ネットワークデバイスの
コラボラティブプロテクションプロファイル

バージョン 2.0

2017 年 5 月 5 日

平成 29 年 10 月 25 日　翻訳第 1.0 版
独立行政法人情報処理推進機構
技術本部 セキュリティセンター
情報セキュリティ認証室

謝辞

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

0. 序文

0.1 本書の目的

本書は、ネットワークデバイスのセキュリティ機能要件 (SFR) 及びセキュリティ保証要件 (SAR) を記述するコモンクライテリア (CC) コラボラティブプロテクションプロファイル (cPP) として提供する。製品が、本 cPP の SFR を満たしているかどうかを決定するために評価者が実行するアクションを特定する評価アクティビティは、 [SD] に記述される。

0.2 本書の適用範囲

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

0.3 想定される読者

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

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

0.4 関連する文書

コモンクライテリア [1]

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

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

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

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

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

その他の文書

[SD] ネットワークデバイス cPP の評価アクティビティ、バージョン 2.0

改版履歴

バージョン	日付	説明
2.0	2017 年 5 月 5 日	正式リリース
1.1	2016 年 7 月 21 日	公開レビュー用に発行された改訂版
1.0	2015 年 2 月 27 日	正式リリース
0.4	2015 年 1 月 26 日	CCDB レビューからのコメントを取り込む
0.3	2014 年 10 月 17 日	サポート文書の CCDB レビューに伴うドラフト版のリリース
0.2	2014 年 10 月 13 日	iTC レビュー用、公開レビューのコメントに対応した内部ドラフト
0.1	2014 年 9 月 05 日	公開レビュー用ドラフト発行

目次

謝辞 2

0. 序文 3
0.1 本書の目的 3
0.2 本書の適用範囲 3
0.3 想定される読者 3
0.4 関連する文書 3

1. PP 序説 12
1.1 PP 参照識別 12
1.2 TOE 概要 12
1.3 TOE ユースケース 13

2. CC 適合 15

3. 分散型 TOE の導入 16
3.1 サポートされる分散型 TOE のユースケース 16
3.2 非サポートの分散 TOE のユースケース 19
3.3 分散 TOE のコンポーネントの登録 21
3.4 分散 TOE での要件のアロケーション 24

4. セキュリティ課題定義 27
4.1 脅威 27
4.1.1 ネットワークデバイスとの通信 27
4.1.1.1 T.UNAUTHORIZED_ADMINISTRATOR_ACCESS 28
4.1.1.2 T.WEAK_CRYPTOGRAPHY 28
4.1.1.3 T.UNTRUSTED_COMMUNICATION_CHANNELS 29
4.1.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS 29
4.1.2 有効なアップデート 30
4.1.2.1 T.UPDATE_COMPROMISE 30
4.1.3 監査されたアクティビティ 31
4.1.3.1 T.UNDETECTED_ACTIVITY 31
4.1.4 管理者及びデバイスのクレデンシャル並びにデータ 31
4.1.4.1 T.SECURITY_FUNCTIONALITY_COMPROMISE 32
4.1.4.2 T.PASSWORD_CRACKING 32
4.1.5 デバイスの障害 33
4.1.5.1 T.SECURITY_FUNCTIONALITY_FAILURE 33
4.2 前提条件 33
4.2.1 A.PHYSICAL_PROTECTION 33
4.2.2 A.LIMITED_FUNCTIONALITY 34
4.2.3 A.NO_THRU_TRAFFIC_PROTECTION 34
4.2.4 A.TRUSTED_ADMINISTRATOR 34
4.2.5 A.REGULAR_UPDATES 34
4.2.6 A.ADMIN_CREDENTIALS_SECURE 34
4.2.7 A.COMPONENTS_RUNNING (分散型 TOE のみに適用) 34
4.2.8 A.RESIDUAL_INFORMATION 35
4.3 組織のセキュリティ方針 35
4.3.1 P.ACCESS_BANNER 35

5. セキュリティ対策方針 36
5.1 運用環境のセキュリティ対策方針 36
5.1.1 OE.PHYSICAL 36
5.1.2 OE.NO_GENERAL_PURPOSE 36
5.1.3 OE.NO_THRU_TRAFFIC_PROTECTION 36
5.1.4 OE.TRUSTED_ADMIN 36
5.1.5 OE.UPDATES 36
5.1.6 OE.ADMIN_CREDENTIALS_SECURE 36
5.1.7 OE.COMPONENTS_RUNNING (分散型 TOE のみに適用) 36
5.1.8 OE.RESIDUAL_INFORMATION 36

6. セキュリティ機能要件 37
6.1 表記法 37
6.2 SFR アーキテクチャ 38
6.3 セキュリティ監査 (FAU) 43
6.3.1 セキュリティ監査データ生成 (FAU_GEN) 43
6.3.1.1 FAU_GEN.1 監査データ生成 43
6.3.1.2 FAU_GEN.2 利用者識別情報の関連付け 47
6.3.2 セキュリティ監査事象格納 (拡張—FAU_STG_EXT) 47
6.3.2.1 FAU_ STG_EXT.1 保護された監査事象格納 47
6.3.3 分散型 TOE のセキュリティ監査 48
6.4 暗号サポート (FCS) 49
6.4.1 暗号鍵管理 (FCS_CKM) 49
6.4.1.1 FCS_CKM.1 暗号鍵生成 (詳細化) 49
6.4.1.2 FCS_CKM.2 暗号鍵確立 (詳細化) 50
6.4.1.3 FCS_CKM.4 暗号鍵破棄 51
6.4.2 暗号操作 (FCS_COP) 52
6.4.2.1 FCS_COP.1 暗号操作 52
6.4.3 乱数ビット生成 (拡張—FCS_RBG_EXT) 54
6.4.3.1 FCS_RBG_EXT.1 乱数ビット生成 54
6.5 識別と認証 (FIA) 55
6.5.1 認証失敗管理 (FIA_AFL) 55
6.5.1.1 FIA_AFL.1 認証失敗管理 (詳細化) 55
6.5.2 パスワード管理 (拡張—FIA_PMG_EXT) 56
6.5.2.1 FIA_PMG_EXT.1 パスワード管理 56
6.5.3 利用者の識別と認証 (拡張—FIA_UIA_EXT) 57
6.5.3.1 FIA_UIA_EXT.1 利用者の識別と認証 57
6.5.4 利用者認証 (FIA_UAU) (拡張—FIA_UAU_EXT) 57
6.5.4.1 FIA_UAU_EXT.2 パスワードベースの認証メカニズム 57
6.5.4.2 FIA_UAU.7 保護された認証フィードバック 58
6.6 セキュリティ管理 (FMT) 58
6.6.1 TSF における機能の管理 (FMT_MOF) 59
6.6.1.1 FMT_MOF.1/ManualUpdate セキュリティ機能のふるまいの管理 59
6.6.2 TSF データの管理 (FMT_MTD) 59
6.6.2.1 FMT_MTD.1/CoreData TSF データの管理 59
6.6.3 管理機能の特定 (FMT_SMF) 59
6.6.3.1 FMT_SMF.1 管理機能の特定 59
6.6.4 セキュリティ管理役割 (FMT_SMR) 61
6.6.4.1 FMT_SMR.2 セキュリティ役割における制限 61
6.7 TSF の保護 (FPT) 62
6.7.1 TSF データの保護 (拡張—FPT_SKP_EXT) 62
6.7.1.1 FPT_SKP_EXT.1 TSF データの保護 (すべての対称鍵の読み出し) 62
6.7.2 管理者パスワードの保護 (拡張—FPT_APW_EXT) 63
6.7.2.1 FPT_APW_EXT.1 管理者パスワードの保護 63
6.7.3 TSF テスト (拡張—FPT_TST_EXT) 63
6.7.3.1 FPT_TST_EXT.1 TSF テスト (拡張) 63
6.7.4 高信頼アップデート (FPT_TUD_EXT) 64
6.7.4.1 FPT_TUD_EXT.1 高信頼アップデート 64
6.7.5 タイムスタンプ (拡張－FPT_STM_EXT) 67
6.7.5.1 FPT_STM_EXT.1 高信頼タイムスタンプ 67
6.8 TOE アクセス (FTA) 68
6.8.1 TSF 起動セションロック (拡張—FTA_SSL_EXT) 68
6.8.1.1 FTA_SSL_EXT.1 TSF 起動セションロック 68
6.8.2 セションロックと終了 (FTA_SSL) 68
6.8.2.1 FTA_SSL.3 TSF 起動による終了(詳細化) 68
6.8.2.2 FTA_SSL.4 利用者起動による終了(詳細化) 69
6.8.3 TOE アクセスバナー (FTA_TAB) 69
6.8.3.1 FTA_TAB.1 デフォルト TOE アクセスバナー(詳細化) 69

6.9 高信頼パス／チャネル (FTP) ... 69
6.9.1 高信頼チャネル (FTP_ITC) ... 69
6.9.1.1 FTP_ITC.1 TSF 間高信頼チャネル (詳細化) ... 69
6.9.2 高信頼パス (FTP_TRP) ... 70
6.9.2.1 FTP_TRP.1/Admin 高信頼パス (詳細化) ... 70

7. セキュリティ保証要件 ... 72
7.1 ASE：セキュリティターゲット ... 72
7.2 ADV：開発 ... 73
7.2.1 基本機能仕様 (ADV_FSP.1) ... 73
7.3 AGD：ガイダンス文書 ... 73
7.3.1 利用者操作ガイダンス (AGD_OPE.1) ... 74
7.3.2 準備手続き (AGD_PRE.1) ... 74
7.4 ALC クラス：ライフサイクルサポート ... 74
7.4.1 TOE のラベル付け (ALC_CMC.1) ... 74
7.4.2 TOE CM 範囲 (ALC_CMS.1) ... 74
7.5 ATE クラス：テスト ... 74
7.5.1 独立テスト—適合 (ATE_IND.1) ... 75
7.6 AVA クラス：脆弱性評定 ... 75
7.6.1 脆弱性調査 (AVA_VAN.1) ... 75

A. オプションの要件 ... 76
A.1 オプション SFR 用の監査事象 ... 76
A.2 セキュリティ監査 (FAU) ... 78
A.2.1 セキュリティ監査事象格納 (FAU_STG.1 及び拡張—FAU_STG_EXT) ... 78
A.2.1.1 FAU_STG.1 保護された監査証跡格納 ... 78
A.2.1.2 FAU_STG_EXT.2/LocSpace 消失した監査データの集計 ... 78
A.2.1.3 FAU_STG.3/LocSpace 監査データ喪失の可能性がある場合のアクション ... 79
A.3 識別と認証 (FIA) ... 79
A.3.1 X.509 証明書を用いた認証 (拡張－FIA_X509_EXT) ... 79
A.3.1.1 FIA_X509_EXT.1 証明書有効性確認 ... 79
A.4 セキュリティ管理 (FMT) ... 81
A.4.1 TSF における機能の管理 (FMT_MOF) ... 81
A.4.1.1 FMT_MOF.1/Services セキュリティ機能のふるまいの管理 ... 81
A.4.2 TSF データの管理 (FMT_MTD) ... 81
A.4.2.1 FMT_MTD.1/CryptoKeys TSF データの管理 ... 81
A.5 TSF の保護 (FPT) ... 81
A.5.1 TOE 内 TSF データ転送(FPT_ITT) ... 81
A.5.1.1 FPT_ITT.1 基本 TSF 内データ転送保護 (詳細化) ... 81
A.6 高信頼パス／チャネル (FTP) ... 82
A.6.1 高信頼パス (FTP_TRP) ... 82
A.6.1.1 FTP_TRP.1/Join 高信頼パス (詳細化) ... 82
A.7 通信 (FCO) ... 83
A.7.1 通信相手の管理 (FCO_CPC_EXT) ... 83
A.7.1.1 FCO_CPC_EXT.1 コンポーネント登録チャネル定義 ... 83

B. 選択ベース要件 ... 85
B.1 選択ベース SFR の監査事象 ... 85
B.2 暗号サポート (FCS) ... 87
B.2.1 暗号プロトコル (拡張—FCS_DTLC_EXT、FCS_DTLSS_EXT、FCS_HTTPS_EXT, FCS_IPSEC_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT) ... 87
B.2.1.1 FCS_DTLSC_EXT & FCS_DTLSS_EXT DTLS プロトコル ... 87
B.2.1.2 FCS_HTTPS_EXT.1 HTTPS プロトコル ... 97
B.2.1.3 FCS_IPSEC_EXT.1 IPsec プロトコル ... 98
B.2.1.4 FCS_SSHC_EXT & FCS_SSHS_EXT SSH プロトコル ... 103
B.2.1.5 FCS_TLSC_EXT & FCS_TLSS_EXT TLS プロトコル ... 108
B.3 識別と認証 (FIA) ... 116
B.3.1 X.509 証明書を用いた認証 (拡張—FIA_X509_EXT) ... 116

B.3.1.1 FIA_X509_EXT.1 X.509 証明書有効性確認 117
B.3.1.2 FIA_X509_EXT.2 X.509 証明書認証 118
B.3.1.3 FIA_X509_EXT.3 X.509 証明書要求 119
B.4 TSF の保護 (FPT) 119
B.4.1 TSF 自己テスト (拡張) 119
B.4.1.1 FPT_TST_EXT.2 証明書に基づく自己テスト 119
B.4.2 高信頼アップデート (FPT_TUD_EXT) 120
B.4.2.1 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート 120
B.5 セキュリティ管理 (FMT) 120
B.5.1 TSF における機能の管理 (FMT_MOF) 120
B.5.1.1 FMT_MOF.1/AutoUpdate セキュリティ機能のふるまいの管理 120
B.5.1.2 FMT_MOF.1/Functions セキュリティ機能のふるまいの管理 121

C. 拡張コンポーネントの定義 122
C.1 セキュリティ監査 (FAU) 122
C.1.1 保護された監査事象格納 (FAU_STG_EXT) 122
C.1.1.1 FAU_ STG_EXT.1 保護された監査事象格納 123
C.1.1.2 FAU_ STG_EXT.2 消失した監査データの集計 124
C.2 暗号サポート (FCS) 124
C.2.1 乱数ビット生成 (FCS_RBG_EXT) 124
C.2.1.1 FCS_RBG_EXT.1 乱数ビット生成 124
C.2.2 暗号プロトコル (拡張—FCS_DTLSC_EXT, FCS_DTLSS_EXT, FCS_HTTPS_EXT, FCS_IPSEC_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT) 125
C.2.2.1 FCS_DTLSC_EXT DTLSC クライアントプロトコル 126
C.2.2.2 FCS_DTLSS_EXT DTLS サーバプロトコル 130
C.2.2.3 FCS_HTTPS_EXT.1 HTTPS プロトコル 135
C.2.2.4 FCS_IPSEC_EXT.1 IPsec プロトコル 135
C.2.2.5 FCS_SSHC_EXT.1 SSH クライアント 140
C.2.2.6 FCS_SSHS_EXT.1 SSH サーバプロトコル 142
C.2.2.7 FCS_TLSC_EXT TLS クライアントプロトコル 144
C.2.2.8 FCS_TLSS_EXT TLS サーバプロトコル 149
C.3 識別と認証 (FIA) 152
C.3.1 パスワード管理 (FIA_PMG_EXT) 152
C.3.1.1 FIA_PMG_EXT.1 パスワード管理 152
C.3.2 利用者識別と認証 (FIA_UIA_EXT) 152
C.3.2.1 FIA_UIA_EXT.1 利用者識別と認証 153
C.3.3 利用者認証 (FIA_UAU) (FIA_UAU_EXT) 154
C.3.3.1 FIA_UAU_EXT.2 パスワードベースの認証メカニズム 154
C.3.4 X.509 証明書を用いた認証 (拡張—FIA_X509_EXT) 155
C.3.4.1 FIA_X509_EXT.1 X.509 証明書有効性確認 156
C.3.4.2 FIA_X509_EXT.2 X509 証明書認証 157
C.3.4.3 FIA_X509_EXT.3 X.509 証明書要求 158
C.4 TSF の保護 (FPT) 159
C.4.1 TSF データの保護 (FPT_SKP_EXT) 159
C.4.1.1 FPT_SKP_EXT.1 TSF データの保護 (すべての対称鍵の読み出しについて) 159
C.4.2 管理者パスワードの保護 (FPT_APW_EXT) 160
C.4.2.1 FPT_APW_EXT.1 管理者パスワードの保護 160
C.4.3 TSF 自己テスト 160
C.4.3.1 FPT_TST_EXT.1 TSF テスト 160
C.4.4 高信頼アップデート (FPT_TUD_EXT) 162
C.4.4.1 FPT_TUD_EXT.1 高信頼アップデート 163
C.4.4.2 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート 166
C.4.5 タイムスタンプ (FPT_STM_EXT) 166
C.4.5.1 FPT_STM_EXT.1 信頼できるタイムスタンプ 167
C.5 TOE アクセス (FTA) 168
C.5.1 FTA_SSL_EXT.1 TSF 起動によるセションロック 168
C.5.1.1 FTA_SSL_EXT.1 TSF 起動によるセションロック 169

C.6 通信 (FCO)..... 169
C.6.1 通信相手の管理 (FCO_CPC_EXT)..... 169
C.6.1.1 FCO_CPC_EXT.1 コンポーネント登録チャネル定義..... 170

D. エントロピーに関する証拠資料及び評定..... 171
D.1 設計記述..... 171
D.2 エントロピーの正当化..... 171
D.3 動作条件..... 172
D.4 ヘルステスト..... 172

E. 根拠..... 173
E.1 SFR 依存性分析..... 173

用語集..... 179

略語..... 180

図 / 表

図 1：一般化された分散 TOE モデル 16
図 2：基本的な分散型 TOE ユースケース 16
図 3：非分散型 TOE のユースケース 17
図 4：適用範囲外の管理コンポーネントを持つ分散型 TOE ユースケース 17
図 5：cPP 要件を満たすことが要求される管理コンポーネント 18
図 6：分散型ネットワークデバイスと cPP 要件を満たすことが要求される管理コンポーネント 18
図 7：等価性の説明を通して拡張された分散型 TOE 19
図 8：サポートされない企業での管理のユースケース 20
図 9：複数の管理コンポーネントを持つサポートされないユースケース 21
図 10：FPT_ITT.1 または FTP_ITC.1 を満たすチャネルを用いる分散型 TOE の登録 22
図 11：FTP_TRP.1/Join を満たすチャネルを用いた分散型 TOE の登録 22
図 12：登録チャネルなしの分散型 TOE の登録 23
図 13：分散型 TOE の参入者有効化オプション 23
図 14：保護された通信の SFR アーキテクチャ 39
図 15：管理者認証の SFR アーキテクチャ 40
図 16：正しい動作の SFR アーキテクチャ 40
図 17：高信頼アップデートと監査の SFR アーキテクチャ 41
図 18：管理の SFR アーキテクチャ 42
図 19：分散型 TOE の SFR アーキテクチャ 42

表 1：分散型 TOE のセキュリティ機能要件 26
表 2：セキュリティ機能要件及び監査対象事象 46
表 3：セキュリティ保証要件 72
表 4：TOE オプション SFR 及び監査対象事象 77
表 5：選択ベース SFR 及び監査対象事象 86
表 6：必須の SFR についての SFR 依存性根拠 174
表 7：オプションの SFR についての SFR 依存性根拠 175
表 8：選択ベースの SFR についての SFR 依存性根拠 178

1. PP 序説

1.1 PP 参照識別

PP 参照：collaborative Protection Profile for Network Devices
ネットワークデバイスのコラボラティブプロテクションプロファイル

PP バージョン：2.0

PP 日付：2017 年 5 月 5 日

1.2 TOE 概要

本書は、評価対象 (TOE) をネットワークデバイスとするコラボラティブプロテクションプロファイル (cPP) である。本書は、定義された複数の脅威 (訳注：の顕在化) の低減を目的とするすべてのネットワークデバイスに期待される最小限のセキュリティ要件を提供する。本ベースライン要件は、将来の cPP によって強化され、通信事業者やエンタープライズ規模に至るネットワーク全体のセキュリティソリューションを提供することになる。本 cPP におけるネットワークデバイスとは、ネットワークに接続された、ネットワークにおける基盤的な役割を有する、ハードウェアとソフトウェアの両方から構成されるデバイスである。TOE は、スタンドアロン型または分散型でもよい、ここで分散型 TOE とは、本 cPP の要件 (分散型ネットワークデバイス TOE のより詳細な記述がセクション 3 で提供される) を満たすために複数の特有のコンポーネントが論理的な部分の全体として動作することを要求するようなものとする。

仮想的なネットワークデバイス(vND)とは、仮想マシンの中で実行するようなネットワークデバイス機能のソフトウェア実装である。本 cPP は、本 cPP で要求されるものとして、製品が物理的な ND のすべての要件及び前提条件を満たすことができないような vND の評価を明確に除外する

これは以下を意味する：

- 仮想化レイヤ (またはハイパーバイザまたは仮想マシンマネジャー(VMM)) は、ND のソフトウェアスタックの一部と見なされ、ゆえに TOE の一部であり、関連する SFR を満たさなければならない (例、ハイパーバイザ管理者をセキュリティ管理者として扱うことによって)[2]。複数の VMM 上で実行可能な vND は、ベンダが等価性についてうまく説明できない限り、それぞれの主張された VMM 上でテストされなければならない(must)。

- 物理的ハードウェアは、(上記に含まれる例のように) TOE に同じように含まれる。vND は、ベンダが等価性についてうまく説明できない限り、それぞれの主張され

[2] セキュリティターゲットの関連 SFR を繰り返すことは、仮想化ソフトウェアのプロパティを別々にカバーするために役に立つかもしれない。

たハードウェアプラットフォームについてテストされなければならない(must)。

- 各物理的ハードウェアプラットフォームについて、vND インスタンスが 1 つだけ存在する。

- 非ネットワークデバイス機能を提供するような物理的プラットフォーム上には、その他一切のゲスト VM は存在しない。

本書の意図は、デバイスの究極のセキュリティ目的、またはデバイスが採用し得る追加のセキュリティ機能に関わらず、すべてのネットワークデバイスに期待される共通セキュリティ機能のベースラインとして定義することである。本ベースラインには、リモート管理用の経路をセキュアに保つこと、ローカルとリモートの両方のログイン用の識別と認証サービスの提供、セキュリティ関連事象の監査、アップデートの供給元に対する暗号技術的な検証、及び一般的なネットワークベースの攻撃に対する保護の提供、が含まれる。

ねらいは、本 cPP を満たすネットワークデバイスがネットワーク上で「行儀よくふるまう」こと、そして害をなさないと信頼できることである。これを達成するため、外部エンティティへの通信パスを保護するため、分散型 TOE の場合、TOE コンポーネント間の通信を保護するため、ネットワークデバイスには、IPsec、TLS/DTLS、または SSH 等の標準ベースのトンネルプロトコルを採用することが期待される。許容されるセキュアチャネルプロトコルのほとんどの選択肢については、また、X.509 証明書が認証目的で使用されることも要求される ; 証明書の用途は、コード署名／ディジタル署名用のオプションとしてサポートされる。

ネットワークデバイスが採用できる追加のセキュリティ機能は、本 cPP の適用範囲外であり、このような機能は、他のデバイス種別に特化した cPP で規定される。同様に適用範囲外とみなされるものには、ウイルス (訳注 : ウイルス対策ソフト) 及び電子メールのスキャン、侵入検知／防止機能、セキュリティ機能としてのネットワークアドレス変換 (NAT)、及び上記で説明された事例を除き仮想化ネットワーク機能がある。本 cPP は、弾力性を増し、さまざまな実装 (例えばソフトウェアのみのネットワークデバイス) に対応し、そして技術の進歩に追随するために望まれるセキュリティ機能を拡張するために更新されることが期待される。しかし現時点では、本 cPP への完全適合 (Exact Conformance)[3] が要求され、また追加の機能は評価されない。

1.3 TOE ユースケース

ネットワークデバイス TOE 用の要件の本質は、デバイスがセキュアな方法でリモートから管理できること、そして適用されるソフトウェアアップデートが信頼される供給元からのものであることである。

本 cPP の要件によって網羅されるネットワークデバイスの例には、ルータ、ファイアウォール、VPN ゲートウェイ、IDS、及びスイッチ等が挙げられる。このようなデバイスが、その製品の個別のセキュリティ要件として重要な追加機能が含まれる場合には、別の cPP が

[3] 完全適合(Exact Conformance)は、完全適合(Strict Conformance)のサブセットとして特定される。セクション 2 の定義を参照のこと。

それらのデバイスで使用するために作成されるかもしれない、その cPP には、ネットワークデバイス cPP の要件のスーパーセットが含まれることになる。 例えば、この種の別 cPP として、ステートフルトラフィクフィルタファイアウォール用に作成されている。

ネットワークへ接続するデバイスではあるが、本 cPP への適合評価されるものに含まれないものの例としては、モバイルデバイス、エンドユーザ向けワークステーション、及び仮想化ネットワークデバイス機能等が含まれる。

2. CC 適合

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

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

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

本 cPP に適合するためには、TOE は完全適合 (Exact Conformance) を論証しなければならない。完全適合は、CC に定義されている正確適合 (Strict Conformance) のサブセットとして、本 cPP のセクション 6 のすべての SFR (これらは必須要件である) を含み、本 cPP の附属書 A (これらはオプション SFR である) または附属書 B (これらは選択ベース SFR であって、その一部は他の SFR における選択に従って必須とされる) の SFR を含む可能性のある ST として定義されている。繰り返しは許容されるが、いかなる追加の要件 (CC パート 2 または 3 からのもの、または本 cPP に既に含まれているもの以外の拡張コンポーネントの定義からのもの) も ST に含めることは許容されない。さらに、本 cPP のセクション 6 のいかなる SFR も、省略は許されない。

3. 分散型 TOE の導入

本 cPP は、分散型ネットワークデバイスのサポートを含む。ネットワークデバイスは、しばしば論理的な部分の全体としてとして動作している複数のコンポーネントから構成される可能性がある。多くの場合、我々は、分散したコンポーネントに対して管理を提供するために集中管理コンソールが使用されるような製品を取り扱うときに、このアーキテクチャを目にする。

数多くの異なるアーキテクチャがあるが、基本的に、以下のようなモデルの派生品であり、それらは 2 つのコンポーネントが設置され、一緒に動作する場合にのみ、本 cPP の SFR が満たされる可能性がある。

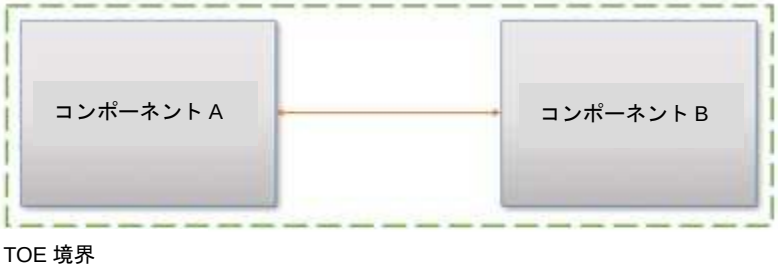


図 1：一般化された分散 TOE モデル

3.1 サポートされる分散型 TOE のユースケース

以下の説明は、本 cPP の本バージョンでサポートされる分散型 TOE にわたるガイダンスを提供する。

ケース 1：本 cPP 要件は、いくつかの TOE コンポーネントが一緒に動作する場合にのみ満たされることができる

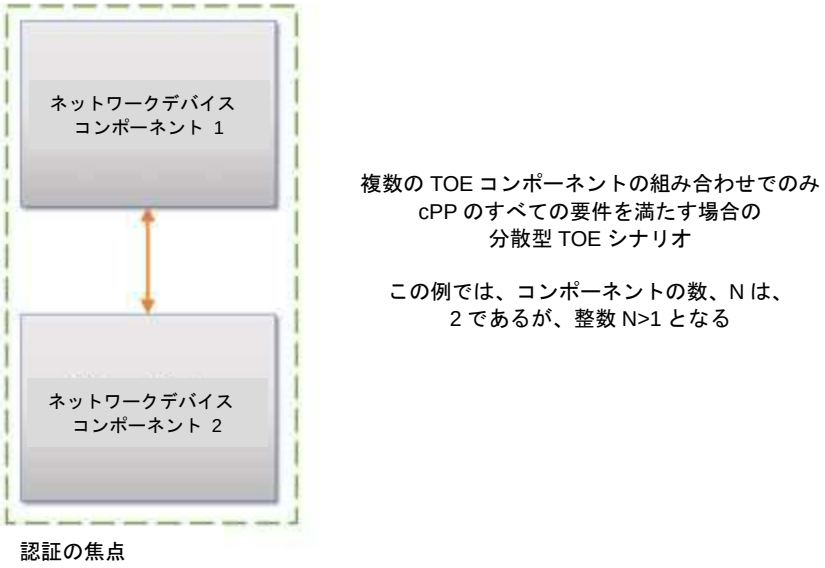


図 2：基本的な分散型 TOE ユースケース

最初の、最も基本的なユースケースは、本 cPP の要件を満たすために、複数の相互接続されたネットワークデバイスコンポーネントが一緒に動作する必要があるようなものである。分散型 TOE と見なされるために、少なくとも 2 つの相互接続されたコンポーネントが要求される。

ケース 2：cPP 要件が管理コンポーネントなしに満たされることができる。

いくつかのネットワークデバイスが管理コンポーネントと並行して動作するよう設計されている。このやり方で動作するが管理コンポーネントなしに本 cPP のすべての SFR を満たすことのできるネットワークデバイスは、分散型 TOE として見なされてはならない(shall not)、そして管理コンポーネントなしで本 cPP に従って認証されなければならない(shall)。

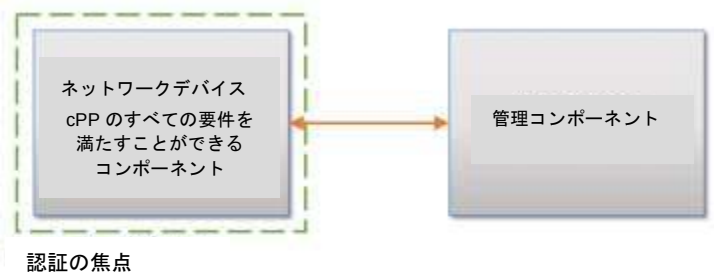


図 3：非分散型 TOE のユースケース

それとは別に、ネットワークデバイスは、本 cPP の要件すべてを満たすために、複数のコンポーネントを必要とすることがある。本 cPP を満たすために必要なコンポーネントへの追加として、管理コンポーネントが、TOE を用いた利用のために提供されることがある。しかし、上記の図 3 で示されるケースのように、認証には、このケースの管理コンポーネントを含んではならない(shall not)。この状況は、図 4 で図示される。

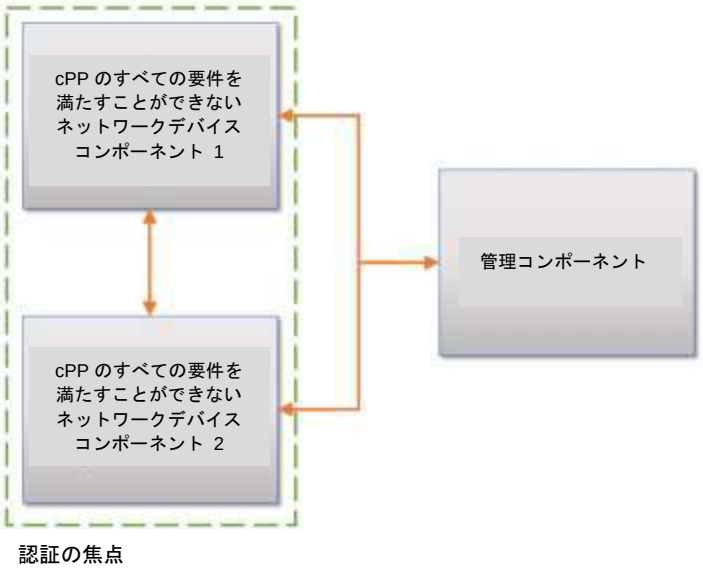


図 4：適用範囲外の管理コンポーネントを持つ分散型 TOE ユースケース

図 3 と図 4 の両方の場合について、管理コンポーネントは、異なる(c)PP に従って、別途、認証されてもよい。

ケース 3：cPP 要件は、管理コンポーネントなしに満たされることができない

本 cPP のすべての SFR を満たすために管理コンポーネントが必要とされるようなネットワークデバイスは、分散型 TOE とあると見なされ、本 cPP に従って管理コンポーネントと一緒に認証されなければならない(shall)。

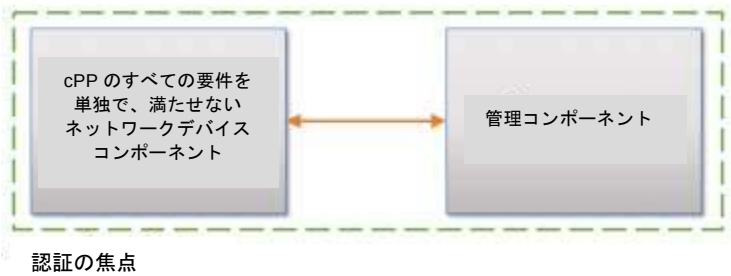


図 5：cPP 要件を満たすことが要求される管理コンポーネント

管理コンポーネントは、本 cPP のすべての SFR を満たすことが要求される場合、複数の分散型ネットワークデバイスと共に分散型 TOE の一部としても見なされてもよい。

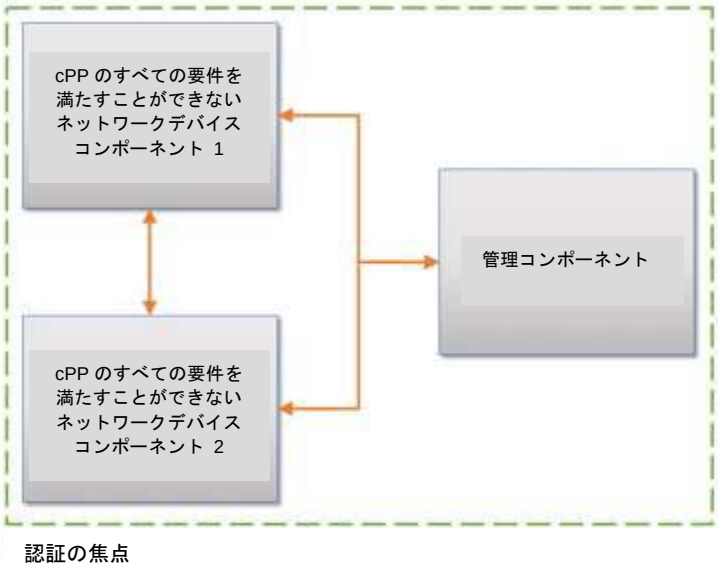


図 6：分散型ネットワークデバイスと cPP 要件を満たすことが要求される管理コンポーネント

1 つの管理コンポーネントによって複数のネットワークデバイスが管理されるような場合、TOE は、分散型であると見なされるが、認証の焦点は、ネットワークデバイスと管理コンポーネントの最も簡単な組み合わせに制限されるべきである(should)。等価性の説明を

用いることにより、1 つの管理コンポーネントと一緒に複数のネットワークデバイスの組み合わせは、認証されたソリューション [4]として見なされることが可能である。

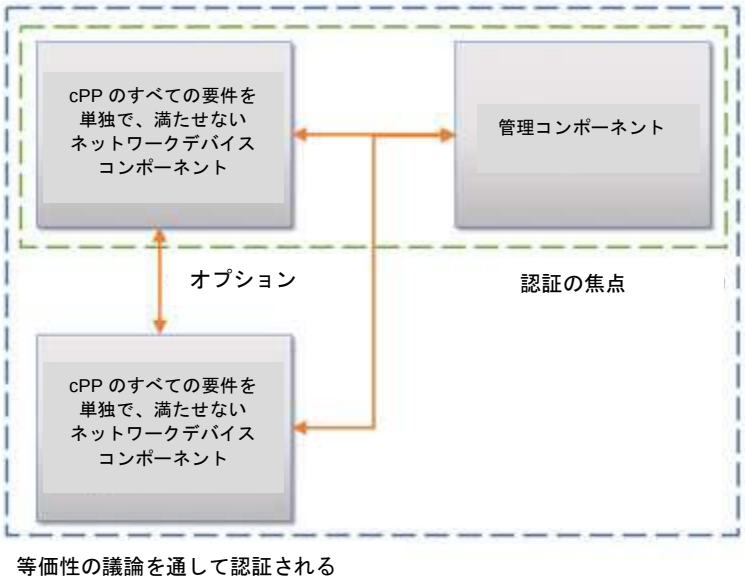


図 7：等価性の説明を通して拡張された分散型 TOE

このモデルでは、個別のネットワークデバイスコンポーネントは、本 cPP の要件を満たすために管理コンポーネント内の機能に依存しており、ゆえにネットワークデバイスコンポーネント自体の間の直接的な関係は、オプションである。

1 つ以上の管理コンポーネントは冗長性の目的だけのためである場合に使用されてもよい。

3.2 非サポートの分散 TOE のユースケース

以下の説明は、本 cPP のバージョンによってサポートされないような、分散型 TOE ユースケースについてのガイダンスを提供する。

ケース 4：cPP 要件が分散型 TOE の適用範囲外にあるその他のコンポーネントと共有される管理コンポーネントの利用に依存する

[4] [SD、B.4] には、「最小構成」および等価なコンポーネントのくりかえりの許容の観点から分散型 TOE のコンポーネントの定義方法について記述されている。

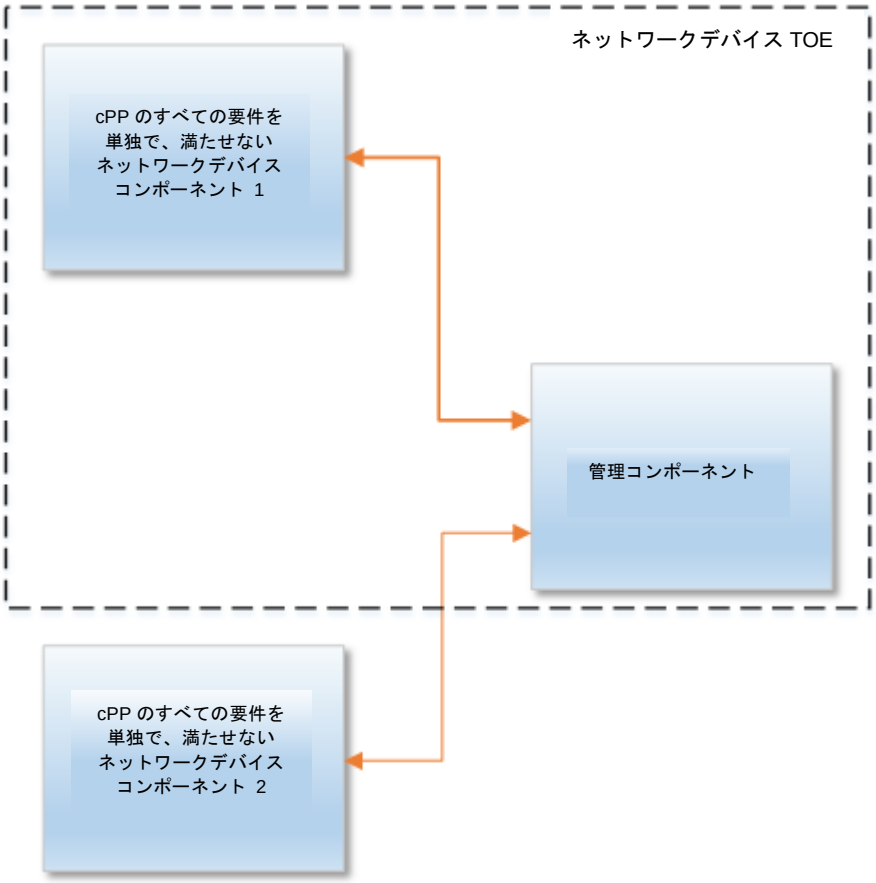


図 8：サポートされない企業での管理のユースケース

上記ケース 3 と明らかに似ているが、このケースでは単一の管理コンポーネントが分散型ネットワークデバイス TOE と別の区別された製品 (図 8 は、その他の製品がファイアウォールデバイスであるような例を示す) と共有される。このケースでは、管理コンポーネントは、「企業の管理者」(異なる種別のデバイスのための集中管理コンポーネント) であると見なされ、このユースケースは、本 cPP のこのバージョンではサポートされない。同様な状況は、その他のネットワークデバイス TOE コンポーネントが別の製品と共有された場合に適用される。

ケース 5：cPP 要件が複数の管理コンポーネントなしに満たされることが可能でない

上記ケース 3 に従った、分散型 TOE または TOE の組み合わせからなる 1 つのデバイスが 1 つ以上の管理コンポーネントによって管理されるようなケース (冗長性の目的は除く) は、本 cPP のこのバージョンによってカバーされない。

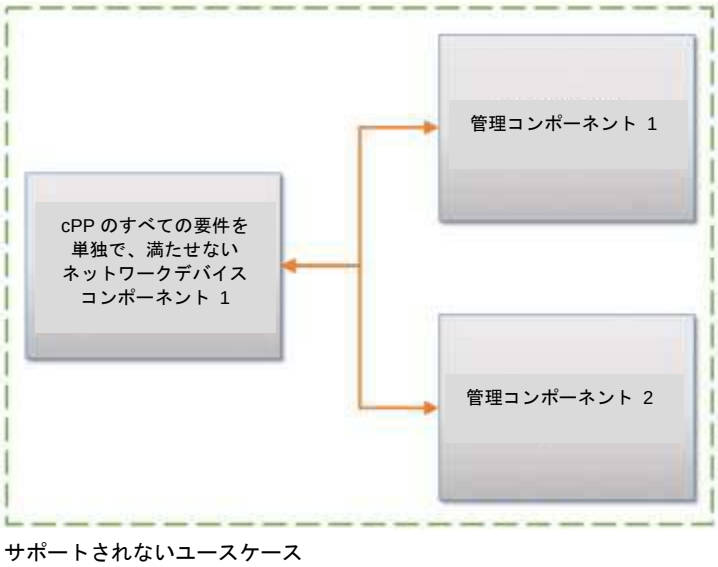
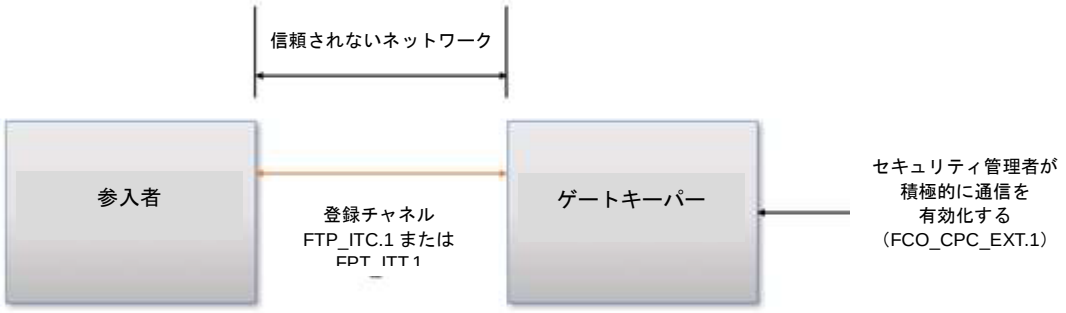


図 9：複数の管理コンポーネントを持つサポートされないユースケース

3.3 分散 TOE のコンポーネントの登録

分散型 TOE を取り扱うとき、多くの別々のコンポーネントは、TOE を作成するために運用環境に一緒に持ち込まれる必要がある：この要件は高信頼通信チャネルがコンポーネントの特定のペアに間でセットアップされることを要求する(すべてのコンポーネントが少なくとも 1 つのその他のコンポーネントと通信する必要があるが、すべてのコンポーネントがすべてのその他のコンポーネントと通信する必要はないと仮定される)。

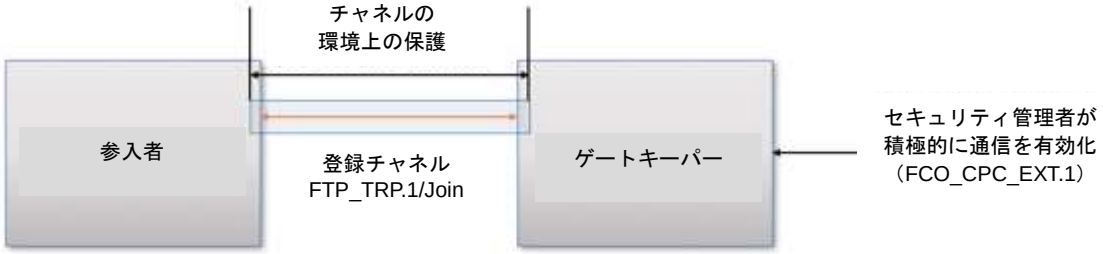
TOE の作成用に基礎となるモデルは、コンポーネントが TOE に「参入(join)」する「登録プロセス」を持つ。登録プロセスは、どちらかの 1 つ(「参入者(joiner)」)がその他(「ゲートキーパー」)に登録することによって既存の TOE に参入しようとする、2 つのコンポーネントから開始する。2 つのコンポーネントは、1 つ以上の規定された認証と通信チャネルオプションを使用するので、コンポーネントは相互に認証し、登録プロセス中に送信されるあらゆる機微なデータを保護する(例、鍵はゲートキーパーによって参入者へ登録の結果として送信される)。以下の図は、3 つのサポートされる登録モデルについて説明する。図 10 は、登録交換を保護するために FPT_ITT.1 または FTP_ITC.1 のインスタンスを用いるような分散型 TOE 登録アプローチについて説明する。



1) 登録は、任意の信頼されないネットワークを介して行われるかもしれない
2) 登録は、IPsec、TLS、SSH、または HTTPS チャネルを介して実行される
3) 証明書失効チェックが実行されない場合、FPT_ITT.1 を選択する
4) 証明書失効チェックが実行される場合、FTP_ITC.1 を選択する
5) 登録チャネルは、TSF 内通信のために再利用されるかもしれない

図 10：FPT_ITT.1 または FTP_ITC.1 を満たすチャネルを用いる分散型 TOE の登録

第 2 のアプローチ (図 11) は、別の登録チャネルを活用し、そのチャネルが登録情報交換に必要な保護を提供するための環境セキュリティ制約に依拠するようなユースケースをサポートする。



1) 登録チャネルは、認証され、完全性保護とオプションで機密性保護を提供しなければならない
2) 登録チャネルは、その保護のいくつかの観点について環境上の制約に依存し、または保護の強度の増加に依存する、例、参入者とゲートキーパー間の直接的で物理的なコネクション(FTP_TRP.1/Join)
3) 登録チャネルは、再利用されてはならず、登録が FPT_ITT.1 または FTP_ITC.1 のいずれかを満たす TSF 内チャネルを用いて登録が完了した後に置換されなければならない

図 11：FTP_TRP.1/Join を満たすチャネルを用いた分散型 TOE の登録

最後のアプローチ (図 12) は、登録が参入者とゲートキーパーの両方での直接設定することによって手動で実行されるようなユースケースをサポートする。一度設定されると、2 つのコンポーネントは FPT_ITT.1 または FTP_ITC.1 を満たす内部 TSF チャネルを確立する。

図 12：登録チャネルなしの分散型 TOE の登録

それぞれの場合、登録プロセス中、セキュリティ管理者は、参入しようとするコンポーネントを、それが TSF の一部として動作できる前に、積極的に有効化しなければならない (must)。以下の図は、この有効化ステップが取ることのできるアプローチについて説明する：

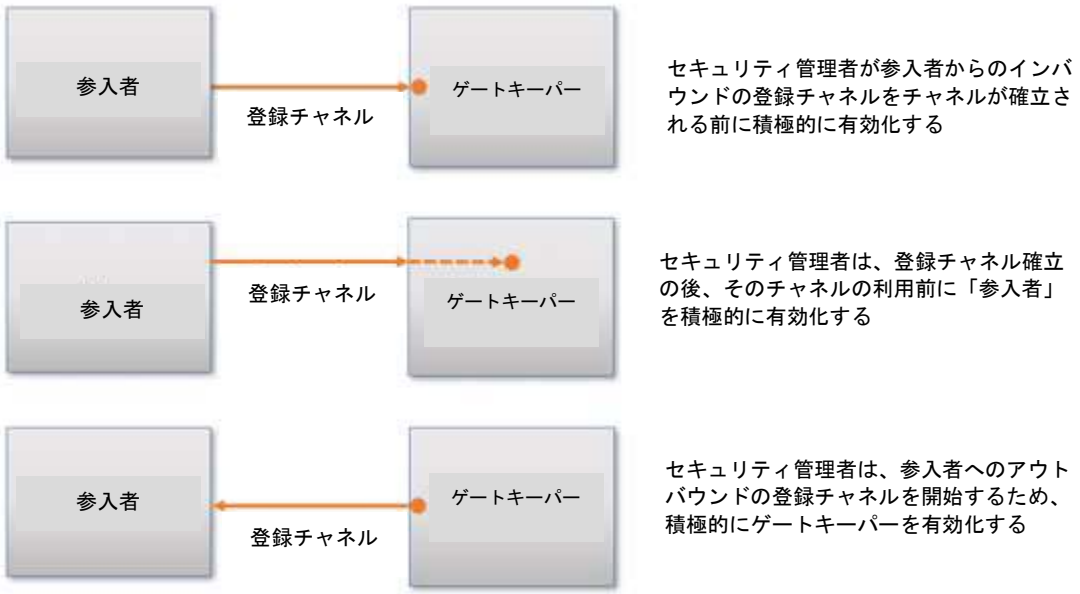


図 13：分散型 TOE の参入者有効化オプション

一切の登録チャネルが要求されず、参入者とゲートキーパーが直接設定される (図 12) ような場合に、有効化は、この直接設定プロセスの一部として含まれることに留意されたい。

登録後、コンポーネントは、通常の SSH/TLS/DTLS/IPsec/HTTPS チャネル (セクション 6 及び附属書 A の観点で FTP_ITC.1 または FPT_ITT.1 のインスタンスとして、ST で規定される) を用いてそれら自身の間で通信する。このコンポーネント間通信用のチャネルは、

新規の(拡張) SFR FCO_CPC_EXT.1 (セクション A.7.1 を参照) を用いて最上位レベルで規定され、さらに TOE の外部のエンティティとの通信用に要求されるその他の通信チャネル (FTP_ITC.1 および FPT_TRP.1 のインスタンスとして ST に規定される) へ追加である。

3.4 分散 TOE での要件のアロケーション

分散型 TOE について、本 cPP でのセキュリティ機能要件は、全体として TOE によって満たされる必要があるが、すべての SFR が必ずしもすべてのコンポーネントによって実装されるわけではない。以下の分類が、いつそれぞれの SFR が 1 つのコンポーネントによって実装されなければならないかを規定するために定義される：

- **すべてのコンポーネント （「すべて」）** — 分散型 TOE からなるすべてのコンポーネントは、独立に要件を満たさなければならない(must)。

- **少なくとも 1 つのコンポーネント（「1 つ」）** — 本要件は、分散型 TOE 内の少なくとも 1 つのコンポーネントによって満たされなければならない(must)。

- **機能依存 （「機能依存」）** — これらの要件は、機能が分散型 TOE コンポーネントによって実装されるようにのみ満たされる (全体として本 cPP を満たす要件がセクション 6 で規定される場合、これらは少なくとも 1 つのコンポーネントがこれらの要件を実装することを要求することに留意されたい)。

表 1 は、本 cPP のそれぞれの SFR が上記分類を用いて、どのように満たされなければならない(must) かについて規定する。

要件	記述	分散型 TOE SFR の割り当て
FAU_GEN.1	監査データ生成	すべて
FAU_GEN.2	利用者識別情報の関連付け	すべて
FAU_STG_EXT.1	保護された監査対象事象格納	すべて
FAU_STG.1	保護された監査証跡格納	機能依存
FAU_STG_EXT.2/LocSpace	喪失した監査データのカウント	機能依存
FAU_STG.3/LocSpace	ローカル格納領域の警告表示	機能依存
FCO_CPC_EXT.1	通信相手の制御	すべて
FCS_CKM.1	暗号鍵生成	1 つ [5]
FCS_CKM.2	暗号鍵確立	すべて
FCS_CKM.4	暗号鍵破棄	すべて

[5] 分散型 TOE のそれぞれのコンポーネントは、オンボード鍵生成および (TOE が附属書 B.3.1 のように X.509 証明書を使用する場合) RFC2986 証明書要求の生成を実行するか、またはそのコンポーネント TOE へ参入しようとするときにセキュアな登録チャネルを用いてその他の何らかの TOE のコンポーネント上で生成された鍵と証明書を受け取るか、のいずれかが要求されている。証明書要求の生成は、鍵を生成するコンポーネントか、鍵を受け取るコンポーネント化のいずれか、から要求されること。

要件	記述	分散型 TOE SFR の割り当て
FCS_COP.1/DataEncryption	暗号操作(AES データ暗号化／復号)	すべて
FCS_COP.1/SigGen	暗号操作(署名検証)	すべて
FCS_COP.1/Hash	暗号操作(ハッシュアルゴリズム)	すべて
FCS_COP.1/KeyedHash	暗号操作(鍵付きハッシュアルゴリズム)	すべて
FCS_DTLSC_EXT.1	DTLS クライアント	機能依存
FCS_DTLSC_EXT.2	相互認証付き DTLS クライアント	機能依存
FCS_DTLSS_EXT.1	DTLS サーバ	機能依存
FCS_DTLSS_EXT.2	相互認証付き DTLS サーバ	機能依存
FCS_HTTPS_EXT.1	HTTPS プロトコル	機能依存
FCS_IPSEC_EXT.1	IPsec プロトコル	機能依存
FCS_SSHC_EXT.1	SSH クライアント	機能依存
FCS_SSHS_EXT.1	SSH サーバ	機能依存
FCS_TLSC_EXT.1	TLS クライアント	機能依存
FCS_TLSC_EXT.2	相互認証付き TLS クライアント	機能依存
FCS_TLSS_EXT.1	TLS サーバ	機能依存
FCS_TLSS_EXT.2	相互認証付き TLS サーバ	機能依存
FCS_RBG_EXT.1	乱数ビット生成	すべて
FIA_AFL.1	認証失敗管理	1 つ
FIA_PMG_EXT.1	パスワード管理	1 つ
FIA_UIA_EXT.1	利用者の識別と認証	1 つ
FIA_UAU_EXT.2	パスワードベースの認証メカニズム	1 つ
FIA_UAU.7	保護された認証フィードバック	機能依存
FIA_X509_EXT.1/Rev	X.509 証明書検証	機能依存
FIA_X509_EXT.1/ITT	X.509 証明書検証	機能依存
FIA_X509_EXT.2	X.509 証明書認証	機能依存
FIA_X509_EXT.3	証明書要求	機能依存 [5]
FMT_MOF.1/ManualUpdate	高信頼アップデートーセキュリティ機能のふるまいの管理	すべて
FMT_MOF.1/Services	高信頼アップデートーTSF データの管理	すべて
FMT_MOF.1/Functions	セキュリティ機能のふるまいの管理	すべて
FMT_MTD.1/CoreData	TSF データの管理	すべて
FMT_MTD.1/CryptoKeys	TSF データの管理	機能依存
FMT_SMF.1	セキュリティ機能の特定	機能依存
FMT_SMR.2	セキュリティ役割における制限	1 つ
FPT_SKP_EXT.1	TSF データの保護(すべての対称鍵の読み出し)	すべて
FPT_APW_EXT.1	管理者パスワードの保護	機能依存
FPT_TST_EXT.1	テスト(拡張)	すべて

要件	記述	分散型 TOE SFR の割り当て
FPT_ITT.1	基本 TSF 内データ転送保護	機能依存 [6]
FPT_STM.1	高信頼タイムスタンプ	すべて
FPT_TST_EXT.2	証明書に基づく自己テスト	機能依存
FPT_TUD_EXT.1	高信頼アップデート	すべて
FPT_TUD_EXT.2	証明書に基づく高信頼アップデート	機能依存
FTA_SSL.3	TSF 起動による終了	機能依存
FTA_SSL.4	利用者起動による終了	機能依存
FTA_SSL_EXT.1	TSF 起動セションロック	機能依存
FTA_TAB.1	デフォルト TOE アクセスバナー	1 つ
FTP_ITC.1	TSF 間高信頼チャネル	1 つ
FTP_TRP.1/Admin	高信頼パス(詳細化)	1 つ
FTP_TRP.1/Join	高信頼パス	機能依存
FMT_MOF.1/ManualUpdate	セキュリティ機能のふるまいの管理	機能依存
FMT_MOF.1/AutoUpdate	セキュリティ機能のふるまいの管理	機能依存

表 1：分散型 TOE のセキュリティ機能要件

分散型 TOE 用の ST には、TOE のそれぞれのコンポーネントに対する SFR のマッピングを含まなければならない(must)。(この評価用提供物件は、ASE_TSS.1 および AVA_VAN.1 評価アクティビティの一部としてそれぞれ [SD、5.1.2] および [SD、5.6.1.1] で記述されるとおり検査されることに留意されたい。分差型 TOE 用の ST には、「最小構成」を導入してもよいし、CC 評価の有効性に影響しない運用上の構成に追加されるインスタンスを持ってもよいようなコンポーネントを特定してもよい。[SD、B.4]には、分散型 TOE のこれらの等価性の観点に関連する評価アクティビティ(およびゆえに ST で期待されるもの) が記述されている。)

[6] TSF 間データ転送を保護するため、FPT_ITT.1 または FTP_ITC.1 はそれぞれの分散型 TOE コンポーネントによって満たされなければならない(must)。これは、外部エンティティとの通信を保護するために FTP_ITC.1 の繰返しに追加である。

4. セキュリティ課題定義

ネットワークデバイスは、それが提供するように設計されたネットワーク基盤の役割を持つ。そうするにあたって、ネットワークデバイスは他のネットワークデバイスや他のネットワークエンティティ (即ち、基盤としての役割を持たないため、ネットワークデバイスとして定義されないエンティティ) とネットワーク上で通信する。同時に、すべてのネットワークデバイスに期待される最小限の共通セキュリティ機能を提供しなければならない。適合ネットワークデバイスによって対処されるべきセキュリティ課題は、特定の種別のネットワークデバイスの具体的な機能をターゲットとするものではなく、ネットワークデバイスに共通する脅威へ対抗する共通セキュリティ機能として定義される。共通セキュリティ機能は、ネットワークデバイス (正当なものと不当なものの両方) との通信、有効かつセキュアなアップデートを行う能力、デバイスアクティビティの監査を行う能力、デバイス及び管理者のクレデンシャル及びデータをセキュアに保存し利用する能力、そして重要なデバイスコンポーネントの故障を自己テストする能力に対処する。

4.1 脅威

ネットワークデバイスへの脅威は、以下のセクションに、デバイスの機能分野に従ってグループ化されている。それぞれの脅威の記述には、次にセクション 6、附属書 A、及び附属書 B の SFR によってどのように対処されるかを記述している根拠が続く。

4.1.1 ネットワークデバイスとの通信

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

許可された通信には、設計され意図されたとおりに、ネットワークデバイス宛へ及びネットワークデバイスからの、ポリシーによって許可されるネットワークトラフィクが含まれる。これには、通信を保護するためのセキュアなチャネルが要求され、ネットワークデバイス管理、及び認証または監査ログサーバとの通信等の重要なネットワークトラフィクが含まれる。 ネットワークデバイスのセキュリティ機能には、許可された通信のみが許されることを保証する機能、及び重要なネットワークトラフィク用のセキュアなチャネルを提供する機能が含まれる。それ以外の任意の通信は、不正な通信と考えられる。(ネットワークデバイスをトラバースするがそのデバイスが最終の宛先でないネットワークトラフィク、例、「ネットワークデバイスと通信」であると見なされないような、ルーティングされたパケット ー 参照、セクション 4.2.3 の A.NO_THRU_TRAFFC_PROTECTION。)

本 cPP で対処されるネットワークデバイス通信への主たる脅威は、重要なネットワークトラフィクに対するアクセス、改変、あるいは暴露を試行するような、外部の、許可されないエンティティに焦点を絞っている。 暗号アルゴリズムの不十分な選択、または非標準トン

ネルプロトコルの使用は、容易に推測できるパスワードやデフォルトパスワードの使用等の弱い管理者クレデンシャルと同様に、脅威エージェントに対してデバイスへの不正なアクセスを許可することになる。 弱い暗号または暗号化なしでは、トラフィクの保護はほとんどまたは全く提供されないため、ほとんど労力なしで脅威エージェントが重要なデータを読み出したり、操作したり、あるいは制御することができてしまう。非標準トンネルプロトコルは、デバイスの相互接続性を制限してしまうだけでなく、ピアレビューによる規格化が提供する保証及び信頼を欠くことになる。

4.1.1.1 T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

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

SFR 根拠：

- 管理者役割は、FMT_MOF.1/Services 及び FMT_MOF.1/Functions のオプションの追加機能とともに、FMT_SMR.2 で定義され、関連する管理者機能は、FMT_SMF.1 及び FMT_MTD.1/CoreData で定義される。
- 管理者の認証の前に許可されるアクションは、FIA_UIA_EXT.1 によって制約を受け、FTA_TAB.1 に従って表示されるアドバイザリ通知と同意警告メッセージを含む。
- 管理者認証プロセスの要件は、FIA_UAU_EXT.1 に記述されている。
- 管理者セションのロックは、FTA_SSL_EXT.1 (ローカルセション用)、FTA_SSL.3 (リモートセション用)、及び FTA_SSL.4 (すべての対話セション用) によって保証される。
- リモート管理者コネクション用に使用されるセキュアチャネルは、FPT_TRP.1/Admin で規定される。
- (管理者セションから実行される悪意のあるアクションは、T.UNDETECTED_ACTIVITY によって別々に対処される)
- (管理者クレデンシャルの保護は、T.PASSWORD_CRACKING によって別々に対処される)。

4.1.1.2 T.WEAK_CRYPTOGRAPHY

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

SFR 根拠：

- 鍵生成と鍵配付の要件は、FCS_CKM.1 及び FCS_CKM.2 でそれぞれ設定される
- 暗号スキームの使用の要件は、FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、及び FCS_COP.1/KeyedHash で設定される
- 鍵生成とセキュアプロトコルをサポートするための乱数ビット生成の要件 (T.UNTRUSTED_COMMUNICATION_CHANNELS からの SFR を参照) は、FCS_RBG_EXT.1 で設定される
- 暗号機能の管理は、FMT_SMF.1 で規定される。

4.1.1.3 T.UNTRUSTED_COMMUNICATION_CHANNELS

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

SFR 根拠：

- 規定された通信チャネルのセキュアプロトコルの一般的な使用は、FTP_ITC.1 及び FTP_TRP.1/Admin の最上位レベルで記述されている；分散型 TOE については、コンポーネント間通信の要件は、FPT_ITT.1 の要件によって対処される
- セキュア通信プロトコルの使用のための要件は、FCS_HTTPS_EXT.1、FCS_IPSEC_EXT.1、FCS_SSHC_EXT.1、FCS_SSHS_EXT.1、FCS_TLSC_EXT.1、FCS_TLSC_EXT.2、FCS_TLSS_EXT.1、FCS_TLSS_EXT.2 で許容されたすべてのプロトコルについて設定される
- セキュアプロトコルをサポートするための公開鍵証明書の使用のためのオプション及び選択ベースの要件は、FIA_X509_EXT.1、FIA_X509_EXT.2、FIA_X509_EXT.3 で定義される。

4.1.1.4 T.WEAK_AUTHENTICATION_ENDPOINTS

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

SFR 根拠：

- エンドポイントの認証を提供するための適切なセキュアプロトコルの使用 (T.UNTRUSTED_COMMUNICATION_CHANNELS に対処している SFR にあるような) は、FTP_ITC.1 及び FTP_TRP.1/Admin の要件によって保証される ; 分散型 TOE については、コンポーネント間通信におけるエンドポイントのための認証要件は、FPT_ITT.1 の要件によって対処される
- 分散型 TOE コンポーネントの登録中のセキュアな認証の追加的な起こりうる特別な場合について、FCO_CPC_EXT.1 及び FTP?TRP.1/Join によって対処される。

4.1.2 有効なアップデート

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

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

4.1.2.1 T.UPDATE_COMPROMISE

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

SFR 根拠：

- アップデートの保護のための要件は、FPT_TUD_EXT.1 で設定される
- 署名の証明書ベースの保護の追加的なオプションの使用については、FIA_X509_EXT.1、FIA_X509_EXT.2 及び FIA_X509_EXT.3 の X.509 証明書を処理する要件によってサポートされる、FPT_TUD_EXT.2 を用いて規定が可能である
- アップデートの管理のための要件は、FMT_MOF.1/AutoUpdate の自動アップデートのオプション要件とともに、FMT_SMF.1 及び(手動アップデートについては) FMT_MOF.1/ManualUpdate で定義される

4.1.3 監査されたアクティビティ

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

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

4.1.3.1 T.UNDETECTED_ACTIVITY

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

SFR 根拠：

- 基本監査機能の要件は、FPT_STM.1 に従って提供されるタイムスタンプとともに、FAU_GEN.1 及び FAU_GEN.2 で規定される
- TOE に格納されたローカル監査記録のセキュアな送信の要件は、FAU_STG.1 で規定される
- セキュアなチャネル経由でのローカル監査記録の外部 IT エンティティへのセキュアな送信の要件は、FAU_STG_EXT.1 で規定される
- ローカルに格納された監査記録の潜在的な喪失に対処するためのオプションの追加的な要件は、FAU_STG_EXT.2/LocSpace、FAU_STG_EXT.3/LocSpace 及び FPT_FLS.1/LocSpace で規定される
- 監査機能の (オプションの) 設定が TOE によって提供される場合、これは FMT_SMF.1 で規定され、この機能をセキュリティ管理者へ制限することは、FMT_MOF.1/Functions によって要求される。

4.1.4 管理者及びデバイスのクレデンシャル並びにデータ

ネットワークデバイスには、セキュアに保存しなければならない、かつ許可されたエンティティに対してアクセスを適切に制限しなければならない、データ及びクレデンシャルが含

まれている。例としては、デバイスのファームウェア、ソフトウェア、セキュアチャネル用の設定認証クレデンシャル、及び管理者クレデンシャル等が含まれる。デバイス及び管理者の鍵、鍵材料、及び認証クレデンシャルは、不正な暴露及び改変から保護される必要がある。さらに、デバイスのセキュリティ機能は、管理者パスワードのような、デフォルトの認証クレデンシャルが変更されることを要求する必要がある。

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

4.1.4.1 T.SECURITY_FUNCTIONALITY_COMPROMISE

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

SFR 根拠：

- セキュリティ侵害に対する秘密／プライベート鍵の保護は、FPT_SKP_EXT.1 で規定される
- 鍵のセキュアな破壊は、FCS_CKM.4 で規定される
- (オプションで)鍵の管理が TOE によって提供される場合、これは、FMT_SMF.1 で規定され、本機能をセキュリティ管理者に限定することは FMT_MTD.1/CryptoKeys によって要求される。
- (パスワードの保護は、別々に T.PASSWORD_CRACKING の下でカバーされる)。

4.1.4.2 T.PASSWORD_CRACKING

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

SFR 根拠：

- パスワード長及び利用可能な文字の要件は、FIA_PMG_EXT.1 で設定される
- 見えなくされたフィードバックのみを提供することによるパスワード入力の保護は、FIA_UAU.7 で規定される

- 連続したパスワード失敗回数がしきい値に達した時のアクションは、FIA_AFL.1 で規定される
- パスワードのセキュアなストレージの要件は、FPT_APW_EXT.1 で設定される。

4.1.5 デバイスの障害

ネットワークデバイスのセキュリティメカニズムは、信頼のルートからより複雑な一連のメカニズムが構築されるのが一般的である。障害は、デバイスのセキュリティ機能の危殆化を引き起こす可能性がある。起動時及び実行中の両方でセキュリティ上重要なコンポーネントの自己テストを行うネットワークデバイスは、デバイスのセキュリティ機能の信頼性を保証する。

4.1.5.1 T.SECURITY_FUNCTIONALITY_FAILURE

ネットワークデバイスのコンポーネントは、起動時または運用中に、ネットワークデバイスのセキュリティ機能の危殆化または障害により、デバイスが攻撃者の影響を受け、機能しなくなるかもしれない。

SFR 根拠：

- 自己テストの実行の要件は、FPT_TST_EXT.1 で定義される
- 自己テストをサポートするため、オプションでの証明書の使用は FPT_TST_EXT.2 で定義される (FIA_X509_EXT.1、FIA_X509_EXT.2、及び FIA_X509_EXT.3 の証明書の使用に対するサポートを用いて)。

4.2 前提条件

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

4.2.1 A.PHYSICAL_PROTECTION

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

[OE.PHYSICAL]

4.2.2 A.LIMITED_FUNCTIONALITY

デバイスは、そのコアな機能としてネットワーク機能を提供し、また汎用コンピューティングとみなされるような機能／サービスは提供しないと想定される。例えば、デバイスは、(ネットワーク機能と無関係な) 汎用アプリケーション用のコンピューティングプラットフォームを提供するべきでない。

[OE.NO_GENERAL_PURPOSE]

4.2.3 A.NO_THRU_TRAFFIC_PROTECTION

標準的な／一般的なネットワークデバイスは、それを通過するトラフィクの保護に関して一切の保証を提供しない。その意図は、デバイスが、管理用データ及び監査データを含め、ネットワークデバイスからの、またはデバイス宛のデータを保護することである。他のネットワークエンティティ宛の、ネットワークデバイスを通過するようなトラフィクは、ND cPP により対処されない。この保護は、特定の種別のネットワークデバイス (例、ファイアウォール等) 用の cPP により対処されると想定される。

[OE.NO_THRU_TRAFFIC_PROTECTION]

4.2.4 A.TRUSTED_ADMINISTRATOR

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

[OE.TRUSTED_ADMIN]

4.2.5 A.REGULAR_UPDATES

ネットワークデバイスのファームウェア及びソフトウェアは、既知の脆弱性による製品アップデートのリリースに対応して定期的に管理者によってアップデートされると想定される。

[OE.UPDATES]

4.2.6 A.ADMIN_CREDENTIALS_SECURE

ネットワークデバイスへアクセスするために使用される管理者のクレデンシャル (プライベート鍵) は、それが動作するプラットフォームによって保護される。

[OE.ADMIN_CREDENTIALS_SECURE]

4.2.7 A.COMPONENTS_RUNNING (分散型 TOE のみに適用)

分散型 TOE について、すべての TOE コンポーネントの可用性が 1 つ以上の TOE コンポーネント (またはその障害) 上での検知されない攻撃のリスクを軽減するために適切であることがチェックされていることが想定されている。すべてのコンポーネントの可用性に追

加してすべての TOE コンポーネント上で監査機能の適切な動作がチェックされ期待通りに適切であることも想定されている。

[OE.COMPONENTS_RUNNING]

4.2.8 A.RESIDUAL_INFORMATION

その装置が廃棄され、または運用環境から除去されるとき、管理者は、ネットワーク装置上の機微な残存情報 (例、暗号鍵、鍵材料、PIN、パスワード等) に対して発生し得る一切の許可されないアクセスがないことを保証しなければならない(must)。

[OE.RESIDUAL_INFORMATION]

4.3 組織のセキュリティ方針

組織のセキュリティ方針は、組織がそのセキュリティニーズへ対処するために課している一連の規則、実践、及び手続きである。各方針の記述は、セクション 6、附属書 A,及び附属書 B の SFR によってどのように対処されるかについての根拠が後に続く。

4.3.1 P.ACCESS_BANNER

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

SFR 根拠：

- アドバイザリ通知及び同意警告メッセージは、FTA_TAB.1 によって表示されるよう要求される

5. セキュリティ対策方針

5.1 運用環境のセキュリティ対策方針

以下のサブセクションで、運用環境の対策方針を記述する。

5.1.1 OE.PHYSICAL

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

5.1.2 OE.NO_GENERAL_PURPOSE

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

5.1.3 OE.NO_THRU_TRAFFIC_PROTECTION

TOE は、それを通過するトラフィクの保護を一切提供しない。このトラフィクの保護は、運用環境の他のセキュリティ及び保証対策によって対処されると想定される。

5.1.4 OE.TRUSTED_ADMIN

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

5.1.5 OE.UPDATES

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

5.1.6 OE.ADMIN_CREDENTIALS_SECURE

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

5.1.7 OE.COMPONENTS_RUNNING (分散型 TOE のみに適用)

分散型 TOE について、TOE 管理者は、すべての TOE コンポーネントの可用性が 1 つ以上の TOE コンポーネント (またはその障害) 上での検知されない攻撃のリスクを軽減するために適切であることがチェックされていることを保証する。TOE 管理者は、監査機能が適切に実行中のすべてのコンポーネントについて適切であることがチェックされることも保証する。

5.1.8 OE.RESIDUAL_INFORMATION

TOE 管理者は、その装置が廃棄され、または運用環境から除去されるとき、ネットワーク装置上の機微な残存情報 (例、暗号鍵、鍵材料、PIN、パスワード等) に対して発生し得る一切の許可されないアクセスがないことを保証する。

6. セキュリティ機能要件

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

分散型 TOE について、ST 作成者は、各 SFR がどのように満たされるべき (should) かについてのガイダンスのため表 1 を参照するべきである。表は、SFR がすべての TOE コンポーネントによって、少なくとも 1 つの TOE コンポーネントによって、満たされるべきか、または TOE コンポーネントによって実装されている機能にそれらが依存しているかどうかについて詳述する。分散型 TOE の ST は、TOE のコンポーネントのそれぞれに対する SFR のマッピングを含まなければならない(must)。(この評価用提供物件が[SD、5.1.2]及び[SD、5.6.1.1]のそれぞれに記述される通り、ASE_TSS.1 及び AVA_VAN.1 評価アクティビティの一部として検査されることに留意されたい)。

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

6.1 表記法

SFR の記述に用いられる表記法は以下のとおり：

- 変更されない SFR は、[CC2] またはそれらの拡張コンポーネント定義 (ECD) で利用される様式で記述される；
- 本 PP でなされた詳細化：詳細化されたテキストは、**太字テキスト**及び~~取り消し線~~で示される；
- 本 PP で全体または一部完成された選択：選択の値 (即ち、本 PP で採用された選択の値または ST で利用可能なものとして残っている選択の値) は、下線付きテキストで示される

  例、[CC2]または ECD での「[選択：*暴露*、*改変*、*利用の喪失*]」は、本 PP では「暴露」(完成) または 「[選択：暴露、改変]」(部分完成) となるだろう；
- 本 PP で全体または一部完成された割付：*イタリック体*テキストで示される；
- 本 PP での選択内で完成された割付：完成された割付テキストは、*イタリック体の下線付きテキスト*で示される

  例、[CC2] または ECD での「[選択：*デフォルト変更*、*問い合わせ*、*改変*、*削除*、*[割付：その他の操作]*]」は、本 PP では「*デフォルト変更*、*タグ選択*」(選択と割付の両方の完成) または「[選択：*デフォルト変更*、*タグ選択*、*値選択*]」(選択の部分完成と割付の完成) となるだろう；
- 繰り返し：「/」で始まる文字列を追加して示される (例、「FCS_COP.1/Hash」) 。

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

RFC への適合が SFR において参照されているが、これは、関連する SFR について、[SD]における関連する保証アクティビティを強制するによって実証されることを意図している。

6.2 SFR アーキテクチャ

図 14、図 15、図 16、図 17、図 18 及び図 19 は、セクション 6.3～6.9、附属書 A 及び附属書 B のセキュリティ機能要件と、TOE が提供する基盤となる機能領域及び操作との間の結び付きを図示したものである。この図では、TOE の利用に関する SFR の文脈を提供しているが、その他のセクションでは [CC2] の抽象クラス及びファミリグループによってグループ分けして SFR を定義している。

図において、附属書 B からの SFR は、「裁量」としても記述される、それらを ST への含めるかどうかは製品の特定の特性に依存することを意味している。ST により要求される附属書 B からの SFR は、他の SFR で行われた選択により決定される。例えば: (それぞれ 6.9.1.1 及び 6.9.2.1 における) FTP_ITC.1 及び FTP_TRP.1/Admin はそれぞれ、SFR によって記述されるセキュアなチャネルの種別において使用されるプロトコルの選択を含んでいる。ここでのプロトコルの選択が、セクション B.2.1 のプロトコル特有 SFR のどれが ST に要求されるかについても決定する。附属書 A の SFR は、それらが TOE によって提供される場合に ST に含めることができるが、TOE が本 cPP への適合を主張するために必須ではない。

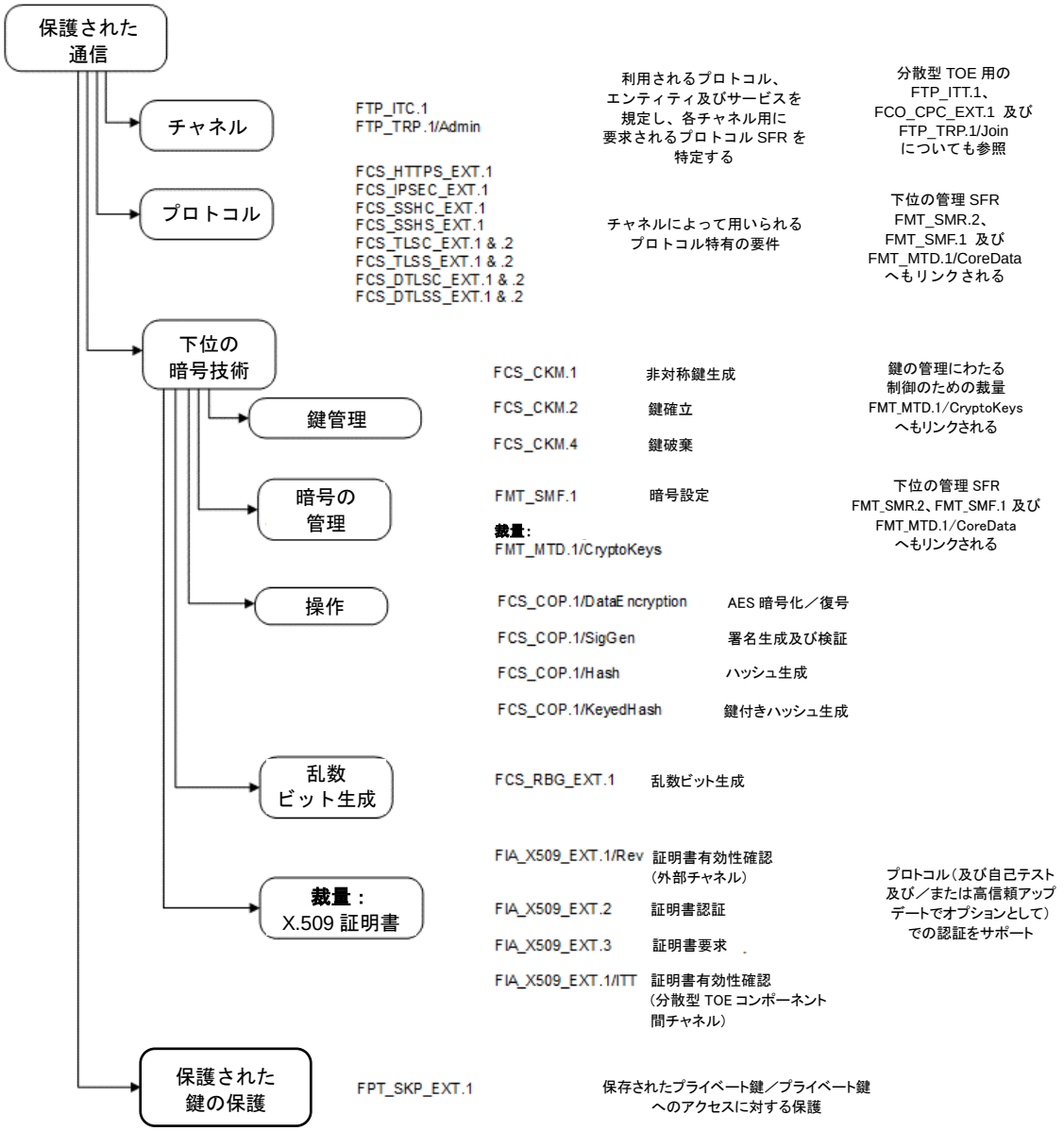


図 14：保護された通信の SFR アーキテクチャ

図 15：管理者認証の SFR アーキテクチャ

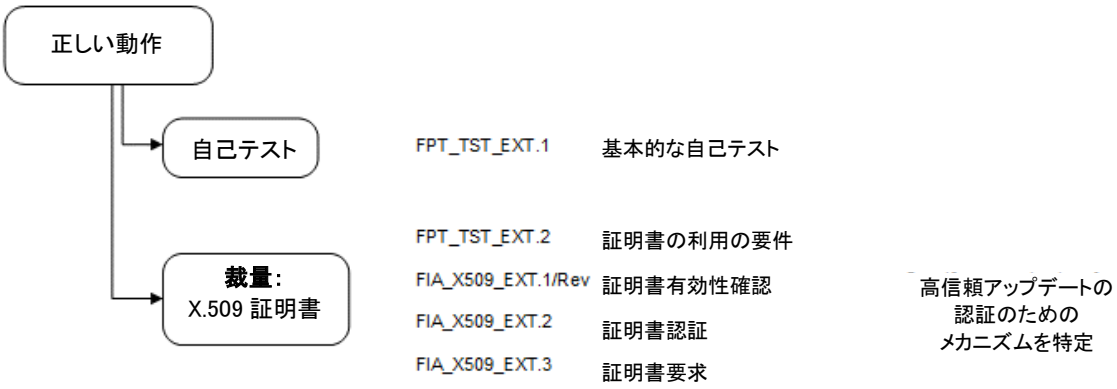


図 16：正しい動作の SFR アーキテクチャ

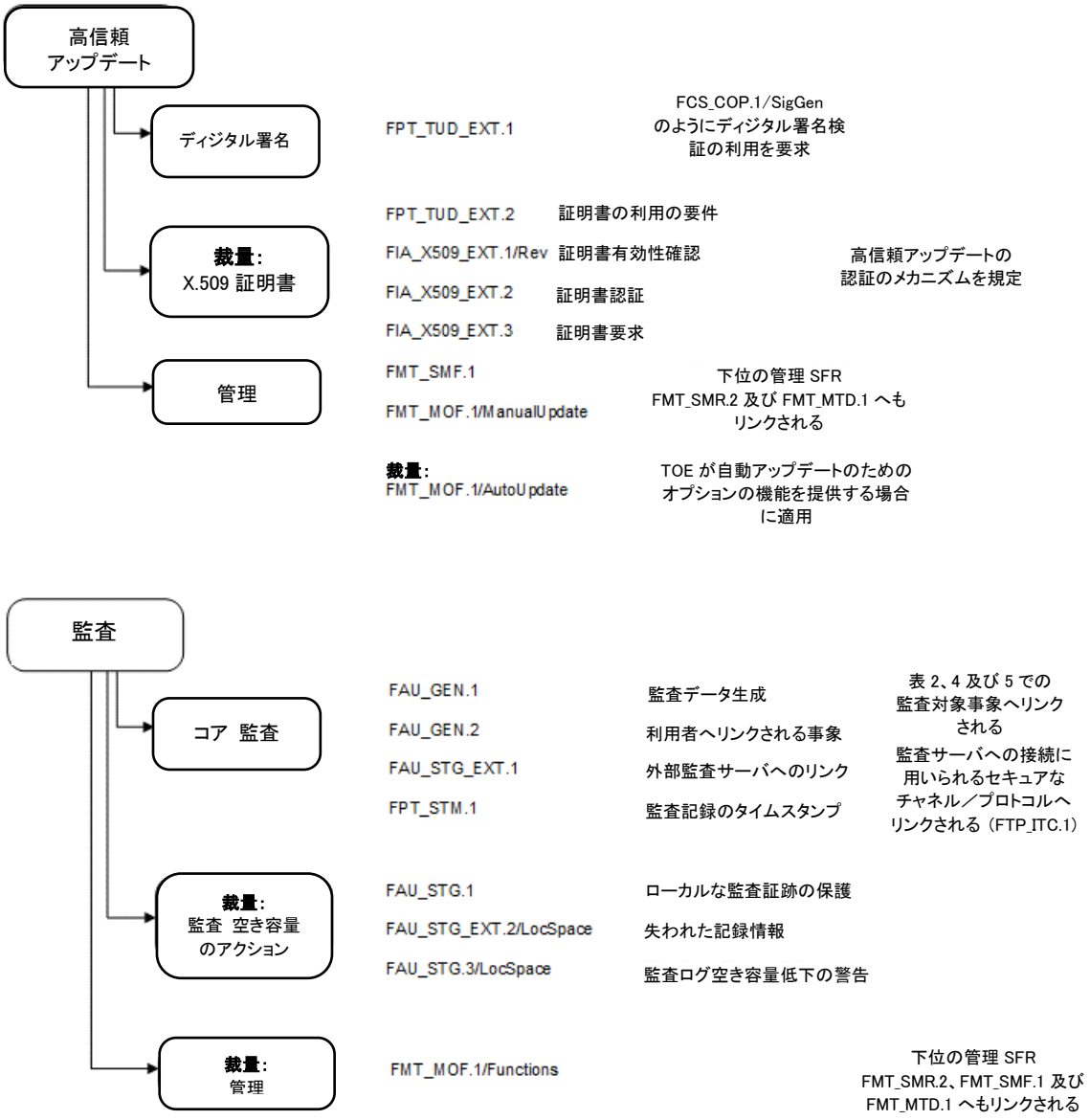


図 17：高信頼アップデートと監査の SFR アーキテクチャ

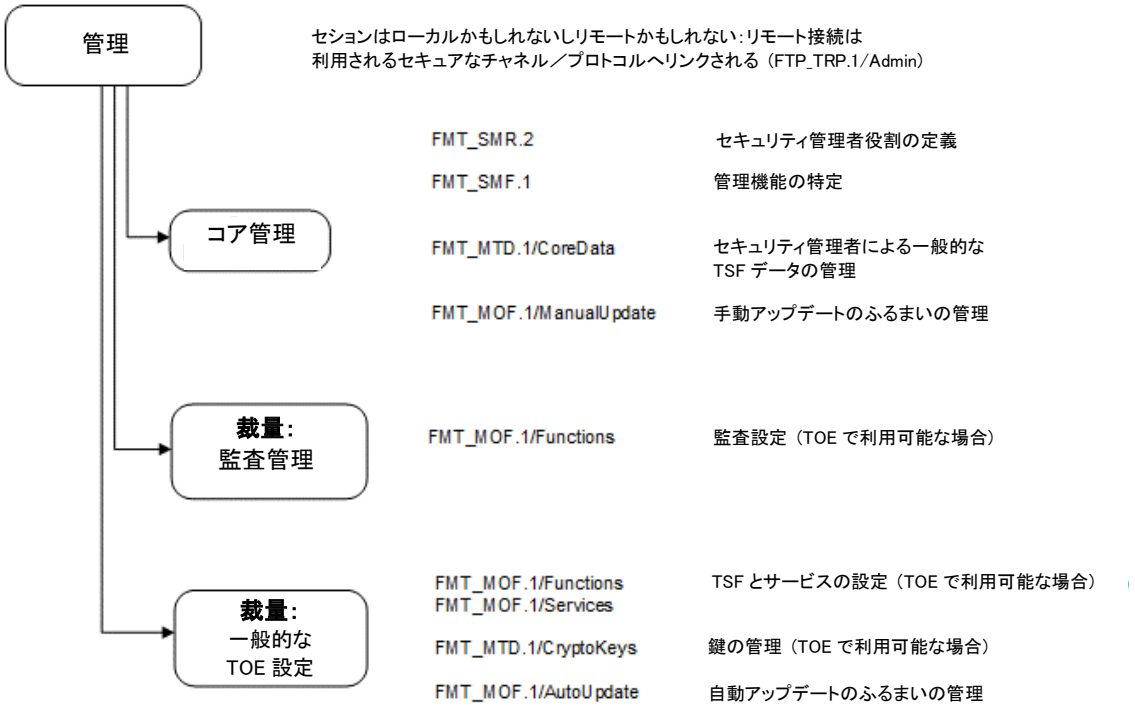


図 18：管理の SFR アーキテクチャ

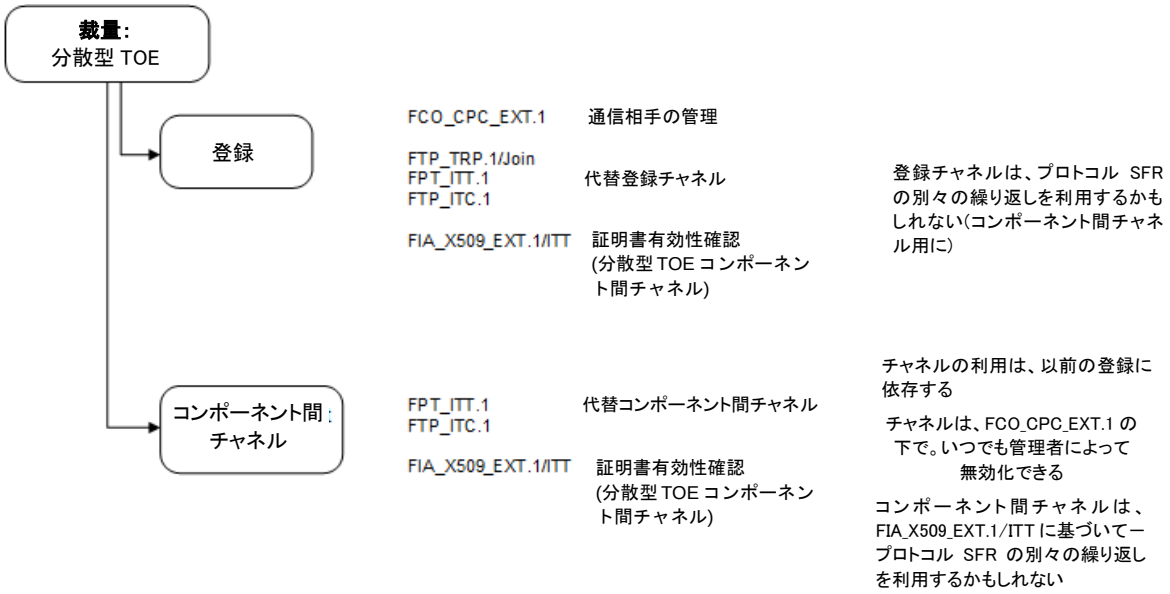


図 19：分散型 TOE の SFR アーキテクチャ

6.3 セキュリティ監査 (FAU)

6.3.1 セキュリティ監査データ生成 (FAU_GEN)

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

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

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

6.3.1.1 FAU_GEN.1 監査データ生成

FAU_GEN.1	監査データ生成

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない：

a) 監査機能の起動及び終了；

b) 監査のレベルが特定されないすべての監査対象事象；及び

c) 以下から構成されるすべての管理アクション：

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

d) 表 2 に列挙された具体的に定義された監査対象事象。

適用上の注釈 1

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

ST 作成者は、監査事象の表への相互参照を、ST への適切な相互参照で置き換えること。これには、ST に含まれるオプション SFR 及び選択ベース SFR に対応する表 4 及び表 5 の関連する部分についても含まれなければならない。

分散型 TOE について、それぞれのコンポーネントは、実装する SFR のそれぞれについての監査記録を生成しなければならない(must)。監査対象事象が発生するときに 1 つ以上の TOE コンポーネントが含まれる場合、その事象はそれぞれのコンポーネント(例、2 つのコンポーネント間のセキュアな通信チャネルを確立する試行が両方のコンポーネントによって生成されている監査対象事象にもたらすべきであるが) 1 つのコンポーネントによるコネクションの拒絶)において監査されなければならない(has to)。これは、エラーの場合に限定されないが、TOE コンポーネント間のセキュアな通信チャネルのビルドアップ／ティアダウンの成功のような成功アクションについての事象も含む。

適用上の注釈 2

ST 作成者は、他の監査対象事象を表に直接含めることができる；それらは、提示されたリストに限定されない。

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

FAU_GEN.1.1 に関して、「サービス」という用語は、高信頼パス及び高信頼チャネル通信、オンデマンドの自己テスト、高信頼アップデート及び管理者セション (高信頼パスの下に存在するもの)を指している。(例、 netconf) オプションの SFR FMT_MOF.1/Services が ST に含まれる場合、選択肢「サービスの開始及び停止」が FAU_GEN.1.1 の選択から選ばれる必要がある。

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

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

b) 各監査事象種別に対して、cPP／ST の機能コンポーネントの監査対象事象の定義に基づいた、*表 2 の 3 列目に指定される情報。*

適用上の注釈 3

ST 作成者は、監査事象の表への相互参照を、ST への適切な相互参照で置き換えること。これには、ST に含まれるオプション SFR 及び選択ベース SFR に対応する表 4 及び表 5 の関連する部分についても含まれなければならない。

要件	監査対象事象	追加の監査記録の内容
FAU_GEN.1	なし。	なし。
FAU_GEN.2	なし。	なし。
FAU_STG_EXT.1	なし。	なし。
FCS_CKM.1	なし。	なし。
FCS_CKM.2	なし。	なし。
FCS_CKM.4	なし。	なし。
FCS_COP.1/DataEncryption	なし。	なし。
FCS_COP.1/SigGen	なし。	なし。
FCS_COP.1/Hash	なし。	なし。
FCS_COP.1/KeyedHash	なし。	なし。
FCS_RBG_EXT.1	なし。	なし。
FIA_AFL.1	ログイン試行失敗の制限に達するまたは超える	試行の生成元 (例、IP アドレス)
FIA_PMG_EXT.1	なし。	なし。
FIA_UIA_EXT.1	識別と認証のメカニズムの利用のすべて。	試行の生成元 (例、IP アドレス)。
FIA_UAU_EXT.2	識別と認証のメカニズムの利用のすべて。	試行の生成元 (例、IP アドレス)。
FIA_UAU.7	なし。	なし。
FMT_MOF.1/ManualUpdate	手動アップデートを開始するような、あらゆる試行	なし。
FMT_MTD.1/CoreData	TSF データの管理アクティビティのすべて。	なし。
FMT_SMF.1	なし。	なし。
FMT_SMR.2	なし。	なし。
FPT_SKP_EXT.1	なし。	なし。
FPT_APW_EXT.1	なし。	なし。
FPT_TST_EXT.1	なし。	なし。
FPT_TUD_EXT.1	アップデートの開始；アップデート試行の結果 (成功または失敗)。	なし。

FPT_STM_EXT.1	時刻への非連続の変更 – 管理関与または自動化プロセスを介した変更。(連続しない自国への変更はログ記録される必要があることに留意されたい。FPT_STM_EXT.1 の適用上の注釈についても参照されたい)	自国への非連続の変更：時刻の新旧の値。成功及び失敗した時刻を変更する試行の生成元 (例、IP アドレス)。
FTA_SSL_EXT.1 (「セションをロックする」が選択される場合)	対話セションのロック解除時のあらゆる試行。	なし。
FTA_SSL_EXT.1 (「セションを終了する」が選択される場合)	セションロックメカニズムによるローカルセションの終了。	なし。
FTA_SSL.3	セションロックメカニズムによるリモートセションの終了。	なし。
FTA_SSL.4	対話セションの終了。	なし。
FTA_TAB.1	なし。	なし。
FTP_ITC.1	高信頼チャネルの開始。 高信頼チャネルの終了。 高信頼チャネル機能の失敗。	失敗した高信頼チャネル確立試行の開始者及びターゲットの識別情報。
FTP_TRP.1/Admin	高信頼パスの開始。 高信頼パスの終了。 高信頼パス機能の失敗。	なし。

表 2：セキュリティ機能要件及び監査対象事象

適用上の注釈 4

追加の監査事象が、附属書 A 及び附属書 B から採用されたオプション及び選択ベースの要件により、TOE へ適用される。ゆえに、ST 作成者は、表 4 及び表 5 の表において規定された関連する追加の事象を含めなければならない。

6.3.1.2 FAU_GEN.2 利用者識別情報の関連付け

FAU_GEN.2	利用者識別情報の関連付け

FAU_GEN.2.1 識別された利用者のアクションがもたらす監査事象に対し、TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

適用上の注釈 5

監査対象事象が別のコンポーネントによって発生した場合、その事象を記録するコンポーネントは、その事象を発生した起動コンポーネントの識別とそれを関連付けなければならない (分散型 TOE のみに適用)。

6.3.2 セキュリティ監査事象格納 (拡張—FAU_STG_EXT)

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

6.3.2.1 FAU_ STG_EXT.1 保護された監査事象格納

FAU_STG_EXT.1	保護された監査事象格納

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

適用上の注釈 6

生成された監査データを外部 IT エンティティへ送信するオプションの選択について、TOE は監査記録の格納とレビューに関して非 TOE 監査サーバに依存している。これらの監査記録の格納、及びこれらの監査記録のレビューを管理者に許可する能力は、その場合の運用環境により提供される。外部監査サーバは TOE の一部でないため、監査データの ITC 転送のための機能を除きそれに関して一切の要件がない。転送される監査データのフォーマットまたは基礎となるプロトコルについての要件が一切ない。TOE は、管理者の仲介なしに外部 IT エンティティへ監査データを転送するように構成される機能を持たなければならない (must)。手動での転送は、本要件を満たさない。送信がリアルタイムまたは定期的に行われることできる。送信がリアルタイムに行われない場合、TSS には、どの事象がなされるべき送信を刺激するか、どの範囲の頻度で TOE が監査データを監査サーバへ送信するようサポートするかについて記述される ; TSS には、送信の受け入れ可能な通常の頻度についても示すこと。

分散型 TOE については、それぞれのコンポーネントは、監査データを適切に保護された外部のチャネル (FTP_ITC.1) またはコンポーネント間 (FPT_ITT.1 または FTP_ITC.1) を通して送出できなければならない (must)。TOE の少なくとも 1 つのコンポーネントは、すべての TOE 監査記録が外部 IT エンティティへ抄出されることが可能となるように、FTP_ITC.1 経由で監査データを創出できなければならない (must)。

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

らない。

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

適用上の注釈 7

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

分散型 TOE について、それぞれのコンポーネントは、生成される監査データをローカルに格納することを要求されないが、TOE 全体としては監査データをローカルに格納できる必要がある。それぞれのコンポーネントは、ネットワーク接続性に問題がある場合に監査記録が維持されることを保証するため、少なくとも一時的に監査情報をローカルにバッファする能力を提供しなければならない(must)。監査情報をローカルにバッファすることには、不揮発性メモリを必ずしも含まない：監査情報は揮発性メモリにバッファされることも可能である。しかし、FAU_STG_EXT.1.3 という意味の監査情報のローカルストレージは、不揮発性メモリ内で行われる必要がある。監査情報のローカルストレージを実行するそれぞれのコンポーネントについて、ローカルストレージが枯渇するときのふるまいは記述される必要がある。監査情報を自分自身がローカルにバッファリングするそれぞれのコンポーネントについて、バッファ領域が枯渇する場合に何が起こるかについて記述される必要がある。

6.3.3 分散型 TOE のセキュリティ監査

分散型 TOE について、監査情報の取り扱いは、1 つのコンポーネントだけからなる TOE よりもさらに福猿であるかもしれない。基本的にいくつかの満たされるべき基本的な要件がある：

- すべてのコンポーネントは、監査情報を生成できなければならない(must)。
- すべてのコンポーネントは、監査情報をバッファして、別の TOE コンポーネントへ転送するか、または監査データをローカルに格納するかのいずれかができなければならない(must)。
- TOE 全体について、すべての監査情報をローカルに格納できなければならない(must)。
- TOE 全体について、監査情報を外部監査サーバへ送信できなければならない(must)。

一般にすべてのコンポーネントは、自身の監査情報を生成できなければならない(must)。すべてのコンポーネントが監査データを外部監査サーバへ送出できることと同様に、すべてのコンポーネントが自身の監査情報をローカルにも格納することは可能であろう。しかし、これのかわりに、すべてのコンポーネントが自身の監査データを生成し、ローカルストレージ及び／または外部監査サーバへの送信のために 1 つ以上のその他のコンポーネントに情報が送出される前にそれをローカルにバッファすることが可能であれば、それで十分であろう。TOE コンポーネント間の監査記録の転送について、FTP_ITC.1 または FPT_ITT.1 経由

のセキュアコネクションが使用されなければならない(must)。

このようなソリューションは、またすべての監査関連 SFR がすべての TOE コンポーネントによって満たされなければならない(have to) という要件を満たすために適しているが、正式には、必ずしもすべてのコンポーネントがローカルストレージをサポートするか、外部監査サーバ自身へ転送する訳ではない。

TOE 間通信の確立に関して、成功したコネクション／ティアダウン事象と同様にエラー条件は、コネクションの両方の端点によってキャプチャされるべきである(should)。

すべての TOE コンポーネントは、FAU_GEN.1 に従って実装されたすべての SFR について自身の監査データを生成できなければならない(shall)が、必ずしもすべての TOE コンポーネントがすべての事象について監査データを提供しなくてもよい。分散型 TOE について、マッピングは、FAU_GEN.1 に従ったどの監査対象事象がどのコンポーネントによってカバーされるか (各コンポーネントによって生成された記録が実装されたすべての SFR をカバーすることの正当化を与えることも) を示すよう提供されなければならない(shall)。TOE 全体は、FAU_GEN.1 で定義されたすべての事象についての監査情報を提供しなければならない(has to)。結果として、少なくとも 1 つの TOE コンポーネントは、FAU_GEN.1 で定義されたすべての監査対象事象に割り当てられなければならない(has to)。表 2 に関連するマッピングの一部は、特定の SFR についての監査情報生成として定義されたすべてのコンポーネントが ASE_TSS.1 のマッピングにおける SFR にも寄与するべきであるという理解における ASE_TSS.1 の TOE コンポーネントへの SFR のマッピングと一貫していなければならない(shall)。これは、必須の SFR で定義された監査対象事象だけでなく、附属書 A 及び附属書 B で定義されたオプション SFR 及び選択ベースの SFR についてのすべての監査対象事象にも適用される。

オプション監査コンポーネント FAU_STG.1、FAU_STG_EXT.2/LocSpace 及び FAU_STG.3/LocSpace の 1 つ以上が、本 cPP から導出されたセキュリティターゲットで選択される場合、ASE_TSS.1 へマッピングしている SFR は、適用される TOE コンポーネントの具体的な識別を含まなければならない(must)。

6.4 暗号サポート (FCS)

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

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

6.4.1 暗号鍵管理 (FCS_CKM)

6.4.1.1 FCS_CKM.1 暗号鍵生成 (詳細化)

FCS_CKM.1	**暗号鍵生成**

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

ルゴリズム： **[選択：**

- **2048 ビット以上の暗号鍵長を用い、以下を満たす RSA スキーム： FIPS PUB 186-4, "Digital Signature Standard (DSS)", 附属書 B.3；**
- **「NIST 曲線」 [選択：P-256、P-384、P-521] を用い、以下を満たす ECC スキーム： FIPS PUB 186-4, "Digital Signature Standard (DSS)", 附属書 B.4；**
- **2048 ビット以上の暗号鍵長を用い、以下を満たす FFC スキーム： FIPS PUB 186-4, "Digital Signature Standard (DSS)", 附属書 B.1**

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

適用上の注釈 8

ST 作成者は、鍵確立及びデバイス認証のために使用されるすべての鍵生成スキームを選択すること。鍵生成が鍵確立用に使用される場合、FCS_CKM.2.1 におけるスキーム及び選択された暗号プロトコルがその選択と一致しなければならない。鍵生成が ssh-rsa、ecdsa-sha2-nistp256、ecdsa-sha2-nistp384 及び ecdsa-sha2-nistp521 以外のデバイス認証用に使用される場合、公開鍵は X.509v3 証明書と関連付けられることが期待されている。

TOE が鍵確立スキームで受信側として動作する場合、及び相互認証をサポートするよう構成されない場合、TOE は、鍵生成を実装する必要はない。

分散型 TOE の場合、TOE コンポーネントが鍵確立スキームにおける受信側として動作する場合、TOE は鍵生成を実装する必要はない。

6.4.1.2 FCS_CKM.2 暗号鍵確立 (詳細化)

FCS_CKM.2	**暗号鍵確立**

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

- **RSA ベースの鍵確立スキームであって、以下を満たすもの： NIST Special Publication 800-56B Revision 1, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"；**
- **楕円曲線ベースの鍵確立スキームであって、以下を満たすもの：NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"；**
- **有限体ベースの鍵確立スキームであって、以下を満たすもの：NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";**
- **Diffie-Hellman グループ 14 を用いる鍵確立スキームであって、以下を満たすもの：RFC 3526, Section 3；**

] に従って、暗号**鍵確立**を**行わ**なければならない。

適用上の注釈 9

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

ST 作成者は、選択された暗号プロトコル用に使用されるすべての鍵確立スキームを選択すること。Diffie-Hellman グループ 14 について、ST 作成者は、有限体ベース（Finite field-based）鍵確立の選択肢を用いる代わりに SFR から対応する選択を行うべきである。

RSA ベースの鍵確立スキームは、NIST SP 800-56B Revision 1 のセクション 9 に記述されている；しかし、セクション 9 は SP 800-56B Revision 1 の他のセクションの実装に依存している。

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

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

6.4.1.3 FCS_CKM.4 暗号鍵破棄

FCS_CKM.4	暗号鍵破棄

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

- *揮発性ストレージにおける平文の鍵については、[選択：[選択：TSF の RBG を用いた疑似ランダムパタンからなる、ゼロ、1、その鍵の新しい値、[割付：任意の CSP を含まないような静的または動的な値]]からなる一回の上書き、ガーベージコレクションの要求が続くその鍵への直接的な参照の破棄] により実行されなければならない(shall)。*
- *不揮発性ストレージにおける平文の鍵については、破棄は、以下のような TSF の一部により提供されるインタフェースの起動によって、実行されなければならない [選択：*
  - *鍵のストレージ場所に論理的にアドレスを指定し、[選択：TSF の RBG を用いた疑似ランダムパタン、ゼロ、1、その鍵の新しい値、[割付：任意の CSP を含まないような静的または動的な値]]からなる[選択：一回。[割付：回数] 回] の上書きを実行する；*
  - *その鍵を表すような抽象化を破棄するための TSF の一部を命令する]]*

に従って、暗号鍵を破棄しなければならない。

適用上の注釈 10

「TSF の一部」によって破棄されるとして特定される鍵の選択肢の一部において、TSS は、関連部分と含まれるインタフェースを特定する。本要件で参照されるインタフェースは、OS カーネルへのアプリケーションプログラミングインタフェースのようなものである、異なる TOE のための異なる様式を取ることもできる。例えば所与の実装において、アプリケーションは、ファイルシステムの詳細にアクセスしてもよく、具体的なメモリロケーションに論理的にアドレスを指定できてもよい。別の実装において、アプリケーションは、単にリソースへのハンドルを持ってもよいし、リソースを削除するためのインタープリタまたは OS

のような TSF の別の一部に依頼のみをできてもよい。

異なる鍵の破棄方法が異なる鍵及び／または異なる破棄の状況に使用されるような場合、それらが適用される異なる方法及び鍵／状況は、TSS に記述される(また ST には、明確化を助けるため、SFR の繰り返しを別々に使用してもよい)。TSS には、SFR の実装に使用されたすべての関連する鍵が、鍵が非平文の形式で保存されているような場合を含めて、記述される。非平文のストレージの場合、暗号化方式及び関連する鍵暗号化鍵が TSS において特定される。

いくつかの選択肢は、「任意の CSP を含まないような値」の割付を許容している。これは、TOE がいくつかの具体的なデータで、FCS_RBG_EXT 要件を満たしている RBG から取り出されたものでないもの、かつその他の選択肢として列挙された任意の具体的な値でないものを使用することを意味している。「任意の CSP を含まないような値」という不レースの点は、上書きデータが注意深く選択され、それ自身が機密性保護を要求するような現在のまたは残存データを含むかもしれないような一般的なものの中から取りだされないことを保証することである。

誤解を避けるため：本 SFR での「暗号鍵」は、セション鍵を含む。鍵破棄は、非対称鍵ペアの公開鍵のコンポーネントには適用されない。

6.4.2 暗号操作 (FCS_COP)

6.4.2.1 FCS_COP.1 暗号操作

FCS_COP.1/DataEncryption	**暗号操作 (AES データ暗号化／復号)**

FCS_COP.1.1/DataEncryption TSF は、以下の標準に合致する、[*割付：[選択：CBC、CTR、GCM]* モードで使用される、規定された暗号アルゴリズム *AES* と暗号鍵長 *[割付：128 ビット、192 ビット、256 ビット]*に従って、***暗号化／復号***を実行しなければならない： [*割付：ISO 18033-3 で規定される AES*、 *[*選択：*ISO 10116 で規定される CBC、ISO10116 で規定される CTR、ISO 19772 で規定される GCM]*。

適用上の注釈 11

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

FCS_COP.1/SigGen	**暗号操作 (署名生成及び検証)**

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

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

]

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

- RSA スキームについて：PKCS #1 v2.1 Signature Schemes RSASSA-PSS 及び／または RSASSA-PKCS1v1_5 を用いる FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5；ISO/IEC 9796-2, Digital signature scheme 2 または Digital Signature scheme 3、
- ECDSA スキームについて：「NIST 曲線」[選択：P-256、P-384、P-521] を実装する FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 及び附属書 D；ISO/IEC 14888-3, Section 6.4

]。

適用上の注釈 12

ST 作成者は、ディジタル署名を行うために実装されたアルゴリズムを選択する。選択された 1 つまたは複数のアルゴリズムについて、ST 作成者はそのアルゴリズムに実装されるパラメタを規定するため、適切な割付／選択を行う。ST 作成者は、本 SFR の割付と選択が ST に含まれているプロトコル SFR (附属書 B.2.1 を参照)用に選択された暗号スイートに必要なパラメタ値のすべてを含むことを保証する。ST 作成者は、特に楕円曲線をサポートするとき、その他の FCS 要件との選択肢の一貫性をチェックする。

FCS_COP.1/Hash	**暗号操作 (ハッシュアルゴリズム)**

FCS_COP.1.1/Hash TSF は、以下の標準に合致する、規定された暗号アルゴリズム [選択：SHA-1、SHA 256、SHA 384、SHA 512] ~~と暗号鍵長 [割付：*暗号鍵長*]~~ 及びメッセージダイジェスト長[選択：160、256、384、512] ビットに従って**暗号ハッシュサービス**を実行しなければならない： [*割付：ISO/IEC 10118-3:2004*]。

適用上の注釈 13

ベンダには、SHA-2 ファミリをサポートする改訂されたプロトコルの実装が強く推奨される；改訂されたプロトコルがサポートされるまで、本 cPP は SP 800-131A に適合した SHA-1 の実装のサポートを許容する。本 cPP の将来のバージョンでは、SHA-256 がすべての TOE についての最小限の要件となるだろう。

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

FCS_COP.1/KeyedHash	**暗号操作 (鍵付きハッシュアルゴリズム)**

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

適用上の注釈 14

割付における鍵長 [k] は、L1 と L2 の間の範囲内にあること (適切なハッシュ関数について ISO/IEC 10118 で定義されている)。例えば、SHA-256 について、L1=512、L2=256、ここで L2<=k<=L1 とする。

6.4.3 乱数ビット生成 (拡張—FCS_RBG_EXT)

6.4.3.1 FCS_RBG_EXT.1 乱数ビット生成

FCS_RBG_EXT.1	**乱数ビット生成**

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

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

適用上の注釈 13

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

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

ここで用いられる AES 実装の鍵長が利用者データの暗号化に用いられるものと異なる場合には、FCS_COP.1 を調整するか、または異なる鍵長を反映して繰り返す必要があるかもしれない。FCS_RBG_EXT.1.2 の選択については、ST 作成者は RBG にシードを供給するために用いられるエントロピーの最小ビット数を選択する、これは TOE によって生成されるあらゆる鍵のセキュリティ強度と等しいか、またはそれ以上でなければならない(must)。

6.5 識別と認証 (FIA)

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

6.5.1 認証失敗管理 (FIA_AFL)

6.5.1.1 FIA_AFL.1 認証失敗管理 (詳細化)

FIA_AFL.1	**認証失敗管理**

FIA_AFL.1.1 TSF は、**リモート認証を試行する管理者**に関して、[*割付：許容可能な値の範囲*] **内における管理者設定可能な正の整数回の**不成功の認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数に達するとき、TSF は、[選択：*[割付：アクション]*がローカル管理者によって取られるまでリモート管理者に認証成功の提供の防止；管理者が定義した時間が経過するまでリモート管理者に認証成功の提供の防止 *]*をしなければならない。

適用上の注釈 16

本要件は、ローカルコンソールでの管理者には適用されない、なぜならこのやり方ではローカルの管理者アカウントをロックするのは道理にかなわないからである。これは、ローカル管理者には (例えば) 別のアカウントを要求するか、ローカルとリモートのログイン試行を区別する認証メカニズム実装を有することで対処可能である。ローカル管理者によって取られる「アクション」は、具体的な実装であり、管理者ガイダンスに定義されるだろう(例えば、ロックアウトのリセットまたはパスワードのリセット)。ST 作成者は TOE がこのハンドラをどのように実装するかに依存する認証失敗の取り扱いについての選択肢の中から 1 つを選択する。

TSS には、リモート管理者による認証失敗が、永久にまたは一時的にのいずれかの一切の管理者アクセスができないような状況を招くことができないこと (例、ブロッキングの対象でないようなローカルログオンを提供することによって) を TOE がどのように保証するかについて記述する。運用ガイダンスには、リモート管理が FIA_AFL.1 の結果としてアカウントのブロックのために永久にまたは一時的に使用可能でなくなったとしても、管理者アクセスが常に維持されることを保証するために要求される任意のアクションの、重要性について記述され、かつ特定される。

6.5.2 パスワード管理 (拡張—FIA_PMG_EXT)

6.5.2.1 FIA_PMG_EXT.1 パスワード管理

FIA_PMG_EXT.1	パスワード管理

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

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

b) 最小のパスワード長は、[*割付：TOE によってサポートされる最小文字数*]かつ[*割付：15 文字以上*]に設定可能でなければならない。

適用上の注釈 17

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

2 番目の割付は、セキュリティ管理者が設定可能な最大の最小パスワード長を用いて設定されるべきである(should)。

6.5.3 利用者の識別と認証 (拡張—FIA_UIA_EXT)

6.5.3.1 FIA_UIA_EXT.1 利用者の識別と認証

FIA_UIA_EXT.1	利用者の識別と認証

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

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

FIA_UIA_EXT.1.2 TSF は、その管理利用者を代行するその他のあらゆる TSF 仲介アクションを許可する前に、各管理利用者の識別と認証の成功を要求しなければならない。

適用上の注釈 18

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

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

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

FMT_SMR.2 の適用上の注釈に従って、分散型 TOE については、少なくとも 1 つの TOE コンポーネントは、FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってセキュリティ管理者の認証をサポートしなければならないが、必ずしもすべての TOE コンポーネントがサポートしなくてもよい。必ずしもすべての TOE コンポーネントがセキュリティ管理者の認証のこのやり方をサポートしない場合、TSS には、セキュリティ管理者がどのように認証され識別されるかについて記述しなければならない (shall)。

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

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

FIA_UAU_EXT.2	パスワードベースの認証メカニズム

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

適用上の注釈 19

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

FMT_SMR.2 のための適用上の注釈に従って、分散型 TOE については、少なくとも 1 つの TOE コンポーネントは、FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってセキュリティ管理者の認証をサポートしなければならないが、必ずしもすべての TOE コンポーネントがサポートしなくてもよい。必ずしもすべての TOE コンポーネントがセキュリティ管理者の認証のこのやり方をサポートしない場合、TSS には、セキュリティ管理者がどのように認証され識別されるかについて記述しなければならない(shall)。

6.5.4.2 FIA_UAU.7 保護された認証フィードバック

FIA_UAU.7	保護された認証フィードバック

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

適用上の注釈 20

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

6.6 セキュリティ管理 (FMT)

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

分散型 TOE について、TOE コンポーネントのセキュリティ管理は、すべての TOE コンポーネントについて直接に、またはその他の TOE コンポーネントを通して実現かのうである。TSS は、どの管理 SFR 及び管理機能がそれぞれの TOE コンポーネントに適用されるかについて記述しなければならない(shall) (分散型 TOE のみに適用)。

これらの主要な管理要件は、TOE 機能に従って、セクション A.4 のオプション要件及びセクション B.5 の選択ベース要件において補足されている。

6.6.1 TSF における機能の管理 (FMT_MOF)

6.6.1.1 FMT_MOF.1/ManualUpdate セキュリティ機能のふるまいの管理

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

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

適用上の注釈 21

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

6.6.2 TSF データの管理 (FMT_MTD)

6.6.2.1 FMT_MTD.1/CoreData TSF データの管理

FMT_MTD.1/CoreData	**TSF データの管理**

FMT_MTD.1.1/CoreData TSF は、**TSF データ**を**管理する**能力を、**セキュリティ管理者**に限定しなければならない。

適用上の注釈 22

「管理」という言葉には、作成、初期化、閲覧、デフォルト変更、改変、削除、消去、及び追加が含まれるが、これらには限定されない。本 SFR には、セキュリティ管理者による利用者パスワードのリセットも含まれる。識別子「CoreData」は、附属書 A.4.2.1(FMT_MTD.1/CryptoKeys)で定義された FMT_MTD.1 のオプションとなる繰り返しから FMT_MTD.1 の本繰り返しを区別するために、ここでは追加している。

6.6.3 管理機能の特定 (FMT_SMF)

6.6.3.1 FMT_SMF.1 管理機能の特定

FMT_SMF.1	**管理機能の特定**

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

[*割付：*

- *TOE をローカル及びリモートに管理する能力；*
- *アクセスバナーを設定する能力；*
- *セションの終了またはロックまでのセション非アクティブ時間を設定する能力；*
- *TOE をアップデートし、アップデートのインストールに先立って[選択：ディジタル署名、ハッシュ値の比較] 機能を用いてそのアップデートを検証する能力；*
- *FIA_AFL.1 の認証失敗パラメタを設定する能力；*

- *[選択：*
  - *監査のふるまいを設定する能力；*
  - *FIA_UIA_EXT.1 で規定されるように、エンティティが識別され認証される前に TOE が提供する利用可能なサービスのリストを設定する能力；*
  - *暗号機能を設定する能力；*
  - *SSH rekeying のしきい値を設定する能力；*
  - *IPsec SA のライフタイムを設定する能力；*
  - *適用可能な場合、TOE コンポーネント間の対話を設定する能力；*
  - *管理者アカウントを再度、有効化する能力；*
  - *タイムスタンプに利用される時刻をセットする能力；*
  - *ピアの参照識別子を設定する能力；*
  - *その他の機能なし。]*

適用上の注釈 23

TOE は、一般的にローカル及びリモート管理のための機能を提供しなければならない。しかし、本 cPP は、ローカル管理者インタフェース、リモート管理者インタフェースまたは両方のいずれかを通して利用可能であるような、特定のセキュリティ機能を義務付けていない。TSS は、どのインタフェースを通してどのセキュリティ管理機能が利用可能であるかについて詳述しなければならない。TOE は、FTA_TAB.1 のアクセスバナー及び FTA_SSL_EXT.1 及び FTA_SSL.3 のセション非アクティブ時間を設定する機能を提供しなければならない(must)。項目「TOE をアップデートし、アップデートのインストールに先立ってディジタル署名機能を用いてそのアップデートを検証する能力」には、FMT_MOF.1/ManualUpdate、FMT_MOF.1/AutoUpdate(ST に含まれる場合)、FIA_X509_EXT.2.2 及びFPT_TUD_EXT.1.2 及びFPT_TUD_EXT.2.2 (ST に含まれ、またこれらに管理者によって設定可能なアクションが含まれる場合) からの関連する管理機能が含まれる。同様に、選択肢「監査のふるまいを設定する能力」には、FMT_MOF.1/Services 及びFMT_MOF.1/Functions, (これらの SFR のうち ST に含まれるものすべてについて) からの関連する管理機能が含まれる。リモート管理者アカウントに FIA_AFL.1 に適合して無効化される能力を TOE が提供する場合 ST 作成者は、ローカル管理者によってそのアカウントを再度有効化することを許容するため、「管理者アカウントを再度有効化する能力」を選択するべきである(should)。TOE が管理者に監査のふるまいを設定、あるいは識別または認証に先立って利用可能なサービスを設定する能力を提供する場合、もしくは TOE 上の暗号化機能のいずれかが設定可能な場合、または ST には分散型 TOE について記述されている場合には、ST 作成者は 2 番目の選択内で適切な 1 つまたは複数の選択を行い、それ以外の場合には「その他の機能なし」を選択する (後者の場合、ST での選択は左側を代わりに空欄としてもよい)。

選択肢「SSH rekeying のしきい値を設定する能力」は、TOE が FCS_SSHC_EXT.1.8 または FCS_SSHS_EXT.1.8 を満たすために使用されるメカニズムについてのしきい値の設定をサポートする場合、ST に含まれなければならない(shall) (このような設定は、次に FMT_MOF.1/Functions を ST に含むことを要求する)。TOE がしきい値について受入れられる値についての制限を設定する場合、TSS に記述される。

選択肢「IPsec SA のライフタイムを設定する能力」は、TOE が ST において含まれる IPsec を介したセキュア通信と FCS_IPSEC_EXT.1 要件をサポートする場合、ST に含まれなければならない(shall)。IPsec SA のライフタイムの設定は、FCS_IPSEC_EXT.1.7 での選択と一致し

ている必要がある(このような設定は、次に ST へ FMT_MOF.1/Functions を含めることを要求する)。

選択肢「タイムスタンプに利用される時刻をセットする能力」は、TOE がタイムスタンプで利用されるデバイスの時刻の設定を管理者に許可する場合、含まれなければならない(shall)。このオプションは、TOE が手動時刻セッティングを許可しないが NTP サーバのような外部時刻ソースとの同期にのみ依拠する場合、選択されてはならない(shall not)。

選択肢「ピアの参照識別子を設定する能力」は、TOE が ST において IPsec プロトコル及び FCS_IPSEC_EXT.1 要件をサポートする場合、ST に含まれなければならない(shall)。IP アドレスと FQDN 識別子種別のみをサポートするような TOE について、参照識別子の設定は、接続の目的でピアの名称の設定と同じであってもよい。

分散型 TOE について、TOE コンポーネント間の繰り返しは、設定可能である(FCO_CPC_EXT.1 を参照)。ゆえに ST 作成者は、分散型 TOE について、選択肢「TOE コンポーネント間の対話を設定する能力」を含む。単純な例は、FPT_ITT.1 に従って通信プロトコルの変更である。別の例は、別の TOE コンポーネントを通してリモート管理からリモート管理へ直接の TOE コンポーネントの管理を変更することである。より複雑なユースケースは、SFR の実現が 2 つ以上のコンポーネントを通してアーカイブされる場合であり、2 つ以上のコンポーネント間の責任は、変更可能である。

登録チャネルを実装する分散型 TOE について(FCO_CPC_EXT.1.2 で記述される)、ST 作成者は、本 SFR において選択肢「暗号機能を設定する能力」、及び TSS ではその関係するマッピングを使用し、チャネルセキュリティを改善するために運用環境によって変更可能な登録チャネルの任意の暗号の観点からの設定について記述する(参照、[SD、3.6.1.2]の準備手続きの内容の記述)。

6.6.4 セキュリティ管理役割 (FMT_SMR)

6.6.4.1 FMT_SMR.2 セキュリティ役割における制限

FMT_SMR.2	**セキュリティ役割における制限**

FMT_SMR.2.1 TSF は、以下の役割を維持しなければならない：

- **セキュリティ管理者。**

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

FMT_SMR.2.3 TSF は、以下の条件

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

が満たされていることを保証しなければならない。

適用上の注釈 24

FMT_SMR.2.3 は、ローカルコンソール、及びリモートメカニズムを通して、セキュリティ管理者が TOE を管理できることを要求する。ST 作成者は、セキュアな通信がどのように達

成されるかを実証するため、FTP_ITC.1、FPT_ITT.1 及び／または FTP_TRP.1/Admin を選択しなければならない(must)。

分散型 TOE について、必ずしもすべての TOE コンポーネントが本 SFR を満たすそれ自身の利用者管理を実装することを要求される訳ではない。少なくとも 1 つのコンポーネントがFIA_UIA_EXT.1 及びFIA_UAU_EXT.2 に従ってセキュリティ管理者の認証と識別をサポートしなければならない(has to)。その他の TOE コンポーネントについて、セキュリティ管理者としての認証は、FIA_UIA_EXT.1 及びFIA_UAU_EXT.2 に従ったセキュリティ管理者の認証をサポートするようなコンポーネントからの高信頼チャネル(FTP_ITC.1 または FPT_ITT.1 のいずれかに従って)の使用を通して実現可能である。FIA_UIA_EXT.1.2 に従った利用者の識別と FMT_SMR.2.2 に従った利用者と役割の関連付けは、FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってセキュリティ管理者の認証をサポートするコンポーネントを通して行われる。高信頼チャネルの利用を通してセキュリティ管理者を認証する TOE コンポーネントは、FMT_SMR.2.3 で定義されるようなコンポーネントのローカル管理をサポートすることを要求されない。

6.7 TSF の保護 (FPT)

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

6.7.1 TSF データの保護 (拡張—FPT_SKP_EXT)

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

FPT_SKP_EXT.1	**TSF データの保護 (すべての事前共有鍵、対称鍵、及びプライベート鍵の読み出し)**

FPT_SKP_EXT.1.1 TSF は、すべての事前共有鍵、対称鍵、及びプライベート鍵の読み出しを防止しなければならない。

適用上の注釈 25

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

6.7.2 管理者パスワードの保護 (拡張—FPT_APW_EXT)

6.7.2.1 FPT_APW_EXT.1 管理者パスワードの保護

FPT_APW_EXT.1	管理者パスワードの保護

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

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

適用上の注釈 26

本要件の意図は、生のパスワード認証データが平文で保存されず、また利用者または管理者の誰も平文パスワードを「通常の」インタフェースを介して読み出すことができないことである。もちろん全能の管理者は、直接メモリを読み出してパスワードを取り出すことができるだろうが、そのようなことはしないと信頼されている。パスワードは、FIA_UAU.7 に従ってローカルコンソール上で入力中に見えなくされるべきである(should)。

6.7.3 TSF テスト (拡張—FPT_TST_EXT)

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

(本コンポーネントについては、選択ベース要件が附属書 B に存在する)

6.7.3.1 FPT_TST_EXT.1 TSF テスト (拡張)

FPT_TST_EXT.1	TSF テスト

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

適用上の注釈 27

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

非分散型 TOE は、内部的には、SFR 実施に寄与するようないくつかのコンポーネントから

構成されてもよい。自己テストは、SFR 実施に寄与するすべてのコンポーネントをカバーしなければならない(shall)、かつ完全性検証は、すべてのコンポーネント上の SFR 実施に寄与するすべてのソフトウェアをカバーしなければならない(shall)。

分散型 TOE について、すべての TOE コンポーネントは自己テストを実行しなければならない(have to)。これは、常にそれぞれの TOE コンポーネントが同じ自己テスト実行しなければならないことを意味している訳ではない ; ST には、それぞれの TOE コンポーネントへの選択肢の適用可能性 (即ち、いつ自己テストが実行されるか)と最終的な割付 (即ち、どの自己テストが実行されるか) について記述される。

適用上の注釈 28

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

6.7.4 高信頼アップデート (FPT_TUD_EXT)

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

(本ファミリについて、選択ベース要件として附属書 B に存在する)

6.7.4.1 FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1	高信頼アップデート

FPT_TUD_EXT.1.1 TSF は、セキュリティ管理者に TOE ファームウェア／ソフトウェアの現在実行中のバージョン及び[選択：TOE ファームウェア／ソフトウェアの一番最近にインストールされたバージョン、その他の TOE ファームウェア／ソフトウェアバージョンなし]を問い合わせる能力を提供しなければならない。

適用上の注釈 29

高信頼アップデートが後で活性化する機能を用いて TOE にインストール可能である場合、現在実行中のイメージ、及びインストールされたが非アクティブなイメージの両方のバージョンが提供されなければならない(must)。この場合、選択肢「TOE ファームウェア／ソフトウェアの一番最近にインストールされたバージョン」が FPT_TUD_EXT.1.1 の選択から選ばれる必要があり、TSS には非アクティブなバージョンがアクティブになる方法と時期について記述する必要がある。すべての高信頼アップデートがインストールプロセスの一部としてアクティブになる場合、現在実行中のバージョンのみが提供される必要がある。この場合、選択肢「その他の TOE ファームウェア／ソフトウェアバージョンなし」が FPT_TUD_EXT.1.1 の選択で選ばれなければならない(shall)。

分散型 TOE について、TOE のそれぞれのコンポーネント上にインストールされたバージョンを決定する方法は、運用ガイダンスに記述される。

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

適用上の注釈 30

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

TSS は、「アップデートの自動的なチェックをサポートする」または「自動アップデートをサポートする」選択肢を使用するとき、どのアクションが TOE サポートに含まれるかについて説明する。

公開ハッシュ値 (FPT_TUD_EXT.1.3 を参照)が高信頼アップえーとメカニズムを保護するために使用されるとき、TOE は、ハッシュ値と共に(アップデートファイルに含まれるか、別々かのいずれかで)アップデートファイルを自動的にダウンロードしてはならない(must not)、かつ、例え計算されたハッシュ値が公開ハッシュ値と一致したとしても、セキュリティ管理者によるアクティブな認証なしに自動的インストールしてはならない。高信頼アップデートメカニズムを保護するために公開ハッシュ値を使用するとき、オプション「自動アップデートのサポート」は、使用されてはならない(must not)(自動化されたアップデートのチェックは許容されるが)。TOE は、自動的にアップデートファイル自体をダウンロードしてもよいが、ハッシュ値はいけない。公開ハッシュアプローチについて、セキュリティ管理者は、以下の通り、常にアップデートのインストールについてのアクティブな許可を与えることが要求されることが意図されている(FPT_TUD_EXT.1.3 の下で、より詳細について記述される通り)。これゆえに、アップデートメカニズムの種別は、例え、アップデートファイルが自動的にダウンロードされても「手動による起動アップデート」と見なされる。完全に自動化されたアプローチ(セキュリティ管理者の介在なしに)は、「ディジタル署名メカニズム」が以下の FPT_TUD_EXT.1.3 で選択されているときにのみ利用可能である。

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

適用上の注釈 31

FPT_TUD_EXT.1.3 での選択において参照されるディジタル署名メカニズムは、FCS_COP.1/SigGen で規定されるアルゴリズムの 1 つである。FPT_TUD_EXT.1.3 において参照される公開ハッシュ値は、FCS_COP.1/Hash で規定される機能の 1 つによって生成される。ST 作成者は、TOE によって実装されるメカニズムを選択すべきである；両方のメカニズム

を実装することは受け入れ可能である。

公開ハッシュ値が高信頼アップデートメカニズムをセキュアにするために使用されるとき、セキュリティ管理者によるアップデートプロセスのアクティブな許可が常に要求される。開発者からセキュリティ管理者への真正なハッシュ値のセキュアな送信は、公開ハッシュが使用されるとき高信頼アップデートメカニズムを保護するための鍵となる要素の一つであり、ガイダンス文書には、この転送がどのように実行されなければならないかについて記述する必要がある。セキュリティ管理者による高信頼ハッシュ値の検証について、異なるユースケースも可能である。セキュリティ管理者は、アップデートファイルと同様に公開ハッシュ値を取得でき、アップデートファイルのハッシュが TOE またはその他の手段によって行われる間に、TOE の外部で検証を実行できる。セキュリティ管理者としての認証と高信頼アップデートの開始は、この場合、高信頼アップデートの「アクティブな許可」と見なされる。代わりに、管理者は、TOE にアップデートファイルとともに公開ハッシュ値を提供できる、そしてハッシュとハッシュ比較は TOE によって実行される。ハッシュ検証が成功する場合、TOE は、セキュリティ管理者による追加のステップなしでアップデートを実行できる。セキュリティ管理者としての認証と TOE へのハッシュ値の送信は、高信頼アップデートの「アクティブな許可」と見なされる、なぜなら管理者は、アップデートを実行しようとするとき、TOE にのみハッシュ値をロードすると期待されるからである。TOE へのハッシュ値の転送がセキュリティ管理者によって実行される限り、アップデートファイルのロードは、セキュリティ管理者によって実行できる、またはリポジトリから TOE によって自動的にダウンロードが可能である。

ディジタル署名メカニズムが選択される場合、署名の検証は TOE 自身によって実行されなければならない(shall)。公開ハッシュオプションについて、検証は、セキュリティ管理者による場合と同様に TOE 自身によって行われることが可能である。後者の場合、検証についての TOE 機能の利用は、必須ではないので、検証は、TOE を含むデバイスの非 TOE 機能を用いて、または TOE を含むデバイスを使用せずに、行われることか可能である。

分散型 TOE について、すべての TOE コンポーネントが高信頼アップデートをサポートしなければならない(shall)。アップデート上の署名またはハッシュの検証は、それぞれの TOE コンポーネント自身によって行われるか (署名検証)、またはそれぞれのコンポーネントについて(ハッシュ検証)行われなければならない(shall)。

分散型 TOE のアップデートは、異なる TOE コンポーネントが異なるソフトウェアバージョンを実行するような状況へ導くに違いない。異なるソフトウェアバージョン間の際によって、異なるソフトウェアバージョンの混合の影響は、全く問題にならないか、または TOE の適切な機能に対してクリティカルであるかもしれない。TSS は、分散型 TOE の高信頼アップデート中に TOE の継続的な適切な機能をサポートするようなメカニズムを詳細に記述しなければならない(shall)。

適用上の注釈 32

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

適用上の注釈 33

アップデート検証メカニズムによって証明書が用いられる場合、証明書は FIA_X509_EXT.1 に従って有効性確認され、また FIA_X509_EXT.2.1 で選択されるべきである。さらに、

FPT_TUD_EXT.2 が ST に含まれなければならない。

適用上の注釈 34

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

保護される必要のある、TSF のすべての個別のソフトウェアコンポーネント (例えば、アプリケーション、ドライバ、カーネル、ファームウェア)、即ち、それらは、対応する製造業者によってディジタル署名され、その後アップデートを行うメカニズムによって検証されるべきである。コンポーネントは異なる製造業者によって署名されるべき(should) であるか、またはハッシュがアップデート前に検証される必要があるアップデートについて発行されるべき(should)かのいずれかである。

6.7.5 タイムスタンプ (拡張－FPT_STM_EXT)

6.7.5.1 FPT_STM_EXT.1 高信頼タイムスタンプ

FPT_STM_EXT.1	**高信頼タイムスタンプ**

FPT_STM_EXT.1.1 TSF は、それ自身の利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。

FPT_STM_EXT.1.2 TSF は、[選択 : 時刻のセットをセキュリティ管理者に許可、外部時刻ソースと時刻を同期] しなければならない。

適用上の注釈 35

信頼できるタイムスタンプは、その他の TSF と共に使用されることが期待される、例、セキュリティ管理者が、事象の順序をチェックすることによりインシデントを調査し、いつ監査対象事象が発生したかの実際のローカル時刻を決定することを可能にするため、監査データの生成用として。その情報の要求されるレベルの正確さについての決定は管理者に依存する。TOE は、セキュリティ管理者によって手動で提供されるか、または NTP サーバのような外部時刻ソースを 1 つまたは複数利用することによって提供されるかのいずれかであるような、外部の時刻及び日付情報に依存する。対応する選択肢が FPT_STM_EXT.1.2 の選択から選ばれなければならない(shall)。ローカルリアルタイムクロックの利用と外部時刻ソース(例、NTP サーバ)との自動同期は、推奨されるが必須ではない。NTP サーバのような外部時刻ソースとの通信について、FTP_ITC.1 の利用はオプションであるが必須ではないことに留意されたい。ST 作成者は、TSS に外部の時刻と日付の情報が TOE によって受信される方法及びこの情報が維持される方法について記述すること。

「高信頼タイムスタンプ」という用語は、外部的に提供される時刻及び日付情報の厳密な使用、及び変更前と変更後の時刻に関する情報を含めた時刻設定へのすべての変更のログ出

力を指す。この情報を用いて、すべての監査データの実際の時刻を決定することが可能である。自動化プロセスを介した関与または変更のすべての不連続時刻変更は、監査されなければならない(must)ことに留意されたい。デイタイム(3)のような － 時刻に不連続が一切示されないような、時刻がカーネルまたはシステム設備を介して変更されるとき、一切の監査は必要とされない。

分散型 TOE について、セキュリティ管理者は異なる TOE コンポーネントの時刻設定間の同期を保証することが期待される。すべての TOE コンポーネントは、同期されているか (例、TOE コンポーネント間の同期を通して、または異なる TOE コンポーネントの外部 NTP サーバを用いた同期を通して)、またはオフセットが TOE コンポーネントのすべてのペアについて管理者に既知であるべき(should) であるか、のいずれかでなければならない(shall)。これは、異なるタイムゾーンに同期された TOE コンポーネントを含む。

6.8 TOE アクセス (FTA)

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

6.8.1 TSF 起動セションロック (拡張—FTA_SSL_EXT)

6.8.1.1 FTA_SSL_EXT.1 TSF 起動セションロック

FTA_SSL_EXT.1	TSF 起動セションロック

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

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

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

6.8.2 セションロックと終了 (FTA_SSL)

6.8.2.1 FTA_SSL.3 TSF 起動による終了(詳細化)

FTA_SSL.3	TSF 起動による終了

FTA_SSL.3.1 : TSF は、**セキュリティ管理者によって設定可能なセション非アクティブ時間間隔**後に、**リモート**対話セションを終了しなければならない。

6.8.2.2 FTA_SSL.4 利用者起動による終了(詳細化)

FTA_SSL.4	利用者起動による終了

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

6.8.3 TOE アクセスバナー (FTA_TAB)

6.8.3.1 FTA_TAB.1 デフォルト TOE アクセスバナー(詳細化)

FTA_TAB.1	デフォルト TOE アクセスバナー

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

適用上の注釈 36

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

6.9 高信頼パス／チャネル (FTP)

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

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

6.9.1 高信頼チャネル (FTP_ITC)

6.9.1.1 FTP_ITC.1 TSF 間高信頼チャネル (詳細化)

FTP_ITC.1	TSF 間高信頼チャネル

FTP_ITC.1.1 TSF は **[選択：IPsec、SSH、TLS、DTLS、HTTPS] を用いて、**他の通信チャネルと論理的に区別され、その端点の保証された識別、及びチャネルデータの暴露からの保

護及びチャネルデータの改変の検知を提供する、それ自身と**以下の機能をサポートする許可された IT エンティティ：監査サーバ、 [選択：認証サーバ、*割付：[その他の機能]*、その他の機能なし]** との間の高信頼通信チャネルを**提供でき**なければならない。

FTP_ITC.1.2 TSF は、**TSF、または許可された IT エンティティ**が、高信頼チャネルを介して通信を開始することを許可しなければならない。

FTP_ITC.1.3 TSF は、 [*割付：**TSF が通信を開始できるサービス**のリスト*] のために、高信頼チャネルを介して通信を開始しなければならない。

適用上の注釈 37

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

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

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

公開鍵証明書が FTP_ITC チャネルのサポートで使用される場合、FIA_X509_EXT.1/Rev が使用されるべきである(これは、証明書失効をチェックすることを要求する)、そして分散型 TOE のコンポーネント間チャネルでの使用のみである繰り返し FIA_X509_EXT.1/ITT は使用されない。

6.9.2 高信頼パス (FTP_TRP)

6.9.2.1 FTP_TRP.1/Admin 高信頼パス (詳細化)

FTP_TRP.1/Admin	**高信頼パス**

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

FTP_TRP.1.2/Admin TSF は、**リモート管理者**が高信頼パスを介して通信を開始することを

許可しなければならない。

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

適用上の注釈 38

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

7. セキュリティ保証要件

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

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

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

TOE のセキュリティ保証要件は、表 3 に識別される。

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

表 3：セキュリティ保証要件

7.1 ASE：セキュリティターゲット

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

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

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

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

7.2 ADV：開発

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

7.2.1 基本機能仕様 (ADV_FSP.1)

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

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

7.3 AGD：ガイダンス文書

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

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

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

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

7.3.1 利用者操作ガイダンス (AGD_OPE.1)

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

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

7.3.2 準備手続き (AGD_PRE.1)

操作ガイダンスと同様に、開発者は、準備手続きに関して必要とされる内容を決定するために評価アクティビティを確認するべきである。

準備手続きの具体的な要件は、FCO_CPC_EXT.1とFTP_TRP.1/Joinについての評価アクティビティの一部として、分散型TOEについて[SD]で定義されることに留意する。

7.4 ALC クラス：ライフサイクルサポート

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

7.4.1 TOE のラベル付け (ALC_CMC.1)

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

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

7.4.2 TOE CM 範囲 (ALC_CMS.1)

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

7.5 ATE クラス：テスト

テストは、システムの機能的な側面、及び設計または実装の弱点を利用するような側面について特定される。前者は、ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 cPP では、テストは公表された機能及びインタフェースに基づ

き、設計情報の利用可能性に依存して行われる。評価プロセスの主要なアウトプットの一つは、以下の要件で特定されるテスト報告書である。

7.5.1 独立テスト—適合 (ATE_IND.1)

テストは、TSS とガイダンス文書 (「評価される構成」の指示を含む) に記述された機能を確認するために実施される。テストで重視されるのは、セクション 5.1.7 で規定された要件が満たされていることを確認することである。SD における評価アクティビティは、SFR への適合を検証するために必要な具体的なテストアクティビティを識別している。評価者は、本 cPP への適合を主張するプラットフォーム／TOE の組み合わせにフォーカスしたカバレージ論拠とともに、テストの計画及び結果を文書化したテスト報告書を作成する。

7.6 AVA クラス：脆弱性評定

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

7.6.1 脆弱性調査 (AVA_VAN.1)

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

A. オプションの要件

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

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

TOE がオプション要件のいずれかを満たす場合、ベンダは関連する機能を ST へ追加することが推奨される。ゆえにこの章の適用上の注釈において「本オプションは、 . . . 選択されるべきである」という言い回しが繰り返し利用される。しかし、このオプションは TOE が関連する機能を提供する場合にのみ選択されるべきであること、及び本 cPP に適合するための関連機能を実装することは必要ではないことを強調するためにも利用される。ST 作成者が、何も選択しない、本章で定義されるいくつかまたはすべての SFR を選択するのは自由である。ある製品が特定の機能をサポートするという事実は、本章で定義される任意の SFR を追加することを必須とはしない。

A.1 オプション SFR 用の監査事象

要件	監査対象事象	追加監査記録の内容
FAU_STG.1	なし。	なし。
FAU_STG_EXT.2/LocSpace	なし。	なし。
FAU_STG.3/LocSpace	監査事象の格納領域低下。	なし。
FIA_X509_EXT.1/ITT	証明書検証の不成功な試行	失敗の理由
FMT_MOF.1/Services	サービスの開始と終了	なし
FMT_MTD.1/CryptoKeys	暗号鍵の管理	なし
FMT_ITT.1	高信頼チャネルの開始。 高信頼チャネルの終了。 高信頼チャネル機能の失敗	開始者及び失敗した高信頼チャネル確立試行の対象の特定。
FTP_TRP.1/Join	高信頼パスの開始。	なし。

	高信頼パスの終了。 高信頼パス機能の失敗。	
FCO_CPC_EXT.1	コンポーネントのペア間の通信の有効化。 コンポーネントペア間の通信の無効化。	有効化または無効化されたエンドポイントペアの特定。

表 4：TOE オプション SFR 及び監査対象事象

適用上の注釈 39

FIA_X509_EXT.1/ITT の監査事象は、以下を保証することによって証明書検証を完了できないような TOE に基づいている：

- *basicConstraints 拡張の存在及びその拡張において CA フラグがすべての CA 証明書について TRUE にセットされている。*
- *信頼される階層構造の CA のディジタル署名の検証*
- *CRL を読み出し／アクセスまたは OCSP サーバへアクセスする(ST における選択に従って)。*

これらのチェックのいずれかが失敗する場合、失敗の監査事象が監査ログに書き込まれるべきである(should)。

A.2 セキュリティ監査 (FAU)

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

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

A.2.1.1 FAU_STG.1 保護された監査証跡格納

FAU_STG.1	保護された監査証跡格納

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を防止できなければならない。

A.2.1.2 FAU_STG_EXT.2/LocSpace 消失した監査データの集計

FAU_STG_EXT.2	消失した監査データの集計

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

適用上の注釈 40

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

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

分散型 TOE について、監査データ喪失のカウントを実装するそれぞれのコンポーネントは管理者がこの情報にアクセスするメカニズム、及びこの情報の管理を提供しなければならない(has to)。

FAU_STG_EXT.2/LocSpace が ST に追加される場合、ST は喪失した監査データがカウントされないようなあらゆる状態について明確化しなければならない(has to)。

A.2.1.3 FAU_STG.3/LocSpace 監査データ喪失の可能性がある場合のアクション

FAU_STG.3/LocSpace	監査データ喪失の可能性がある場合のアクション

FAU_STG.3.1/LocSpace TSF は、監査証跡がローカルの監査証跡格納容量を超える場合、利用者へ通知するために警告を生成しなければならない。

適用上の注釈 41

このオプションは、監査データのローカルの格納領域が使い尽くされる前に TOE が利用者へ通知するために警告を生成して場合に選択されるべきである(should)。これは、監査対象事象がローカルの格納領域のみに格納される場合に役立つに違いない。

FAU_STG.3.1/LocSpace によって要求される警告メッセージが利用者に伝達可能であることが保証されなければならない(has to)。伝達は、監査ログ自体を経由してなされるべきである(should)、なぜなら管理者セションが事象発生時にアクティブであることが保証されないからである。

警告は、監査データを格納するためのローカルの領域が使い尽くされるとき及び／または TOE が不十分なローカル領域のための監査データを喪失するときに利用者に通知するべきである(should)。

監査データのローカルの格納領域が使い尽くされるとき警告の表示を実装するような分散型 TOE について、どの TOE コンポーネントがこの機能をサポートするかについて記述しなければならない(has to)。その機能をサポートするそれぞれのコンポーネントは、それ自体でまたは別のコンポーネントを通してのいずれかで、警告を生成しなければならない(shall)。

FAU_STG.3/LocSpace が ST に追加される場合、ST には、監査記録が「目に見えないように消失した」かもしれないようなあらゆる状況について明確化しなければならない(has to)。

A.3 識別と認証 (FIA)

A.3.1 X.509 証明書を用いた認証 (拡張－FIA_X509_EXT)

A.3.1.1 FIA_X509_EXT.1 証明書有効性確認

FIA_X509_EXT.1/ITT	X.509 証明書有効性確認

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

- RFC 5280 証明書有効性確認及び証明書パス検証。
- 証明書パスは、信頼された CA 証明書で終端しなければならない。
- TSF は、すべての CA 証明書について、basicConstraints 拡張の存在と CA フラグが TRUE にセットされていることを保証することによって、証明書パスを検証しなければならない。
- TSF は、[選択:*RFC6960 で規定されるオンライン証明書状態プロトコル (OCSP)*、

RFC5280 セクション6.3 で規定される証明書失効リスト(CRL)、RFC 5759 セクション5 で規定される証明書失効リスト (CRL)、失効方法なし] を用いて証明書の失効状態を検証しなければならない。

- TSF は、以下の規則に従って、extendedKeyUsage フィールドを検証しなければならない：
  - TLS 用に提示されるサーバ証明書は、extendedKeyUsage フィールドにサーバ認証目的 (OID 1.3.6.1.5.5.7.3.1 を持つ id-kp 1) を持たなければならない。
  - TLS 用に提示されるクライアント証明書は、extendedKeyUsage フィールドにクライアント認証目的 (OID 1.3.6.1.5.5.7.3.2 を持つ id-kp 2)を持たなければならない。
  - OCSP 応答用に提示される OCSP 証明書は、extendedKeyUsage フィールドに OCSP 署名目的 (OID 1.3.6.1.5.5.7.3.9 を持つ id-kp 9) を持たなければならない、なし。

適用上の注釈 42

本 SFR は、TOE が分散型であり、かつ FPT_ITT.1 で選択されるプロトコルピア認証用の X.509 証明書を活用する場合に選択されるべきである。この場合、FCO_CPC_EXT.1 で定義されるような ITT チャネルの有効化と無効化に関連する追加の要件があるので、失効リストチェックの利用は、オプションである。もし失効チェックがサポートされない場合、ST 作成者は、失効方法なしを選択するべきである。しかし、証明書失効チェックがサポートされる場合、ST 作成者は、これが OCSP を用いて実行されるかまたは CRL を用いるかを選択する。

TOE は、2 つの証明書の最小のパス長をサポートできなければならない。即ち、少なくとも自己署名されたルート証明書及び TOE 自身の証明書からなる証明書階層をサポートしなければならない。

TSS には、失効チェックがいつ実行されるかについて記述されなければならない(shall)。証明書が認証ステップで利用されるとき失効チェックが実行されることが期待される。ドライブ上に X.509 証明書がロードされるときのみに X.509 証明書の状態を検証することでは不十分である。

TOE が FIA_X509_EXT.1.1 の extendedKeyUsage 規則で列挙された証明書種別のいずれかを利用するような機能をサポートしない場合、これが TSS に記述され、SFR の関連する部分が自明に満たされると見なされる。しかし、TOE がこれらの種別いずれかの証明書を利用するような機能をサポートする場合、対応する規則は SFR において、もちろん満たされなければならない。

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

適用上の注釈 43

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

A.4 セキュリティ管理 (FMT)

A.4.1 TSF における機能の管理 (FMT_MOF)

A.4.1.1 FMT_MOF.1/Services セキュリティ機能のふるまいの管理

FMT_MOF.1/Services	セキュリティ機能のふるまいの管理

FMT_MOF.1.1/Services TSF は、機能サービスを有効化及び無効化する能力を、セキュリティ管理者に制限しなければならない。

適用上の注釈 44

FMT_MOF.1Services は、セキュリティ管理者がサービスを開始及び停止する能力を持つ場合のみに選択されるべきである(should)。この場合、選択肢「サービスを開始及び停止」が FAU_GEN.1.1 での選択において選ばれなければならない(shall)。用語「サービス」は、FAU_GEN.1.1 のために定義される (FAU_GEN.1.1 の関連する適用上の注釈を参照)。

A.4.2 TSF データの管理 (FMT_MTD)

A.4.2.1 FMT_MTD.1/CryptoKeys TSF データの管理

FMT_MTD.1/CryptoKeys	TSF データの管理

FMT_MTD.1.1/CryptoKeys TSF は、*暗号鍵を管理する*能力を、*セキュリティ管理者*に制限しなければならない。

適用上の注釈 45

FMT_MTD.1.1/CryptoKeys は、暗号鍵の管理をセキュリティ管理者に制限する。セキュリティ管理者によって暗号鍵が管理される (例、変更、削除、または生成／インポート)ことが可能である場合にのみ、選択されるべきである。識別子「CryptoKeys」は、FMT_MTD.1 のこの繰り返しを第 6.6.2.1 節 (FMT_MTD.1/CoreData)で定義された FMT_MTD.1 の必須の繰り返しから分離するためにここに追加された。

A.5 TSF の保護 (FPT)

A.5.1 TOE 内 TSF データ転送(FPT_ITT)

A.5.1.1 FPT_ITT.1 基本 TSF 内データ転送保護 (詳細化)

FPT_FITT.1	基本 TSF 内データ転送保護

FPT_ITT.1.1 TSF は、TSF データが TOE の異なるパーツ間で送られる場合、TSF データを **[選択 : IPsec、SSH、DTLS、TLS、HTTPS]** の利用を通して暴露から保護し*かつその改変を検知し*なければならない。

適用上の注釈 46

本要件は、分散型 TOE にのみ適用され、分散型 TOE のコンポーネント間のすべての通信が暗号化された通信チャネルの利用を通して保護されることを保証する。この高信頼通信チャネルにおいて通過するデータは、選択において選択されたプロトコルにより定義される通り暗号化される。ST 作成者は、分散型 TOE における通信を行うコンポーネントのそれぞれのペアによって使用されるチャネル及びプロトコルを、本 SFR を適切に繰り返しつつ、特定するべきである(should)。

このチャネルは、セクション 3.3 及び FCO_CPC_EXT.1.2 で記述されたとおり、登録プロセスについての登録チャネルとしても使用されてもよい。

TLS が使用される場合、利用者によって確率される参照識別子を持つ要件(FCS_TLSC_EXT.1.2)は、軽減され、識別子は、「ゲートキーパー」探索プロセスを通して確立されてもよい。TSS には、探索プロセス及び参照識別子が「参入しようとする」コンポーネントに提供される方法についてのハイライトについて記述されるべきである(should)。

A.6 高信頼パス／チャネル (FTP)

A.6.1 高信頼パス (FTP_TRP)

A.6.1.1 FTP_TRP.1/Join 高信頼パス (詳細化)

FTP_TRP.1 の本繰り返しは、FCO_CPC_EXT.1 (セクション A.7.1)における分散型 TOE コンポーネント登録のための選択可能な尾オプションの１つとして定義される。

FTP_TRP.1/Join	**高信頼パス**

FTP_TRP.1.1/Join TSF は、それ自身と**参入しようとするコンポーネント**~~[選択：リモート、ローカル]~~利用者間に、他の通信パスと論理的に区別され、**[選択：TSF 端点、参入しようとするコンポーネントと TSF 端点の両方]**~~その端点~~の保証された識別と、**改変 [選択：及び暴露、なし]**からの通信データの保護を提供する通信パスを提供しなければならない。

FTP_TRP.1.2/Join TSF は、[選択 : TSF、**参入しようとするコンポーネント**~~ローカル利用者、リモート利用者~~] に、高信頼パスを介して通信を開始することを許可しなければならない。

FTP_TRP.1.3/Join TSF は、*運用ガイダンスへの参照*で**特定された環境上の制約の下にある TSF へ参入しようとするコンポーネント**に対して、高信頼パスの使用を要求しなければならない。

適用上の注釈 47

本 SFR は、FCO_CPC_EXT.1.2 の主たる選択において特定されたチャネル種別の 1 つを実装する。FTP_TRP.1/Join における「参入しようとするコンポーネント」は、登録プロセスを用いることによって分散型 TOE に参入を試行するような IT エンティティである。

本 SFR の影響は、分散された TSF が生成されようとしている間に(または、既存の分散された TSF へコンポーネントが追加されるときに)セキュアなやり方で通信する能力をコンポーネントに要求することである。コンポーネントの初期ペアから TSF を生成しようとするとき、これらのコンポーネントのいずれかが本 SFR における「TSF」の意味を満たす目的で

TSF として特定されてもよい。

FTP_TRP.1.1/Join における選択は、チャネルによって機密性(即ち、暴露からのデータの保護)が提供されないかもしれないような場合について認識する。ST 作成者は、このような場合における TOE が機密性を提供するために頼る運用環境 (FTP_TRP.1.3/Join で参照される制約条件の一部として)があるかまたは好感される登録データが機密性を要求しないか(この主張は正当化されなければならない(must)ような場合)を TSS において区別すること。もし、「なし」が選択された場合には、この用語は、可読性を向上するために ST において省略されてもよい。

FTP_TRP.1.3/Join における割付は、ST が登録環境を保護するために必要とされるあらゆる具体的な詳細について注記していることを保証する。

ST にて登録チャネル用に FTP_TRP.1/Join が使用されるとき、このチャネルは通常のコンポーネント間通信チャネル(後者のチャネルは FTP_ITC.1 または FPT_ITT.1 を満たさなければならない)として再利用できないことに留意されたい。

FTP_TRP.1/Join に関連する準備手続きの具体的な要件は、[SD] の評価アクティビティで定義される。

A.7 通信 (FCO)

A.7.1 通信相手の管理 (FCO_CPC_EXT)

本セクションの SFR は、分散型 TOE (参照、セクション 3.3) を構成するためにセキュリティ管理者の管理下にあるコンポーネントが共に参入するようなやり方を用いた管理に関する最上位の要件を定義する。SFR は、登録プロセスで使用されるかもしれない下位レベルの特性を持つチャネル種別を定義するため、その他の SFR への参照を用いている。

A.7.1.1 FCO_CPC_EXT.1 コンポーネント登録チャネル定義

FCO_CPC_EXT.1	**コンポーネント登録チャネル定義**

FCO_CPC_EXT.1.1 TSF は、TOE コンポーネントの任意のペア間の通信が行われる前に、このような通信を有効化することをセキュリティ管理者に要求しなければならない(shall)。

FCO_CPC_EXT.1.2 TSF は、コンポーネントが、少なくとも TSF データ用に以下を用いるような通信チャネルを確立し、使用するための登録プロセスを実装しなければならない (shall)：[選択：

- [選択：FTP_ITC.1、FPT_ITT.1]のセキュアチャネル要件を満たすようなチャネル、
- FTP_TRP.1/Join のセキュア登録チャネル要件を満たすようなチャネル、
- チャネルなし]。

FCO_CPC_EXT.1.3 TSF は、TOE コンポーネントの任意のペア間での通信の無効化をセキュリティ管理者が可能としなければならない(shall)。

適用上の注釈 48

本 SFR は、TOE が分散型である場合にのみ適用可能であり、ゆえに内部 TSF チャネル経由で通信する必要がある複数のコンポーネントを持つ。コンポーネントの初期のペアから TSF を作るとき、これらのコンポーネントのいずれかは、本 SFR の「TSF」の意味を満たす目的の TSF として特定されてもよい。

本要件の意図は、分散型 TOE に参入しようとするコンポーネントが TOE のその他のコンポーネントと通信できる前、及び新たなコンポーネントが TSF の一部として動作する前に、管理者による積極的な有効化ステップを含む登録プロセスがあることを保証することである。登録プロセスは、参入しようとするコンポーネントとの通信にそれ自身が含まれてもよい：多くのネットワークデバイスがこの特注のプロセスを使用し、「登録通信」のセキュリティ要件は、FCO_CPC_EXT.1.2 でそのときに定義される。本「登録通信」チャネルの使用は、FCO_CPC_EXT.1.1 の要件と不整合と見なされない(即ち、登録チャネルは、有効化ステップの前に使用されることが可能であるが、登録プロセスを完了するためだけのものである)。

FCO_CPC_EXT.1.2 のチャネル選択(登録チャネルについて)は、基本的に、外部 IT エンティティ(FPT_ITC.1)または既存の TOE コンポーネント(FPT_ITT.1)と通信するために使用されるチャネルと等価であるような通常のセキュアチャネルの利用、または登録に特化した別の種別のチャネル(FTP_TRP.1/Join)の間の選択である。TOE が登録用の通信チャネルを要求しない場合(例、登録は各コンポーネントにおいて管理者によって設定アクションにより完全に達成されているから)、FCO_CPC_EXT.1.2 の主たる選択は「チャネルなし」選択肢で完了する。

ST 作成者が FCO_CPC_EXT.1.2 の主たる選択で FTP_ITC.1/FPT_ITT.1 チャネル種別を選択する場合、TSS は、使用されるチャネルを規定するような関連する SFR の繰り返しを特定すること。ST 作成者が FTP_TRP.1/Join チャネル種別を選択する場合、TOE 要約仕様(おそらく、運用ガイダンスからのサポートと共に)には、使用するチャネルとメカニズムの詳細について記述すること(また、そのチャネルが意図した参入者とゲートキーパーによってのみ使用可能であることを登録プロセスがどのように保証するかについて記述すること)。FTP_TRP.1/Join チャネル種別が運用環境におけるセキュリティ対策からのサポートを要求してもよいことに留意されたい(詳細については、FTP_TRP.1/Join の定義を参照)。

ST 作成者が FCO_CPC_EXT.1.2 の主たる選択で FTP_ITC.1/FPT_ITT.1 チャネル種別を選択する場合、ST は FTP_ITC.1 または FPT_ITT.1 の別々の繰り返しとして登録チャネルを特定し、FCO_CPC_EXT.1 の ST 適用上の注釈における繰り返し識別子を与えること(例、「FPT_ITT.1/Join」)。

登録用にセットアップされ、使用されるチャネルは、そのチャネルが FTP_ITC.1 または FPT_ITT.1 の要件を満たすことを提供する(即ち、異なる TOE コンポーネント間で)継続している内部通信チャネルとして適用されてもよい。さもなければ、登録チャネルが使用後に閉鎖され、別のチャネルが内部通信用に使用される。

FCO_CPC_EXT.1 に関連する準備手続きの具体的な要件は、[SD]の評価アクティビティで定義される。

B. 選択ベース要件

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

B.1 選択ベース SFR の監査事象

要件	監査対象事象	追加監査記録の内容
FCS_DTLSC_EXT.1	DTLS セション確立の失敗	失敗の理由
FCS_DTLSC_EXT.2	DTLS セション確立の失敗	失敗の理由
FCS_DTLSC_EXT.2	検出されたリプレイ攻撃	リプレイ攻撃元のアイデンティティ(例、送信元 IP アドレス)
FCS_DTLSS_EXT.1	DTLS セション確立の失敗	失敗の理由
FCS_DTLSS_EXT.1	検出されたリプレイ攻撃	リプレイ攻撃元のアイデンティティ(例、送信元 IP アドレス)
FCS_DTLSS_EXT.2	DTLS セション確立の失敗	失敗の理由
FCS_DTLSS_EXT.2	検出されたリプレイ攻撃	リプレイ攻撃元のアイデンティティ(例、送信元 IP アドレス)
FCS_HTTPS_EXT.1	HTTPS セション確立の失敗	失敗の理由
FCS_IPSEC_EXT.1	IPsec SA の確立失敗	失敗の理由
FCS_SSHC_EXT.1	SSH セション確立の失敗	失敗の理由
FCS_SSHS_EXT.1	SSH セション確立の失敗	失敗の理由
FCS_TLSC_EXT.1	TLS セションの確立失敗	失敗の理由
FCS_TLSC_EXT.2	TLS セションの確立失敗	失敗の理由
FCS_TLSS_EXT.1	TLS セションの確立失敗	失敗の理由
FCS_TLSS_EXT.2	TLS セションの確立失敗	失敗の理由

FIA_X509_EXT.1/Rev	証明書の有効性確認の不成功の試行	失敗の理由
FIA_X509_EXT.2	なし	なし
FIA_X509_EXT.3	なし。	なし。
FPT_TST_EXT.2	自己テストの失敗	失敗の理由 (無効な証明書の識別子を含む)
FPT_TUD_EXT.2	アップデートの失敗	失敗の理由 (無効な証明書の識別子を含む)
FMT_MOF.1/AutoUpdate	アップデートの自動チェックまたは自動アップデートの有効化または無効化。	なし。
FMT_MOF.1/Functions	外部 IT エンティティへの監査データの送信ふるまいの改変、監査データの取扱、ローカル監査格納領域が満杯のときの監査機能。	なし。

表 5：選択ベース SFR 及び監査対象事象

適用上の注釈 49

FIA_X509_EXT.1/Rev の監査事象は、以下を保証することによる証明書有効性確認を完了できないような TOE に基づいている：

- *basicConstraints 拡張の存在及び CA フラグがすべての CA 証明書について TRUE にセットされるもの。*
- *信頼される階層的な CA のディジタル署名の検証*
- *CRL を閲覧／アクセス、または OCSP サーバをアクセス(ST での選択に従って)。*

これらのチェックのいずれかが失敗する場合、失敗の監査事象が監査ログに書かれるべきである(should)。

B.2 暗号サポート (FCS)

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

B.2.1.1 FCS_DTLSC_EXT & FCS_DTLSS_EXT DTLS プロトコル

Datagram TLS (DTLS) は、NDcPP の要求されるコンポーネントではない。TOE が DTLS を実装する場合、FTP_ITC.1、FTP_TRP.1/Admin、または FPT_ITT.1 の対応する選択が、DTLS プロトコルが何を保護するために実装されるかについて定義するためになされるべきである。

TOA は、DTLS セションでのクライアント、サーバまたは両方として動作することがある。本要件は、これらの際を許容するため、DTLS クライアント (FCS_DTLSC_EXT) と DTLS サーバ (FCS_DTLSS) の要件へ分割される。

TOE が主張される DTLS セションの間にクライアントとして動作する場合、ST 作成者は FCS_DTLSC_EXT 要件の一つを主張するべきである。TOE がアプリケーションそうデータを外部エンティティへ DTLS によって提供される高信頼チャネルを用いて送信のみ行う場合、(即ち、DTLS を介して syslog を送信する) FCS_DTLSC_EXT.1 が選択されるべきである。

アプリケーションそう通信が双方向である場合、即ち、TOE がアプリケーションデータを送信及び受信の両方を行う、または DTLS サーバによって管理される場合、FCS_DTLSC_EXT.2 が要求される。FCS_DTLSC_EXT.2 はクライアントが以下を実行できなければならないことを要求する：

- 相互認証のために DTLS サーバへ証明書を提示する。
- DTLS サーバからの DTLS メッセージが無効なメッセージ認証コード(MAC)を含む場合選択されたアクションを実行する。
- リプレイされたメッセージを検出する

監査要件が適切に満たされることを保証するため、DTLS 受信者は、アプリケーション層で DTLS 接続状態を監視する必要があるかもしれない。長期間 (アプリケーションは「長い」が何を意味するかを決定するような) DTLS 接続から一切データを受信されないとき、受信者は close_notify アラートメッセージを送信し、接続を終了するべきである。

FCS_DTLSC_EXT.1	**DTLS クライアントプロトコル**

FCS_DTLSC_EXT.1.1 TSF は、以下の暗号スイートをサポートする[選択：DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall)：

- [選択：
  - RFC 3268 で定義された TLS_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_192_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_256_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA

- RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- RFC 5246 で定義された TLS_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 で定義された TLS_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 で定義された TLS_RSA_WITH_AES_256_CBC_SHA256
- RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

]。

適用上の注釈 50

評価される構成でテストされるべき暗号スイートは、本要件によって限定される。ST 作成者は、サポートされる暗号スイートを選択するべきである。テスト環境におけるサーバ上で管理上評価される構成において利用可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない、RFC6347 への適合を主張する場合に要求される。

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべての TOE に対して DTLS v1.2 が要求される。

FCS_DTLSC_EXT.1.2 TSF は、RFC 6125 セクション 6 に従って、提示される識別子が参照識別子と一致することを検証しなければならない(shall)。

適用上の注釈 51

アイデンティティ検証の規則は、RFC 6125 のセクション 6 で記述される。参照識別子は、

アプリケーションサービスによって、管理者により(例、ウェブサーバへ URL を入力またはリンクをクリック)、設定により(例、メールサーバまたは認証サーバの名称を設定)、またはアプリケーションにより(例、API のパラメタ)確立される。単一の参照識別子のソースドメインとアプリケーションサービス種別(例、HTTP、SIP、LDAP)に基づいて、クライアントは、証明書の Subject Name フィールドの Common Name 及び Subject Alternative Name フィールドの (機微でない場合) DNS 名、URI 名、及び Service Name のような、受け入れ可能なすべての参照識別子を確立する。次に、クライアントは、すべての受け入れ可能な参照識別子のこのリストを DTLS サーバ証明書における提示された識別子と比較する。

検証の望ましい方法は、DNS 名、URI 名、または Service Name を用いて Subject Alternative Name である。Common Name を用いる検証は、後方互換の目的で要求される。さらに、Subject Name または Subject Alternative 名 における IPA アドレスの利用のサポートは、ベストプラクティスに反するため推奨されないが、実装されもよい。最後に、クライアントは、ワイルドカードを用いて参照識別子を構築することを避けるべきである。しかし、提示された識別子がワイルドカードを含む場合に、クライアントはマッチングに関するベストプラクティスに従わなければならない ; このようなベストプラクティスは、評価アクティビティに取り込まれる。

FCS_DTLSC_EXT.1.3 TSF は、サーバ証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効であると思われる場合、TSF は、[選択 : 接続を確立しない、接続を確立するための許可を要求、*[割付 : その他のアクション]*]しなければならない(shall)。

適用上の注釈 52

DTLS が FTP_ITC で選択される場合、有効性は、RFC 5280 に従って、識別子検証、証明書パス、有効期限、及び失効状態によって決定される。証明書有効性は、FIA_X509_EXT.1/Rev で実行されるテストに従ってテストされる。DTLS が FPT_ITT で選択される場合、証明書有効性は、FIA_X509_EXT.1/ITT で実行されるテストに従ってテストされる。

FCS_DTLSC_EXT.1.4 TSF は、Client Hello において、[選択 : Supported Elliptic Curves Extension を提示しない、以下の NIST 曲線と共に Supported Elliptic Curves Extension を提示する : [選択 : secp256r1、secp384r1、secp521r1] 及びその他の曲線なし] ようにしなければならない(shall)。

適用上の注釈 53

楕円曲線を用いた暗号スイートが FCS_DTLSC_EXT.1.1 で選択された場合、1 つまたはそれ以上の曲線の選択が要求される。楕円曲線を用いる暗号スイートが FCS_DTLSC_EXT.1.1 で選択されなかった場合、「Supported Elliptic Curves Extension を提示しない」が選択されるべきである。

本要件は、認証及び鍵共有のために許可される楕円曲線を FCS_COP.1/SigGen 及び FCS_CKM.1 及び FCS_CKM.2 からの NIST 曲線に限定する。本拡張は、楕円曲線暗号シートをサポートしているクライアントに対して要求される。

FCS_DTLSC_EXT.2	**DTLS クライアントプロトコル － 認証付き**

FCS_DTLSC_EXT.2.1 TSF は、以下の暗号スイートをサポートする[選択 : DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall) :

- [選択：
  - RFC 3268 で定義された TLS_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_192_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_256_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - RFC 5246 で定義された TLS_RSA_WITH_AES_128_CBC_SHA256
  - RFC 5246 で定義された TLS_RSA_WITH_AES_192_CBC_SHA256
  - RFC 5246 で定義された TLS_RSA_WITH_AES_256_CBC_SHA256
  - RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA256
  - RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256
  - RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
  - RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

  ]。

適用上の注釈 54

ST 作成者は、サポートされる暗号スイートを選択するべきである。テスト環境におけるサーバ上で管理上評価される構成において利用可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない、RFC6347 への適合を主張する場合に要求される。

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべての TOE に対して DTLS v1.2 が要求される。

FCS_DTLSC_EXT.2.2 TSF は、RFC 6125 セクション 6 に従って、提示される識別子が参照識別子と一致することを検証しなければならない(shall)。

適用上の注釈 55

アイデンティティ検証の規則は、RFC 6125 のセクション 6 で記述される。参照識別子は、アプリケーションサービスによって、管理者により(例、ウェブサーバへ URL を入力またはリンクをクリック)、設定により(例、メールサーバまたは認証サーバの名称を設定)、またはアプリケーションにより(例、API のパラメタ)確立される。単一の参照識別子のソースドメインとアプリケーションサービス種別(例、HTTP、SIP、LDAP)に基づいて、クライアントは、証明書の Subject Name フィールドの Common Name 及び Subject Alternative Name フィールドの (機微でない場合) DNS 名、URI 名、及び Service Name のような、受け入れ可能なすべての参照識別子を確立する。次に、クライアントは、すべての受け入れ可能な参照識別子のこのリストを DTLS サーバ証明書における提示された識別子と比較する。

検証の望ましい方法は、DNS 名、URI 名、または Service Name を用いて Subject Alternative Name である。Common Name を用いる検証は、後方互換の目的で要求される。さらに、Subject Name または Subject Alternative 名 における IPA アドレスの利用のサポートは、ベストプラクティスに反するため推奨されないが、実装されもよい。最後に、クライアントは、ワイルドカードを用いて参照識別子を構築することを避けるべきである。しかし、提示された識別子がワイルドカードを含む場合に、クライアントはマッチングに関するベストプラクティスに従わなければならない ; このようなベストプラクティスは、評価アクティビティに取り込まれる。

FCS_DTLSC_EXT.2.3 TSF は、サーバ証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効であると思われる場合、TSF は、[選択 : 接続を確立しない、接続を確立するための許可を要求、*[割付 : その他のアクション]*]しなければならない(shall)。

適用上の注釈 56

DTLS が FTP_ITC で選択される場合、有効性は、RFC 5280 に従って、識別子検証、証明書パス、有効期限、及び失効状態によって決定される。証明書有効性は、FIA_X509_EXT.1/Rev で実行されるテストに従ってテストされる。DTLS が FPT_ITT で選択される場合、証明書有効性は、FIA_X509_EXT.1/ITT で実行されるテストに従ってテストされる。

FCS_DTLSC_EXT.2.4 TSF は、Client Hello において、[選択 : Supported Elliptic Curves Extension を提示しない、以下の NIST 曲線と共に Supported Elliptic Curves Extension を提示する : [選択 : secp256r1、secp384r1、secp521r1] 及びその他の曲線なし] ようにしなければならない(shall)。

適用上の注釈 57

楕円曲線を用いた暗号スイートが FCS_DTLSC_EXT.2.1 で選択された場合、1 つまたはそれ以上の曲線の選択が要求される。楕円曲線を用いる暗号スイートが FCS_DTLSC_EXT.2.1 で選択されなかった場合、「Supported Elliptic Curves Extension を提示しない」が選択されるべきである。

本要件は、認証及び鍵共有のために許可される楕円曲線を FCS_COP.1/SigGen 及び FCS_CKM.1 及び FCS_CKM.2 からの NIST 曲線に限定する。本拡張は、楕円曲線暗号シート

をサポートしているクライアントに対して要求される。

FCS_DTLSC_EXT.2.5 TSF は、X.509v3 証明書を用いて相互認証をサポートしなければならない(shall)。

適用上の注釈 58

DTLS 用の X.509v3 証明書の利用は、FIA_X509_EXT.2.1 で対処される。本要件は、クライアントがDTLS 相互認証のためDTLS サーバへ証明書を提示できなければならないことを追加する。

FCS_DTLSC_EXT.2.6 TSF は、受信したメッセージが無効な MAC を含む場合、[選択：DTLS セションを終了、レコードを静かに破棄] しなければならない(shall)。

適用上の注釈 59

メッセージ認証コード（MAC）は、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関するである。MAC はDTLS ハンドシェイクフェーズ中にネゴシエーションされ、DTLS データ交換中に送信者から受信されるメッセージの完全性を保護するために利用される。MAC 検証が失敗する場合、セションは終了されなければならない(must)、またはレコードは静かに破棄されなければならない(must)。

FCS_DTLSC_EXT.2.7 TSF は、以下についてのリプレイされたメッセージを検出し、静かに破棄しなければならない(shall)：

- 以前受信した DTLS レコード。
- スライド窓にフィットするには古すぎる DTLS レコード。

適用上の注釈 60

リプレイ検出は、DTLS 1.2 (RFC 6347) のセクション 4.1.2.6 及びDTLS 1.0 (RFC 4347) のセクション 4.1.2.5 で記述される。それぞれの受信されたレコードについて、受信者は、そのレコードがスライディング受信ウィンドウの範囲内にあり、セション中に受信されたその他のレコードのシーケンス番号を重複しないようなシーケンス番号を含むことを検証する。

「静かに破棄」は、TOE が応答することなしにパケットを破棄することを意味する。

FCS_DTLSS_EXT.1	**DTLS サーバプロトコル**

FCS_DTLSS_EXT.1.1 TSF は、以下の暗号スイートをサポートする[選択：DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall)：

- [選択：
  - RFC 3268 で定義された TLS_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_192_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_256_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

- RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
- RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- RFC 5246 で定義された TLS_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 で定義された TLS_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 で定義された TLS_RSA_WITH_AES_256_CBC_SHA256
- RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

]。

適用上の注釈 61

評価される構成でテストされるべき暗号スイートは、本要件によって限定される。ST 作成者は、サポートされる暗号スイートを選択するべきである。テスト環境におけるサーバ上で管理上評価される構成において利用可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、RFC6347 への適合を主張する場合に要求される。

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべての TOE に対して DTLS v1.2 が要求される。

FCS_DTLSS_EXT.1.2　TSF は、[なし(訳注 : 拒否する DTLS バージョンなし)]を要求するクライアントからの接続を拒否しなければならない(shall)。

適用上の注釈 62

本 cPP の本バージョンは、DTLS v1.0 を TOE が拒否することを要求しない。本 cPP の将来のバージョンでは、DTLS v1.0 はすべての TOE に対して供されることを要求されるだろう。

FCS_DTLSS_EXT.1.3 TSF は、DTLS クライアントが検証を失敗する場合、接続ハンドシェイク試行を進めてはならない(shall not)。

適用上の注釈 63

DTLS クライアントを検証するプロセスは、RFC 6347（DTLS 1.2）のセクション 4.2.1 及び RFC 4347（DTLS 1.0）で規定される。TOE は、接続確立 (ハンドシェイク) 中に、かつ Server Hello メッセージを TSF が送信する前に、DTLS クライアントを検証する。ClientHello を受信後に、DTLS サーバは、HelloVerifyRequest をクッキーと共に送信する。クッキーは、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関数を用いた署名メッセージである。DTLS クライアントは、次に別の ClientHello にクッキーを添付して送信する。DTLS サーバが署名されたクッキーの検証に成功する場合、クライアントは、なりすましされた IP アドレスを用いていない。

FCS_DTLSS_EXT.1.4 TSF は、 [選択：鍵長[選択 2048 ビット、3072 ビット、4096 ビット]を用いて RSA 鍵確立を実行 ; NIST 曲線[選択：secp256r1、secp384r1、secp521r1]及びその他の曲線なしを介した EC Diffie-Hellman パラメタを生成 ; [選択：2048 ビット、3072 ビット]長の Diffie-Hellman パラメタを生成] しなければならない(shall)。

適用上の注釈 64

ST に FCS_DTLSS_EXT.1.1 における DHE または ECDHE 暗号スイートを列挙する場合、ST には、本要件の Diffie-Hellman または NIST 曲線の選択を含まなければならない(must)。FMT_SMF.1 は、DTLS 接続のセキュリティ強度を確立するため、鍵共有パラメタの設定を要求する。

FCS_DTLSS_EXT.1.5 TSF は、受信したメッセージに無効な MAC が含まれる場合、 [選択：DTLS セションを終了、レコードを静かに破棄] しなければならない(shall)。

適用上の注釈 65

メッセージ認証コード（MAC）は、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関数である。MAC は DTLS ハンドシェイクフェーズ中にネゴシエーションされ、DTLS データ交換中に送信者から受信されるメッセージの完全性を保護するために利用される。MAC 検証が失敗する場合、セションは終了されなければならない(must)、またはレコードは静かに破棄されなければならない(must)。

FCS_DTLSS_EXT.1.6 TSF は、以下についてのリプレイされたメッセージを検出し、静かに破棄しなければならない(shall)：

- 以前受信した DTLS レコード。
- スライド窓にフィットするには古すぎる DTLS レコード。

適用上の注釈 66

リプレイ検出は、DTLS 1.2 (RFC 6347) のセクション 4.1.2.6 及び DTLS 1.0 (RFC 4347) のセクション 4.1.2.5 で記述される。それぞれの受信されたレコードについて、受信者は、そのレコードがスライディング受信ウィンドウの範囲内にあり、セション中に受信されたその他のレコードのシーケンス番号を重複しないようなシーケンス番号を含むことを検証する。

「静かに破棄」は、TOE が応答することなしにパケットを破棄することを意味する。

FCS_DTLSS_EXT.2	**DTLS サーバプロトコル － 相互認証付き**

FCS_DTLSS_EXT.2.1 TSF は、以下の暗号スイートをサポートする[選択：DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall)：

- [選択：
  - RFC 3268 で定義された TLS_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_192_CBC_SHA
  - RFC 3268 で定義された TLS_RSA_WITH_AES_256_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA
  - RFC 3268 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
  - RFC 4492 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
  - RFC 5246 で定義された TLS_RSA_WITH_AES_128_CBC_SHA256
  - RFC 5246 で定義された TLS_RSA_WITH_AES_192_CBC_SHA256
  - RFC 5246 で定義された TLS_RSA_WITH_AES_256_CBC_SHA256
  - RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_192_CBC_SHA256
  - RFC 5246 で定義された TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
  - RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256
  - RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
  - RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
  - RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

  ]。

適用上の注釈 67

評価された構成においてテストされるべき暗号スイートは、本要件によって限定される。ST 作成者は、サポートされる暗号スイートを選択するべきである。テスト環境におけるサーバ上で管理上評価される構成において利用可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、

RFC6347 への適合を主張する場合に要求される。

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべての TOE に対して DTLS v1.2 が要求される。

FCS_DTLSS_EXT.2.2 TSF は、[なし(訳注 : 拒否する DTLS バージョンなし)]を要求するクライアントからの接続を拒否しなければならない(shall)。

適用上の注釈 68

本 cPP の本バージョンは、DTLS v1.0 を TOE が拒否することを要求しない。本 cPP の将来のバージョンでは、DTLS v1.0 はすべての TOE に対して供されることを要求されるだろう。

FCS_DTLSS_EXT.2.3 TSF は、DTLS クライアントが検証を失敗する場合、接続ハンドシェイク試行を進めてはならない(shall not)。

適用上の注釈 69

DTLS クライアントを検証するプロセスは、RFC 6347 (DTLS 1.2) のセクション 4.2.1 及び RFC 4347 (DTLS 1.0)で規定される。TOE は、接続確立 (ハンドシェイク) 中に、かつ Server Hello メッセージを TSF が送信する前に、DTLS クライアントを検証する。ClientHello を受信後に、DTLS サーバは、HelloVerifyRequest をクッキーと共に送信する。クッキーは、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関数を用いた署名メッセージである。DTLS クライアントは、次に別の ClientHello にクッキーを添付して送信する。DTLS サーバが署名されたクッキーの検証に成功する場合、クライアントは、なりすましされた IP アドレスを用いていない。

FCS_DTLSS_EXT.2.4 TSF は、 [選択：鍵長[選択 2048 ビット、3072 ビット、4096 ビット]を用いて RSA 鍵確立を実行 ; NIST 曲線[選択：secp256r1、secp384r1、secp521r1]及びその他の曲線なしを介した EC Diffie-Hellman パラメタを生成 ; [選択：2048 ビット、3072 ビット]長の Diffie-Hellman パラメタを生成] しなければならない(shall)。

適用上の注釈 70

ST に FCS_DTLSS_EXT.1.1 における DHE または ECDHE 暗号スイートを列挙する場合、ST には、本要件の Diffie-Hellman または NIST 曲線の選択を含まなければならない(must)。FMT_SMF.1 は、DTLS 接続のセキュリティ強度を確立するため、鍵共有パラメタの構成を要求する。

FCS_DTLSS_EXT.2.5 TSF は、受信したメッセージに無効な MAC が含まれる場合、 [選択：DTLS セションを終了、レコードを静かに破棄] しなければならない(shall)。

適用上の注釈 71

メッセージ認証コード (MAC)は、DTLS ハンドシェイクフェーズ中にネゴシエーションされ、DTLS データ交換中に送信者から受信されるメッセージの完全性を保護するために利用される。MAC 検証が失敗する場合、セションは終了されなければならない(must)、またはレコードは静かに破棄されなければならない(must)。

FCS_DTLSS_EXT.2.6 TSF は、以下についてのリプレイされたメッセージを検出し、静かに破棄しなければならない(shall)：

- 以前受信した DTLS レコード。
- スライド窓にフィットするには古すぎる DTLS レコード。

適用上の注釈 72

リプレイ検出は、DTLS 1.2 (RFC 6347) のセクション 4.1.2.6 及び DTLS 1.0 (RFC 4347) のセクション 4.1.2.5 で記述される。それぞれの受信されたレコードについて、受信者は、そのレコードがスライディング受信ウィンドウの範囲内にあり、セション中に受信されたその他のレコードのシーケンス番号を重複しないようなシーケンス番号を含むことを検証する。

「静かに破棄」は、TOE が応答することなしにパケットを破棄することを意味する。

FCS_DTLSS_EXT.2.7 TSF は、X.509v3 証明書を用いて DTLS クライアントの相互認証をサポートしなければならない(shall)。

FCS_DTLSS_EXT.2.8 TSF は、クライアント証明書が無効である場合、高信頼チャネルを確立してはならない(shall not)。もし、クライアント証明書が無効と思われる場合、TSF は [選択 : 接続を確立しない、接続の確立するための許可を要求、*[割付 : その他のアクション]*] ようにしなければならない(shall)。

適用上の注釈 73

DTLS 用の X.509v3 の利用は、FIA_X509_EXT.2.1 で対処される。本要件は、この利用に、DTLS 相互認証のクライアント側の証明書のサポートを含まなければならない(shall)。

DTLS が FTP_ITC で選択される場合、有効性は、RFC5280 に従って、識別子検証、証明書パス、有効期限、及び失効状態によって決定される。証明書有効性は、FIA_X509_EXT.1/Rev のために実行されるテストに従ってテストされる。DTLS は、FPT_ITT で選択される場合、証明書有効性は、FIA_X509_EXT.1/ITT のために実行されるテストに従ってテストされる。

FCS_DTLSS_EXT.2.9 TSF は、証明書に含まれる distinguished name(DN) または Subject Alternative Name (SAN) がクライアントの期待される識別子と合致しない場合、高信頼チャネルを確立してはならない(shall)。X.509v3 証明書を用いて DTLS クライアントの相互認証をサポートしなければならない(shall)。

適用上の注釈 74

クライアント識別子は、証明書の Subject フィールドまたは Subject Alternative extension にあるかもしれない。規定される識別子は、設定されるか、ピアによってドメイン名、IP アドレス、又は電子メールアドレスと比較されるか、または比較のためにディレクトリサーバへ渡されるかのいずれかであるかもしれない。

B.2.1.2 FCS_HTTPS_EXT.1 HTTPS プロトコル

HTTPS は、本 cPP の要求されるコンポーネントではない。TOE が HTTPS を実装する場合、FTP_ITC.1、FPT_ITT.1 及び／または FTP_TRP.1/Admin の対応する選択は、HTTPS プロトコルが何を保護するために実装されるかを定義するようになされるべきである。

FCS_HTTPS_EXT.1	**HTTPS プロトコル**

FCS_HTTPS_EXT.1.1 TSF は、RFC 2818 に適合する HTTPS プロトコルを実装しなければな

らない(shall)。

適用上の注釈 75

ST 作成者は、規定された規格に実装がどのように適合しているかを決定するために十分な詳細情報を提供しなければならない；これは、TSS での追加の詳細情報によって達成されることが可能である。

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

FCS_HTTPS_EXT.1.3 ピア証明書が提示される場合、TSF は、そのぴあ証明書が無効と思われる場合に [選択：クライアント認証を要求しない、接続を確立しない、接続を確立するための許可を要求する、*[割付：その他のアクション]*] を行わなければならない(shall)。

適用上の注釈 76

HTTPS が FTP_TRP.1/Admin または FTP_ITC.1 で選択される場合、有効性は、RFC 5280 に従って、識別子検証、証明書パス、有効期限、及び失効状態により決定される。証明書有効性は、FIA_X509_EXT.1/Rev 用に実行されるテストに従ってテストされる。HTTPS が FPT_ITT.1 で選択される場合、証明書有効性は、FIA_X509_EXT.1/ITT 用に実行されるテストに従ってテストされる。

B.2.1.3 FCS_IPSEC_EXT.1 IPsec プロトコル

ネットワークデバイスの通信の端点は、地理的にも論理的にも遠く離れている可能性があり、さまざまな他の信頼されないシステムを通過するかもしれない。ネットワークデバイスのセキュリティ機能は、任意の重要なネットワークトラフィク (管理トラフィク、認証トラフィク、監査トラフィク等) を保護できなければならない(must)。ネットワークデバイスと外部 IT エンティティとの間の相互認証された通信チャネルを提供する一つの方法は、IPsec を実装することである。

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

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

FCS_IPSEC_EXT.1	**IPsec プロトコル**

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

適用上の注釈 77

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

実装の詳細にかかわらず、パケットが「規則」に「一致」して、その結果アクションが実行されるという「規則」がある。

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

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

FCS_IPSEC_EXT.1.3 TSF は、[選択：トランスポートモード、トンネルモード] を実装しなければならない(shall)。

適用上の注釈 78

ST 作成者は、IPsec についてサポートされる操作モードを選択する。

FCS_IPSEC_EXT.1.4 TSF は、暗号アルゴリズム[選択 : AES-CBC-128、AES-CBC-192、AES-CBC-256 (RFC 3602 で規定)、その他のアルゴリズムなし]を用いて、セキュアハッシュアルゴリズム(SHA) ベースの HMAC[選択 : HMAC-SHA-1、HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512、その他のアルゴリズムなし] 及び [選択 : AES-GCM-128、AES-GCM-192、AES-GCM-256 (RFC 4106 で規定)、その他のアルゴリズムなし]と共に、RFC 4303 によって定義される IPsec プロトコル ESP を実装しなければならない(shall)。

適用上の注釈 79

AES-CBC アルゴリズムが選択されるとき、少なくとも 1 つの SHA ベースの HMAC も選ばれなければならない(must)。AES-GCM アルゴリズムだけが選択される場合、SHA ベースの HMAC は要求されない、なぜなら AES-GCM は機密性と完全性機能の両方を満たすためである。IPsec は、選択において含まれる SHA ベースの HMAC 関数の切り詰められた(truncated) バージョン(訳注：RFC4868 に記載の HMAC 出力値を切り詰められたデータを利用する方法) を利用してもよい。切り詰められた出力が利用される場合、TSS において強調されなければならない(shall)。

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

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

]。

適用上の注釈 80

TOE が IKEv1 用または IKEv2 用に SHA-2 ハッシュアルゴリズムを実装する場合、ST 作成者は RFC 4868 を選択する。TOE が、RFC4868 で記述されるとおりに切り詰められた SHA ベースの HMAC の利用を実装する場合、それらは、TSS において強調されなければならない

(shall)。

FCS_IPSEC_EXT.1.6　TSF は、[選択：IKEv1、IKEv2] プロトコルにおける暗号化されたペイロードが、暗号アルゴリズム[選択： AES-CBC-128、AES-CBC-192、AES-CBC-256(RFC 3602 で規定)、 AES-GCM-128、AES-GCM-128、AES-GCM-256 (RFC 5282 で規定)] を利用することを保証しなければならない(shall)。

適用上の注釈 81

AES-GCM-128、AES-GCM-192 及びAES-GCM-256 は、IKEv1 にはAES-GCM を定義する RFC が存在しないため、IKEv2 もまた選択される場合にのみ選択が可能である。

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

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

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

  ]

]。

適用上の注釈 82

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

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

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

  ]；

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

  ]

]。

適用上の注釈 83

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

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

適用上の注釈 84

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

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

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

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

] 。

適用上の注釈 85

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

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

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

FCS_IPSEC_EXT.1.11 TSF は、すべての IKE プロトコルが DH グループ[選択：14 (2048 ビット MODP)、19 (256 ビットランダム ECP)、20 (384 ビットランダム ECP)、24 (256 ビット POS 付の 2048 ビット MODP)] を実装していることを保証しなければならない(shall)。

適用上の注釈 86

この選択は、サポートされた追加の DH グループを特定するために使用される。これは、IKEv1 及び IKEv2 鍵交換に適用される。

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

適用上の注釈 87

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

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

適用上の注釈 88

本 cPP に適合するため、少なくとも 1 つの公開鍵ベースのピア認証方法が必須となる；何が実装されているかを反映するため、ST 作成者によって 1 つ以上の公開鍵スキームが選択される。ST 作成者は、使用されるアルゴリズム (及び鍵生成機能、提供される場合) を反映

した適切な FCS 要件が、それらの方法のサポートのため列挙されていることについても保証する。TSS には、これらのアルゴリズムが用いられる方法も詳述されることになる (例えば、RFC 2409 には、公開鍵を用いる 3 つの認証方法が規定されている；サポートされるそれぞれが TSS において記述される) ことに留意されたい。

FCS_IPSEC_EXT.1.14 TSF は、提示された識別子と参照識別子が以下の種別：[選択：IP アドレス、完全修飾ドメイン名(Fully Qualified Domain Name：FQDN)、利用者 FQDN、Distinguished Name(DN)] 及び [選択：その他の参照識別子なし、*[割付：その他のサポートされる参照識別子種別]*]であるような、受信した証明書の提示された識別子が設定された参照識別子と一致する場合にのみ、高信頼チャネルを確立しなければならない(shall)。

適用上の注釈 89

ピア認証のために RSA または ECDSA を用いるとき、参照識別子と提示される識別子が DN、IP アドレス、FQDN または利用者 FQDN のいずれかの形式を取る。参照識別子は、TOE が IKE 認証中にピアから受信すると期待する識別子である。提示される識別子は、ぴあの証明書本体内に含まれる識別子である。ST 作成者は、提示される識別と参照識別子のサポートされる種別を選択しなければならず、オプションで追加のサポートされる識別子種別を 2 番目の選択で割り付けることができる。DN 識別種別(ピア証明書における必ず Subject DN である)を除いて、TOE は、Common Name または Subject Alternative Name(SAN)のいずれか、またはその両方における識別子をサポートしてもよい。

望ましい検証方法は、DNS 名、URI 名、サービス名を用いた Subject Alternative Name である。Common N あめを用いる検証は、後方互換の目的で要求される。さらに、Subject Name または Subject Alternative Name における IP アドレスの利用のサポートは、ベストプラクティスに反するため、推奨されないが、実行されてもよい。

サポートされるピア証明書アルゴリズムは、FCS_IPSEC_EXT.1.13 と同じである。

B.2.1.4 FCS_SSHC_EXT ＆ FCS_SSHS_EXT SSH プロトコル

SSH は、本 cPP の要求されるコンポーネントではない、FTP_ITC.1、FPT_ITT.1 及び／または FTP_TRP.1/Admin での対応する選択は、SSH プロトコルが何を保護するために実装されるかを定義するようなされるべきである(should)。

TOA は、SSH セションにおいて、クライアントまたはサーバとして動作してもよい。要件は、これらの違いを許容するために SSH クライアント (FCS_SSHC_EXT) と SSH サーバ (FCS_SSHS_EXT)の要件へ分けられる。

FCS_SSHC_EXT.1	**SSH クライアントプロトコル**

FCS_SSHC_EXT.1.1 TSF は、RFC [選択：4251、4252、4253、4254、5647、5656、6187、6668、その他の RFC なし] に適合する SSH プロトコルを実装しなければならない(shall)。

適用上の注釈 90

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

ではなく、実装がそのサポートを含んでいなければならないことを意味する。「必須」と示されているが本コンポーネントの後のエレメントに列挙されないアルゴリズムが実装されていることを保証することは、本要件の評価アクティビティの適用範囲外である。

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

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

適用上の注釈 91

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

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

適用上の注釈 92

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの利用を特定している。RFC 5647 に記述されるように、AEAD_AES_128_GCM 及び AEAD_AES_256_GCM を暗号化アルゴリズムとして選ぶことができるのは、同一のアルゴリズムが MAC アルゴリズムとして用いられる場合のみである。対応する FCS_COP エントリがここで選択されたアルゴリズムについて ST に含まれる。

FCS_SSHC_EXT.1.5 TSF は、SSH 公開鍵ベース認証の実装がその公開鍵アルゴリズムとして [選択 : ssh-rsa、ecdsa-sha2-nistp256] 及び [選択 : ecdsa-sha2-nistp384、ecdsa-sha2-nistp521、x509v3-ecdsa-sha2-nistp256、x509v3-ecdsa-sha2-nistp384、x509v3-ecdsa-sha2-nistp521、その他の公開鍵アルゴリズムなし] を使用し、他のすべての公開鍵アルゴリズムを拒否することを保証しなければならない(shall)。

適用上の注釈 93

x509v3-ecdsa-sha2-nistp256、x509v3-ecdsa-sha2-nistp384 または x509v3-ecdsa-sha2-nistp521 が選択される場合、信頼される認証局のリストが FCS_SSHC_EXT.1.9 において選択されなければならない(shall)、また附属書 B の FIA_X509_EXT SFR が適用可能である。

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

適用上の注釈 94

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの利用を規定する。RFC 5647 で記述されるように、AEAD_AES_128_GCM 及び

AEAD_AES_256_GCM は、同じアルゴリズムが暗号化アルゴリズムとして利用されるときの MAC アルゴリズムとしてのみ選ばれることが可能である。RFC 6668 は、SSH における sha2 アルゴリズムの利用を規定する。

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

FCS_SSHC_EXT.1.8 TSF は、SSH コネクション内で同じセション鍵が 1 時間以内、かつ 1 ギガバイト未満の送信データというしきい値で利用されることを保証しなければならない(shall)。しきい値のいずれかに達した後、鍵変更(rekey)が実行される必要がある。

適用上の注釈 95

本 SFR は、2 つのしきい値を定義する－1 つは最大時間同じセション鍵が使用可能であり、他方はデータの最大容量まで同じセション鍵を用いて送信可能である。両方のしきい値が実装される必要があり、いずれかのしきい値に達すると鍵変更が実行される必要がある。最大送信データについて、受信及び送信データの合計が集計される必要がある。鍵変更は、送受信トラフィクについてのすべてのセション鍵 (暗号化、完全性保護) に提供される。

TOE が本 SFR で定義された最大値よりも低いしきい値を実装することは、受け入れ可能である。

本要件に関連する設定可能な、あらゆるしきい値について、ガイダンス証拠資料は、そのしきい値の可能な設定方法について規定する必要がある。許可された値がガイダンス証拠資料に規定され、本 SFR で規定されたしきい値以下でなければならないか、または TOE が本 SFR で規定されたしきい値を超えた値を受け付けてはならないかの、いずれかでなければならない。

FCS_SSHC_EXT.1.9 TSF は、SSH クライアントが RFC 4251 のセクション 4.1 で記述されるように、その対応する公開鍵、[選択：信頼された認証局のリスト、それ他の方法なし] を持つそれぞれのホスト名に結び付いたローカルなデータベース を用いる SSH サーバの識別情報を認証することを保証しなければならない。

適用上の注釈 96

信頼された認証局のリストは、FCS_SSHC_EXT.1.5 において x509v3-ecdsa-sha2-nistp256、x509v3-ecdsa-sha2-nistp384 または x509v3-ecdsa-sha2-nistp521 が指定される場合にのみ選択可能である。

FCS_SSHS_EXT.1	**SSH サーバプロトコル**

FCS_SSHS_EXT.1.1 TSF は、RFC [選択：4251、4252、4253、4254、5647、5656、6187、6668、その他の RFC なし] に適合する SSH プロトコルを実装しなければならない(shall)。

適用上の注釈 97

ST 作成者は、適合主張されている RFC を選択すること。これらは、本コンポーネントの後のエレメントにおける選択 (例えば、許可される暗号アルゴリズム) と一貫している必要が

あることに注意されたい。RFC 4253 は、特定の暗号アルゴリズムが「必須」であることを示している。これは、そのアルゴリズムが利用のため有効化されていなければならないことではなく、実装がそのサポートを含んでいなければならないことを意味する。「必須」と示されているが本コンポーネントの後のエレメントに列挙されないアルゴリズムが実装されていることを保証することは、本要件の評価アクティビティの適用範囲外である。

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

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

適用上の注釈 98

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

FCS_SSHS_EXT.1.4 TSF は、SSH トランスポートの実装が以下の暗号化アルゴリズムを使用し、他のすべての暗号アルゴリズムを拒否することを保証しなければならない(shall) : [選択 : aes123-cbc(訳注：正しくは「aes128-cbc」)、aes256-cbc、aes128-ctr、aes256-ctr、AEAD_AES_128_GCM、AEAD_AES_256_GCM]。

適用上の注釈 99

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの利用を規定する。RFC 5647 に記述されるように、AEAD_AES_128_GCM 及び AEAD_AES_256_GCM を暗号化アルゴリズムとして選ぶことができるのは、同じアルゴリズムが MAC アルゴリズムとして用いられる場合のみである。対応する FCS_COP のエントリがここで選択されたアルゴリズムについて ST に含まれる。

FCS_SSHS_EXT.1.5 TSF は、SSH 公開鍵ベース認証の実装がその公開鍵アルゴリズムとして [選択 : ssh-rsa、ecdsa-sha2-nistp256] 及び [選択 : ecdsa-sha2-nistp384、ecdsa-sha2-nistp521、x509v3-ecdsa-sha2-nistp256、x509v3-ecdsa-sha2-nistp384、x509v3-ecdsa-sha2-nistp521、その他の公開鍵アルゴリズムなし] を利用し、その他のすべての公開鍵アルゴリズムを拒否することを保証しなければならない(shall)。

適用上の注釈 100

x509v3-ecdsa-sha2-nistp256、x509v3-ecdsa-sha2-nistp384 または x509v3-ecdsa-sha2-nistp521 が選択される場合、附属書 B の FIA_X509_EXT の SFR が適用可能である。

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

適用上の注釈 101

RFC 5647 は、SSH における AEAD_AES_128_GCM 及び AEAD_AES_256_GCM アルゴリズムの利用を規定する。RFC 5647 に記述されるように、AEAD_AES_128_GCM 及び

AEAD_AES_256_GCM を MAC アルゴリズムとして選ぶことができるのは、同じアルゴリズムが暗号化アルゴリズムとして用いられる場合のみである。RFC 6668 は、SSH における sha2 アルゴリズムの利用を規定する。

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

FCS_SSHS_EXT.1.8 TSF は、SSH コネクション内で同じセション鍵が 1 時間以内、かつ 1 ギガバイト未満の送信データのしきい値で利用されることを保証しなければならない(shall)。しきい値のいずれかに達した後、鍵変更(rekey)が実行される必要がある。

適用上の注釈 102

本 SFR は、2 つのしきい値を定義する－1 つは最大時間同じセション鍵が使用可能であり、他方はデータの最大容量まで同じセション鍵を用いて送信可能である。両方のしきい値が実装される必要があり、いずれかのしきい値に達すると鍵変更が実行される必要がある。最大送信データについて、受信及び送信データの合計が集計される必要がある。鍵変更は、送受信トラフィクについてのすべてのセション鍵 (暗号化、完全性保護) に提供される。

TOE が本 SFR で定義された最大値よりも低いしきい値を実装することは、受け入れ可能である。

本要件に関連する設定可能な、あらゆるしきい値について、ガイダンス証拠資料は、そのしきい値の可能な設定方法について規定する必要がある。許可された値がガイダンス証拠資料に規定され、本 SFR で規定されたしきい値以下でなければならないか、または TOE が本 SFR で規定されたしきい値を超えた値を受け入れてはならないか、いずれかでなければならない。

B.2.1.5 FCS_TLSC_EXT & FCS_TLSS_EXT TLS プロトコル

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

TOE は、TLS セションにおいて、クライアント、サーバ、またはその両方として動作することがある。要件は、これらの違いを考慮して TLS クライアント (FCS_TLSC_EXT) と TLS サーバ (FCS_TLSS_EXT) 要件に分離されている。主張された TLS セションで TOE がクライアントとして動作する場合、ST 作成者は FCS_TLSC_EXT 要件の 1 つを主張すべきである(should)。TOE が主張される TLS セション中にサーバとして動作する場合、ST 作成者は、FCS_TLSS_EXT 要件の 1 つを主張するべきである(should)。TOE が主張される TLS セション中にクライアントとサーバの両方として動作する場合、ST 作成者は、FCS_TLSC_EXT 及び FCS_TLSS_EXT 要件の 1 つを主張するべきである(should)。

さらに、TLS は、クライアント認証が行われるかもしれないし、行われないかもしれない。ST 作成者は、TOE がクライアント認証をサポートしない場合、FCS_TLSC_EXT.1 及び FCS_TLSS_EXT.1 を主張しなければならない(shall)。ST 作成者は、TOE によりクライアント認証が行われる場合、FCS_TLSC_EXT.2 及び FCS_TLSS_EXT.2 を主張するべきである(should)。

FCS_TLSC_EXT.1	**TLS クライアントプロトコル**

FCS_TLSC_EXT.1.1 TSF は、[選択：TLS 1.2 (RFC 5246)、TLS 1.1 (RFC 4346)] を実装し、その他のすべての TLS 及び SSL バージョンを拒否しなければならない(shall)。TLS 実装は、以下の暗号スイートをサポートする：

[選択：

- RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_ SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256

- RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

]。

適用上の注釈 103

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである。テスト環境におけるサーバ上で評価される構成で管理的に使用されることが可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、RFC 5246 への適合を主張する場合には要求される。

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

本 cPP の将来のバージョンにおいて、すべての TOE に対して TLS v1.2 が要求される。

FCS_TLSC_EXT.1.2 TSF は、RFC 6125 セクション 6 に従って、提示された識別子が参照識別子と一致することを検証しなければならない(shall)。

適用上の注釈 104

アイデンティティの検証のための規則は、RFC 6125 のセクション 6 で記述される。参照識別子は、管理者によって(例、ウェブブラウザへの URL 入力、またはリンクをクリック)、設定 によって(例、メールサーバまたは認証サーバの名前の設定)、またはアプリケーションサービスに応じてアプリケーションによって (例、API のパラメタ)、確立される。単一の参照識別子の生成元ドメイン及びアプリケーションサービス種別 (例、HTTP、SIP、LDAP) に基づき、クライアントは受け入れ可能なすべての参照識別子、例えば、証明書の Subject Name フィールドの Common Name、及び Subject Alternative Name フィールドの (大文字と小文字を区別しない) DNS 名、URI 名、及びサービス名等を確立する。クライアントは、次にこのすべての受け入れ可能な参照識別子のリストを、TLS サーバの証明書において提示された識別子と比較する。

望ましい検証方法は、DNS 名、URI 名、またはサービス名を用いた Subject Alternative Name である。Common Name を用いる検証は、上位互換性 (backward compatibility) の目的で要求される。さらに、Subject Name または Subject Alternative Name 中の IP アドレス使用のサポートは、ベストプラクティスに反するため推奨されないが、実装されてもよい。最後に、クライアントは、ワイルドカードを用いた参照識別子の構築を避けるべきである。しかし、提示

された識別子がワイルドカードを含む場合、クライアントは一致に関するベストプラクティスに従わなければならない；これらのベストプラクティスは、評価アクティビティに取り込まれている。

FCS_TLSC_EXT.1.3 TSF は、サーバ証明書が有効である場合のみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効であると見なされる場合、TSF は、[選択：接続を確立しない、接続を確立するために許可を要求する、*[割付：その他のアクション]*]を行わなければならない(shall)。

適用上の注釈 105

TLS が FTP_TRP.1/Admin または FTP_ITC で選択される場合、有効性は、識別子の検証、証明書パス、有効期限、及び失効状態により、RFC 5280 に従って決定される。証明書の有効性は、FIA_X509_EXT.1/Rev 用に実行されるテストに従いテストされる。TLS が FPT_ITT で選択される場合、証明書の有効性は、FIA_X509_EXT.1/ITT について実行されるテストに従ってテストされる。

FCS_TLSC_EXT.1.4 TSF は、Client Hello において、[選択：Supported Elliptic Curves Extension を提示してはならない(shall not)、以下の NIST 曲線と共に Supported Elliptic Curves Extension を提示しなければならない(shall)： [選択：secp256r1、secp384r1、secp521r1] 及びその他の曲線なし]。

適用上の注釈 106

楕円曲線を用いる暗号スイートが FCS_TLSC_EXT.1.1 において選択された場合、1 つ以上の曲線の選択が要求される。楕円曲線を用いる暗号スイートが FCS_TLS_EXT.1.1 において一つも選択されない場合、「なし」が選択されるべきである(should)。

本要件は、認証及び鍵共有のために許可される楕円曲線を、FCS_COP.1/SigGen 及び FCS_CKM.1 ならびに FCS_CKM.2 からの NIST 曲線に制限する。本拡張は、楕円曲線暗号スイートをサポートしているクライアントに対して要求される。

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

FCS_TLSC_EXT.2.1 TSF は、 [選択：TLS 1.2 (RFC 5246)、TLS 1.1 (RFC 4346)] を実装し、その他のすべての TLS 及び SSL バージョンを拒否しなければならない(shall)。TLS 実装は、以下の暗号スイートをサポートする：

[選択：

- RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_ SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_ SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

]。

適用上の注釈 107

評価される構成においてテストされるべき暗号スイートは、本要件により制限される。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである(should)。テスト環境におけるサーバ上で評価される構成で管理的に使用されることが可能な暗号スイートを制限する必要がある。上記 Suite B アルゴリズム (RFC 6460) は、実装が望まれるアルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、RFC 5246 への適合を主張する場合には要求される。

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

本 cPP の将来のバージョンにおいて、すべての TOE に対して TLS v1.2 が要求される。

FCS_TLSC_EXT.2.2 TSF は、RFC 6125 セクション 6 に従って提示された識別子が参照識別子と一致することを検証しなければならない(shall)。

適用上の注釈 108

アイデンティティの検証のための規則は、RFC 6125 のセクション 6 で記述される。参照識別子は、管理者によって(例、ウェブブラウザへの URL 入力、またはリンクをクリック)、設定 によって(例、メールサーバまたは認証サーバの名前の設定)、またはアプリケーションサービスに応じてアプリケーションによって (例、API のパラメタ)、確立される。単一の参

照識別子の生成元ドメイン及びアプリケーションサービス種別 (例、HTTP、SIP、LDAP) に基づき、クライアントは受け入れ可能なすべての参照識別子、例えば、証明書の Subject Name フィールドの Common Name、及び Subject Alternative Name フィールドの (大文字と小文字を区別しない) DNS 名、URI 名、及びサービス名等を確立する。クライアントは、次にこのすべての受け入れ可能な参照識別子のリストを、TLS サーバの証明書において提示された識別子と比較する。

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

FCS_TLSC_EXT.2.3 TSF は、サーバ証明書が有効である場合のみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効と見なされる場合、TSF は、[選択：接続を確立してはならない(shall not)、接続を確立するために許可を要求しなければならない(shall)、*[割付：その他のアクション]*]を行わなければならない(shall)。

適用上の注釈 109

TLS が FTP_TRP.1/Admin または FTP_ITC で選択される場合、有効性は、識別子の検証、証明書パス、有効期限、及び失効状態により、RFC 5280 に従って決定される。証明書の有効性は、FIA_X509_EXT.1/Rev 用に実行されるテストに従いテストされなければならない(shall)。TLS が FPT_ITT で選択される場合、証明書の有効性は、FIA_X509_EXT.1/ITT のために実行されるテストに従ってテストされる。

FCS_TLSC_EXT.2.4 TSF は、Client Hello において、[選択：Supported Elliptic Curves Extension を提示してはならない(shall not)、以下の NIST 曲線と共に Supported Elliptic Curves Extension を提示しなければならない(shall)： [選択：secp256r1、secp384r1、secp521r1] 及びその他の曲線なし]。

適用上の注釈 110

楕円曲線を用いる暗号スイートが FCS_TLSC_EXT.2.1 において選択された場合、1 つ以上の曲線の選択が要求される。楕円曲線を用いる暗号スイートが FCS_TLS_EXT.2.1 において全く選択されなかった場合、「なし」が選択されるべきである(should)。

本要件は、認証及び鍵共有のために許可される楕円曲線を、FCS_COP.1/SigGen 及び FCS_CKM.1 ならびに FCS_CKM.2 からの NIST 曲線に制限する。本拡張は、楕円曲線暗号スイートをサポートしているクライアントに対して要求される。

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

適用上の注釈 111

TLS 用の X.509v3 証明書の使用は、FIA_X509_EXT.2.1 において対処される。本要件は、クライアントが TLS 相互認証のために TLS サーバへ証明書を提示できなければならない(must)

ことを追加している。

FCS_TLSS_EXT.1	**TLS サーバプロトコル**

FCS_TLSS_EXT.1.1 TSF は、[選択：TLS 1.2 (RFC 5246)、TLS 1.1 (RFC 4346)] を実装し、その他のすべての TLS 及び SSL バージョンを拒否しなければならない(shall)。TLS 実装は、以下の暗号スイートをサポートする：

[選択：

- RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

]。

適用上の注釈 112

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

ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである。テスト環境におけるサーバ上で評価される構成で管理者に使用されることが可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、RFC 5246 への適合を主張する場合には要求される。

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

本 cPP の将来のバージョンにおいて、すべての TOE に対して TLS v1.2 が要求される。

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

適用上の注釈 113

すべてのバージョンの SSL、及び TLS v1.0 は拒否される。FCS_TLSS_EXT.1.1 で選択されない TLS のあらゆるバージョンが、ここで選択されるべきである(should)。(本エレメントの選択で「なし」が選択される場合、ST 作成者は、「及びなし」という言葉を省略してもよい。)

FCS_TLSS_EXT.1.3 TSF は、[選択：鍵長 [選択：2048 ビット、3072 ビット、4096 ビット] を用いて RSA 鍵確立を実行 ； NIST 曲線 [選択：secp256r1, secp384r1、secp521r1] 及びその他の曲線なしを介して EC Diffie-Hellman パラメタを生成 ； パラメタ長 [選択：2048 ビット、3072 ビット] の Diffie-Hellman パラメタを生成]]を行わなければならない(shall)。

適用上の注釈 114

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

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

FCS_TLSS_EXT.2.1 TSF は、[選択：TLS 1.2 (RFC 5246)、TLS 1.1 (RFC 4346)] を実装し、その他のすべての TLS 及び SSL バージョンを拒否しなければならない(shall)。TLS 実装は、以下の暗号スイートをサポートする：

[選択：

- RFC 3268 に定義される TLS_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_RSA_WITH_AES_256_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_SHA
- RFC 3268 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA

- RFC 4492 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- RFC 5246 に定義される TLS_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 に定義される TLS_RSA_WITH_AES_256_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5246 に定義される TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_128_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_192_GCM_SHA256
- RFC 5288 で定義された TLS_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_CBC_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_192_GCM_SHA256
- RFC 5289 に定義される TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_192_CBC_SHA256
- RFC 5289 で定義された TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

]。

適用上の注釈 115

評価される構成においてテストされるべき暗号スイートは、本要件により制限されている。ST 作成者は、サポートされるオプションの暗号スイートを選択すべきである(should)。テスト環境におけるサーバ上で評価される構成で管理者に使用されることが可能な暗号スイートを制限する必要がある。上記 Suite B アルゴリズム (RFC 6460) は、実装が望まれるアルゴリズムである。TLS_RSA_WITH_AES_128_CBC_SHA は、RFC 5246 への適合を保証するために必須となっている。

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

本 cPP の将来のバージョンにおいて、すべての TOE に対して TLS v1.2 が要求される。

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

適用上の注釈 116

すべての SSL バージョン及び TLS v1.0 は拒否される。FCS_TLSS_EXT.2.1 で選択されないあらゆる TLS バージョンがここで選択されるべきである(should)。(「なし」がこのエレメントの選択である場合、ST 作成者は、「及びなし」という言葉を省略してもよい。)

FCS_TLSS_EXT.2.3 TSF は、[選択：鍵長 [選択：2048 ビット、3072 ビット、4096 ビット] を用いて RSA 鍵確立を実行 ； NIST 曲線 [選択：secp256r1, secp384r1、secp521r1] 及びそ

の他の曲線なしを介して EC Diffie-Hellman パラメタを生成 ； パラメタ長 2048 ビット及び [選択：3072 ビット、その他のパラメタ長なし] の Diffie-Hellman パラメタを生成]] を行わなければならない(shall)。

適用上の注釈 117

ST にて、FCS_TLSS_EXT.2.1 の DHE または ECDHE 暗号スイートが列挙される場合、ST には、本要件の Diffie-Hellman または NIST 曲線の選択を含まなければならない(must)。FMT_SMF.1 は、TLS 接続のセキュリティ強度を確立するための鍵共有パラメタの設定を要求する。

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

FCS_TLSS_EXT.2.5 TSF は、クライアント証明書が無効である場合、高信頼チャネルを確立してはならない(shall not)。クライアント証明書が無効であると思われる場合、TSF は[選択 : 接続を確立してはならない(shall not)、接続を確立するための許可を要求しなければならない(shall)、*[割付：その他のアクションを行わなければならない(shall)]*]。

適用上の注釈 118

TLS 用の X.509v3 証明書の利用は、FIA_X509_EXT.2.1 において対処される。本要件は、本用途が TLS 相互認証用のクライアント側証明書のサポートを含まなければならない(must)ことを追加する。

TLS が FTP_TRP または FTP_ITC 用に選択される場合、有効性は、RFC 5280 に従って、証明書パス、有効期限、及び失効状態によって決定される。証明書の有効性は、FIA_X509_EXT.1/Rev 用に実行されるテストに従って、テストされなければならない(shall)。TLS が FPT_ITT 用に選択される場合、証明書の有効性は、FIA_X509_EXT.1/ITT 用に実行されるテストに従ってテストされる。

FCS_TLSS_EXT.2.6 TSF は、証明書に含まれる Distinguished Name (DN) または Subject Alternative Name (SAN) がクライアント用に期待される識別子と一致しない場合、高信頼チャネルを確立してはならない(shall not)。

適用上の注釈 119

クライアントの識別子は、証明書の Subject フィールドまたは Subject Alternative Name extension にあるかもしれない。期待される識別子は、設定されてもよいし、またはクライアントによって使用される Domain Name、IP アドレス、利用者名、または電子メールアドレスと比較されてもよいし、または比較のためディレクトリサーバへ渡されたりしてもよい。

B.3 識別と認証 (FIA)

B.3.1 X.509 証明書を用いた認証 (拡張—FIA_X509_EXT)

IPsec または TLS 通信が FPT_ITT、FTP_ITC.1 または FTP_TRP について主張される場合、X.509 証明書ベースの認証が要求される。FPT_TUD.EXT.2 または FPT_TST_EXT.2 が主張される場合も、これらの SFR が要求される。SSH クライアント通信が主張され、かつ任意の

x509 アルゴリズムが FCS_SSHC_EXT.1.5 または FCS_SSHS_EXT.1.5 で主張される場合、これらの SFR が要求される。TOE が SSH サーバとしてのみ動作するか、またはクライアントとしてのみ動作するかの場合であるが、FCS_SSHC_EXT.1.5 または FCS_SSHS_EXT.1.5 において x509 アルゴリズムを主張していない場合、これらの SFR はオプションである。

B.3.1.1 FIA_X509_EXT.1 X.509 証明書有効性確認

FIA_X509_EXT.1/Rev	**X.509 証明書有効性確認**

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

- RFC 5280 証明書有効性確認及び証明書パス検証で、3 つの証明書の最小パス(経路)長をサポートする。
- 証明書パスは、信頼された CA 証明書で終端しなければならない(must)。
- TSF は、すべての CA 証明書について、basicConstraints 拡張の存在と CA フラグが TRUE にセットされていることを保証することによって、証明書パスを検証しなければならない(shall)。
- TSF は、[選択：RFC 6960 で規定されたオンライン証明書状態プロトコル (OCSP)、RFC 5280 セクション 6.3 で規定された証明書失効リスト (CRL)、RFC 5759 セクション 5 で規定された証明書失効リスト (CRL)] を用いて証明書の失効状態を検証しなければならない(shall)。
- TSF は、以下の規則に従って、extendedKeyUsage フィールドを検証しなければならない(shall)：
  - *高信頼アップデート及び実行可能コードの完全性検証用の証明書は、extendedKeyUsage フィールドにコード署名目的 (OID 1.3.6.1.5.5.7.3.3 を持つ id-kp 3) を持たなければならない(shall)。*
  - *TLS 用のサーバ証明書は、extendedKeyUsage フィールドにサーバ認証目的 (OID 1.3.6.1.5.5.7.3.1 を持つ id-kp 1) を持たなければならない(shall)。*
  - *TLS 用のクライアント証明書は、extendedKeyUsage フィールドにクライアント認証目的 (OID 1.3.6.1.5.5.7.3.2 を持つ id-kp 2)を持たなければならない(shall)。*
  - *OCSP 応答のため提示された OCSP 証明書は、extendedKeyUsage フィールドに OCSP 署名目的 (OID 1.3.6.1.5.5.7.3.9 を持つ id-kp 9) を持たなければならない (shall)。*

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

適用上の注釈 120

FIA_X509_EXT.1.1/Rev には、証明書の有効性確認を行うための規則が列挙される。ST 作成者は、失効状態が OCSP か CRL かのどちらを用いて検証されるかを選択する。高信頼チャネル／パスのプロトコルは、証明書が利用されることを要求することができる；この利用は、

extendedKeyUsage 規則が検証されることを要求する。TOE が FIA_X509_EXT.1.1 の extendedKeyUsage 規則に列挙される証明書種別のいずれかを利用する機能をサポートしない場合、これは TSS で記述され、かる本 SFR の関連部分が自明に満たされると見なされる。しかし、TOE がこれらの種別のいずれかの証明書を利用する機能をサポートする場合、対応する規則は本 SFR 内のものとして満たされなければならない(must)。

TOE は、3 つの証明書の最小パス(経路)長をサポートできなければならない(shall)。即ち、それは、少なくとも自己署名ルート証明書、下位の CA 証明書及び TOE アイデンティティ証明書から成る階層をサポートしなければならない(shall)。

有効性確認では、プラットフォームによって管理されるルートストア内の信頼されたルート CA 証明書で終端することが期待される。

TSS には、失効チェックがいつ実行されるかについて記述されなければならない(shall)。失効チェックが、証明書が認証ステップで使用されるとき、及び高信頼アップデートを実行するとき (選択された場合) に実行されることが期待される。X.509 証明書の状態がデバイスにロードされるときのみに検証されるだけでは不十分である。

電源投入時の自己テスト中に X.509 証明書の失効状態の検証をする必要は必ずしもない(自己テスト用に X.509 証明書を用いるオプションが選択された場合)。

FIA_X509_EXT.1.2/Rev は、TSF によって利用され、処理される証明書に適用され、信頼された CA 証明書として追加されてもよいような証明書を制限する。

ST 作成者は、SSH のみが FTP_ITC.1 または FPT_ITT.1 内で選択され、かつ ssh-rsa 認証も選択されるときのみ以外のすべてのインスタンスに FIA_X509_EXT.1/Rev を含まなければならない(must)。さらに、FIA_X509_EXT.1/Rev は、FPT_TUD_EXT または FPT_TST_EXT のいずれかが X509 証明書を利用するために選択した場合にも含まれなければならない(must)。

B.3.1.2 FIA_X509_EXT.2 X.509 証明書認証

FIA_X509_EXT.2	**X.509 証明書認証**

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

FIA_X509_EXT.2.2 TSF が証明書の有効性を決定するための接続を確立できないとき、TSF は、[選択：このような場合に証明書を受け入れるかどうかの選択を管理者に許可する、証明書を受け入れる、証明書を受け入れしない] ようにしなければならない(shall)。

適用上の注釈 121

FIA_X509_EXT.2.1 において、これらのプロトコルが FTP_ITC.1.1 または FPT_ITT.1 に含まれる場合、ST 作成者の選択には、IPsec、TLS、または HTTPS が含まれる。ssh-rsa、ecdsa-sha2-nistp256 、 ecdsa-sha2-nistp384 、 及び／または ecdsa-sha2-nistp521 以外の認証が FCS_SSHC_EXT.1.5 または FCS_SSHS_EXT.1.5 で選択される場合に、SSH が含まれるべきである(should)。証明書は、システムソフトウェアの高信頼アップデート (FPT_TUD_EXT.2) 及び完全性検証 (FPT_TST_EXT.2)用にオプションとして使用されてもよい。

CRL をダウンロードするか、OCSP を用いてルックアップを実行するかのいずれかで一証明

書の失効状態をチェックするために、しばしばコネクションが確立されなければならない(must)。コネクションが確立できないような事象におけるふるまいについて記述するため、FIA_X509_EXT.2 において選択が使用される(例えば、ネットワークエラーのため)。TOE が FIA_X509_EXT.1 のその他すべての規則に従って証明書が有効であると決定した場合、選択で示されるふるまいが有効性を決定する。TOE は、FIA_X509_EXT.1 でのその他の有効性確認の規則のいずれにも失敗する場合、証明書を受け入れてはならない(must not)。管理者設定されるオプションが ST 作成者によって選択される場合、ST 作成者は、FMT_SMF.1 における対応する機能についても選択する。その選択は、FCS_IPSEC_EXT.1.14、FCS_TLSC_EXT.1.3 及びFCS_TLSC_EXT.2.3 の有効性確認要件と一貫しているべきである(should)。

TOE が分散型であり、FIA_X509_EXT.1/ITT が選択される場合、証明書失効チェックはオプションである。これは、FCO_CPC_EXT.1 で定義されるような、TOE 内高信頼チャネルの有効化と無効化で実行される追加の許可アクションがあるためである。この場合、接続は証明書の有効性を決定するために要求されず、本 SFR は自明に満たされる。

ST 作成者は、SSH のみが FTP_ITC.1 または FPT_ITT.1 内で選択され、かつ ssh-rsa、ecdsa-sha2-nistp256、ecdsa-sha2-nistp384、及び／または ecdsa-sha2-nistp521 認証も選択されるとき以外のすべてのインスタンスで FIA_X509_EXT.2 を含まなければならない(must)。さらに、FIA_X509_EXT.2 は、FPT_TUD_EXT または FPT_TST_EXT のいずれかが X509 証明書を選択した場合にも含まれなければならない(must)。

B.3.1.3 FIA_X509_EXT.3 X.509 証明書要求

FIA_X509_EXT.3	X.509 証明書要求

FIA_X509_EXT. 3.1 TSF は、RFC 2986 によって規定される証明書要求メッセージを生成し、その要求で以下の情報を提供できなければならない(shall)：公開鍵及び [選択：デバイス固有情報、Common Name、Organization、Organizational Unit、Country]。

適用上の注釈 122

公開鍵は、FCS_CKM.1 で規定されるとおり、TOE によって生成される公開鍵―プライベート鍵ペアの公開鍵部分である。

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

B.4 TSF の保護 (FPT)

B.4.1 TSF 自己テスト (拡張)

B.4.1.1 FPT_TST_EXT.2 証明書に基づく自己テスト

FPT_TST_EXT.2	証明書に基づく自己テスト

FPT_TST_EXT.2.1 TSF は、証明書が自己テスト用に利用され、かつ対応する証明書が無

効と見なされる場合、自己テストを失敗させなければならない(shall)。

適用上の注釈 123

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

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

B.4.2 高信頼アップデート (FPT_TUD_EXT)

B.4.2.1 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート

FPT_TUD_EXT.2	証明書ベースの高信頼アップデート

FPT_TUD_EXT.2.1 TSF は、コード署名証明書が無効とみなされる場合、アップデートをインストールしてはならない(shall not)。

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

適用上の注釈 124

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

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

B.5 セキュリティ管理 (FMT)

B.5.1 TSF における機能の管理 (FMT_MOF)

B.5.1.1 FMT_MOF.1/AutoUpdate セキュリティ機能のふるまいの管理

FMT_MOF.1/AutoUpdate	セキュリティ機能のふるまいの管理

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

ならない(shall)。

適用上の注釈 125

FMT_MOF.1/AutoUpdate は、TOE がアップデートの自動チェック及び／または自動アップデートをサポートし、それらが有効化及び無効化されることを許可する場合にのみ適用される。アップデートの自動チェック及び／または自動アップデートの有効化及び無効化は、セキュリティ管理者に制限される。選択肢「自動アップデート」は、高信頼アップデートの有効性を検証するためにディジタル署名が使用される場合にのみ選択できる。

B.5.1.2 FMT_MOF.1/Functions セキュリティ機能のふるまいの管理

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

FMT_MOF.1.1/Functions TSF は、機能 [選択：監査データの外部 IT エンティティへの送信、監査データの取扱、ローカル監査ストレージ領域が満杯であるときの監査機能] の [選択：ふるまいを決定、ふるまいを改変] する能力を、セキュリティ管理者に制限しなければならない(shall)。

適用上の注釈 126

FMT_MOF.1/Functions は、以下のシナリオの 1 つ以上が適用される場合に選ばれるべきである：

- *監査データの外部 IT エンティティへの送信のための送信プロトコルが FAU_STG_EXT.1.1 で定義されるとおり設定可能である場合、「監査データの外部 IT エンティティへの送信」が選択されなければならない(shall)。*
- *監査データの取扱が設定可能である場合、「監査データの取扱」が選ばれなければならない(shall)。用語「監査データの取扱」は、SFR FAU_STG_EXT.1.2、FAU_STG_EXT.1.3 及び FAU_STG_EXT.2/LocSpace における選択と割付のための異なるオプションを指す。*
- *ローカル監査ストレージ領域が満杯であるときの監査機能のふるまいが設定可能な場合、「ローカル監査ストレージ領域が満杯であるときの監査機能」が選ばれなければならない(shall)。*

「ふるまいを決定」及び「ふるまいを改変」のための 2 番目の選択 (訳注：原文では 1 番目の選択である) は、適切に行われるべきである(should)。1 番目の選択に応じて 2 番目の選択について異なる選択を行うことが必要である (例、「監査データの取扱」は、2 番目の選択で「ふるまいを決定」と「ふるまいを改変」を要求する一方、「TOE セキュリティ機能」は「ふるまいの改変」のみを要求する)。その場合、FMT_MOF.1/Functions は、追加する数を増やしつつ繰り返しするべきである(should) (即ち、FMT_MOF.1/Functions1、FMT_MOF.1/Functions2、等)。

C. 拡張コンポーネントの定義

本附属書には、附属書 A 及び B で使用されるものを含め、本 cPP で利用される拡張要件の定義が含まれる。

(注釈：本附属書における選択と割付の様式表記法は、[CC2]にあるものである。)

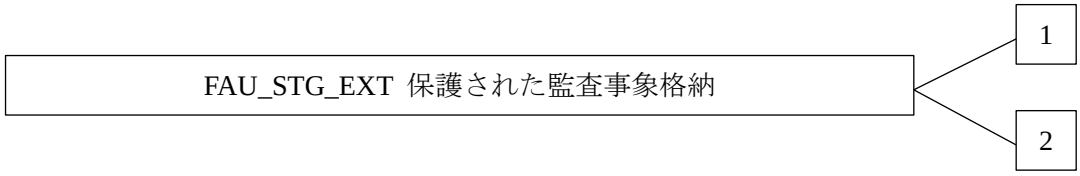
C.1 セキュリティ監査 (FAU)

C.1.1 保護された監査事象格納 (FAU_STG_EXT)

ファミリのふるまい

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

コンポーネントのレベル付け



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

FAU_STG_EXT.2 消失した監査データの集計は、監査ログが満杯になった際に影響を受ける監査記録に関する情報を提供することを TSF に要求する。

管理：FAU_STG_EXT.1, FAU_STG_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) TSF は、暗号機能を設定する能力を持たなければならない。

監査：FAU_STG_EXT.1, FAU_STG_EXT.2

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

a) 監査の必要なし。

C.1.1.1 FAU_ STG_EXT.1 保護された監査事象格納

FAU_STG_EXT.1	保護された監査事象格納

下位階層： なし

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

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

適用上の注釈 127

生成された監査データを外部 IT エンティティへ送信するオプションの選択について、TOE は監査記録の格納とレビューに関して非 TOE 監査サーバに依存している。これらの監査記録の格納、及びこれらの監査記録のレビューを管理者に許可する能力は、その場合の運用環境により提供される。外部監査サーバが TOE の一部でないため、監査データの ITC 配送の機能以外一切の要件はない。監査データが転送されるフォーマットまたは基礎となるプロトコルについて、一切の要件はない。TOE は管理者の介在なしに外部 IT エンティティへ監査データを転送するように構成可能でなければならない(must)。手動転送は、本要件を満たさない。送信は、リアルタイムに、または定期的に行われること。送信がリアルタイムに行われない場合、TSS には、どの事象が転送を行わせるように刺激するか、及び監査データの監査サーバへの転送を行うために TOE がサポートする頻度の範囲について、記述されること；TSS には、通常受け入れ可能な転送の頻度についても示すこと。

分散型 TOE については、それぞれのコンポーネントは、保護された外部のチャネル(FTP_ITC.1)またはコンポーネント間(FPT_ITT.1 または FTP_ITC.1)を介して監査データを適切に送出できなければならない(must)。少なくとも TOE の 1 つのコンポーネントがすべての TOE 監査記録が外部 IT エンティティへ送出できるように、FTP_ITC.1 経由で監査記録を送出できなければならない(must)。

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

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

適用上の注釈 128

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

分散型 TOE について、それぞれのコンポーネントは、ネットワーク接続性問題の場合に監査記録が保存されることを保証するために一定の容量のローカルの格納領域を提供しなければならない。ローカルの格納領域が満杯であるときのふるまいは、それぞれのコンポーネントについて記述されなければならない(must)。

C.1.1.2 FAU_ STG_EXT.2 消失した監査データの集計

FAU_STG_EXT.2	消失した監査データの集計

下位階層： なし

依存性： FAU_GEN.1 監査データ生成
FAU_STG_EXT.1 ~~外部監査証跡格納~~ (訳注：保護された監査事象格納)

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

適用上の注釈 129

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

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

分散型 TOE については、喪失した監査データの集計を実装するようなそれぞれのコンポーネントは、管理者によるこの情報へのアクセス及び管理のためのメカニズムを提供しなければならない(has to)。

FAU_STG_EXT.2 が ST に追加される場合、ST には、喪失した監査データが集計されるような状況について明確化されなければならない(has to)。

C.2 暗号サポート (FCS)

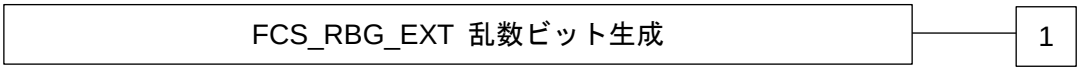
C.2.1 乱数ビット生成 (FCS_RBG_EXT)

C.2.1.1 FCS_RBG_EXT.1 乱数ビット生成

ファミリのふるまい

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

コンポーネントのレベル付け



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

管理：FCS_RBG_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない

監査：FCS_RBG_EXT.1

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

a) 最小：攪拌処理の失敗

FCS_RBG_EXT.1	**乱数ビット生成**

下位階層： なし

依存性： なし

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

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

適用上の注釈 130

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

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

C.2.2 暗号プロトコル (拡張—FCS_DTLSC_EXT, FCS_DTLSS_EXT, FCS_HTTPS_EXT, FCS_ IPSEC_EXT, FCS_SSHC_EXT, FCS_SSHS_EXT,

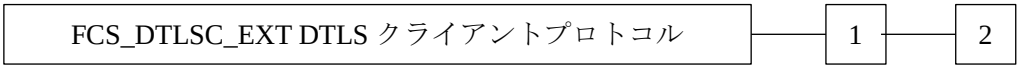
FCS_TLSC_EXT, FCS_TLSS_EXT)

C.2.2.1 FCS_DTLSC_EXT DTLSC クライアントプロトコル

ファミリのふるまい

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

コンポーネントのレベル付け



FCS_DTLSC_EXT.1 DTLS クライアントは、DTLS のクライアント側が規定されるとおりに実装されることを要求する。

FCS_DTLSC_EXT.2 DTLS クライアントは、DTLS 実装のクライアント側が相互認証を含むことを要求する。

管理：FCS_DTLSC_EXT.1, FCS_DTLSC_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_ DTLSC_EXT.1, FCS_DTLSC_EXT.2

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

a) DTLS セション確立の失敗
b) DTLS セション確立
c) DTLS セション終了

FCS_DTLSC_EXT.1	**DTLS クライアントプロトコル**

下位階層： なし

依存性： FCS_CKM.1DataEncryption1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作(AES データ暗号化／復号)
FCS_COP.1/SigGen1 暗号操作(署名生成と検証)
FCS_COP.1/Hash 暗号操作(ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作(鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

FCS_DTLSC_EXT.1.1 TSF は、以下の暗号スイートをサポートする[選択：DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall)：

- [割付：オプションの暗号スイートとそれぞれ定義される RFC への参照のリスト]

適用上の注釈 131

評価される構成でテストされるべき暗号スイートは、本要件によって限定される。ST 作成者は、サポートされる暗号スイートを選択するべきである(should)。テスト環境におけるサーバ上で評価される構成において管理的に利用可能な暗号スイートを限定する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、RFC6347 への適合を主張する場合には要求される。

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべての TOE に対して DTLS v1.2 が要求される。

FCS_DTLSC_EXT.1.2 TSF は、TSF は、RFC 6125 セクション 6 に従って、提示される識別子が参照識別子と一致することを検証しなければならない(shall)。

適用上の注釈 132

アイデンティティ検証の規則は、RFC 6125 のセクション 6 で記述される。参照識別子は、アプリケーションサービスによって、管理者により(例、ウェブサーバへ URL を入力またはリンクをクリック)、設定により(例、メールサーバまたは認証サーバの名称を設定)、またはアプリケーションにより(例、API のパラメタ)確立される。単一の参照識別子のソースドメインとアプリケーションサービス種別(例、HTTP、SIP、LDAP)に基づいて、クライアントは、証明書の Subject Name フィールドの Common Name 及び Subject Alternative Name フィールドの (機微でない場合) DNS 名、URI 名、及び Service Name のような、受け入れ可能なすべての参照識別子を確立する。次に、クライアントは、すべての受け入れ可能な参照識別子のこのリストを DTLS サーバ証明書における提示された識別子と比較する。

FCS_DTLSC_EXT.1.3 TSF は、サーバ証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効であると思われる場合、TSF は、[選択 : *接続を確立しない、接続を確立するための許可を要求、[割付 : その他のアクション]*]しなければならない(shall)。

適用上の注釈 133

DTLS が FTP_ITC で選択される場合、有効性は、RFC 5280 に従って、識別子検証、証明書パス、有効期限、及び失効状態によって決定される。証明書有効性は、FIA_X509_EXT.1/Rev で実行されるテストに従ってテストされる。DTLS が FPT_ITT で選択される場合、証明書有効性は、FIA_X509_EXT.1/ITT で実行されるテストに従ってテストされる。

FCS_DTLSC_EXT.1.4 TSF は、Client Hello において、[選択 : *Supported Elliptic Curves Extension を提示しない、以下の NIST 曲線と共に Supported Elliptic Curves Extension を提示する : [選択 : secp256r1、secp384r1、secp521r1] 及びその他の曲線なし*] ようにしなければならない(shall)。

適用上の注釈 134

楕円曲線を用いた暗号スイートが FCS_DTLSC_EXT.1.1 で選択された場合、1 つまたはそれ以上の曲線の選択が要求される。楕円曲線を用いる暗号スイートが FCS_DTLSC_EXT.1.1 で選択されなかった場合、「Supported Elliptic Curves Extension を提示しない」が選択されるべきである。

本要件は、認証及び鍵共有のために許可される楕円曲線を FCS_COP.1/SigGen 及び

FCS_CKM.1 及びFCS_CKM.2 からのNIST 曲線に限定する。本拡張は、楕円曲線暗号シートをサポートしているクライアントに対して要求される。

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

下位階層： FCS_DTLSC_EXT.1 DTLS クライアントプロトコル

依存性： FCS_CKM.1/DataEncryption1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作(AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作(署名生成と検証)
FCS_COP.1/Hash 暗号操作(ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作(鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

FCS_DTLSC_EXT.2.1 TSF は、以下の暗号スイートをサポートする[選択：DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall)：

- [割付:オプションの暗号スイートとそれぞれ定義される RFC への参照のリスト]。

適用上の注釈 135

ST 作成者は、サポートされる暗号スイートを選択するべきである。テスト環境におけるサーバ上で管理上評価される構成において利用可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；RFC6347 への適合を主張する場合に要求される。

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべてのTOE に対してDTLS v1.2 が要求される。

FCS_DTLSC_EXT.2.2 TSF は、RFC 6125 セクション 6 に従って、提示される識別子が参照識別子と一致することを検証しなければならない(shall)。

適用上の注釈 136

アイデンティティ検証の規則は、RFC 6125 のセクション6 で記述される。参照識別子は、アプリケーションサービスによって、管理者により(例、ウェブサーバへ URL を入力またはリンクをクリック)、設定により(例、メールサーバまたは認証サーバの名称を設定)、またはアプリケーションにより(例、API のパラメタ)確立される。単一の参照識別子のソースドメインとアプリケーションサービス種別(例、HTTP、SIP、LDAP)に基づいて、クライアントは、証明書の Subject Name フィールドの Common Name 及び Subject Alternative Name フィールドの (機微でない場合) DNS 名、URI 名、及びService Name のような、受け入れ可能なすべての参照識別子を確立する。次に、クライアントは、すべての受け入れ可能な参照識別子のこのリストをDTLS サーバ証明書における提示された識別子と比較する。

FCS_DTLSC_EXT.2.3 TSF は、サーバ証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効であると思われる場合、TSF は、[選択：*接続を確立しない、接続を確立するための許可を要求、[割付：その他のアクション]*]しなければならない(shall)。

適用上の注釈 137

DTLS が FTP_ITC で選択される場合、有効性は、RFC 5280 に従って、識別子検証、証明書パス、有効期限、及び失効状態によって決定される。証明書有効性は、FIA_X509_EXT.1/Rev で実行されるテストに従ってテストされる。DTLS が FPT_ITT で選択される場合、証明書有効性は、FIA_X509_EXT.1/ITT で実行されるテストに従ってテストされる。

FCS_DTLSC_EXT.2.4 TSF は、Client Hello において、[選択：*Supported Elliptic Curves Extension を提示しない、以下の NIST 曲線と共に Supported Elliptic Curves Extension を提示する：[選択：secp256r1、secp384r1、secp521r1] 及びその他の曲線なし*] ようにしなければならない(shall)。

適用上の注釈 138

楕円曲線を用いた暗号スイートが FCS_DTLSC_EXT.2.1 で選択された場合、1 つまたはそれ以上の曲線の選択が要求される。楕円曲線を用いる暗号スイートが FCS_DTLSC_EXT.2.1 で選択されなかった場合、「Supported Elliptic Curves Extension を提示しない」が選択されるべきである。

本要件は、認証及び鍵共有のために許可される楕円曲線を FCS_COP.1/SigGen 及び FCS_CKM.1 及び FCS_CKM.2 からの NIST 曲線に限定する。本拡張は、楕円曲線暗号シートをサポートしているクライアントに対して要求される。

FCS_DTLSC_EXT.2.5 TSF は、X.509v3 証明書を用いて相互認証をサポートしなければなければならない(shall)。

適用上の注釈 139

TLS 用の X.509v3 証明書の利用は、FIA_X509_EXT.2.1 で対処される。本要件は、クライアントが DTLS 相互認証のため DTLS サーバへ証明書を提示できなければならないことを追加する。

FCS_DTLSC_EXT.2.6 TSF は、受信したメッセージが無効な MAC を含む場合、[選択：*DTLS セションを終了、レコードを静かに破棄*] しなければならない(shall)。

適用上の注釈 140

メッセージ認証コード（MAC）は、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関するである。MAC は DTLS ハンドシェイクフェーズ中にネゴシエーションされ、DTLS データ交換中に送信者から受信されるメッセージの完全性を保護するために利用される。MAC 検証が失敗する場合、セションは終了されなければならない(must)、またはレコードは静かに破棄されなければならない(must)。

FCS_DTLSC_EXT.2.7 TSF は、以下についてのリプレイされたメッセージを検出し、静かに破棄しなければならない(shall)：

- 以前受信した DTLS レコード。
- スライド窓にフィットするには古すぎる DTLS レコード。

適用上の注釈 141

リプレイ検出は、DTLS 1.2 (RFC 6347) のセクション 4.1.2.6 及び DTLS 1.0 (RFC 4347) のセクション 4.1.2.5 で記述される。それぞれの受信されたレコードについて、受信者は、その

レコードがスライディング受信ウィンドウの範囲内にあり、セション中に受信されたその他のレコードのシーケンス番号を重複しないようなシーケンス番号を含むことを検証する。

「静かに破棄」は、TOE が応答することなしにパケットを破棄することを意味する。

C.2.2.2 FCS_DTLSS_EXT DTLS サーバプロトコル

ファミリのふるまい

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

コンポーネントのレベル付け

FCS_DTLSC_EXT.1　DTLS サーバは、DTLS のサーバ側が規定されるとおりに実装されることを要求する。

FCS_DTLSC_EXT.2　DTLS サーバは、相互認証が DTLS 実装に含まれることを要求する。

管理：FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

b) 予見される管理アクティビティはない。

監査：FCS_ DTLSS_EXT.1, FCS_DTLSS_EXT.2

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

d) DTLS セション確立の失敗
e) DTLS セション確立
f) DTLS セション終了

FCS_DTLSS_EXT.1	**DTLS サーバプロトコル**

下位階層：　なし

依存性：　FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1//DataEncryption 暗号操作(AES データ暗号化／復号)
FCS_COP.1//SigGen 暗号操作(署名生成と検証)
FCS_COP.1/Hash 暗号操作(ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作(鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

FCS_DTLSS_EXT.1.1　TSF は、以下の暗号スイートをサポートする[選択：DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall)：

- [割付：オプションの暗号スイートとそれぞれ定義される RFC への参照のリスト]

評価される構成でテストされるべき暗号スイートは、本要件によって限定される。ST 作成者は、サポートされる暗号スイートを選択するべきである(should)。テスト環境におけるサーバ上で評価される構成において管理的に利用可能な暗号スイートを限定する必要がある。*TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、RFC6347 への適合を主張する場合には要求される。*

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべての TOE に対して DTLS v1.2 が要求される。

FCS_DTLSS_EXT.1.2 TSF は、[割付：*プロトコルバージョンのリスト*]を要求するクライアントからの接続を拒否しなければならない(shall)。

適用上の注釈 142

本 cPP の本バージョンは、DTLS v1.0 を TOE が拒否することを要求しない。本 cPP の将来のバージョンでは、DTLS v1.0 はすべての TOE に対して供されることを要求されるだろう。

FCS_DTLSS_EXT.1.3 TSF は、DTLS クライアントが検証を失敗する場合、接続ハンドシェイク試行を進めてはならない(shall not)。

適用上の注釈 143

DTLS クライアントを検証するプロセスは、RFC 6347（DTLS 1.2）のセクション 4.2.1 及び RFC 4347 （DTLS 1.0）で規定される。TOE は、接続確立 (ハンドシェイク) 中に、かつ Server Hello メッセージを TSF が送信する前に、DTLS クライアントを検証する。ClientHello を受信後に、DTLS サーバは、HelloVerifyRequest をクッキーと共に送信する。クッキーは、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関数を用いた署名メッセージである。DTLS クライアントは、次に別の ClientHello にクッキーを添付して送信する。DTLS サーバが署名されたクッキーの検証に成功する場合、クライアントは、なりすましされた IP アドレスを用いていない。

FCS_DTLSS_EXT.1.4 TSF は、 [選択：*鍵長[選択 2048 ビット、3072 ビット、4096 ビット]を用いて RSA 鍵確立を実行；NIST 曲線[選択：secp256r1、secp384r1、secp521r1]及びその他の曲線なしを介した EC Diffie-Hellman パラメタを生成；[選択：2048 ビット、3072 ビット]長の Diffie-Hellman パラメタを生成*] しなければならない(shall)。

適用上の注釈 144

ST に FCS_DTLSS_EXT.1.1 における DHE または ECDHE 暗号スイートを列挙する場合、ST には、本要件の Diffie-Hellman または NIST 曲線の選択を含まなければならない(must)。FMT_SMF.1 は、DTLS 接続のセキュリティ強度を確立するため、鍵共有パラメタの設定を要求する。

FCS_DTLSS_EXT.1.5 TSF は、受信したメッセージに無効な MAC が含まれる場合、 [選択：*DTLS セションを終了、レコードを静かに破棄*] しなければならない(shall)。

適用上の注釈 145

メッセージ認証コード（MAC）は、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関数

である。MAC はDTLS ハンドシェイクフェーズ中にネゴシエーションされ、DTLS データ交換中に送信者から受信されるメッセージの完全性を保護するために利用される。MAC 検証が失敗する場合、セションは終了されなければならない(must)、またはレコードは静かに破棄されなければならない(must)。

FCS_DTLSS_EXT.1.6 TSF は、以下についてのリプレイされたメッセージを検出し、静かに破棄しなければならない(shall)：

- 以前受信した DTLS レコード。
- スライド窓にフィットするには古すぎる DTLS レコード。

適用上の注釈 146

リプレイ検出は、DTLS 1.2 (RFC 6347) のセクション 4.1.2.6 及びDTLS 1.0 (RFC 4347) のセクション 4.1.2.5 で記述される。それぞれの受信されたレコードについて、受信者は、そのレコードがスライディング受信ウィンドウの範囲内にあり、セション中に受信されたその他のレコードのシーケンス番号を重複しないようなシーケンス番号を含むことを検証する。

「静かに破棄」は、TOE が応答することなしにパケットを破棄することを意味する。

FCS_DTLSS_EXT.2	**認証を伴う DTLS サーバプロトコル**

下位階層： FCS_DTLSS_EXT.1 DTLS サーバプロトコル

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1//DataEncryption 暗号操作(AES データ暗号化／復号)
FCS_COP.1//SigGen 暗号操作(署名生成と検証)
FCS_COP.1/Hash 暗号操作(ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作(鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

FCS_DTLSS_EXT.2.1 TSF は、以下の暗号スイートをサポートする[選択：DTLS 1.2 (RFC 6347)、DTLS 1.0 (RFC 4347)] を実装しなければならない(shall)：

- [割付：オプションの暗号スイートとそれぞれ定義される RFC への参照のリスト]

適用上の注釈 147

評価された構成においてテストされるべき暗号スイートは、本要件によって限定される。ST 作成者は、サポートされる暗号スイートを選択するべきである。テスト環境におけるサーバ上で管理上評価される構成において利用可能な暗号スイートを制限する必要がある。TLS_RSA_WITH_AES_128_CBC_SHA は、ND cPP v2.0 適合のために必須ではない；しかし、RFC6347 への適合を主張する場合に要求される。

これらの要件は、IETF によって新しいバージョンの DTLS が標準化されると、改訂される予定である。

本 cPP の将来のバージョンにおいて、すべての TOE に対してDTLS v1.2 が要求される。

FCS_DTLSS_EXT.2.2 TSF は、[割付：*プロトコルバージョンのリスト*]を要求するクライ

アントからの接続を拒否しなければならない(shall)。

適用上の注釈 148

本 cPP の本バージョンは、DTLS v1.0 を TOE が拒否することを要求しない。本 cPP の将来のバージョンでは、DTLS v1.0 はすべての TOE に対して供されることを要求されるだろう。

FCS_DTLSS_EXT.2.3 TSF は、DTLS クライアントが検証を失敗する場合、接続ハンドシェイク試行を進めてはならない(shall not)。

適用上の注釈 149

DTLS クライアントを検証するプロセスは、RFC 6347 (DTLS 1.2) のセクション 4.2.1 及び RFC 4347 (DTLS 1.0) で規定される。TOE は、接続確立 (ハンドシェイク) 中に、かつ Server Hello メッセージを TSF が送信する前に、DTLS クライアントを検証する。ClientHello を受信後に、DTLS サーバは、HelloVerifyRequest をクッキーと共に送信する。クッキーは、FCS_COP.1/KeyedHash で規定される鍵付きハッシュ関数を用いた署名メッセージである。DTLS クライアントは、次に別の ClientHello にクッキーを添付して送信する。DTLS サーバが署名されたクッキーの検証に成功する場合、クライアントは、なりすましされた IP アドレスを用いていない。

FCS_DTLSS_EXT.2.4 TSF は、 [選択：*鍵長[選択 2048 ビット、3072 ビット、4096 ビット]を用いて RSA 鍵確立を実行；NIST 曲線[選択：secp256r1、secp384r1、secp521r1]及びその他の曲線なしを介した EC Diffie-Hellman パラメタを生成；[選択：2048 ビット、3072 ビット]長の Diffie-Hellman パラメタを生成*] しなければならない(shall)。

適用上の注釈 150

ST に FCS_DTLSS_EXT.1.1 における DHE または ECDHE 暗号スイートを列挙する場合、ST には、本要件の Diffie-Hellman または NIST 曲線の選択を含まなければならない(must)。FMT_SMF.1 は、DTLS 接続のセキュリティ強度を確立するため、鍵共有パラメタの構成を要求する。

FCS_DTLSS_EXT.2.5 TSF は、受信したメッセージに無効な MAC が含まれる場合、 [選択：*DTLS セションを終了、レコードを静かに破棄*] しなければならない(shall)。

適用上の注釈 151

メッセージ認証コード (MAC)は、DTLS ハンドシェイクフェーズ中にネゴシエーションされ、DTLS データ交換中に送信者から受信されるメッセージの完全性を保護するために利用される。MAC 検証が失敗する場合、セションは終了されなければならない(must)、またはレコードは静かに破棄されなければならない(must)。

FCS_DTLSS_EXT.2.6 TSF は、以下についてのリプレイされたメッセージを検出し、静かに破棄しなければならない(shall)：

- 以前受信した DTLS レコード。
- スライド窓にフィットするには古すぎる DTLS レコード。

適用上の注釈 152

リプレイ検出は、DTLS 1.2 (RFC 6347) のセクション 4.1.2.6 及び DTLS 1.0 (RFC 4347) のセクション 4.1.2.5 で記述される。それぞれの受信されたレコードについて、受信者は、その

レコードがスライディング受信ウィンドウの範囲内にあり、セション中に受信されたその他のレコードのシーケンス番号を重複しないようなシーケンス番号を含むことを検証する。

「静かに破棄」は、TOE が応答することなしにパケットを破棄することを意味する。

FCS_DTLSS_EXT.2.7 TSF は、X.509v3 証明書を用いて DTLS クライアントの相互認証をサポートしなければならない(shall)。

FCS_DTLSS_EXT.2.8 TSF は、クライアント証明書が無効である場合、高信頼チャネルを確立してはならない(shall not)。もし、クライアント証明書が無効と思われる場合、TSF は [選択 : *接続を確立しない*、*接続の確立するための許可を要求*、*[割付 : その他のアクション]*] ようにしなければならない(shall)。

適用上の注釈 153

DTLS 用の X.509v3 の利用は、FIA_X509_EXT.2.1 で対処される。本要件は、この利用に、DTLS 相互認証のクライアント側の証明書のサポートを含まなければならない(shall)。

DTLS が FTP_ITC で選択される場合、有効性は、RFC5280 に従って、識別子検証、証明書パス、有効期限、及び失効状態によって決定される。証明書有効性は、FIA_X509_EXT.1/Rev のために実行されるテストに従ってテストされる。DTLS は、FPT_ITT で選択される場合、証明書有効性は、FIA_X509_EXT.1/ITT のために実行されるテストに従ってテストされる。

FCS_DTLSS_EXT.2.9 TSF は、証明書に含まれる distinguished name(DN) または Subject Alternative Name (SAN) がクライアントの期待される識別子と合致しない場合、高信頼チャネルを確立してはならない(shall)。

適用上の注釈 154

クライアント識別子は、証明書の Subject フィールドまたは Subject Alternative extension にあるかもしれない。規定される識別子は、設定されるか、ピアによってドメイン名、IP アドレス、又は電子メールアドレスと比較されるか、または比較のためにディレクトリサーバへ渡されるかのいずれかであるかもしれない

C.2.2.3 FCS_HTTPS_EXT.1 HTTPS プロトコル

ファミリのふるまい

本ファミリのコンポーネントは、TOE とセキュリティ管理者との間のリモート管理者セションを保護するための要件を定義する。本ファミリは、どのように HTTPS が実装されるかを記述する。これは、FCS クラスに定義される新たなファミリである。

コンポーネントのレベル付け

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

管理：FCS_HTTPS_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_HTTPS_EXT.1

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

a) 予見される監査対象事象はない。

FCS_HTTPS_EXT.1	**HTTPS プロトコル**

下位階層： なし

依存性： [FCS_TLSC_EXT.1 TLS クライアントプロトコル、または
FCS_TLSS_EXT.1 TLS サーバプロトコル]

FCS_HTTPS_EXT.1.1 TSF は、RFC 2818 に適合する HTTPS プロトコルを実装しなければならない。

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

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

C.2.2.4 FCS_IPSEC_EXT.1 IPsec プロトコル

ファミリのふるまい

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

コンポーネントのレベル付け

FCS_IPSEC_EXT IPsec プロトコル	1

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

管理：FCS_IPSEC_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) SA ライフタイムの設定

監査：FCS_IPSEC_EXT.1

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

a) TOE によって処理されるネットワークパケットを廃棄 (DISCARD)、バイパス (BYPASS)、保護 (PROTECT) するための決定
b) IPsec SA の確立失敗
c) IPsec SA の確立
d) IPsec SA の終了
e) IKEv2 から IKEv1 交換への「ダウン」ネゴシエーション

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

下位階層： なし

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作 (AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作 (署名の検証)
FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作 (鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

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

適用上の注釈 155

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

されるという「規則」がある。

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

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

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

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

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

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

FCS_IPSEC_EXT.1.6 TSF は、[選択：*IKEv1*、*IKEv2*] プロトコルにおける暗号化されたペイロードが、暗号アルゴリズムとして[選択：*RFC 3602 に特定される AES-CBC-128*、*AES-CBC-256* 、*RFC 5282 に特定される AES-GCM-128*、*AES-GCM-256*、*その他のアルゴリズムなし*] を使用することを保証しなければならない。

適用上の注釈 156

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

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

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

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

[選択：
- *バイト数；*
- *ライフタイムの長さ、ここで時間の値は [割付：24 を含む整数範囲] 時間以内で設定可能*

]

]。

適用上の注釈 157

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

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

- *IKEv1 フェーズ 2 の SA ライフタイムがセキュリティ管理者によって、以下に基づいて設定可能であること*

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

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

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

  ]

]。

適用上の注釈 158

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

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

適用上の注釈 159

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

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

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

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

] 。

適用上の注釈 160

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

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

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

FCS_IPSEC_EXT.1.11 TSF は、すべての IKE プロトコルが DH グループ[選択：*14 (2048 ビット MODP)*、*19 (256 ビットランダム ECP)*、*5 (1536 ビット MODP)*、*24 (256 ビット POS 付*

の 2048 ビット MODP)、20 (384 ビットランダム ECP)、[割付 : TOE の実装するその他の DH グループ]、その他の DH グループなし] を実装していることを保証しなければならない。

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

適用上の注釈 161

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

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

FCS_IPSEC_EXT.1.14 TSF は、受信された証明書内で提示される識別子が設定された参照識別子と一致する場合、高信頼チャネルのみを確立しなければならない(shall)、ここで、提示された識別子と参照識別子は以下の種別とする : [選択 : *IP アドレス*、*Fully Qualified Domain Name(FQDN)*、*利用者 FQDN*、*Distinguished Name(DN)*]及び[選択 : *その他の参照識別子種別なし*、*[割付 : その他のサポートされる参照識別子種別]*]。

C.2.2.5 FCS_SSHC_EXT.1 SSH クライアント

ファミリのふるまい

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

コンポーネントのレベル付け

FCS_SSHC_EXT SSH クライアントプロトコル	1

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

管理 : FCS_SSHC_EXT.1

以下のアクションは、FMT における管理機能と考えられる :

a) 予見される管理アクティビティはない。

監査 : FCS_SSHC_EXT.1

FAU_GEN セキュリティ監査データ生成が PP/ST に含まれていれば、以下のアクションを

監査対象とするべきである：

a) SSH セションの確立失敗
b) SSH セションの確立
c) SSH セションの終了

FCS_SSHC_EXT.1	**SSH クライアントプロトコル**

下位階層： なし

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作 (AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作 (署名の生成／検証)
FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作 (鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

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

適用上の注釈 162

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

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

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

適用上の注釈 163

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

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

FCS_SSHC_EXT.1.5 TSF は、SSH 公開鍵ベースの認証実装がその公開鍵アルゴリズムとして [選択 : *ssh-rsa*、*ecdsa-sha2-nistp256*] 及び [選択 : *ecdsa-sha2-nistp384*、*ecdsa-sha2-nistp521*、

x509v3-ecdsa-sha2-nistp256、*x509v3-ecdsa-sha2-nistp384*、*x509v3-ecdsa-sha2-nistp521*、*その他の公開鍵アルゴリズムなし*] を使用し、他のすべての公開鍵アルゴリズムを拒否することを保証しなければならない(shall)。

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

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

FCS_SSHC_EXT.1.8 TSF は、SSH コネクション内で同じセション鍵が 1 時間以内、かつ 1 ギガバイト未満の送信データのしきい値で使用されることを保証しなければならない(shall)。いずれかのしきい値に達した後、鍵変更が実行される必要がある。

適用上の注釈 164

本 SFR は、2 つのしきい値を定義する－1 つは最大時間同じセション鍵が使用可能であり、他方はデータの最大容量まで同じセション鍵を用いて送信可能である。両方のしきい値が実装される必要があり、いずれかのしきい値に達すると鍵変更が実行される必要がある。最大送信データについて、受信及び送信データの合計が集計される必要がある。鍵変更は、送受信トラフィクについてのすべてのセション鍵 (暗号化、完全性保護) に提供される。

TOE が本 SFR で定義された最大値よりも低いしきい値を実装することは、受け入れ可能である。

本要件に関連する設定可能な、あらゆるしきい値について、ガイダンス証拠資料は、そのしきい値の可能な設定方法について規定する必要がある。許可された値がガイダンス証拠資料に規定され、本 SFR で規定されたしきい値以下でなければならない(must)か、または TOE が本 SFR で規定されたしきい値を超えた値を受け付けてはならない(must not)かの、いずれかでなければならない(must)。

FCS_SSHC_EXT.1.9 TSF は、SSH クライアントが RFC 4251 のセクション 4.1 に記述されるように、その対応する[選択：*公開鍵*、*信頼された認証局のリスト*、*それ他の方法なし*] を持つそれぞれのホスト名に結び付いたローカルなデータベースを用いる SSH サーバの識別情報を認証することを保証しなければならない(shall)。

適用上の注釈 165

信頼された認証局のリストは、FCS_SSHC_EXT.1.5 において x509v3-ecdsa-sha2-nistp256 または x509v3-ecdsa-sha2-nistp384 が指定される場合にのみ選択可能である。

C.2.2.6 FCS_SSHS_EXT.1 SSH サーバプロトコル

ファミリのふるまい

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

コンポーネントのレベル付け

FCS_SSHS_EXT SSH サーバプロトコル — 1

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

管理：FCS_SSHS_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_SSHS_EXT.1

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

a) SSH セションの確立失敗
b) SSH セションの確立
c) SSH セションの終了

FCS_SSHS_EXT.1	**SSH サーバプロトコル**

下位階層： なし

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作 (AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作 (署名の生成／検証)
FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作 (鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

FCS_SSHS_EXT.1.1 TSF は、RFC [選択 : *4251*、*4252*、*4253*、*4254*、*5647*、*5656*、*6187*、*6668*、*その他の RFC なし*] に適合する SSH プロトコルを実装しなければならない(shall)。

適用上の注釈 166

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

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

FCS_SSHS_EXT.1.3 TSF は、RFC 4253 に記述されるように、SSH トランスポート接続中の

[割付：*バイト数*] より大きいパケットが破棄されることを保証しなければならない(shall)。

適用上の注釈 167

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

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

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

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

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

FCS_SSHS_EXT.1.8 TSF は、SSH コネクション内で同じセション鍵が 1 時間以内、かつ 1 ギガバイト未満の送信データのしきい値で使用されることを保証しなければならない(shall)。いずれかのしきい値に達した後、鍵変更が実行される必要がある。

適用上の注釈 168

本 SFR は、2 つのしきい値を定義する－1 つは最大時間同じセション鍵が使用可能であり、他方はデータの最大容量まで同じセション鍵を用いて送信可能である。両方のしきい値が実装される必要があり、いずれかのしきい値に達すると鍵変更が実行される必要がある。最大送信データについて、受信及び送信データの合計が集計される必要がある。鍵変更は、送受信トラフィクについてのすべてのセション鍵 (暗号化、完全性保護) に提供される。

TOE が本 SFR で定義された最大値よりも低いしきい値を実装することは、受け入れ可能である。

本要件に関連する設定可能な、あらゆるしきい値について、ガイダンス証拠資料は、そのしきい値の可能な設定方法について規定する必要がある。許可された値がガイダンス証拠資料に規定され、本 SFR で規定されたしきい値以下でなければならない(must)か、または TOE が本 SFR で規定されたしきい値を超えた値を受け付けてはならない(must not)かの、いずれかでなければならない(must)。

C.2.2.7 FCS_TLSC_EXT TLS クライアントプロトコル

ファミリのふるまい

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

コンポーネントのレベル付け

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

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

管理：FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

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

a) TLS セションの確立失敗
b) TLS セションの確立
c) TLS セションの終了

FCS_TLSC_EXT.1	**TLS クライアントプロトコル**

下位階層： なし

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作 (AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作 (署名の生成／検証)
FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作 (鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

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

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

適用上の注釈 169

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

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

適用上の注釈 170

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

FCS_TLSC_EXT.1.3 TSF は、サーバ証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効であると思われる場合、TSF は、[選択：*接続を確立してはならない(shall not)、接続を確立するための許可を要求しなければならない(shall)、[割付：その他のアクションを取らなければならない(shall)]*]。

適用上の注釈 171

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

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

適用上の注釈 172

楕円曲線を伴う暗号スイートが FCS_TLSC_EXT.1.1 において選択された場合、1 つ以上の曲線の選択が必須となる。楕円曲線を伴う暗号スイートが FCS_TLS_EXT.1.1 において一つも選択されない場合、「なし」が選択されるべきである(should)。

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

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

下位階層： FCS_TLSC_EXT.1 TLS クライアントプロトコル

依存性： FCS_CKM.1 暗号鍵生成

FCS_CKM.2　暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作 (AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作 (署名の生成／検証)
FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)
FCS_COP.1/KeyedHash　暗号操作 (鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

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

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

適用上の注釈 173

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

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

適用上の注釈 174

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

FCS_TLSC_EXT.2.3 TSF は、サーバ証明書が有効である場合にのみ、高信頼チャネルを確立しなければならない(shall)。サーバ証明書が無効であると思われる場合、TSF は、[選択：*接続を確立してはならない(shall not)*、*接続を確立するための許可を要求しなければならない(shall)*、*[割付：その他のアクションを取らなければならない(shall)]*]。

適用上の注釈 175

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

て決定される。

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

適用上の注釈 176

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

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

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

適用上の注釈 177

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

C.2.2.8 FCS_TLSS_EXT TLS サーバプロトコル

ファミリのふるまい

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

コンポーネントのレベル付け

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

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

管理：FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FCS_TLSS_EXT.1, FCS_TLSS_EXT.2

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

a) TLS セションの確立失敗
b) TLS セションの確立
c) TLS セションの終了

FCS_TLSS_EXT.1	**TLS サーバプロトコル**

下位階層： なし

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作 (AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作 (署名の生成／検証)
FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作 (鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

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

- *必須の暗号スイート：*
  - *[割付：必須の暗号スイートのリスト及びそれぞれが定義される RFC への参照]*

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

適用上の注釈 178

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

FCS_TLSS_EXT.1.2 TSF は、[割付：*拒否するプロトコルバージョンのリスト*] を要求するクライアントからの接続を拒否しなければならない(shall)。

適用上の注釈 179

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

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

適用上の注釈 180

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

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

下位階層： FCS_TLSS_EXT.1 TLS サーバプロトコル

依存性： FCS_CKM.1 暗号鍵生成
FCS_CKM.2 暗号鍵確立
FCS_COP.1/DataEncryption 暗号操作 (AES データ暗号化／復号)
FCS_COP.1/SigGen 暗号操作 (署名の生成／検証)
FCS_COP.1/Hash 暗号操作 (ハッシュアルゴリズム)
FCS_COP.1/KeyedHash 暗号操作 (鍵付きハッシュアルゴリズム)
FCS_RBG_EXT.1 乱数ビット生成

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

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

- *その他の暗号スイートなし]]。*

適用上の注釈 181

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

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

適用上の注釈 182

FCS_TLSS_EXT.2.1 において選択されなかったあらゆる TLS のバージョンが、ここで選択されるべきである(should)。(「なし」が本エレメントに対して選択される場合、ST 作成者は、「及び なし」という言葉をしょうりゃくしてもよい。)

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

適用上の注釈 183

割付は、FCS_TLSS_EXT.2.1 において行われた割付に基づいて記入されるだろう。

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

適用上の注釈 184

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

FCS_TLSS_EXT.2.5 TSF は、クライアント証明書が無効である場合、高信頼チャネルを確立してはならない(shall not)。クライアント証明書が無効であると思われる場合、TSF は、[選択：*接続を確立してはならない(shall not)*、*接続を確立するための許可を要求しなければならない(shall)*、*[割付：その他のアクション]を行わなければならない(shall)*]。

適用上の注釈 185

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

FCS_TLSS_EXT.2.6 TSF は、証明書に含まれる Distinguished Name (DN) または Subject Alternative Name (SAN) がピアに期待される識別子と一致しない場合、高信頼チャネルを確立してはならない(shall not)。

適用上の注釈 186

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

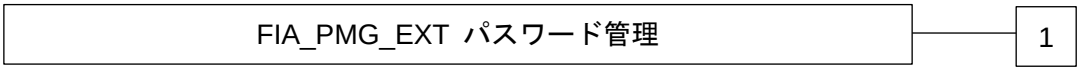
C.3 識別と認証 (FIA)

C.3.1 パスワード管理 (FIA_PMG_EXT)

ファミリのふるまい

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

コンポーネントのレベル付け



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

管理：FIA_PMG_EXT.1

管理機能なし。

監査：FIA_PMG_EXT.1

具体的な監査要件なし。

C.3.1.1 FIA_PMG_EXT.1 パスワード管理

FIA_PMG_EXT.1	**パスワード管理**

下位階層： なし

依存性： なし

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

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

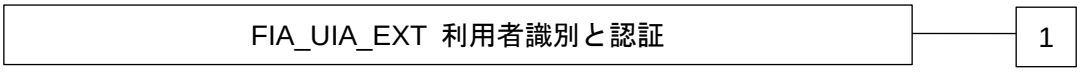
b) 最小のパスワード長は、セキュリティ管理者によって設定可能でなければならず、また 15 文字以上のパスワードをサポートしなければならない。

C.3.2 利用者識別と認証 (FIA_UIA_EXT)

ファミリのふるまい

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

コンポーネントのレベル付け



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

管理：FIA_UIA_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

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

監査：FIA_UIA_EXT.N

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

a) 識別と認証のメカニズムの利用すべて
b) 提供された利用者識別情報、試行の生成元 (例えば、IP アドレス)

C.3.2.1 FIA_UIA_EXT.1 利用者識別と認証

FIA_UIA_EXT.1	利用者識別と認証

下位階層： なし

依存性： FTA_TAB.1 デフォルト TOE アクセスバナー

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

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

FIA_UIA_EXT.1.2 TSF は、その管理利用者を代行する他の TSF 仲介アクションを許可する前に、各管理利用者に識別と認証が成功することを要求しなければならない(shall)。

適用上の注釈 187

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

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

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

FMT_SMR.2 の適用上の注釈に従って、分散型 TOE については、少なくとも 1 つの TOE コンポーネントは、FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってセキュリティ管理者の認証をサポートしなければならない(has to)が、必ずしもすべての TOE コンポーネントがサポートしなくてもよい。必ずしもすべての TOE コンポーネントがセキュリティ管理者の認証のこのやり方をサポートしない場合、TSS には、セキュリティ管理者がどのように認証され識別されるかについて記述しなければならない(shall)。

C.3.3 利用者認証 (FIA_UAU) (FIA_UAU_EXT)

ファミリのふるまい

ローカルの管理利用者認証メカニズムを提供する

コンポーネントのレベル付け

FIA_UAU_EXT パスワードベースの認証メカニズム	2

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

管理：FIA_UAU_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) なし

監査：FIA_UAU_EXT.2

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

a) 最小：認証メカニズムのすべての使用

C.3.3.1 FIA_UAU_EXT.2 パスワードベースの認証メカニズム

FIA_UAU_EXT.2	**パスワードベースの認証メカニズム**

下位階層： なし

依存性： なし

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

適用上の注釈 188

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

FMT_SMR.2 のための適用上の注釈に従って、分散型 TOE については、少なくとも 1 つの TOE コンポーネントは、FIA_UIA_EXT.1 及び FIA_UAU_EXT.2 に従ってセキュリティ管理者の認証をサポートしなければならない(has to)が、必ずしもすべての TOE コンポーネントがサポートしなくてもよい。必ずしもすべての TOE コンポーネントがセキュリティ管理者の認証のこのやり方をサポートしない場合、TSS には、セキュリティ管理者がどのように認証され識別されるかについて記述しなければならない(shall)。

C.3.4 X.509 証明書を用いた認証 (拡張—FIA_X509_EXT)

ファミリのふるまい

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

コンポーネントのレベル付け

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

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

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

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

以下のアクションは、FMT における管理機能と考えられる：

a) インポートされた X.509v3 証明書の削除
b) X.509v3 証明書のインポート及び削除の承認
c) 証明書要求の開始

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

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

a) 最小：具体的な監査要件はない。

C.3.4.1 FIA_X509_EXT.1 X.509 証明書有効性確認

FIA_X509_EXT.1	**X.509 証明書有効性確認**

下位階層： なし

依存性： FIA_X509_EXT.2 X.509 証明書認証
FIA_X509_EXT.3 X.509 証明書要求

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

- RFC 5280 証明書有効性確認及び証明書パス検証。
- 証明書パスは、信頼された CA 証明書で終端しなければならない(must)。
- TSF は、すべての CA 証明書について、basicConstraints 拡張の存在と CA フラグが TRUE にセットされていることを保証し、証明書パスを検証しなければならない(shall)。
- TSF は、[選択：*RFC 6960 で規定されたオンライン証明書状態プロトコル (OCSP)*、*RFC 5280 で規定された証明書失効リスト (CRL)*、*RFC 5759 で規定された証明書失効リスト (CRL)*、*[割付：TSF が実施するセクションのリスト]*、*失効方法なし*] を用いて、証明書の失効状態を検証しなければならない(shall)。
- TSF は、以下の規則に従って extendedKeyUsage フィールドを検証しなければならない(shall)：[割付：*検証が必要な extendedKeyUsage フィールドの内容を定める規則*]。

適用上の注釈 189

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

的」) が指定される。

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

適用上の注釈 190

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

C.3.4.2 FIA_X509_EXT.2 X509 証明書認証

FIA_X509_EXT.2	**X.509 証明書認証**

下位階層： なし

依存性： FIA_X509_EXT.1 X.509 証明書有効性確認
FIA_X509_EXT.3 X.509 証明書要求

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

適用上の注釈 191

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

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

適用上の注釈 192

しばしば、CRL をダウンロードするか、OCSP を用いてルックアップを実行するかのいずれかで一証明書の失効状態をチェックするために、コネクションが確立されなければならない(must)。FIA_X509_EXT.2 で、コネクションが確立できないような事象におけるふるまいについて記述するために、選択が使用される(例えば、ネットワークエラーより)。TOE が FIA_X509_EXT.1 でのその他すべての規則に従って証明書の有効性を決定した場合、選択において示されたふるまいが有効性を決定する。TOE は、FIA_X509_EXT.1 でのその他の有効性確認の規則のいずれにも失敗する場合、証明書を受け入れてはならない(must not)。管理者設定されたオプションが ST によって選択されている場合、ST 作成者は、FMT_SMF.1 における対応する機能についても選択する。

TOE が分散型であり、FIA_X509_ExT.1/ITT が選択される場合、証明書失効チェックはオプションである。これは、追加の許可アクションが FCO_CPC_EXT.1 で定義されるとおりの TOE

内高信頼チャネルの有効化と無効化において実行されるからである。このケースでは、接続は、証明書有効性を毛呈するために要求されない、また本 SFR は自明に満たされる。

C.3.4.3 FIA_X509_EXT.3 X.509 証明書要求

FIA_X509_EXT.3	**X.509 証明書要求**

下位階層： なし

依存性： FCS_CKM.1 暗号鍵生成
FIA_X509_EXT.1 X.509 証明書有効性確認
FIA_X509_EXT.3 X.509 証明書要求

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

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

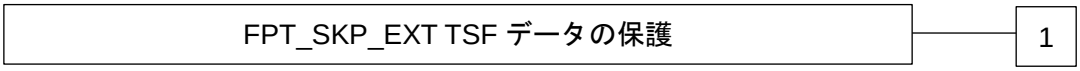
C.4 TSF の保護 (FPT)

C.4.1 TSF データの保護 (FPT_SKP_EXT)

ファミリのふるまい

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

コンポーネントのレベル付け



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

管理：FPT_SKP_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 予見される管理アクティビティはない。

監査：FPT_SKP_EXT.1

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

a) 予見される監査対象事象はない。

C.4.1.1 FPT_SKP_EXT.1 TSF データの保護 (すべての対称鍵の読み出しについて)

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

下位階層： なし

依存性： なし

FPT_SKP_EXT.1.1 TSF は、すべての事前共有鍵、対称鍵、及びプライベート鍵の読み出しを防止しなければならない(shall)。

適用上の注釈 193

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

すことを制限している。

C.4.2 管理者パスワードの保護 (FPT_APW_EXT)

C.4.2.1 FPT_APW_EXT.1 管理者パスワードの保護

ファミリのふるまい

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

コンポーネントのレベル付け

FPT_APW_EXT 管理者パスワードの保護	1

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

管理：FPT_APW_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 管理機能なし。

監査：FPT_APW_EXT.1

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

a) 監査の必要なし。

FPT_APW_EXT.1	**管理者パスワードの保護**

下位階層： なし

依存性： なし

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

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

C.4.3 TSF 自己テスト

C.4.3.1 FPT_TST_EXT.1 TSF テスト

ファミリのふるまい

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

コンポーネントのレベル付け

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

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

管理：FPT_TST_EXT.1, FPT_TST_EXT.2

以下のアクションは、FMT における管理機能と考えられる：

a) 管理機能なし。

監査：FPT_TST_EXT.1, FPT_TST_EXT.2

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

a) TSF の自己テストが完了したことの通知

FPT_TST_EXT.1	**TSF テスト**

下位階層： なし

依存性： なし

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

適用上の注釈 194

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

分散型 TOE について、すべての TOE コンポーネントは自己テストを実行しなければならない(have to)。これは、常にそれぞれの TOE コンポーネントが同じ自己テスト実行しなければならないことを意味している訳ではない ; ST には、それぞれの TOE コンポーネントへの選択肢の適用可能性 (即ち、いつ自己テストが実行されるか)と最終的な割付 (即ち、どの自己テストが実行されるか) について記述される。

適用上の注釈 195

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

FPT_TST_EXT.2	**証明書ベースの自己テスト**

下位階層： なし

依存性： なし

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

適用上の注釈 196

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

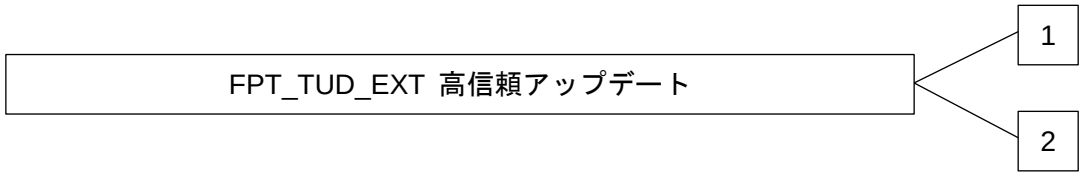
有効性は、証明書パス、有効期限、及び失効状態により、FIA_X509_EXT.1 に従って決定される。

C.4.4 高信頼アップデート (FPT_TUD_EXT)

ファミリのふるまい

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

コンポーネントのレベル付け



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

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

管理：FPT_TUD_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) TOE をアップデートする能力及びアップデートを検証する能力
b) ディジタル署名機能 (FCS_COP.1/SigGen) を用いて TOE をアップデートする能力及びアップデートを検証する能力ならびに [選択：*その他の機能なし*、*[割付：アップデート機能を支援するために用いられるその他の暗号機能 (またはその他の機能)]*]
c) TOE をアップデートする能力、及びこれらのアップデートをインストールする前に [選択：*ディジタル署名*、*公開ハッシュ*、*その他のメカニズムなし*] 機能を用いてアップデートを検証する能力

監査：FPT_TUD_EXT.1

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

a) アップデートプロセスの開始。
b) アップデートの完全性検証のあらゆる失敗。

C.4.4.1 FPT_TUD_EXT.1 高信頼アップデート

FPT_TUD_EXT.1	**高信頼アップデート**

下位階層： なし

依存性： FCS_COP.1/SigGen 暗号操作 (暗号署名と検証に関して)、または FCS_COP.1/Hash 暗号操作 (暗号ハッシュに関して)

FPT_TUD_EXT.1.1 TSF は、 [割付：*管理者*]に TOE ファームウェア／ソフトウェアの一番最近にインストールされたバージョンと同様に、TOE ファームウェア／ソフトウェアの現在実行中のバージョンを問い合わせる能力を提供しなければならない(shall)。

適用上の注釈 197

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

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

適用上の注釈 198

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

TSS は、「アップデートの自動的なチェックをサポートする」または「自動アップデートをサポートする」選択肢を使用するとき、どのアクションが TOE サポートに含まれるかについて説明する。

公開ハッシュ値 (FPT_TUD_EXT.1.3 を参照)が高信頼アップえーとメカニズムを保護するために使用されるとき、TOE は、ハッシュ値と共に(アップデートファイルに含まれるか、別々かのいずれかで)アップデートファイルを自動的にダウンロードしてはならない(must not)、かつ、例え計算されたハッシュ値が公開ハッシュ値と一致したとしても、セキュリティ管理者によるアクティブな認証なしに自動的インストールしてはならない。高信頼アップデートメカニズムを保護するために公開ハッシュ値を使用するとき、オプション「自動アップデートのサポート」は、使用されてはならない(must not)(自動化されたアップデートのチェックは許容されるが)。TOE は、自動的にアップデートファイル自体をダウンロードしてもよいが、ハッシュ値はいけない。公開ハッシュアプローチについて、セキュリティ管理者は、以下の通り、常にアップデートのインストールについてのアクティブな許可を与えることが要求されることが意図されている(FPT_TUD_EXT.1.3 の下で、より詳細について記述される通り)。これゆえに、アップデートメカニズムの種別は、例え、アップデートファイルが自動的にダウンロードされても「手動による起動アップデート」と見なされる。完全に自動化されたアプローチ(セキュリティ管理者の介在なしに)は、「ディジタル署名メカニズム」が以下の FPT_TUD_EXT.1.3 で選択されているときにのみ利用可能である。

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

適用上の注釈 199

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

公開ハッシュ値が高信頼アップデートメカニズムをセキュアにするために使用されるとき、セキュリティ管理者によるアップデートプロセスのアクティブな許可が常に要求される。開発者からセキュリティ管理者への真正なハッシュ値のセキュアな送信は、公開ハッシュが使用されるとき高信頼アップデートメカニズムを保護するための鍵となる要素の一つであり、ガイダンス文書には、この転送がどのように実行されなければならないかについて記述する必要がある。セキュリティ管理者による高信頼ハッシュ値の検証について、異なるユースケースも可能である。セキュリティ管理者は、アップデートファイルと同様に公開ハッ

シュ値を取得でき、アップデートファイルのハッシュが TOE またはその他の手段によって行われる間に、TOE の外部で検証を実行できる。セキュリティ管理者としての認証と高信頼アップデートの開始は、この場合、高信頼アップデートの「アクティブな許可」と見なされる。代わりに、管理者は、TOE にアップデートファイルとともに公開ハッシュ値を提供できる、そしてハッシュとハッシュ比較は TOE によって実行される。ハッシュ検証が成功する場合、TOE は、セキュリティ管理者による追加のステップなしでアップデートを実行できる。セキュリティ管理者としての認証と TOE へのハッシュ値の送信は、高信頼アップデートの「アクティブな許可」と見なされる、なぜなら管理者は、アップデートを実行しようとするとき、TOE にのみハッシュ値をロードすると期待されるからである。TOE へのハッシュ値の転送がセキュリティ管理者によって実行される限り、アップデートファイルのロードは、セキュリティ管理者によって実行できる、またはリポジトリから TOE によって自動的にダウンロードが可能である。

ディジタル署名メカニズムが選択される場合、署名の検証は TOE 自身によって実行されなければならない(shall)。公開ハッシュオプションについて、検証は、セキュリティ管理者による場合と同様に TOE 自身によって行われることが可能である。後者の場合、検証についての TOE 機能の利用は、必須ではないので、検証は、TOE を含むデバイスの非 TOE 機能を用いて、または TOE を含むデバイスを使用せずに、行われることか可能である。

分散型 TOE について、すべての TOE コンポーネントが高信頼アップデートをサポートしなければならない(shall)。アップデート上の署名またはハッシュの検証は、それぞれの TOE コンポーネント自身によって行われるか (署名検証)、またはそれぞれのコンポーネントについて(ハッシュ検証)行われなければならない(shall)。

分散型 TOE のアップデートは、異なる TOE コンポーネントが異なるソフトウェアバージョンを実行するような状況へ導くに違いない。異なるソフトウェアバージョン間の際によって、異なるソフトウェアバージョンの混合の影響は、全く問題にならないか、または TOE の適切な機能に対してクリティカルであるかもしれない。TSS は、分散型 TOE の高信頼アップデート中に TOE の継続的な適切な機能をサポートするようなメカニズムを詳細に記述しなければならない(shall)。

適用上の注釈 200

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

適用上の注釈 201

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

適用上の注釈 202

本 SFR において「アップデート」とは、不揮発性のシステム常駐ソフトウェアコンポーネントを、別のものと置き換えるプロセスを意味する。前者は NV イメージと呼ばれ、後者はアップデートイメージと呼ばれる。アップデートイメージは通常 NV イメージよりも新しいが、これは要件ではない。システム所有者がコンポーネントをより古いバージョンへロール

バックすることを望むような正当なケースは存在する (例えば、コンポーネント製造業者が欠陥のあるアップデートをリリースしたり、アップデート中にはもはや存在しない文書化されていない機能にシステムが依存していたりする場合等)。同様に、所有者は障害のあるストレージから回復させるために、NV イメージと同一のバージョンでアップデートすることを望むかもしれない。

TSF のすべての個別のソフトウェアコンポーネント (例、アプリケーション、ドライバ、及びカーネル) は、保護される必要のある、即ち、それらは、対応する製造業者によってディジタル署名されて、その後でアップデートを実行するメカニズムによって検証されるべきである(should)か、またはハッシュがアップデートの前に検証される必要があるものについて発行されるべきである(should)かのいずれかである。(アップデートを保護するために署名が使用される場合) コンポーネントが異なる製造業者によって署名されるかもしれないことが認識されるため、アップデートプロセスがそのアップデートと NV イメージの両方が同一の製造業者によって製造されたこと (例、公開鍵を比較することによって) または正当な署名鍵によって署名されたこと (例、X.509 証明書を使用する際に証明書の有効性確認が成功すること) を検証することは基本である。

C.4.4.2 FPT_TUD_EXT.2 証明書ベースの高信頼アップデート

FPT_TUD_EXT.2	**証明書ベースの高信頼アップデート**

下位階層： なし

依存性： FPT_TUD_EXT.1

FPT_TUD_EXT.2.1 TSF は、コード署名証明書が無効とみなされる場合、アップデートをインストールしてはならない(shall not)。

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

適用上の注釈 203

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

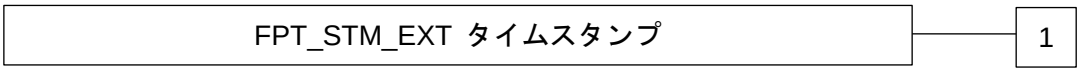
有効性は、証明書パス、有効期限、及び失効状態により FIA_X509_EXT.1 に従って決定されること。有効期限の過ぎた証明書について、ST 作成者は、その証明書が受け入れられなければならないか、拒否されなければならないか、またはその証明書を受け入れるか拒否するかの選択を管理者に委ねるかを、選択すること。

C.4.5 タイムスタンプ (FPT_STM_EXT)

ファミリのふるまい

本ファミリのコンポーネントは、タイムスタンプで利用される時刻の情報源を記述することによって FPT_STM 要件を拡張する。

コンポーネントのレベル付け



FPT_STM_EXT.1　信頼できるタイムスタンプは、FPT_STM.1 の階層である：TSF は信頼できるタイムスタンプを提供し、それらのタイムスタンプで利用される時刻の情報源を識別すること要求する。

管理：FPT_STM_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

a) 時刻の管理

b) 時刻の管理者セッティング。

監査：FPT_STM_EXT.1

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

a) 時刻の不連続な変更。

C.4.5.1　FPT_STM_EXT.1 信頼できるタイムスタンプ

FPT_STM_EXT.1	**信頼できるタイムスタンプ**

下位階層：　なし

依存性：　　なし

FPT_SKP_EXT.1.1 TSF は、それ自身の利用のための信頼できるタイムスタンプを提供できなければならない(shall)。

FPT_SKP_EXT.1.2 TSF は、[選択：時刻の設置を管理者に許可、NTP サーバを用いて時刻を同期] しなければならない(shall)。

適用上の注釈 204

信頼できるタイムスタンプは、その他の TSF を用いて利用されることが規定される、例、セキュリティ管理者が事象の順序をチェックすることによってインシデントを調査すること、及びいつ事象が発生したかについての実際のローカル時刻を決定することを、可能とするような監査データ生成のため。その情報のも読められる正確性のレベルについての決定は、管理に任される。TOE は、セキュリティ管理者によって手動でていきょうされるか、または NTP サーバ等の 1 つ以上の外部時刻情報源の利用を通して、外部の時刻と日付の情報に依存する。対応する選択肢は、FPT_STM_EXT.1.2 の選択から選ばれなければならない。ローカルのリアルタイムクロックと外部の時刻情報源 (例、NTP サーバ) との自動同期の利用

が推奨されるが、義務付けられる訳ではない。NTP サーバのような外部時刻情報源との通信について、FTP_ITC.1 の利用はオプションであるが義務付けられる訳ではないことに留意されたい。ST 作成者は、TSS にて外部時刻と日付の情報が TOE によってどのように受信され、そのようにこの情報が維持されるかについて記述する。

用語「信頼できるタイムスタンプ」は、時刻と日付の情報の厳密な利用、外部提供され、古い時刻と新しい時刻についての情報を含めて時刻セッティングへのすべての不連続な変更のログを指す。この情報を用いて、すべての監査データについての実際の時刻は決定されることが可能となる。自動化プロセスを介して管理者がヒラクチュエートし変更した、すべての不連続な時刻変更は、監査されなければならないことを留意されたい。時刻において不連続が一切見られないような、カーネルまたはシステムファシリティ－daytime (3)のような－の利用を介して時刻が変更されるときは、一切の監査は必要とされない。

分散型 TOE について、セキュリティ管理者が異なる TOE コンポーネントの時刻セッティングの間で同期を保証することが期待される。すべての TOE コンポーネントは、いずれも同期されるか(例、TOE コンポーネント間での同期を通して、または外部 NTP サーバとの異なる TOE コンポーネントの同期を通して) またはオフセットが TOE コンポーネントのいずれのペアについて管理者に知られているべきである。これには、異なるタイムゾーンへ同期される TOE コンポーネントが含まれる。

C.5 TOE アクセス (FTA)

C.5.1 FTA_SSL_EXT.1 TSF 起動によるセションロック

ファミリのふるまい

本ファミリのコンポーネントは、TSF 起動及び利用者起動によるロック、ロック解除、及び対話セションの終了を行うための要件に対処する。

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

コンポーネントのレベル付け

FTA_SSL_EXT：TSF 起動によるセションロック	1

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

管理：FTA_SSL_EXT.1

以下のアクションは、FMT における管理機能と考えられる：

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

監査：FTA_SSL_EXT.1

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

a) 対話セションをロック解除しようとするあらゆる試行。

C.5.1.1 FTA_SSL_EXT.1 TSF 起動によるセションロック

FTA_SSL_EXT.1	TSF 起動によるセションロック

下位階層： なし

依存性： FIA_UAU.1 認証のタイミング

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

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

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

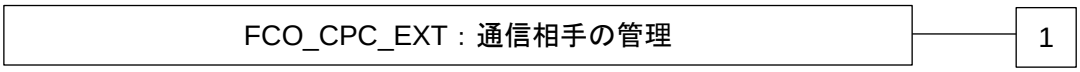
C.6 通信 (FCO)

C.6.1 通信相手の管理 (FCO_CPC_EXT)

ファミリのふるまい

本ファミリは、IT エンティティが相手と通信する方法についての上位の制約条件を定義するために使用される。例えば、いつ通信チャネルが使用可能か、それらがどのように確立されるかについての制約条件となるかもしれない、またチャネルの下位セキュリティ特性を表現している SFR へリンクする。

コンポーネントのレベル付け



FCO_CPC_EXT.1 コンポーネント登録チャネル定義、これは、分散型 TOE のコンポーネントと共に参入するための登録チャネルをサポートすること、及びこのチャネルの能力が管理者の管理下にあることを保証することを TSF に要求する。また、使用されるチャネルの種別についての記述を要求する(その他の SFR への参照によるさらなる下位のセキュリティ要件の特定を許しつつ)。

管理：FCO_CPC_EXT.1

個別の管理機能は要求されない。SFR のエレメントは、すでに分散型 TOE を構成するプロセスが管理されたアクティビティであることを保証するための通信における特性の制約条

件を特定していることに留意されたい。

監査：FCO_CPC_EXT.1

FCO_CPC__EXT.1 が PP/ST に含まれていれば、以下のアクションを監査対象とするべきである：

a) FCO_CPC_EXT.1.1 のようなコンポーネントのペア間の通信を有効化する (端点の本人性を含めて)。

b) FCO_CPC_EXT.1.3 のようなコンポーネントのペア間の通信を無効化する (無効化される端点の同一性を含めて)

FCO_CPC_EXT.1.2 のチャネルの要求された種別がその他の SFR を用いることによって特定される場合、登録チャネルの使用は、それらの SFR について監査要件によって十分に網羅されるかもしれない：さもなければ、チャネルの使用を監査するための別々の監査要件が FCO_CPC_EXT.1 について特定されるべきである。

C.6.1.1 FCO_CPC_EXT.1 コンポーネント登録チャネル定義

FCO_CPC_EXT.1	**コンポーネント登録チャネル定義**

下位階層： なし

依存性： なし

FCO_CPC_EXT.1.1 TSF は、TOE コンポーネントの任意のペア間の通信が行われる前に、このような通信を有効化することをセキュリティ管理者に要求しなければならない(shall)。

FCO_CPC_EXT.1.2 TSF は、少なくとも[割付：*チャネルが使用されなければならないデータの種別*]用に[割付：*選択の形で与えられる異なる種別のチャネルのリスト*]を用いるような通信チャネルをコンポーネントが確立し、使用するための登録プロセスを実装しなければならない(shall)。

FCO_CPC_EXT.1.3 TSF は、TOE コンポーネントの任意のペア間での通信の無効化をセキュリティ管理者に対して可能となるようにしなければならない(shall)。

適用上の注釈 205

本 SFR は、TOE が分散型である場合にのみ適用可能であり、ゆえに内部 TSF チャネル経由で通信する必要がある複数のコンポーネントを持つ。コンポーネントの初期のペアから TSF を作るとき、これらのコンポーネントのいずれかは、本 SFR の「TSF」の意味を満たす目的の TSF として特定されてもよい。

本要件の意図は、分散型 TOE に参入しようとするコンポーネントが TOE のその他のコンポーネントと通信できる前、及び新たなコンポーネントが TSF の一部として動作する前に、管理者による積極的な有効化ステップを含む登録プロセスがあることを保証することである。登録プロセスは、参入しようとするコンポーネントとの通信にそれ自身が含まれてもよい：多くのネットワークデバイスがこの特注のプロセスを使用し、「登録通信」のセキュリティ要件は、FCO_CPC_EXT.1.2 でそのときに定義される。本「登録通信」チャネルの使用は、FCO_CPC_EXT.1.1 の要件と不整合と見なされない(即ち、登録チャネルは、有効化ステップの前に使用されることが可能であるが、登録プロセスを完了するためだけのものである)。

D. エントロピーに関する証拠資料及び評定

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

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

D.1 設計記述

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

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

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

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

D.2 エントロピーの正当化

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

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

開発者が提供するエントロピー源について、最小エントロピー割合を正当化するため、大量

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

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

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

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

D.3 動作条件

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

D.4 ヘルステスト

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

E. 根拠

E.1 SFR 依存性分析

TOE に実装された SFR 間の依存性は以下の通り対処される。

SFR	依存性	根拠ステートメント
FAU_GEN.1	FPT_STM.1	FPT_STM.1 に含まれる
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 に含まれる 関連する管理者認証を規定する FIA_UIA_EXT.1 により満たされる
FAU_STG_EXT.1	FAU_GEN.1 FTP_ITC.1	FAU_GEN.1 に含まれる FTP_ITC.1 に含まれる
FCS_CKM.1	FCS_CKM.2 または FCS_COP.1 FCS_CKM.4	FCS_CKM.2 に含まれる FCS_CKM.4 に含まれる
FCS_CKM.2	FTP_ITC.1 または FTP_ITC.2 または FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 に含まれる (インポートで使用できたセキュアなチャネルとしての FTP_ITC.1 についても) FCS_CKM.4 に含まれる
FCS_CKM.4	FTP_ITC.1 または FTP_ITC.2 または FCS_CKM.1	FCS_CKM.1 に含まれる (インポートで使用できたセキュアなチャネルとしての FTP_ITC.1 についても)
FCS_COP.1/DataEncryption	FTP_ITC.1 または FTP_ITC.2 または FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 に含まれる (インポートで使用できたセキュアなチャネルとしての FTP_ITC.1 についても) FCS_CKM.4 に含まれる
FCS_COP.1/SigGen	FTP_ITC.1 または FTP_ITC.2 または FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 に含まれる (インポートで使用できたセキュアなチャネルとしての FTP_ITC.1 についても) FCS_CKM.4 に含まれる
FCS_COP.1/Hash	FTP_ITC.1 または FTP_ITC.2 または	本 SFR は、鍵なしのハッシュ操作を規定するので、鍵

	FCS_CKM.1 FCS_CKM.4	の初期化及び破壊は関連しない
FCS_COP.1/KeyedHash	FTP_ITC.1 または FTP_ITC.2 または FCS_CKM.1 FCS_CKM.4	FCS_CKM.1 に含まれる(インポートで使用できたセキュアなチャネルとしての FTP_ITC.1 についても) FCS_CKM.4 に含まれる
FCS_RBG_EXT.1	なし	
FIA_AFL.1	FIA_UAU.1	関連する管理者認証を規定する FIA_UIA_EXT.1 により満たされる
FIA_PMG_EXT.1	なし	
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1 に含まれる
FIA_UAU_EXT.2	なし	
FIA_UAU.7	FIA_UAU.1	関連する管理者認証を規定する FIA_UIA_EXT.1 により満たされる
FMT_MOF.1/ManualUpdate	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 に含まれる FMT_SMF.1 に含まれる
FMT_MTD.1/CoreData	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 に含まれる FMT_SMF.1 に含まれる
FMT_SMF.1	なし	
FMT_SMF.2	FIA_UID.1	関連する管理者認証を規定する FIA_UIA_EXT.1 により満たされる
FPT_SKP_EXT.1	なし	
FPT_APW_EXT.1	なし	
FPT_TST_EXT.1	なし	
FPT_TUD_EXT.1	FCS_COP.1/SigGen または FCS_COP.1/Hash	FCS_COP.1/SigGen 及び FCS_COP.1/Hash に含まれる
FPT_STM.1	なし	
FTA_SSL_EXT.1	FIA_UAU.1	関連する管理者認証を規定する FIA_UIA_EXT.1 により満たされる
FTA_SSL.3	なし	
FTA_SSL.4	なし	
FTA_TAB.1	なし	
FTP_ITC.1	なし	
FTP_TRP.1/Admin	なし	

表 6：必須の SFR についての SFR 依存性根拠

SFR	依存性	根拠ステートメント
FAU_STG.1	FAU_STG.3	オプション SFR として FAU_STG.3/LocSpace に含まれる
FAU_STG_EXT.2/LocSpace	FAU_GEN.1 FAU_STG_EXT.1	FAU_GEN.1 及び FAU_STG_EXT.1 に含まれる
FAU_STG.3/LocSpace	FAU_STG.1	オプション SFR として FAU_STG.1 に含まれる
FIA_X509_EXT.1/ITT	なし	
FMT_MOF.1/Service	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 に含まれる FMT_SMF.1 に含まれる
FMT_MOF.1/Functions	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 に含まれる FMT_SMF.1 に含まれる
FMT_MTD.1/CryptoKeys	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 に含まれる FMT_SMF.1 に含まれる
FPT_FLS.1/LocSpace	なし	
FPT_ITT.1	なし	
FTP_TRP.1/Join	なし	
FCO_CPC_EXT.1	なし	

表 7：オプションの SFR についての SFR 依存性根拠

SFR	**依存性**	**根拠ステートメント**
FIA_X509_EXT.1/Rev	なし	
FIA_X509_EXT.2	なし	
FIA_X509_EXT.3	FCS_CKM.1	
FCS_HTTPS_EXT.1	FCS_TLSC_EXT.1 または FCS_TLSS_EXT.1	選択ベースの SFR として FCS_TLSC_EXT.1 及び

		FCS_TLSS_EXT.1 に含まれる
FCS_IPSEC_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 に含まれる FCS_CKM.2 に含まれる FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、FCS_COP.1/KeyedHash に含まれる FCS_RBG_EXT.1 に含まれる
FCS_SSHC_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 に含まれる FCS_CKM.2 に含まれる FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、FCS_COP.1/KeyedHash に含まれる FCS_RBG_EXT.1 に含まれる
FCS_SSHS_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 に含まれる FCS_CKM.2 に含まれる FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、FCS_COP.1/KeyedHash に含まれる FCS_RBG_EXT.1 に含まれる
FCS_TLSC_EXT.1	FCS_CKM.1	FCS_CKM.1 に含まれる

	FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.2 に含まれる FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、FCS_COP.1/KeyedHash に含まれる FCS_RBG_EXT.1 に含まれる
FCS_TLSC_EXT.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 に含まれる FCS_CKM.2 に含まれる FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、FCS_COP.1/KeyedHash に含まれる FCS_RBG_EXT.1 に含まれる
FCS_TLSS_EXT.1	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_CKM.1 に含まれる FCS_CKM.2 に含まれる FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、FCS_COP.1/KeyedHash に含まれる FCS_RBG_EXT.1 に含まれる
FCS_TLSS_EXT.2	FCS_CKM.1 FCS_CKM.2	FCS_CKM.1 に含まれる FCS_CKM.2 に含まれる

	FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	FCS_COP.1/DataEncryption、FCS_COP.1/SigGen、FCS_COP.1/Hash、FCS_COP.1/KeyedHash に含まれる FCS_RBG_EXT.1 に含まれる
FPT_TST_EXT.2	なし	
FPT_TUD_EXT.2	FPT_TUD_EXT.1	FPT_TUD_EXT.1 に含まれる
FMT_MOF.1/AutoUpdate	FMT_SMR.1 FMT_SMF.1	FMT_SMR.2 に含まれる FMT_SMF.1 に含まれる

表 8：選択ベースの SFR についての SFR 依存性根拠

用語集

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

その他のコモンクライテリア略語や用語については、[CC1] を参照されたい。

略語

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