# AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 セキュリティターゲット

**Version:** 1.7.15
**Last Updated:** 2026/04/13

**Prepared by**

https://www.cybertrust.co.jp

## 変更履歴

| Version | 日付 | 修正者 | 変更履歴 |
|---|---|---|---|
| 0.0.0 | 2024/09/02 | 田中 | ドラフト版作成 |
| 0.1.0 | 2024/10/01 | 田中 | ORに対する修正（ドラフト版） |
| 0.2.0 | 2024/10/25 | 田中 | ORに対する修正（ドラフト版） |
| 0.3.0 | 2024/10/30 | 田中 | ORに対する修正（ドラフト版） |
| 0.3.1 | 2024/11/25 | 田中, 三上 | 第7章修正（ドラフト版） |
| 0.3.2 | 2024/12/25 | 田中, 三上, 弦本 | ORに対する修正（ドラフト版） |
| 0.4.0 | 2025/02/02 | 田中, 三上, 弦本 | ORに対する修正（ドラフト版） |
| 0.5.0 | 2025/03/10 | 田中, 弦本 | ORに対する修正（ドラフト版） |
| 0.5.1 | 2025/03/14 | 田中 | ORに対する修正（ドラフト版）<br>第1章から第6章の誤記修正（ドラフト版） |
| 0.5.2 | 2025/03/19 | 田中 | ORに対する修正（ドラフト版） |
| 0.6.0 | 2025/03/27 | 田中 | 第7章の誤記修正（ドラフト版） |
| 1.0.0 | 2025/03/28 | 田中 | 初版 |
| 1.0.1 | 2025/04/24 | 田中 | ORに対する修正 |
| 1.1.0 | 2025/05/16 | 田中, 三上 | ORに対する修正 |
| 1.2.0 | 2025/05/30 | 田中, 三上 | ORに対する修正 |
| 1.2.1 | 2025/06/06 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.2 | 2025/06/13 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.3 | 2025/06/20 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.4 | 2025/06/27 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.5 | 2025/07/02 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.6 | 2025/07/03 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.7 | 2025/07/04 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.8 | 2025/07/11 | 田中, 三上, 松田 | ORに対する修正 |
| 1.2.9 | 2025/07/18 | 田中, 三上, 松田 | ORに対する修正 |
| 1.3.0 | 2025/07/29 | 田中, 三上, 松田 | ORに対する修正 |

| | | | |
|---|---|---|---|
| 1.3.1 | 2025/08/01 | 田中, 三上, 松田 | ORに対する修正 |
| 1.3.2 | 2025/08/06 | 田中, 三上, 松田 | ORに対する修正 |
| 1.3.3 | 2025/08/14 | 田中, 三上, 松田 | ORに対する修正 |
| 1.3.4 | 2025/08/21 | 三上, 田中 | パスワード長に関する記載を修正<br>RPMパッケージリストのソート |
| 1.3.5 | 2025/08/27 | 三上, 田中, 松田 | ORに対する修正<br>誤記および体裁の修正 |
| 1.4.0 | 2025/08/29 | 三上, 田中, 松田 | ORに対する修正 |
| 1.4.1 | 2025/09/03 | 三上, 田中 | ORに対する修正 |
| 1.4.2 | 2025/09/05 | 三上 | 誤記および体裁の修正 |
| 1.4.3 | 2025/09/10 | 田中 | ORに対する修正 |
| 1.4.4 | 2025/09/17 | 田中 | ORに対する修正 |
| 1.4.5 | 2025/09/22 | 三上, 田中 | ORに対する修正 |
| 1.4.6 | 2025/09/25 | 三上, 田中 | ORに対する修正 |
| 1.4.7 | 2025/09/29 | 三上, 田中 | ORに対する修正 |
| 1.4.8 | 2025/10/01 | 三上, 松田, 田中 | ORに対する修正<br>1.4.1 TOEの物理的範囲に追加パッケージの記述追加 |
| 1.5.0 | 2025/10/02 | 田中, 松田 | ORに対する修正 |
| 1.5.1 | 2025/10/03 | 三上 | 各ガイダンスのバージョン、SHA256SUM値を更新 |
| 1.5.2 | 2025/10/06 | 三上 | ORに対する修正<br>各ガイダンスのバージョン、SHA256SUM値を更新 |
| 1.5.3 | 2025/10/08 | 松田, 田中 | ORに対する修正<br>AlamLinux OS Updateパッケージの調整 |
| 1.5.4 | 2025/10/08 | 松田, 田中 | ORに対する修正<br>AlamLinux OS Updateパッケージの調整 |
| 1.5.5 | 2025/10/16 | 松田, 田中 | ORに対する修正<br>OS更新パッケージにshim-x64を追加 |
| 1.5.6 | 2025/10/20 | 松田, 田中 | 不要パッケージの削除<br>TSSの修正 |

| | | | |
|---|---|---|---|
| 1.5.7 | 2025/10/23 | 田中, 松田 | ORに対する修正<br>スタック保護に関する記述の修正<br>表記ゆれの修正 |
| 1.5.8 | 2025/10/30 | 田中, 松田 | ORに対する修正 |
| 1.5.9 | 2025/11/05 | 田中 | ORに対する修正 |
| 1.6.0 | 2025/11/10 | 田中, 松田 | ORに対する修正 |
| 1.6.1 | 2025/11/10 | 田中, 松田 | ORに対する修正 |
| 1.6.2 | 2025/11/25 | 田中, 松田 | ORに対する修正<br>パッケージURLをvault.almalinux.orgへ変更 |
| 1.6.3 | 2025/12/02 | 田中 | ORに対する修正 |
| 1.6.4 | 2025/12/15 | 田中 | 各ガイダンスのバージョンを更新 |
| 1.6.5 | 2025/12/18 | 田中, 松田 | CCガイダンスのバージョンを更新<br>TSSの誤記修正 |
| 1.6.6 | 2026/01/07 | 田中 | ORに対する修正<br>CCガイダンスのバージョンを更新 |
| 1.6.7 | 2026/01/07 | 田中 | ORに対する修正 |
| 1.6.8 | 2026/01/27 | 田中 | ORに対する修正 |
| 1.6.9 | 2026/01/28 | 田中 | ORに対する修正<br>CCガイダンスのバージョンを更新 |
| 1.7.0 | 2026/02/16 | 田中 | ORに対する修正<br>各ガイダンスのバージョンを更新 |
| 1.7.1 | 2026/02/25 | 田中, 三上 | ORに対する修正 |
| 1.7.2 | 2026/02/25 | 田中, 三上, 松田 | ORに対する修正 |
| 1.7.3 | 2026/02/26 | 田中 | ORに対する修正 |
| 1.7.4 | 2026/03/02 | 田中 | CCガイダンスのバージョンを更新 |
| 1.7.5 | 2026/03/04 | 田中 | CCガイダンスのバージョンを更新<br>誤記の修正 |
| 1.7.6 | 2026/03/05 | 田中 | CCガイダンスのバージョンを更新 |
| 1.7.7 | 2026/03/05 | 田中 | CCガイダンスのバージョンを更新 |
| 1.7.8 | 2026/03/10 | 田中 | ORに対する修正 |
| 1.7.9 | 2026/03/26 | 田中 | ORに対する修正 |

| | | | |
|---|---|---|---|
| 1.7.10 | 2026/04/04 | 田中 | ORに対する修正 |
| 1.7.11 | 2026/04/06 | 田中 | ORに対する修正 |
| 1.7.12 | 2026/04/09 | 田中 | ORに対する修正 |
| 1.7.13 | 2026/04/09 | 田中 | ORに対する修正 |
| 1.7.14 | 2026/04/10 | 田中 | ORに対する修正 |
| 1.7.15 | 2026/04/13 | 田中 | ORに対する修正 |

目次

# 1 ST概説

## 1.1 ST参照

本STの識別情報を以下に示す。

Table 1: ST識別子

| | |
|---|---|
| ST Title | AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3<br>セキュリティターゲット |
| ST Version | 1.7.15 |
| ST Date | 2026/04/13 |
| ST Author | サイバートラスト株式会社 |

## 1.2 TOE参照

TOEの識別情報を以下に示す。

Table 2: TOE識別子

| | |
|---|---|
| TOE Identifier | AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 1.00 |
| | FIPS140-3 を含むAlmaLinux OS 9.2 for x86_64のパッケージをバージョン1.00とし、以下に示す。<br><br>**RPM**パッケージ名 バージョン<br>aide 0.16-103.el9_6.2<br>attr 2.5.1-3.el9<br>bind-libs 9.16.23-31.el9_6<br>bind-license 9.16.23-31.el9_6<br>bind-utils 9.16.23-31.el9_6<br>binutils 2.35.2-63.el9<br>binutils-gold 2.35.2-63.el9<br>bzip2-libs 1.0.8-10.el9_5<br>cpp 11.5.0-5.el9_5.alma.1<br>cryptsetup 2.6.0-2.el9<br>dbus 1.12.20-8.el9<br>dbus-common 1.12.20-8.el9<br>dbus-libs 1.12.20-8.el9<br>device-mapper 1.02.202-6.el9<br>device-mapper-event 1.02.202-6.el9 |

| | | |
|---|---|---|
| | device-mapper-event-libs | 1.02.202-6.el9 |
| | device-mapper-libs | 1.02.202-6.el9 |
| | dmidecode | 3.6-1.el9 |
| | dosfstools | 4.2-3.el9 |
| | expat | 2.5.0-5.el9_6 |
| | file | 5.39-16.el9 |
| | file-libs | 5.39-16.el9 |
| | gcc | 11.5.0-5.el9_5.alma.1 |
| | glib2 | 2.68.4-16.el9_6.2 |
| | glibc | 2.34-168.el9_6.23 |
| | glibc-common | 2.34-168.el9_6.23 |
| | glibc-devel | 2.34-168.el9_6.23 |
| | glibc-gconv-extra | 2.34-168.el9_6.23 |
| | glibc-headers | 2.34-168.el9_6.23 |
| | glibc-langpack-en | 2.34-168.el9_6.23 |
| | gmp | 6.2.0-13.el9 |
| | gnutls | 3.8.3-6.el9 |
| | gnutls-dane | 3.8.3-6.el9 |
| | gnutls-utils | 3.8.3-6.el9 |
| | grub2-common | 2.06-104.el9_6.alma.1 |
| | grub2-efi-x64 | 2.06-104.el9_6.alma.1 |
| | grub2-tools | 2.06-104.el9_6.alma.1 |
| | grub2-tools-minimal | 2.06-104.el9_6.alma.1 |
| | ima-evm-utils | 1.5-3.el9 |
| | iputils | 20210202-11.el9_6.1 |
| | iwl1000-firmware | 39.31.5.1-151.3.el9_6 |
| | iwl100-firmware | 39.31.5.1-151.3.el9_6 |
| | iwl105-firmware | 18.168.6.1-151.3.el9_6 |
| | iwl135-firmware | 18.168.6.1-151.3.el9_6 |
| | iwl2000-firmware | 18.168.6.1-151.3.el9_6 |
| | iwl2030-firmware | 18.168.6.1-151.3.el9_6 |
| | iwl3160-firmware | 25.30.13.0-151.3.el9_6 |
| | iwl5000-firmware | 8.83.5.1_1-151.3.el9_6 |
| | iwl5150-firmware | 8.24.2.2-151.3.el9_6 |
| | iwl6000g2a-firmware | 18.168.6.1-151.3.el9_6 |
| | iwl6050-firmware | 41.28.5.1-151.3.el9_6 |
| | iwl7260-firmware | 25.30.13.0-151.3.el9_6 |
| | kernel | 5.14.0-284.11.1.el9_2.tuxcare.5 |
| | kernel-core | 5.14.0-284.11.1.el9_2.tuxcare.5 |
| | kernel-headers | 5.14.0-284.11.1.el9_2.tuxcare.5 |
| | kernel-modules | 5.14.0-284.11.1.el9_2.tuxcare.5 |
| | kernel-modules-core | 5.14.0-284.11.1.el9_2.tuxcare.5 |
| | keyutils | 1.6.3-1.el9 |
| | krb5-libs | 1.21.1-8.el9_6 |

| | | |
|---|---|---|
| | less | 590-5.el9 |
| | libarchive | 3.5.3-6.el9_6 |
| | libblkid | 2.37.4-21.el9 |
| | libcap | 2.48-9.el9_2 |
| | libcap-ng-utils | 0.8.2-7.el9 |
| | libdnf-plugin-subscription-manager | 1.29.45.1-1.el9_6.alma.1 |
| | libeconf | 0.4.1-4.el9 |
| | libfastjson | 0.99.9-5.el9 |
| | libfdisk | 2.37.4-21.el9 |
| | libgcc | 11.5.0-5.el9_5.alma.1 |
| | libgcrypt | 1.10.0-11.el9 |
| | libgomp | 11.5.0-5.el9_5.alma.1 |
| | libicu | 67.1-10.el9_6 |
| | libmount | 2.37.4-21.el9 |
| | libmpc | 1.2.1-4.el9 |
| | libndp | 1.9-1.el9 |
| | libnghttp2 | 1.43.0-6.el9 |
| | libnvme | 1.11.1-1.el9 |
| | libpkgconf | 1.7.3-10.el9 |
| | libqb | 2.0.8-1.el9 |
| | libsmartcols | 2.37.4-21.el9 |
| | libsss_certmap | 2.9.6-4.el9_6.2 |
| | libsss_idmap | 2.9.6-4.el9_6.2 |
| | libsss_nss_idmap | 2.9.6-4.el9_6.2 |
| | libsss_sudo | 2.9.6-4.el9_6.2 |
| | libstdc++ | 11.5.0-5.el9_5.alma.1 |
| | libtasn1 | 4.16.0-9.el9 |
| | libtevent | 0.16.1-1.el9 |
| | libuuid | 2.37.4-21.el9 |
| | libuv | 1.42.0-2.el9_4 |
| | libxcrypt-devel | 4.4.18-3.el9 |
| | libxml2 | 2.9.13-12.el9_6 |
| | libxslt | 1.1.34-13.el9_6 |
| | linux-firmware | 20250716-151.3.el9_6 |
| | linux-firmware-whence | 20250716-151.3.el9_6 |
| | lsof | 4.94.0-3.el9 |
| | lvm2 | 2.03.28-6.el9 |
| | lvm2-libs | 2.03.28-6.el9 |
| | make | 4.3-8.el9 |
| | man-pages | 5.10-6.el9 |
| | microcode_ctl | 20250211-1.20250512.1.el9_6 |
| | mlocate | 0.26-30.el9 |
| | ncurses | 6.2-10.20210508.el9_6.2 |
| | ncurses-base | 6.2-10.20210508.el9_6.2 |

| | | |
|---|---|---|
| | ncurses-libs | 6.2-10.20210508.el9_6.2 |
| | nettle | 3.10.1-1.el9 |
| | NetworkManager | 1.52.0-5.el9_6 |
| | NetworkManager-libnm | 1.52.0-5.el9_6 |
| | NetworkManager-team | 1.52.0-5.el9_6 |
| | NetworkManager-tui | 1.52.0-5.el9_6 |
| | openssh | 8.7p1-45.el9 |
| | openssh-clients | 8.7p1-45.el9 |
| | openssh-server | 8.7p1-45.el9 |
| | openssl | 3.0.7-20.el9_2.tuxcare.1 |
| | openssl-libs | 3.0.7-20.el9_2.tuxcare.1 |
| | pam | 1.5.1-26.el9_6 |
| | pciutils | 3.7.0-5.el9 |
| | pkgconf | 1.7.3-10.el9 |
| | pkgconf-m4 | 1.7.3-10.el9 |
| | pkgconf-pkg-config | 1.7.3-10.el9 |
| | postfix | 3.5.25-1.el9 |
| | procps-ng | 3.3.17-14.el9 |
| | protobuf | 3.14.0-16.el9 |
| | protobuf-c | 1.3.3-13.el9 |
| | python3 | 3.9.21-2.el9_6.2 |
| | python3-cloud-what | 1.29.45.1-1.el9_6.alma.1 |
| | python3-idna | 2.10-7.el9_4.1 |
| | python3-libs | 3.9.21-2.el9_6.2 |
| | python3-pip-wheel | 21.3.1-1.el9 |
| | python3-requests | 2.25.1-10.el9_6 |
| | python3-rpm | 4.16.1.3-37.el9 |
| | python3-setuptools | 53.0.0-13.el9_6.1 |
| | python3-setuptools-wheel | 53.0.0-13.el9_6.1 |
| | python3-subscription-manager-rhsm | 1.29.45.1-1.el9_6.alma.1 |
| | python3-urllib3 | 1.26.5-6.el9 |
| | python-unversioned-command | 3.9.21-2.el9_6.2 |
| | quota | 4.06-6.el9 |
| | rpm | 4.16.1.3-37.el9 |
| | rpm-build-libs | 4.16.1.3-37.el9 |
| | rpm-libs | 4.16.1.3-37.el9 |
| | rpm-plugin-audit | 4.16.1.3-37.el9 |
| | rpm-plugin-fapolicyd | 4.16.1.3-37.el9 |
| | rpm-plugin-selinux | 4.16.1.3-37.el9 |
| | rpm-plugin-systemd-inhibit | 4.16.1.3-37.el9 |
| | rpm-sign-libs | 4.16.1.3-37.el9 |
| | rsync | 3.2.5-3.el9 |
| | rsyslog-gnutls | 8.2102.0-111.el9 |
| | scrub | 2.6.1-4.el9 |

| | | |
|---|---|---|
| | shadow-utils | 4.9-12.el9 |
| | shim-x64 | 15.8-4.el9_3.alma.2 |
| | smartmontools | 7.2-6.el9 |
| | sqlite-libs | 3.34.1-8.el9_6 |
| | squashfs-tools | 4.4-10.git1.el9 |
| | sssd-client | 2.9.6-4.el9_6.2 |
| | sssd-common | 2.9.6-4.el9_6.2 |
| | sssd-kcm | 2.9.6-4.el9_6.2 |
| | subscription-manager | 1.29.45.1-1.el9_6.alma.1 |
| | sudo | 1.9.5p2-10.el9_6.1 |
| | systemd | 252-51.el9_6.1.alma.1 |
| | systemd-libs | 252-51.el9_6.1.alma.1 |
| | systemd-pam | 252-51.el9_6.1.alma.1 |
| | systemd-rpm-macros | 252-51.el9_6.1.alma.1 |
| | systemd-udev | 252-51.el9_6.1.alma.1 |
| | tar | 1.34-6.el9_1 |
| | tpm2-tss | 3.2.3-1.el9 |
| | traceroute | 2.1.1-1.el9 |
| | unbound-libs | 1.16.2-19.el9_6.1 |
| | usbutils | 013-4.el9 |
| | util-linux | 2.37.4-21.el9 |
| | util-linux-core | 2.37.4-21.el9 |
| | vim-common | 8.2.2637-22.el9_6 |
| | vim-enhanced | 8.2.2637-22.el9_6 |
| | vim-filesystem | 8.2.2637-22.el9_6 |
| | vim-minimal | 8.2.2637-22.el9_6 |
| | wget | 1.21.1-8.el9_4 |

# 1.3 TOE概要

## 1.3.1 TOE種別

TOEは、マルチユーザーとアプリケーションのためのアクセス制御、監査機能のサポート、および暗号機能によるSecure Shell(SSH)を使用したセキュアなリモートログイン、TLSなどのセキュアなネットワークサービスを提供するLinuxベースの汎用オペレーティングシステム(OS)である。

## 1.3.2 TOEの使用方法及び主要なセキュリティ機能

### 1.3.2.1 TOEの使用方法

TOEは、一般的なサーバー用環境にオペレーティングシステムとしてインストールされ、ネットワークに接続されることを想定している。オペレーティングシステム(OS)はユーザーが実行したい

アプリケーションに対し共通化・抽象化したハードウェア操作及び、基礎的なアプリケーション・共有ライブラリや規格、セキュリティ機能を提供する。

#### 1.3.2.2 主要なセキュリティ機能

- セキュリティ監査
  - セキュリティ関連の監査イベントをセキュリティ監査ログに記録
- 暗号サポート
  - TOEのセキュリティ機能をサポートするための暗号操作
- ユーザーデータの保護
  - ファイルおよびディレクトリに対してのアクセス制御
- 識別と認証
  - 認証情報を用いたユーザーまたはリモートエンティティの識別と認証
- セキュリティ管理
  - 管理者または特権ユーザーのみによる、TOEのセキュリティ機能の設定管理
- TOEアクセス
  - ユーザーセッション確立前に未認可使用に関する警告を表示
- TSFの保護
  - データおよび実行されるソフトウェアを保護するための自己保護メカニズム
- 高信頼パス/チャネル
  - TOEとユーザー・ITエンティティ間に信頼された通信経路を確保

#### 1.3.2.3 TOE評価に含まれない機能

以下のTOE機能は評価範囲に含まれない。

**a) SELinux**

SELinuxはLSM(Linux Security Module)上で動くモジュールの一つであり、ロールやドメインによるラベルベースのポリシー設定によって、強制アクセス制御(Mandatory Access Control: MAC)と呼ばれる、任意アクセス制御よりも強力かつ細かい制限をプロセスにかける機能である。

**b) OS**仮想化インフラ

KVM(Kernel-based Virtual Machine)や QEMU(Quick Emulator)、libvirtなどのオープンソースのソフトウェア群を提供し、仮想化環境のインフラを構築する方法を提供する。

**c)** コンテナ化インフラ

Open Container Initiativeが策定している標準コンテナイメージ規格による、コンテナ仮想化環境を構築するための管理ツール・ランタイム・イメージ作成ツールなどのソフトウェア群を提供する。

**d)** グラフィカルユーザーインターフェイス**(Gnome**デスクトップ環境等**)**

グラフィカルユーザーインターフェイス環境は、X Window SystemまたはWaylandと組み合わせて提供され、GUIツールキットやライブラリ、簡易に利用できる標準的なアプリケーション(ブラウ

ザ・テキストエディタ・メーラー・ファイラー・仮想ターミナル等)を含み、コマンドラインを用いずにユーザーが視覚的に利用できるGnomeデスクトップ環境等を提供する。

### 1.3.3 TOE動作環境

TOEは、Table 4のPlatform上にインストールされて動作する。TOEが想定する動作環境を図1に示す。

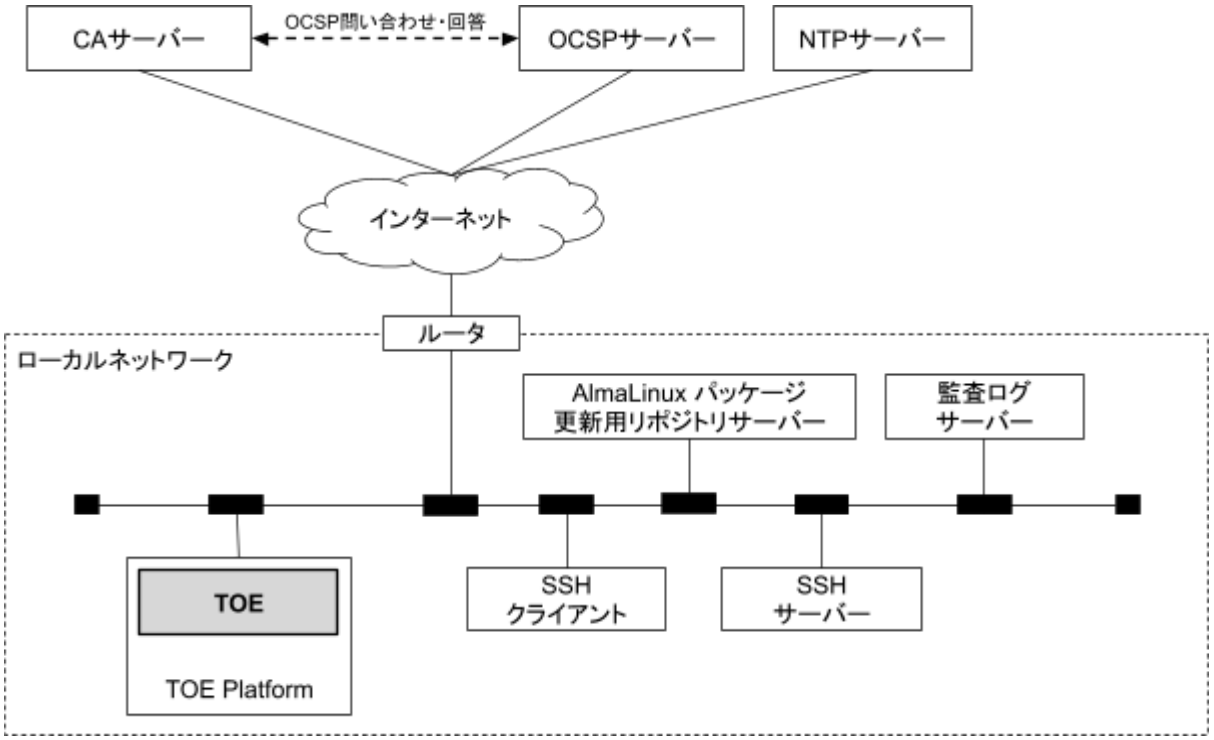



図1: TOE動作環境

TOE環境の各サーバー概要を以下に記載する。

Table 3: TOE動作環境の概要

| **TOE**動作環境の構成要素 | 概要 |
|---|---|
| TOE Platform | TOEを実行するために必要な物理的環境であり、CPU・メモリ・周辺デバイス等のハードウェア、およびそれらを制御するファームウェアで構成される。 |
| AlmaLinux OSパッケージ<br>更新用リポジトリサーバー | LinuxのRPMパッケージを効率的に配付・管理するためのサーバー。TOEはTLSを用いたパッケージ管理ツールを通じて、リモートリポジトリ、または組織のローカルリポジトリからパッケージのインストールや更新を行う。<br><br>組織のローカルリポジトリはリモートリポジトリをreposyncコマンドを使用してコピーしローカルネットワーク内に構築したもので、TOEが参照する先をローカルリポジトリに変更することでリモートリポジトリの代わり使用することができる。 |

| | |
|---|---|
| SSHサーバー | SSHプロトコルを利用してクライアントからの接続要求を受け入れ、認証を行い、セキュアな通信を提供する機能を備えたサーバー。<br><br>SSHサーバーは、管理者がTOEからリモートにある他サーバーに対してセキュアな保守・管理を実施する場合に必要となる。 |
| SSHクライアント | SSHプロトコルを利用してサーバーとのセキュアな通信を確立する機能を提供するホストまたはアプリケーション。<br><br>SSHクライアントは、管理者がリモートの管理端末から、TOEに対してセキュアな保守・管理を実施する場合に必要となる。 |
| 監査ログサーバー | 遠隔システムに監査ログを送信するため、TLSプロトコルにより確立されたセキュアな通信経路を通じて、クライアントから監査ログを受信する機能を提供するサーバー。 |
| NTPサーバー | NTP（Network Time Protocol）を利用してクライアントからの時刻同期要求を受信し、正確な時刻情報を提供する機能を持つサーバー。<br><br>TOEの運用環境において、NTPサーバーの物理的・論理的配置は特定の構成に限定されない。利用者は組織のセキュリティ要件に基づき、内部ネットワークへのNTPサーバーの設置、または外部の信頼された時刻情報の利用を任意に選択することが可能である。<br><br>※図1では外部の信頼されたNTPサーバを使用する構成を示している。 |
| OCSPサーバー/レスポンダ | クライアントが提示したX.509証明書情報に基づき、失効状態をリアルタイムに確認できるサービスを提供するサーバー。<br><br>TOEの運用環境において、OCSPサーバーは外部のPKI（公開鍵基盤）が提供するサービスを利用することを前提とする。そのため、特別な理由がない限り、TOEの導入にあたって利用者が個別にOCSPサーバーを構築・運用する必要はない。 |
| CAサーバー | 公開鍵基盤（PKI）の基幹として公開鍵証明書の発行、検証および失効情報の提供を行うサーバー。これにより、各種認証、暗号化および電子署名の信頼性を確保する。 |

| | |
|---|---|
| | TOEの運用環境において、CAサーバーは外部のPKI（公開鍵基盤）が提供するサービスを利用することを前提とする。そのため、特別な理由がない限り、TOEの導入にあたって利用者が個別にCAサーバーを構築・運用する必要はない。 |

### 1.3.4 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

TOEを評価構成で動作させるため、TOEのPlatform、および必要な評価コンポーネントのハードウェア・ソフトウェアを以下に示す。

Table 4: TOEのPlatform

| **Hardware** | 推奨値 | 補足事項 |
|---|---|---|
| CPU | 1CPU以上 | Intel x86_64 アーキテクチャ のCPUであること |
| メモリ | 1.5GB以上 | ※2論理CPU 以上の場合、<br>1論理CPU につき、1GBを推奨<br>(4論理CPU なら4GB) |
| ディスク | 20GB以上 | UEFIシステムにおいて、ターゲットディスクがGPT（GUIDパーティションテーブル）を使用していることを確認する。<br>一部のUEFIファームウェアは<br>UEFI/MBRブートをサポートしない。 |

Table 5: テストされたハードウェア

| 種別 | 説明 |
|---|---|
| ベンダ名 | 日本電気株式会社 |
| 製品名 | FC-R16W |
| CPU | Intel Xeon プロセッサー E5-2680 v4<br>(x86_64 アーキテクチャ、14物理CPU、28Thread、計 28 論理CPU) |
| メモリ | 16GB |
| HDD | 600GB×2(RAID1) |
| ファームウェア名称 | R24W・R16Wシリーズ用　マザーボード Firmware (FPGA) |
| ファームウェア提供元 | 日本電気株式会社 |

Table 6: TOE評価環境で使用したソフトウェア

| サーバー | ソフトウェア |
| --- | --- |
| AlmaLinux OSパッケージ<br>更新用リポジトリサーバー | Apache 2.4.65 |
| SSHサーバー | OpenSSH 10.0p2 |
| SSHクライアント | OpenSSH 10.0p2 |
| 監査ログサーバー | rsyslogd 8.2504.0 |
| NTPサーバー | chronyd 4.4 |
| OCSPサーバー<br>(OCSPレスポンダ) | OpenSSL 3.5.1-1 |
| CAサーバー | OpenSSL 3.5.1-1 |

# 1.4 TOE記述

## 1.4.1 TOEの物理的範囲

TOEは、汎用オペレーティングシステムであり、以下のシステムソフトウェアをベースとする。

- AlmaLinux OS 9.2 for x86_64

TOEを構成するソフトウェアは、Table 7に記載されたURLを通じて、ISOイメージ形式、RPMパッケージ、ならびにRPMパッケージ署名検証用のGPG鍵として配付される。また、TOEのガイダンス文書は、Table 11に記載された方法で入手可能である。ISOイメージを用いてインストールした環境に、Table 8、Table 9、Table 10にリストされたRPMパッケージを追加インストールすることで、「Table 2: TOE識別子」に示すTOE環境を構築できる。

TOEを構成するソフトウェア、およびガイダンスを以下のTableに示す。

Table 7: TOEを構成するソフトウェア一覧

| | | | |
|---|---|---|---|
| No.1 | 識別 | 名称 | AlmaLinux OS 9.2 for x86_64 |
| | | ファイル名 | AlmaLinux-9.2-x86_64-dvd.iso |
| | | バージョン | 9.2 |
| | 配付方法 | 形式 | ISOイメージ |
| | | URL | https://vault.almalinux.org/9.2/isos/x86_64/ |
| No.2 | 識別 | 名称 | FIPS対応RPMパッケージ |
| | | ファイル名 | 「Table 8: FIPS対応RPMパッケージ一覧」を参照 |
| | 配付方法 | 形式 | RPMパッケージ |
| | | URL | https://repo.tuxcare.com/fips/9.2/x86_64/Packages/ |
| No.3 | 識別 | 名称 | FIPS対応RPMパッケージ用GPG鍵 |
| | | ファイル名 | RPM-GPG-KEY-TuxCare |
| | 配付方法 | 形式 | テキストファイル |
| | | URL | https://repo.tuxcare.com/fips/ |
| No.4 | 識別 | 名称 | AlmaLinux OS Updateパッケージ |
| | | ファイル名 | 「Table 9: AlmaLinux OS Updateパッケージ一覧」を参照 |
| | 配付方法 | 形式 | RPMパッケージ |
| | | URL | https://vault.almalinux.org/9.6/BaseOS/x86_64/os/Packages/ |

| | | | |
|---|---|---|---|
| | | | https://vault.almalinux.org/9.6/AppStream/x86_64/os/Packages/ |
| No.5 | 識別 | 名称 | 開発環境構築パッケージ |
| | | ファイル名 | 「Table 10: 開発環境構築パッケージ一覧」を参照 |
| | 配付方法 | 形式 | RPMパッケージ |
| | | URL | https://vault.almalinux.org/9.6/BaseOS/x86_64/os/Packages/<br>https://vault.almalinux.org/9.6/AppStream/x86_64/os/Packages/ |

Table 8: FIPS対応RPMパッケージ一覧

| No. | RPMパッケージ名称 |
|---|---|
| 1 | kernel-5.14.0-284.11.1.el9_2.tuxcare.5.x86_64.rpm |
| 2 | kernel-core-5.14.0-284.11.1.el9_2.tuxcare.5.x86_64.rpm |
| 3 | kernel-headers-5.14.0-284.11.1.el9_2.tuxcare.5.x86_64.rpm |
| 4 | kernel-modules-5.14.0-284.11.1.el9_2.tuxcare.5.x86_64.rpm |
| 5 | kernel-modules-core-5.14.0-284.11.1.el9_2.tuxcare.5.x86_64.rpm |
| 6 | openssl-3.0.7-20.el9_2.tuxcare.1.x86_64.rpm |
| 7 | openssl-libs-3.0.7-20.el9_2.tuxcare.1.x86_64.rpm |

Table 9: AlmaLinux OS Update RPMパッケージ一覧

| No. | RPMパッケージ名称 |
|---|---|
| 1 | aide-0.16-103.el9_6.2.x86_64.rpm |
| 2 | attr-2.5.1-3.el9.x86_64.rpm |
| 3 | bind-libs-9.16.23-31.el9_6.x86_64.rpm |
| 4 | bind-license-9.16.23-31.el9_6.noarch.rpm |
| 5 | bind-utils-9.16.23-31.el9_6.x86_64.rpm |
| 6 | binutils-2.35.2-63.el9.x86_64.rpm |
| 7 | binutils-gold-2.35.2-63.el9.x86_64.rpm |

| | |
|---|---|
| 8 | bzip2-libs-1.0.8-10.el9_5.x86_64.rpm |
| 9 | curl-minimal-7.76.1-29.el9_4.1.x86_64.rpm |
| 10 | dbus-1.12.20-8.el9.x86_64.rpm |
| 11 | dbus-common-1.12.20-8.el9.noarch.rpm |
| 12 | dbus-libs-1.12.20-8.el9.x86_64.rpm |
| 13 | device-mapper-1.02.202-6.el9.x86_64.rpm |
| 14 | device-mapper-event-1.02.202-6.el9.x86_64.rpm |
| 15 | device-mapper-event-libs-1.02.202-6.el9.x86_64.rpm |
| 16 | device-mapper-libs-1.02.202-6.el9.x86_64.rpm |
| 17 | dmidecode-3.6-1.el9.x86_64.rpm |
| 18 | expat-2.5.0-5.el9_6.x86_64.rpm |
| 19 | file-5.39-16.el9.x86_64.rpm |
| 20 | file-libs-5.39-16.el9.x86_64.rpm |
| 21 | glib2-2.68.4-16.el9_6.2.x86_64.rpm |
| 22 | glibc-2.34-168.el9_6.23.x86_64.rpm |
| 23 | glibc-common-2.34-168.el9_6.23.x86_64.rpm |
| 24 | glibc-gconv-extra-2.34-168.el9_6.23.x86_64.rpm |
| 25 | glibc-langpack-en-2.34-168.el9_6.23.x86_64.rpm |
| 26 | gmp-6.2.0-13.el9.x86_64.rpm |
| 27 | gnutls-3.8.3-6.el9.x86_64.rpm |
| 28 | gnutls-dane-3.8.3-6.el9.x86_64.rpm |
| 29 | gnutls-utils-3.8.3-6.el9.x86_64.rpm |
| 30 | grub2-common-2.06-104.el9_6.alma.1.noarch.rpm |
| 31 | grub2-efi-x64-2.06-104.el9_6.alma.1.x86_64.rpm |
| 32 | grub2-tools-2.06-104.el9_6.alma.1.x86_64.rpm |
| 33 | grub2-tools-minimal-2.06-104.el9_6.alma.1.x86_64.rpm |
| 34 | ima-evm-utils-1.5-3.el9.x86_64.rpm |

| | |
|---|---|
| 35 | iputils-20210202-11.el9_6.1.x86_64.rpm |
| 36 | iwl1000-firmware-39.31.5.1-151.3.el9_6.noarch.rpm |
| 37 | iwl100-firmware-39.31.5.1-151.3.el9_6.noarch.rpm |
| 38 | iwl105-firmware-18.168.6.1-151.3.el9_6.noarch.rpm |
| 39 | iwl135-firmware-18.168.6.1-151.3.el9_6.noarch.rpm |
| 40 | iwl2000-firmware-18.168.6.1-151.3.el9_6.noarch.rpm |
| 41 | iwl2030-firmware-18.168.6.1-151.3.el9_6.noarch.rpm |
| 42 | iwl3160-firmware-25.30.13.0-151.3.el9_6.noarch.rpm |
| 43 | iwl5000-firmware-8.83.5.1_1-151.3.el9_6.noarch.rpm |
| 44 | iwl5150-firmware-8.24.2.2-151.3.el9_6.noarch.rpm |
| 45 | iwl6000g2a-firmware-18.168.6.1-151.3.el9_6.noarch.rpm |
| 46 | iwl6050-firmware-41.28.5.1-151.3.el9_6.noarch.rpm |
| 47 | iwl7260-firmware-25.30.13.0-151.3.el9_6.noarch.rpm |
| 48 | krb5-libs-1.21.1-8.el9_6.x86_64.rpm |
| 49 | less-590-5.el9.x86_64.rpm |
| 50 | libarchive-3.5.3-6.el9_6.x86_64.rpm |
| 51 | libblkid-2.37.4-21.el9.x86_64.rpm |
| 52 | libcap-2.48-9.el9_2.x86_64.rpm |
| 53 | libcurl-minimal-7.76.1-29.el9_4.1.x86_64.rpm |
| 54 | libdnf-plugin-subscription-manager-1.29.45.1-1.el9_6.alma.1.x86_64.rpm |
| 55 | libeconf-0.4.1-4.el9.x86_64.rpm |
| 56 | libfastjson-0.99.9-5.el9.x86_64.rpm |
| 57 | libfdisk-2.37.4-21.el9.x86_64.rpm |
| 58 | libgcc-11.5.0-5.el9_5.alma.1.x86_64.rpm |
| 59 | libgcrypt-1.10.0-11.el9.x86_64.rpm |
| 60 | libgomp-11.5.0-5.el9_5.alma.1.x86_64.rpm |
| 61 | libicu-67.1-10.el9_6.x86_64.rpm |

| | |
|---|---|
| 62 | libmount-2.37.4-21.el9.x86_64.rpm |
| 63 | libndp-1.9-1.el9.x86_64.rpm |
| 64 | libnghttp2-1.43.0-6.el9.x86_64.rpm |
| 65 | libnvme-1.11.1-1.el9.x86_64.rpm |
| 66 | libqb-2.0.8-1.el9.x86_64.rpm |
| 67 | libsmartcols-2.37.4-21.el9.x86_64.rpm |
| 68 | libsss_certmap-2.9.6-4.el9_6.2.x86_64.rpm |
| 69 | libsss_idmap-2.9.6-4.el9_6.2.x86_64.rpm |
| 70 | libsss_nss_idmap-2.9.6-4.el9_6.2.x86_64.rpm |
| 71 | libsss_sudo-2.9.6-4.el9_6.2.x86_64.rpm |
| 72 | libstdc++-11.5.0-5.el9_5.alma.1.x86_64.rpm |
| 73 | libtasn1-4.16.0-9.el9.x86_64.rpm |
| 74 | libtevent-0.16.1-1.el9.x86_64.rpm |
| 75 | libuuid-2.37.4-21.el9.x86_64.rpm |
| 76 | libuv-1.42.0-2.el9_4.x86_64.rpm |
| 77 | libxml2-2.9.13-12.el9_6.x86_64.rpm |
| 78 | libxslt-1.1.34-13.el9_6.x86_64.rpm |
| 79 | linux-firmware-20250716-151.3.el9_6.noarch.rpm |
| 80 | linux-firmware-whence-20250716-151.3.el9_6.noarch.rpm |
| 81 | lvm2-2.03.28-6.el9.x86_64.rpm |
| 82 | lvm2-libs-2.03.28-6.el9.x86_64.rpm |
| 83 | microcode_ctl-20250211-1.20250512.1.el9_6.noarch.rpm |
| 84 | ncurses-6.2-10.20210508.el9_6.2.x86_64.rpm |
| 85 | ncurses-base-6.2-10.20210508.el9_6.2.noarch.rpm |
| 86 | ncurses-libs-6.2-10.20210508.el9_6.2.x86_64.rpm |
| 87 | nettle-3.10.1-1.el9.x86_64.rpm |
| 88 | NetworkManager-1.52.0-5.el9_6.x86_64.rpm |

| | |
|---|---|
| 89 | NetworkManager-libnm-1.52.0-5.el9_6.x86_64.rpm |
| 90 | NetworkManager-team-1.52.0-5.el9_6.x86_64.rpm |
| 91 | NetworkManager-tui-1.52.0-5.el9_6.x86_64.rpm |
| 92 | openssh-8.7p1-45.el9.x86_64.rpm |
| 93 | openssh-clients-8.7p1-45.el9.x86_64.rpm |
| 94 | openssh-server-8.7p1-45.el9.x86_64.rpm |
| 95 | pam-1.5.1-26.el9_6.x86_64.rpm |
| 96 | postfix-3.5.25-1.el9.x86_64.rpm |
| 97 | procps-ng-3.3.17-14.el9.x86_64.rpm |
| 98 | protobuf-3.14.0-16.el9.x86_64.rpm |
| 99 | protobuf-c-1.3.3-13.el9.x86_64.rpm |
| 100 | python3-3.9.21-2.el9_6.2.x86_64.rpm |
| 101 | python3-cloud-what-1.29.45.1-1.el9_6.alma.1.x86_64.rpm |
| 102 | python3-idna-2.10-7.el9_4.1.noarch.rpm |
| 103 | python3-libs-3.9.21-2.el9_6.2.x86_64.rpm |
| 104 | python3-pip-wheel-21.3.1-1.el9.noarch.rpm |
| 105 | python3-requests-2.25.1-10.el9_6.noarch.rpm |
| 106 | python3-rpm-4.16.1.3-37.el9.x86_64.rpm |
| 107 | python3-setuptools-53.0.0-13.el9_6.1.noarch.rpm |
| 108 | python3-setuptools-wheel-53.0.0-13.el9_6.1.noarch.rpm |
| 109 | python3-subscription-manager-rhsm-1.29.45.1-1.el9_6.alma.1.x86_64.rpm |
| 110 | python3-urllib3-1.26.5-6.el9.noarch.rpm |
| 111 | python-unversioned-command-3.9.21-2.el9_6.2.noarch.rpm |
| 112 | rpm-4.16.1.3-37.el9.x86_64.rpm |
| 113 | rpm-build-libs-4.16.1.3-37.el9.x86_64.rpm |
| 114 | rpm-libs-4.16.1.3-37.el9.x86_64.rpm |
| 115 | rpm-plugin-audit-4.16.1.3-37.el9.x86_64.rpm |

| | |
|---|---|
| 116 | rpm-plugin-fapolicyd-4.16.1.3-37.el9.x86_64.rpm |
| 117 | rpm-plugin-selinux-4.16.1.3-37.el9.x86_64.rpm |
| 118 | rpm-plugin-systemd-inhibit-4.16.1.3-37.el9.x86_64.rpm |
| 119 | rpm-sign-libs-4.16.1.3-37.el9.x86_64.rpm |
| 120 | rsync-3.2.5-3.el9.x86_64.rpm |
| 121 | shadow-utils-4.9-12.el9.x86_64.rpm |
| 122 | shim-x64-15.8-4.el9_3.alma.2.x86_64.rpm |
| 123 | sqlite-libs-3.34.1-8.el9_6.x86_64.rpm |
| 124 | squashfs-tools-4.4-10.git1.el9.x86_64.rpm |
| 125 | sssd-client-2.9.6-4.el9_6.2.x86_64.rpm |
| 126 | sssd-common-2.9.6-4.el9_6.2.x86_64.rpm |
| 127 | sssd-kcm-2.9.6-4.el9_6.2.x86_64.rpm |
| 128 | subscription-manager-1.29.45.1-1.el9_6.alma.1.x86_64.rpm |
| 129 | sudo-1.9.5p2-10.el9_6.1.x86_64.rpm |
| 130 | systemd-252-51.el9_6.1.alma.1.x86_64.rpm |
| 131 | systemd-libs-252-51.el9_6.1.alma.1.x86_64.rpm |
| 132 | systemd-pam-252-51.el9_6.1.alma.1.x86_64.rpm |
| 133 | systemd-rpm-macros-252-51.el9_6.1.alma.1.noarch.rpm |
| 134 | systemd-udev-252-51.el9_6.1.alma.1.x86_64.rpm |
| 135 | tpm2-tss-3.2.3-1.el9.x86_64.rpm |
| 136 | traceroute-2.1.1-1.el9.x86_64.rpm |
| 137 | unbound-libs-1.16.2-19.el9_6.1.x86_64.rpm |
| 138 | util-linux-2.37.4-21.el9.x86_64.rpm |
| 139 | util-linux-core-2.37.4-21.el9.x86_64.rpm |
| 140 | vim-common-8.2.2637-22.el9_6.x86_64.rpm |
| 141 | vim-enhanced-8.2.2637-22.el9_6.x86_64.rpm |
| 142 | vim-filesystem-8.2.2637-22.el9_6.noarch.rpm |

| | |
|---|---|
| 143 | vim-minimal-8.2.2637-22.el9_6.x86_64.rpm |
| 144 | wget-1.21.1-8.el9_4.x86_64.rpm |

Table 10: 開発環境構築RPMパッケージ一覧

| No. | RPMパッケージ名称 |
|---|---|
| 1 | cpp-11.5.0-5.el9_5.alma.1.x86_64.rpm |
| 2 | gcc-11.5.0-5.el9_5.alma.1.x86_64.rpm |
| 3 | glibc-devel-2.34-168.el9_6.23.x86_64.rpm |
| 4 | glibc-headers-2.34-168.el9_6.23.x86_64.rpm |
| 5 | libmpc-1.2.1-4.el9.x86_64.rpm |
| 6 | libpkgconf-1.7.3-10.el9.x86_64.rpm |
| 7 | libxcrypt-devel-4.4.18-3.el9.x86_64.rpm |
| 8 | make-4.3-8.el9.x86_64.rpm |
| 9 | pkgconf-1.7.3-10.el9.x86_64.rpm |
| 10 | pkgconf-m4-1.7.3-10.el9.noarch.rpm |
| 11 | pkgconf-pkg-config-1.7.3-10.el9.x86_64.rpm |

Table 11: TOEを構成するガイダンス一覧

| | | | |
|---|---|---|---|
| No.1 | 識別 | 名称 | AlmaLinux OS 9.2  for x86_64 Compatible FIPS140-3 Common Criteria  ガイダンス |
| | | ファイル名 | almalinux_os_92_for_x86_64_compatible_fips140-3_common_criteria_guidance.pdf |
| | | バージョン | 1.43 |
| | 配付形式 | | PDF |
| | 配付方法 | | サイバートラスト株式会社より購入者へダウンロードURLを通知 |
| No.2 | 識別 | 名称 | AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 一般用ガイダンス |
| | | ファイル名 | almalinux_os_92_for_x86_64_compatible_fips140-3_general_guidance.pdf |

| | | | |
|---|---|---|---|
| | | バージョン | 1.14 |
| | 配付形式 | | PDF |
| | 配付方法 | | サイバートラスト株式会社より購入者へダウンロードURLを通知 |

## 1.4.2 TOEの論理的範囲

### 1.4.2.1 TOEセキュリティ機能

TOEは以下のセキュリティ機能を提供する。

**a)** セキュリティ監査

TOEは、以下に示すセキュリティ関連の監査イベントを生成し、それらを監査ログとして記録する。

- 監査機能のスタートアップとシャットダウン
- 認証イベント（成功/失敗）
- 特権/特別権限イベントの使用（セキュリティ、監査、構成変更の成功と失敗）
- 特権またはロールのエスカレーションイベント（成功/失敗）
- RPMパッケージのインストールと署名検証に関するイベント（成功/失敗）
- SSH接続に関する事象・イベント（接続の確立および失敗、セッション終了）

監査レコードには、イベントの日時、イベントのタイプ、サブジェクトの識別（該当する場合）、およびイベントの結果（成功または失敗）が含まれる。

**b)** 暗号サポート

TOEは、ストレージ暗号化機能、SSHサーバー機能、SSHクライアント機能、ならびにTLS のクライアント機能を提供する。また、これらに関連する機能として、以下の機能を提供する。

- 非対称鍵の生成
- 暗号鍵の確立スキーム
- 鍵および鍵マテリアルの消去
- 暗号アルゴリズムを用いたデータの暗号化・復号機能
- ハッシュアルゴリズム
- 電子署名アルゴリズム
- ハッシュメッセージ認証
- 決定論的ランダムビット生成

**c)** ユーザーデータの保護

TOEは、権限のないユーザーが他のユーザーのファイルやディレクトリにアクセスできないよう権限を設定するアクセス制御を提供する。アクセス制御は、TOEが提供するDAC（任意アクセス制御）によって行われ、ユーザー自身が所有するファイルやディレクトリのアクセス権を管理する。

**d)** 識別と認証

TOEは、ユーザー認証方式としてパスワード認証および公開鍵認証をサポートする。パスワード認証では、認証失敗の回数が所定の閾値に達した場合、当該ユーザーアカウントをロックアウトする。また、TOEは、TLS接続およびHTTPS接続時のリモートエンティティ認証方式として X.509v3証明書による認証をサポートする。証明書の失効確認は、OCSP Staplingにより行う。

**e)** セキュリティ管理

管理者または特権ユーザーのみが、TOEのセキュリティ機能に関する以下の設定を管理できる。

- Enable/disable [session timeout]
    - セッションタイムアウトの有効・無効化の設定
- Configure [session] inactivity timeout
    - セッションの非アクティブタイムアウト時間の設定
- Import keys/secrets into the secure key storage
    - 秘密鍵および証明書をインポートする操作
- Configure local audit storage capacity
    - 監査ログを保存するストレージのサイズ設定
- Configure minimum password length
    - パスワードの最小長の設定
- Configure minimum number of special characters in password
    - パスワードに含まれる記号の最小数の設定
- Configure minimum number of numeric characters in password
    - パスワードに含まれる数字の最小数の設定
- Configure minimum number of uppercase characters in password
    - パスワードに含まれる英大文字の最小数の設定
- Configure minimum number of lowercase characters in password
    - パスワードに含まれる英小文字の最小数の設定
- Configure lockout policy for unsuccessful authentication attempts through [timeouts between attempts]
    - 認証失敗時のロックアウトポリシーである、タイムアウト時間と一定期間内の試行回数の制限設定
- Configure host-based firewall
    - ホスト単位のファイアウォールの設定
- Configure name/address of audit/logging server to which to send audit/logging records
    - 監査ログサーバーの設定
- Configure audit rules
    - 監査ログのルールの設定
- Configure name/address of network time server
    - 使用する NTP サーバーの設定と、NTPサーバーからの時刻取得の有効・無効化

- Enable/disable automatic software update
    - dnf automatic によるソフトウェアの自動更新の有効・無効化の設定
- Configuration of object ownership and allowed access
    - ファイル・ディレクトリの所有権と許可されたアクセスに基づくアクセス制御の設定
- Configuration of the roles that may manage the behavior of the TSF management functions
    - 管理機能のふるまいを管理するロールの設定

### f) TOEアクセス

TOEは、ユーザーがセッションを確立する前に、未認可使用に関する警告を含む情報バナーを画面に表示することで明確に注意喚起を行う。

### g) TSFの保護

TOEは、TOEによって実行されるソフトウェアに対する攻撃、許可されていないソフトウェアの実行およびTSFデータに対する不正アクセスや改ざんから保護するため、以下の自己保護メカニズムを提供する。

- Access controls
    - システムファイルの保護
- Address Space Layout Randomization(ASLR)
    - アドレス空間配置のランダム化
- Stack Buffer Overflow Protection
    - スタックカナリアを用いたスタックバッファオーバーフロー保護
- Software Restriction Policies
    - 既知または信頼されたアプリケーションのみを実行
- Boot Integrity
    - セキュアブート
- Trusted Update
    - TOE自体とアプリケーション・ソフトウェアのアップデートの有無の確認
    - デジタル署名によるパッケージの検証

### h) 高信頼パス/チャネル

TOEは、SSHv2およびTLS 1.2により通信経路を暗号化し、許可されたITエンティティとのリモート通信を保護する高信頼チャネルを提供する。高信頼チャネルの利用例としては、監査ログをTLS 1.2経由でリモート監査ログサーバーへ安全に転送する用途が挙げられる。また、TOEは、認証済みユーザーに論理的に分離された高信頼パスを提供する。高信頼パスは、ローカルユーザーにはローカルコンソール、リモートユーザーにはSSHv2により提供され、管理者は高信頼パスを通じてTOEを安全にリモート管理できる。

## 1.5 頭字語

Table 12: 頭字語

| 頭字語 | 定義 |
|---|---|
| ACL | Access Control List |
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| ASLR | Address Space Layout Randomization |
| CA | Certificate Authorities |
| CC | Common Criteria |
| CMC | Certificate Management over CMS |
| CMS | Cryptographic Message Syntax |
| CN | Common Names |
| CSP | Critical Security Parameters |
| CVE | Common Vulnerabilities and Exposures |
| DAC | Discretionary Access Control |
| DHE | Diffie-Hellman Ephemeral |
| DNS | Domain Name System |
| DRBG | Deterministic Random Bit Generator |
| DSS | Digital Signature Standard |
| DTLS | Datagram Transport Layer Security |
| ECDHE | Elliptic Curve Diffie-Hellman Ephemeral |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| EST | Enrollment over Secure Transport |
| FFC | Finite Field Cryptosystems |
| FIPS | Federal Information Processing Standards |
| FP | Functional Package |

| | |
|---|---|
| GCM | Galois/Counter Mode |
| HMAC | Hash-based Message Authentication Code |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | Hypertext Transfer Protocol Secure |
| IP | Internet Protocol |
| LAF | Lightweight Audit Framework |
| NIAP | National Information Assurance Partnership |
| NIST | National Institute of Standards and Technology |
| OCSP | Online Certificate Status Protocol |
| OE | Operational Environment |
| OID | Object Identifier |
| OS | Operating System |
| PAM | Pluggable Authentication Module |
| PKI | Public Key Infrastructure |
| PP | Protection Profile |
| RBG | Random Bit Generator |
| RFC | Request for Comment |
| S/MIME | Secure/Multi-purpose Internet Mail Extensions |
| SAN | Subject Alternative Name |
| SAR | Security Assurance Requirement |
| SFR | Security Functional Requirement |
| SHA | Secure Hash Algorithm |
| SSL | Secure Socket Layer |
| SSH | Secure Shell |
| ST | Security Target |

| | |
|---|---|
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSF | TOE Security Functionality |
| TSFI | TSF Interface |
| TSS | TOE Summary Specification |
| UEFI | Unified Extensible Firmware Interface |
| URI | Uniform Resource Identifier |
| URL | Uniform Resource Locator |
| VPN | Virtual Private Network |

## 1.6 用語

Table 13: 用語

| 用語 | 意味 |
|---|---|
| サーバー | ユーザーに対しサービスを提供するコンピュータ |
| アプリケーション | ユーザー空間上で動作する応用ソフトウェア |
| ライブラリ | ソフトウェアの汎用的なコードを再利用できる共通部品にしたプログラム |
| カーネル | オペレーティングシステムの中心として動作し、アプリケーションが操作する代わりにハードウェアの操作と抽象化を担当するプログラム |
| プロセス | 独自のメモリ空間とリソースを持った実行中のプログラムのコピー |
| 不正アクセス | セキュリティ機能によって制限される範囲を何らかの方法で超越して行われる操作 |
| アドレス空間 | プロセスが使用できるメモリの範囲 |
| オーバーフロー | データが格納できるアドレス空間を超えて書き込まれる現象 |
| バッファオーバーフロー | オーバーフローにより、隣接するメモリ領域を上書きし、プログラムが意図しない動作が発生する事象 |
| ユーザー空間 | アプリケーションが動作する領域を指す。 |
| スタック | 関数呼び出しやローカル変数の管理に使用されるメモリ領域 |
| UEFI | コンピュータのブートプロセスを管理するためのインターフェース。従来のBIOSに代わるものであり、より高度な機能やセキュリティを提供する。 |
| セキュアブート | UEFIの機能として実装されている、署名されていない低レイヤーのマルウェアの起動を防ぐセキュリティ機能 |
| ブートチェーン | コンピュータが電源を入れてからオペレーティングシステムを起動するまでの一連のプロセスや手順 |
| 公開鍵 | 暗号化と復号に異なる暗号鍵を使う、非対称暗号形式において公開される側の暗号鍵 |
| 署名 | デジタル署名のことを指し、暗号学的に改ざんがされていないことや特定の暗号鍵を持つ名義人によって作成されたことを保証する技術 |

| | |
|---|---|
| rootユーザー | TOE全体への無制限の権限を持ち、全てのファイル・ディレクトリ・プロセスへアクセスできるユーザー |
| 管理者<br>Administrator | 管理者は、企業全体でオペレーティングシステムに適用されているポリシーの設定など、管理業務を担当する。管理者は、システムが構成ポリシーを受信する管理サーバーを介してリモートで操作を行うこともできる。管理者は、管理者以外のユーザーが上書きできない設定をシステムに適用することができる。T |
| ユーザー<br>user | ユーザーは、管理者によってオペレーティングシステムに適用される構成ポリシーの対象となる。特定の構成のシステムでは、通常のユーザーが一時的に管理者権限に昇格できる場合がある。その場合、そのようなユーザーは管理者とみなされる。 |

# 2 適合主張

## 2.1 CC適合主張

本STは以下のCC適合を主張する。

Table 14: CC適合主張

| | |
|---|---|
| CC version | CC Version 3.1 Revision 5 |
| CC conformance | Part2 (CCMB-2017-04-002) Extended<br>Part3 (CCMB-2017-04-003) Extended |
| addenda | CC and CEM addenda -Exact Conformance, Selection-Based SFRs, Optional SFRs(Version: 2.0 , Date of issue: 2021-Sep-30) |

## 2.2 PP適合主張

本STは、以下のPPに完全適合(Exact Conformance)する。

- [PPOS] Protection Profile for General Purpose Operating Systems, Version 4.3

評価実施時における[PPOS]のNIAP Techinical Decisionsと適用根拠を以下に示す。

Table 15: NIAP Technical Decisions

| TD# | Name | Source | Applicability Rationale |
|---|---|---|---|
| TD0442 | Updated TLS Ciphersuites for TLS Package | PKG_TLS_V1.1 | Applicable |
| TD0469 | Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1 | PKG_TLS_V1.1 | Not Applicable - FCS_TLSS_EXT not claimed. |
| TD0499 | Testing with pinned certificates | PKG_TLS_V1.1 | Applicable |
| TD0513 | CA Certificate loading | PKG_TLS_V1.1 | Applicable |
| TD0675 | Make FPT_W^X_EXT.1 Optional | PP_OS_V4.3 | Applicable |
| TD0682 | Addressing Ambiguity in FCS_SSHS_EXT.1 Tests | PKG_SSH_V1.0 | Applicable |
| TD0691 | OSPP 4.3 Conditional authentication testing | PP_OS_V4.3 | Applicable |

| | | | |
|---|---|---|---|
| TD0693 | Typos in OSPP 4.3 | PP_OS_V4.3 | Applicable |
| TD0695 | Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package. | PKG_SSH_V1.0 | Applicable |
| TD0696 | Removal of 160 bit selection from FCS_COP.1/HASH & FCS_COP.1/KEYHMAC | PP_OS_V4.3 | Applicable |
| TD0701 | Incomplete selection references in FCS_CKM_EXT.4 TSS activities | PP_OS_V4.3 | Applicable |
| TD0712 | Support for Bluetooth Standard 5.3 | PP_OS_V4.3 | Applicable |
| TD0713 | Functional Package SFR mappings to objectives | PP_OS_V4.3 | Applicable |
| TD0726 | Corrections to (D)TLSS SFRs in TLS 1.1 FP | PKG_TLS_V1.1 | Not Applicable - FCS_TLSS_EXT not claimed. |
| TD0732 | FCS_SSHS_EXT.1.3 Test 2 Update | PKG_SSH_V1.0 | Applicable |
| TD0739 | PKG_TLS_V1.1 has 2 different publication dates | PKG_TLS_V1.1 | Not Applicable - FCS_TLSS_EXT not claimed. |
| TD0770 | TLSS.2 connection with no client cert | PKG_TLS_V1.1 | Not Applicable - FCS_TLSS_EXT.2 not claimed. |
| TD0773 | Updates to FIA_X509_EXT.1 for Exception Processing and Test Conditions | PP_OS_V4.3 | Applicable |
| TD0777 | Clarification to Selections for Auditable Events for FCS_SSH_EXT.1 | PKG_SSH_V1.0 | Applicable |
| TD0779 | Updated Session Resumption Support in TLS package V1.1 | PKG_TLS_V1.1 | Not Applicable - FCS_TLSS_EXT not claimed. |

| | | | |
|---|---|---|---|
| TD0789 | Correction to TLS Selection in FIA_X509_EXT.2.1 | PP_OS_V4.3 | Applicable |
| TD0812 | Updated CC Conformance Claims in PP_OS_V4.3 | PP_OS_V4.3 | Applicable |
| TD0821 | Corrections to ECD for PP_OS_V4.3 | PP_OS_V4.3 | Applicable |
| TD0839 | Clarification for Local Administration in FTP_TRP.1.3 | PP_OS_V4.3 | Applicable |
| TD0844 | Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim | PP_OS_V4.3 | Not Applicable to this Security Target |
| TD0904 | Addition of MOD_VPNC_V2.5 to Conformance Claims | PP_OS_V4.3 | Applicable |
| TD0906 | Clarification to List of Examples in FPT_SBOP_EXT.1 | PP_OS_V4.3 | Applicable |
| TD0955 | Adding FIPS 186-5 in PP_OS_V4.3 | PP_OS_V4.3 | Applicable |

## 2.3 パッケージ適合主張

本STは以下の機能パッケージに適合を主張する。

- [PKGSSH] Functional Package for Secure Shell (SSH), Version 1.0
- [PKGTLS] Functional Package for Transport Layer Security (TLS) 1.1

## 2.4 適合主張根拠

PP適合主張に関して、以下に根拠を示す。

### 2.4.1 TOE種別

TOEは、第1章で特定されている汎用オペレーティングシステムであり、[PPOS]、[PKGSSH]および[PKGTLS]と適合している。

### 2.4.2 セキュリティ課題定義

第3章に記載のとおり、セキュリティ課題定義の脅威、および前提条件は、[PPOS]より転記した。

### 2.4.3 セキュリティ対策方針

第4章に記載のとおり、セキュリティ対策方針は、[PPOS]より転記した。

### 2.4.4 セキュリティ要件

第6章に記載のとおり、セキュリティ機能要件は、[PPOS]、[PKGSSH]および[PKGTLS]からTDを適用して操作を完了したSFRが複製されている。また、セキュリティ保証要件(SAR)は[PPOS]の内容から追加や削減をしておらず、[PPOS]と一貫している。

# 3 セキュリティ課題定義

セキュリティ課題定義は、[PPOS]、[PKGTLS],および[PKGSSH]より転記したものを以下のTableに示す。

## 3.1 脅威

Table 16: 脅威 [PPOS]

| Identifier | Description |
|---|---|
| T.NETWORK_ATTACK | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications. |
| T.NETWORK_ EAVESDROP | An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS. |
| T.LOCAL_ATTACK | An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system. |
| T.LIMITED_ PHYSICAL_ACCESS | An attacker may attempt to access data on the OS while having a limited amount of time with the physical device. |

[PKGSSH]と[PKGTLS]においては、脅威は定義されていない。

## 3.2 前提条件

Table 17: 前提条件 [PPOS]

| Identifier | Description |
|---|---|
| A.PLATFORM | The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP. |
| A.PROPER_USER | The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act as the user, so requirements which confine malicious subjects are still in scope. |
| A.PROPER_ADMIN | The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy. |

[PKGSSH]と[PKGTLS]においては、前提条件は定義されていない。

## 3.3 組織のセキュリティ方針

[PPOS]、[PKGTLS]および[PKGSSH]においては、組織のセキュリティ方針(OSP)は定義されていない。

# 4 セキュリティ対策方針

セキュリティ対策方針は、[PPOS]セクション4より転記した。[PKGSSH]と[PKGTLS]においては、セキュリティ対策方針は定義されていない。

## 4.1 TOEのセキュリティ対策方針

セキュリティ対策方針は[PPOS]セクション4.1より転記した。

Table 18: TOEのセキュリティ対策方針 [PPOS]

| Identifier | Description |
|---|---|
| O.ACCOUNTABILITY | Conformant OSes ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise. |
| O.INTEGRITY | Conformant OSes ensure the integrity of their update packages. OSes are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant OSes provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. |
| O.MANAGEMENT | To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration and application execution control. |
| O.PROTECTED_STORAGE | To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant OSes provide data-at-rest protection for credentials. Conformant OSes also provide access controls which allow users to keep their files private from other users of the same system. |
| O.PROTECTED_COMMS | To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSes provide mechanisms to create trusted channels for CSP and sensitive |

| | |
|---|---|
| | data. Both CSP and sensitive data should not be exposed outside of the platform. |

## 4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針は [PPOS] セクション4.2より転記した。

The following security objectives for the operational environment assist the OS in correctly providing its security functionality. These track with the assumptions about the environment.

Table 19: 運用環境のセキュリティ対策方針 [PPOS]

| Identifier | Description |
|---|---|
| OE.PLATFORM | The OS relies on being installed on trusted hardware. |
| OE.PROPER_USER | The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use. |
| OE.PROPER_ADMIN | The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy. |

## 4.3 セキュリティ対策方針根拠

セキュリティ対策方針根拠は [PPOS] セクション4.3より転記した。

This section describes how the assumptions, threats, and organizational security policies map to the security objectives.

Table 20: セキュリティ対策方針根拠

| Threat, Assumption, or OSP | Security Objectives | Rationale |
|---|---|---|
| T.NETWORK_ATTACK | O.PROTECTED_COMMS | The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS as this provides for integrity of transmitted data. |
| | O.INTEGRITY | The threat T.NETWORK_ATTACK is countered by O.INTEGRITY as this provides for integrity of software that is installed onto the system from the network. |
| | O.MANAGEMENT | The threat T.NETWORK_ATTACK is countered by O.MANAGEMENT as this provides for the ability to configure the OS to defend against network attack. |
| | O.ACCOUNTABILITY | The threat T.NETWORK_ATTACK is countered by O.ACCOUNTABILITY as this provides a mechanism for the OS to report behavior that may indicate a network attack has occurred. |
| T.NETWORK_EAVESDROP | O.PROTECTED_COMMS | The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS as this provides for confidentiality of transmitted data. |

| | | |
|---|---|---|
| | O.MANAGEMENT | The threat T.NETWORK_EAVESDROP is countered by O.MANAGEMENT as this provides for the ability to configure the OS to protect the confidentiality of its transmitted data. |
| T.LOCAL_ATTACK | O.INTEGRITY | The objective O.INTEGRITY protects against the use of mechanisms that weaken the TOE with regard to attack by other software on the platform. |
| | O.ACCOUNTABILITY | The objective O.ACCOUNTABILITY protects against local attacks by providing a mechanism to report behavior that may indicate a local attack is occurring or has occurred. |
| T.LIMITED_PHYSICAL_ACCESS | O.PROTECTED_STORAGE | The objective O.PROTECTED_STORAGE protects against unauthorized attempts to access physical storage used by the TOE. |
| A.PLATFORM | OE.PLATFORM | The operational environment objective OE.PLATFORM is realized through A.PLATFORM. |
| A.PROPER_USER | OE.PROPER_USER | The operational environment objective OE.PROPER_USER is realized through A.PROPER_USER. |
| A.PROPER_ADMIN | OE.PROPER_ADMIN | The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN. |

# 5 拡張コンポーネント定義

## 5.1 拡張セキュリティ機能コンポーネント

### Background and Scope

本STで導入されたすべての拡張コンポーネントは以下のTableで特定される。

Table 21: Extended Component Definitions

| Functional Class | Functional Components |
|---|---|
| **Cryptographic Support (FCS)** | FCS_CKM_EXT.4 Cryptographic Key Management |
| | FCS_RBG_EXT.1 Random Bit Generation |
| | FCS_STO_EXT.1 Storage of Sensitive Data |
| | FCS_SSH_EXT.1 SSH Protocol |
| | FCS_SSHC_EXT.1 SSH Client Protocol |
| | FCS_SSHS_EXT.1 SSH Server Protocol |
| | FCS_TLS_EXT.1 TLS Protocol |
| | FCS_TLSC_EXT.1 TLS Client Protocol |
| | FCS_TLSC_EXT.3 TLS Client Support for Signature Algorithms Extension |
| | FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension |
| **User Data Protection (FDP)** | FDP_ACF_EXT.1 Access Controls for Protecting User Data |
| **Identification and Authentication (FIA)** | FIA_X509_EXT.1 Authentication Using X.509 Certificates |
| **Security Management (FMT)** | FMT_MOF_EXT.1 Management of Functions Behavior |
| | FMT_SMF_EXT.1 Specification of Management Functions |
| **Protection of the TSF (FPT)** | FPT_ACF_EXT.1 Access Controls |
| | FPT_ASLR_EXT.1 Address Space Layout Randomization |
| | FPT_SBOP_EXT.1 Stack Buffer Overflow Protection |
| | FPT_SRP_EXT.1 Software Restriction Policies |
| | FPT_TST_EXT.1 Boot Integrity |
| | FPT_TUD_EXT.1 Integrity for Installation and Update |

| | |
|---|---|
| | FPT_TUD_EXT.2 Integrity for Installation and Update of Application Software |
| **Trusted Path/Channels (FTP)** | FTP_ITC_EXT.1 Trusted Channel Communication |

# Extended Component Definitions

## Class FCS: Cryptographic Support

### *FCS_CKM_EXT Cryptographic Key Management*

**Family Behavior**

This family defines requirements for key management. It differs from FCS_CKM in CC Part 2 by defining technology-specific details for the implementation of these functions.

**Component Leveling**


FCS_CKM_EXT.4, Cryptographic Key Destruction, requires the TSF to destroy cryptographic keys based on one or more specific methods, depending on the physical medium on which the key data is stored. Note that 4 was chosen for the family's sole component number to show that this requirement is similar to FCS_CKM.4, from which it was originally derived.

**Management: FCS_CKM_EXT.4**

There are no management activities foreseen.

**Audit: FCS_CKM_EXT.4**

There are no auditable events foreseen.

**FCS_CKM_EXT.4 Cryptographic Key Destruction**

Hierarchical to: No other components

Dependencies:

FCS_CKM.1 Cryptographic Key Generation

**FCS_CKM_EXT.4.1** The OS shall destroy cryptographic keys and key material in accordance with a specified cryptographic key destruction method [**selection**:

- *For volatile memory, the destruction shall be executed by a [**selection**:*
    - *single overwrite consisting of [**selection**: a pseudo-random pattern using the TSF's DRBG, zeroes, ones, a new value of a key [**assignment**: any value that does not contain any CSP]]*
    - *removal of power to the memory*
    - *destruction of reference to the key direction followed by a request for garbage collection ]*

• *For non-volatile memory that consists of [**selection**:*

○ *destruction of all key encrypting keys (KEKs) protecting the target key according to FCS_CKM_EXT.4.1, where none of the KEKs protecting the target key are derived* ○ *the invocation of an interface provided by the underlying platform that [**selection**:*

▪ *logically addresses the storage location of the key and performs a [**selection**: single, [**assignment**: ST author defined multi-pass] overwrite consisting of [**selection**: zeroes, ones, pseud-random pattern, a new value of a key of the same size, [**assignment**: any value that does not contain any CSP]]]*

▪ *instructs the underlying platform to destroy the abstraction that represents the key*

*]*

*]*

].

**FCS_CKM_EXT.4.2** The OS shall destroy all keys and key material when no longer needed.

## *FCS_RBG_EXT Random Bit Generation*

**Family Behavior**

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

**Component Leveling**


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**

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:

- Failure of the randomization process

**FCS_RBG_EXT.1 Random Bit Generation**

Hierarchical to: No other components

Dependencies: No dependencies

**FCS_RBG_EXT.1.1** The OS shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [**selection**:

- *Hash_DRBG (any)*
- *HMAC_DRBG (any)*
- *CTR_DRBG (AES)*

].

**FCS_RBG_EXT.1.2** The deterministic RBG used by the OS shall be seeded by an entropy source that accumulates entropy from a [**selection**:

- *software-based noise source*
- *platform-based noise source*

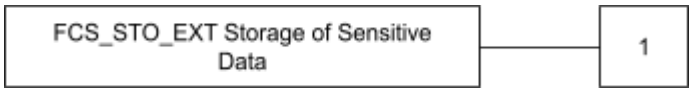
] with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

## *FCS_STO_EXT Storage of Sensitive Data*

**Family Behavior**

Components in this family describe the requirements for storing sensitive data (such as cryptographic keys). This is a new family defined for the FCS class.

**Component Leveling**




FCS_STO_EXT.1, Storage of Sensitive Data, requires the TSF to include a mechanism that encrypts sensitive data and that can be invoked by third-party applications in addition to internal TSF usage.

**Management: FCS_STO_EXT.1**

There are no management activities foreseen.

**Audit: FCS_STO_EXT.1**

There are no auditable events foreseen.

**FCS_STO_EXT.1 Storage of Sensitive Data**

Hierarchical to: No other components

Dependencies:

FCS_COP.1 Cryptographic Operation

**FCS_STO_EXT.1.1** The OS shall implement functionality to encrypt sensitive data stored in non-volatile storage and provide interfaces to applications to invoke this functionality.

## *FCS_SSH_EXT SSH Protocol*

**Family Behavior**

This family defines requirements for implementation of the SSH protocol that goes beyond the level of detail specified for trusted communications in CC Part 2.

**Component Leveling**


FCS_SSH_EXT.1, SSH Protocol, requires the TSF to specify the details of its SSH protocol implementation.

**Management: FCS_SSH_EXT.1**

No specific management functions are identified.

**Audit: FCS_SSH_EXT.1**

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP, PP-Module, FP, or ST:

- Failure to establish SSH connection
- Establishment of SSH connection
- Termination of SSH connection
- Dropping of packets outside defined size limits

**FCS_SSH_EXT.1 SSH Protocol**

Hierarchical to: No other components.

Dependencies:

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.2 Cryptographic Key Derivation

FCS_COP.1 Cryptographic Operation

FCS_RBG_EXT.1 Random Bit Generation

**FCS_SSH_EXT.1.1**

The TOE shall implement SSH acting as a [**selection:** client, server] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [**selection:** 4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308, 8332, 8709, 8731, no other RFCs] and [no other standard].

**FCS_SSH_EXT.1.2**

The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [**selection:**

- *"password" (RFC 4252),*
- *"keyboard-interactive" (RFC 4256),*
- *"publickey" (RFC 4252): [**selection:***
    - *ssh-rsa (RFC 4253),*
    - *rsa-sha2-256 (RFC 8332),*
    - *rsa-sha2-512 (RFC 8332),*
    - *ecdsa-sha2-nistp256 (RFC 5656),*
    - *ecdsa-sha2-nistp384 (RFC 5656),*
    - *ecdsa-sha2-nistp521 (RFC 5656),*
    - *ssh-ed25519 (RFC 8709),*
    - *ssh-ed448 (RFC 8709),*
    - *x509v3-ecdsa-sha2-nistp256 (RFC 6187),*
    - *x509v3-ecdsa-sha2-nistp384 (RFC 6187),*
    - *x509v3-ecdsa-sha2-nistp521 (RFC 6187),*
    - *x509v3-rsa2048-sha256 (RFC 6187)*

*]*

] and no other methods.

**FCS_SSH_EXT.1.3**

The TSF shall ensure that, as described in RFC 4253, packets greater than [**assignment:** number of bytes between 35,000 and 1 GB (inclusive)] in an SSH transport connection are dropped.

**FCS_SSH_EXT.1.4**

The TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [**selection:**

- *aes128-ctr (RFC 4344),*
- *aes256-ctr (RFC 4344),*
- *aes128-cbc (RFC 4253),*
- *aes256-cbc (RFC 4253),*
- *AEAD_AES_128_GCM (RFC 5647),*

- *AEAD_AES_256_GCM (RFC 5647),*
- *aes128-gcm@openssh.com (RFC 5647),*
- *aes256-gcm@openssh.com (RFC 5647)*

] and no other mechanisms.

**FCS_SSH_EXT.1.5**

The TSF shall protect data in transit from modification, deletion, and insertion using: [**selection:**

- *hmac-sha2-256 (RFC 6668),*
- *hmac-sha2-512 (RFC 6668),*
- *AEAD_AES_128_GCM (RFC 5647),*
- *AEAD_AES_256_GCM (RFC 5647),*
- *implicit*

] and no other mechanisms.

**FCS_SSH_EXT.1.6**

The TSF shall establish a shared secret with its peer using: [**selection:**

- *diffie-hellman-group14-sha256 (RFC 8268),*
- *diffie-hellman-group15-sha512 (RFC 8268),*
- *diffie-hellman-group16-sha512 (RFC 8268),*
- *diffie-hellman-group17-sha512 (RFC 8268),*
- *diffie-hellman-group18-sha512 (RFC 8268),*
- *ecdh-sha2-nistp256 (RFC 5656),*
- *ecdh-sha2-nistp384 (RFC 5656),*
- *ecdh-sha2-nistp521 (RFC 5656),*
- *curve25519-sha256 (RFC 8731),*
- *curve448-sha512 (RFC 8731)*

] and no other mechanisms.

**FCS_SSH_EXT.1.7**

The TSF shall use SSH KDF as defined in [**selection:**

- *RFC 4253 (Section 7.2),*
- *RFC 5656 (Section 4)*

] to derive the following cryptographic keys from a shared secret: session keys.

**FCS_SSH_EXT.1.8**

The TSF shall ensure that [**selection:**

- a rekey of the session keys,
- connection termination

] occurs when any of the following thresholds are met:

- one hour connection time
- no more than one gigabyte of transmitted data, or

- no more than one gigabyte of received data.

## *FCS_SSHC_EXT SSH Client Protocol*

**Family Behavior**

This family defines requirements for implementation of the SSH protocol when the TSF is acting as a client.

**Component Leveling**


FCS_SSHC_EXT.1, SSH Client Protocol, requires the TSF to specify the details of its SSH client implementation.

**Management: FCS_SSHC_EXT.1**

No specific management functions are identified.

**Audit: FCS_SSHC_EXT.1**

There are no auditable events foreseen.

**FCS_SSHC_EXT.1 SSH Client Protocol**

Hierarchical to: No other components.

Dependencies:

FCS_SSH_EXT.1 SSH Protocol

**FCS_SSHC_EXT.1.1**

The TSF shall authenticate its peer (SSH server) using: [**assignment**: *peer authentication method*] as described in RFC 4251, Section 4.1.

## *FCS_SSHS_EXT SSH Server Protocol*

**Family Behavior**

This family defines requirements for implementation of the SSH protocol when the TSF is acting as a server.

**Component Leveling**


FCS_SSHS_EXT.1, SSH Server Protocol, requires the TSF to specify the details of its SSH server implementation.

**Management: FCS_SSHS_EXT.1**

No specific management functions are identified.

**Audit: FCS_SSHS_EXT.1**

There are no auditable events foreseen.

**FCS_SSHS_EXT.1 SSH Server Protocol**

Hierarchical to: No other components.

Dependencies:

FCS_SSH_EXT.1 SSH Protocol

**FCS_SSHS_EXT.1.1**

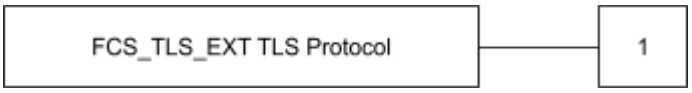
The TSF shall authenticate itself to its peer (SSH client) using: [**assignment**: *peer authentication method*].

## *FCS_TLS_EXT TLS Protocol*

**Family Behavior**

This family defines the TLS claims that can be made by a conformant TOE.

**Component Leveling**




FCS_TLS_EXT.1, TLS Protocol, requires the TSF to specify whether it implements TLS or DTLS as a client or as a server.

**Management: FCS_TLS_EXT.1**

No specific management functions are identified.

**Audit: FCS_TLS_EXT.1**

There are no auditable events foreseen.

**FCS_TLS_EXT.1 TLS Protocol**

Hierarchical to: No other components.

Dependencies: No dependencies.

**FCS_TLS_EXT.1.1**

The TSF shall implement [**selection:**

- *TLS as a client*
- *TLS as a server*
- *DTLS as a client*
- *DTLS as a server*

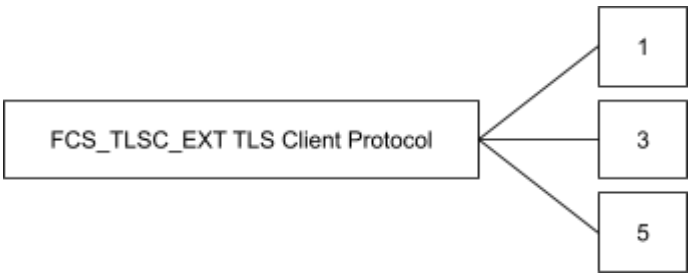
].

## *FCS_TLSC_EXT TLS Client Protocol*

**Family Behavior**

This family defines requirements for implementation of TLS as a client.

**Component Leveling**




FCS_TLSC_EXT.1, TLS Protocol, requires the TSF to specify whether it implements TLS as a client.

FCS_TLSC_EXT.3, TLS Client Support for signature_algorithms extension, is required to be in Client Hello.

FCS_TLSC_EXT.5, TLS Client Support for Supported Groups Extension, is required to be in Client Hello.

**Management: FCS_TLSC_EXT.1**

No specific management functions are identified.

**Audit: FCS_TLSC_EXT.1**

There are no auditable events foreseen.

**FCS_TLSC_EXT.1 TLS Client Protocol**

Hierarchical to: No other components.

Dependencies:

FCS_TLS_EXT.1 TLS Protocol

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.2 Cryptographic Key Derivation

FCS_COP.1 Cryptographic Operation

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 product shall implement TLS 1.2 (RFC 5246) and [**selection:** TLS 1.1 (RFC 4346), no earlier TLS versions] as a client that supports the cipher suites [**selection:**

- *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246,*
- *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_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*
- *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_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_128_GCM_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_ECDSA_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_128_GCM_SHA256 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*

] and also supports functionality for [**selection:**

- *mutual authentication,*
- *session renegotiation,*
- *none*

].

**FCS_TLSC_EXT.1.2**

The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

**FCS_TLSC_EXT.1.3**

The product shall not establish a trusted channel if the server certificate is invalid [**selection:**

- *with no exceptions,*
- *except when override is authorized*

].

**Management: FCS_TLSC_EXT.3**

No specific management functions are identified.

**Audit: FCS_TLSC_EXT.3**

There are no auditable events foreseen.

**FCS_TLSC_EXT.3 TLS Client Support for Signature Algorithms Extension**

Hierarchical to: No other components.

Dependencies: FCS_TLSC_EXT.1 TLS Client Protocol

**FCS_TLSC_EXT.3.1**

The product shall present the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [**selection:** *SHA256, SHA384, SHA512*] and no other hash algorithms.

**Management: FCS_TLSC_EXT.5**

No specific management functions are identified.

**Audit: FCS_TLSC_EXT.5**

There are no auditable events foreseen.

**FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension**

Hierarchical to: No other components.

Dependencies: FCS_TLSC_EXT.1 TLS Client Protocol

**FCS_TLSC_EXT.5.1**

The product shall present the Supported Groups Extension in the Client Hello with the supported groups [**selection:**

- *secp256r1,*
- *secp384r1,*
- *secp521r1,*
- *ffdhe2048(256),*
- *ffdhe3072(257),*
- *ffdhe4096(258),*
- *ffdhe6144(259),*
- *ffdhe8192(260)*

].

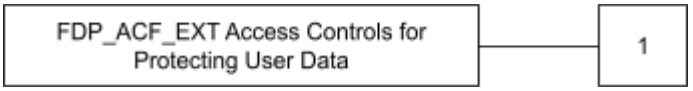
## Class FDP: User Data Protection

### *FDP_ACF_EXT Access Controls for Protecting User Data*

**Family Behavior**

This family specifies methods for ensuring that data stored or maintained by the TSF cannot be accessed without authorization. This family differs from FDP_ACF in CC Part 2 by defining technology-specific details for the implementation of these functions.

**Component Leveling**




FDP_ACF_EXT.1, Access Controls for Protecting User Data, requires the TSF to prevent unprivileged users from accessing operating system objects owned by other users.

**Management: FDP_ACF_EXT.1**

The following actions could be considered for the management functions in

FMT: • Configuration of object ownership and allowed access

**Audit: FDP_ACF_EXT.1**

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

- Successful and unsuccessful attempts to access data

**FDP_ACF_EXT.1 Access Controls for Protecting User Data**

Hierarchical to: No other components

Dependencies: No dependencies

**FDP_ACF_EXT.1.1** The OS shall implement access controls which can prohibit unprivileged users from accessing files and directories owned by other users.

## Class FIA: Identification and Authentication

### *FIA_X509_EXT Authentication Using X.509 Certificates*

**Family Behavior**

This family defines the behavior, 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 and use of certificates for authentication for protocols and integrity verification. This is a new family defined for the FIA class.

**Component Leveling**


FIA_X509_EXT.1, X.509 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, X.509 Certificate Authentication, requires the TSF to use certificates for authentication functions.

**Management: FIA_X509_EXT.1**

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

- Import and removal of X.509v3 certificates
- Approval of import and removal of X.509v3 certificates

**Audit: FIA_X509_EXT.1**

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

- Failure of certificate validation

**Management: FIA_X509_EXT.2**

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

- Import and removal of X.509v3 certificates
- Approval of import and removal of X.509v3 certificates

**Audit: FIA_X509_EXT.2**

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

- Success or failure of authentication attempt

**FIA_X509_EXT.1 X.509 Certificate Validation**

Hierarchical to: No other components

Dependencies:

FCS_COP.1 Cryptographic Operation

**FIA_X509_EXT.1.1** The OS shall implement functionality to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a trusted CA certificate
- The OS shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The TSF shall validate that any CA certificate includes "Certificate Signing" as a purpose the key usage field
- The OS shall validate the revocation status of the certificate using [**selection**: *OCSP as specified in RFC 6960, CRL as specified in RFC 8603, an OCSP TLS Status Request Extension (OCSP stapling) as specified in RFC 6066, OCSP TLS Multi-Certificate Status Request Extension (i.e., OCSP Multi Stapling) as specified in RFC 6961*] with [**selection**: *no exceptions, [**assignment**: exceptional use cases and alternative status check]*]
- The OS 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 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 TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
    - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU 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 EKU field.

- Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field. (conditional)

.

**FIA_X509_EXT.1.2** The OS 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 Certificate Validation

**FIA_X509_EXT.2.1** The OS shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [**selection**: *TLS, DTLS, HTTPS, [**assignment**: other protocols]*] connections.

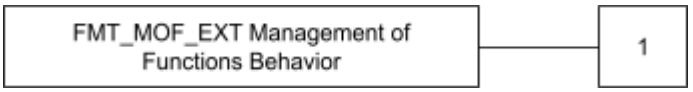
## Class FMT: Security Management

### *FMT_MOF_EXT Management of Functions Behavior*

**Family Behavior**

This family defines the administrative privileges required to modify the behavior of the security functions that are defined specifically for operating systems.

**Component Leveling**




FMT_MOF_EXT.1, Management of Security Functions Behavior, requires the TSF to define a set of management functions for the TOE and the privileges that are required to administer them.

**Management: FMT_MOF_EXT.1**

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

Configuration of the roles that may manage the behavior of the TSF management functions

**Audit: FMT_MOF_EXT.1**

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

- Successful or unsuccessful management of the behavior of any TOE functions
- Change in permissions to set of users that have the ability to manage a given

function **FMT_MOF_EXT.1 Management of Functions Behavior**

Hierarchical to: No other components

Dependencies: FMT_SMF_EXT.1 Specification of Management Functions

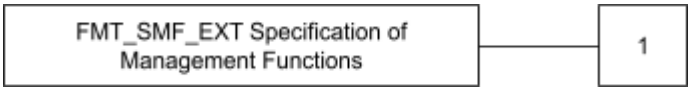
**FMT_MOF_EXT.1.1** The OS shall restrict the ability to perform the function indicated in the "Administrator" column in FMT_SMF_EXT.1.1 to the administrator.

### *FMT_SMF_EXT Specification of Management Functions*

**Family Behavior**

This family defines management functions that are defined specifically for operating systems.

**Component Leveling**




FMT_SMF_EXT.1, Specification of Management Functions, requires the TSF to define a set of management functions for the TOE.

**Management: FMT_SMF_EXT.1**

There are no management activities foreseen.

**Audit: FMT_SMF_EXT.1**

There are no auditable events foreseen.

**FMT_SMF_EXT.1 Specification of Management Functions**

Hierarchical to: No other components

Dependencies: No dependencies

**FMT_SMF_EXT.1.1** The OS shall be capable of performing the following management functions:

| # | Management Function | Administrator | User |
|---|---|---|---|
| 1 | Enable/disable [**selection**: *screen lock, session timeout*] | M | O |
| 2 | Configure [**selection**: *screen lock, session*] inactivity timeout | M | O |
| 3 | Import keys/secrets into the secure key storage | O | O |
| 4 | Configure local audit storage capacity | O | O |
| 5 | Configure minimum password length | O | O |
| 6 | Configure minimum number of special characters in password | O | O |
| 7 | Configure minimum number of numeric characters in password | O | O |

| # | Management Function | Administrator | User |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 8 | Configure minimum number of uppercase characters in password | O | O |
| 9 | Configure minimum number of lowercase characters in password | O | O |
| 10 | Configure lockout policy for unsuccessful authentication attempts through [**selection**: *timeouts between attempts, limiting number of attempts during a time period*] | O | O |
| 11 | Configure host-based firewall | O | O |
| 12 | Configure name/address of directory server with which to bind | O | O |
| 13 | Configure name/address of remote management server from which to receive management settings | O | O |
| 14 | Configure name/address of audit/logging server to which to send audit/logging records | O | O |
| 15 | Configure audit rules | O | O |
| 16 | Configure name/address of network time server | O | O |
| 17 | Enable/disable automatic software update | O | O |
| 18 | Configure Wi-Fi interface | O | O |
| 19 | Enable/disable Bluetooth interface | O | O |
| 20 | Enable/disable [***assignment**: list of other external interfaces*] | O | O |
| 21 | [***assignment**: list of other management functions to be provided by the TSF*] | O | O |

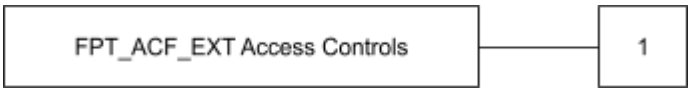
## Class FPT: Protection of the TSF

### *FPT_ACF_EXT Access Controls*

**Family Behavior**

This family defines specific TOE components that are protected against unprivileged access. This is a new family defined for the FPT class.

**Component Leveling**




FPT_ACF_EXT.1, Access Controls, requires the TSF to prohibit unauthorized users from reading or modifying specific TSF data.

**Management: FPT_ACF_EXT.1**

No specific management functions are identified.

**Audit: FPT_ACF_EXT.1**

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

- Unauthorized attempts to perform operations against protected data

**FPT_ACF_EXT.1 Access Controls**

Hierarchical to: No other components

Dependencies: No dependencies

**FPT_ACF_EXT.1.1** The OS shall implement access controls which prohibit unprivileged users from modifying:

- Kernel and its drivers/modules
- Security audit logs
- Shared libraries
- System executables
- System configuration files
- [**assignment***: other objects*]

.

**FPT_ACF_EXT.1.2** The OS shall implement access controls which prohibit unprivileged users from reading:

- Security audit logs
- System-wide credential repositories
- [**assignment***: list of other objects*]

.

## *FPT_ASLR_EXT Address Space Layout Randomization*

**Family Behavior**

This family defines the ability of the TOE to implement address space layout randomization (ASLR). This is a new family defined for the FPT class.

**Component Leveling**


FPT_ASLR_EXT.1, Address Space Layout Randomization, defines the ability of the TOE to use ASLR as well as the objects that ASLR is applied to.

**Management: FPT_ASLR_EXT.1**

There are no management functions foreseen.

**Audit: FPT_ASLR_EXT.1**

There are no auditable events foreseen.

**FPT_ASLR_EXT.1 Address Space Layout Randomization**

Hierarchical to: No other components

Dependencies: No dependencies

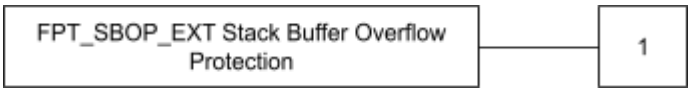
**FPT_ASLR_EXT.1.1** The OS shall always randomize process address space memory locations with [**selection**: *8,* [***assignment****: number greater than 8]*] bits of entropy except for [**assignment***: list of explicit exceptions*].

## *FPT_SBOP_EXT Stack Buffer Overflow Protection*

**Family Behavior**

This family requires the TSF to be compiled using stack-based buffer overflow protections. This is a new family defined for the FPT class.

**Component Leveling**




FPT_SBOP_EXT.1, Stack Buffer Overflow Protection, requires the TSF to be compiled using stack-based buffer overflow protections or to store data in such a manner that a stack-based buffer overflow cannot compromise the TSF.

**Management: FPT_SBOP_EXT.1**

There are no management functions foreseen.

**Audit: FPT_SBOP_EXT.1**

There are no auditable events foreseen.

**FPT_SBOP_EXT.1 Stack Buffer Overflow Protection**

Hierarchical to: No other components

Dependencies: No dependencies

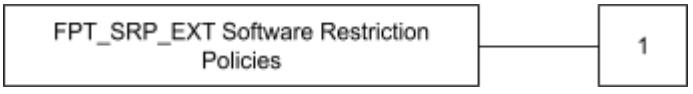
**FPT_SBOP_EXT.1.1** The OS shall [**selection**: *employ stack-based buffer overflow protections, not store parameters/variables in the same data structures as control values*].

## *FPT_SRP_EXT Software Restriction Policies*

**Family Behavior**

This family defines the ability of the TOE to restrict the execution of software unless it meets defined criteria. This is a new family defined for the FPT class.

**Component Leveling**




FPT_SRP_EXT.1, Software Restriction Policies, defines the criteria the TSF can use to prevent execution of restricted programs.

**Management: FPT_SRP_EXT.1**

The following actions could be considered for the management functions in

FMT: • Specification of restriction policies

**Audit: FPT_SRP_EXT.1**

There are no auditable events foreseen.

**FPT_SRP_EXT.1 Software Restriction Policies**

Hierarchical to: No other components

Dependencies: No dependencies

**FPT_SRP_EXT.1.1** The OS shall restrict execution to only programs which match an administrator specified [**selection**:

- *file path*
- *file digital signature*
- *version*
- *hash*
- *[**assignment**: other characteristics]*

].

## *FPT_TST_EXT Boot Integrity*

**Family Behavior**

This family defines the ability of the TOE to provide a mechanism that can be used to verify its integrity when started.

**Component Leveling**


FPT_TST_EXT.1, Boot Integrity, defines the mechanisms that the TSF uses to assert its own integrity at startup.

**Management: FPT_TST_EXT.1**

There are no management functions foreseen.

**Audit: FPT_TST_EXT.1**

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

- Failure of the integrity checking mechanism

**FPT_TST_EXT.1 Boot Integrity**

Hierarchical to: No other components
Dependencies:

FCS_COP.1 Cryptographic Operation

FIA_X509_EXT.1 X.509 Certificate Validation

**FPT_TST_EXT.1.1** The OS shall verify the integrity of the bootchain up through the OS kernel and [**selection**:

- *all executable code stored in mutable media*
- *[**assignment**: list of other executable code]*
- *no other executable code*

] prior to its execution through the use of [**selection**:

- *a digital signature using a hardware-protected asymmetric key*
- *a digital signature using an X509 certificate with hardware-based protection*
- *a hardware-protected hash*

].

## *FPT_TUD_EXT Trusted Update*

**Family Behavior**

This family defines the ability of the TOE to provide mechanisms for assuring the integrity of updates to the TSF or to non-TOE components that that rely on the TSF to function. This is a new family defined for the FPT class.

**Component Leveling**


FPT_TUD_EXT.1, Trusted Update, requires the TOE to provide a mechanism to verify the integrity of updates to itself.

FPT_TUD_EXT.2, Trusted Update for Application Software, requires the TOE to provide a mechanism to verify the integrity of updates to non-TSF applications that are running on the TOE.

**Management: FPT_TUD_EXT.1**

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

- Configuration of update checking mechanism
- Initiation of update

**Audit: FPT_TUD_EXT.1**

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

- Failure of the integrity checking mechanism
- Successful completion of updates

**Management: FPT_TUD_EXT.2**

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

- Configuration of update checking mechanism
- Initiation of update

**Audit: FPT_TUD_EXT.2**

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

- Failure of the integrity checking mechanism
- Successful completion of updates

**FPT_TUD_EXT.1 Integrity for Installation and Update**

Hierarchical to: No other components

Dependencies:

FCS_COP.1 Cryptographic Operation

**FPT_TUD_EXT.1.1** The OS shall provide the ability to check for updates to the OS software itself and shall use a digital signature scheme specified in FCS_COP.1/SIGN to validate the authenticity of the response.

**FPT_TUD_EXT.1.2** The OS shall [**selection**: *cryptographically verify, invoke platform-provided functionality to cryptographically verify*] updates to itself using a digital signature prior to installation using schemes specified in FCS_COP.1/SIGN.

**FPT_TUD_EXT.2 Integrity for Installation and Update of Application Software**

Hierarchical to: No other components

Dependencies:

FCS_COP.1 Cryptographic Operation

**FPT_TUD_EXT.2.1** The OS shall provide the ability to check for updates to application software and shall use a digital signature scheme specified in FCS_COP.1 to validate the authenticity of the response.

**FPT_TUD_EXT.2.2** The OS shall cryptographically verify the integrity of updates to applications using a digital signature specified by FCS_COP.1 prior to installation.

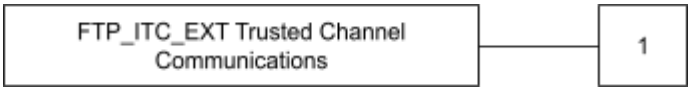
## Class FTP: Trusted Path/Channels

### *FTP_ITC_EXT Trusted Channel Communication*

**Family Behavior**

This family defines the ability of the TOE to use specific trusted communications channels to communicate with specific non-TOE entities in the Operational Environment. This family differs from FTP_ITC in Part 2 by defining technology-specific details for the implementation of these functions.

**Component Leveling**




FTP_ITC_EXT.1, Trusted channel communications, defines the specific secure communications protocols the TSF uses to communicate with a specific set of non-TOE entities in the Operational Environment.

**Management: FTP_ITC_EXT.1**

No specific management functions are identified.

**Audit: FTP_ITC_EXT.1**

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

- Initiation of trusted channel
- Termination of trusted channel
- Failure of trusted channel functions

**FTP_ITC_EXT.1 Trusted Channel Communication**

Hierarchical to: No other components

Dependencies:

[FCS_DTLS_EXT.1 DTLS Implementation or
FCS_IPSEC_EXT.1 IPsec or
FCS_SSH_EXT.1 SSH Protocol or
FCS_TLSC_EXT.1 TLS Client Protocol]

**FTP_ITC_EXT.1.1** The OS shall use [**selection***:*

- *TLS as conforming to the Functional Package for Transport Layer Security (TLS), version 1.1 as a [**selection**: client, server]*
- *DTLS as conforming to the Functional Package for Transport Layer Security (TLS), version 1.1 as a [**selection**: client, server]*
- *IPsec as conforming to the PP-Module for Virtual Private Network (VPN) Clients, version 2.4*
- *SSH as conforming to the Functional Package for Secure Shell (SSH), version 1.0 as a [**selection**: client, server]*

] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [**selection**: *audit server, authentication server, management server, [**assignment**: 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 disclosure and detection of modification of the channel data.

## 5.2 拡張保証コンポーネント

拡張保証コンポーネントの一覧を以下に示す。

Table 22: 拡張保証コンポーネント

| Requirements | source | Descriptions |
|---|---|---|
| ALC_TSU_EXT.1 | [PPOS] | Timely Security Updates |

### *Timely Security Updates (ALC_TSU_EXT)*

**Objectives**

This component requires the OS developer, in conjunction with any other necessary parties, to provide information as to how the end-user devices are updated to address security issues in a timely manner. The documentation describes the process of providing updates to the public from the time a security flaw is reported/discovered, to the time an update is released. This description includes the parties involved (e.g., the developer, carriers(s)) and the steps that are performed (e.g., developer testing, carrier testing), including worst case time periods, before an update is made available to the public.

**Component Leveling**

This family contains only one component.

**Application Notes:**

None.

**ALC_TSU_EXT.1 Timely Security Updates**

Dependencies: No dependencies

**Developer action elements:**

ALC_TSU_EXT.1.1D

The developer shall provide a description in the TSS of how timely security updates are made to the OS.

ALC_TSU_EXT.1.2D

The developer shall provide a description in the TSS of how users are notified when updates change security properties or the configuration of the product.

**Content and presentation elements:**

ALC_TSU_EXT.1.1C

The description shall include the process for creating and deploying security updates for the OS software.

ALC_TSU_EXT.1.2C

The description shall include the mechanisms publicly available for reporting security issues pertaining to the OS.

**Note:** The reporting mechanism could include web sites, email addresses, as well as a means to protect the sensitive nature of the report (e.g., public keys that could be used to encrypt the details of a proof-of-concept exploit).

**Evaluator action elements:**

ALC_TSU_EXT.1.1E

The evaluator will confirm that the information provided meets all requirements for content and presentation of evidence.

**Evaluation Activities**

ALC_TSU_EXT.1

The evaluator will verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator will verify that this description addresses the entire application. The evaluator will also verify that, in addition to the OS developer's process, any third-party processes are also addressed in the description. The evaluator will also verify that each mechanism for deployment of security updates is described. The evaluator will verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the OS patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator will verify that this time is expressed in a number or range of days. The evaluator will verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the OS.The evaluator will verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.

# 6 セキュリティ要件

本セクションでは、TOEのセキュリティ機能要件(SFR)とセキュリティ保証要件(SAR)を特定する。
本セクションに記載されるSFRは、適用可能なSelectionおよびAssignment操作を完了した[PPOS]、[PKGSSH]、および[PKGTLS]より転記した。

## 6.1 表記方法

本ドキュメントでは、[PPOS]によって定義された操作を完了するために、以下の規約に従う。

ボールド書式は、PPで完了または詳細化したことを示す。なお、本章に記載された取り消し線は、[PPOS]で既に実施された操作を示すものであり、本STでは操作は行っていない。
STで選択もしくは割り付けた値は、[]を示しその値をイタリック書式で示す。
繰返し操作は、SFR名にスラッシュ("/")と、操作の目的を表す一意の識別子を付加する。
拡張コンポーネントは、SFR識別に「_EXT」を追加して識別する。

## 6.2 セキュリティ機能要件

Table 23: セキュリティ機能要件の概要

| **Requirement** | **Title** |
|---|---|
| FAU_GEN.1 | Audit Data Generation (Refined) |
| FCS_CKM.1 | Cryptographic Key Generation (Refined) |
| FCS_CKM.2 | Cryptographic Key Establishment (Refined) |
| FCS_CKM_EXT.4 | Cryptographic Key Destruction |
| FCS_COP.1/ENCRYPT | Cryptographic Operation - Encryption/Decryption (Refined) |
| FCS_COP.1/HASH | Cryptographic Operation - Hashing (Refined) |
| FCS_COP.1/SIGN | Cryptographic Operation - Signing (Refined) |
| FCS_COP.1/KEYHMAC | Cryptographic Operation - Keyed-Hash Message Authentication (Refined) |
| FCS_RBG_EXT.1/KCAPI | Random Bit Generation (Kernel) |
| FCS_RBG_EXT.1/OSSL | Random Bit Generation (OpenSSL) |
| FCS_STO_EXT.1 | Storage of Sensitive Data |
| FCS_SSH_EXT.1 | SSH Protocol |

| | |
|---|---|
| FCS_SSHC_EXT.1 | SSH Protocol - Client |
| FCS_SSHS_EXT.1 | SSH Protocol - Server |
| FCS_TLS_EXT.1 | TLS Protocol |
| FCS_TLSC_EXT.1 | TLS Client Protocol |
| FCS_TLSC_EXT.3 | TLS Client Support for Signature Algorithms Extension |
| FCS_TLSC_EXT.5 | TLS Client Support for Supported Groups Extension |
| FDP_ACF_EXT.1 | Access Controls for Protecting User Data |
| FIA_AFL.1 | Authentication failure handling (Refined) |
| FIA_UAU.5 | Multiple Authentication Mechanisms (Refined) |
| FIA_X509_EXT.1 | X.509 Certificate Validation |
| FIA_X509_EXT.2 | X.509 Certificate Authentication |
| FMT_MOF_EXT.1 | Management of security functions behavior |
| FMT_SMF_EXT.1 | Specification of Management Functions |
| FPT_ACF_EXT.1 | Access controls |
| FPT_ASLR_EXT.1 | Address Space Layout Randomization |
| FPT_SBOP_EXT.1 | Stack Buffer Overflow Protection |
| FPT_SRP_EXT.1 | Software Restriction Policies |
| FPT_TST_EXT.1 | Boot Integrity |
| FPT_TUD_EXT.1 | Trusted Update |
| FPT_TUD_EXT.2 | Trusted Update for Application Software |
| FTA_TAB.1 | Default TOE access banners |
| FTP_ITC_EXT.1 | Trusted channel communication |
| FTP_TRP.1 | Trusted Path |

### 6.2.1 Security Audit (FAU)

| **FAU_GEN.1** | **Audit Data Generation (Refined)** |
|---|---|
| FAU_GEN.1.1 | The **OS** shall be able to generate an audit record of the following auditable events:<br><br>a) Start-up and shut-down of the audit functions;<br>b) All auditable events for the **not specified** level of audit; and [<br>c)<br>● *Authentication events (Success/Failure);*<br>● *Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes);*<br>● *Privilege or role escalation events (Success/Failure);*<br>● *[*<br>○ *File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions)*<br>○ *User and Group management events (Successful and unsuccessful add, delete, modify, disable, enable, and credential change)*<br>○ *Audit and log data access events (Success/Failure)*<br>○ *Cryptographic verification of software (Success/Failure)*<br>○ *Attempted application invocation with arguments (Success/Failure e.g. due to software restriction policy)*<br>○ *System reboot, restart, and shutdown events (Success/Failure)*<br>○ *Kernel module loading and unloading events (Success/Failure)*<br>○ *Administrator or root-level access events (Success/Failure)*<br>○ *[**assignment**: specifically defined auditable events listed in Table 24].*<br>*]*<br>] |
| FAU_GEN.1.2 | The **OS** shall record within each audit record at least the following information:<br><br>a) Date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event;<br>and<br><br>b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**assignment**: *information specified in column 3 of Table 24*] |

Table 24. SSH Auditable Events

| Requirement | Auditable Events | Additional Audit Record Contents |
|---|---|---|
| FCS_SSH_EXT.1 | [*Failure to establish SSH connection*] | [*Reason for failure and Non-TOE endpoint of attempted connection (IP Address)*] |
| FCS_SSH_EXT.1 | [*Establishment of SSH connection*] | [*Non-TOE endpoint of connection (IP Address)*] |
| FCS_SSH_EXT.1 | [*Termination of SSH connection session*] | [*Non-TOE endpoint of connection (IP Address)*] |
| FCS_SSH_EXT.1 | [*No events specified.*] | [*None*] |
| FCS_SSHC_EXT.1 | [*No events specified.*] | [*None*] |
| FCS_SSHS_EXT.1 | [*No events specified.*] | [*None*] |

**Application Note:** This table has been modified by TD0777.

### 6.2.2 Cryptographic Support (FCS)

| FCS_CKM.1 | Cryptographic Key Generation (Refined) |
|---|---|
| FCS_CKM.1.1 | The **OS** shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [<br>● *RSA schemes using cryptographic key sizes of 3072-bit and 4096-bit that meet the following: FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.1*<br>● *ECC schemes using "NIST curves" P-384 and [P-521] that meet the following: FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2*<br>● *FFC schemes using [safe primes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes"]*<br>]. |

**Application Note:** This SFR has been modified by TD0955 and TD0712.

| FCS_CKM.2 | Cryptographic Key Establishment (Refined) |
|---|---|
| FCS_CKM.2.1 | The OS shall **implement functionality to perform cryptographic key establishment** in accordance with a specified cryptographic key **establishment** method: [<br>● *Elliptic curve-based key establishment schemes that* |

| | |
|---|---|
| | *meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"*<br>● *Finite field-based key establishment schemes that meets NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"*<br>]. |

| **FCS_CKM_EXT.4** | **Cryptographic Key Destruction** |
|---|---|
| FCS_CKM_EXT.4.1 | The OS shall destroy cryptographic keys and key material in accordance with a specified cryptographic key destruction method [<br>● *For volatile memory, the destruction shall be executed by a [*<br>○ *single overwrite consisting of [zeroes]*<br>○ *removal of power to the memory*<br>*]*<br>● *For non-volatile memory that consists of [*<br>○ *the invocation of an interface provided by the underlying platform that [*<br>■ *logically addresses the storage location of the key and performs a [[**assignment**: administrator specified number (default of 3) of]] overwrite consisting of [pseudo-random pattern]*<br>*]*<br>*]*<br>]. |
| FCS_CKM_EXT.4.2 | The OS shall destroy all keys and key material when no longer needed. |

| **FCS_COP.1/ENCRYPT** | **Cryptographic Operation – Encryption/Decryption (Refined)** |
|---|---|
| FCS_COP.1.1/ENCRYPT | The **OS** shall perform **encryption/decryption services for data** in accordance with a specified cryptographic algorithm **[**<br>● ***AES-XTS (as defined in NIST SP 800-38E)***<br>● ***AES-CBC (as defined in NIST SP 800-38A)***<br>● ***AES-CTR (as defined in NIST SP 800-38A)***<br>**] and [**<br>● ***AES-GCM (as defined in NIST SP 800-38D)***<br>**]** and cryptographic key sizes 256-bit and [*no other bit size*]<br>~~**that meet the following: [assignment: list of standards].**~~ |

**Application Note:** This SFR has been modified by TD0712.

| **FCS_COP.1/HASH** | **Cryptographic Operation – Hashing (Refined)** |
|---|---|
| FCS_COP.1.1/HASH | The **OS** shall perform **cryptographic hashing services** in accordance with a specified cryptographic algorithm **[**<br>● ***SHA-256***<br>● ***SHA-384***<br>● ***SHA-512***<br>**] and message digest sizes [**<br>● ***256 bits***<br>● ***384 bits***<br>● ***512 bits***<br>**]** that meet the following: **FIPS Pub 180-4**. |

**Application Note:** This SFR has been modified by TD0696.

| **FCS_COP.1/SIGN** | **Cryptographic Operation – Signing (Refined)** |
|---|---|
| FCS_COP.1.1/SIGN | The **OS** shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm **[**<br>● ***RSA schemes using cryptographic key sizes of [2048-bit (for secure boot only) or greater] that meet the following: FIPS PUB 186-4 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5***<br>● ***ECDSA schemes using "NIST curves" P-384 and [P-521] that meet the following: FIPS PUB 186-4 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6, SP 800-186 Section 3***<br>**] ~~and cryptographic key sizes [assignment: cryptographic algorithm] that meet the following. [assignment: list of standards]~~.** |

**Application Note:** This SFR has been modified by TD0955.

| **FCS_COP.1/KEYHMAC** | **Cryptographic Operation – Keyed-Hash Message Authentication (Refined)** |
|---|---|
| FCS_COP.1.1/KEYHMAC | The **OS** shall perform **keyed-hash message authentication services** in accordance with a specified cryptographic algorithm **[*SHA-256, SHA-384, SHA-512*] with key sizes [*assignment: 256-bits, 384-bits,512-bits*] and message digest** sizes [*256 bits, 384 bits,512 bits*] that meet the following: [*FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard*]. |

**Application Note:** This SFR has been modified by TD0696.

| FCS_RBG_EXT.1/KCAPI | Random Bit Generation (Kernel) |
|---|---|
| FCS_RBG_EXT.1.1/KCAPI | The OS shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [<br>● *HMAC_DRBG (SHA-512)*<br>] . |
| FCS_RBG_EXT.1.2/KCAPI | The deterministic RBG used by the OS shall be seeded by an entropy source that accumulates entropy from a [<br>● *software-based noise source*<br>] with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate. |

| FCS_RBG_EXT.1/OSSL | Random Bit Generation (OpenSSL) |
|---|---|
| FCS_RBG_EXT.1.1/OSSL | The OS shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [<br>● *CTR_DRBG (AES)*<br>] . |
| FCS_RBG_EXT.1.2/OSSL | The deterministic RBG used by the OS shall be seeded by an entropy source that accumulates entropy from a [<br>● *software-based noise source*<br>] with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate. |

| FCS_STO_EXT.1 | Storage of Sensitive Data |
|---|---|
| FCS_STO_EXT.1.1 | The OS shall implement functionality to encrypt sensitive data stored in non-volatile storage and provide interfaces to applications to invoke this functionality. |

| FCS_SSH_EXT.1 | SSH Protocol |
|---|---|
| FCS_SSH_EXT.1.1 | The TOE shall implement SSH acting as a [*client, server*] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [*4344, 5647, 5656, 6668, 8268, 8308, 8332*] and [*no other standard*]. |

| | |
|---|---|
| FCS_SSH_EXT.1.2 | The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [<br>● *"password" (RFC 4252),*<br>● *"publickey" (RFC 4252): [*<br>○ *rsa-sha2-256 (RFC 8332),*<br>○ *rsa-sha2-512 (RFC 8332),*<br>○ *ecdsa-sha2-nistp384 (RFC 5656),*<br>○ *ecdsa-sha2-nistp521 (RFC 5656),*<br>*]*<br>] and no other methods. |
| FCS_SSH_EXT.1.3 | The TSF shall ensure that, as described in RFC 4253, packets greater than [**assignment**: *262144 bytes*] in an SSH transport connection are dropped. |
| FCS_SSH_EXT.1.4 | The TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [<br>● *aes256-ctr (RFC 4344),*<br>● *aes256-gcm@openssh.com (RFC 5647)*<br>] and no other mechanisms. |
| FCS_SSH_EXT.1.5 | The TSF shall protect data in transit from modification, deletion, and insertion using: [<br>● *hmac-sha2-256 (RFC 6668),*<br>● *hmac-sha2-512 (RFC 6668),*<br>● *Implicit*<br>] and no other mechanisms. |
| FCS_SSH_EXT.1.6 | The TSF shall establish a shared secret with its peer using: [<br>● *diffie-hellman-group16-sha512 (RFC 8268),*<br>● *diffie-hellman-group18-sha512 (RFC 8268),*<br>● *ecdh-sha2-nistp384 (RFC 5656),*<br>● *ecdh-sha2-nistp521 (RFC 5656),*<br>] and no other mechanisms. |
| FCS_SSH_EXT.1.7 | The TSF shall use SSH KDF as defined in [<br>● *RFC 4253 (Section 7.2),*<br>● *RFC 5656 (Section 4)*<br>] to derive the following cryptographic keys from a shared secret: session keys. |
| FCS_SSH_EXT.1.8 | The TSF shall ensure that [<br>● *a rekey of the session keys*<br>] occurs when any of the following thresholds are met:<br>● one hour connection time<br>● no more than one gigabyte of transmitted data, or<br>● no more than one gigabyte of received data. |

| | |
|---|---|
| **FCS_SSHC_EXT.1** | **SSH Protocol - Client** |

| | |
|---|---|
| FCS_SSHC_EXT.1.1 | The TSF shall authenticate its peer (SSH server) using: [<br>● *using a local database by associating each host name with a public key corresponding to the following list: [*<br>○ *rsa-sha2-256 (RFC 8332),*<br>○ *rsa-sha2-512 (RFC 8332),*<br>○ *ecdsa-sha2-nistp384 (RFC 5656),*<br>○ *ecdsa-sha2-nistp521 (RFC 5656),*<br>*] ,*<br>] as described in RFC 4251 Section 4.1. |

| **FCS_SSHS_EXT.1** | **SSH Protocol - Server** |
|---|---|
| FCS_SSHS_EXT.1.1 | The TSF shall authenticate itself to its peer (SSH Client) using: [<br>● *rsa-sha2-256 (RFC 8332),*<br>● *rsa-sha2-512 (RFC 8332),*<br>● *ecdsa-sha2-nistp384 (RFC 5656),*<br>● *ecdsa-sha2-nistp521 (RFC 5656),*<br>]. |

| **FCS_TLS_EXT.1** | **TLS Protocol** |
|---|---|
| FCS_TLS_EXT.1.1 | The product shall implement [<br>● *TLS as a client,*<br>]. |

| **FCS_TLSC_EXT.1** | **TLS Client Protocol** |
|---|---|
| FCS_TLSC_EXT.1.1 | The product shall implement TLS 1.2 (RFC 5246) and [*no earlier TLS versions*] as a client that supports the cipher suites [<br>● *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,*<br>● *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,*<br>● *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*<br>] and also supports functionality for [<br>● *none*<br>]. |
| FCS_TLSC_EXT.1.2 | The product shall verify that the presented identifier matches the reference identifier according to RFC 6125. |
| FCS_TLSC_EXT.1.3 | The product shall not establish a trusted channel if the server certificate is invalid [<br>● *with no exceptions,* |

| | |
|---|---|
| | ]. |

**Application Note:** This SFR has been modified by TD0442.

| **FCS_TLSC_EXT.3** | **TLS Client Support for Signature Algorithms Extension** |
|---|---|
| FCS_TLSC_EXT.3.1 | The product shall present the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [*SHA256, SHA384, SHA512*] and no other hash algorithms. |

| **FCS_TLSC_EXT.5** | **TLS Client Support for Supported Groups Extension** |
|---|---|
| FCS_TLSC_EXT.5.1 | The product shall present the Supported Groups Extension in the Client Hello with the supported groups [<br>● *secp384r1*<br>● *secp521r1*<br>]. |

### 6.2.3 User Data Protection (FDP)

| **FDP_ACF_EXT.1** | **Access Controls for Protecting User Data** |
|---|---|
| FDP_ACF_EXT.1.1 | The OS shall implement access controls which can prohibit unprivileged users from accessing files and directories owned by other users. |

### 6.2.4 Identification and Authentication (FIA)

| **FIA_AFL.1** | **Authentication Failure Handling (Refined)** |
|---|---|
| FIA_AFL.1.1 | The **OS** shall detect when [<br>● *an administrator configurable positive integer within [**assignment**: 1 – 65,535]*<br>] unsuccessful authentication attempts occur related to **events with [**<br>● ***authentication based on user name and password***<br>**]** . |
| FIA_AFL.1.2 | When the defined number of unsuccessful authentication attempts for an account has been **met**, the **OS** shall: **[*Account*** |

| | |
|---|---|
| | ***Lockout***]. |

| **FIA_UAU.5** | **Multiple Authentication Mechanisms (Refined)** |
|---|---|
| FIA_UAU.5.1 | The **OS** shall provide the following authentication mechanisms **[**<br>● ***authentication based on username and password***<br>● ***for use in SSH only, SSH public key-based authentication as specified by the Functional Package for Secure Shell (SSH), version 1.0***<br>**]** to support user authentication. |
| FIA_UAU.5.2 | The **OS** shall authenticate any user's claimed identity according to the [assignment: *username and password: used at the local console and over SSH: the TOE locally verifies the password hash matches the stored password hash associated with the provided username;*<br>*SSH public key: used over SSH: the TOE verifies the signature can be verified using a public key in the authorized_keys file associated with the provided username*]. |

| **FIA_X509_EXT.1** | **X.509 Certificate Validation** |
|---|---|
| FIA_X509_EXT.1.1 | The OS shall implement functionality to validate certificates in accordance with the following rules:<br>● RFC 5280 certificate validation and certificate path validation<br>● The certificate path must terminate with a trusted CA certificate<br>● The OS shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.<br>● The TSF shall validate that any CA certificate includes "Certificate Signing" as a purpose the key usage field<br>● The OS shall validate the revocation status of the certificate using [*an OCSP TLS Status Request Extension (OCSP stapling) as specified in RFC 6066*] with [*no exceptions*]<br>● The OS shall validate the extendedKeyUsage field according to the following rules:<br>○ 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.<br>○ Server certificates presented for 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.<br>○ Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.<br>○ S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.<br>○ 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 EKU field.<br>○ Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.(conditional) |
| FIA_X509_EXT.1.2 | The OS 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 OS shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [*TLS, HTTPS*] connections. |

**Application Note:** This SFR has been modified by TD0789.

### 6.2.5 Security Management (FMT)

| **FMT_MOF_EXT.1** | **Management of Security Functions Behavior** |
|---|---|
| FMT_MOF_EXT.1.1 | The OS shall restrict the ability to perform the function indicated in the "Administrator" column in FMT_SMF_EXT.1.1 to the administrator. |

| **FMT_SMF_EXT.1** | **Specification of Management Functions** |
|---|---|
| FMT_SMF_EXT.1.1 | The OS shall be capable of performing the following management functions: |

Table 25: Management Functions

| # | Management Function | Administrator | User |
|---|---|---|---|
| 1 | Enable/disable [*session timeout*] | M | - |
| 2 | Configure [*session*] inactivity timeout | M | - |
| 3 | Import keys/secrets into the secure key storage | M | - |
| 4 | Configure local audit storage capacity | M | - |
| 5 | Configure minimum password length | M | - |
| 6 | Configure minimum number of special characters in password | M | - |
| 7 | Configure minimum number of numeric characters in password | M | - |
| 8 | Configure minimum number of uppercase characters in password | M | - |
| 9 | Configure minimum number of lowercase characters in password | M | - |
| 10 | Configure lockout policy for unsuccessful authentication attempts through [*timeouts between attempts*] | M | - |
| 11 | Configure host-based firewall | M | - |
| 12 | Configure name/address of directory server with which to bind | - | - |
| 13 | Configure name/address of remote management server from which to receive management settings | - | - |
| 14 | Configure name/address of audit/logging server to which to send audit/logging records | M | - |
| 15 | Configure audit rules | M | - |
| 16 | Configure name/address of network time server | M | - |
| 17 | Enable/disable automatic software update | M | - |
| 18 | Configure WiFi interface | - | - |
| 19 | Enable/disable Bluetooth interface | - | - |
| 20 | Enable/disable [**assignment**: *no other external interfaces*] | - | - |
| 21 | [**assignment**: *Configuration of object ownership and* | M | - |

| | | | |
|---|---|---|---|
| | *allowed access, Configuration of the roles that may manage the behavior of the TSF management functions*] | | |

**Application Note:** This table has been modified by TD0693.

## 6.2.6 Protection of the TSF (FPT)

| **FPT_ACF_EXT.1** | **Access Controls** |
|---|---|
| FPT_ACF_EXT.1.1 | The OS shall implement access controls which prohibit unprivileged users from modifying:<br>● Kernel and its drivers/modules<br>● Security audit logs<br>● Shared libraries<br>● System executables<br>● System configuration files<br>● [**assignment**: *no other objects*] |
| FPT_ACF_EXT.1.2 | The OS shall implement access controls which prohibit unprivileged users from reading:<br>● Security audit logs<br>● System-wide credential repositories<br>● [**assignment**: *no other objects*] |

| **FPT_ASLR_EXT.1** | **Address Space Layout Randomization** |
|---|---|
| FPT_ASLR_EXT.1.1 | The OS shall always randomize process address space memory locations with [***[assignment**: at least 22]*] bits of entropy except for [**assignment**: *no exceptions*]. |

| **FPT_SBOP_EXT.1** | **Stack Buffer Overflow Protection** |
|---|---|
| FPT_SBOP_EXT.1.1 | The OS shall [*employ stack-based buffer overflow protections*]. |

| **FPT_SRP_EXT.1** | **Software Restriction Policies** |
|---|---|
| FPT_SRP_EXT.1.1 | The OS shall restrict execution to only programs which match an administrator-specified [<br>● *file path*<br>● *hash*<br>] . |

| **FPT_TST_EXT.1** | **Boot Integrity** |
|---|---|
| FPT_TST_EXT.1.1 | The OS shall verify the integrity of the bootchain up through the |

| | |
|---|---|
| | OS kernel and [<br>● *no other executable code*<br>] prior to its execution through the use of [<br>● *a digital signature using a hardware-protected asymmetric key*<br>] . |

| **FPT_TUD_EXT.1** | **Trusted Update** |
|---|---|
| FPT_TUD_EXT.1.1 | The OS shall provide the ability to check for updates to the OS software itself and shall use a digital signature scheme specified in FCS_COP.1/SIGN to validate the authenticity of the response. |
| FPT_TUD_EXT.1.2 | The OS shall [*cryptographically verify*] updates to itself using a digital signature prior to installation using schemes specified in FCS_COP.1/SIGN. |

| **FPT_TUD_EXT.2** | **Trusted Update for Application Software** |
|---|---|
| FPT_TUD_EXT.2.1 | The OS shall provide the ability to check for updates to application software and shall use a digital signature scheme specified in FCS_COP.1/SIGN to validate the authenticity of the response. |
| FPT_TUD_EXT.2.2 | The OS shall cryptographically verify the integrity of updates to applications using a digital signature specified by FCS_COP.1/SIGN prior to installation. |

### 6.2.7 TOE Access (FTA)

| **FTA_TAB.1** | **Default TOE Access Banners** |
|---|---|
| FTA_TAB.1.1 | Before establishing a user session, the **OS** shall display an advisory warning message regarding unauthorized use of the OS. |

### 6.2.8 Trusted Path/Channels (FTP)

| **FTP_ITC_EXT.1** | **Trusted Channel Communication** |
|---|---|
| FTP_ITC_EXT.1.1 | The OS shall use [<br>● *TLS as conforming to the Functional Package for Transport Layer Security (TLS), version 1.1 as a [client]*<br>*]*<br>*and [*<br>● *SSH as conforming to the Functional Package for Secure Shell (SSH), version 1.0 as a [client, server]*<br>*]*<br>] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [*audit server, [**assignment**: application initiated TLS, software updates, remote administration via SSH, connections to remote SSH servers]*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data. |

**Application Note:** This SFR has been modified by TD0789.

| **FTP_TRP.1** | **Trusted Path** |
|---|---|
| FTP_TRP.1.1 | The **OS** shall provide a communication path between itself and [*remote, local*] users that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communicated data from **modification, disclosure**. |
| FTP_TRP.1.2 | The **OS** shall permit [*local users, remote users*] to initiate communication via the trusted path. |
| FTP_TRP.1.3 | The **OS** shall require use of the trusted path for [*initial user authentication,* **all remote administrative actions**]. |

**Application Note:** This SFR has been modified by TD0839.

## 6.3 セキュリティ機能要件の依存性

Table 26は、Common Criteriaが規定するセキュリティ機能要件に要求される依存性と、TOEで満たしている依存性、依存性を満たしていない理由を示す。Table 27は、TOEが依存性を満たしていないことの正当性を示すもので[PPOS] Appendix.Dより転記した。これら2つのTableは、依存性を満たしていないセキュリティ機能要件名により対応付けられる。

Table 26: 依存分析表

| 機能要件 | 要求される依存性 | **TOE**で満たしている依存性 | 依存性を満たしていない理由 |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | なし | Table 27参照 (FPT_STM.1- Reliable timestamps) |
| FCS_CKM.1 | [FCS_CKM.2 or FCS_COP.1] FCS_CKM.4 | FCS_CKM.2 | FCS_CKM.4は、拡張コンポーネント FCS_CKM_EXT.4が定義されているため、依存性を満たしていなくても問題ない。 |
| FCS_CKM.2 | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 | FCS_CKM.1 | FCS_CKM.4は、拡張コンポーネント FCS_CKM_EXT.4が定義されているため、依存性を満たしていなくても問題ない。 |
| FCS_CKM_EXT.4 | FCS_CKM.1 | FCS_CKM.1 | |
| FCS_COP.1/ ENCRYPT | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 | FCS_CKM.1 | FCS_CKM.4は、拡張コンポーネント FCS_CKM_EXT.4が定義されているため、依存性を満たしていなくても問題ない。 |
| FCS_COP.1/HASH | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 | FCS_CKM.1 | FCS_CKM.4は、拡張コンポーネント FCS_CKM_EXT.4が定義されているため、依存性を満たしていなくても問題ない。 |
| FCS_COP.1/SIGN | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 | FCS_CKM.1 | FCS_CKM.4は、拡張コンポーネント FCS_CKM_EXT.4が定義されているため、依存 |

| | | | |
|---|---|---|---|
| | | | 性を満たしていなくても問題ない。 |
| FCS_COP.1/KEYHMAC | [FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4 | FCS_CKM.1 | FCS_CKM.4は、拡張コンポーネントFCS_CKM_EXT.4が定義されているため、依存性を満たしていなくても問題ない。 |
| FCS_RBG_EXT.1/KCAPI | なし | なし | |
| FCS_RBG_EXT.1/OSSL | なし | なし | |
| FCS_STO_EXT.1 | FCS_COP.1 | FCS_COP.1/ENCRYPT<br>FCS_COP.1/HASH<br>FCS_COP.1/KEYHMAC | |
| FCS_SSH_EXT.1 | FCS_CKM.1<br>FCS_CKM.2<br>FCS_COP.1<br>FCS_RBG_EXT.1 | FCS_CKM.1<br>FCS_CKM.2<br>FCS_COP.1/ENCRYPT<br>FCS_COP.1/HASH<br>FCS_COP.1/SIGN<br>FCS_COP.1/KEYHMAC<br>FCS_RBG_EXT.1/OSSL | |
| FCS_SSHC_EXT.1 | FCS_SSH_EXT.1 | FCS_SSH_EXT.1 | |
| FCS_SSHS_EXT.1 | FCS_SSH_EXT.1 | FCS_SSH_EXT.1 | |
| FCS_TLS_EXT.1 | なし | なし | |
| FCS_TLSC_EXT.1 | FCS_TLS_EXT.1<br>FCS_CKM.1<br>FCS_CKM.2<br>FCS_COP.1<br>FCS_RBG_EXT.1<br>FIA_X509_EXT.1<br>FIA_X509_EXT.2 | FCS_TLS_EXT.1<br>FCS_CKM.1<br>FCS_CKM.2<br>FCS_COP.1/ENCRYPT<br>FCS_COP.1/HASH<br>FCS_COP.1/SIGN<br>FCS_COP.1/KEYHMAC<br>FCS_RBG_EXT.1/OSSL<br>FIA_X509_EXT.1<br>FIA_X509_EXT.2 | |
| FCS_TLSC_EXT.3 | FCS_TLSC_EXT.1 | FCS_TLSC_EXT.1 | |
| FCS_TLSC_EXT.5 | FCS_TLSC_EXT.1 | FCS_TLSC_EXT.1 | |
| FDP_ACF_EXT.1 | なし | なし | |
| FIA_AFL.1 | FIA_UAU.1 | なし | Table 27参照 |

| | | | |
|---|---|---|---|
| | | | (FIA_UAU.1 - Timing of authentication) |
| FIA_UAU.5 | なし | なし | |
| FIA_X509_EXT.1 | FCS_COP.1 | FCS_COP.1/HASH<br>FCS_COP.1/SIGN | |
| FIA_X509_EXT.2 | FIA_X509_EXT.1 | FIA_X509_EXT.1 | |
| FMT_MOF_EXT.1 | FMT_SMF_EXT.1 | FMT_SMF_EXT.1 | |
| FMT_SMF_EXT.1 | なし | なし | |
| FPT_ACF_EXT.1 | なし | なし | |
| FPT_ASLR_EXT.1 | なし | なし | |
| FPT_SBOP_EXT.1 | なし | なし | |
| FPT_SRP_EXT.1 | なし | なし | |
| FPT_TST_EXT.1 | FCS_COP.1<br>FIA_X509_EXT.1 | FCS_COP.1/HASH<br>FCS_COP.1/SIGN<br>FIA_X509_EXT.1 | |
| FPT_TUD_EXT.1 | FCS_COP.1 | FCS_COP.1/HASH<br>FCS_COP.1/SIGN | |
| FPT_TUD_EXT.2 | FCS_COP.1 | FCS_COP.1/HASH<br>FCS_COP.1/SIGN | |
| FTA_TAB.1 | なし | なし | |
| FTP_ITC_EXT.1 | [FCS_DTLS_EXT.1 or<br>FCS_IPSEC_EXT.1 or<br>FCS_SSH_EXT.1 or<br>FCS_TLSC_EXT.1] | FCS_SSH_EXT.1<br>FCS_TLSC_EXT.1 | |
| FTP_TRP.1 | なし | なし | |

Table 27 セキュリティ要件の依存関係が満たされていないことの正当性

| Requirement | Rationale for Satisfaction |
|---|---|
| FIA_UAU.1 - Timing of authentication | FIA_AFL.1 implicitly requires that the OS perform all necessary actions, including those on behalf of the user who has not been authenticated, in order to authenticate; therefore it is duplicative to include these actions as a separate assignment and test. |
| FIA_UID.1 - Timing of identification | FIA_AFL.1 implicitly requires that the OS perform all necessary actions, including those on behalf of the user who has not been identified, in order to authenticate; therefore it is duplicative to include these actions as a separate assignment and test. |
| FMT_SMR.1 - Security roles | FMT_MOF_EXT.1 specifies role-based management functions that implicitly defines user and privileged accounts; therefore, it is duplicative to include separate role requirements. |
| FPT_STM.1 - Reliable time stamps | FAU_GEN.1.2 explicitly requires that the OS associate timestamps with audit records; therefore it is duplicative to include a separate timestamp requirement. |
| FTA_SSL.1 - TSF-initiated session locking | FMT_MOF_EXT.1 defines requirements for managing session locking; therefore, it is duplicative to include a separate session locking requirement. |
| FTA_SSL.2 - User-initiated locking | FMT_MOF_EXT.1 defines requirements for user-initiated session locking; therefore, it is duplicative to include a separate session locking requirement. |
| FAU_STG.1 - Protected audit trail storage | FPT_ACF_EXT.1 defines a requirement to protect audit logs; therefore, it is duplicative to include a separate protection of audit trail requirements. |
| FAU_GEN.2 - User identity association | FAU_GEN.1.2 explicitly requires that the OS record any user account associated with each event; therefore, it is duplicative to include a separate requirement to associate a user account with each event. |
| FAU_SAR.1 - Audit review | FPT_ACF_EXT.1.2 requires that audit logs (and other objects) are protected from reading by unprivileged users; therefore, it is duplicative to include a separate requirement to protect only the audit information. |

## 6.4 セキュリティ保証要件

このSTのTOEセキュリティ保証要件は、Common Criteria Version 3.1, Revision 5に基づいた[PPOS]より転記した。転記したTOEセキュリティ保証要件は、[PPOS]で選択されたセキュリティ保証要件を選択している。[PKGTLS]と[PKGSSH]は、TOEセキュリティ保証要件を定義しない。以下のTableにTOEセキュリティ保証要件の概要を示す。

Table 28: TOEセキュリティ保証要件

| 保証クラス | 保証コンポーネント |
|---|---|
| Class ASE: Security Target | Conformance claims (ASE_CCL.1) |
| | Extended components definition (ASE_ECD.1) |
| | ST introduction (ASE_INT.1) |
| | Security objectives (ASE_OBJ.2) |
| | Derived security requirements (ASE_REQ.2) |
| | Security Problem Definition (ASE_SPD.1) |
| | TOE summary specification (ASE_TSS.1) |
| Class ADV: Development | Basic Functional Specification (ADV_FSP.1) |
| Class AGD: Guidance Documentation | Operational User Guidance (AGD_OPE.1) |
| | Preparative Procedures (AGD_PRE.1) |
| Class ALC: Life-cycle Support | Labeling of the TOE (ALC_CMC.1) |
| | TOE CM Coverage (ALC_CMS.1) |
| | Timely Security Updates (ALC_TSU_EXT.1) |
| Class ATE: Tests | Independent Testing - Conformance (ATE_IND.1) |
| Class AVA: Vulnerability Assessment | Vulnerability Survey (AVA_VAN.1) |

## 6.5 セキュリティ要件根拠

TOEのセキュリティ保証要件(SAR)は、[PPOS]にて選択されたセキュリティ保証要件をその通りに転記した。

以下のTable でTOEのセキュリティ機能要件(SFR)および根拠の対応を示す。[PPOS]より転記した。

Table 29: セキュリティ機能要件の根拠

| Objective | Addressed By | Rationale |
|---|---|---|
| O.ACCOUNTABILITY | FAU_GEN.1 | Supports the objective by requiring that critical event information be gathered by the TOE. |
| | FTP_ITC_EXT.1 | Supports the objective by ensuring that audit information can be securely transmitted to remote systems for analysis. |
| O.INTEGRITY | FPT_SBOP_EXT.1<br>FPT_ASLR_EXT.1 | Supports the objective by requiring that OS applications be hardened against buffer overflow attacks |
| | FPT_TUD_EXT.1 | Supports the objective by requiring that the OS be able to check for critical updates. |
| | FPT_TUD_EXT.2 | Supports the objective by requiring that the OS verify updates before applying them. |
| | FCS_COP.1/HASH | Supports the objective by requiring the TSF to implement hash algorithms that are used in support of protected communications. |
| | FCS_COP.1/SIGN | Supports the objective by requiring the TSF to implement digital signature algorithms that are used in support of protected communications. |
| | FCS_COP.1/KEYHMAC | Supports the objective by requiring the TSF to implement HMAC algorithms that are used in support of protected communications. |
| | FPT_ACF_EXT.1 | Supports the objective by requiring the TSF restrict unprivileged users from changing critical components. |

| | | |
|---|---|---|
| | FPT_SRP_EXT.1 | Supports the objective by requiring the TSF to implement a configurable allowlist mechanism. |
| | FIA_X509_EXT.1 | Supports the objective by requiring the TSF to validate certificates using industry standards. |
| | FPT_TST_EXT.1 | Supports the objective by requiring the TSF to verify executable code critical to its operation. |
| | FTP_ITC_EXT.1 | Supports the objective by requiring the OS to provide a trusted channel for critical communication. |
| | FIA_AFL.1 | Supports the objective by requiring the TSF to respond accordingly when the number of failed authentication attempts reaches a specified threshold. |
| | FIA_UAU.5 | Supports the objective by requiring the OS to provide standard authentication mechanisms. |
| O.MANAGEMENT | FMT_MOF_EXT.1 | Supports this objective by requiring the TOE to restrict the ability to perform certain management functions to a privileged user. |
| | FMT_SMF_EXT.1 | Supports this objective by requiring the TOE to implement specific management functions. |
| | FTA_TAB.1 | Supports this objective by requiring the TOE to implement a trusted path between itself and users. |
| | FTP_TRP.1 | Supports this objective by requiring a trusted path between users and the OS. |
| O.PROTECTED_STORAGE | FCS_STO_EXT.1 | Supports this objective by requiring the OS to provide encrypted storage. |
| | FCS_RBG_EXT.1/ KCAPI FCS_RBG_EXT.1/ OSSL | Supports this objective by requiring the OS to generate random bits according to industry standards. |
| | FCS_COP.1/ENCRYPT | Supports this objective by requiring the OS to perform encryption according to |

| | | |
|---|---|---|
| | | industry standards. |
| | FDP_ACF_EXT.1 | Supports this objective by requiring the OS to implement access controls. |
| O.PROTECTED_COMMS | FCS_RBG_EXT.1/ KCAPI | Supports this objective by requiring the OS to generate random bits according to industry standards. |
| | FCS_RBG_EXT.1/ OSSL | Supports this objective by requiring the OS to generate random bits according to industry standards. |
| | FCS_CKM.1 | Supports this objective by requiring the TSF to generate asymmetric cryptographic keys to industry standards. |
| | FCS_CKM.2 | Supports this objective by requiring the TSF to perform key establishment according to industry standards. |
| | FCS_CKM_EXT.4 | Supports this objective by requiring the TSF to destroy key material according to industry standards. |
| | FCS_COP.1/ENCRYPT | Supports this objective by requiring the TSF to encrypt data according to industry standards |
| | FCS_COP.1/HASH | Supports this objective by requiring the TSF to hash data according to industry standards. |
| | FCS_COP.1/SIGN | Supports this objective by requiring the TSF to cryptographically sign data according to industry standards. |
| | FCS_COP.1/KEYHMAC | Supports this objective by requiring the TSF to perform keyed hashes according to industry standards. |
| | FIA_X509_EXT.1 | Supports the objective by requiring the TSF to validate certificates using industry standards. |
| | FIA_X509_EXT.2 | Supports this objective by requiring the TSF to validate TLS and related encrypted connections with x509 certificates. |
| | FTP_ITC_EXT.1 | Supports the objective by requiring the OS to provide a trusted channel for |

| | | |
|---|---|---|
| | | critical communication. |
| | FCS_TLS_EXT.1<br>(TLS Package) | Supports the objective by defining the TOE's implementation of TLS and DTLS if this protocol is used for protected communications. |
| | FCS_TLSC_EXT.1<br>(TLS Package) | FCS_TLSC_EXT.1 supports the objective by defining the TOE's implementation of TLS as a client for protected communications. |
| | FCS_TLSC_EXT.3<br>(TLS Package)<br>(Objective) | FCS_TLSC_EXT.3 supports the objective by requiring the TSF to support the TLS signature algorithms extension as part of establishing TLS protected communications. |
| | FCS_TLSC_EXT.5<br>(TLS Package) | FCS_TLSC_EXT.5 supports the objective by defining the TOE's implementation of supported groups extension for TLS as a client for protected communications. |
| | FCS_SSH_EXT.1<br>(SSH Package) | FCS_SSH_EXT.1 supports the objective by defining the TOE's implementation of SSH if this protocol is used for protected communications. |
| | FCS_SSHC_EXT.1<br>(SSH Package) | FCS_SSHC_EXT.1 supports the objective by defining the TOE's implementation of SSH as a client if this protocol is used for protected communications. |
| | FCS_SSHS_EXT.1<br>(SSH Package) | FCS_SSHS_EXT.1 supports the objective by defining the TOE's implementation of SSH as a server if this protocol is used for protected communications. |

NOTE: Table 29 has been modified by TD0713 from its original presentation in [PPOS]. The table has also been modified to reflect the claimed SFRs.

# 7 TOE要約仕様

本章では、TOEがセクション6.2に記載されている各SFRをどのように満たすかを詳述する。

## 7.1 セキュリティ監査

### 7.1.1 FAU_GEN.1

TOEは、以下のイベントを含む監査記録を生成する。:

a) 監査機能の開始/終了イベント
b) 認証の成功/失敗イベント
c) セキュリティ、監査（/etc/audit/）、設定変更（sudo/su、pam、sshd、暗号化ポリシーの変更、passwdやshadowを含む信頼されたデータベースの変更）に関連する成功/失敗したイベントを含む特権/特別権限の使用
d) ‘sudo'コマンドや'su'コマンド、次に記載するイベントを含む特権/ロールの昇格への成功/失敗イベント
    i) ファイル及びオブジェクト事象（成功及び不成功の、作成、アクセス、削除、変更、アクセス権限変更の試行）
    ii) ユーザーおよびグループの管理イベント（追加、削除、変更、無効化、有効化、および資格情報の変更の成功と失敗）
    iii) 監査及びログデータへのアクセス事象（成功／失敗）
    iv) 引数を伴うアプリケーション起動の試み（ソフトウェア制限ポリシーなどによる成功／失敗）
    v) カーネルモジュールのロード及びアンロード事象（成功／失敗）

e) RPMパッケージのインストールと署名検証に関するイベント（成功／失敗）

f) 次に挙げるSSH接続に関する事象・イベント
    i) SSH接続の確立（当該接続の非TOEエンドポイントのIPアドレス）
    ii) SSH接続の確立の失敗（当該接続試行の失敗理由および非TOEエンドポイントのIPアドレス）
    iii) SSH接続セッションの終了（当該接続の非TOEエンドポイントのIPアドレス）

FCS_SSHC_EXT.1およびFCS_SSHS_EXT.1に関しては指定された事象・イベントはない。

TOEが監査機能を開始するためには、TOEを搭載したハードウェアの電源を起動する。
また、TOEが監査機能を終了するためには、shutdown/poweroff/reboot/serviceコマンドにより、電源OFFのための操作または、再起動操作を行う。

TOEは、Lightweight Audit Framework（LAF）を使用して監査イベントをローカルに生成し、保存する。LAFは、ユーザー空間を起点とするイベントをシリアライズして記録したり、管理者が定義したルールで指定されたシステムコールをインターセプトしたりするように設計されている。生成されたイベントは、監査デーモンがデキューしてログに書き込むまで、カーネルのバックログキューに置かれる。監査ログ・エントリを選択的に取得するための検索およびレポート・ユーティリティを

備えている。このフレームワークでは、記録するイベントを選択することができる。

監査イベントは、"keyword=value"形式のフィールドを含む1行以上のテキスト（
レコード）から構成される。以下の情報は、すべての監査レコードに含まれる：

a) タイプ：SYSCALL、PATH、USER_LOGIN、LOGINなどといったイベントの種類

b) タイムスタンプ：監査記録が生成された日付と時刻（ミリ秒単位まで記録）

c) シリアルナンバー：同一時刻・日付(同じミリ秒内)のイベントを区切るために、タイムスタンプに付加される一意の数値識別子。

d) Auid（Login ID）：ユーザーがその後に実際のユーザーIDまたは有効なユーザーIDを変更したかにかかわらず、ユーザーがシステムに最初に認証したユーザーID。

e) セッションID：イベントがどのログインセッションに属するかを識別するための一意の識別子。

f) Uid: 監査イベントが発生した時点でのプロセスの実ユーザーID

g) Pid：イベントを発生させたサブジェクトのプロセスID

h) レスポンス成功/失敗の結果

i) イベントの種類に応じた以下のオプション情報
　i )イベントの原因となったプロセスが行ったシステムコール

　ii) サブジェクトのグループID

　iii) サブジェクトが操作の実行に使用したホスト名または端末

　iv) 意図した操作に関する情報
※イベントの種類に応じて、上記のオプション情報が含まれる場合がある。（含まれない場合もある）。また、オプション情報は上記の内容に限定されない。

## 7.2 暗号サポート

### 7.2.1 FCS_CKM.1

TOEは、以下の非対称鍵生成アルゴリズムを提供する。

- FIPS PUB 186-5 “Digital Signature Standard (DSS) Appendix A.1”に準拠したRSAスキーム
- FIPS PUB 186-5 “Digital Signature Standard (DSS) Appendix A.2”に準拠したECCスキーム
- NIST SP  800-56A rev 3, "Recommendation for Pair-Wise Key Establishment Schemes"に準拠したFFCスキーム

TOEは、以下の非対称鍵の生成を行う。

Table 30: 鍵生成方法

| 鍵種 | 鍵長 | 用途 |
|---|---|---|
| RSA | ・3072<br>・4096 | SSHでのサーバー認証/クライアント認証 |
| ECC | ・384(P-384楕円曲線)<br>・521(P-521楕円曲線) | TLS鍵の確立<br>SSH鍵の確立<br>SSHでのサーバー認証/クライアント認証 |
| FFC<br>(safe primes) | ・4096 MODP<br>(DH Group16)<br>・8192 MODP<br>(DH Group18) | TLS鍵の確立<br>SSH鍵の確立 |

### 7.2.2 FCS_CKM.2

TOEは、以下の暗号鍵確立スキームを提供する。

- NIST SP 800-56A rev 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"に準拠した、P-384およびP-521を用いた楕円曲線ベースの鍵確立スキーム

- NIST SP 800-56A rev 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"に準拠した、鍵長4096、および8192ビットの安全素数を用いた有限体ベースの鍵確立スキーム

TOEは、TLS通信およびSSH通信における鍵確立スキームとして、楕円曲線ベースおよび有限体ベースの方式をサポートする。

### 7.2.3 FCS_CKM_EXT.4

以下の鍵および鍵マテリアルは、TLSハンドシェイク中に生成され、揮発性メモリ上に保存される。TOEは、ゼロで構成されたデータを揮発性メモリ内の鍵および鍵マテリアルの保存エリアに上書きすることにより、当該鍵を破棄する。また、揮発性メモリの電源が遮断された場合、当該メモリ上の鍵および鍵マテリアルは、揮発性メモリの特性により保持されず復元不能となる。

- TLS Diffie-Hellman Private Key
- TLS Pre-Master Secret
- TLS Session Keys

以下の鍵および鍵マテリアルは、不揮発性メモリに保存される。サーバー秘密鍵は、sshdサービスの起動ユニットによって自動生成されるか、鍵の更新時に管理者がssh-keygenコマンドを使用して手動で生成する。生成されたサーバー秘密鍵は、サーバー上の/etc/sshディレクトリに保存される。ユーザー秘密鍵は、ユーザーが公開鍵認証を利用する際に、ssh-keygenコマンドで生成され、各ユーザーの~/.sshディレクトリに保存される。これらのSSH秘密鍵は、SSH通信のハンドシェイク中に不揮発性メモリからロードされ、新たな鍵に更新された場合には破棄される。TOEは、shredコマンドを使用してSSH秘密鍵の論理記憶ロケーションを消去する。消去は、/dev/urandomを用いて生成された擬似ランダム・パターンにより、デフォルトで3回の上書きを行うことで実施される。

- SSH Server Private Key
- SSH User Private Key

以下の鍵および鍵マテリアルは、SSH通信のSSHハンドシェイク中に生成され、揮発性メモリ上に保存される。TOEは、ゼロで構成されたデータを揮発性メモリ内の鍵および鍵マテリアルの保存エリアに上書きすることにより、当該鍵を破棄する。また、揮発性メモリの電源が遮断された場合、当該メモリ上の鍵および鍵マテリアルは、揮発性メモリの特性により保持されず復元不能となる。

- SSH ephemeral Diffie-Hellman Private Key
- SSH Shared Secret
- SSH Session Keys

下記Tableに、生成される鍵についての、消去までの取扱い方法を記した。

Table 31: 暗号鍵の詳細

| 鍵種 | 使用箇所 | 生成方法 | 保存場所 | 消去方法 |
|---|---|---|---|---|
| TLS Diffie-Hellman Private Key | 鍵認証と鍵の確立 | FCS_CKM.1 と FCS_CKM.2 によって規程されるDRBGによる生成 | 揮発性メモリ | 0による上書き消去、またはメモリの電源遮断 |
| TLS Pre-Master Secret | 鍵認証と鍵の確立 | Diffie-Hellmanを使用しての確立 | 揮発性メモリ | 0による上書き消去、またはメモリの電源遮断 |

| | | | | |
|---|---|---|---|---|
| TLS Session Keys | TLSセッション暗号化 | TLS Pre-Master Secretからの派生 | 揮発性メモリ | 0による上書き消去、またはメモリの電源遮断 |
| SSH Server Private Key | SSHセッション認証 | FCS_CKM.1 によって規程されるDRBGによる生成、又はファイルシステムからのロード | 不揮発性メモリ(ファイルシステムAPI) | pseudoランダムパターンによる上書き消去 |
| SSH User Private Key | SSHセッション認証 | FCS_CKM.1 によって規程されるDRBGによる生成、又はファイルシステムからのロード | 不揮発性メモリ(ファイルシステムAPI) | pseudoランダムパターンによる上書き消去 |
| SSH ephemeral Diffie-Hellman Private Key | 鍵認証と鍵の確立 | FCS_CKM.1 と FCS_CKM.2 によって規程されるDRBGによる生成 | 揮発性メモリ | 0による上書き消去、またはメモリの電源遮断 |
| SSH Shared Secret | SSHセッション暗号化 | Diffie-Hellmanを使用しての確立 | 揮発性メモリ | 0による上書き消去、またはメモリの電源遮断 |
| SSH Session Keys | SSHセッション暗号化 | SSH Shared Secretからの派生 | 揮発性メモリ | 0による上書き消去、またはメモリの電源遮断 |

不揮発性メモリにRAIDが使用される場合は、実行される鍵の破棄に遅延が発生する可能性がある。

### 7.2.4 FCS_COP.1/ENCRYPT

TOEは、256ビットの鍵を使用するAESの以下の暗号利用モードを提供する。

- NIST PUB SP 800-38Eに準拠したAES-XTS
- NIST PUB SP 800-38Aに準拠したAES-CBC
- NIST PUB SP 800-38Aに準拠したAES-CTR
- NIST PUB SP 800-38Dに準拠したAES-GCM

TOE は、TLSやSSHによる通信データ、ファイル、ブロックデバイス上の情報の暗号化および復号にAES を使用する。

### 7.2.5 FCS_COP.1/HASH

TOEは、FIPS PUB 180-4に準拠した以下のハッシュアルゴリズムを提供する。

- SHA-256
- SHA-384
- SHA-512

TOEにおけるハッシュアルゴリズムは、以下の用途に利用される。

- ファイルおよびTLS/SSH通信データの完全性検証
- ファイルおよびTLS/SSH通信データの改ざん検出
- TLS/SSHにおける鍵確立および鍵導出
- OSインストールおよびアップデート時におけるrpmパッケージの完全性検証
- ログインパスワードの秘匿化
- X.509証明書を識別するデジタルフィンガープリント

TOEは、ハッシュアルゴリズムを用いてファイルおよびデータの完全性を検証する。ハッシュアルゴリズムは、TLS/SSH通信時において、鍵確立時のデジタル署名検証および通信データの完全性検証に利用される。OSのインストールおよびアップデートでは、rpmパッケージのファイルの完全性検証に利用される。また、ハッシュアルゴリズムの持つ不可逆性は、TLS/SSH通信時の鍵導出関数による鍵生成、およびログインパスワードをハッシュ化して保存することによるアカウントの安全性確保に活用される。さらに、X.509証明書のハッシュ値は、その証明書のデジタルフィンガープリントとしても利用される。

### 7.2.6 FCS_COP.1/SIGN

TOEは、以下の電子署名アルゴリズムを提供し、電子署名の作成と検証を行う。

- FIPS PUB 186-5 Digital Signature Standard (DSS) Section 4 で指定されたRSA署名の検証
    - 鍵長は、2048 ビット(セキュアブートのみ)、3072 ビット、4096 ビットをサポート
    - ハッシュアルゴリズムは、SHA-256、SHA-384、SHA-512をサポート
- SP 800-186 Section 3で指定されたECDSA署名の生成と検証
    - 楕円曲線は、P-384およびP-521をサポート
    - ハッシュアルゴリズムは、SHA-384、SHA-512をサポート

TOEは、電子署名アルゴリズムを用いて証明書やソフトウェアに署名を施し、改ざんやなりすましの検出、さらに否認の防止を実現する。TLS/SSH通信時は、通信相手の証明書の発行元が正当であり、改ざんされていないことを確認することで認証を行う。セキュアブートでは、システム起動時のソフトウェアの電子署名を検証することで不正なコードが実行されることを防ぐ。また、ソフトウェア更新では、更新ファイルの電子署名を検証することで更新ファイルが正規の提供者によるものであり、改ざんされていないことを確認する。

### 7.2.7 FCS_COP.1/KEYHMAC

TOEは、FIPS PUB 198-1 "The Keyed-Hash Message Authentication Code" と FIPS PUB 180-4 "Secure Hash Standard"に準拠した鍵付きハッシュメッセージ認証を提供する。

- HMAC-SHA-256
- HMAC-SHA-384

- HMAC-SHA-512

TOEは、鍵付きハッシュメッセージ認証によって、TLSやSSHの通信データの完全性と正当性を検証する。

### 7.2.8 FCS_RBG_EXT.1/KCAPI

TOEは、カーネルに実装されたNIST SP 800-90A に準拠したHMAC_DRBG（SHA-512）を使用して決定論的ランダムビット生成を行う。このDRBGは、Kernel内に実装されたメモリアクセスの乱雑性をノイズ元とする乱数生成機から出力された乱数をシードとし、それは少なくとも256ビットのエントロピーを有する。そして、暗号学的に安全な疑似乱数を生成する。生成された擬似乱数はデバイスファイル経由でユーザー空間に公開される。アプリケーションは、getrandom() システムコール、/dev/random 又は /dev/urandom デバイス、若しくは libkcapi ライブラリ関数のいずれかにより当該疑似乱数を取得できる。

### 7.2.9 FCS_RBG_EXT.1/OSSL

TOEは、NIST SP 800-90Aに準拠したCTR-DRBG（AES-256）を実装したOpenSSLライブラリを提供する。OpenSSLライブラリのDRBGは、getrandom()システムコールにより少なくとも256ビットのエントロピーをもった乱数を取得してシードとし、安全な疑似乱数を提供する。getrandom()システムコールは、上述のFCS_RBG_EXT.1/KCAPIの実装を利用し、乱数生成機から出力された乱数をシードとし、hmacDRBGにて再度乱数を生成し呼び出し元へ出力する。
アプリケーションは、OpenSSLライブラリ関数をコールすることでDRBGが生成する暗号学的に安全な疑似乱数を利用できる。特に、TLSプロトコルにおけるセッションキーとエフェメラルキーの生成、ノンスといった十分なエントロピーを求められるインスタンスにも使用する。

### 7.2.10 FCS_STO_EXT.1

TOEは、AES-XTS（256ビット）によるディスク暗号化機能を提供する。TOEが扱う機密データは、ディスク暗号化機能により保護されたディスクに保存される。加えて、TOEは厳格なファイルアクセス制御により、当該データへのアクセスを管理者および当該データを利用するアプリケーションのみに限定する。

以下のTableに、TOEに保存される機密データの利用目的を示す。機密データは、ディスク暗号化機能によりブロックデバイスレベルで透過的に暗号化して保存され、ファイルアクセス制御で保護される。

Table 32: 機密データの利用目的および保存方式

| 機密データ | 利用目的 |
|---|---|
| ユーザー/グループパスワード (パスワードハッシュ) | OSのユーザー認証 |
| SSH秘密鍵 | サーバー認証 |

| | |
|---|---|
| | クライアント公開鍵認証 |
| TLS証明書に対応する秘密鍵 | サーバー認証<br>クライアント証明書認証 |
| 設定ファイル | SSHデーモン、監査及び暗号化設定のようなシステム全体に関わる設定 |
| ログファイル | システムログおよび監査ログの保存 |

### 7.2.11 FCS_SSH_EXT.1, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1

TOEは、SSHサーバーおよびクライアント機能を提供する。リモートユーザーは、SSHプロトコルを使用して安全な通信を確立しTOEにアクセスする。

Table 33: サポートされるSSHプロトコル

| | |
|---|---|
| 認証方法 | 公開鍵 (RFC 4252) |
| | パスワード (RFC 4252) |
| 対称アルゴリズム | aes256-ctr (RFC 4344) |
| | aes256-gcm@openssh.com (RFC 5647) |
| 公開鍵アルゴリズム | rsa-sha2-256 (RFC 8332) |
| | rsa-sha2-512 (RFC 8332) |
| | ecdsa-sha2-nistp384 (RFC 5656) |
| | ecdsa-sha2-nistp521 (RFC 5656) |
| MAC | hmac-sha2-256 (RFC 6668) |
| | hmac-sha2-512 (RFC 6668) |
| | Implicit (aes256-gcm@openssh.com) |
| 鍵交換の方法 | diffie-hellman-group16-sha512 (RFC 8268) |
| | diffie-hellman-group18-sha512 (RFC 8268) |
| | ecdh-sha2-nistp384 (RFC 5656) |
| | ecdh-sha2-nistp521 (RFC 5656) |

TOEは、RFC 4253およびRFC 5656に準拠したSSH鍵導出関数（KDF）を使用し、鍵交換で得られた共有秘密鍵からセッション鍵、暗号化鍵、HMAC鍵を導出する。TOEは、パケットサイズが262,144バイトを超えるSSHパケットを破棄する。また、TOEはSSHセッション鍵の再鍵交換（

Rekey）タイミングを指定できる。SSHサーバーおよびクライアントの設定ファイルにおいて RekeyLimitオプションを適切に設定することで、TOEはセッション鍵の使用時間が1時間を超えた場合、またはデータ転送量が1GBを超えた場合にRekey処理を開始する。

## 7.2.12 FCS_TLS_EXT.1, FCS_TLSC_EXT.1, FCS_TLSC_EXT.3, FCS_TLSC_EXT.5

TOEは、TLS 1.2プロトコルのクライアント機能を提供する。TLS1.2クライアントは、以下のTableに示す暗号スイートをサポートし、サーバー証明書の有効性を検証することでユーザーと管理者に安全な通信を提供する。

Table 34: サポートされる暗号スイート

| 暗号スイート名 | RFC |
|---|---|
| TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | RFC 5288 |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | RFC 5289 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | RFC 5289 |

TOEは、Client Helloメッセージに含まれるsupported_groups拡張を使用して、以下の楕円曲線暗号の曲線リストを提供する。

- secp384r1
- secp521r1

TOEは、TLSのClient Helloメッセージに含まれるsignature_algorithms拡張を使用して、TOEが対応する署名アルゴリズムとハッシュ関数の組み合わせをサーバーに通知する。TOEが対応可能なアルゴリズムは、FIPSモード準拠の暗号化ポリシーを定義するポリシー設定（/etc/crypto-policies/back-ends/opensslcnf.config）に基づいて決定される。

TOEのデフォルト設定で対応可能な署名アルゴリズムとハッシュ関数の組み合わせを以下に示す。RSAの鍵長は3072及び4096をサポートする。

- ECDSA-SECP384R1-SHA384
- ECDSA-SECP521R1-SHA512
- RSA_PSS_PSS_SHA256
- RSA_PSS_PSS_SHA384
- RSA_PSS_PSS_SHA512
- RSA_PSS_RSAE_SHA256
- RSA_PSS_RSAE_SHA384
- RSA_PSS_RSAE_SHA512
- RSA_PKCS1_SHA256
- RSA_PKCS1_SHA384
- RSA_PKCS1_SHA512

FIPSモード準拠の暗号化ポリシーは、以下のコマンドによりセットアップされる。
# fips-mode-setup --enable

TOEは、サーバーが提示する証明書に含まれる識別子について、以下のとおり検証を行う。証明書が無効な場合、TOEは高信頼チャネルを確立しない。

- TLSサーバーのDNS名またはIPアドレスを解析して参照識別子を構築する
- SANが存在する場合、参照識別子は、SANと照合される
- SANが存在しない場合、参照識別子はDNSのCNと照合される

- 参照識別子がIPアドレスの場合、SANに対してのみ識別子を照合する
- サーバー証明書のDNS名のワイルドカードはサポートされる
- URI参照識別子、SRV参照識別子、および証明書のピンニングはサポートされない

# 7.3 ユーザーデータ保護（FDP）

## 7.3.1 FDP_ACF_EXT.1

TOEは、DACの1つの形式を提供するxfsファイルシステムを使用する。
ファイルシステムにおけるアクセス制御については、Unix権限によるファイルとディレクトリに対する基本的なアクセス制御と、POSIXタイプのアクセス制御リスト(POSIX ACL)によるアクセス制御をサポートしている。

### 7.3.1.1 Unix権限によるファイルとディレクトリに対する基本的なアクセス制御

#### 7.3.1.1.1 所有者、所有グループ、パーミッション

TOEではファイルおよびディレクトリは所有者、所有グループ、パーミッションを保持し、ls　–lのコマンドによりこれらの情報を確認することができる。

```
$ ls –l /etc/passwd
-rw-r--r--. 1 root root 2471 Mar 25 12:59 /etc/passwd
```

上記の出力においては、1番目のフィールド(-rw-r--r--)がパーミッション、3番目(root)、4番目(root)のフィールドがそれぞれ所有者、所有グループを示す。

パーミッションは10個の文字によって表現される。一番左の1文字がファイルタイプであり、残りの9文字が3文字ずつのカテゴリ(所有者のパーミッション、所有グループのパーミッション、その他のパーミッション)を表す。各文字の意味を以下のTableに示す。

Table 35: パーミッション一覧

| | | |
|---|---|---|
| ファイルタイプ | - | 通常のファイル |
| | d | ディレクトリ |
| | l | シンボリックリンク |
| | b | ブロックデバイスファイル |
| | c | キャラクタデバイスファイル |
| | s | UNIXドメインソケット |
| | p | 名前付きパイプ |
| ファイルの場合の<br>・ 所有者のパーミッション<br>・ 所有グループのパーミッション<br>・ その他のパーミッション | r | ファイルの内容を参照可能 |
| | w | ファイルに変更を加えることが可能 |
| | x | ファイルを実行することが可能 |
| | - | 権限なし |

| | | |
|---|---|---|
| ディレクトリの場合の<br>・ 所有者のパーミッション<br>・ 所有グループのパーミッション<br>・ その他のパーミッション | R | ディレクトリ内のファイル参照が可能 |
| | W | ディレクトリ内にファイル作成が可能 |
| | X | ディレクトリ内への移動が可能 |
| | - | 権限なし |

上記の/etc/passwdファイルの場合、次のようなセキュリティ属性となる。

- rootユーザーが読み込み、書き込み可能( -**rw-**r--r-- の太文字部分)
- rootグループに所属するユーザーが読み込み可能( -rw-**r--**r-- の太文字部分)
- rootユーザーではなく、rootグループに所属しないユーザーが読み込み可能( -rw-r--**r--** の太文字部分)

また、このパーミッションはそれぞれ3桁の数値で表されることもあり、r=4、w=2、x=1、-=0として合計した値で表す。上記の/etc/passwdファイルの場合、所有者のパーミッション= rw- = 4+2+0 = 6、所有グループのパーミッション = r-- = 4+0+0 = 4、その他のパーミッション = r-- = 4+0+0 =4として、644と表現する。

#### 7.3.1.1.2 setuid / setgid

ファイルの特殊なパーミッションとして、setuid/setgidが存在し、ls -lコマンドで確認することができる。

```
$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 32656 Apr 14  2022 /usr/bin/passwd
```

所有者のパーミッションの実行権限に付与されている"s"がsetuidを表し、setuidが付加されたプログラムを実行した場合、生成されるプロセスが保持するユーザーIDは、そのファイルの所有者と同一となる。上記のpasswdコマンドの場合、どのユーザーが実行する場合でも、生成されるプロセスの権限はrootとなる。

setuidと同様に、setgidの場合は生成されるプロセスのプロセスが保持するグループIDが、そのファイルの所有グループと同一になる。

setuid/setgidパーミッションはプログラムに大きな権限を与えることも可能であることから、使用方法を間違えるとセキュリティホールになることがあるため、使用に際しては注意が必要である。特に、Setuid-rootと呼ばれる管理者権限で実行できるsetuidパーミッションは必要でない限り使用すべきではない。

#### 7.3.1.1.3 スティッキービット

ディレクトリの特殊なパーミッションとして、スティッキービットが存在し、ls -lコマンドで確認することができる。

```
$ ls -l /
drwxrwxrwt.  12 root root 4096 Jul  9 10:32 tmp
```

その他のパーミッションの実行権限に付与されている"t"がスティッキービットを表し、スティッキービットが付与されたディレクトリ下に作成されたファイルは、書込み権限のあるディレクトリ下のファイルであっても、所有者でない限り削除を行うことができない。

#### 7.3.1.1.4 ファイルおよびディレクトリ新規作成時のデフォルトのパーミッション

ファイルおよびディレクトリを作成した際のデフォルトのパーミッションは、それぞれ666、777となり、その後、umaskの値を引いた値が最終的なデフォルトのパーミッション値となる。

デフォルトでは、/etc/bashrcにてumaskの値は 022 に設定されており、このumaskの値をそれぞれ引くことで、ファイルは 644 に、ディレクトリは 755 に設定される。また、このumaskの値を変更することで、全てのユーザー・管理者が作成するファイル・ディレクトリのデフォルト値を制御することが可能となる。

ただし、ファイルに対して実行権限を付与するumaskの値を設定した場合、ファイル生成時には、当該パーミッションには +1 された値が設定され、実行権限が付与されないように制御される。

#### 7.3.1.1.5 インタフェース

- ファイル、又はディレクトリを操作するコマンド。

### 7.3.1.2 POSIX タイプのアクセス制御リスト(POSIX ACL) によるアクセス制御

POSIXタイプのアクセス制御リスト(以下、POSIX ACL )は、ファイルやディレクトリのアクセス制御をより細かく管理するための仕組みである。POSIX ACLを利用すると、特定のユーザーに対し、ファイルの削除のみを許可して書き込みを禁止するといった制御が可能となる。

POSIX ACL では、ACL( Access Control List )に定義された、複数のACLエントリーに基づいてファイル・ディレクトリのアクセス制御を行う。
ACLエントリーは、主に次の項目で構成される。

- タグタイプ
    - どの対象へ適用されるかを定義する。主なタグタイプには次のものがある。
    - ユーザー：特定のユーザーに対するエントリー
    - グループ：特定のグループに対するエントリー
    - マスク：グループエントリーに適用される権限を制限するためのエントリー
    - その他：特定のユーザーやグループに該当しない全てのユーザーに対するエントリー
- 識別子
    - タグタイプに応じて、対象のユーザー名またはグループ名が指定される。たとえば、ユーザーエントリーの場合はユーザー名、グループエントリーの場合はグループ名が入る。
- 権限
    - 対象に対して付与される具体的な権限を示す。一般的な権限には以下がある。
    - 読み取り(read): ファイルの内容を読み取る権限。
    - 書き込み(write): ファイルの内容を変更する権限。
    - 実行(execute): ファイルを実行する権限（スクリプトやプログラムの場合）。
- マスク
    - マスクは、グループエントリーに適用される権限を制限するための特別なエントリーである。マスクは、グループに対する権限を制御するために使用され、通常は「m:」で始まる。

また、デフォルトACLというものがある。デフォルトACLは、特定のディレクトリに設定され、そのディレクトリ内に新しく作成されるファイルやサブディレクトリに対して自動的に適用される。これにより、ユーザーは新しいファイルやディレクトリの権限を手動で設定する必要がなくなる。通常のACLエントリーと同様に、ユーザー、グループ、マスク、その他のエントリーを含むことができる。これにより、特定のユーザーやグループに対して適切な権限を設定できる。デフォルトACLを使用することで、特定のディレクトリ内のファイルやサブディレクトリに対するアクセス権限を一貫して管理できる。

##### 7.3.1.2.1 インタフェース

- ファイル、又はディレクトリを操作するコマンド。

## 7.4 識別と認証

### 7.4.1 FIA_AFL.1

TOEは、ローカルコンソールおよびSSH接続によるリモートコンソール上でのパスワードベースの認証に関連して、/etc/security/faillock.confファイルにて、deny値を指定することでユーザー名とパスワードに基づく認証（パスワード認証）に失敗した回数が、fail_interval値(秒)の間に 1～65,535回の範囲で管理者が設定可能な整数に達したことを検出できる。指定された認証失敗回数に達すると、TOEはそのアカウントをロックする。デフォルトのdeny値は 3 に設定されているため、デフォルトでは 3回失敗するとアカウントはロックされる。

### 7.4.2 FIA_UAU.5

TOEは、ローカルコンソールおよびSSH接続によるリモートコンソール上でのユーザー名とパスワードに基づく認証をサポートしている。また、TOE上では、TOEに含まれているopenssh serverがSSHサーバーとして動作し、公開鍵ベースの認証もサポートしている。

TOEは、ローカルの認証情報セットを使用して、ユーザー名とパスワードの認証を実行する。パスワードベースのログインでは、ユーザー名とパスワードを収集するPAMモジュール（Pluggable Authentication Module）であるpam_unixモジュールが呼び出される。pam_unixモジュールは、ユーザーがパスワード・データベースにあるかどうかを確認し、提供されたパスワードのハッシュ値と以前に保存されたパスワードのハッシュ値を比較する。比較した結果、一致していれば、ユーザーの認証が成功したと判断し、ユーザーはログインすることができる。一致しなければ、パスワードの再入力を促す。

TOE上のSSHサーバーは公開鍵ベースの認証を行なうことができる。ユーザーがログオンしようとすると、パスワードを入力する代わりに、署名入りのSSH_MSG_USERAUTH_REQUESTメッセージを送信する。TOE上のSSHサーバーが、ユーザーの~/.ssh/authorized_keysファイルにある公開鍵を使ってその署名を検証できた場合、TOE上のSSHサーバーはそのユーザーの認証が成功したとみなす。

TOEにて、公開鍵認証を有効にしている場合、~/.ssh/authorized_keysにTOE接続元（クライアント）の公開鍵が登録されていない場合は、パスワード認証を行う。

TOEにて、公開鍵認証を有効にしていてかつ、パスワード認証を禁止としている場合において、クライアントの公開鍵が登録されていない場合は、ログインできない。

### 7.4.3 FIA_X509_EXT.1

TLS接続においてX.509v3証明書が提示された場合、TOEは証明書パスの検証を行い、以下のルールに基づいて証明書検証プロセスを確認する。

- RFC 5280に基づく証明書および証明書パスの検証

    - 公開鍵アルゴリズムとパラメータ
    - 証明書の有効期間
- RFC 6066に基づくOCSP Staplingによる証明書の失効状況
    - 失効状況の確認ができなければ証明書は拒否される
- 証明書パスが信頼できるCA証明書で終了していること
- 証明書にbasicConstraintsエクステンションが存在し、CAフラグがTRUEに設定されているものだけがCA証明書として扱われること
- 証明書パスの制約が満たされていること
- keyUsageフィールドにCertificate Signingが設定されているものがCA証明書として扱われること

TOEは、以下のルールに従ってextendedKeyUsageフィールドを検証する。

- 高信頼アップデート及び実行可能コードの完全性検証に用いられる証明書は、extendedKeyUsageフィールドにCode Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) を持たなればならない
- TLSに提示されるサーバー証明書は、extendedKeyUsageフィールドにServer Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) を持たなければならない
- TLSに提示されるクライアント証明書は、EKUフィールドにClient Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) を持たなければならない
- 電子メールの暗号化及び署名に提示されるS/MIME証明書は、EKUフィールドにEmail Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) を持たなければならない
- OCSP応答に提示されるOCSP証明書は、EKUフィールドにOCSP Signing Purpose(id-kp 9 with OID1.3.6.1.5.5.7.3.9) を持たなければならない
- EST(Enrollment over Secure Transport)に提示されるサーバー証明書は、EKUフィールドにCMCRegistration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) を持たなければならない。(条件付き)

TOE は、X.509証明書パスの検証に失敗した場合、当該失敗の原因を示すメッセージを表示し、TLS接続を直ちに切断する。

### 7.4.4 FIA_X509_EXT.2

TOEは、TLS接続およびHTTPS接続時のリモートエンティティ認証において、公開鍵基盤（PKI）で広く利用されているRFC 5280に準拠したX.509v3証明書を使用する。X.509v3証明書の失効状態は、OCSP Staplingにより検証される。失効が判明した場合、TLSクライアントはハンドシェイクを中止し、HTTPSクライアントは 接続を遮断して警告を表示する。

# 7.5 セキュリティ管理

## 7.5.1 FMT_MOF_EXT.1

TOEは、FMT_SMF_EXT.1.1に記載されているすべての管理機能を、wheelグループのメンバーであるユーザーに制限する。このグループのメンバーは管理者とみなされ、グループのメンバーになることで、当該ユーザーは、sudoコマンドまたはsuコマンドを使用して管理者権限へと昇格することができるため、TOEを管理することができる。

## 7.5.2 FMT_SMF_EXT.1

管理者または権限を与えられたユーザーは、以下に示す管理機能を設定することができる。管理機能の設定ファイルの編集はviコマンドを用いて実行する。

1. Enable/disable [session timeout]
   セッションタイムアウトの制御は、/etc/systemd/logind.confのStopIdleSessionSecで行う。
   - セッションタイムアウトを有効にする場合
     - StopIdleSessionSecにセッションがタイムアウトする時間を設定する。
   - セッションタイムアウトを無効にする場合
     - StopIdleSessionSecにinfinityを設定する。
     - StopIdleSessionSecの行をコメントアウトまたは削除する。

2. Configure [session] inactivity timeout
   /etc/systemd/logind.confのStopIdleSessionSecにセッションがアイドル状態になってからタイムアウト（終了）するまでの時間を設定する。ユーザーが SSHによるログインまたはコンソール接続によるログインを行った後、設定した時間だけアイドル状態が続くと、自動的にセッションがログアウトされる。

3. Import keys/secrets into the secure key storage
   opensslコマンドまたは、gpgコマンドを用いて、秘密鍵や証明書をインポートする。

4. Configure local audit storage capacity
   /etc/audit/auditd.confのmax_log_fileに最大ログファイルサイズ(MB)を設定し、serviceコマンドを用いてauditdを再起動する。

5. Configure minimum password length
   /etc/security/pwquality.confのmin_lenにパスワードの最小長を数字で設定する。

6. Configure minimum number of special characters in password

/etc/security/pwquality.confのocreditに負の数字で最小数を設定する。

7. Configure minimum number of numeric characters in password
   /etc/security/pwquality.confのdcreditに負の数字で最小数を設定する。

8. Configure minimum number of uppercase characters in password
   /etc/security/pwquality.confのucreditに負の数字で最小数を設定する。

9. Configure minimum number of lowercase characters in password
   /etc/security/pwquality.confのlcreditに負の数字で最小数を設定する。

10. Configure lockout policy for unsuccessful authentication attempts through [timeouts between attempts]
    authselectコマンドを用いてアカウントロックアウト機能を有効化する。その後、/etc/security/faillock.confのdeny にロックアウト回数、unlock_timeにロックアウト解除時間を設定する。

11. Configure host-based firewall
    firewall-cmdコマンドにより、ファイアウォールの設定を行う。

12. Configure name/address of audit/logging server to which to send audit/logging records
    TOE上のauditdから監査ログをrsyslogに流すために、/etc/audit/plugins.d/syslog.confを編集する。また、TOE上のrsyslogから監査ログサーバーに監査ログを送信するために、/etc/rsyslog.d/audit.confファイルを新規作成し、適切に設定する。

13. Configure audit rules
    /etc/audit/audit.rulesファイルを編集し、設定を追加・削除・変更する。

14. Configure name/address of network time server
    /etc/chrony.confに、NTPサーバーのドメイン名またはIPアドレスを設定する。

15. Enable/disable automatic software update
    systemctlコマンドにより、ソフトウェアの自動アップデートの有効/無効を行う。

16. Configuration of object ownership and allowed access
    chownコマンドにより、ファイル、又はディレクトリの所有者/所属グループを変更する。chmodコマンドにより、実行/書き込み/読み込み権限を変更する。chgrpコマンドにより、ファイル、又はディレクトリの所属グループを変更する。

    getfaclコマンドにより、ファイル、又はディレクトリのファイルアクセスコントロールリストを取得する。setfaclコマンドにより、ファイル、又はディレクトリのファイルアクセスコントロールリストを設定する。

17. Configuration of the roles that may manage the behavior of the TSF management functions
    管理者権限で操作を実行できるsudoコマンドまたはsuコマンドを利用するため、対象ユーザーをwheelグループに追加する。

# 7.6 TSFの保護

## 7.6.1 FPT_ACF_EXT.1

### 7.6.1.1 FPT_ACF_EXT.1.1

TOEはxfsファイルシステムを利用し、ファイル、又はディレクトリに対してFDP_ACF_EXT.1で規定されたパーミッションを設定する。ファイル、又はディレクトリを操作するコマンドは、このパーミッションに基づくアクセス制御により、ユーザーによる保護対象ファイルやディレクトリの変更を防止する。

TOEは、以下ディレクトリに対して非管理者による変更を禁止するアクセス制御を提供する。

a) カーネルとそのドライバ／モジュール
- `/boot`
- `/lib/modules`

b) セキュリティ監査ログ
- `/var/log/audit`

c) 共有ライブラリ
- `/lib`
- `/usr/lib`
- `/lib64`
- `/usr/lib64`

d) システム実行可能ファイル
- `/sbin`
- `/usr/sbin`
- `/bin`
- `/usr/bin`

e) システム構成ファイル
- `/etc`

### 7.6.1.2 FPT_ACF_EXT.1.2

TOEはxfsファイルシステムを利用し、ファイル、又はディレクトリに対してFDP_ACF_EXT.1で規定されたパーミッションを設定する。ファイル、又はディレクトリを操作するコマンドは、このパーミッションに基づくアクセス制御により、ユーザーによる保護対象ファイルやディレクトリの読み込みを防止する。

TOEは、以下ディレクトリおよびファイルに対して非特権ユーザーの読み込みを禁止するアクセス制御を提供する。

a) セキュリティ監査ログ
- `/var/log/audit`

b) システム全体の認証情報および機密ファイル

- /etc/grub.d
- /etc/gshadow
- /etc/shadow
- /etc/sssd
- /etc/pki/tls/private/localhost.key
- /etc/pki/CA/private
- /etc/ssh/ssh_host_ecdsa_key
- /etc/ssh/ssh_host_rsa_key
- /etc/ssh/sshd_config
- /etc/sysconfig/sshd
- /etc/fapolicyd
- /etc/audit
- /etc/libaudit.conf
- /etc/crypttab

### 7.6.2 FPT_ASLR_EXT.1

TOEは、プログラム実行毎にプロセスのアドレス空間内におけるメモリ領域の配置をランダム化することで、バッファオーバーフロー等の攻撃に対する耐性を向上させる。

ランダム化の対象となるメモリ領域を以下に示す。ランダム化のオフセットアドレスは、/proc/sys/vm/mmap_rnd_bitsにより制御され、x86_64アーキテクチャにおいては、28ビットをデフォルト値として、28から32ビットの範囲で設定可能である。

- 実行ファイル
  /proc/sys/vm/mmap_rnd_bitsに設定されたビット数の範囲内で、コードセグメントおよびデータセグメントの開始アドレスがランダム化される。

- 共有ライブラリ（.soファイル）
  共有ライブラリの開始アドレスは、/proc/sys/vm/mmap_rnd_bitsに設定されたビット数の範囲内でランダム化される。

- mmap領域
  mmapシステムコールによって割り当てられるメモリ領域の開始アドレスは、/proc/sys/vm/mmap_rnd_bitsに設定されたビット数の範囲内でランダム化される。

- ヒープ領域
  ヒープ領域の開始アドレスは、25ビットの範囲内でランダム化される。

- スタック領域
  スタック領域の開始アドレスは、22ビットの範囲内でランダム化される。

### 7.6.3 FPT_SBOP_EXT.1

TOEは、スタックベースのバッファオーバーフロー保護のためのスタックカナリアを用いている。

TOEは、提供するRPMパッケージビルド時に、以下の二つのstack-protector-strongとpieコンパイラーオプションを用いており、これによりスタック保護を行っている。

1. stack-protector-strongフラグは、スタック保護自体をプログラム内の関数に実装せずに、スタック保護のスコープを広げるために開発された。
   例) -fstack-protector-strong --param=ssp-buffer-size=4
2. ASLR(Address Space Layout Randomization)は、メモリのランダム化とアクセス保護に関して実行ファイルのセキュリティを改善する。
   例) -fpie -Wl,-pie

以下にスタック保護されていないバイナリーファイル、それを提供するパッケージ名とその理由を示す。

attrでは以下のバイナリーファイルが該当する。スタック内に配列を持たず、結論としてスタック保護を必要としない。
/usr/bin/setfattr

bind-utilsパッケージでは以下のバイナリーファイルが該当する。named-nzd2nzfは一つのメイン関数と他の問題のないバイナリーファイルでも使用されるオブジェクトファイルから構成される。このメイン関数はスタック内に配列を持たず、結論としてスタック保護を必要としない。
/usr/sbin/named-nzd2nzf

gccパッケージでは以下のバイナリーファイルが該当する。これらはリンカーに渡される特別なオブジェクトファイルであり問題ない。
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtbegin.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtbeginS.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtbeginT.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtend.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtendS.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtfastmath.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtoffloadbegin.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtoffloadend.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtoffloadtable.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtprec32.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtprec64.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/crtprec80.o
/usr/lib/gcc/x86_64-redhat-linux/11/32/libasan_preinit.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtbegin.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtbeginS.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtbeginT.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtend.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtendS.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtfastmath.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtoffloadbegin.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtoffloadend.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtoffloadtable.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtprec32.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtprec64.o
/usr/lib/gcc/x86_64-redhat-linux/11/crtprec80.o
/usr/lib/gcc/x86_64-redhat-linux/11/libasan_preinit.o
/usr/lib/gcc/x86_64-redhat-linux/11/liblsan_preinit.o
/usr/lib/gcc/x86_64-redhat-linux/11/libtsan_preinit.o

同様に、gccパッケージでは以下のバイナリーファイルが該当する。一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。結論として、スタック保護を必要としない。
/usr/lib/gcc/x86_64-redhat-linux/11/32/libgcc.a
/usr/lib/gcc/x86_64-redhat-linux/11/32/libgcc_eh.a

/usr/lib/gcc/x86_64-redhat-linux/11/32/libgcov.a
/usr/lib/gcc/x86_64-redhat-linux/11/libgcc.a
/usr/lib/gcc/x86_64-redhat-linux/11/libgcc_eh.a
/usr/lib/gcc/x86_64-redhat-linux/11/libgcov.a

glib2では以下のバイナリーファイルが該当する。ただし、いくつかの関数を有しているが、配列を全く有しておらずスタック保護を必要としない。
/usr/lib64/libgthread-2.0.so.0.6800.4

glibcパッケージでは以下のバイナリーファイルが該当する。glibcパッケージは、スタックアンワインド、例外処理、並びに他の手書きのアセンブラというコードの特別な処理が必要となるため問題ない。
/usr/lib64/ld-linux-x86-64.so.2

同様に、glibcパッケージでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/lib64/libanl.so.1
/usr/lib64/libdl.so.2
/usr/lib64/libmvec.so.1
/usr/lib64/libnss_dns.so.2
/usr/lib64/libnss_files.so.2
/usr/lib64/libpthread.so.0
/usr/lib64/librt.so.1
/usr/lib64/libutil.so.1

同様に、glibcパッケージでは以下のバイナリーファイルが該当する。これらは、glibc-commonで提供される getconf と同一のファイルである。glibc-commonを参照すること。
/usr/libexec/getconf/XBS5_LP64_OFF64
/usr/libexec/getconf/POSIX_V7_LP64_OFF64
/usr/libexec/getconf/POSIX_V6_LP64_OFF64

同様に、glibcパッケージでは以下のバイナリーファイルが該当する。一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。結論として、スタック保護を必要としない。
/usr/sbin/ldconfig

glibc-commonlibcパッケージでは以下のバイナリーファイルが該当する。一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。結論として、スタック保護を必要としない。
/usr/bin/getconf

glibc-develパッケージでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/lib64/libanl.a
/usr/lib64/libdl.a

/usr/lib64/libg.a
/usr/lib64/libmcheck.a
/usr/lib64/libpthread.a
/usr/lib64/librt.a
/usr/lib64/libutil.a

同様に、glibc-develパッケージでは以下のバイナリーファイルが該当する。これらのファイルはCランタイムスタートアップオブジェクトであり問題ない。
/usr/lib64/Mcrt1.o
/usr/lib64/Scrt1.o
/usr/lib64/crt1.o
/usr/lib64/crti.o
/usr/lib64/crtn.o
/usr/lib64/grcrt1.o
/usr/lib64/rcrt1.o

glibc-gconv-extraパッケージでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/lib64/gconv/libCNS.so
/usr/lib64/gconv/libGB.so
/usr/lib64/gconv/libISOIR165.so
/usr/lib64/gconv/libJIS.so
/usr/lib64/gconv/libJISX0213.so
/usr/lib64/gconv/libKSC.so

grub2-toolsでは以下のバイナリーファイルが該当する。grub2-file と grub2-menulst2cfgはスタック上に配列を有していない。grub2-mkimage, grub2-mkrelpath, grub2-script-check, grub2-bios-setupはスタック上に配列を有しているが、全て静的である。grub2-installは一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。結論として、スタック保護を必要としない。
/usr/bin/grub2-file
/usr/bin/grub2-menulst2cfg
/usr/bin/grub2-mkimage
/usr/bin/grub2-mkrelpath
/usr/bin/grub2-script-check
/usr/sbin/grub2-bios-setup
/usr/sbin/grub2-install

grub2-tools-minimalでは以下のバイナリーファイルが該当する。一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。結論として、スタック保護を必要としない。
/usr/bin/grub2-editenv s
/usr/bin/grub2-mkpasswd-pbkdf2
/usr/bin/grub2-mount
/usr/sbin/grub2-probe

/usr/sbin/grub2-set-bootflag

iputilsでは以下のバイナリーファイルが該当する。一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。結論として、スタック保護を必要としない。
/usr/bin/clockdiff

kernel-modules-coreパッケージには以下のスタック保護されていないバイナリーファイルが存在する。ただし、スタック上に配列を定義しておらず、それゆえスタックスマッシュ保護(stack smashing protection)を必要としない。
/lib/modules/5.14.0-284.11.1.el9_2.tuxcare.5.x86_64/vdso/vdso32.so
/lib/modules/5.14.0-284.11.1.el9_2.tuxcare.5.x86_64/vdso/vdso64.so

libcapでは以下のバイナリーファイルが該当する。非静的配列は適切に使用されており、スタック保護を必要とするコードは見当たらない。
/usr/sbin/setcap

libgccでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/lib64/libgcc_s-11-20240719.so.1

libicuでは以下のバイナリーファイルが該当する。これは他のlibicuが提供するライブラリから呼び出される静的データのみを提供している。結論としてスタック保護を必要としない。
/usr/lib64/libicudata.so.67.1

libqbでは以下のバイナリーファイルが該当する。単一のシンプルな関数から成り、スタック保護を必要としない。
/usr/sbin/qb-blackbox

ncursesでは以下のバイナリーファイルが該当する。clearはスタック上に配列を有しているが、全て静的である。tabsは一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。結論として、スタック保護を必要としない。
/usr/bin/clear
/usr/bin/tabs

ncurses-libsでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/lib64/libpanel.so.6.2
/usr/lib64/libpanelw.so.6.2

openssl-libsでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/lib64/engines-3/capi.so

pamでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/lib64/security/pam_debug.so
/usr/lib64/security/pam_deny.so
/usr/lib64/security/pam_postgresok.so

同様に、pamでは以下のバイナリーファイルが該当する。非静的配列は適切に使用されており、スタック保護を必要とするコードは見当たらない。
/usr/lib64/security/pam_filter/upperLOWER

postfixパッケージでは、canvil, spawn, trivial-rewrite postdrop, postfix, postlogは、スタック上に配列を有しているが、全て静的であるため、スタック保護を必要としない。postkick, postlockに関しては、スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/libexec/postfix/anvil
/usr/libexec/postfix/spawn
/usr/libexec/postfix/trivial-rewrite
/usr/sbin/postdrop
/usr/sbin/postfix
/usr/sbin/postkick
/usr/sbin/postlock
/usr/sbin/postlog

procps-ngでは以下のバイナリーファイルが該当する。スタック上に配列を有しているが、全て静的であるため、スタック保護を必要としない。
/usr/bin/free

python3では以下のバイナリーファイルが該当する。単一のシンプルな関数から成り、配列を全く有しておらずスタック保護を必要としない。
/usr/bin/python3.9

python3-libsでは以下のバイナリーファイルが該当する。libpython3.soは、スタック上に配列を有さない。他は、スタック上に配列を有しているが、静的である。結論としてスタック保護を必要としない。
/usr/lib64/libpython3.so
/usr/lib64/python3.9/lib-dynload/_contextvars.cpython-39-x86_64-linux-gnu.so
/usr/lib64/python3.9/lib-dynload/_curses_panel.cpython-39-x86_64-linux-gnu.so
/usr/lib64/python3.9/lib-dynload/_heapq.cpython-39-x86_64-linux-gnu.so
/usr/lib64/python3.9/lib-dynload/_statistics.cpython-39-x86_64-linux-gnu.so

rpmでは以下のバイナリーファイルが該当する。rpmdbは、一部は静的な配列を有している。他の非静的な配列に関しては適切に使用されており、スタック保護を必要とするコードは見当たらない。rpmkeyは、スタック上に配列を有しているが、静的であるため、スタック保護を必要としない。
/usr/bin/rpmdb
/usr/bin/rpmkeys

systemdでは以下のバイナリーファイルが該当する。スタック上に配列を有さない。結論としてスタック保護を必要としない。
/usr/lib/systemd/systemd-ac-power
/usr/lib/systemd/systemd-cgroups-agent
/usr/lib/systemd/systemd-user-sessions

systemd-udevでは以下のバイナリーファイルが該当する。スタック上に配列を有しているが、全て静的であるため、スタック保護を必要としない。
/usr/lib/systemd/systemd-quotacheck

util-linuxでは以下のバイナリーファイルが該当する。スタック上に配列を有しているが、全て静的であるため、スタック保護を必要としない。
/usr/bin/rev
/usr/sbin/findfs
/usr/sbin/pivot_root

vim-commonでは以下のバイナリーファイルが該当する。スタック上に配列を有しているが、全て静的であるため、スタック保護を必要としない。
/usr/bin/xxd

### 7.6.4 FPT_SRP_EXT.1

TOEは、実行されようとするファイルの識別情報（パス、ハッシュ値）に基づき、あらかじめ定義されたルールと照合を行い、実行を許可または拒否することで、未承認アプリケーションの実行を防止する。TOEが信頼するファイルの識別情報は、トラストデータベースと呼ばれるデータベースに格納されており、これは/var/lib/fapolicyd/data.mdbに保存される。実行判定に用いられるルールは、/etc/fapolicyd/rules.dディレクトリに保存されている

### 7.6.5 FPT_TST_EXT.1

ブートチェーンはIntel x86_64 UEFIプラットフォーム上で行われる。
Intel x86-64 UEFIプラットフォームにおけるブートチェーンは、次の1～4のステップで行われる。

1. 電源を入れると、UEFIファームウェアは、ハードウェアの初期化を行い、First Stage Bootloaderであるshimをロードする。UEFIファームウェアが、ハードウェアで保護された非対称鍵でshimのデジタル署名を検証する。UEFIファームウェアは信頼された証明書のデータベース（db）を保持している。dbには、証明書が格納されており、UEFIファームウェアは、dbに格納されている証明書の公開鍵を使用して、shimの署名を検証する。証明書の検証に使う暗号アルゴリズムは2048bit鍵長のRSA-2048を用い、ハッシュ関数としてSHA-256を使用する。

2. shimのデジタル署名の検証に成功したら、UEFIファームウェアは、shimを起動する。起動したshimは、Second-stage bootloaderであるGRUB2のデジタル署名を検証する。デ

ジタル署名の検証は、コンパイル時に組み込まれた対応する証明書の公開鍵を使用して検証する。署名検証は、暗号アルゴリズムとしてRSA-2048を、ハッシュ関数としてSHA-256を用いる。

3. grub2のデジタル署名の検証に成功したら、shimはGRUB2を起動する。
   起動したGRUB2は、OSが起動する前の初期化処理を行い、TOEのLinux kernelのデジタル署名を検証する。GRUB2はshimと連携し、デジタル署名の検証をshimに委任して実施する。署名検証は、暗号アルゴリズムとしてRSA-2048を、ハッシュ関数としてSHA-256を用いる。

4. Linux kernelの署名検証に成功したら、GRUB2はLinux kernelを起動する。

## T7.6.6 FPT_TUD_EXT.1, FPT_TUD_EXT.2

TOEには、TOE自体とアプリケーション・ソフトウェアのアップデートをチェックする機能がある。どちらのタイプのアップデートも、インストール前にRSA-4096とSHA-256によって検証される。TOEおよびアプリケーション・ソフトウェアのアップデートは、次のコマンドによりリポジトリサーバーからTOEによってダウンロードされる。

```
# dnf upgrade
```

リポジトリサーバーの設定は、/etc/yum.repos.dディレクトリ内の設定ファイルに記述されている。これらのファイルでは、デフォルトでmirrorlist項目にミラーサーバーのURLが指定されており、TOEはそのミラーサーバーに接続して、更新に必要なソフトウェアをダウンロードする。

## 7.7 TOEアクセス

### 7.7.1 FTA_TAB.1

TOEは、ローカルまたはリモートの対話型ユーザーセッションを確立する前に、管理者が設定した未認可使用に関する警告を含む情報バナーを画面に表示することで明確に注意喚起を行う。

TOEのローカルコンソールからログインする場合は、/etc/issueに記述したメッセージの内容が表示され、リモートからログインする場合は、/etc/issue.netに記述したメッセージの内容が表示される。/etc/issue、/etc/issue.netについては、管理者のみが編集できる。

## 7.8 高信頼パス/チャネル

### 7.8.1 FTP_ITC_EXT.1

TOEは、「Functional Package for Secure Shell (SSH), version 1.0」に適合するSSHv2プロトコルおよび、「Functional Package for Transport Layer Security (TLS), version 1.1」に適合するTLS 1.2クライアントプロトコルを提供する。

SSHプロトコルは、TOEがクライアントおよびサーバーとして動作し、TOEと許可されたITエンティティとの通信を保護する高信頼チャネルを提供する。これにより、TOEはリモートユーザーとの通信を保護し、ユーザーが次の通信動作を実行するためにリモートサーバーへ安全に接続することを可能とする。

- remote administration via SSH
    - TOEとは別のSSHクライアントからTOEへ接続するためのsshコマンド
- connections to remote SSH servers
    - TOEが接続するのに必要とするSSHサーバーへ接続するためのsshコマンド

TLSプロトコルは、アプリケーションと許可されたリモートITエンティティとの通信を保護する高信頼チャネルを提供する。また、TOEは、次の通信動作を実行するために、TLSクライアントプロトコルを提供する。

- application initiated TLS
    - リポジトリサーバーからTOEの更新に必要なソフトウェアのダウンロードを行うためのdnf downloadコマンド
    - TOEが生成した監査ログをリモートのrsyslogサーバーに送信するrsyslogデーモン
- software updates
    - リポジトリサーバーからTOEの更新に必要なソフトウェアのダウンロードとインストールを行うためのdnf upgradeコマンド

### 7.8.2 FTP_TRP.1

TOEは、ローカルユーザーおよびリモートユーザーとの間に論理的に区別された通信パスを提供し、ユーザーとTOE間のエンドポイントを確実に識別可能な高信頼パスを確立する。高信頼パスへのアクセスは、OSに認証されたユーザーによってのみ開始される。認証されたユーザーは、ローカルコンソールまたは、リモートコンソールからアクセスすることが出来る。

ローカルユーザーに対しては、直接接続されたローカルコンソールを高信頼パスとして提供する。ローカルコンソールは、TOEと物理的に直接接続されており保護されており、リモートユーザーとの保護されない通信は実施されない。リモートユーザーに対しては、通信経路における盗聴および改ざんを防止するために、暗号化通信を実現するSSHプロトコルを用いた高信頼パスを提供する。

TOEの管理は高信頼パスを通じてのみ行われるため、リモート管理者はTOEを安全に管理することが可能となる。

## 7.9 タイムリーなセキュリティ・アップデート

### 7.9.1 ALC_TSU_EXT.1

AlmaLinux OS Foundationはセキュリティ問題の報告を security@almalinux.org の電子メールアドレスで受け付けている。このメールアドレスで受け付けた内容は、AlmaLinux OS Foundationの限られたメンバーのみが参照できるように制限をかけられている。AlmaLinux OS Foundation は2-3日以内に報告への返答と問題の確認を行うように努める。報告者は電子メールをsecurity vulnerability reporting information (https://almalinux.org/.well-known/security.txt を参照)のEncryption欄で指定されたURIにある、PGPキーを使って暗号化することができる。

AlmaLinux OS Foundationは、情報公開抑止中のセキュリティ上の問題については、調査が実施され、脆弱性が公表されるまで、開示、議論並びに確認を行わない。問題の情報公開抑止期間が経過し、公表されるとその日のうちにAlmaLinux OS Foundationは問題の技術的な詳細、CVE(Common Vulnerabilities and Exposures)識別子および脆弱性によって影響を受けるソフトウェアをセキュリティ勧告として公表する。ユーザーはセキュリティ勧告を受け取ることにより、セキュリティアップデートが公開されたことを知ることができる。

セキュリティ勧告はannounceメーリングリストを通じて配信される。セキュリティアップデートパッケージは、FPT_TUD_EXT.1に記載されている標準アップデートメカニズムを通じて配信される。

AlmaLinux OS Foundationは、オープンソースコミュニティより公開されたセキュリティパッチを評価し、速やかにセキュリティアップデートとして提供する。FIPS 140-3準拠(TuxCareのRPMパッケージ)が必要なセキュリティアップデートの場合、AlmaLinux OS Foundationは、当該アップデート内容をTuxCare(※)へ共有してRPMパッケージの修正を依頼する。TuxCareによる修正作業完了後、AlmaLinux OS Foundationは、TuxCareより当該パッケージがリポジトリへ配置された旨の通知を受け取る。また、AlmaLinux OS Foundationは、新たに発見された脆弱性に対しては、当該コミュニティへ直接参画してセキュリティパッチの開発を支援するなど、問題解決に貢献できるよう努力する。

※TuxCareは、AlmaLinuxの商業的な部分を担っており、AlmaLinux OS Foundationに開発者を派遣している。さらに、FIPS140-3準拠のパッケージのメインテナンスを行っている。

# 8 リファレンス


[PPOS] Protection Profile for General Purpose Operating Systems
Version: 4.3
2022-09-27
https://www.niap-ccevs.org/static_html/protection-profile/469/OS%204.3%20PP/index.html

[PKGSSH] Functional Package for Secure Shell (SSH)
Version: 1.0
2021-05-13
https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/pkg_ssh_v1.0.pdf

[PKGTLS] Functional Package for Transport Layer Security (TLS)
Version: 1.1
2019-02-12
https://www.commoncriteriaportal.org/nfs/ccpfiles/files/ppfiles/PKG_TLS_V1.1.pdf