JISEC

特定用途機器
共通プロテクションプロファイル

ドラフト版

2019年12月11日

IPA
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

目　　次

改版履歴

版数	発行年月日	備考
ドラフト版	2019 年 12 月 11 日	公募用途限り

1. はじめに

1.1. 概要

本「特定用途機器共通プロテクションプロファイル」（以下「本 PP」と言う。）は、「政府機関等の情報セキュリティ対策のための統一基準」（以下「政府統一基準」と言う。）において IoT 機器を含む特定用途機器（以下「特定用途機器」と言う。）に共通的に求められる情報セキュリティ対策要件集である。調達仕様策定において本 PP のセキュリティ要件を満たす特定用途機器を指定することにより、政府統一基準に準拠した安全な公共サービスの提供を可能とすることができる。

また、本 PP はシステム調達時の仕様として政府統一基準からも参照されるチェックリスト[1]における特定用途機器に共通の必須要件と一致している。製品提供者は、自らの製品がこれらのチェックリストを満たしていることの自主的宣言にとどまらず、本 PP 適合の認証を取得することで、それらの製品がチェックリストの機能要件を満たすことを国際標準に従って客観的に評価されたことを主張することができる。

なお、本バージョンは公募案件「特定用途機器 PP を用いた認証の実効性調査」の参考資料である。本 PP 単独で公開、または利用するものではない。

[1] https://www.ipa.go.jp/security/jisec/choutatsu/
IoT 機器を含む特定用途機器のチェックリスト（2019 年 10 月現在、ネットワークカメラシステム、及び入退管理システムが公開）

1.2. 用語

この章では、本 PP で用いられる用語及びコモンクライテリアに関する用語について解説する。

1.3. 用語集

政府機関等の情報セキュリティ対策のための統一基準（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。

IoT 機器を含む特定用途機器（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とする。

チェックリスト ： IPA が公開している特定用途機器によるシステム毎の機能及び運用の要件集であり、政府や自治体などのシステム調達時のセキュリティ要件として平成 30 年度版の政府統一基準のガイドラインからも参照されている。https://www.ipa.go.jp/security/jisec/choutatsu/

調達者 ： 政府や自治体などの特定用途機器を含むシステム調達を行う担当者のこと。

管理者 ： 特定用途機器を含むシステムを利用する組織において、管理機能にアクセスできる利用者（付属書 A の U.ADMIN）のこと。

IP ネットワーク ： インターネットプロトコル（IP）による通信を行う特定用途機器間の接続のこと。本 PP ではアナログ接続のような IP ネットワーク以外の接続による特定用途機器は対象外としている。

入室制限された部屋 ： サーバルームやデータセンター等、物理的に隔離されており、管理者しか出入り出来ないように管理された部屋のこと。

1.4. コモンクライテリアに関する用語

プロテクションプロファイル（PP) ： 製品分野（本 PP では「特定用途機器」）に対するセキュリティの要求仕様のこと。特定の製品の実装には依存しない形で記載され、その製品分野のシステムや機器調達時に参照される。

セキュリティターゲット（ST） ： PP に準じて、評価対象の製品のセキュリティ機能を具体的に記載したセキュリティ基本仕様書のこと。

TOE ： Target of Evaluation の略で、評価対象の製品のこと。本 PP では政府統一基準における IoT 機器を含む特定用途機器を表す。

資産 ： 漏えいすると問題となるデータのこと。本 PP では付属書 A に記載した D.USR.ASSETS 及び D.TSF.ASSETS が資産となる。

本 PP に登場する利用者や資産の定義は**付属書 A** に記載している。

2. プロテクションプロファイル概説

本 PP を識別する参照と本 PP で対象とする評価対象製品（以下「TOE」と言う。）について概説する。

2.1. PP 参照

PP 名称：	**特定用途機器共通プロテクションプロファイル**
PP バージョン：	1.0 版
PP 識別：	JGPP-IOTBASE-1.0
PP 作成日：	2019 年 12 月 11 日
PP スポンサー：	特定用途機器情報セキュリティ対策検討委員会

2.2. TOE 概要

本 PP の対象となる TOE は、府省庁等の特定の用途に使用される情報システムにおける構成要素として IP ネットワークへの接続や情報の蓄積の機能を持つ機器とし、かつその機器自身は情報セキュリティを目的としたものではない機器(特定用途機器)とする。これらの情報システムの例は、テレビ会議システム、IP 電話システム、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であり、TOE である特定用途機器はネットワークカメラやレコーダーといったサーバやクライアントの機能を持ったシステムを構成する機器となる。

但し、情報システムを構成する特定用途機器の中でも、IP ネットワークに接続されない機器である防犯センサーやアラームなどは本 PP の対象外とする。（図 1 参照）

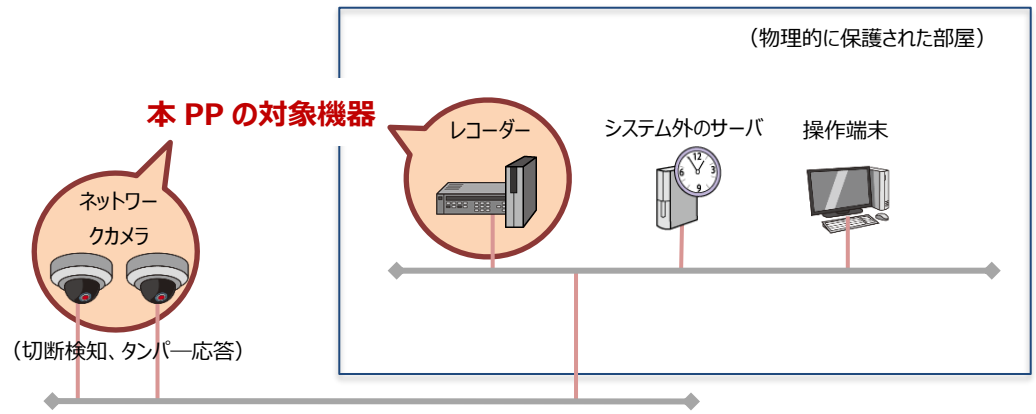


図 1　本 PP の対象機器（ネットワークカメラシステム）

本 PP は統一基準の基本対策事項において特定用途機器に対して求められる共通的な機能要件をまとめたものであり、以下の機能要件を定義している。なお、セキュリティ課題はシステムの適用場面については多岐にわたるため、本 PP は低保証とする。

(1) 初回の管理機能利用前の強制的なパスワード設定機能
(2) 管理者を識別認証する機能。
(3) 情報システムの運用に不要なネットワークサービスを管理者が停止する機能。
(4) ファームウェア／ソフトウェアをアップデートする機能。
(5) 上記の機能へのアクセスを管理者が認知できる監査機能

3. CC 適合

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

- コモンクライテリア v3.1、改訂第 5 版の要件へ適合し
- パート 2 拡張、パート 3 適合であり
- その他のいかなる PP への適合も主張しない。

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

本 PP に適合するためには、TOE は完全適合を論証しなければならない。完全適合は、本 PP の第 6 章のすべての要件を含むセキュリティターゲット（ST）として定義される。繰り返しは許容されているが、いかなる追加の要件(CC パート 2 または 3 からのもの) も ST に含めることは許容されない。さらに、本 PP の第 6 章のいかなる要件も、省略は許されない。

4. セキュリティ対策方針

4.1. 運用環境のセキュリティ対策方針

4.1.1.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る。

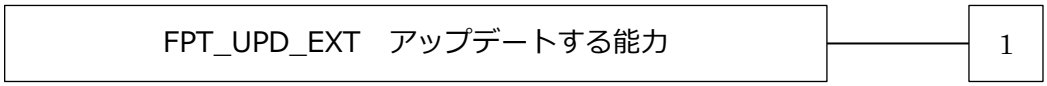
5. 拡張コンポーネント定義

5.1. FPT_UPD_EXT.1　アップデートする能力

ファミリのふるまい

ファミリのコンポーネントは、TOE のファームウェア及び／またはソフトウェアをアップデートするための要件に対処する。

コンポーネントのレベル付け



FPT_UPD_EXT.1 アップデートする能力は、TOE のファームウェア及びソフトウェアをアップデートするために提供される管理機能を要求する。

監査：FPT_UPD_EXT.1

　セキュリティ監査データ生成(FAU_GEN)が PP に含まれていれば、以下のアクションを監査対象にすべきである:

a)　　最小: アップデートの成功と成功したバージョン。

FPT_UPD_EXT.1　アップデートする能力

下位階層：	なし
依存性：	FMT_SMF.1 管理機能の特定 FMT_SMR.1
FPT_UPD_EXT.1.1	TSF は、[割付：許可され識別された役割]に TOE ファームウェア及びソフトウェアの現在実行中のバージョンを通知する能力を提供しなければならない。
FPT_UPD_EXT.1.2	TSF は、[割付：許可され識別された役割]に TOE ファームウェア及びソフトウェアのアップデートを手動で開始する能力及び[選択：アップデートを自動で行う、その他のアップデートメカニズムなし] 能力を提供しなければならない。

5.2. FMT_PWD_EXT.1　ID 及びパスワード管理機能の制限

ファミリのふるまい

ファミリのコンポーネントは、TOE で使用される ID 及びパスワードを管理するために必要とされる機能を定義する。

コンポーネントのレベル付け

FMT_PWD_EXT.1　TSF がユーザー名及びパスワードの管理機能の制限を提供する。

監査：FMT_PWD_EXT.1

a)　　最小:なし

FMT_PWD_EXT.1　ユーザー名及びパスワードの管理

下位階層：　なし

依存性：　FMT_SMF.1 管理機能の特定

FMT_SMR.1

FMT_PWD_EXT.1.1	TSF は、パスワードの変更を[割付：許可され識別された役割]に限定しなければならない。
FMT_PWD_EXT.1.2	TSF は、ユーザー名の変更を[割付：許可され識別された役割]に限定しなければならない。
FMT_PWD_EXT.1.3	TSF は、次の機能を提供しなければならない [選択：設置後初めて起動する時にユーザー名及びパスワードを設定する，設置後初めて起動する時にパスワードを設定する，TOE が設置後初めて許可された管理者を認証する時にユーザー名及びパスワードを変更する，TOE が設置後初めて許可された管理者を認証する時にパスワードを変更する]

6. セキュリティ機能要件

個別のセキュリティ機能要件を以下に定義する。本 PP のセキュリティ機能要件（以下、「SFR」と言う。）は、本 PP の対象となる全ての TOE が満たさなければならない必須 SFR である。

6.1. 表記法

SFRの記述に用いられる表記法は以下のとおり：

- 割付：*イタリック体*で示される；
- PP作成者による詳細化：オリジナルのSFRへの追加は**太字、**SFRからの削除は~~取り消し線~~で示される；
- 選択：下線で示される；
- 選択内の割付：*イタリックと下線*で示される；
- 繰り返し：SFRに、それぞれの繰り返しについて一意の文字を含むような括弧を追加することで示される、例、(a)、(b)、(c) 及び／またはスラッシュ(/) と後に続くSFRの目的についての記述文字列、例、/Server；

太字、*イタリック*、及び下線のSFRテキストは、オリジナルSFRが割付操作を定義したことを示すが、PP作成者はオリジナルSFRの詳細化であると見なされるような、選択操作としてそれを詳細化することによってその割付を完成したことを示す。

選択または割付がST作成者によって完成されるべきである場合、「選択：」または「割付：」で開始される。。

拡張SFR (即ち、CCパート2で定義されていないようなSFR) は、SFR名称の末尾に「_EXT」ラベルを持つことにより特定される。

6.2. SFR アーキテクチャ

本 PP で必須の SFR を以下に列挙する。

表 1：TOE セキュリティ機能要件

機能クラス	機能コンポーネント
セキュリティ監査（FAU）	FAU_GEN.1　監査データ生成
	FAU_SAR.1　監査レビュー
	FAU_STG.1　保護された監査証跡格納
識別と認証（FIA）	FIA_UAU.1　認証のタイミング
	FIA_UID.1　識別のタイミング
セキュリティ管理（FMT）	FMT_MOF.1　セキュリティ機能のふるまいの管理
	FMT_MTD.1　TSF データの管理
	FMT_PWD_EXT.1　管理機能の制限
	FMT_SMF.1　管理機能の特定
	FMT_SMR.1　セキュリティの役割
TSF の保護（FPT）	FPT_STM.1　高信頼タイムスタンプ
	FPT_UPD_EXT.1　アップデートする能力
高信頼パス／チャネル（FTP）	FTP_TRP.1　高信頼パス

6.3. セキュリティ監査(FAU)

6.3.1.FAU_GEN.1　監査データ生成

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

a) 監査機能の起動と終了；

b) 監査の**最小**レベルのすべての監査対象事象；及び

c) 以下から構成されるすべてのアクション：

- 通信断
- ケース開け
- [選択：[その他のアクションなし、割付：*[その他のアクション]*]]；

表 2：最小レベルのすべての監査対象事象

機能コンポーネント	最小レベルの監査
FAU_GEN.1	–
FAU_SAR.1	–
FAU_STG.1	–
FIA_UAU.1	認証メカニズムの不成功になった使用
FIA_UID.1	提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用
FMT_MOF.1	–
FMT_MTD.1	–
FMT_PWD_EXT.1	–
FMT_SMF.1	管理機能の使用
FMT_SMR.1	役割の一部をなす利用者のグループに対する改変
FPT_STM.1	時間の変更
FPT_UPD_EXT.1	アップデートの成功と成功したバージョン
FTP_TRP.1	高信頼パス機能の失敗

6.3.2.FAU_SAR.1 監査レビュー

FAU_SAR.1.1 TSF は、**U.ADMIN** が**すべての記録**を監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

6.3.3.FAU_STG.1 保護された監査証跡格納

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

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を[選択: 防止、検出: から 1 つのみ選択]できなければならない。

6.4. 識別と認証（FIA）

6.4.1.FIA_UAU.1 認証のタイミング

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる[割付 : ***D.TSF.ASSETS* へのアクセスをせず、かつ*D.TSF.OTHER* を変更しない** *TSF 仲介アクションのリスト*]を許可しなければならない。

FIA_UAU.1.2 TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

6.4.2.FIA_UID.1 識別のタイミング

FIA_UID.1.1 TSF は、利用者が識別される前に利用者を代行して実行される[割付 : ***D.TSF.ASSETS* へのアクセスをせず、かつ*D.TSF.OTHER* を変更しない** *TSF 仲介アクションのリスト*]を許可しなければならない。

FIA_UID.1.2 TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.5. セキュリティ管理（FMT）

6.5.1.FMT_MOF.1 セキュリティ機能のふるまいの管理

FMT_MOF.1.1 詳細化： TSF は、**IP ネットワークサーバサービスを停止及び動作させる能力、及び**機能[割付 : *機能のリスト*] [選択 : のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を **U.ADMIN** に制限しなければならない。

6.5.2.FMT_MTD.1　TSF データの管理

FMT_MTD.1.1 TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を U.ADMIN に制限しなければならない。

6.5.3.FMT_PWD_EXT.1　ユーザー名及びパスワード管理機能の制限

FMT_PWD_EXT.1.1 TSF は、パスワードの次の管理機能[割付： *管理機能のリスト*]を[割付：*許可され識別された役割*]に限定しなければならない。

FMT_PWD_EXT.1.2 TSF は、ユーザー名の次の管理機能[割付： *管理機能のリスト*]を[割付：*許可され識別された役割*]に限定しなければならない。

FMT_PWD_EXT.1.3 TSF は、次の機能を提供しなければならない。

[選択：設置後初めて起動する時にユーザー名及びパスワードを設定する, 設置後初めて起動する時にパスワードを設定する,TOE が許可された管理者を設置後初めて認証する時にユーザー名及びパスワードを変更する, TOE が許可された管理者を設置後初めて認証する時にパスワードを変更する: から 1 つのみ選択]

6.5.4.FMT_SMF.1 管理機能の特定

FMT_SMF.1.1 詳細化：TSF は、以下の管理機能を実行できなければならない： **[**

a) 利用者（U.OTHER）の登録及び削除 ;

b) 自身（U.ADMIN）及び U.OTHER のパスワードの変更 ;

c) IP ネットワークサーバサービスの停止と開始 ;

d) ファームウェアのアップデート]。

6.5.5.FMT_SMR.1 セキュリティの役割

FMT_SMR.1.1 TSF は、U.ADMIN を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連付けできなければならない。

6.6. TSF の保護（FPT）

6.6.1.FPT_STM.1 高信頼タイムスタンプ

FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなければならない。

6.6.2.FPT_UPD_EXT.1 アップデートする能力

FPT_UPD_EXT.1.1 TSF は、U.ADMIN に TOE ファームウェア及びソフトウェアの現在実行中のバージョンを問い合わせる能力を提供しなければならない。

FPT_UPD_EXT.1.2 TSF は、**U.ADMIN** に TOE ファームウェア及びソフトウェアのアップデートを手動で開始する能力及び[選択：自動アップデートを有効化及び無効化する、その他のアップデートメカニズムなし] 能力を提供しなければならない。

6.7. 高信頼パス／チャネル（FTP）

6.7.1.FTP_TRP.1 高信頼パス

FTP_TRP.1.1 TSF は、それ自身と**リモート**利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、[選択：改変、暴露、[割付：*ほかのタイプの完全性、または機密性侵害*]]からの通信データの保護を提供する通信パスを提供しなければならない。

FTP_TRP.1.2 TSF は、**リモート利用者**が、高信頼パスを介して通信を開始することを許可しなければならない。

FTP_TRP.1.3 TSF は、[選択: **管理機能**、[割付: *高信頼パスが要求される他のサービス*]]に対して、高信頼パスの使用を要求しなければならない。

7. セキュリティ保証要件

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

本セクションには、本 PP に対する評価で必要とされる、CC パート 3 の SAR 一式が列挙されている。

本 PP に適合するために作成された ST に対する TOE 評価についての一般的なモデルは、以下のとおりである：ST が評価可能と承認された後、評価機関は、TOE、IT 支援環境(必要な場合)、及び TOE のガイダンス文書を入手する。評価機関は、ASE 及び ALC の SAR について情報技術セキュリティ評価のための共通方法(CEM) により義務付けられたアクションを実行することが期待されている。

表 2：セキュリティ保証要件

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

7.1. ASE：セキュリティターゲット

ST は、CEM で定義された ASE アクティビティにより評価される。

7.2. ADV：開発

TOE についての設計情報は、ST の TSS 部分や、最終利用者が利用可能なガイダンス証拠資料にも含まれている。

7.2.1. 基本機能仕様(ADV_FSP.1)

本ファミリの評価アクティビティは追加の「機能仕様」証拠資料は必要としない。TSS に存在する機能要件に対応したインタフェース及び AGD に存在するインタフェースを理解することにフォーカスしている。

7.3. AGD：ガイダンス文書

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

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

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

7.3.1. 利用者操作ガイダンス(AGD_OPE.1)

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

7.3.2. 準備手続き(AGD_PRE.1)

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

7.4. ALC クラス：ライフサイクルサポート

本 PP に適合する TOE に提供される保証レベルでは、ライフサイクルサポートは TOE ベンダの開発及び構成管理プロセスの検査よりもむしろ、ライフサイクルのエンドユーザーから見えるような側面に限定されている。

7.4.1. TOE のラベル付け(ALC_CMC.1)

本コンポーネントは、TOE を同一ベンダの他の製品またはバージョンから区別でき、またエンドユーザーによって調達される際に容易に指定できるように、TOE を識別することを目標としている。ラベルは、「ハードラベル」(特定用途機器への刻印やラベル) または「ソフトラベル」(ネットワークからのアクセス時のレスポンス) からなる。評価者は、ALC_CMC.1 と関連付けられた CEM ワークユニットを実行する。

7.4.2. TOE の CM 範囲(ALC_CMS.1)

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

7.5. ATE：テスト

テストは、システムの機能的な側面、及び設計または実装の弱点を利用するような側面について特定される。前者は、ATE_IND ファミリによって行われるが、後者は AVA_VAN ファミリによって行われる。本 PP では、テストは公表された機能及びインタフェースに基づき、設計情報の利用可能性に依存して行われる。但し運用に不要で管理機能でのみ停止できることを確認済みの IP ネットワークサーバサービスの機能や弱点を確認する必要は無い。評価プロセスの主要なアウトプットの一つは、以下の要件で特定されるテスト報告書である。

7.5.1. 独立テスト―適合(ATE_IND.1)

テストは、TSS とガイダンス文書(「評価される構成」の指示を含む) に記述された機能を確認するために実施される。テストで重視されるのは、6 章で規定されたセキュリティ機能要件が満たされていることを確認することである。評価者は、本 PP への適合を主張するプラットフォーム／TOE の組み合わせにフォーカスしたカバレージ論拠とともに、テストの計画及び結果を文書化したテスト報告書を作成する。

7.6. AVA クラス：脆弱性評定

評価機関は、これらの種類の製品にどのような脆弱性が発見されているかを見つけるために公開情報を調査することが期待され、その内容を AVA_VAN の議論へ提供することが期待される。

7.6.1.脆弱性調査(AVA_VAN.1)

評価機関は、ST、ガイダンス証拠資料、TOE である特定用途機器、及び公開情報源を調査した上で評価者は AVA_VAN.1 に関連する CEM ワークユニットを実行する。追加の証拠資料を必要としてはならない。

公開情報源の探索は TOE、TOE が利用している OS、及びアプリケーションソフトウェアだけではなく、特定用途機器が SFR に利用するサービスから想定されるソフトウェアの脆弱性を含む。

ウェブサーバによる管理機能を提供している TOE であれば、ウェブサーバソフトウェアのバージョンに該当する公知脆弱性に加えて、動的なウェブページに対する公知脆弱性（各種インジェクションやセション管理の不備、パラメータのオーバーフローなど）の確認を行う。

ウェブページは、識別認証後のページや特別な条件でのみアクセスできるページ（初回のみ表示されるパスワードを設定するページや、一般的な単語の探索で検出される隠されたページなど）を含めて巡回し、その中から動的なページのみを評価対象とする。

評価機関は、管理機能により停止できない IP ネットワークへのサービスや、システム運用上停止することができない独自のサービスを確認した場合、そのサービスの通信内容を分析して、SFR の侵害や資産の漏えいが行えないことを確認する。

付属書 A　　利用者と資産の定義

本 PP の利用者や資産の定義は、特定用途機器単位で必要となる最低限の分類に留めている。実際の特定用途機器で構成されたシステムにおいては、以下で定義された利用者以外に、一部の管理機能にアクセス可能な別の利用者が登場する場合があり、チェックリストでは利用者の行動の記録と監視によりそれらの利用者による悪意のある行為を抑止している。本 PP では管理者機能の監視を機能要件として定義することにより、チェックリストのそれらの要件に対応している。

A.1.利用者の定義

本 PP では、2 つの利用者分類を定義する：

名称	分類名	定義
U.ADMIN	管理者	ユーザー名とパスワードにより識別認証され、管理者役割を持つ利用者
U.OTHER	その他の利用者	ユーザー名とパスワードにより識別認証される上記以外の利用者

A.2.資産の定義

本 PP では、2 つの資産を定義する：

名称	分類名	定義
D.USR	利用者データ	TSF に影響を及ぼさないデータ 蓄積された映像データなど
D.TSF	TSF データ	TSF の操作に影響を与えるデータ 管理機能の設定値 利用者の認証情報 監査データなど

A.2.1.利用者データ

D.USR（利用者データ）は 2 つの種類から構成される：

名称	分類名	定義
D.USR.ASSETS	保護すべき利用者データ	漏えいすると問題となる利用者データ 利用者の個人情報や 蓄積された映像データなど
D.USR.OTHER	その他の利用者データ	上記以外の利用者データで漏洩は問題としないが改ざんされると問題となるデータ 公開しているデータ

A.2.2.TSF データ

D.TSF（TSF データ）は 2 つの種類から構成される：

名称	分類名	定義
D.TSF.ASSETS	保護すべき TSF データ	漏えいすると問題となる TSF データ 利用者の認証情報など
D.TSF.OTHER	その他の TSF データ	漏えいしても問題は無いが、改ざんされ、その改ざんを管理者が気づけないと問題となるデータ 監査データなど

付属書 B　　根拠

B.1.SFR 依存性分析

TOE に実装された SFR 間の依存性は以下の通り対処される：

SFR	依存性	根拠記述
FAU_GEN.1	FPT_STM.1	FPT_STM.1 が対応し、依存性が満たされる。
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1 が対応し、依存性が満たされる。
FAU_STG.1	FAU_GEN.1	FAU_GEN.1 が対応し、依存性が満たされる。
FIA_UAU.1	FIA_UID.1	FIA_UID.1 が対応し、依存性が満たされる。
FIA_UID.1	なし	不要
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 及び FMT_SMR.1 が対応し、依存性が満たされる。
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 及び FMT_SMR.1 が対応し、依存性が満たされる
FMT_PWD_EXT.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 及び FMT_SMR.1 が対応し、依存性が満たされる
FMT_SMF.1	なし	不要
FMT_SMR.1	FIA_UID.1	FIA_UID.1 が対応し、依存性が満たされる。
FPT_STM.1	なし	不要
FPT_UPD_EXT.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 及び FMT_SMR.1 が対応し、依存性が満たされる。
FTP_TRP.1	なし	不要