認 証 報 告 書

東京都文京区本駒込2丁目28番8号
独立行政法人情報処理推進機構
理事長　齊藤　裕

押印済

IT製品（TOE）

申請受付日（受付番号）	令和7年4月14日（IT認証5912）
認証識別	JISEC-C0869
製品名称	AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3
バージョン及びリリース番号	1.00
製品製造者	サイバートラスト株式会社
プロテクションプロファイル	Protection Profile for General Purpose Operating Systems Version 4.3（認証識別：CCEVS-VR-PP-0091） Functional Package for Secure Shell (SSH) Version 1.0（認証識別：CCEVS-VR-PP-0075） Functional Package for Transport Layer Security (TLS) Version 1.1
機能要件適合	プロテクションプロファイル適合、CCパート2拡張
保証パッケージ	プロテクションプロファイル適合、CCパート3拡張
ITセキュリティ評価機関の名称	株式会社ECSEC Laboratory 評価センター

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
令和8年6月16日

セキュリティセンター 技術評価部
技術管理者　矢野 達朗

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 3.1 Release 5
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 5
③ CC and CEM addenda - Exact Conformance, Selection-based SFRs, and Optional SFRs, Version 2.0

評価結果：合格

「AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3、バージョン 1.00」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証等に関する要求事項に従い、定められた規格

に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、サイバートラスト株式会社が開発した「AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3、バージョン 1.00」（以下「本 TOE」という。）について株式会社 ECSEC Laboratory 評価センター（以下「評価機関」という。）が令和 8 年 4 月 13 日に完了した IT セキュリティ評価に対し、その認証結果を申請者であるサイバートラスト株式会社に報告するとともに、本 TOE に関心を持つ調達者に対しセキュリティ情報を提供するものである。

本認証報告書は、本 TOE を購入する調達者を読者と想定している。本認証報告書の読者は、10 章のセキュリティターゲット（以下「ST」という。）を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 プロテクションプロファイル又は保証パッケージ

本 TOE は、次のプロテクションプロファイル[11]、及びプロテクションファイルが要求する機能パッケージ[12][13] （以下、これらを合わせて「適合 PP」という。）に適合する。

Protection Profile for General Purpose Operating Systems Version 4.3
(認証識別：CCEVS-VR-PP-0091)

Functional Package for Secure Shell (SSH) Version 1.0
(認証識別：CCEVS-VR-PP-0075)

Functional Package for Transport Layer Security (TLS) Version 1.1

1.1.2 TOEとセキュリティ機能性

本 TOE は、一般的なサーバー環境で使用される、Linux ベースの汎用オペレーティングシステム（以下「OS」という。）である。

本 TOE は、TOE が扱うデータ及び TOE 上で実行されるアプリケーションのデータを保護するために、適合 PP が要求するセキュリティ機能を提供する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について適合 PP の要求する保証要件の範囲で評価が行われた。

本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本 TOE が扱うデータ及び TOE 上で実行されるアプリケーションのデータは、TOE と外部 IT 機器との間の通信データへの不正なアクセスや、TOE に保存されたデータへの不正なアクセスによって、暴露されたり改ざんされたりする脅威がある。

また、本 TOE 上で不正なアプリケーションが実行されることにより、TOE のセキュリティ機能が損なわれる脅威がある。

それらの脅威に対抗するために、本 TOE は、識別認証、アクセス制御、暗号化、電子署名、セキュリティ機能保護などの、適合 PP が要求するセキュリティ機能を提供する。

1.1.2.2 構成要件と前提条件

本 TOE は、次のような構成及び前提で運用することを想定する。

本 TOE は、信頼できるコンピューター機器にインストールされ、組織内のネットワークに接続して利用される。

TOE の設定及び維持管理は、信頼できる管理者がガイダンス文書に従って行わなければならない。また、TOE の利用者は、組織のセキュリティポリシーに従い TOE を使用しなければならない。

1.1.3 免責事項

本 TOE の名称には FIPS140-3 が含まれるが、本報告書で報告する評価は FIPS140-3 への適合を保証するものではない。

また、本評価では、以下の運用を保証していない。

- 「4.2 運用環境と構成」の記載と異なる運用環境や構成
- 「7.5 評価構成について」の記載と異なる設定の TOE

1.2 評価の実施

認証機関が運営する IT セキュリティ評価及び認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、令和 8 年 4 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[10]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC[4][5][6]、CEM[7]及び補足文書[8]に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称：	AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3
バージョン：	1.00

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。

製品のガイダンスの記載に従ってコマンドを入力し、出力された以下の情報を確認する。

・OS の名称及びリリース情報：「AlmaLinux release 9.2」

・アーキテクチャ：「x86_64」

・FIPS140-3 対応及びバージョン(1.00)：

ST 1.2 節 Table 2 記載の 174 個の RPM パッケージの名称とバージョンがすべて表示されること。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は､TOE が扱うデータ及び TOE 上で実行されるアプリケーションのデータを保護するために、適合 PP が要求するセキュリティ機能を提供する。

3.1 セキュリティ機能方針

3.1.1 脅威とセキュリティ機能方針

本 TOE は、3.1.1.1 に示す脅威に対抗するセキュリティ機能を具備する。

3.1.1.1 脅威

本 TOE の対抗すべき脅威を表 3-1 に示す。

表3-1 脅威

識別子	脅威
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. 攻撃者は、通信チャネル上又はネットワークインフラのどこかに存在する。攻撃者は、侵害を意図して、TOEであるOS上又はOSの一部として実行されるアプリケーションやサービスの通信に関与するかもしれない。関与には既存の正当な通信の改ざんを含むかもしれない。

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. 攻撃者は、通信チャネル上又はネットワークインフラのどこかに存在する。攻撃者は、TOEであるOS上又はOSの一部として実行されるアプリケーションやサービス間でやり取りされるデータを監視しアクセスするかもしれない。
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. 攻撃者は、TOEであるOS上で実行されるアプリケーションを侵害するかもしれない。侵害されたアプリケーションは、権限のないシステムコールやファイルシステム経由のメッセージングを含む様々な経路を通じて、悪意のある形式の入力をTOEであるOSに供給するかもしれない。
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. 攻撃者は、物理デバイスを使用できる限られた時間に、TOEであるOS上のデータへのアクセスを試みるかもしれない。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。なお、各セキュリティ機能の詳細は、5 章に示す。

(1) 脅威「T.NETWORK_ATTACK」への対抗

TOE は、「高信頼パス/チャネル機能」、「識別認証機能」、「TSF 保護機能」、「暗号サポート機能」、「セキュリティ管理機能」及び「セキュリティ監査機能」で対抗する。

「高信頼パス/チャネル機能」は、TOE と外部 IT 機器との間の通信に、暗号通信プロトコルを適用し、通信データを改ざんから保護する。

「識別認証機能」は、「高信頼パス/チャネル機能」の外部 IT 機器の認証で使用する X.509 証明書の検証機能を提供する。

「TSF 保護機能」は、ネットワーク経由でインストールされるソフトウェアの完全性検証を行う。

「暗号サポート機能」は、「高信頼パス/チャネル機能」、「識別認証機能」及び「TSF 保護機能」で使用する各種暗号機能を提供する。

「セキュリティ管理機能」は、各種セキュリティ機能を設定するための管理機能を提供し、その操作を管理者だけに許可する。

「セキュリティ監査機能」は、セキュリティ機能に関連する事象を監査ログとして生成し、管理者がネットワーク経由の攻撃を把握可能にする。

以上の機能により、TOE は通信データの改ざんを防止する。

(2) 脅威「T.NETWORK_EAVESDROP」への対抗

TOE は、「高信頼パス/チャネル機能」、「識別認証機能」、「暗号サポート機能」及び「セキュリティ管理機能」で対抗する。

「高信頼パス/チャネル機能」は、TOE と外部 IT 機器との間の通信に、暗号通信プロトコルを適用し、通信データを暗号化する。

「識別認証機能」は、「高信頼パス/チャネル機能」の外部 IT 機器の認証で使用する X.509 証明書の検証機能を提供する。

「暗号サポート機能」は、「高信頼パス/チャネル機能」及び「識別認証機能」で使用する各種暗号機能を提供する。

「セキュリティ管理機能」は、各種セキュリティ機能を設定するための管理機能を提供し、その操作を管理者だけに許可する。

以上の機能により、TOE は通信データの盗聴を防止する。

(3) 脅威「T.LOCAL_ATTACK」への対抗

TOE は、「識別認証機能」、「暗号サポート機能」、「TSF 保護機能」及び「セキュリティ監査機能」で対抗する。

「識別認証機能」は、識別認証に成功した利用者のみに TOE の利用を許可する。

「TSF 保護機能」は、TOE のセキュリティ機能や TSF データへの不正アクセスや改ざんから保護するための自己保護メカニズムを提供する。

「暗号サポート機能」は、「識別認証機能」及び「TSF 保護機能」で使用する各種暗号機能を提供する。

「セキュリティ監査機能」は、セキュリティ機能に関連する事象を監査ログとして生成し、管理者が TOE 上での攻撃を把握可能にする。

以上の機能により、TOE は TOE 上での攻撃を防止する。

(4) 脅威「T.LIMITED_PHYSICAL_ACCESS」への対抗

TOE は、「暗号サポート機能」及び「ユーザーデータ保護機能」で対抗する。

「暗号サポート機能」は、ストレージの暗号化を行う。

「ユーザーデータ保護機能」はファイルやディレクトリへのアクセス制御機能を提供する。

以上の機能により、TOE は OS が扱うデータへの不正アクセスを防止する。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 TOE には、要求される組織のセキュリティ方針は無い。

4 前提条件と評価範囲の明確化

本章では、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を**表 4-1** に示す。これらの前提条件が満たされない場合、本 TOE のセキュリティ機能が有効に動作することは保証されない。

表 4-1 前提条件

識別子	前提条件
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP. TOEであるOSは、その実行のために、信頼できるコンピューティングプラットフォームに依存する。この基盤となるプラットフォームは適合PPの範囲外である。
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. TOEであるOSの利用者は、故意の過失や敵意を持たず、企業のセキュリティポリシーに従ってソフトウェアを使用する。その一方で、悪意のあるソフトウェアが利用者として動作する可能性があるため、悪意のあるサブジェクトを制限する要件は依然として適用される。
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. TOEであるOSの管理者は、不注意、故意の過失や敵意を持たず、企業のセキュリティポリシーに従ってTOEであるOSを管理する。

4.2 運用環境と構成

本 TOE の一般的な運用環境を図 4-1 に示す。OS である本 TOE は、実行環境である TOE Platform にインストールされ、ローカルネットワーク（以下「LAN」という。）に接続されており、TOE Platform のコンソール（以下「ローカルコンソール」という。）又は同様に LAN に接続された SSH クライアントから利用される。

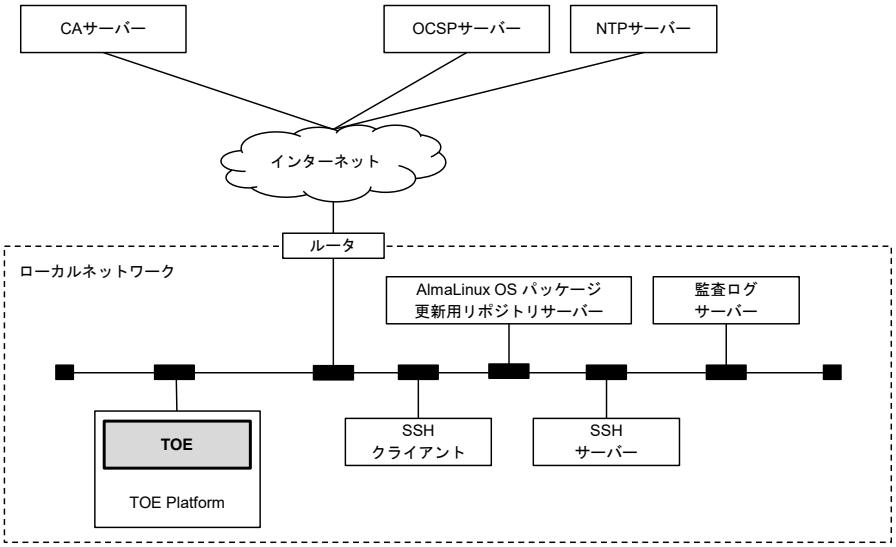

図 4-1 TOEの運用環境

本 TOE の運用環境の構成品を以下に示す。

(1) TOE Platform

本 TOE を実行させるために必要なコンピューター機器であり、Intel x86_64 アーキテクチャの CPU、メモリ、HDD、コンソール等のハードウェア、及びそれらを制御する UEFI ファームウェアで構成される。本評価では以下の機器を使用。

・機器：日本電気株式会社 FC-R16W
（構成）
CPU：Intel Xeon プロセッサー E5-2680 v4
メモリ：16GB
HDD：600GB×2(RAID1)
UEFI ファームウェア：
日本電気株式会社
R24W・R16W シリーズ用　マザーボード Firmware (FPGA)

(2) AlmaLinux OS パッケージ更新用リポジトリサーバー

本 TOE のソフトウェアのインストールや更新に使用される RPM パッケージを配付するための Web サーバーである。OCSP Stapling を利用可能な、TLS 1.2 対応の HTTPS プロトコルをサポートするソフトウェアが必要である。リポジトリサーバーは、LAN 内に設置するほかに、インターネットで公開されているリポジトリサーバーが使用可能である。本評価では以下のソフトウェアを使用。

・OS：Kali-Linux 2025.2
・Web サーバー：Apache 2.4.65

(3) SSH サーバー

管理者が必要に応じて本 TOE から他のサーバーをリモートで管理する場合を想定しており、その場合の他のサーバーを指す。SSHv2 プロトコルをサポートする SSH サーバーソフトウェアが必要である。本評価では以下のソフトウェアを使用。

・OS：Kali-Linux 2025.2
・SSH サーバー：OpenSSH 10.0p2

(4) SSH クライアント

本 TOE へ SSH 接続する端末であり、管理者が TOE の管理をリモートで実施する場合に必要となる。SSHv2 プロトコルをサポートする SSH クライアントソフトウェアが必要である。本評価では以下のソフトウェアを使用。

・OS：Kali-Linux 2025.2
・SSH クライアント：OpenSSH 10.0p2

(5) 監査ログサーバー

本 TOE の生成した監査ログを受信するサーバーである。OCSP Stapling を利用可能な、TLS 1.2 対応の Syslog プロトコルをサポートするソフトウェアが必要である。本評価では以下のソフトウェアを使用。

・OS：Kali-Linux 2025.2
・監査ログサーバー：rsyslogd 8.2504.0

(6) NTP サーバー

TOE に正確な時刻情報を提供するサーバーである。NTP サーバーは、インターネット上の信頼できる NTP サーバーを使用するほか、組織内のネットワークに設置した NTP サーバーも使用可能である。NTP プロトコルをサポートするソフトウェアが必要である。本評価では以下のソフトウェアを使用。

・OS：Kali-Linux 2025.2
・NTP サーバー：chronyd 4.4

(7) OCSP サーバー（OCSP レスポンダ）

AlmaLinux OS パッケージ更新用リポジトリサーバーと監査ログサーバーが、X.509 証明書の失効状態を確認するためのサーバーである。インターネット上の認証局が提供する OCSP サーバーの使用を想定している。本評価では以下のソフトウェアを使用。

・OS：Kali-Linux 2025.2
・OCSP サーバー：OpenSSL 3.5.1-1

(8) CA サーバー

TOE の取り扱う X.509 証明書の発行を行うサーバーである。インターネット上の認証局が提供する CA サーバーの使用を想定している。本評価では以下のソフトウェアを使用。

・OS：Kali-Linux 2025.2
・CA サーバー：OpenSSL 3.5.1-1

なお、本構成に示されている TOE 以外のハードウェア及びソフトウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

本 TOE の提供する機能、及び、本評価で保証される本 TOE の機能には、以下の制約がある。

(1) 評価対象外の機能

本 TOE は、Linux ベースの OS として以下の機能を提供するが、評価構成では無効化されており本評価の範囲には含まれない。

・SELinux

・OS 仮想化インフラ及びコンテナ仮想化インフラ

・グラフィカルユーザーインターフェース

(2) 高信頼パス/チャネル

本 TOE の高信頼パス/チャネル機能は、本 TOE と AlmaLinux OS パッケージ更新用リポジトリサーバー、SSH サーバー、SSH クライアント及び監査ログサーバーとの間の通信に適用され、本 TOE とその他の機器との間の通信には適用されない。

(3) SSH の認証方式

SSH サーバー又は SSH クライアントとの SSH 接続時の認証では、SSH 規定の公開鍵認証方式をサポートしており、X.509 証明書による認証はサポートしていない。そのため、SSH の用途では、CA サーバー及び OCSP サーバーは必要としない。

(4) 各種サーバー及びクライアント PC

TOE と連携して動作する各種サーバーやクライアント PC がセキュアに運用されることは、管理者の責任である。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成を説明する。

5.1 TOE境界とコンポーネント構成

本 TOE は、2 章で説明したように、AlmaLinux OS 9.2 for x86_64 をベースに、必要なパッケージをインストールした OS 全体である。

本 TOE は、以下のセキュリティ機能を提供する。

(1) セキュリティ監査機能

本機能は、セキュリティ機能に関する監査事象を監査ログとして生成する機能である。

なお、生成された監査ログは、TOE に保存されると共に監査ログサーバーに送信され、TSF 保護機能及び高信頼パス/チャネル機能によって保護される。

(2) 暗号サポート機能

本機能は、ストレージを暗号化する機能を提供する。また、他の高信頼パス/チャネル機能、識別認証機能及び TSF 保護機能で使用する各種暗号機能を提供する。提供する暗号機能には以下が含まれる。

・暗号通信プロトコル（SSHv2, TLS 1.2）
・非対称暗号鍵の生成
・暗号鍵の確立
・暗号鍵及び鍵マテリアルの破棄
・データの暗号化及び復号
・ハッシュ関数
・電子署名の生成及び検証
・鍵付ハッシュメッセージ認証コード
・決定論的ランダムビット生成

上記の各種暗号機能で使用される暗号通信プロトコル、暗号アルゴリズム、暗号鍵長は、適合 PP が指定するものである。

決定論的ランダムビット生成のシード入力は、CPU 命令実行のばらつきから得たデータであり、推測の困難な十分なエントロピーを持つ。

(3) ユーザーデータ保護機能

本機能は、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にアクセスを制御する機能である。アクセス制御の

方式は、一般的な UNIX のパーミッションと POSIX タイプのアクセス制御リストの 2 つの方式を提供する。

(4) 識別認証機能

本機能は、TOE の利用者を認証する機能である。また、外部 IT 機器の認証のための X.509 証明書の検証機能を提供する。

利用者はユーザー名で識別を行い、ローカルコンソールではパスワードを用いて、SSH 接続ではパスワード又は SSH 規定の公開鍵を用いて認証される。パスワード認証については、最小パスワード長の制限、パスワード文字種の設定、連続した認証失敗によるアカウントのロックアウトの機能性を備えている。パスワードのハッシュ化及び SSH の公開鍵認証の電子署名の検証機能は、暗号サポート機能により提供される。

X.509 証明書の検証機能は、高信頼パス/チャネル機能を使用した TLS 接続時の接続先の外部 IT 機器の認証に用いられる。TOE は、TLS 接続時に OCSP Stapling を用いて、接続先の外部 IT 機器から X.509 証明書の失効情報を取得する。X.509 証明書の電子署名の検証機能は、暗号サポート機能により提供される。

(5) セキュリティ管理機能

本機能は、各種セキュリティ機能の設定を管理者に制限する機能である。

(6) TOE アクセス機能

本機能は、利用者が TOE にログインする前に、不正利用に関する警告バナーを表示し注意喚起を行う機能である。

(7) TSF 保護機能

本機能は、TOE のセキュリティ機能及び TSF データを不正アクセスや改ざんから保護する機能である。以下の機能が含まれる。

・システムファイルのアクセス制御
・ファイルの識別情報に基づく未承認アプリケーションの実行防止
・スタックカナリア及びアドレス空間配置のランダム化（ASLR）による
バッファオーバーフロー攻撃の保護や耐性強化
・OS 起動時のソフトウェアの電子署名の検証（セキュアブート）
・ソフトウェアアップデートの電子署名の検証

セキュアブート及びソフトウェアアップデートで使用される電子署名の検証機能は、暗号サポート機能により提供される。

(8) 高信頼パス/チャネル機能

本機能は、TOE と AlmaLinux OS パッケージ更新用リポジトリサーバー又は監査ログサーバーとの通信を暗号通信プロトコル TLS1.2、TOE と SSH サーバー又は SSH クライアントとの通信を暗号通信プロトコル SSHv2 で保護する機能である。暗号通信プロトコル TLS1.2、SSHv2 及び関連する暗号機能は、暗号サポート機能により提供される。

なお、ローカルコンソールも高信頼パス/チャネル機能の対象であり、LAN を経由せずに TOE と直接接続することで保護される。

5.2 IT環境

TOE の「高信頼パス/チャネル機能」は、外部 IT 機器と連携して実現され、以下のプロトコルを使用する。

- AlmaLinux OS パッケージ更新用リポジトリサーバー：HTTP over TLS
- SSH サーバー：SSH
- SSH クライアント：SSH
- 監査ログサーバー：Syslog over TLS

また、TOE の「TSF 保護機能」のセキュアブートは、TOE Platform に搭載された UEFI ファームウェアと連携して実現される。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を表 6-1 に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

表 6-1　ガイダンス

名称	バージョン
AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 Common Criteria ガイダンス	1.43
AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 一般用ガイダンス	1.14

7 評価機関による評価実施及び結果

7.1 評価機関

評価を実施した株式会社 ECSEC Laboratory 評価センターは、IT セキュリティ評価及び認証制度により承認されるとともに、ISO/IEC 17025 の要求に基づいて認定機関（独立行政法人製品評価技術基盤機構認定センター）により認定を受けており、評価品質維持のためのマネジメント及び要員等の適切性についての要求事項を満たしていることが定期的に確認されている。

7.2 評価方法

評価は、適合 PP が要求する CC パート 3 の保証要件について、CEM に規定された評価方法及び適合 PP の評価アクティビティを用いて行われた。

評価の詳細は、評価報告書において報告された。評価報告書では、CEM のワークユニット及び適合 PP の評価アクティビティごとの評価内容及び判断結果を説明する。

7.3 評価実施概要

評価は、令和 7 年 4 月に始まり、令和 8 年 4 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、令和 7 年 10 月から令和 8 年 3 月にかけて評価機関において評価者テストを実施した。

評価機関が評価作業中に検出した問題点は、所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が評価の認証作業中に検出した問題点は、認証レビューとして発行され、評価機関に報告された。それらの問題点は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.4 製品テスト

評価者は、評価証拠資料に基づいて、製品のセキュリティ機能が確実に実現されていることを保証するための評価者独立テスト及び脆弱性評定に基づく評価者侵入テストを実施した。

7.4.1 開発者テスト

本評価において、開発者テストは保証要件には含まれない。

7.4.2 評価者独立テスト

評価者は、評価証拠資料に基づいて、製品のセキュリティ機能が確実に実現されていることを保証するための評価者独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、図 4-1 に示した TOE の運用環境に準じた構成である。独立テストの環境で使用した構成品を表 7-1 に示す。

表 7-1　独立テスト環境の構成品

構成品	詳細
TOE Platform	日本電気株式会社 FC-R16W ・CPU: Intel Xeon プロセッサー E5-2680 v4 ・メモリ: 16GB ・HDD: 600GB×2(RAID1) ・UEFIファームウェア: 日本電気株式会社 R24W・R16Wシリーズ用 マザーボード Firmware (FPGA)
各種サーバー	・OS: Kali-Linux 2025.2 ・AlmaLinux OSパッケージ 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: OpenSSL 3.5.1-1 ・CAサーバー: OpenSSL 3.5.1-1

独立テストの構成は、ST において識別されている TOE の構成と以下のような違いがある。評価者は、それらの違いに問題はなく、評価者の実施した独立テストによって、ST において識別されている TOE の構成のセキュリティ機能が適切にテストされたと見なすことができると判断している。

① テスト用ツールの追加使用

独立テストでは、通信データの確認や変更などのために、テスト用のツールが使用された。それらのテスト用ツールの妥当性は評価者によって確認されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が、適合PPの要求及び評価証拠資料から考案した独立テストの観点は以下のとおりである。

＜独立テストの観点＞

① セキュリティ機能をセキュリティ機能要件（SFR）ごとに確認する。

② 暗号アルゴリズムの実装が正しいことを確認する。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

TOE に対して、ローカルコンソール、SSH クライアント、テストツールを使用して入力を行い、そのふるまいを TOE の外部インタフェースを利用して確認する。

＜独立テストの実施内容＞

独立テストの観点に対応したテスト内容を表 7-2 に示す。

表 7-2　実施した独立テスト

観点	テスト概要
①	＜セキュリティ機能の確認> 適合PPのSFRごとに指定された評価アクティビティ、又は、SFRの要件に基づいて作成したテスト項目により、すべてのセキュリティ機能が仕様どおりに動作することを確認する。
②	＜暗号アルゴリズムの実装の確認＞ 以下の暗号アルゴリズムが仕様どおりに実装されていることを確認する。 - RSA-2048、RSA-3072、RSA-4096 - ECDSA P-384、ECDSA P-521 - KAS-ECC-SSC - AES-CBC-256、AES-CTR-256、AES-GCM-256、AES-XTS-256 - SHA-256、SHA-384、SHA-512

	- HMAC-SHA-256、HMAC-SHA-384、HMAC-SHA-512 - CTR_DRBG (AES-256)、HMAC_DRBG (SHA-512)

c) 結果

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.4.3 評価者侵入テスト

評価者は、想定される運用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、公知の情報及びTOEに含まれるパッケージ情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① TOEに意図しないネットワークポートが開いている懸念がある。

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テストの環境は、独立テストの環境に、侵入テスト用のツールを追加した環境である。侵入テストで使用したツールを表 7-3 に示す。

表 7-3 侵入テスト用ツール

名称	概要・利用目的
Nmap Version 7.95	利用可能なネットワークポートを検出するツール

＜侵入テストの実施内容＞

懸念される脆弱性に対応する侵入テスト内容を表 7-4 に示す。

表 7-4　侵入テスト概要

脆弱性	テスト概要
①	Nmapを使用して、TOEに想定外のネットワークポートが開いていないことを確認する。

c) 結果

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.5　評価構成について

本評価の前提となる TOE の構成条件は、6 章に示したガイダンスに記述されているとおりである。本TOEを評価で保証されたとおりに安全に使用するためには、ガイダンスの記述のとおりに TOE を設定しなければならない。ガイダンスと異なる設定にした場合は、本評価による保証の対象ではない。

7.6 評価結果

評価者は、評価報告書をもって本 TOE が CEM のワークユニット及び適合 PP の評価アクティビティのすべてを満たしていると判断した。

評価では以下について確認された。

PP 適合：

Protection Profile for General Purpose Operating Systems Version 4.3
Functional Package for Secure Shell (SSH) Version 1.0
Functional Package for Transport Layer Security (TLS) Version 1.1

セキュリティ機能要件：　コモンクライテリア　パート2　拡張

セキュリティ保証要件：　コモンクライテリア　パート3　拡張

評価の結果として、適合 PP が要求する以下の保証コンポーネントについて「合格」判定がなされた。

ASE_INT.1, ASE_CCL.1, ASE_SPD.1, ASE_OBJ.2, ASE_ECD.1, ASE_REQ.2, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ALC_TSU_EXT.1, ATE_IND.1, AVA_VAN.1

評価の結果は、2 章に記述された識別に一致する TOE について、「4.2 運用環境と構成」及び「7.5 評価構成について」に記述された構成のみに適用される。

7.7 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の観点で認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するCEMのワークユニット及び適合PPの評価アクティビティが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEM及び適合PPの評価アクティビティに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

評価機関より提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE の評価が適合 PP の要求する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE に興味のある調達者は、「4.2 運用環境と構成」及び「7.5 評価構成について」の記載内容を参照し、本 TOE の評価範囲や運用上の要求事項が、各自の想定する運用条件に合致しているかどうか注意が必要である。

本評価で保証される TOE のバージョン「1.00」は、TOE では表示されないため、2 章の記述のとおり、TOE にインストールされた 174 個のパッケージ名称とバージョンの表示を確認しなければならない。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[9]は、本報告書とは別文書として提供され、以下のとおり識別される。

AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 セキュリティターゲット, バージョン 1.7.15, 2026 年 4 月 13 日, サイバートラスト株式会社

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
PP	Protection Profile（プロテクションプロファイル）
SFR	Security Functional Requirement（セキュリティ機能要件）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

ASLR	Address Space Layout Randomization
CA	Certification Authority
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LAN	Local Area Network
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OS	Operating System
RPM	Red Hat Package Manager
SSH	Secure Shell
TLS	Transport Layer Security

本報告書で使用された用語の定義を以下に示す。

FIPS140-3	暗号モジュールのセキュリティ要件に関する米国連邦標準規格。
OCSP Stapling	RFC 6066で規定されたTLS拡張機能。TLSサーバー側がOCSPサーバーに問い合わせを行い、得られたX.509証明書の失効情報をTLS接続時にTLSクライアントに提供する。
RPMパッケージ	Linuxのソフトウェア配布形式の一種。
評価アクティビティ	PP適合のために評価者が実施しなければならない評価作業。CEMの補足であり、適合PP [11][12][13]では適合PPの中に記述されている。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 令和7年8月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 令和5年12月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 令和3年10月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] Common Methodology for Information Technology Security Evaluation : Evaluation methodology Version 3.1 Revision 5, April 2017, CCMB-2017-04-004

[8] CC and CEM addenda - Exact Conformance, Selection-based SFRs, and Optional SFRs, Version 2.0, Sep 2021, CCDB-013

[9] AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 セキュリティターゲット, バージョン 1.7.15, 2026年4月13日, サイバートラスト株式会社

[10] AlmaLinux OS 9.2 for x86_64 Compatible FIPS140-3 1.00, 評価報告書, 第1.13版, 2026年4月13日, 株式会社 ECSEC Laboratory 評価センター

[11] Protection Profile for General Purpose Operating Systems, Version 4.3, 2022-09-27 (認証識別：CCEVS-VR-PP-0091)

[12] Functional Package for Secure Shell (SSH), Version 1.0, 2021-05-13 (認証識別：CCEVS-VR-PP-0075)

[13] Functional Package for Transport Layer Security (TLS), Version 1.1, 2019-02-12