場所、時刻、日付、および期待するセションのセキュリティと完全性の水準に基づいてセション確立を拒否できるようにしなければならない。

5.9 Trusted Path/Channels(FTP)
5.9 高信頼パス／チャネル(FTP)

5.9.1 Trusted Path(FTP_TRP)
5.9.1 高信頼パス(FTP_TRP)

5.9.1.1 Explicit: Trusted Path (FTP__TRP__EXP.1)
5.9.1.1 明示: 高信頼パス(FTP_TRP_EXP.1)

FTP_TRP_EXP.1.1 The TSF shall provide a communication path between itself and remote and local users that is logically distinct from other communication paths and provides assured identification of the TSF to the requesting user and protection of the communicated data from modification or disclosure.
FTP_TRP_EXP.1.1 TSF は他の通信パスと論理的に区別された通信パスを自己とリモートやローカルのユーザに提供して、その要求ユーザにTSFの保証のある識別子と 通信データを改竄や暴露からの防護を提供しなければ ならない。

Application Note: This `distinct' path is merely invoked for the duration of its belong needed (e.g., for re- authenticating the user); it need not be invoked for the duration of the user's session.
適用上の注釈：この'区別された'パスは、（例えばユーザ再認証時のように） 必要となる期間だけ呼び出されれば良く、セション確立の期間を通して常に呼び出されている必要はない。

FTP_TRP_EXP.1.2 The TSF shall permit local users and remote users to initiate communication via the trusted path.
FTP_TRP_EXP.1.2 TSF は、ローカルやリモートユーザに高信頼パス経由の通信開始を許可しなければならない。

FTP_TRP_EXP.1.3 The TSF shall require the use of the trusted path for user authentication and user identification during TOE session establishment, for operations to modify authentication data, for protection of authentication data when a locked

session is being unlocked and all other operations requiring a human user to enter authentication data.
FTP_TRP_EXP.1.3 **詳細化： TSF はTOEがセションを確立中にユーザ認証とユーザ識別を行う時、認証データの修正を行う時、ロックされていたセッションがロック解除され認証データを防護しなければならない時、その他のユーザ（人間）に認証データの投入を要求する操作の時は高信頼パスの使用を要求しなければならない。**