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　富田　達夫

原紙押印済

プロテクションプロファイル（PP）

申請受付日（受付番号）	令和4年2月8日（IT認証2805）
認証識別	JISEC-C0755
プロテクションプロファイル名称／識別	特定用途機器 - 共通セキュリティ　プロテクションプロファイル
プロテクションプロファイルバージョン番号	1.0版
プロテクションプロファイル開発者	独立行政法人情報処理推進機構、 特定用途機器情報セキュリティ対策検討委員会
プロテクションプロファイル申請者	独立行政法人情報処理推進機構
要求する保証要件	ASE_INT.1, ASE_CCL.1, ASE_OBJ.1, ASE_ECD.1, ASE_REQ.1, ASE_TSS.1, ADV_FSP.1, AGD_OPE.1, AGD_PRE.1, ALC_CMC.1, ALC_CMS.1, ATE_IND.1, AVA_VAN.1
ITセキュリティ評価機関の名称	一般社団法人ITセキュリティセンター　評価部

上記のPP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4年8月3日

セキュリティセンター セキュリティ技術評価部
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 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 リリース5
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース5

評価結果：合格

「特定用途機器 - 共通セキュリティ　プロテクションプロファイル 1.0版」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、独立行政法人情報処理推進機構及び特定用途機器情報セキュリティ対策検討委員会が開発した「特定用途機器 - 共通セキュリティ　プロテクションプロファイル 1.0 版」[12]（以下「本 PP」という。）について一般社団法人 IT セキュリティセンター　評価部（以下「評価機関」という。）が令和 4 年 6 月 17 日に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である独立行政法人情報処理推進機構に報告するとともに、本 PP に関心を持つ調達者や消費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 PP に適合した製品開発を行う開発者及び製品調達者を読者と想定している。本認証報告書は、本 PP 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。

また、本認証報告書の読者は本 PP を併読されたい。特に本 PP が要求するセキュリティ機能要件及び保証要件について詳述されている。

1.1 評価対象PP概要

本 PP 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 PP概要

本 PP は、ネットワークに接続されたカメラやセンサのような特定の用途に使用される機器（以下「特定用途機器」という。）に関するセキュリティ要件を規定するものである。

本 PP に適合する特定用途機器（以下、「TOE」という。）は、IoT 機器のような IP ネットワークに接続される機器を対象としており、テレビ会議やモニタリング等の情報システムの構成要素として使用される。

本 PP では、政府統一基準[14]が特定用途機器に求める遵守事項及び技適セキュリティ基準が IoT 機器に求める技術基準の、基本的かつ共通的なセキュリティ機能を TOE に要求する。

1.1.1.1 保証要件

本 PP が要求する保証要件は以下のものである。

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

1.1.1.2 セキュリティ対策方針

TOE はカメラやセンサのような機器であり、情報の保護を主目的とした機器ではない。しかし、工場出荷時の機器共通のパスワード、運用に不要なネットワークサービス、セキュリティパッチが適用されず放置された脆弱性等が悪用され TOE への不正なアクセスが発生すると、TOE の取り扱う情報だけでなく、TOE と同じ IP ネットワークに接続された他の情報システムへ危害を及ぼす可能性がある。

そこで本 PP では、TOE への不正なアクセスを防止し、自身を安全に動作させるため、以下のようなセキュリティ機能を TOE に要求する。

① 初回の管理機能利用前の強制的なパスワード設定・変更機能

② 管理者を識別・認証する機能

③ 運用に不要なネットワークサービスを管理者が停止できる機能

④ ファームウェア／ソフトウェアのアップデートデータを検証する機能

⑤ 上記①～④の機能へのアクセスを管理者が認知できる監査機能

1.1.1.3 構成要件と前提条件

本 PP は、TOE が次のような構成及び前提で運用されることを想定する。

TOE は、IP ネットワークに接続され、利用者の端末や各種サーバとともにテレビ会議やモニタリング等の情報システムの構成要素として使用される。

TOE の更新用のソフトウェアやファームウェアは、IP ネットワークに接続された遠隔のサーバから配信される。

TOE の運用にあたっては、管理者は組織の責任者により信頼される人物が選定され、管理者ガイダンスに従った設置・設定、運用及び対処を行う。

1.1.2 免責事項

本 PP で TOE に要求するセキュリティ要件は、特定用途機器に対する基本的な共通要件であり、各特定用途機器の個別の用途やその運用環境に特有の脅威には対抗していない。

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・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]及び「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 PP 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 4 年 6 月 17 日に完了した。

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[13]、所見報告書、及び関連する評価証拠資料を検証し、本 PP 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。本 PP の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）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 PP識別

本 PP は、以下のとおり識別される。

名称：	特定用途機器 - 共通セキュリティ　プロテクションプロファイル
バージョン：	1.0版
作成日：	2022年6月15日
開発者：	独立行政法人情報処理推進機構、 特定用途機器情報セキュリティ対策検討委員会

3 セキュリティ方針

本章では、本 PP に適合する TOE が実装すべきセキュリティ機能について述べる。

TOE は特定の用途の情報システムを構成する機器であり、IP ネットワークを介して利用者の端末や各種サーバと通信を行う機能を有する。本 PP は TOE が安易な初期パスワードの設定や運用に必要のないネットワークサービス等を悪用した TOE への不正なアクセスを防止し、自身を安全に動作させるためのセキュリティ機能を提供することを要求する。

3.1 セキュリティ対策

本 PP は、以下のセキュリティ機能を TOE に要求する。

3.1.1 初回の管理機能利用前の強制的なパスワード設定・変更機能

本機能の目的は、TOE が、管理者のパスワードが工場出荷時の機器共通の初期パスワードのまま、IP ネットワークに接続され運用されることを防止することである。

本 PP は、TOE に以下のいずれかの機能を要求する。

- 安易な初期パスワードの設定を防止するため、TOE の工場出荷時に TOE 毎に異なる推測不能なパスワードを設定する機能
- 初期パスワードのまま運用されることを防止するため、TOE の設置時に管理者のパスワードの設定・変更を強制する機能

3.1.2 管理者の識別認証機能

本機能の目的は、不正な利用者が TOE の管理機能にアクセスすることを防止することである。

本 PP は、TOE に管理機能にアクセスしようとする管理者の識別及び認証を行う機能を要求する。識別認証に成功した管理者には TOE の管理機能の利用が許可される。

3.1.3 運用に不要なネットワークサービスを管理者が停止できる機能

本機能の目的は、TOE の運用上必要のない TOE のネットワークサービスが起動されたまま運用されることを防止することである。

本 PP は、TOE に IP ネットワークに対しオープンとなっている TOE のサービスポートを管理者が停止及び起動できる機能を要求する。

3.1.4 ファームウェア／ソフトウェアのアップデートデータを検証する機能

本機能の目的は、TOE のソフトウェアやファームウェアをアップデートする際に、不正なソフトウェアやファームウェアによって TOE 自身が改ざんされることを防止することである。

本 PP は、TOE に遠隔のサーバから配信されるソフトウェアやファームウェアのアップデートデータの完全性を検証する機能を要求する。

3.1.5 監査機能

本機能の目的は、上記セキュリティ機能の使用等のセキュリティ事象を管理者が認知できるようにすることである。

本 PP は、TOE にセキュリティ事象が発生した際に、事象種別、発生日時、結果等の項目からなる監査ログを生成し、記録する機能を要求する。また、生成した監査ログを TOE 内部で安全に管理し、管理者が監査ログを読み出せる機能を TOE に要求する。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 PP に適合する TOE の利用の判断に有用な情報として、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 PP に適合する TOE を運用する際の運用環境のセキュリティ対策方針を**表 4-1** に示す。これらの対策方針が遵守されない場合、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 運用環境のセキュリティ対策方針

識別子	運用環境のセキュリティ対策方針
OE.TRUSTED_ADMIN	管理者は、組織の責任者により信頼される人物が選定され、管理者ガイダンスに従った設置・設定、運用及び対処を行う。

4.2 運用環境と構成

本 PP に適合する TOE は、IP ネットワークに接続され、利用者の端末や各種サーバとともにテレビ会議やモニタリング等の情報システムの構成要素として使用される。

IP ネットワークは、インターネットのような不特定多数の利用者がアクセスできるネットワーク環境、組織の内部のネットワークのようなアクセスが制限された LAN 環境の、どちらの環境でも良い。

TOE の更新用のソフトウェアやファームウェアは、IP ネットワークに接続された遠隔のサーバから配信される。

4.3 運用環境におけるTOE範囲

本 PP に適合する TOE は、各特定用途機器の個別の用途やその運用環境に特有の脅威に対抗したセキュリティ機能を持つ可能性がある。しかし、本 PP はそれらの付加的なセキュリティ機能についての保証を要求していない。

例えば、以下の要件は、本 PP には含まれていない。

・パスワードの推測を防止するためのパスワード文字列の品質の要件

・遠隔サーバの真正性を確認する要件

5 評価機関による評価実施及び結果

5.1 評価機関

評価を実施した「一般社団法人 IT セキュリティセンター　評価部」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、ILAC（国際試験所認定協力機構）の相互承認に加盟している認定機関（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。

5.2 評価方法

評価は、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を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本 PP の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

5.3 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、令和 4 年 2 月に始まり、令和 4 年 6 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。

各ワークユニットの評価作業中に発見された問題点は、すべて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。

5.4 評価結果

評価者は、評価報告書をもって本 PP が CEM のワークユニット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。

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 適合

評価の結果として、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。

APE_INT.1, APE_CCL.1, APE_OBJ.1, APE_ECD.1, APE_REQ.1

5.5 評価者コメント/勧告

本 PP に適合した製品開発を行う開発者及び製品調達者に喚起すべき評価者勧告は、特にない。

6 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、関連するワークユニット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に適合していること。

6.1 認証結果

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 PP が CC パート 3 の保証コンポーネント APE_INT.1, APE_CCL.1, APE_OBJ.1, APE_ECD.1, APE_REQ.1 に対する保証要件を満たすものと判断する。

6.2 注意事項

「1.1.2 免責事項」に記載されているとおり、本 PP で TOE に要求するセキュリティ要件は、特定用途機器に対する基本的な共通要件であり、各特定用途機器の個別の用途やその運用環境に特有の脅威に対しては対抗していない。そのため、本 PP に適合した TOE を調達する調達者は、購入する製品の機能構成を踏まえ情報システムやその運用環境に必要なセキュリティ機能が実装されていることを別途確認する必要があることに注意されたい。

7 附属書

特になし。

8 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）
TOE	Target of Evaluation（評価対象）

本報告書で使用された TOE に関する略語を以下に示す。

IoT	Internet of Things（物のインターネット）
IP	Internet Protocol（インターネットプロトコル）

本報告書で使用された用語の定義を以下に示す。

特定用途機器	ネットワークカメラシステム、テレビ会議システム、IP電話システム、入退管理システム、施設管理システム、及び環境モニタリングシステム等の特定の用途に使用されるシステムにおいて、ネットワークに接続され、記録媒体を内蔵している機器の総称。
政府統一基準	国の行政機関等のサイバーセキュリティに関する対策基準であり、それぞれの府省庁や独立行政法人が情報セキュリティの確保のために採るべき対策やその基準を定めている。
技適セキュリティ基準	「端末設備等規則及び電気通信主任技術者規則の一部を改正する省令（平成31年総務省令第12号）」によりIoT機器の技術基準に追加されたセキュリティ要件。

9 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2年10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2年10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 Part 1: Introduction and general model, Version 3.1 Revision 5, April 2017, CCMB-2017-04-001

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-002

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017, CCMB-2017-04-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-001, (平成29年7月, 翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント, バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-002, (平成29年7月, 翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント, バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-003, (平成29年7月, 翻訳第1.0版)

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

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第5版, 2017年4月, CCMB-2017-04-004 (平成29年7月, 翻訳第1.0版)

[12] 特定用途機器 - 共通セキュリティ　プロテクションプロファイル, 1.0版, 2022年6月15日, 独立行政法人情報処理推進機構, 特定用途機器情報セキュリティ対策検討委員会

[13] 特定用途機器 - 共通セキュリティ　プロテクションプロファイル 評価報告書, 第2.0版, 2022年6月17日, 一般社団法人ITセキュリティセンター　評価部

[14] 政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）, 令和3年7月7日, サイバーセキュリティ戦略本部