Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box セキュリティターゲット

発行日：　2026 年 6 月 10 日

バージョン：　1.15

作成：　日立ヴァンタラ株式会社

変更来歴

来歴	作成日	章	変更内容
1.01	2026/2/20	全	新規作成
1.02	2026/2/25	1	TOE の識別情報に関する見直し
1.03	2026/3/2	1 7	TOE の識別情報に関する見直し パスワードに使用可能な文字種別の見直し
1.04	2026/3/3	1 7	TOE の識別情報に関する見直し、TOE 以外のハードウェア/ソフトウェア/ファームウェアの見直し CSR 作成時に含めることが可能な情報の見直し
1.05	2026/3/5	1	表 5 の見直し
1.06	2026/3/9	1	表 5 の見直し
1.07	2026/3/10	6,7	パスワードに使用可能な文字種別の見直し
1.08	2026/3/12	1	ガイダンス文書のバージョン変更
1.09	2026/4/6	1,7 8	TLS 通信対象機器の見直し 用語の見直し
1.10	2026/4/9	1 8	TOE 運用環境などの見直し 用語の見直し
1.11	2026/4/17	1	リモート管理 PC とローカル管理 PC の定義の追記
1.12	2026/4/27	1	プライベート CA に関する記載の追記 利用者の役割の見直し
1.13	2026/5/19	1	識別認証機能の説明文章の修正
1.14	2026/6/4	1	ガイダンス文書のバージョン変更
1.15	2026/6/10	1	ガイダンス文書のバージョン変更

目次

1. ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1. ST 参照

本節では ST の識別情報を記述する。

タイトル ：Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box セキュリティターゲット
バージョン ：1.15
発行日 ：2026 年 6 月 10 日
作成 ：日立ヴァンタラ株式会社

1.2. TOE 参照

本節では TOE の識別情報を記述する。

TOE 参照：Hitachi Virtual Storage Platform One Block 23/24/26/28 with Drive Box HA-DKC-04A-03X

TOE の物理コンポーネントはコントローラシャーシとドライブボックスの 2 つである。
本 TOE は以下のいずれかの商品である。

表 1 TOE の識別情報

#	TOE 名称	コントローラシャーシの識別			ドライブボックスの識別
		ブランド識別名称	モデル識別名称		
1	Hitachi Virtual Storage Platform One Block 23 with Drive Box HA-DKC-04A-03X	HITACHI	VSP One B 23	ファームウェア (バージョン：HA-DKC-04A-03X)	DBN2
2	Hitachi Virtual Storage Platform One Block 24 with Drive Box HA-DKC-04A-03X		VSP One B 24		
3	Hitachi Virtual Storage Platform One Block 26 with Drive Box HA-DKC-04A-03X		VSP One B 26		
4	Hitachi Virtual Storage Platform One Block 28 with Drive Box HA-DKC-04A-03X		VSP One B 28		

Hitachi Virtual Storage Platform One Block 23 with Drive Box HA-DKC-04A-03X は国内販売のみ、Hitachi Virtual Storage Platform One Block 24 with Drive Box HA-DKC-04A-03X は海外販売のみのモデル。Hitachi Virtual Storage Platform One Block 26 with Drive Box HA-DKC-04A-03X および Hitachi Virtual Storage Platform One Block 28 with Drive Box HA-DKC-04A-03X は国内/海外販売共通のモデルです。

1.3. TOE 概要

1.3.1. TOE 種別

TOE はリモート管理付きディスクストレージ装置である。

TOE は TOE をリモート管理するためのユーザインタフェースや外部の監査ログサーバへの監査ログ送信などのネットワーク機能を有しており、ネットワークデバイスである。

1.3.2. TOE の使用方法

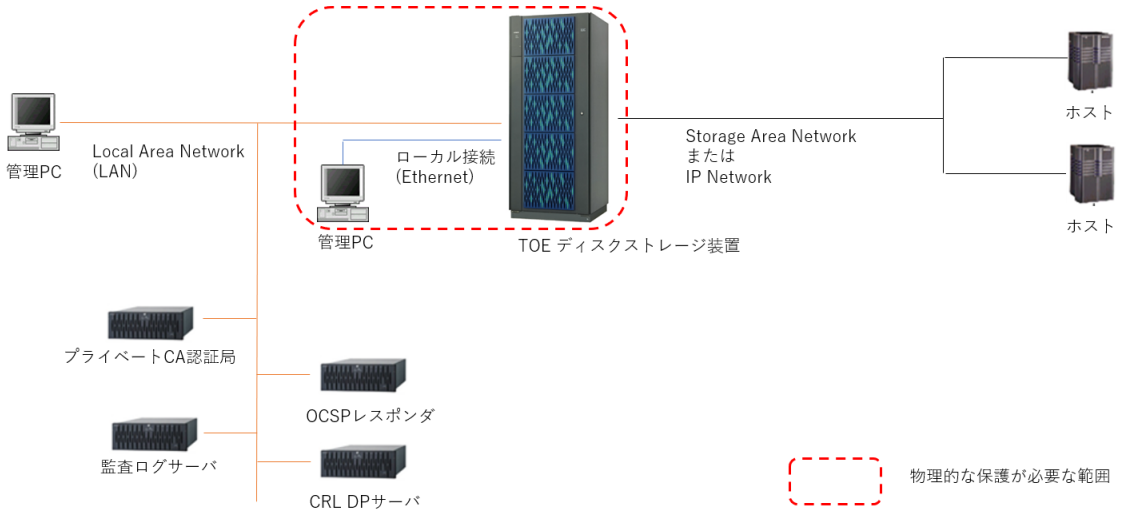


図 1 TOE の利用環境

TOE の利用環境を図 1 に示す。図 1 に示される環境に登場する機器の詳細は、1.3.4 章 表 2 を参照。

TOE には Storage Area Network または IP Network を介して、多数のホストが接続される。TOE は接続されたホストに対してディスクストレージ機能を提供する。

また、TOE は、Local Area Network(LAN)接続されたリモート管理 PC またはローカル接続(Ethernet)されたローカル管理 PC へのセキュリティ管理機能や、監査ログサーバへの監査ログの転送を行う機能などのネットワーク機能、CRL DP サーバ/OCSP レスポンダを使用した証明書の失効検証機能を提供する。

なお、証明書の発行のためにネットワーク内にはプライベート CA 認証局が必要となる。

1.3.3. TOE の主要なセキュリティ機能

TOE は TOE が扱うセキュリティ機能に関連する設定情報等の保護資産に対して、TOE への不正アクセス、セキュリティ機能のバイパス、特権の悪用、ネットワーク通信の傍受、データの改ざんのようなネットワークデバイスに対する脅威を防止するセキュリティ機能を提供する。TOE の提供するセキュリティ機能には、TOE における発生事象を監査ログに記録するセキュリティ監査機能、通信データの暗号化などの各種暗号機能、管理者や機器の識別と認証を行う機能、ファームウェア交換などのセキュリティ管理を提供する機能、TOE の起動時に自己テストを行うなどのセキュリティ機能を保護する機能、管理者セッションのセッション管理機能、LAN 接続されたリモート管理 PC への HTTPS を使用したセキュア通信、LAN 接続された監査ログサーバへの TLS を使用したセキュア通信を提供する機能が存在する。

なお、ストレージ機能に関連するセキュリティ機能(例えば格納データの暗号化機能、Storage Area Network および IP Network 上のユーザデータの暗号化機能、ホスト認証機能など)に関しては本 ST に基づく評価の対象外である。

1.3.4. TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア

この節では TOE に必要な TOE 以外のハードウェア/ソフトウェア/ファームウェアを示す。表 2 では必要なハードウェア/ソフトウェアを示す。なお、OCSP レスポンダと CRL DP サーバはいずれも証明書の失効検証を行うために必要だが、運用環境には OCSP レスポンダまたは CRL DP サーバいずれかが用意されていればよい。

表 2 TOE 以外のハードウェア/ソフトウェア/ファームウェア

ハードウェア	ソフトウェア/ファームウェア	説明
ホスト	● 以下の通信プロトコルをサポートするホストコンピューター ➢ Storage Area Network 向け ✧ Fibre Channel ➢ IP Network 向け ✧ iSCSI、NVMe/TCP	ディスクストレージ装置にアクセスするコンピュータ。Storage Area Network または IP Network を介してディスクストレージ装置と接続する。ホストおよび Storage Area Network /IP Network は本 ST に基づく評価の対象外である。
リモート管理 PC	● OS	HTTPS を利用して TOE

ハードウェア	ソフトウェア/ファームウェア	説明
	➢ Windows 11 ● ブラウザ ➢ Google Chrome、Mozilla Firefox をサポート ● REST API クライアント ➢ REST API を利用したソフトウェアまたはスクリプトであり HTTPS リクエストを送信するためのツール（curl 等）	をリモート管理するためのコンピュータ。 ESM(Embedded Storage Manager)と呼ぶ TOE 管理プログラムとの通信に使用する。
ローカル管理 PC	● OS ➢ Windows 11 ● ブラウザ ➢ Google Chrome、Mozilla Firefox をサポート	リモートで管理者がアカウントロックされ TOE にログインできない状態になった際に、TOE と直結し、HTTPS を利用して TOE をローカル管理するためのコンピュータ。 ESM と呼ぶ TOE 管理プログラムとの通信に使用する。
監査ログサーバ	本運用では rsyslogd を使用したサーバを想定している。	Syslog over TLS を利用して TOE の監査ログの蓄積を行うサーバ。
OCSP レスポンダ	本運用では OpenSSL を使用したサーバを想定している。	OCSP プロトコルを利用して認証局の証明書失効リストを参照して当該証明書の状態について返答するサーバ。
CRL DP サーバ	本運用では HTTP プロトコルを使用可能な Python の動作するサーバを想定している。	HTTP プロトコルを利用して認証局によって失効された証明書のリストをホストするサーバ。
プライベート CA 認証局	本運用では OpenSSL を使用したサーバを想定している。	証明書の署名を行うためのプライベート CA 認証局サーバ。

1.3.5. 評価者テスト構成

TOE の評価に用いた構成を以下に示す。

表 3 TOE の評価に用いた構成

種別	ソフトウェア
リモート管理 PC	OS：Windows 11 Pro ブラウザ：Google Chrome 141.0.7390.108、Mozilla Firefox 144.0 REST API クライアント：Python 3.13.5 を使用したスクリプト
ローカル管理 PC	OS：Windows 11 Pro ブラウザ：Google Chrome 141.0.7390.108
監査ログサーバ	OS：Ubuntu 21.10 監査ログサーバ：rsyslogd 8.2302.0
OCSP レスポンダ	OS：Kali Linux 2023.4 OCSP レスポンダ：OpenSSL3.0.8 を使用したサーバ
CRL DP サーバ	OS：Kali Linux 2023.4 CRL DP サーバ：Python3.13.5 を使用した http サーバ
プライベート CA 認証局	OS：Kali Linux 2023.4 CA 認証局：OpenSSL3.0.8 を使用した認証局

ローカル管理 PC とリモート管理 PC で使用できる管理機能に差異はないが、評価者テストにおいて各機能提供の確認は原則としてリモート管理 PC でのみ評価されている。

1.4. TOE 記述

1.4.1. TOE の物理的範囲

TOE は、ハードウェアおよびファームウェアから構成されるディスクストレージ装置(Hitachi Virtual Storage Platform One Block 23、24、26 及び 28)とガイダンス文書である。TOE はコントローラシャーシ、ドライブボックスから構成される。TOE はコントローラシャーシとドライブボックスの 2 つの筐体から構成されるが、SFR を提供する機能はコントローラシャーシ上のみで動作するため、非分散型の TOE である。

TOE ハードウェアは表 4 のモデルのいずれかを顧客が注文することで、製造現場より対象のモデルの構成で配送される。TOE のファームウェアは、あらかじめコントローラシャーシにインストールされた状態で配布される。

TOE のガイダンス文書は Web ページから PDF で顧客へ配布される。また、日本国内向けの販売の場合は製品に添付されるメディア媒体(DVD-R)からも PDF で顧客へ配布される。Web ページでは国内/海外それぞれ以下から配布される。

国内：
https://itpfdoc.hitachi.co.jp/Pages/document_list/manuals/vsp_rh20k_mid2u_1040.html
海外：
https://docs.hitachivantara.com/p/vsp-one-block
TOE の物理的範囲に含まれる構成要素を以降に示す。

各モデルの識別情報を以下に示す。TOE はコントローラシャーシとドライブボックスの 2 つから構成されるが、コントローラシャーシにドライブボックスが接続された状態で配布される。

表 4　TOE を構成するハードウェアと識別

#	TOE 名称	販売先	コントローラシャーシ			ドライブボックス
			ブランド識別名称	モデル識別名称		
1	Hitachi Virtual Storage Platform One Block 23 with Drive Box HA-DKC-04A-03X	国内	HITACHI	VSP One B 23	ファームウェア（バージョン：HA-DKC-04A-03X）	DBN2
2	Hitachi Virtual Storage Platform One Block 24 with Drive Box HA-DKC-04A-03X	海外		VSP One B 24		
3	Hitachi Virtual Storage Platform One Block 26 with Drive Box HA-DKC-04A-03X	国内 / 海外		VSP One B 26		
4	Hitachi Virtual Storage Platform One Block 28 with Drive Box HA-DKC-04A-03X	国内 / 海外		VSP One B 28		

TOE の構成物として TOE のガイダンスを以下に示す。

表 5 TOE のガイダンス

#	販売先	ガイダンス名称	形式	バージョン
1	国内	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 システム管理者ガイド	PDF	4050-1J-U50-41
2	国内	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One	PDF	4050-1J-U07-41

		Block 26 Hitachi Virtual Storage Platform One Block 28 ESM メッセージガイド		
3	国内	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 監査ログリファレンスガイド	PDF	4050-1J-U00-41
4	国内	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 システム構築ガイド	PDF	4050-1J-U09-41
5	国内	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 VSP One Block Administrator REST API リファレンスガイド	PDF	4050-1J-U41-40
6	国内	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 VSP One Block Administrator ユーザーズガイド	PDF	4050-1J-U40-40
7	国内	Hitachi Virtual Storage Platform One Block 23, Block 26, Block 28 Hitachi Virtual Storage Platform 5100, 5200, 5500, 5600, 5100H, 5200H, 5500H, 5600H Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H Hitachi Virtual Storage Platform F350, F370, F700, F900 Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900 REST API リファレンスガイド	PDF	4060-1J-U71-60

8	国内	Hitachi Virtual Storage Platform One Block 23 Hitachi Virtual Storage Platform One Block 26 Hitachi Virtual Storage Platform One Block 28 SIM リファレンス	PDF	4050-1J-U21-41
9	国内	Hitachi Virtual Storage Platform One Block 23/26/28 with Drive Box HA-DKC-04A-03X 利用者ガイダンス	PDF	1.14
10	海外	Hitachi Virtual Storage Platform One Block A3-04-0x System Administrator Guide	PDF	MK-23VSP1B009-03
11	海外	Hitachi Virtual Storage Platform One Block 20 A3-03-2x Installation Guide	PDF	MK-23VSP1B008-03
12	海外	Hitachi Virtual Storage Platform One Block SVOS 10.4 Maintenance Utility Messages	PDF	MK-23VSP1B005-03
13	海外	Hitachi Virtual Storage Platform One Block SVOS 10.4 Provisioning Guide	PDF	MK-23VSP1B012-03
14	海外	Hitachi Virtual Storage Platform One Block SVOS 10.4 VSP One Block Administrator REST API Reference Guide	PDF	MK-23VSP1B002-02
15	海外	Hitachi Virtual Storage Platform One Block SVOS 10.4 VSP One Block Administrator Users Guide	PDF	MK-23VSP1B001-02
16	海外	Hitachi Virtual Storage Platform One Block Hitachi Virtual Storage Platform 5000 Series Hitachi Virtual Storage Platform E Series Hitachi Virtual Storage Platform G130, G/F350, G/F370, G/F700, G/F900 SVOS 10, SVOS RF 9 REST API Reference Guide	PDF	MK-23VSP1B003-05
17	海外	Hitachi Virtual Storage Platform One Block 24/26/28 with Drive Box HA-DKC-04A-03X	PDF	1.13

		Users guidance		

1.4.2. TOE の論理的範囲

1.4.2.1. TOE 関連の利用者の役割

ディスクストレージ装置に関係する者として、本 ST では以下のような利用者を想定している。本 TOE では、セキュリティ機能要件に関わる設定を行う管理者として、セキュリティ管理者(参照・編集)、ストレージ管理者(初期設定)、監査ログ管理者(参照・編集)、保守(ユーザ)の 4 つのロールが存在する。以下表 6 に各利用者の役割を記載する。

表 6 TOE のロール

#	ロール	説明
1	セキュリティ管理者(参照・編集)	Web GUI または REST API を用いて、管理者アカウントの登録、変更、削除などのアカウント管理、Web サーバ証明書の更新、鍵の管理を実施する管理者。
2	ストレージ管理者(初期設定)	Web GUI または REST API を用いて、ディスクストレージ装置の日付と時刻の設定やアクセスバナーに表示するメッセージの設定などの初期設定を実施する管理者。
3	監査ログ管理者(参照・編集)	Web GUI または REST API を用いて、監査ログのダウンロード、および監査ログサーバに関する設定などストレージ装置で生成する監査ログに関する設定を実施する管理者。
4	保守(ユーザ)	Web GUI を用いて、プログラム交換などのユーザ保守作業を実施する管理者。

1.4.2.2. TOE が提供するセキュリティ機能

1.4.2.2.1. セキュリティ監査

セキュリティ監査とは TOE のセキュリティ機能に関連する操作または事象を監査情報として記録し、TOE 内部に蓄積する機能である。記録した監査データは管理者がダウンロードでき、また Syslog プロトコルを使用して TOE 外部の監査ログサーバへ転送することができる。

TOE の監査ログには操作を実行した管理者のユーザ情報、操作に伴う処理の成否情報、対象の操作、および処理の情報および操作を実施した日時情報が含まれる。TOE の監査ログには日付・時刻情報が付与される。TOE 内部の監査ログファイルに監査ログを追加で記録する領域が存在しない場合、最も古い監査ログを上書きして最新の監査ログを記録する。

1.4.2.2.2. 暗号サポート

暗号サポートとは TOE が使用する暗号鍵の鍵生成/鍵交換/鍵破棄、データの暗号化及び復号、署名の生成/検証、ハッシュ/HMAC の生成/検証、乱数を生成する機能である。TOE はこれらの暗号機能をリモート管理 PC との HTTPS を使用した暗号通信または監査ログサーバとの TLS を使用した暗号通信や、TSF データの保護のために使用する。

1.4.2.2.3. 識別と認証

識別と認証とはリモート管理者およびローカル管理者アカウントのログイン時に行うユーザ ID とパスワードを使用した管理者アカウントの識別・認証または、監査ログの監査ログサーバへの転送時に、TLS の認証をサポートする x509v3 証明書の検証を行う機能である。TOE はリモート管理者およびローカル管理者による Web GUI や REST API からのログインに、ユーザ ID とパスワードを使用した識別・認証方式をサポートしている。TOE はリモート管理者の識別・認証に関連して、管理者アカウントのパスワードを管理する機能やセキュリティ管理者が設定した認証失敗回数以上に連続して認証に失敗した管理者アカウントをセキュリティ管理者が定義した時間ロックアウトする機能を提供する。
また、TOE は x509v3 証明書を使用した監査ログサーバの識別・認証時に、監査ログサーバ証明書の失効検証のために OCSP レスポンダまたは CRL DP サーバとの通信を行う。証明書が失効している場合には TOE は対象の監査ログサーバとの通信を遮断する。

1.4.2.2.4. セキュリティ管理

セキュリティ管理とは管理者アカウントのロールに基づいて TSF データの操作に関する制御や、設定を行う機能である。制御や設定を可能にするために、TOE にはセキュリティ管理機能の操作をするロールを維持し識別・認証機能で認証された TOE の許可利用者に紐づける機能がある。また、TOE は管理者アカウントのパスワードポリシーを設定する機能や認証失敗回数の設定および再認証可能になるまでの時間を設定する機能などのセキュリティ管理機能を提供する。

1.4.2.2.5. TSF の保護

TSF の保護とは TOE が持つ TSF および TSF データを保護するための以下のような機能である。
・TOE の起動時に行うファームウェアのインテグリティテストおよび暗号アルゴリズムの既知解テスト
・TOE のファームウェアアップデート時に行うファームウェアの真正性の検証
・管理者アカウントの保存時に行うパスワードのハッシュ化
・x509v3 証明書の有効期限の検証および監査ログに付与するタイムスタンプ向けに管理者が行う日付と時刻の設定

1.4.2.2.6. TOE アクセス

TOE アクセスとは Web GUI/REST API を使用したリモート/ローカル管理者アクセスに関するセッションの管理を行う機能または、TOE へのアクセス時に管理者が設定した TOE 使用に関する注意事項などをアクセスバナーに表示する機能である。
TOE は管理者アクセスに関するセッションを管理するために以下のような機能を提供する。
・管理者アクセスの設定した時間無操作だったセッションの破棄
・管理者がログアウトを実施することで行うセッションの破棄

1.4.2.2.7. トラステッドパス/チャネル

トラステッドパス/チャネルとは TOE とリモート管理 PC 間の通信に HTTPS を、TOE と監査ログサーバとの通信に TLS を使用して通信路を保護する機能である。

2. 適合主張

2.1. CC 適合主張

本 ST は以下の規格に適合する。
Common Criteria for Information Technology Security Evaluation,
Part1：Introduction and general model, CCMB-2017-04-001, Version 3.1 Revision 5, April 2017
Part2：Security functional requirements, CCMB-2017-04-002, Version 3.1 Revision 5, April 2017
Part3：Security assurance requirements, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017
セキュリティ機能要件： Part2 拡張
セキュリティ保証要件： Part3 適合

2.2. PP 主張

本 ST および TOE が適合する PP は以下に示すとおりである
PP Reference: collaborative Protection Profile for Network Devices
PPVersion: 3.0e
PP Date: 06-December-2023

また、本 ST および TOE は Network Device International Community から発行されている以下の Technical Decisions を適用する

表 7 適用する Technical Decisions

#	ID	タイトル
1	RFI#202401	Redundant requirements in FPT_TST_EXT.1
2	RFI#202402a	Separation of test definitions for TLSv1.2 v1.3 (renegotiation) Client
3	RFI#202402b	Separation of test definitions for TLSv1.2 v1.3 (renegotiation) Server
4	RFI#202405	Clarification of audit selections in FMT_SMF.1.1
5	RFI#202409	Correction of FCS_TLSS_EXT.1.4
6	RFI#202413	Missing section header in NDcPP Appendix B
7	RFI#202415	FCS_COP.1.1/SigGen Needs assignment added
8	RFI#202418	FAU_STG_EXT.1

2.3. パッケージ主張

本 ST において適合を主張するパッケージはない。

2.4. 適合主張根拠

PP の要求する以下の要件を満足し、PP の要求通り「Exact Conformance」であるため、TOE 種別は NDcPP v3.0e と一貫している。

a) TOE 種別：TOE はリモート管理や監査データ送信向けのネットワーク機能を有しており、ネットワークデバイスである。(1.3 節に記載)

b) セキュリティ課題定義：脅威、前提条件、組織のセキュリティ方針について NDcPP の内容を直接記載している。(3 章に記載)

c) セキュリティ対策方針：セキュリティ対策方針について NDcPP の内容を直接記載している。(4 章に記載)

d) セキュリティ要件：セキュリティ要件について NDcPP の内容を直接記載しており、追加の要件は一切含まれない。(6 章に記載)

3. セキュリティ課題定義

3.1. 脅威

TOE はこの章に示した脅威に対抗している。

T.UNAUTHORIZED_ADMINISTRATOR_ACCESS

Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device

to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.

T.WEAK_CRYPTOGRAPHY

Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.

T.UNTRUSTED_COMMUNICATION_CHANNELS

Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself

T.WEAK_AUTHENTICATION_ENDPOINTS

Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.

T.UPDATE_COMPROMISE

Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Nonvalidated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.

T.UNDETECTED_ACTIVITY

Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

T.SECURITY_FUNCTIONALITY_COMPROMISE

Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.

T.SECURITY_FUNCTIONALITY_FAILURE

An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.2. 前提条件

A.PHYSICAL_PROTECTION

The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.

A.LIMITED_FUNCTIONALITY

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

If a virtual TOE evaluated as a pND, following Case 2 vNDs, the VS is considered part of the

TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.

A.NO_THRU_TRAFFIC_PROTECTION

A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

A.TRUSTED_ADMINISTRATOR

The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

A.REGULAR_UPDATES

The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.

A.RESIDUAL_INFORMATION

The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on

networking equipment when the equipment is discarded or removed from its operational environment.

3.3. 組織のセキュリティ方針

P.ACCESS_BANNER

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which Administrator consent by accessing the TOE.

4. セキュリティ対策方針

4.1. 運用環境のセキュリティ対策方針

OE.PHYSICAL

Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

OE.NO_GENERAL_PURPOSE

There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.

OE.NO_THRU_TRAFFIC_PROTECTION

The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.

OE.TRUSTED_ADMIN

Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE’s trust store in case such certificate can no longer be trusted

OE.UPDATES

The TOE firmware and software is updated by an Administrator on a regular basis in response

to the release of product updates due to known vulnerabilities.

OE.ADMIN_CREDENTIALS_SECURE

The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.

OE.RESIDUAL_INFORMATION

The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.

5. 拡張コンポーネント定義

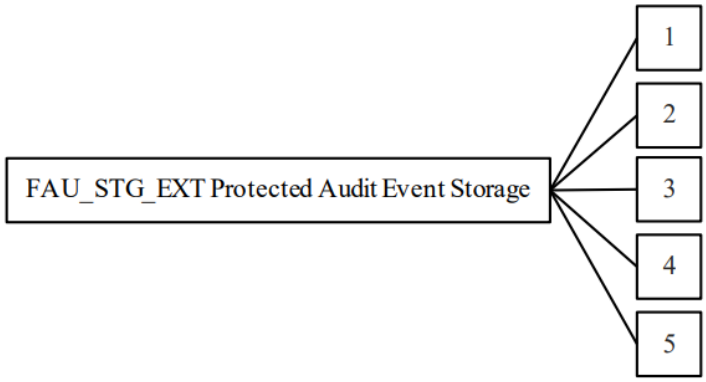
5.1. Security Audit (FAU)

5.1.1. Protected Audit Event Storage(FAU_STG_EXT)

Family Behaviour

This component defines the requirements for the TSF to be able to securely transmit audit data between the TOE and an external IT entity.

Component Levelling



FAU_STG_EXT.1 Protected audit event storage requires the TSF to use a trusted channel implementing a secure protocol.

FAU_STG_EXT.2 Counting lost audit data requires the TSF to provide information about auditrecords affected when the audit log becomes full.

FAU_STG_EXT.3 Action in case of possible audit data loss requires the TSF to generate a

warning before the audit trail exceeds the local storage capacity.
FAU_STG_EXT.4 Protected Local audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.
FAU_STG_EXT.5 Protected Remote audit event storage for distributed TOEs requires the TSF to use a trusted channel to protect audit transfer to another TOE component.

Management: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3,FAU_STG_EXT.4, FAU_STG_EXT.5

The following actions could be considered for the management functions in FMT:

a. The TSF shall have the ability to configure the cryptographic functionality.

Audit: FAU_STG_EXT.1, FAU_STG_EXT.2, FAU_STG_EXT.3, FAU_STG_EXT.4. FAU_STG_EXT.5

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FAU_STG_EXT.1 Protected Audit Event Storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FTP_ITC.1 Inter-TSF Trusted Channel

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition [selection:

- The TOE shall consist of a single standalone component that stores audit data locally,
- The TOE shall be a distributed TOE that stores audit data on the following TOE components: [assignment: identification of TOE components],
- The TOE shall be a distributed TOE with storage of audit data provided externally for the following TOE components: [assignment: list of TOE components that do not store audit data locally and the other TOE components to which they transmit their generated audit data].

FAU_STG_EXT.1.3 The TSF shall maintain a [selection: log file, database, buffer, [assignment:other local logging method]] of audit records in the event that an interruption of communication with the remote audit server

occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [selection: persistent, nonpersistent] audit records locally with a minimum storage size of [assignment: number of records and/or file/buffer size(s)].

FAU_STG_EXT.1.5 The TSF shall [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]] when the local storage space for audit data is full.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [selection: none, manual export, ability to view locally].

5.2. Cryptographic Support (FCS)

5.2.1. Random Bit Generation (FCS_RBG_EXT)

Family Behaviour

Components in this family address the requirements for random bit/number generation. This is a new family defined for the FCS class.

Component Levelling

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FCS_RBG_EXT.1 Random Bit Generation

Hierarchical to: No other components

Dependencies: No other components

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: Hash_DRBG

[selection: SHA-256, SHA-384, SHA-512], HMAC_DRBG [selection: SHA-256, SHA384, SHA-512], CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of platform-based sources] platform-based noise source] with a minimum of [selection: 128 bits, 192 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.2.2. Cryptographic Protocols (FCS_HTTPS_EXT, FCS_TLSC_EXT, FCS_TLSS_EXT)

5.2.2.1. FCS_HTTPS_EXT.1 HTTPS Protocol

Family Behaviour

Components in this family define the requirements for protecting remote management sessions between the TOE and a Security Administrator. This family describes how HTTPS will be implemented. This is a new family defined for the FCS Class.

Component Levelling

FCS_HTTPS_EXT.1 HTTPS Protocol requires that HTTPS be implemented according to RFC 2818 and supports TLS.

Management: FCS_HTTPS_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FCS_HTTPS_EXT.1 HTTPS Protocol

Hierarchical to: No other components

Dependencies: [FCS_TLSC_EXT.1 TLS Client Protocol, or FCS_TLSS_EXT.1 TLS Server Protocol]

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

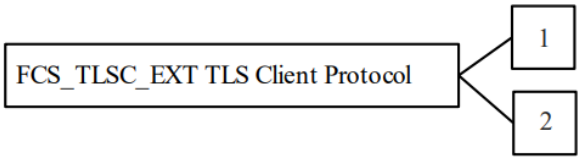
FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

5.2.2.2. FCS_TLSC_EXT TLS Client Protocol

Family Behaviour

The component in this family addresses the ability for a client to use TLS to protect data between the client and a server using the TLS protocol. This is a new family defined for the FCS class.

Component Levelling



FCS_TLSC_EXT.1 TLS Client Protocol requires that the client side of TLS be implemented as specified.

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication requires that the client side of the TLS implementation include mutual authentication.

Management: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Failure of TLS session establishment
b. TLS session establishment
c. TLS session termination

FCS_TLSC_EXT.1 TLS Client Protocol

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption)
- FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification)
- FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)

- FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
- FCS_RBG_EXT.1 Random Bit Generation
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSC_EXT.1.1

The TSF shall implement [selection: TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:
[selection:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in

RFC 5288

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256

TLS_AES_128_CCM_8_SHA256] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [selection: the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN, IPv6 address in the CN or in the SAN, IPv4 address in the SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using [selection: id-at-commonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, id-at-givenName, id-at-initials, id-at-localityName, id-at-name, id-at-organizationalUnitName, id-at-organizationName, id-at-pseudonym, id-at-serialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title] and no other attribute types].

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [selection:

- Without any administrator override mechanism

- except with the following administrator override: If the TSF fails to determine the revocation status the TSF shall allow the administrator to provide override authorization to establish the connection on a per certificate basis.
  ].

FCS_TLSC_EXT.1.4 The TSF shall [selection: not present the Supported Groups Extension, present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] and no other curves/groups] in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [selection:

- present the signature_algorithms extension with support for the following algorithms:
  [selection:
  - rsa_pkcs1 with sha256(0x0401),
  - rsa_pkcs1with sha384(0x0501),
  - rsa_pkcs1 with sha512(0x0601),
  - ecdsa_secp256r1 with sha256(0x0403),
  - ecdsa_secp384r1 with sha384(0x0503),
  - ecdsa_secp521r1 with sha512(0x0603),
  - rsa_pss_rsae with sha256(0x0804),
  - rsa_pss_rsae with sha384(0x0805),
  - rsa_pss_rsae with sha512(0x0806),
  - rsa_pss_pss with sha256(0x0809),
  - rsa_pss_pss with sha384(0x080a),
  - rsa_pss_pss with sha512(0x080b)
  -] and no other algorithms;
- present the signature_algorithms_cert extension with the following Signature Schemes:
  [selection:
  - rsa_pkcs1 with sha256(0x0401),
  - rsa_pkcs1with sha384(0x0501),
  - rsa_pkcs1 with sha512(0x0601),
  - ecdsa_secp256r1 with sha256(0x0403),
  - ecdsa_secp384r1 with sha384(0x0503),
  - ecdsa_secp521r1 with sha512(0x0603),

- rsa_pss_rsae with sha256(0x0804),
- rsa_pss_rsae with sha384(0x0805),
- rsa_pss_rsae with sha512(0x0806),
- rsa_pss_pss with sha256(0x0809),
- rsa_pss_pss with sha384(0x080a),
- rsa_pss_pss with sha512(0x080b)
-] and no other SignatureSchemes

].

FCS_TLSC_EXT.1.6 The TSF [selection: provides, does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7 The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8 The TSF shall [selection: not use PSKs, only use PSKs in TLS 1.3 session resumption with forward secrecy].

FCS_TLSC_EXT.1.9 The TSF shall [selection: support TLS 1.2 secure renegotiation through use of the “renegotiation_info” TLS extension in accordance with RFC 5746, reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption)
- FCS_COP.1/SigGen Cryptographic operation (Signature Generation and Verification)
- FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
- FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
- FCS_RBG_EXT.1 Random Bit Generation
- FCS_TLSC_EXT.1 TLS Client Protocol

- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication

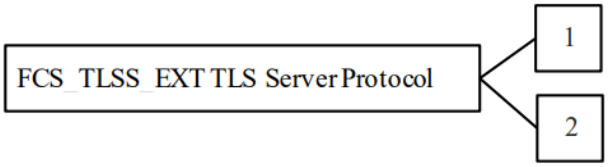
FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

5.2.2.3. FCS_TLSS_EXT TLS Server Protocol

Family Behaviour

The component in this family addresses the ability for a server to use TLS to protect data between a client and the server using the TLS protocol. This is a new family defined for the FCS class.

Component Levelling



FCS_TLSS_EXT.1 TLS Server Protocol requires that the server side of TLS be implemented as specified.

Management: FCS_TLSS_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FCS_TLSS_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Failure of TLS session establishment
b. TLS session establishment
c. TLS session termination

FCS_TLSS_EXT.1 TLS Server Protocol
Hierarchical to: No other components
Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FCS_CKM.2 Cryptographic Key Establishment
- FCS_COP.1/DataEncryption Cryptographic operation (AES Data encryption/decryption)
- FCS_COP.1/SigGen Cryptographic operation (Signature

Generation and Verification)

- FCS_COP.1/Hash Cryptographic operation (Hash Algorithm)
- FCS_COP.1/KeyedHash Cryptographic operation (Keyed Hash Algorithm)
- FCS_RBG_EXT.1 Random Bit Generation
- FIA_X509_EXT.1 X.509 Certificate Validation
- FIA_X509_EXT.2 X.509 Certificate Authentication

FCS_TLSS_EXT.1.1 The TSF shall implement [selection: TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:
[selection:

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 8422
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 8422
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256
- TLS_AES_128_CCM_8_SHA256

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [selection: RSA with key size [selection: 2048, 3072, 4096] bits; ECDSA over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using:

[selection:

- RSA key exchange with key size [selection: 2048, 3072, 4096] bits;
- EC Diffie-Hellman key agreement over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves;
- Diffie-Hellman parameters [selection: of size 2048 bits, of size 3072 bits, of size 4096 bits, of size 6144 bits, of size 8192 bits, ffdhe2048,

ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]

].

FCS_TLSS_EXT.1.4 The TSF shall support [selection: no session resumption, session resumption based on session IDs according to RFC 5246 (TLS 1.2), session resumption based on session tickets according to RFC 5077 (TLS 1.2), session resumption according to RFC 8446 (TLS 1.3)].

FCS_TLSS_EXT.1.5 The TSF [selection: provides, does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6 The TSF shall prohibit the use of the following extensions:

- Early data extension

FCS_TLSS_EXT.1.7 The TSF shall [selection: not use PSKs, only use PSKs in TLS 1.3 session resumption with forward secrecy].

FCS_TLSS_EXT.1.8 The TSF shall [selection: support secure renegotiation in accordance with RFC 5746 by always including the “renegotiation_info” TLS extension in TLS 1.2 ServerHello messages, reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].

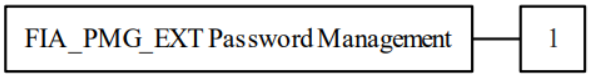
5.3. Identification and Authentication (FIA)

5.3.1. Password Management (FIA_PMG_EXT)

Family Behaviour

The TOE defines the attributes of passwords used by administrative users to ensure that strong passwords and passphrases can be chosen and maintained. This is a new family defined for the FIA class.

Component Levelling



FIA_PMG_EXT.1 Password management requires the TSF to support passwords with varying composition requirements, minimum lengths, maximum lifetime, and similarity constraints.

Management: FIA_PMG_EXT.1

There are no management functions foreseen.

Audit: FIA_PMG_EXT.1

There are no auditable events foreseen.

FIA_PMG_EXT.1 Password Management

Hierarchical to: No other components.

Dependencies: No other components

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [assignment: other characters]];

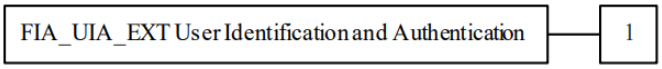
b. Minimum password length shall be configurable to between [assignment: minimum number of characters supported by the TOE] and [assignment: number of characters greater than or equal to 15] characters.

5.3.2. User Identification and Authentication (FIA_UIA_EXT)

Family Behaviour

The TSF allows certain specified actions before the non-TOE entity goes through the identification and authentication process. This is a new family defined for the FIA class.

Component Levelling



FIA_UIA_EXT.1 User Identification and Authentication requires Administrators (including remote Administrators) to be identified and authenticated by the TOE, providing assurance for that end of the communication path. It also ensures that every user is identified and authenticated before the TOE performs any mediated functions.

Management: FIA_UIA_EXT.1

The following actions could be considered for the management functions in FMT:

a. Ability to configure the list of TOE services available before an entity is identified and authenticated

Audit: FIA_UIA_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. All use of the identification and authentication mechanism

b. Provided user identity, origin of the attempt (e.g. IP address)

FIA_UIA_EXT.1 User Identification and Authentication

Hierarchical to: No other components.

Dependencies: FTA_TAB.1 Default TOE Access Banners

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [selection: no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]].

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

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [selection: Web GUI password, SSH password, SSH public key, X.509 certificate, [assignment: other authentication mechanism]] and local authentication mechanisms [selection: none, password-based, [assignment: other authentication mechanism]].

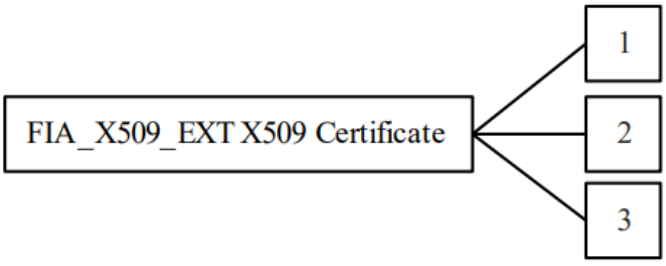
FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

5.3.3. Authentication using X.509 certificates (FIA_X509_EXT)

Family Behaviour

This family defines the behaviour, management, and use of X.509 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules, use of certificates for authentication for protocols and integrity verification, and the generation of certificate requests. This is a new family defined for the FIA class.

Component Levelling



FIA_X509_EXT.1 X509 Certificate Validation, requires the TSF to check and validate certificates in accordance with the RFCs and rules specified in the component.

FIA_X509_EXT.2 X509 Certificate Authentication, requires the TSF to use certificates to authenticate peers in protocols that support certificates, as well as for integrity verification

and potentially other functions that require certificates.
FIA_X509_EXT.3 X509 Certificate Requests, requires the TSF to be able to generate Certificate Request Messages and validate responses.

Management: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions could be considered for the management functions in FMT:

a. Remove imported X.509v3 certificates
b. Approve import and removal of X.509v3 certificates
c. Initiate certificate requests

Audit: FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable functions foreseen.

FIA_X509_EXT.1　X.509 Certificate Validation
Hierarchical to:　No other components
Dependencies:　FIA_X509_EXT.2 X.509 Certificate Authentication
FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, no revocation method].
- The TSF shall validate the extendedKeyUsage field according to the following rules: [assignment: rules that govern contents of the extendedKeyUsage field that need to be verified]

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2　X.509 Certificate Authentication

Hierarchical to: No other components

Dependencies: FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: DTLS, HTTPS, IPsec,SSH,TLS,no protocols], and [selection: code signing for system software updates [assignment: other uses], no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: allow the Administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate]

FIA_X509_EXT.3 X.509 Certificate Requests

Hierarchical to: No other components

Dependencies:

- FCS_CKM.1 Cryptographic Key Generation
- FIA_X509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: device-specific information, Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

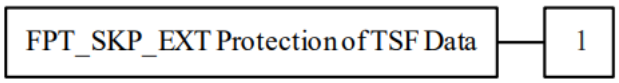
5.4. Protection of the TSF (FPT)

5.4.1. Protection of TSF Data (FPT_SKP_EXT)

Family Behaviour

Components in this family address the requirements for managing and protecting TSF data, such as cryptographic keys. This is a new family modelled after the FPT_PTD Class.

Component Levelling



FPT_SKP_EXT.1 Protection of TSF Data (for reading all symmetric keys), requires preventing symmetric keys from being read by any user or subject. It is the only component of this family.

Management: FPT_SKP_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management activities foreseen.

Audit: FPT_SKP_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

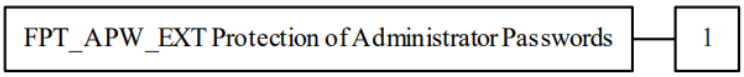
FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)
Hierarchical to: No other components.
Dependencies: No other components.
FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.4.2. Protection of Administrator Passwords (FPT_APW_EXT)

Family Behaviour

Components in this family ensure that the TSF will protect plaintext credential data such as passwords from unauthorized disclosure. This is a new family defined for the FPT class.

Component Levelling



FPT_APW_EXT.1 Protection of Administrator passwords requires that the TSF prevent plaintext credential data from being read by any user or subject.

Management: FPT_APW_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management functions foreseen.

Audit: FPT_APW_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. There are no auditable events foreseen.

FPT_APW_EXT.1 Protection of Administrator Passwords
Hierarchical to: No other components
Dependencies: No other components.
FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.
FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.4.3. TSF Self-Test (FPT_TST_EXT)

Family Behaviour

Components in this family address the requirements for self-testing the TSF for selected correct operation. This is a new family defined for the FPT class.

Component Levelling

FPT_TST_EXT.1 TSF Self-Test requires a suite of self-tests to be run during initial start-up in order to demonstrate correct operation of the TSF.

Management: FPT_TST_EXT.1

The following actions could be considered for the management functions in FMT:

a. There are no management functions foreseen.

Audit: FPT_TST_EXT.1

The following actions should be considered for audit if FAU_GEN Security audit data generation is included in the PP/ST:

a. Indication that TSF self-test was completed
b. Failure of self-test

FPT_TST_EXT.1 TSF Testing

Hierarchical to: No other components.

Dependencies: No other components.

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests:

- During initial start-up (on power on) to verify the integrity of the TOE firmware and software;
- Prior to providing any cryptographic service and [selection: at no other time, on-demand, continuously, [assignment: conditions under which self-tests should occur]] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [selection: no other, start-up, on-demand, continuous, at the conditions [assignment: conditions under which self-tests should occur]] self-tests [assignment: 'list an identifier for each self-test that is additional to those identified in the first two bullet points'].

to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to [selection: all failures, [assignment: list of failures detected by self-tests]] by [selection: entering a maintenance

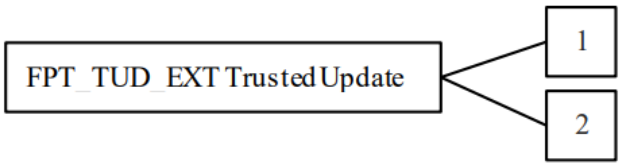
mode, rebooting, [assignment: other methods to enter a secure state]].

5.4.4. Trusted Update (FPT_TUD_EXT)

Family Behaviour

Components in this family address the requirements for updating the TOE firmware and/or software. This is a new family defined for the FPT class.

Component Levelling



FPT_TUD_EXT.1 Trusted Update requires management tools be provided to update the TOE firmware and software, including the ability to verify the updates prior to installation.
FPT_TUD_EXT.2 Trusted update based on certificates applies when using certificates as part of trusted update and requires that the update does not install if a certificate is invalid.

Management: FPT_TUD_EXT.1, FPT_TUD_EXT.2

The following actions could be considered for the management functions in FMT:

a. Ability to update the TOE and to verify the updates
b. Ability to update the TOE and to verify the updates using the digital signature capability (FCS_COP.1/SigGen) and [selection: no other functions, [assignment: other cryptographic functions (or other functions) used to support the update capability]]
c. Ability to update the TOE, and to verify the updates using [selection: digital signature, no other mechanism] capability prior to installing those updates

Audit: FPT_TUD_EXT.1, FPT_TUD_EXT.2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Initiation of the update process.
b. Any failure to verify the integrity of the update

FPT_TUD_EXT.1 Trusted Update
Hierarchical to: No other components
Dependencies: FCS_COP.1/SigGen Cryptographic operation (for Cryptographic Signature and Verification), or FCS_COP.1/Hash Cryptographic operation (for cryptographic hashing)

FPT_TUD_EXT.1.1 The TSF shall provide [assignment: Administrators] the ability to query the currently executing version of the TOE firmware/software and [selection: the most recently installed version of the TOE firmware/software; no other TOE firmware/software version].

FPT_TUD_EXT.1.2 The TSF shall provide [assignment: Administrators] the ability to manually initiate updates to TOE firmware/software and [selection: support automatic checking for updates, support automatic updates, no other update mechanism].

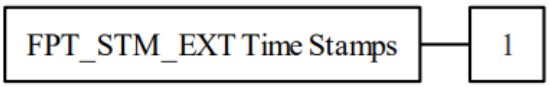
FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: X.509 certificate, digital signature] prior to installing those updates.

5.4.5. Time stamps (FPT_STM_EXT)

Family Behaviour

Components in this family extend FPT_STM requirements by describing the source of time used in timestamps. This is a new family defined for the FPT class.

Component Levelling



FPT_STM_EXT.1 Reliable Time Stamps is hierarchic to FPT_STM.1: it requires that the TSF provide reliable time stamps for TSF and identifies the source of the time used in those timestamps.

Management: FPT_STM_EXT.1

The following actions could be considered for the management functions in FMT:

a. Management of the time
b. Administrator setting of the time.

Audit: FPT_STM_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Discontinuous changes to the time.

FPT_STM_EXT.1 Reliable Time Stamps
Hierarchical to: No other components
Dependencies: No other components.

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [selection: allow the Security Administrator to set the

time, synchronise time with an NTP server, obtain time from the underlying virtualization system].

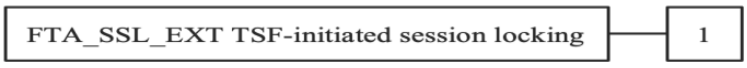
5.5. TOE Access (FTA)

5.5.1. TSF-initiated Session Locking (FTA_SSL_EXT)

Family Behaviour

Components in this family address the requirements for TSF-initiated and userinitiated locking, unlocking, and termination of interactive sessions. The extended FTA_SSL_EXT family is based on the FTA_SSL family.

Component Levelling



FTA_SSL_EXT.1 TSF-initiated session locking, requires system initiated locking of an interactive session after a specified period of inactivity. It is the only component of this family.

Management: FTA_SSL_EXT.1

The following actions could be considered for the management functions in FMT:

a. Specification of the time of user inactivity after which lock-out occurs for an individual user.

Audit: FTA_SSL_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Any attempts at unlocking an interactive session.

FTA_SSL_EXT.1 TSF-initiated Session Locking

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection:

- lock the session - disable any activity of the Administrator's data access/display devices other than unlocking the session, and requiring that the Administrator reauthenticate to the TSF prior to unlocking the session;
- terminate the session]

after a Security Administrator-specified time period of inactivity.

6. セキュリティ要件

本章では、セキュリティ要件を記述する。

6.1. 表記法

セキュリティ機能要件の記述に用いられる表記法は以下のとおり：

- NDcPP で割付/選択完了された部分または詳細化された部分：**ボールド書体**で示す。
- 本 ST で割付/選択完了された部分：*イタリック体*で示す。
- 繰り返し：「/」で始まる文字列を追加して示す。

なお、[ ]内は割付または選択された結果を示す。

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する。

6.2. セキュリティ機能要件

TOE が提供するセキュリティ機能要件を記述する。

以下のコンポーネントは CC パート 2 に含まれるものである。

表 8 TOE が提供するセキュリティ機能要件

機能要件	タイトル
FAU_GEN.1	Audit Data Generation
FAU_GEN.2	User identity association
FAU_STG.1	Protected Audit Trail Storage
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.2	Cryptographic Key Establishment
FCS_CKM.4	Cryptographic Key Destruction
FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/ Decryption)
FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
FIA_AFL.1	Authentication Failure Management
FIA_UAU.7	Protected Authentication Feedback
FMT_MOF.1/ManualUpdate	Management of Security Functions Behaviour
FMT_MOF.1/Functions	Management of Security Functions Behaviour
FMT_MTD.1/CoreData	Management of TSF Data
FMT_MTD.1/CryptoKeys	Management of TSF Data
FMT_SMF.1	Specification of Management Functions

FMT_SMR.2	Restrictions on Security Roles
FTA_SSL.3	TSF-initiated Termination
FTA_SSL.4	User-initiated Termination
FTA_TAB.1	Default TOE Access Banners
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1/Admin	Trusted Path

以下のコンポーネントは CC パート 2 の拡張である。

表 9 TOE が提供するセキュリティ拡張機能要件

FAU_STG_EXT.1	Protected Audit Event Storage
FCS_HTTPS_EXT.1	HTTPS Protocol
FCS_RBG_EXT.1	Random Bit Generation
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FCS_TLSS_EXT.1	TLS Server Protocol
FIA_PMG_EXT.1	Password Management
FIA_UIA_EXT.1	User Identification and Authentication
FIA_X509_EXT.1/Rev	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FIA_X509_EXT.3	X.509 Certificate Requests
FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
FPT_APW_EXT.1	Protection of Administrator Passwords
FPT_TST_EXT.1	TSF Testing
FPT_TUD_EXT.1	Trusted Update
FPT_STM_EXT.1	Reliable Time Stamps
FTA_SSL_EXT.1	TSF-initiated Session Locking

6.2.1. Security Audit (FAU)

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shut-down of the audit functions;

b. All auditable events for the [**not specified**] level of audit; and

c. [**All administrative actions comprising:**

- ✧ **Administrative login and logout (name of Administrator account shall be logged if individual accounts are required for Administrators).**
- ✧ **Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).**
- ✧ **Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).**
- ✧ [*Resetting passwords (name of related Administrator account shall be logged).*]

]

d. [**Specifically defined auditable events listed in Table 表 10.**]

表 10 監査対象事象

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG.1	None	None
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/SigGen	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure
FCS_RBG_EXT.1	None	None
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure
FCS_TLSC_EXT.2	None	None

FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None	None
FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None	None
FIA_X509_EXT.1/Rev	● Unsuccessful attempt to validate a certificate ● Any addition, replacement or removal of trust anchors in the TOE's trust store	● Reason for failure of certificate validation ● Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None
FMT_MOF.1/Functions	None	None
FMT_MTD.1/CoreData	None	None
FMT_MTD.1/CryptoKeys	None	None
FMT_SMF.1	All management activities of TSF data	None
FMT_SMR.2	None	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None
FPT_STM_EXT.1	Discontinuous changes to time Administrator actuated	For discontinuous changes to time: The old and new values for the time. Origin

		of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None
FTA_SSL.4	The termination of an interactive session.	None
FTA_SSL_EXT.1	The termination of a local session by the session lock	None
FTA_TAB.1	None	None
FTP_ITC.1	● Initiation of the trusted channel. ● Termination of the trusted channel. ● Failure of the trusted channel functions.	● None ● None ● Reason for failure
FTP_TRP.1/Admin	● Initiation of the trusted path. ● Termination of the trusted path. ● Failure of the trusted path functions.	● None ● None ● Reason for failure

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

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

b. For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, [**information specified in column three of Table 表 10.**]

FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_STG.1 Protected Audit Trail Storage

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

FAU_STG.1.2 The TSF shall be able to [**prevent**] unauthorized modifications to the stored audit records in the audit trail.

FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition

[

- *The TOE shall consist of a single standalone component that stores audit data locally.*

]

FAU_STG_EXT.1.3 The TSF shall maintain a [*log file*] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [*persistent*] audit records locally with a minimum storage size of [*250000 records*].

FAU_STG_EXT.1.5 The TSF shall [*overwrite previous audit records according to the following rule:* [*overwrite oldest record first*]] when the local storage space for audit data is full.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [*manual export*].

6.2.2. Cryptographic Support (FCS)

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm:

[

- *RSA schemes using cryptographic key sizes of* [*2048-bit, 3072bit, 4096bit*] *that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;*
- *ECC schemes using 'NIST curves'* [*P-256, P-384, P-521*] *that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)",*

Appendix B.4;

- *FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1;*
- *FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and* [*RFC 7919*].

] ~~and specified cryptographic key sizes [assignment: cryptographic key sizes] that meet the following: [assignment: list of standards].~~

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method:

[

- *Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*
- *FFC Schemes using "FIPS 186-Type" parameter-size sets that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";*
- *FFC Schemes using "safe-prime" groups that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and* [*groups listed in RFC 7919*].

] ~~that meets the following: [assignment: list of standards].~~

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

[

- **For plaintext keys in volatile storage, the destruction shall be executed by a** [*single overwrite consisting of zeros*] **;**

- **For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that**

  [

  - *logically addresses the storage location of the key and performs a* [*single*] *overwrite consisting of* [*a new value of the key*] **;**

  ]

]

that meets the following:[**No Standard.**]

FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/ Decryption)

FCS_COP.1.1/DataEncryption The TSF shall perform [**encryption/decryption**] in accordance with a specified cryptographic algorithm [**AES used in** [*CTR, GCM*] **mode**] and cryptographic key sizes [*128 bits, 256 bits*] that meet the following: [**AES as specified in ISO 18033-3,** [*CTR as specified in ISO 10116, GCM as specified in ISO 19772*]].

FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen The TSF shall perform [**cryptographic signature services (generation and verification)**] in accordance with a specified cryptographic algorithm

[

- *RSA Digital Signature Algorithm*
- *Elliptic Curve Digital Signature Algorithm*

]

and cryptographic key sizes

[

- *For RSA: [2048 bits, 3072bits, 4096bits],*
- *For ECDSA: [256 bits, 384bits, 521bits]*

]

that meet the following:

[

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard*

(DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

- *For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves"* [*P-256, P-384, P-521*]*; ISO/IEC 14888-3, Section 6.4*

]

FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash The TSF shall perform [**cryptographic hashing services**] in accordance with a specified cryptographic algorithm [*SHA-256, SHA-384, SHA-512*] ~~**and cryptographic key sizes** [**assignment: cryptographic key sizes**]~~ and **message digest sizes** [*256, 384, 512*] **bits** that meet the following: [**ISO/IEC 10118-3:2004**].

FCS_COP.1/KeydHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash The TSF shall perform [**keyed-hash message authentication**] in accordance with a specified cryptographic algorithm [*HMAC-SHA-256, HMAC-SHA-384*] and cryptographic key sizes [*256, 384*] **and message digest sizes** [*256, 384*] **bits** that meet the following: [**ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2".**]

FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement the HTTPS using TLS.

FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [*CTR_DRBG (AES)*].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*1*] *platform-based noise source*] with a minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and

hashes that it will generate.

FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement [*TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)*] supporting the following ciphersuites:

[

- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_AES_128_GCM_SHA256*
- *TLS_AES_256_GCM_SHA384*

]

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [*the IPv4 address in the SAN, IPv6 address in the SAN*].

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [*without any administrator override mechanism*].

FCS_TLSC_EXT.1.4 The TSF shall [*present the Supported Groups Extension with the following curves/groups:* [*secp256r1, secp384r1, secp521r1, ffdhe3072, ffdhe4096*] *and no other curves/groups*] in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [

- *present the signature_algorithms extension with support for the following algorithms:*

  [

  - *rsa_pkcs1 with sha256(0x0401),*
  - *rsa_pkcs1with sha384(0x0501),*
  - *rsa_pkcs1 with sha512(0x0601),*

- *ecdsa_secp256r1 with sha256(0x0403),*
- *ecdsa_secp384r1 with sha384(0x0503),*
- *ecdsa_secp521r1 with sha512(0x0603),*
- *rsa_pss_rsae with sha256(0x0804),*
- *rsa_pss_rsae with sha384(0x0805),*
- *rsa_pss_rsae with sha512(0x0806),*
- *rsa_pss_pss with sha256(0x0809),*
- *rsa_pss_pss with sha384(0x080a),*
- *rsa_pss_pss with sha512(0x080b)*
-] and no other algorithms;

]

FCS_TLSC_EXT.1.6 The TSF [*does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7 The TSF shall prohibit the use of the following extensions:

- Early data extension
- Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8 The TSF shall [*not use PSKs*].

FCS_TLSC_EXT.1.9 The TSF shall [*reject* [*TLS 1.2, TLS 1.3*] *renegotiation attempts*].

FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 The TSF shall support TLS communication with mutual authentication using X.509v3 certificates.

FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 The TSF shall implement [*TLS 1.3 (RFC 8446), TLS 1.2 (RFC 5246)*] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as*

defined in RFC 5289

- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_AES_128_GCM_SHA256*
- *TLS_AES_256_GCM_SHA384*

] and no other ciphersuites.

FCS_TLSS_EXT.1.2 The TSF shall authenticate itself using X.509 certificate(s) using [*RSA with key size* [*2048, 3072, 4096*] *bits; ECDSA over NIST curves* [*secp256r1, secp384r1, secp521r1*] *and no other curves*].

FCS_TLSS_EXT.1.3 The TSF shall perform key exchange using: [

- *EC Diffie-Hellman key agreement over NIST curves* [*secp256r1, secp384r1, secp521r1*] *and no other curves;*
- *Diffie-Hellman parameters* [*of size 2048 bits, ffdhe3072, ffdhe4096*]

].

FCS_TLSS_EXT.1.4 The TSF shall support [*session resumption based on session tickets according to RFC 5077 (TLS 1.2), session resumption according to RFC 8446 (TLS 1.3)*].

FCS_TLSS_EXT.1.5 The TSF [*does not provide*] the ability to configure the list of supported ciphersuites as defined in FCS_TLSS_EXT.1.1.

FCS_TLSS_EXT.1.6 The TSF shall prohibit the use of the following extensions:

- Early data extension

FCS_TLSS_EXT.1.7 The TSF shall [*only use PSKs in TLS 1.3 session resumption with forward secrecy*].

FCS_TLSS_EXT.1.8 The TSF shall [*support secure renegotiation in accordance with RFC 5746 by always including the "renegotiation_info" TLS extension in TLS 1.2 ServerHello messages*].

6.2.3. Identification and Authentication (FIA)

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [**an Administrator configurable positive integer within** [*1-999*]] unsuccessful authentication attempts occur related to [**Administrators attempting to authenticate remotely using a password**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall [*prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until an Administrator defined time period has elapsed*].

FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [*"!"、"@"、"#"、"$"、"%"、"^"、"&"、"*"、"("、")"、" "、"'"、"+"、","、"-"、"."、"/"、":"、";"、"<"、"="、">"、"?"、"[“、"¥"、"]"、"_"、"`"、"{“、"|"、"}"、"~"*];
- Minimum password length shall be [**configurable to between** [*6*] **and** [*63*] **characters**].

FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [*ICMP echo, REST API(GET/configuration/version, GET /v1/objects/storages)*].

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

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [*Web GUI password,*[*REST API password*]] and local authentication mechanisms [*password-based*].

FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

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

FIA_X509_EXT.1/Rev X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certification path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [*the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3*].
- The TSF shall validate the extendedKeyUsage field according to the following rules:

  [
  - **Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.**
  - **Server certificates presented for DTLS/TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.**
  - **Client certificates presented for DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.**
  - **OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.**

  ]

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*HTTPS, TLS*] and [*no additional uses*].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [*not accept the certificate*].

FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [*Common Name*、*Organization*、*Organizational Unit*、*Country*].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

6.2.4. Security Management (FMT)

FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to [**enable**] the functions [**to perform manual updates**] to [**Security Administrators**].

FMT_MOF.1/Functions Management of Security Functions Behaviour

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [*modify the behaviour of*] the functions [*transmission of audit data to an external IT entity*] to [**Security Administrators**].

FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to [**manage**] the [**TSF data**] to [**Security Administrators**].

FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to [**manage**] the [**cryptographic keys**] to [**Security Administrators**].

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Ability to administer the TOE remotely;**
- **Ability to configure the access banner;**
- **Ability to configure the remote session inactivity time before session termination;**
- **Ability to update the TOE, and to verify the updates**

using digital signature capability prior to installing those updates;

- [
  - *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
  - *Ability to manage the cryptographic keys;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to configure the reference identifier for the peer;*
  - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
  - *Ability to generate Certificate Signing Request (CSR) and process CA certificate response;*
  - *Ability to administer the TOE locally*;
  - *Ability to configure the local session inactivity time before session termination or locking*;
  - *Ability to configure the authentication failure parameters for FIA_AFL.1*

  ].

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

[

- **Security Administrator.**

].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- **The Security Administrator role shall be able to administer the TOE remotely**

are satisfied.

6.2.5. Protection of the TSF (FPT)

FPT_SKP_EXT.1 Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests

- During initial start-up (on power on) to verify the integrity of the TOE firmware and software;
- Prior to providing any cryptographic service and [*at no other time*] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [*no other*] self-tests

to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to [*all failures*] *by* [*rebooting*].

FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide [**Security Administrators**] the ability to query the currently executing version of the TOE firmware/software and [*no other TOE firmware/software version*].

FPT_TUD_EXT.1.2 The TSF shall provide [**Security Administrators**] the ability to manually initiate updates to TOE firmware/software and [*no other update mechanism*].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [*digital signature*] prior to installing those updates.

FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [*allow the Security Administrator to set the time*].

6.2.6. TOE Access (FTA)

FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 The TSF shall terminate **a remote** interactive session after a [**Security Administrator-configurable time interval of session inactivity**].

FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow ~~**user**~~ **Administrator**-initiated termination of the ~~**user's**~~ **Administrator's** own interactive session.

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [*terminate the session*] after a Security Administrator-specified time period of inactivity.

FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing **an administrative** user session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding ~~**unauthorised**~~ use of the TOE.

6.2.7. Trusted Path/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall **be capable of using** [*TLS*] **to** provide a **trusted** communication channel between itself and ~~**another trusted IT product**~~ **authorized IT entities supporting the following capabilities: audit server,** [*no other capabilities*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~**modification or**~~ disclosure **and detection of modification of the channel data.**

FTP_ITC.1.2 The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [*audit server*].

FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin The TSF shall **be capable of using** [*HTTPS*] **to** provide a communication path between itself and **authorized** [**remote**] **Administrators** ~~**users**~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [**disclosure**]

and provides detection of modification of the channel data.

FTP_TRP.1.2/Admin The TSF shall permit [**remote Administrators ~~users~~**] to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for [**initial Administrator authentication and all remote administration actions**].

6.3. セキュリティ保証要件

TOE セキュリティ保証要件を以下表 11 に示す。

表 11 セキュリティ保証要件

Assurance Class	Assurance Component
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labelling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – conformance (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability survey (AVA_VAN.1)

6.4. セキュリティ機能要件根拠

TOE セキュリティ機能要件について、本 ST における依存性の分析結果を表 12 に示す。

表 12 セキュリティ機能要件根拠

TOE セキュリティ機能要件	要求される依存性	ST で満たしている依存性	ST で満たされない依存性
FAU_GEN.1	FPT_STM.1	FPT_STM_EXT.1 (左記の拡張であり、要件である信頼できるタイムスタンプの提供が要件に含まれ	なし

		る)	
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UIA_EXT.1 (要件であるユーザの識別タイミングが要件に含まれる)	なし
FAU_STG.1	FAU_GEN.1	FAU_GEN.1	なし
FAU_STG_EXT.1	FAU_GEN.1, FTP_ITC.1	FAU_GEN.1, FTP_ITC.1	なし
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4	FCS_CKM.2, FCS_CKM.4	なし
FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.1, FCS_CKM.4	なし
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1	なし
FCS_COP.1/ DataEncryption	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.4	FCS_CKM.1 (TLS 通信時にデータの暗号化/復号に使用する鍵はFCS_CKM.1に準拠した非対称鍵ではなく、FCS_CKM.2に準拠した鍵確立で確立した対称鍵を使用するため、FCS_CKM.1の代わりにFCS_CKM.2を使用して依存性を解決する。)
FCS_COP.1/SigGen	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1,	FCS_CKM.1, FCS_CKM.4	なし

	FCS_CKM.4		
FCS_COP.1/Hash	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	なし (この SFR はキーレスハッシュ操作を指定しているため、キーの初期化と破棄は関係ない。)	なし
FCS_COP.1/ KeyedHash	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4	FCS_CKM.4	FCS_CKM.1 (HMAC で使用する鍵は FCS_CKM.1 に準拠した非対称鍵ではなく、FCS_CKM.2 に準拠した鍵確立で確立した対称鍵を使用するため、FCS_CKM.1 の代わりに FCS_CKM.2 を使用して依存性を解決する。)
FCS_HTTPS_EXT.1	FCS_TLSC_EXT.1 or FCS_TLSS_EXT.1	FCS_TLSS_EXT.1	なし
FCS_RBG_EXT.1	なし	なし	なし
FCS_TLSC_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, FIA_X509_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, FIA_X509_EXT.1/Rev,	なし

	FIA_X509_EXT.2	FIA_X509_EXT.2	
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_TLSC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FIA_X509_EXT.3	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_TLSC_EXT.1, FIA_X509_EXT.1/Rev, FIA_X509_EXT.2, FIA_X509_EXT.3	なし
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, FIA_X509_EXT.1, FIA_X509_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, FIA_X509_EXT.1/Rev, FIA_X509_EXT.2	なし
FIA_AFL.1	FIA_UAU.1	FIA_UIA_EXT.1 (要件であるユーザの認証タイミングが要件に含まれる)	なし
FIA_PMG_EXT.1	なし	なし	なし
FIA_UIA_EXT.1	FTA_TAB.1	FTA_TAB.1	なし
FIA_UAU.7	FIA_UAU.1	FIA_UIA_EXT.1	なし

		(要件であるユーザの認証タイミングが要件に含まれる)	
FIA_X509_EXT.1/Rev	FIA_X509_EXT.2	FIA_X509_EXT.2	なし
FIA_X509_EXT.2	FIA_X509_EXT.1	FIA_X509_EXT.1/Rev	なし
FIA_X509_EXT.3	FCS_CKM.1, FIA_X509_EXT.1	FCS_CKM.1, FIA_X509_EXT.1/Rev	なし
FMT_MOF.1/ ManualUpdate	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (左記の上位階層であり、要件であるセキュリティの役割の維持が要件に含まれる), FMT_SMF.1	なし
FMT_MOF.1/ Functions	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (左記の上位階層であり、要件であるセキュリティの役割の維持が要件に含まれる), FMT_SMF.1	なし
FMT_MTD.1/ CoreData	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (左記の上位階層であり、要件であるセキュリティの役割の維持が要件に含まれる), FMT_SMF.1	なし
FMT_MTD.1/ CryptoKeys	FMT_SMR.1, FMT_SMF.1	FMT_SMR.2 (左記の上位階層であり、要件であるセキュリティの役割の維持が要件に含まれる),	なし

		FMT_SMF.1	
FMT_SMF.1	なし	なし	なし
FMT_SMR.2	FIA_UID.1	FIA_UIA_EXT.1 (要件であるユーザの識別タイミングが要件に含まれる)	なし
FPT_SKP_EXT.1	なし	なし	なし
FPT_APW_EXT.1	なし	なし	なし
FPT_TST_EXT.1	なし	なし	なし
FPT_TUD_EXT.1	FCS_COP.1/ SigGen or FCS_COP.1/Hash	FCS_COP.1/ SigGen, FCS_COP.1/Hash	なし
FPT_STM_EXT.1	なし	なし	なし
FTA_SSL.3	なし	なし	なし
FTA_SSL.4	なし	なし	なし
FTA_SSL_EXT.1	FIA_UAU.1	FIA_UIA_EXT.1 (要件であるユーザの認証タイミングが要件に含まれる)	なし
FTA_TAB.1	なし	なし	なし
FTP_ITC.1	なし	なし	なし
FTP_TRP.1/Admin	なし	なし	なし

7. TOE 要約仕様

7.1. セキュリティ監査(FAU)

7.1.1. FAU_GEN.1

TOE の監査機能を表 13 および表 14 に示す。

TOE が取得する監査ログは、基本情報と各監査機能の操作ごとに内容の異なる詳細情報から構成される。なお、FAU_STG_EXT.1 に対する TOE の実装では、ローカル保存される監査ログに関する設定機能を持たないため、FAU_STG_EXT.1 に関する監査記録は TOE では生成されない。

表 13 監査ログ基本情報

#	項目	取得内容

1	バージョン番号	機種名や出力フォーマットのバージョン番号を出力する。
2	日付	事象発生日付を出力する。
3	時刻	事象発生時刻を出力する。
4	タイムゾーン	GMT（Greenwich Mean Time）との時差を出力する。
5	外部インタフェース名	外部インタフェースの中でどのインタフェースで操作された事象かを識別する情報を出力する。
6	ユーザ ID	TOE 利用者を識別するためのユーザ ID を出力する。
7	機能名	設定操作を実行した機能名を示す文字列を出力する。
8	操作名または事象名	機能毎の操作名称を略称で出力する。
9	パラメータ	実行した設定操作のパラメータを出力する。
10	操作の結果	操作結果を出力する。
11	送信元ホスト識別情報	ローカル/リモート管理 PC の IP アドレスを出力する。
12	ログ情報の通し番号	保存されているログ情報の通し番号を出力する。

表 14 機能要件ごとの具体的な監査項目

#	機能要件	監査項目	機能名	操作名または事象名	追加で取得する情報
1	FAU_GEN.1	監査機能の起動	Maintenance	Power On Storage	—
		監査機能の終了	Maintenance	Power Off Storage	—
		管理者のログイン	BASE	Login	・表 13 #11 送信元ホスト識別情報
		管理者のログアウト	BASE	Logout	・表 13 #11 送信元ホスト識別情報
		設定変更に関連する TSF データの変更	TSF データの変更に関しては下記項番を参照 #7、#9、#11		
		RSA・ECDSA 鍵の作成/削除	BASE	Certificate Setting	作成/削除された秘密鍵の識別情報

		監査ログサーバの設定 ・監査ログサーバへの送信の有効/無効 ・監査ログサーバのクライアント証明書の適用/削除(ルート証明書+中間証明書+クライアント証明書などのチェーン証明書も含む) ・監査ログサーバ証明書を署名したルート証明書の適用/削除	AuditLog	Set Up Syslog Serv	・適用/削除された証明書の識別情報 ・証明書検証失敗時には検証失敗理由
		Web サーバ証明書の適用/削除 (ルート証明書+中間証明書+サーバ証明書などのチェーン証明書も含む)	Maintenance	Update Cert Files	・適用/削除された証明書の識別情報 ・証明書検証失敗時には検証失敗理由
		パスワードのリセット(セキュリティ管理者（参照・編集）による他者のパスワードの変更)	Maintenance	Edit User	対象のユーザID
2	FCS_HTTPS_EXT.1	HTTPS 通信を使用した管理 PC との通信失敗	BASE	TLS Connection Establishment	・通信失敗理由 ・通信元の識別情報
3	FCS_TLSC_EXT.1	TOE の TLS クライアント機能を使用した監査ログサーバとの通信失敗	BASE	TLS Connection Establishment	・通信失敗理由 ・通信先の監査ログサーバの識別情報
4	FCS_TLSS_EXT.1	TOE の TLS サーバ機能を使用した管理	#2 を参照		

		PC との通信失敗			
5	FIA_AFL.1	ログイン試行失敗の制限に達する	BASE	Login	・ロックアウトされたユーザのログイン試行には「Lockout=yes」が記録される。 ・表 13 #11 送信元ホスト識別情報
6	FIA_UIA_EXT.1	Web GUI または RESTAPI でのログイン試行	#1 の管理者のログインを参照		
7	FIA_X509_EXT.1/ Rev	TLS 通信時の証明書検証の失敗	BASE	TLS Connection Establishment	証明書検証の失敗理由
		監査ログサーバの設定 ・監査ログサーバのクライアント証明書の適用/削除(ルート証明書+中間証明書+クライアント証明書などのチェーン証明書も含む) ・監査ログサーバ証明書を署名したルート証明書の適用/削除 ・監査ログサーバ向けのクライアント証明書およびルート証明書の適用時の証明書検証失敗	#1 の監査ログサーバの設定を参照		
		Web サーバ証明書の設定	#1 の Web サーバ証明書の適用/削除を参照		

		・Web サーバ証明書の適用/削除 (ルート証明書+中間証明書+サーバ証明書などのチェーン証明書も含む) ・Web サーバのサーバ証明書の適用時の証明書検証失敗			
8	FMT_MOF.1/ ManualUpdate	手動アップデートの開始	Maintenance	Update Firmware	—
9	FMT_SMF.1	アクセスバナーに表示するメッセージの設定	Maintenance	Edit Login Message	—
		リモート/ローカル管理者セッション終了までの非アクティブ時間の設定(Web インタフェース)	Maintenance	Edit Session Mng Info	—
		アカウントポリシー設定 ・認証失敗回数の設定 ・認証失敗後の再認証可能時間の設定 ・管理者パスワードの最小パスワード長設定	Maintenance	Set Up PolicyEmail	・設定した認証失敗回数 ・設定したロックアウト時間 ・設定した管理者パスワードの最小文字数
		CSR 及び RSA・ECDSA 鍵の作成/削除	#1 の RSA・ECDSA 鍵の作成/削除を参照		
		監査ログサーバの設定 ・監査ログサーバのクライアント証明書およびサーバ証明書	#1 の監査ログサーバの設定を参照		

		を署名したルート証明書の適用/削除(チェーン証明書も含む) ・監査ログサーバのクライアント証明書およびサーバ証明書を署名したルート証明書の適用時の証明書検証失敗			
		Web サーバ証明書の設定 ・Web サーバ証明書の適用/削除 (ルート証明書+中間証明書+サーバ証明書などのチェーン証明書も含む) ・Web サーバの証明書適用時の証明書検証失敗	#1 の Web サーバ証明書の適用/削除を参照		
		ロールとユーザグループを関連付けたユーザグループの作成	Maintenance	Create UserGroup	・ユーザグループ ID ・ロール種別
		ユーザの作成(ユーザ ID 及びパスワードの設定、ユーザグループの関連付け)	Maintenance	Create User	—
		パスワード変更(セキュリティ管理者(参照・編集)が行う他者のパスワード変更)	#1 のパスワードのリセットを参照		
		管理者による自身のパスワードの変更	Maintenance	Edit User Password	—
10	FPT_TUD_EXT.1	アップデートの開始 アップデート試行の成功	Maintenance	Update Firmware	・表 13 #10 操作の結果に「 Normal

					end」が記録される。
		アップデート試行の失敗	Maintenance	FcWizard	・表 13 #10 操作の結果に「Error」が記録される。
11	FPT_STM_EXT.1	日付と時刻の変更	Maintenance	Set Up Date & Time	変更前後の日付及び時刻
12	FTA_SSL.3	TSF によるリモートセッションの終了	BASE	Logout	・表 13 #11 送信元ホスト識別情報が空欄 ・セッションタイムアウトしたユーザがリモート接続の場合「Session Type=Remote Session」が記録される。
13	FTA_SSL.4	管理者によるセッション終了	#1 の管理者のログアウトを参照		
14	FTA_SSL_EXT.1	TSF によるローカルセッションの終了	BASE	Logout	・表 13 #11 送信元ホスト識別情報が空欄 ・セッションタイムアウトしたユーザがローカル接続の場合「Session Type=Local Session」が記録される。

15	FTP_ITC.1	高信頼チャネルの開始	BASE	TLS Connection Establishment	・通信先の監査ログサーバの識別情報
		高信頼チャネルの確立失敗	#3 参照		
		高信頼チャネルの終了	BASE	TLS Connection Termination	・通信先の監査ログサーバの識別情報
16	FTP_TRP.1/ Admin	高信頼パスの開始	BASE	TLS Connection Establishment	・通信元の識別情報
		高信頼パスの確立失敗	#2 参照		
		高信頼パスの終了	BASE	TLS Connection Termination	・通信元の識別情報

7.1.2. FAU_GEN.2

表 13 に示す通り、TOE は生成する監査記録に対して各監査対象事象の原因となった管理者アカウントのユーザ ID を付与する。

7.1.3. FAU_STG.1

TOE は、監査記録の変更、削除を実行するインタフェースを提供しない。

また、TOE 内部に保存する監査記録の量は、7.1.4 FAU_STG_EXT.1 に記載する。

ローカルに保存された監査ログは永続的に保存される。

7.1.4. FAU_STG_EXT.1

TOE は、以下の監査機能を有する。

- TOE は監査記録を FTP_ITC.1 に示す通り、TLS 通信によって暗号化されたセキュアチャネルを使用して外部の監査ログサーバへリアルタイムに転送する。外部の監査ログサーバへの転送には Syslog プロトコルを使用する。TOE は監査記録を作成する度に、TOE 内部に保存すると同時に登録済の監査ログサーバへ送信する。なお、TOE には監査ログサーバを 2 台まで登録することができる。監査ログサーバが 2 台登録さ

れている場合、TOE は両方の監査ログサーバへ監査記録を送信する。

- 監査記録は最大で 250,000 行分を内部保存する。監査記録が最大行数に達した場合は、保存を開始した行に戻って新しい情報を上書きするため、古い情報は消去される（ラップアラウンド方式)。
- TOE は、監査記録をローカルに保存する単一のスタンドアロン・コンポーネントで構成される。
- TOE はネットワーク不良などで監査ログサーバへ監査記録の送信が失敗する場合に備えて、管理 PC 上に監査記録をダウンロードする機能を提供する。TOE はこの監査ログのダウンロード機能の操作を監査ログ管理者(参照・編集)のみに許可する。
- TOE は監査記録を編集または削除するインタフェースを利用者向けに提供しない。
- TOE のローカルログのフォーマットはログファイル形式であり、不揮発メモリに保存される。

7.2. 暗号サポート(FCS)

7.2.1. FCS_CKM.1

TOE は表 15 で示す非対称鍵の生成スキームをサポートする。

表 15 TOE の鍵生成仕様

鍵生成スキーム	鍵サイズ	SFR	サービス	備考
RSA	2048 bit, 3072 bit, 4096 bit	FCS_COP.1 /SingGen	TLS 通信時の RSA 署名生成/検証用途	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 に準拠
FFC	2048bit	FCS_CKM.2	TLS 通信時の DH 鍵交換用途	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1 に準拠
FFC (safe-prime)	3072 bit, 4096 bit	FCS_CKM.2	TLS 通信時の DH 鍵交換用途	NIST Special Publication 800-56A Revision 3 および RFC 7919 に準拠
ECC	256bit, 384bit, 521bit (P-256/P-384/P-521)	FCS_CKM.2	TLS 通信時の ECDH 鍵交換用途	FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4 に準拠
	256bit, 384bit, 521bit	FCS_COP.1 /SingGen	TLS 通信時の ECDSA 署名	

	(P-256/P-384/P-521)		生成/検証用途	

7.2.2. FCS_CKM.2

TOE は以下に示す鍵確立スキームをサポートする。

表 16 TOE の鍵確立仕様

鍵確立スキーム		SFR	サービス
DH(FIPS 186-Type)	NIST Special Publication 800-56A Revision 3 に準拠	FCS_TLSS_EXT.1	管理 PC 通信
DH(safe-prime)	NIST Special Publication 800-56A Revision 3 および RFC 7919 に準拠	FCS_TLSC_EXT.1	監査ログサーバ通信
		FCS_TLSS_EXT.1	管理 PC 通信
ECDH	NIST Special Publication 800-56A Revision 3 に準拠	FCS_TLSC_EXT.1	監査ログサーバ通信
		FCS_TLSS_EXT.1	管理 PC 通信

7.2.3. FCS_CKM.4

TOE は以下の鍵破棄をサポートする。

表 17 TOE の鍵破棄仕様

鍵の種類	鍵生成元	保存場所	破棄の要因	破棄方法
TLS セッション鍵	FCS_RBG_EXT.1 の DRBG	RAM	TLS セッションの終了	0 データの 1 度の上書き
TLS ECDH 秘密鍵	FCS_RBG_EXT.1 の DRBG	RAM	TLS セッションの終了	0 データの 1 度の上書き
TLS DH 秘密鍵	FCS_RBG_EXT.1 の DRBG	RAM	TLS セッションの終了	0 データの 1 度の上書き
クライアントの秘密鍵	FCS_RBG_EXT.1 の DRBG	RAM	TLS セッションの終了	0 データの 1 度の上書き
		SSD	管理者による秘密鍵の更新	新しい鍵の 1 度の上書き

Web サーバの秘密鍵	FCS_RBG_EXT.1 の DRBG	RAM	TLS セッションの終了	0 データの 1 度の上書き
		SSD	管理者による秘密鍵の更新	新しい鍵の 1 度の上書き

TOE クライアントの秘密鍵または Web サーバの秘密鍵はセキュリティ管理者(参照・編集)が TOE の秘密鍵の生成機能を使用して生成する秘密鍵である。作成された秘密鍵は SSD に格納される。対象の秘密鍵は、ペアとなる公開鍵を持つクライアント証明書または、Web サーバ証明書を TOE にアップロードすることで監査ログサーバとの通信や管理 PC との通信に使用可能になる。

揮発領域に保存する鍵は OpenSSL の OPENSSL_cleanse() を使用して、0 データの 1 度の上書きによって削除する。揮発領域上の鍵は TLS セッションの終了時に必ず破棄され、鍵破棄に失敗するまたは鍵破棄が遅延する構成や条件はない。

不揮発領域に保存する鍵は、セキュリティ管理者(参照・編集)が Web GUI を使用して新しい鍵を作成する操作を行うと、TOE 内部で fwrite 関数を使用して古い鍵ファイルのファイルパス(論理アドレス)に新しい鍵情報を 1 度上書きすることで古い鍵を削除する。削除操作は他の操作の処理中には失敗するが、他の操作が完了した後に再実施すれば削除できる。また、鍵のファイルを新しい鍵の値で上書き時にウェアレベリングによってアドレスが変わってしまった場合には、ガベージコレクションの発生まで鍵の削除が遅延する。

7.2.4. FCS_COP.1/DataEncryption

TOE は、表に示す各モードで、128 ビット,256 ビット AES(ISO 18033-3 に準拠)を使用した対称暗号化および復号機能を提供する。

CTR,GCM モード毎の鍵の長さと用途を表 18 に示す。

表 18 モード毎の鍵の長さと用途

モード		鍵の長さ	用途
CTR	ISO 10116 に準拠	256 bit	ランダムビットの生成
GCM	ISO 19772 に準拠	128 bit 256 bit	HTTPS/TLS を使用した暗号通信

7.2.5. FCS_COP.1/SigGen

TOE は、以下の鍵長の暗号アルゴリズムを使用した署名生成/検証サービスを提供する。

a) RSA アルゴリズム(FIPS PUB 186-4 Section 5.5 と ISO/IEC 9796-2 に準拠)

- 鍵サイズ 2048 ビット、3072 ビット、4096 ビット

b) ECDSA アルゴリズム(FIPS PUB 186-4 Section 6, Appendix D NIST Curves [P-256, P-384, P-521]と ISO/IEC 14888-3 Section 6.4 に準拠)
   - 鍵サイズ 256 ビット、384 ビット、521 ビット

TOE は下記用途向けに RSA と ECDSA の署名生成/検証サービスを提供する。
・外部エンティティとの TLS プロトコルの通信（TOE がクライアントになる場合、サーバになる場合の両方）
・自己テスト
・TOE のアップデートファイル検証
署名生成/検証サービス、各使用用途に応じて使用する暗号アルゴリズムを以下に示す。

表 19 署名生成/検証サービスの暗号アルゴリズム対応表

サービス	TOE(サーバ)の TLS プロトコル	TOE(クライアント)の TLS プロトコル	自己テスト	TOE のアップデートファイル検証
署名生成サービス	RSA:2048,3072, 4096 bit ECDSA:256,384, 521 bit	RSA:2048,3072, 4096 bit ECDSA:256,384, 521 bit	-	-
署名検証サービス	-	RSA:2048,3072, 4096 bit ECDSA:256,384, 521 bit	RSA:4096 bit	RSA:4096 bit

7.2.6. FCS_COP.1/Hash

TOE は、ISO/IEC 10118-3:2004 に準拠した SHA-256、SHA-384、SHA-512 を用いた暗号ハッシュ化サービスを提供する。
TOE のハッシュ関数は以下の暗号機能で使用される。

表 20 ハッシュ関数と他暗号化機能の関係

ハッシュ関数	メッセージダイジェストサイズ	暗号機能	使用用途
SHA-256	256 bit	HMAC 機能	TLS 通信における HMAC を使用したメッセージのハッシュ化
		RSA 署名生成/署名検証機能	TLS 通信/自己テスト/TOE のアップデート

			ファイル検証におけるディジタル署名検証時のハッシュ化
			TLS 通信における DH/ECDH 鍵交換の公開鍵への署名付与及び検証時のハッシュ化
		ECDSA 署名生成/署名検証機能	TLS 通信におけるディジタル署名検証時のハッシュ化
			TLS 通信における DH/ECDH 鍵交換の公開鍵への署名付与及び検証時のハッシュ化
SHA-384	384 bit	HMAC 機能	TLS 通信における HMAC を使用したメッセージのハッシュ化
		RSA 署名生成/署名検証機能	TLS 通信におけるディジタル署名検証時のハッシュ化
			TLS 通信における DH/ECDH 鍵交換の公開鍵への署名付与及び検証時のハッシュ化
		ECDSA 署名生成/署名検証機能	TLS 通信におけるディジタル署名検証時のハッシュ化
			TLS 通信における DH/ECDH 鍵交換の公開鍵への署名付与及び検証時のハッシュ化
SHA-512	512 bit	RSA 署名生成/署名検証機能	TLS 通信におけるディジタル署名検証時のハッシュ化
			TLS 通信における DH/ECDH 鍵交換の公

			開鍵への署名付与及び検証時のハッシュ化
		ECDSA 署名生成/署名検証機能	TLS 通信におけるディジタル署名検証時のハッシュ化
			TLS 通信における DH/ECDH 鍵交換の公開鍵への署名付与及び検証時のハッシュ化
		パスワードハッシュ	管理者パスワードのハッシュ化

7.2.7. FCS_COP.1/KeyedHash

TOE は、ISO/IEC 10118-3:2004 に準拠した HMAC-SHA-256、HMAC-SHA-384 を使用した鍵付きハッシュメッセージ認証サービスを提供する。HMAC は TLS プロトコルで実装されている。TOE で使用する HMAC を表 21 に示す。

表 21 TOE の HMAC 仕様

アルゴリズム	ハッシュ関数	鍵の長さ	ブロックサイズ	使用される MAC 長
HMAC-SHA-256	SHA-256	256 bits	512 bits	256 bits
HMAC-SHA-384	SHA-384	384 bits	1024 bits	384 bits

7.2.8. FCS_HTTPS_EXT.1

TOE の Web インタフェースは、FCS_TLSS_EXT.1 によって記述された TLS 実装を使用して、HTTPS 接続を介してアクセスされる。TOE はサーバ機能としてのみ HTTPS サービスを提供し、クライアント機能で HTTPS を使用しない。

TOE の Web サーバは RFC 2818 に準拠した HTTPS プロトコル通信を提供する。RFC2818 への準拠内容について以下に示す。

表 22 TOE の HTTPS 実装

要件	TOE の実装内容
Connection Initiation	すべての HTTPS データは”application data”として送付する。
Connection Closure	TLS 接続のクローズ前に「alert close notify」をクライアントと交換する。なお、TOE はセッション再開をサポートする。

Server Behavior	TOE は TLS 接続のクローズ時に「alert close notify」を送付する。
Port Number	TOE は 443 ポートで HTTPS 接続を受け付ける。
URI Format	TOE の Web サーバには”https”フォーマットの URI で接続できる。
Endpoint Identification	TOE は HTTPS サーバとして Web サーバを提供する。TOE の Web サーバは TLS 相互認証をサポートしない。

7.2.9. FCS_RBG_EXT.1

TOE は ISO/IEC 18031:2011 に準拠した CTR_DRBG(AES 256)で 256 ビットの乱数を生成するために、256 ビットのエントロピーに加えてノンス向けにセキュリティ強度の 1/2 倍である 128 ビット、合計 384 ビットのエントロピーが必要になる。TOE の DRBG は、NXP semiconductors 社の CPU である LS1046A をエントロピー源として使用し、エントロピー源から 384 ビットのシードを取得する。LS1046A の出力はフルエントロピー[1]であり、384 ビットのシードには少なくとも 384 ビットのエントロピーが含まれる。

7.2.10. FCS_TLSC_EXT.1

TOE は TLS のクライアント機能を監査ログサーバとの通信で使用する。
TLS クライアントは TLS プロトコルバージョン 1.2(RFC5246)および 1.3(RFC 8446)のみを許可する。ただし、リネゴシエーションをサポートしない。
TOE は以下に示すサイファースイートのみサポートし、通信に使用するサイファースイートを変更する機能は持たない。また、鍵交換に PSK を使用しない。

表 23 クライアント機能でサポートするサイファースイート

#	サイファースイート
1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
4	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
5	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
6	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
7	TLS_AES_128_GCM_SHA256
8	TLS_AES_256_GCM_SHA384

[1] フルエントロピーとは、データが持つ情報量は最大で、どのビットも他のビットから予測することができないデータを指す。

TOE は以下に示す署名アルゴリズムをサポートする。
TOE は署名アルゴリズムを変更する設定機能を持たない。

表 24 サポートする署名アルゴリズム

#	署名アルゴリズム	鍵長
1	RSA	2048bit
2		3072bit
3		4096bit
4	ECDSA	256bit
5		384bit
6		521bit

TOE の signature_algorithms 拡張は以下に示すアルゴリズムをサポートしており、以下に示すアルゴリズム以外は使用しない。
なお、TOE は署名アルゴリズムを設定変更する機能は持たない。

表 25 signature_algorithms 拡張がサポートするアルゴリズム

#	TLS プロトコルバージョン	アルゴリズム
1	1.2	*rsa_pkcs1 with sha256(0x0401)*
2		*rsa_pkcs1with sha384(0x0501)*
3		*rsa_pkcs1 with sha512(0x0601)*
4	1.2/1.3	*ecdsa_secp256r1 with sha256(0x0403)*
5		*ecdsa_secp384r1 with sha384(0x0503)*
6		*ecdsa_secp521r1 with sha512(0x0603)*
7		*rsa_pss_rsae with sha256(0x0804)*
8		*rsa_pss_rsae with sha384(0x0805)*
9		*rsa_pss_rsae with sha512(0x0806)*
10	1.3	*rsa_pss_pss with sha256(0x0809)*
11		*rsa_pss_pss with sha384(0x080a)*
12		*rsa_pss_pss with sha512(0x080b)*

TOE は以下に示す TLS 拡張をサポートしており、Early data extension、RFC 8446, Section 4.2.6 の Post-handshake client authentication などのその他の TLS 拡張を使用しない。

表 26 サポートする TLS 拡張

#	TLS プロトコルバージョン	TLS 拡張
1	1.2	signature_algorithms
2		supported_groups
3	1.3	signature_algorithms
4		supported_versions
5		supported_groups
6		key_share

TOE は、監査ログサーバとの通信時に証明書の検証を実施する。証明書の検証内容については、表 30 TLS ハンドシェイク時の検証内容と対象の証明書を参照。TOE は証明書の検証に失敗した場合、セキュア通信の確立の有無について管理者の介在する余地はなく TOE はセキュア通信を確立しない。

TOE は参照識別子として、SAN(subjectAlternativeName)をサポートする。監査ログ管理者(参照・編集) による監査ログサーバの設定時に Web GUI から参照識別子を設定でき、各サーバの設定時に IP アドレスで設定することができる。ただし、IP アドレスを設定する場合、IP アドレス範囲での指定やサブネットマスクを含む IP アドレスの指定はできない。なお、監査ログ管理者(参照・編集)及びセキュリティ管理者(参照・編集)がサーバ設定を行う際、または証明書を作成する際、TOE は RFC5952 と RFC3986 に準拠した入力は強制しない。

TOE はサーバからサーバ証明書を受領すると、まず証明書内に SAN の値が存在するかを確認し、SAN の値が含まれる場合には、SAN の値についてセキュリティ管理者(参照・編集)の設定した参照識別子と一致するかを検証する。証明書の SAN の値とセキュリティ管理者(参照・編集)の設定した参照識別子情報が一致しない場合には検証が失敗する。証明書内に SAN の値が存在しない場合にも検証が失敗し、サーバとの通信をしない。

参照識別子として IP アドレスを指定する場合、TOE はセキュリティ管理者(参照・編集)の設定した IP アドレスをテキスト表現からネットワークバイトオーダーのバイナリ形式に変換して、SAN の値と比較する。IP アドレスは IPv4、IPv6 の両方をサポートする。

また、TOE は、secp256r1、secp384r1、secp521r1 の楕円曲線及び ffdhe グループの ffdhe3072、ffdhe4096 をサポートしており、Client Hello メッセージにサポートしている楕円曲線及びグループ拡張のアルゴリズムを管理者による構成を必要とせずに提示する。通信相手のサーバが TOE のサポートするグループ拡張(Supported Groups Extension)をサポートしていない場合 TOE は対象のサーバとの通信に失敗する。なお TLS 1.2 の場合、サーバから送付される Server Key Exchange で DHE2048 または ffdhe3072 では TOE はセッションを確立するが、それ以外の DHE パラメータが指定されている場合、TOE は通信を終了する。

監査ログ管理者(参照・編集)が設定する識別子は、監査ログサーバの設定画面の以下で設定する。

- 監査ログサーバの設定画面
  - ホスト名 / IP アドレス欄

7.2.11. FCS_TLSC_EXT.2

TOE は監査ログサーバとの通信時に、相互認証を行う。
TOE は監査ログサーバとの TLS ハンドシェイク時に X509v3 のクライアント証明書を監査ログサーバに送付する。監査ログサーバは TOE のクライアント証明書を検証し、認証を行う。
TOE 利用者は監査ログサーバとの TLS 通信環境を構成するために以下の要件を満たすクライアント証明書を作成し、以下の操作後に TOE にアップロードする必要がある。

① 秘密鍵 + CSR をセキュリティ管理者(参照・編集)が TOE で作成し、CSR をダウンロード
② ダウンロードした CSR を監査ログ管理者(参照・編集)に渡し、監査ログ管理者(参照・編集)が信頼できる CA で署名
③ 監査ログ管理者(参照・編集)は署名された証明書をアップロード

そのために TOE 利用者は、TOE で鍵ペア及び CSR を生成し別途 CA に署名してもらい、発行されたクライアント証明書を TOE にアップロードする。

- 中間証明書が存在する場合は、中間証明書を含んだ証明書チェーンで構成された、署名付き公開鍵証明書を準備しておくこと。
- アップロードするクライアント証明書の証明書チェーンの階層数は、ルート CA 証明書を含めて 20 階層以下であること。
- アップロードするクライアント証明書の公開鍵暗号方式が RSA・ECDSA であること。
- クライアント証明書の Common Name と Subject Alternative Name に ESM の IP アドレスを設定していること。

7.2.12. FCS_TLSS_EXT.1

TOE は TLS のサーバ機能を管理 PC との通信で使用する。
TLS サーバは TLS プロトコルバージョン 1.2(RFC5246)および 1.3(RFC 8446)のみを許可する。また、リネゴシエーションをサポートする。
TOE は以下に示すサイファースイートのみサポートする。

表 27 サーバ機能でサポートするサイファースイート

#	サイファースイート
1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
2	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288

3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
4	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
5	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
6	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
7	TLS_AES_128_GCM_SHA256
8	TLS_AES_256_GCM_SHA384

TOE は、TLS ハンドシェイク時にクライアントの指定するプロトコルバージョンとサイファースイートをチェックし、古い SSL のバージョン(SSL 1.0、SSL 2.0、SSL 3.0)、古い TLS のバージョン TLS 1.0、TLS1.1）を指定された際には通信を拒否する。TOE は TLS1.2 において、セッション ID を使用したセッション再開(RFC5246)をサポートしない。ただし、TOE は TLS 1.2 におけるセッションチケットを使用したセッション再開(RFC5077)と、TLS 1.3 でセッションチケットを使用したセッション再開(RFC8446)をサポートする。セッションチケットは、AES-256-GCM を用いて暗号化される。TOE は TLS1.3 通信時のセッション再開時に前方秘匿性を保つために PSK および DHE 鍵交換を用いる。例えば別のチャネルや手動で設定された PSK を使用した通信は許可しない。TOE は RFC5077 の第 4 節に準拠する構造をサポートする。TOE は確立済のセッションをクライアントが指定した際、対象のセッションの有効期限を確認し、有効期限が切れている場合はフルハンドシェイクを求める。なお、TOE は各コンテキストで独立したセッションキャッシュを持ち、1 つのコンテキストで確立したセッションを他のコンテキストで再開することはできない。
TOE は TLS1.2 の Server Hello に、RFC5746 に従い“renegotiation_info”拡張を含める。
TOE は、DHE/ECDHE を含むサイファースイートをサポートしている。ただしサイファースイートを設定変更することはできない。対向ピアからサポートしているグループ拡張を受領すると、TOE は以下の優先度に基づきセキュリティ強度の高い鍵交換アルゴリズムを優先して使用し、使用する鍵交換アルゴリズムを変更する機能は持たない。もし、対向ピアからサポートしている DHE のグループ拡張を受領しない場合は、TOE は通信を失敗させる。セキュリティ強度が同等のアルゴリズムは鍵長の短いものを優先する。TOE における TLS バージョンごとの場合の鍵交換の優先度を以下に示す。

表 28 鍵交換アルゴリズムの優先度

#	鍵交換アルゴリズム	鍵長	優先度_TLS1.3	優先度_TLS1.2	ffdhe グループ	楕円曲線
1	DHE	2048bit*	—	4	-	-
2		3072bit	5	—	ffdhe3072	-
3		4096bit	3	—	ffdhe4096	-
4	ECDHE	256bit	4	3	-	secp256r1
5		384bit	2	2	-	secp384r1

6		521bit	1	1	-	secp521r1

*鍵長 2048bit の DHE を使用する鍵交換は TLS 1.2 の通信時にのみ使用可能である。

TOE は表 28 に示す優先度に基づいて使用する鍵長などを選択すると、ルールに基づいて選択した鍵合意パラメータを TLS1.2 の場合は Server Key Exchange で、TLS1.3 の場合は Key Share Extension でクライアントへ通知する。

TOE においてサポートされている署名アルゴリズムを以下に示す。

表 29 サポートしている署名アルゴリズム

#	署名アルゴリズム	鍵長
1	RSA	2048 bit
2		3072 bit
3		4096 bit
4	ECDSA	256bit
5		384bit
6		521bit

TOE は Early data extension の拡張を禁止する。

TOE は、TOE 自身の認証に RSA の鍵ペアおよび、ESDSA の鍵ペアの証明書を使用できる。サポートする RSA の鍵長および ECDSA の楕円曲線は以下の通り。

・RSA：2048bit/3072bit/4096bit

・ECDSA：secp256r1/secp384r1/secp521r1

7.3. 識別と認証(FIA)

7.3.1. FIA_AFL.1

TOE は、リモート管理者による Web GUI または REST API からの認証失敗を追跡する。セキュリティ管理者(参照・編集)が定義した回数(1 回~999 回)以上に認証に連続して失敗した管理者アカウントは、セキュリティ管理者(参照・編集)が定義した時間(60 秒~345600 秒)ロックされる。なお、連続した認証失敗回数は管理者アカウントに紐づく。

TOE はロックされた管理者アカウントに対して認証試行は許可するが、常に認証失敗を応答する。ロックされたユーザはロック時間が経過することで再度 TOE にアクセスできる。なお、ロックされる対象の管理者アカウントは認証に失敗した当該管理者アカウントのみで他の管理者アカウントはログインできる。

ローカル接続を使用する場合にはアカウントロック機構は適用されない。このため全ユーザアカウントがロックされてしまった場合でも、ローカル管理によって TOE の管理機能が提供される。

7.3.2. FIA_PMG_EXT.1

TOE は、管理者アカウントのパスワード管理機能を有する。

管理者パスワードの文字種は、英大文字と英小文字、数字、特殊文字「！」「@」「#」「$」「%」「^」「&」「*」「(」「)」「"」「'」「+」「,」「-」「.」「/」「:」「;」「<」「=」「>」「?」「[」「¥」「]」「_」「`」「{」「|」「}」「~」の任意の組み合わせで構成することができる。
パスワードの最小文字数は、セキュリティ管理者(参照・編集)によって 6~63 文字で設定を変更可能であり、セキュリティ管理者(参照・編集)の設定した文字長より短い文字長でのパスワードは設定できない。なお、最大文字数は 63 文字固定である。

7.3.3. FIA_UIA_EXT.1

TOE は TOE へのリモートからの管理者アクセスのために Web GUI と REST API のインタフェースを提供するが、各インタフェースにアクセスするためには、管理者はユーザ ID とパスワードを使用して、識別・認証される必要がある。Web GUI では、テキストボックスにユーザ ID とパスワードを入力しログインボタンを押す。REST API では、ユーザ ID とパスワードを含め POST メソッドを発行しセッションを取得する。Web インタフェースおよび REST API インタフェースともに管理 PC からのリモート接続で使用する。
また、TOE は TOE へのローカルからの管理者アクセスのために Web GUI を提供しており、管理者はユーザ ID とパスワードをテキストボックスに入力しログインボタンを押して、識別・認証される必要がある。

TOE は、ICMP echo 要求を受領した際、要求元が識別/認証された管理者または IT エンティティか否かに関わらず ICMP echo 要求に応答する。また、認証前の管理者が Web GUI にアクセスした際、Web GUI 上にはストレージ管理者(初期設定)が事前に設定するメッセージをログイン画面のアクセスバナー上に表示する。ログインに成功すると管理画面を表示する。
REST API を使用する場合、識別・認証前の管理者には以下のコマンドのみ提供し、TOE セキュリティ機能は提供しない。
・REST API のバージョン情報の取得
・ディスクストレージ装置の一覧情報の取得
認証後の管理者には、TOE セキュリティ機能を含む各種設定/参照機能を提供する。

7.3.4. FIA_UAU.7

ローカル管理を行う際、ログイン画面に表示されるパスワードは秘匿文字で表示される。

7.3.5. FIA_X509_EXT.1/Rev

TOE は以下のタイミングで X.509 証明書の検証を行う。
(a) 各種証明書のインポート時
(b) TLS ハンドシェイク時

検証対象の証明書がチェーン証明書の場合でもリーフ証明書のみの場合でも、TOE は証明書チェーンに含まれるすべての証明書の検証を行い、いずれか 1 つの証明書でも検証条件を満たさない場合は証明書検証失敗とする。このため、検証対象の証明書がチェーン証明書の場合でもリーフ証明書のみの場合でも、検証内容や結果が変わることはない。また、インポート時および、ハンドシェイク時に署名検証を行い、証明書がトラストアンカーまで正しくつながっていることを検証する。TOE は 3 段以上の証明書チェーン検証をサポートする。

(a) 証明書のインポート時に実施する検証項目を以下に示す。
TOE にはルート証明書からのチェーン構成を含む Web サーバ証明書、監査ログサーバ(正・副)のクライアント証明書、監査ログサーバ(正・副)のルート証明書を 1 つずつインポートすることができ、インポートした証明書は TOE 内で用途ごとに管理される。サーバ証明書を証明書チェーンでアップロードする際にチェーンの終端が CA 証明書であることを検証する。監査ログサーバ証明書設定時で、クライアント証明書を証明書チェーンでアップロードする際にチェーンの終端が CA 証明書であることを検証する。各証明書のインポート時、TOE は以下の検証項目を 1 つでも満たさない証明書はインポートしない。

i. 証明書チェーンに含まれるすべての証明書の署名検証
ii. basicConstraints の CA フラグの検証(CA 証明書には CA フラグが TRUE に設定されていることの検証)

(b) TLS ハンドシェイク時に実施する検証項目を以下に示す。
TOE は以下の検証項目を満たさない場合、セキュア通信を確立しない。監査ログサーバのサーバ証明書を受領した際は、あらかじめ監査ログサーバ設定画面で登録されていたルート証明書までチェーンが構成されていることを検証する。なお、以下 iv 記載の失効検証は、OCSP の場合 RFC6960 に準拠しており、CRL の場合 RFC5280 に準拠した検証を行う。

I. TOE がサーバになる場合
TOE がサーバになる場合、サーバ証明書の検証はクライアント側で実施されるため、TOE はハンドシェイク時にいずれの証明書の検証も実施しない。

II. TOE がクライアントになる場合
i. 証明書の有効期限検証
ii. 証明書の署名検証(チェーン検証)
iii. basicConstraints の検証
① basicConstraints 拡張領域が存在し、CA フラグが”TRUE”であること
② basicConstraints 拡張領域が存在し、CA フラグが”FALSE”であること
iv. OCSP/CRL を使用した失効検証

v. extendedKeyUsage の検証
① Server Authentication Purpose の検証
② OCSP Signing Purpose の検証(OCSP)

上記検証をどの証明書に対して行うかは、下記の表のとおりである。

表 30 TLS ハンドシェイク時の検証内容と対象の証明書

証明書 / (b) 検証項目	I. TOE がクライアントになる場合				
	監査ログサーバのサーバ証明書	監査ログサーバ向けのクライアント証明書	監査ログサーバのサーバ証明書チェーンに含まれるルート CA 証明書	監査ログサーバのサーバ証明書チェーンに含まれる中間 CA 証明書	OCSP レスポンダ証明書
i	○	×	×	○	○
ii	○	×	×	○	○
iii①	×	×	×	○	×
iii②	○	×	×	×	×
iv	○	×	×	○	×
v ①	○	×	×	×	×
v ②	×	×	×	×	○

凡例 ○：検証対象
×：検証対象外

TOE は監査ログサーバのサーバ証明書、監査ログサーバのサーバ証明書チェーンに含まれる中間 CA 証明書の失効状態について、OCSP または CRL を用いて検証する機能をサポートしている。
OCSP を用いた失効検証を行うためには、図 1 に示す通り TOE の利用環境に OCSP レスポンダを設置し、ネットワーク接続されている必要がある。また、失効検証の対象にしたい証明書の AuthorityInfoAccess 拡張領域に OCSP の URL が設定されている必要がある。
CRL を用いた失効検証を行うためには、図 1 に示す通り TOE の利用環境に CRL DP(Distribution Point)サーバを設置し、ネットワーク接続されている必要がある。また、

失効検証の対象にしたい証明書の CRL DP 拡張領域に CRL DP サーバの URL が設定されている必要がある。
証明書に AuthorityInfoAccess 拡張領域の情報も CRL DP 拡張領域の情報も含まれる場合、TOE は OCSP の失効検証を優先する。OCSP レスポンダから失効チェックの応答を取得できた場合、TOE はその情報で失効を判断する。OCSP レスポンダとの接続が確立できない場合、TOE は次に CRL DP へアクセスして CRL を取得し失効チェックを行う。CRL DP から CRL を取得できた場合、TOE はその情報で失効を判断する。CRL DP との接続が確立できない場合失効検証は失敗する。
失効検証に失敗した場合、TOE は失効検証対象だった証明書を受け入れず、対象の証明書を提示した IT エンティティとの通信を確立しない。

OCSP レスポンダ証明書または CRL の署名検証は、OCSP レスポンスまたは CRL を発行した CA 機関の証明書、すなわち(ウ)または(エ)の証明書を使用する。

TOE は以下の extendedKeyUsage はサポートしていない。
・Code Signing purpose
・Client Authentication purpose

7.3.6. FIA_X509_EXT.2

TOE は HTTPS/TLS 通信時に RFC5280 に準拠した x509v3 証明書の SAN(subjectAlternativeName)拡張領域を使用して通信相手の機器認証を行う。SAN 拡張領域を使用した機器認証の詳細については 7.2.10 を参照。
また、7.3.5 にも記載の通り、TOE には Web サーバ証明書、監査ログサーバ(正・副)のクライアント証明書、監査ログサーバ(正・副)のルート証明書を 1 つずつインポートすることができ、TOE はそれぞれ 1 世代のみを管理する。このため、どの証明書を使用するか、通信する対象によって一意であり、TOE は通信時に証明書を選択するような挙動を行わない。
TOE が証明書を利用するための運用環境を構築するためには、証明書要求を署名するためのプライベート CA 認証局が必要となる。TOE の利用者は構築したプライベート CA 認証局に証明書要求を送付して署名付きの証明書を取得し、TOE にインポートする。
OCSP/CRL を使用した失効検証を実施する場合には、図 1 に示す通り TOE の利用環境として OCSP レスポンダや CRL DP サーバ を TOE と接続する必要がある。
失効検証に OCSP レスポンダまたは CRL DP サーバのどちらかのみ使用する際、TOE が対向エンティティとの通信が確立できない場合、失効検証は失敗する。OCSP レスポンダと CRL DP サーバの両方を使用する際、OCSP レスポンダと CRL DP サーバのいずれとも通信できない場合、失効検証は失敗する。

7.3.7. FIA_X509_EXT.3

TOE は Web GUI を介して、RFC2986 で規定された CSR を生成するインタフェースを提供する。TOE で CSR を作成する際、CSR には以下の内容を含めることができる(国内向け TOE の画面表記を括弧内に示す)。なお、CSR には公開鍵も含まれる。

・Country Name(国名)
・Organization Name(組織名)
・Organization Unit Name(部門名)
・Common Name (一般名)

TOE は 7.3.5 に記載の通り、証明書をインポートした際に対象の証明書チェーンに含まれるすべての証明書の署名検証を行う。

7.4. セキュリティ管理(FMT)

TOE は操作とロールの対応表を内部に持っており、管理者がある操作を要求した場合に、管理者のロールを基に対象の操作の実行可否を判断する。

7.4.1. FMT_MOF.1/ManualUpdate

TOE は、ファームウェアアップデートを実行する能力をファームウェア更新の実行権限を持つ保守(ユーザ)のみに制限しており、他の管理者の使用するインタフェースからはファームウェアのアップデートを行うことができない。

詳細は 7.4.5 FMT_SMF.1 の表 31 参照。

7.4.2. FMT_MOF.1/Functions

TOE は、監査記録の外部監査サーバへの送信を変更（有効／無効）する能力を監査ログ管理者(参照・編集)に制限しており、他の管理者の使用するインタフェースからは変更できない。

詳細は 7.4.5 FMT_SMF.1 の表 31 参照。

7.4.3. FMT_MTD.1/CoreData

TOE は以下を管理する能力をセキュリティ管理者(参照・編集)に制限しており、他の管理者の使用するインタフェースから管理できない。

・ロールとユーザグループを関連付けたユーザグループの作成
・ユーザの作成（ユーザ ID 及びパスワードの設定、ユーザグループの関連付け）
・管理者パスワードの最小パスワード長設定
・管理者による自身のパスワードの変更
・パスワードのリセット(他者のパスワードの変更)
・管理者セッション終了までの非アクティブ時間の設定

・管理者の認証失敗回数の設定、認証失敗時に再認証可能になるまでの時間の設定
・Web サーバのサーバ証明書のインポート
・TOE のトラストストアへ Web サーバ証明書のルート証明書をインポート/トラストストアから Web サーバ証明書のルート証明書を削除(上書きによって)

TOE は以下を管理する能力を監査ログ管理者(参照・編集)に制限しており、他の管理者の使用するインタフェースからは管理できない。
・管理者による自身のパスワードの変更
・監査ログサーバの設定
・監査ログサーバのクライアント証明書のインポート
・TOE のトラストストアへ監査ログサーバ証明書のルート証明書をインポート/トラストストアから監査ログサーバ証明書のルート証明書を削除(上書きによって)

TOE は以下を管理する能力をストレージ管理者(初期設定)に制限しており、他の管理者の使用するインタフェースからは管理できない。
・管理者による自身のパスワードの変更
・アクセスバナーに表示するメッセージの設定
・日付と時刻の設定

TOE は以下を管理する能力を保守(ユーザ)に制限しており、他の管理者の使用するインタフェースからは管理できない。
・管理者による自身のパスワードの変更

詳細は 7.4.5 FMT_SMF.1 の表 31 参照。

なお、以 7.3.3 FIA_UIA_EXT.1 で示す通り、以下の各機能は管理者の認証前に提供されるが、以下機能は情報の GET リクエストや ICMP への応答のみであり、TSF データを書き換えることはできない。また、GET リクエストでアクセスするアドレスは TSF データが含まれる情報を持たないため、以下機能を使用して TSF データを読み出すことはできない。

- Web GUI でログイン画面へのアクセスおよびログイン画面のアクセスバナー上に表示されるメッセージの参照
- ICMP echo
- 以下の REST API を使用した GET リクエスト
    - /configuration/version
    - /configuration/storages

7.4.4. FMT_MTD.1/CryptoKeys

TOE は、X.509 証明書要求(CSR)や RSA・ECDSA 鍵の生成を行う管理能力を、Web GUI を介してセキュリティ管理者(参照・編集)に制限しており、他の管理者の使用するインタフェースからは生成できない。

TOE に証明書をインポートするときは、検証の為にチェーン構成の証明書をアップロードする必要がある。

TOE にインポートする証明書は、証明書の種類によってインポートするために必要なロールが異なる。各証明書のインポート操作に必要なロールを下記に示す。下記のロール以外の他の管理者の使用するインタフェースからは操作できない。

・監査ログサーバのルート証明書/クライアント証明書(ルート証明書からのチェーン構成を含む):監査ログ管理者(参照・編集)

・TOE の Web サーバ証明書(ルート証明書からのチェーン構成を含む):セキュリティ管理者(参照・編集)

詳細は 7.4.5 FMT_SMF.1 の表 31 参照。

7.4.5. FMT_SMF.1

TOE は WebGUI または REST API のリモート管理インタフェースを介して以下に示す管理機能を管理者へ提供する。また、TOE は WebGUI のローカル管理インタフェースを介して以下に示す管理機能を管理者へ提供する。(すべての WebGUI 管理画面はリモート管理インタフェースでも、ローカル管理インタフェースでも同様に提供される)

なお、ローカル管理インタフェースを使用するためには、TOE と管理 PC を LAN ケーブルで直結する必要がある。

表 31 管理操作とインタフェースとロールの対応表

#	管理機能	インタフェース		操作に必要なロール
		Web GUI 画面	REST API コマンド	
Ability to administer the TOE remotely				
1	ロールとユーザグループを関連付けたユーザグループの作成	—	/v1/objects/user-groups	セキュリティ管理者(参照・編集)
2	ユーザの作成(ユーザ ID 及びパスワードの設定、ユーザグループの関連付け)	[Maintenance Utility] - [管理] - [ユーザ管理画面]	/v1/objects/users	セキュリティ管理者(参照・編集)

3	管理者パスワードの最小パスワード長設定	[Maintenance Utility] - [管理] – [ユーザアカウントポリシー]	—	セキュリティ管理者(参照・編集)
4	管理者による自身のパスワードの変更	[Maintenance Utility] - [メニュー] - [システム管理] – [パスワード変更]	—	セキュリティ管理者(参照・編集)、ストレージ管理者(初期設定)、監査ログ管理者(参照・編集)、保守(ユーザ)
5	パスワードのリセット(他者のパスワードの変更)	[Maintenance Utility] - [管理] - [ユーザ管理画面]	—	セキュリティ管理者(参照・編集)
Ability to configure the access banner				
6	アクセスバナーに表示するメッセージの設定	[Maintenance Utility] - [メニュー] - [システム管理] - [ログインメッセージ編集画面]	—	ストレージ管理者(初期設定)
Ability to configure the remote session inactivity time before session termination/Ability to configure the local session inactivity time before session termination or locking				
7	リモート/ローカル管理者セッション終了までの非アクティブ時間の設定(Web インタフェース)	[Maintenance Utility] - [メニュー] – [システム管理] – [セッションタイムアウト時	—	セキュリティ管理者(参照・編集)

		間]		
Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates				
8	TOE のファームウェアアップデートとアップデート対象ファームウェアの検証	[Maintenance Utility] - [管理] - [ファームウェア画面]	—	保守(ユーザ)
Ability to configure the authentication failure parameters for FIA_AFL.1				
9	管理者の認証失敗回数の設定、認証失敗時に再認証可能になるまでの時間の設定	[Maintenance Utility] - [管理] – [ユーザアカウントポリシー]	—	セキュリティ管理者(参照・編集)
Ability to modify the behavior of the transmission of audit data to an external IT entity				
10	監査ログサーバへの送信の有効/無効	[Maintenance Utility] - [管理] - [監査ログ設定画面]	—	監査ログ管理者(参照・編集)
Ability to manage the cryptographic keys Ability to generate Certificate Signing Request (CSR) and process CA certificate response;				
11	CSR 及び RSA・ECDSA 鍵の作成/削除	[Maintenance Utility] - [メニュー] - [システム管理] – [CSR 作成および自己署名証明書作成]	—	セキュリティ管理者(参照・編集)
12	監査ログサーバの設定 ・クライアント証明書のインポート（クライアント証明書のインポート時にルート証明書および中間 CA 証明書を含むチェーン構成でインポートする）※1	[Maintenance Utility] - [管理] - [監査ログ設定画面]	—	監査ログ管理者(参照・編集)
13	TOE の Web サーバ証明書の更新 ・Web サーバ証明書のインポート（Web サーバ証明書のインポート	[Maintenance Utility] - [メニュー] –	—	セキュリティ管理者(参照・編

	時にルート証明書および中間 CA 証明書を含むチェーン構成でインポートする）※1	[システム管理] – [証明書ファイル更新]		集)
Ability to set the time which is used for time-stamps				
14	以下で使用する日付と時刻の設定 ・タイムスタンプの記録 ・証明書の有効期限の検証	[Maintenance Utility] - [管理] - [日時設定画面]	—	ストレージ管理者(初期設定)
Ability to configure the reference identifier for the peer				
15	監査ログサーバの設定 ・IP アドレス （正/副 2 台まで設定可能）	[Maintenance Utility] - [管理] - [監査ログ設定画面]	—	監査ログ管理者(参照・編集)
Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors				
16	監査ログサーバのルート CA 証明書(中間 CA 証明書またはサーバ証明書を署名)インポート(監査ログサーバの正/副 2 台までインポート可能)※1	[Maintenance Utility] - [管理] - [監査ログ設定画面]	—	監査ログ管理者(参照・編集)
17	TOE の Web サーバ証明書のルート証明書のインポート(Web サーバ証明書のインポート時にルート証明書および中間 CA 証明書を含むチェーン構成でインポートする）※1	[Maintenance Utility] - [メニュー] – [システム管理] – [証明書ファイル更新]	—	セキュリティ管理者(参照・編集)

※1　すでに証明書がインポートされている状態で新しい証明書のインポートを行うと、古い証明書が削除され新しい証明書に変更されます。

7.4.6. FMT_SMR.2

TOE では、セキュリティ管理者(参照・編集)、ストレージ管理者(初期設定)、監査ログ管理者(参照・編集)、保守(ユーザ)のロールを設定したユーザグループに対してユーザを関連付けることでユーザを作成する。さらに、当該ユーザのログイン時にロールが関連付けられその関連付けがログアウトするまで持続する。TOE はこれらによりユーザとロールの関連付けを維持する。

各セキュリティ管理者は TOE をリモート管理することができる。

TOE の管理操作に必要なロールについては 7.4.5 FMT_SMF.1 の表 31 参照。

7.5. TSF の保護(FPT)

7.5.1. FPT_SKP_EXT.1

7.2.3 FCS_CKM.4 に記載した表 17 の通りに各鍵を RAM 上または SSD 上に保存している。TOE は RAM 上/SSD 上の鍵を参照するインタフェースを利用者向けに提供しない。

7.5.2. FPT_APW_EXT.1

各管理者のパスワード情報は、TOE 内でハッシュ化されて保存されるため、平文パスワードを参照することはできない。また、TOE はパスワードを読み出すためのローカル/リモート管理インタフェースを提供しない。なお、管理者パスワードのハッシュ化は PBKDF2(Password-Based Key Derivation Function 2)を使用しており、PBKDF2 内で使用するハッシュ関数には SHA512 を指定している。

7.5.3. FPT_TST_EXT.1

TOE は装置起動時に以下に記載する自己テストを実施する。

a) ファームウェアのインテグリティテスト

b) 下記の暗号アルゴリズムの既知解テスト

(ア) AES

(イ) DRBG

(ウ) RSA

(エ) ECDSA

(オ) HMAC

(カ) DH

(キ) ECDH

a)のテストでは公開鍵を使用してファームウェアに付随するディジタル署名を検証することでファームウェアの完全性をテストする。前述の公開鍵は、ファームウェアの署名を検証するために、TOE に予めインストールされている鍵である。もしファームウェアが改ざんされているなど完全でない場合には、ディジタル署名での検証テストに失敗する。失敗時は、リブートを行うことで検証テストを再実施する。ファームウェアの検証対象には、OS やカーネルなどを含む TSF を構成するファームウェア全体が含まれる。TSF の動作基盤となる OS やカーネルを含むファームウェア全体のインテグリティテストを実施しており、インテグリティテストを実施することで TSF の各機能が完全な状態で提供可能であることを保証できる。

b)のテストでは TOE が提供する各暗号アルゴリズムに対して既知解テストを実施する。暗号アルゴリズムの出力が既知解と異なる場合には、暗号機能が正しく動作していないため

テストに失敗する。失敗時は、リブートを行うことで既知解テストを再実施する。TSF が利用する TOE の暗号機能を構成する全ての暗号アルゴリズムを既知解テストしており、本テストを実施することで TOE の暗号機能が正しく動作することを保証できる。
上記のテストは、オペレーティング・システムと各ファームウェアに変更が加えられていないこと、テスト済みのコードのみが TSF によって実行されていること、基盤となるハードウェアが OS をロードし、各既知解テストを正しく処理できることを確認することで、デバイスの正しい動作を実証する。
テスト失敗時には TOE は TOE 自身の起動を抑止しファームウェアが完全でない旨の SIM(Service Information Message)を記録した上で、システムをリブートさせる。リブート時にも a)および b)のテストを実施する。TOE が正常に起動した場合、TOE のファームウェアに異常がないこと及び TOE の提供する暗号機能が正しく動作し、正しく動作する TSF が提供できることを保証する。

7.5.4. FPT_TUD_EXT.1

TOE は全てのロール(セキュリティ管理者(参照・編集)/ストレージ管理者(初期設定)/監査ログ管理者(参照・編集)/保守(ユーザ))が Web GUI からバージョンを確認した際に、TOE は現在アクティブな TOE バージョンを応答する。
ファームウェア更新の実行権限を持つ保守(ユーザ)は管理 PC から更新対象のファームウェアのメディアを使用してファームウェアの手動更新を行う。ファームウェア検証内容は、装置起動時に行う完全性検証の内容と同等であり、検証方法は 7.5.3 FPT_TST_EXT.1 に記載している。
保守(ユーザ)がファームウェアの手動更新を Web GUI から指示すると、TOE はファームウェア更新処理の前に完全性検証を行い、完全性検証に成功するとファームウェア更新処理を行う。ファームウェアの完全性検証に失敗する場合、TOE は FW 更新処理を実施しない。更新されたファームウェアはインストールが完了した直後からアクティブとなる。

7.5.5. FPT_STM_EXT.1

TOE の以下の機能では日付と時刻が利用される。
a) 監査レコードに記録するタイムスタンプ機能
b) 証明書の有効期限検証機能
TOE は、上記の 2 機能で利用される日付と時刻を管理するために内部時計を内蔵している。日付と時刻の設定変更はストレージ管理者(初期設定)のみがリモート管理インタフェースおよびローカル管理インタフェースから実施可能であり、TOE は日付と時刻の設定変更が行われた際に監査ログに記録する。
a)及び b)の機能は内部時計を使用し、TOE が内蔵する RTC (Real Time Clock)が正確な時刻を提供するため、信頼できる日付と時刻で監査ログが記録され、また信頼できる日付と時

刻で証明書の有効期限が検証される。

7.6. TOE アクセス(FTA)

7.6.1. FTA_SSL.3

Web インタフェースの場合、TOE は、指定された時間経過後に、非アクティブなリモートの Web インタフェースのセッションを終了させる。タイムアウト値はセキュリティ管理者(参照・編集)が 60 分、90 分、120 分の中から設定することができる。
REST API の場合、指定された時間経過後に、非アクティブなリモートの REST API インタフェースのセッションを終了させる。REST API のセッションタイムアウト時間は、セッションを生成する際に各管理者が 1 秒～300 秒の間で設定することができる。

7.6.2. FTA_SSL.4

Web インタフェースの場合、管理者は Web GUI でログアウト操作をすることで、いつでも自分のセッションを終了させることができる。
REST API の場合、管理者は自身のログイン時に TOE によって発行されたセッション情報(トークン)を提示してセッション終了の操作を行うことによっていつでもログアウトすることができる。Web インタフェースおよび REST API インタフェースともに管理 PC からのリモート接続で使用する。

7.6.3. FTA_SSL_EXT.1

ローカル接続セッションは、指定された時間経過後に、非アクティブなローカルの Web インタフェースのセッションを終了させる。タイムアウト値はセキュリティ管理者(参照・編集)が 60 分、90 分、120 分の中から設定することができる。

7.6.4. FTA_TAB.1

TOE を管理するための各リモートインタフェースおよびローカルインタフェースについて、ログイン前のメッセージに関する実装を以下に記載する。
a)Web インタフェースの場合
TOE は、ストレージ管理者(初期設定)が事前に設定する TOE の使用に関する注意事項や警告メッセージを、Web GUI でのログイン前にログイン画面のバナー上に表示する。本挙動はリモートインタフェースでもローカルインタフェースでも同じである。
b) REST API インタフェースの場合
TOE は、リモート管理インタフェースを介した REST API でのアクセス時にはログイン前のメッセージ表示をしない。

7.7. トラステッドパス/チャネル(FTP)

7.7.1. FTP_ITC.1

TOE は、監査ログサーバへの監査ログの送信のために TLS 通信を使用したセキュアな通信をサポートする。また、TOE は監査ログサーバから送付されるサーバ証明書について 7.3.5 FIA_X509_EXT.1/Rev に示す通りに証明書検証を行うことで通信相手となる監査ログサーバを保証する。サーバ証明書の識別方法は 7.2.10FCS_TLSC_EXT.1 に記載している。
また、TOE は監査ログサーバとの TLS 通信時に相互認証を行う。監査ログサーバとの相互認証に関する要約仕様は 7.2.11FCS_TLSC_EXT.2 に記載している。

7.7.2. FTP_TRP.1/Admin

TOE は Web GUI および REST API を使用した TOE 管理者による TOE のリモート管理の提供のために、HTTPS 通信を使用したセキュアな通信をサポートする。すなわち、管理者のログイン認証時を含む全ての操作アクションに対して HTTPS 通信を提供する。

8. 用語

8.1. ST 専門用語

Administrator	Security Administrator を参照。
TOE セキュリティ機能 (TOE security functionality)	SFR の正しい実施のために信頼されなければならない TOE のすべてのハードウェア、ソフトウェア、及びファームウェアの複合機能。[CC パート 1 の用語]
TSF データ	SFR 実施が依存する TOE のふるまいのためのデータ。[CC パート 1 の用語]
SAN	Subject Alternative Name の略。X.509 v3 証明書における拡張フィールドの一つ。SAN を使うことで、1 つの証明書で複数のドメイン名や IP アドレスをまとめて証明できる。
Security Administrator	本書では、「Administrator」と「Security Administrator」という用語は現時点では同一の意味で使用しており、TOE に対して設定および管理作業を実施するための正当なアクセス権限を有する者。
SIM	Service Information Message の略。ディスクストレージ装置の保守が必要な際に Maintenance Utility 上に出力されるメッセージ。
運用環境	TOE が運用される環境。[CC パート 1 の用語]
外部エンティティ	TOE の外部にあって TOE と対話することができる人間

	または IT のエンティティ。[CC パート 1 の用語]
脅威エージェント （threat agent）	資産において悪影響を及ぼす行為を行うことのできるエンティティ。[CC パート 1 の用語]
繰り返し	複数の異なる要件を表現するために同じコンポーネントを使用すること。[CC パート 1 の用語]
高信頼チャネル	TSF と遠隔の信頼できる IT 製品が、必要な信頼をもって通信することができる手段。[CC パート 1 の用語]
高信頼パス	利用者と TSF が必要な信頼をもって通信する手段。[CC パート 1 の用語]
コントローラシャーシ	TOE のコントローラボード、ドライブ、電源を搭載する筐体である。
詳細化	コンポーネントに詳細を追加すること。[CC パート 1 の用語]
選択	コンポーネント内のリストから 1 つまたは複数の項目を特定すること。[CC パート 1 の用語]
組織のセキュリティ方針	組織に対するセキュリティ規則、手続き、またはガイドラインのセット。[CC パート 1 の用語]
セキュリティ課題	TOE が対処しようとする特性やセキュリティの範囲を、形式的な作法で定義するステートメント。[CC パート 1 の用語]
セキュリティ対策方針	識別された脅威に対抗すること、及び/または識別された組織のセキュリティ方針及び/または前提条件を満たすことを目的とするステートメント。[CC パート 1 の用語]
セキュリティ要件	TOE のセキュリティ対策方針の達成に貢献するために、標準化された言語によって述べられる要件。[CC パート 1 の用語]
ドライブボックス	ドライブを搭載する筐体。TOE はコントローラシャーシにもドライブを搭載できるが、システムのドライブ容量を拡張するためにコントローラシャーシに接続可能な筐体である。 なお、本筐体はドライブへのデータの書き込みを行うのみで、本 ST に記載する SFR を提供する機能を持たない。
評価対象 (target of evaluation)	ガイダンスを伴うことがあるソフトウェア、ファームウェア、及び/またはハードウェアのセット。[CC パート

	1 の用語]
ファイバチャネル/iSCSI	Storage Area Network を構築するための高速ネットワークテクノロジー。
プロテクションプロファイル	TOE の種別に対するセキュリティニーズについての実装に依存しないステートメント。[CC パート 1 の用語]
要件拡張	CC のパート 2 に含まれていない機能要件、及び/または CC のパート 3 に含まれていない保証要件を、ST または PP に追加すること。[CC パート 1 の用語]
割付	(CC の)コンポーネントまたは要件内の識別されたパラメータを特定すること。[CC パート 1 の用語]
Maintenance Utility	ストレージシステムやネットワークの設定、ユーザ情報やライセンスキーを管理することができる Web GUI である。
VSP One Block Administrator	ストレージシステムの構成やリソースを操作することができる Web GUI である。

8.2. 略語

この文書では次の略語が使われている。

API	Application Programming Interface
CC	Common Criteria
cPP	collaborative PP
CRL	Certificate Revocation List
CRL DP	CRL Distribution Point
CSR	Certificate Signing Request
DKC	Disk Controller
ESM	Embedded Storage Manager
FIPS	Federal Information Processing Standardization
FW	Firmware
GMT	Greenwich Mean Time
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
LAN	Local Area Network
NDcPP	collaborative Protection Profile for Network Devices
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication

OCSP	Online Certificate Status Protocol
PC	Personal Computer
PP	Protection Profile
REST	Representational State Transfer
REST API	RESTful API
RFC	Request for Comments
SAN	Subject Alternative Name
SIM	Service Information Message
SSD	Solid State Drive
SSL	Secure Sockets Layer
ST	Security Target
SFR	Security Functional Requirement
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE security functionality
VSP	Virtual Storage Platform