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

2022年6月15日

1.0版

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

【はじめに】

国内の政府機関等が実施すべきセキュリティ対策の指針を示す「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」（以下「政府統一基準」と言う。）では、IoT 機器を含む特定用途機器（以下「特定用途機器」と言う。）について、機器の特性に応じた情報セキュリティ対策を講じることが責任者に求められています。

本「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」（以下「本 PP」と言う。）は、この政府統一基準で求められるセキュリティ対策を講じるにあたり、特定用途機器において必要となる共通の情報セキュリティ要件を、世界主要国の調達で用いられているセキュリティ評価基準コモンクライテリア（以下「CC」と言う。）の形式でまとめたものです。

特定用途機器の調達者は、調達する製品のセキュリティ要求仕様として本 PP のセキュリティ要件を指定することにより、政府統一基準に準拠した安全な機器を調達することができます。また本 PP の情報セキュリティ要件は、IoT 機器の技術基準適合認定で求められるセキュリティ基準（以下「技適セキュリティ基準」と言う。）とも整合しています。

特定用途機器の提供者は、本 PP 適合の認証を取得することで、製品がこれらの基準を満たしていることを、セキュリティ評価の国際標準である CC に従って客観的に評価されたことを調達者や利用者に主張することができます。

なお、本 PP においては特定用途機器全般に具備すべき基本的な共通セキュリティ要件について言及しています。調達する機器の特性や想定する使用環境により、付加的なセキュリティ要件が必要となります。

【用語集】

■用語集

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（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。

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。

電子政府推奨暗号リスト ： CRYPTREC（総務省及び経済産業省共同の暗号評価プロジェクト）によって安全性が認められ、利用が推奨された暗号技術のリスト。各府省庁の情報システム等の調達において参照されている。

調達者 ： 政府や自治体などの特定用途機器及びそれを含むシステムの調達を行う担当者。

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。本 PP ではユーザー名（管理者名を要求しない暗黙的な識別を含む）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と定義する。

設置者 ： 特定用途機器の設置・設定時に、初期管理者パスワードを入力または変更することが想定される管理者認証が実施される前の管理者役割を持つ利用者。

初期状態 ： 出荷時や管理者による TOE リセットなどにより、認証情報が未設定となり管理者認証が未実施の状態。

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。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。

■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「IoT を含む特定用途機器」）に対するセキュリティ要求仕様を、CC の規定に基づき記載したもの。特定の製品の実装には依存しない形で記載され、その製品分野の機器の調達要件として参照される。

セキュリティターゲット（ST） ： 評価対象となる製品のセキュリティ機能仕様を、その製品分野の PP に展開して具体的に記載したセキュリティ基本仕様書。ST は、セキュリティ評価において開発者と評価者の製品セキュリティ事項の共通認識として、評価後は調達者の PP 適合製品選択の理解のために利用される。

TOE ： Target of Evaluation の略で、評価対象のこと。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である。

TSF ： TOE Security Functionality の略で、評価対象(TOE)のセキュリティ機能のこと。

【参考資料】

[政府統一基準] ： 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

[CC パート 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
パート 1：概説と一般モデル 2017 年 4 月 バージョン 3.1 改訂第 5 版
CCMB-2017-04-001

[CC パート 2] ： 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 2017 年 4 月 バージョン 3.1 改訂第 5 版
CCMB-2017-04-002

[CC パート 3] ： 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 2017 年 4 月 バージョン 3.1 改訂第 5 版
CCMB-2017-04-003

[CEM] ： 情報技術セキュリティ評価のための共通方法
評価方法 2017 年 4 月 バージョン 3.1 改訂第 5 版
CCMB-2017-04-004

目　　次

改版履歴

版数	発行年月日	備考
1.0 版	2022 年 6 月 15 日	初版発行

1. プロテクションプロファイル概説

本 PP の識別、本 PP で対象とする製品（以下「TOE」と言う。）について概説する。

1.1. PP 参照

PP 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**
PP バージョン：	1.0 版
PP 識別：	JISEC-C0755
PP 作成日：	2022 年 6 月 15 日
PP 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

1.2. TOE 概要

本 PP の対象となる TOE は、府省庁等で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。[政府統一基準]では、これらの情報システムを、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、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としており、TOE である特定用途機器はこれらを構成するネットワークカメラやレコーダーといったサーバーやクライアントの機能を持つ機器となる（図 1）。

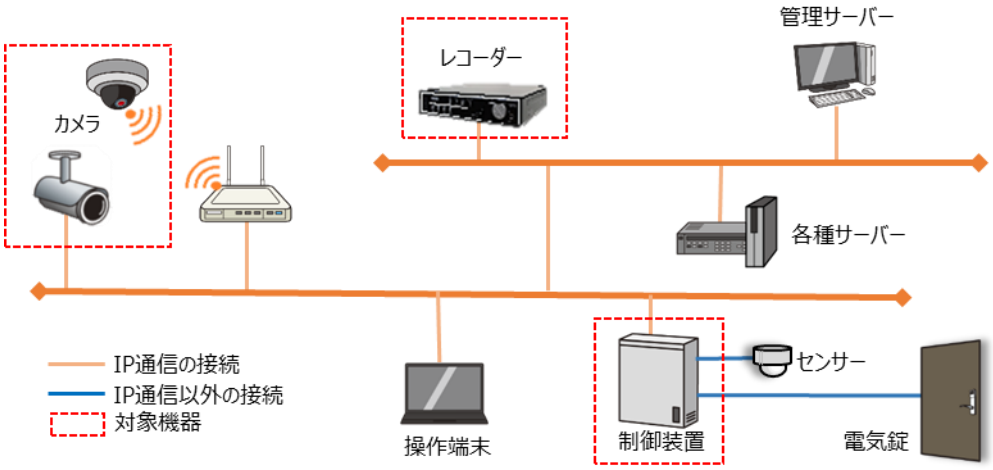


図 1　本 PP の対象機器の例

TOE は、オンライン会議やモニタリング等の特定の用途に使用される情報システムに汎用的な情報処理機器とともに配置される特定の用途のための機器で、カメラやセンサのような IoT 機器を含む市販製品を想定する。それらの機器の用途自体はセキュリティを実現するものではないが、管理機能等を悪用されることで他の情報システムに危害が及ぶ可能性がある。

1.3. 対象とするセキュリティ機能

本 PP では、[政府統一基準]の遵守事項において特定用途機器に対し、また技適セキュリティ基準において IoT 機器に対し求める基本的かつ共通的なセキュリティ機能を対象とし、調達する製品が具備すべきセキュリティ機能要件を以下のとおり定義する。

(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

上記要件は、ネットワークに接続される特定用途機器に対する基本的な共通要件であり、また一般的なセキュリティインシデントの事例を考慮して選択されたものである。本 PP で言及されないセキュリティ機能（例えば、パスワードの強度確保など）を TOE は具備しているであろう。調達者は、想定される使用環境における脅威を特定し、必要に応じて付加的なセキュリティ要件の指定やセキュリティ機能のテストの実施を考えるべきである。

2. 適合主張

2.1. CC 適合主張

本 PP は、CC バージョン 3.1 改訂第 5 版への適合を主張する。

- [CC パート 2]拡張
- [CC パート 3]適合

2.2. PP 及びパッケージ主張

本 PP は、他の PP への適合を主張しない。

2.3. 適合根拠

本 PP は、他の PP 適合を主張しないため、適合根拠はない。

2.4. 適合ステートメント

本 PP への適合を主張するセキュリティターゲット(ST)又は PP は、本 PP に対し論証適合を主張する。つまり ST 作成者は、本 PP で要求するセキュリティ要件の実現において、より制限的な機能実装を以て適合を主張できる。

なお、各セキュリティ要件において、[CEM]のワークユニットに関連する付加的な情報や論証可能なセキュリティ要件の事例について「適用上の注釈」として述べている。さらに保証アクティビティには、本 PP 適合評価のために ST 作成者が提供すべき情報、及び評価者が確認すべき事項が含まれている。

3. セキュリティ対策方針

3.1. 運用環境のセキュリティ対策方針

3.1.1.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、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. 拡張コンポーネント定義

拡張コンポーネントの定義は付属書 A に記載する。

5. 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。

5.1. 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*で示す；
- 選択：下線で示され、選択肢は”,”で区切られる；
- 選択内の割付：*イタリック体と下線*で示す；

PP作成者によるCCパート２又は拡張コンポーネントで定義されたSFR（オリジナルSFR）への追加は**太字**で示し、選択の結果SFRから削除したものは記載しない。選択若しくは割付がST作成者によって完成されるべきである場合、「選択：」若しくは「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。

5.2. 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
	FAU_STG.4　監査データ損失の防止
識別と認証（FIA）	FIA_AFL.1　認証失敗時の取り扱い
	FIA_UAU.1　認証のタイミング
	FIA_UID.2　アクション前の利用者識別
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_IPWD_EXT.1　拡張：初期パスワードの設定
	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_ITI.1　TSF 間改変の検出
	FPT_STM.1　高信頼タイムスタンプ

5.3. セキュリティ監査(FAU)

5.3.1.FAU_GEN.1　監査データ生成

監査：　　なし

依存性：　　FPT_STM.1 高信頼性タイムスタンプ

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) 監査の指定なしレベルのすべての監査対象事象；及び

c) **表 2 の監査対象事象、** [割付：　*左記以外の個別に定義したその他の監査関連情報*]；

適用上の注釈

ST 作成者は、機能要件に規定されている監査項目（表 2 参照）以外に、調達者の要求等に従い機能コンポーネントや監査対象事象を個別に表 2 に追加できる。このような個別の監査対象事象には、常時接続を要する通信（例えば、画像データの送受信、ログやアラートの送受信）を行う機器での通信断がある。また、管理者以外の人間が物理的な接触を行う可能性のある機器（監視カメラや、鍵管理端末）では、いたずら検知やケース開け検知が要求される場合もある。また、セキュリティのふるまいに係る管理アクション（コマンドや設定ファイルの変更）については b)以外についても監査対象事象として含めるか、不要である根拠を ST で述べるべきである。

ST 作成者は、正確な時間がセキュリティ要件に貢献しない場合は依存性 FPT_STM を削除することができる。また、外部環境より適切な時刻の提供がある場合は、この要件が運用環境によって対処され、タイムスタンプの受入れを信頼できるとした根拠を ST で主張するべきである。

保証アクティビティ

操作ガイダンス：

評価者は、特に管理機能における無効化や失敗はセキュリティのふるまいに大きく影響する可能性があるため、必要な管理アクションが監査対象として定義されていることをガイダンスで確認すべきである。

評価者は、ST が運用環境からのタイムスタンプの受入れを信頼できると主張している場合、ガイダンスにおいてそれらの運用環境が明確に記載されていることを確認するべきである。

表 2：機能コンポーネント監査対象事象

機能コンポーネント	監査対象事象	その他の監査関連情報
FAU_GEN.1	–	
FAU_SAR.1	–	
FAU_STG.1	–	

FAU_STG.4	監査格納失敗時にとられるアクション	
FIA_AFL.1	不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション	
FIA_UAU.1	不成功となった認証メカニズムの使用	
FIA_UID.2	提供される利用者識別情報を含む、不成功となった利用者識別メカニズムの使用	
FMT_MOF.1	–	
FMT_MTD.1	TSF データの値の改変	
FMT_IPWD_EXT.1	–	
FMT_SMF.1	特定された管理機能の実施	
FMT_SMR.1	–	
FPT_ITI.1	送信 TSF データの改変の検出	
FPT_STM.1	変更前と変更後の時刻を含む時間の変更	

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報（該当する場合）、事象の結果(成功又は失敗);及び

b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付: *その他の監査関連情報*] 。

適用上の注釈

ST 作成者は、FAU_GEN.1.1 で規定した各監査対象事象に対し、調達者の要求等に従い a)以外の監査情報を表 2 に追加できる。その他の監査関連情報には、FPT_ITI.1 における検出時のアクションなどが含まれる。追加する情報がない場合は「なし」とする。

調達組織のセキュリティ方針等でプライバシー要件を求められた場合、本要件のサブジェクト識別情報について利用者情報の関連付けを組織のプライバシー方針に従い規定する必要があることに注意すべきである。

保証アクティビティ

操作ガイダンス：

評価者は、AGD_OPE の評価とともに、FAU_GEN.1.1 で識別された各監査対象事象及び FAU_GEN.1.2 で規定された各監査情報がガイダンスに記載され、それらのセキュリティ上の意味（管理者がセキュリティインシデントの可能性を判断できる程度の説明）が記されていることを確認すべきである。

テスト：

評価者は、監査対象事象や管理アクションにより実際に監査記録が生成され、それぞれ正しい監査情報がガイダンスの記載の通り記録されていることを、各機能コンポーネントや管理機能のテストを通じて確認すべきである。その際、各監査対象事象及び監査関連情報がどのようにセキュリティ事項に係るかを理解し、その確認に適切なテスト項目を立案すべきである。たとえば監査機能の終了について、明示的・強制的な機能の停止、電源断やリセットなど該当するあらゆるケースを考慮すべきである。同じ機能要件における異なるメカニズムや手法による認証や通信プロトコル、暗号アルゴリズムが使用可能な場合、評価者は監査対象事象の多様性を考慮し、サンプリング時の網羅性に注意すべきである。

格納される監査情報が処理の効率化等の理由によりバイナリ等の可読でない形式である場合、開発者から提供される変換フィルタを用いるか、FAU_SAR のテストとともに事象の記録を確認する。

5.3.2.FAU_SAR.1 監査レビュー

監査：　なし

依存性：　FAU_GEN.1 監査データ生成

FAU_SAR.1.1　TSF は、**管理者**が **FAU_GEN.1 で生成されたすべての記録**を監査記録から読み出せるようにしなければならない。

適用上の注釈

ST 作成者は、監査記録がいくつかの異なる形式や手法により格納されている場合、評価者がすべての記録を読み出すための手段と監査レビュー要件との対応をガイダンス等で結びつけることができる程度の説明を ST に記述すべきである。

本要件は、監査データを管理者が読み出せることを要求しているが、管理者以外のユーザーが監査記録を呼び出すことでセキュリティ上のリスクが発生すると想定される場合、ST 作成者は監査記録への読み出しアクセスを制限するために FAU_SAR.2 を ST に追記することを検討すべきである。

保証アクティビティ

操作ガイダンス：

評価者は、FAU_GEN.1 で生成されたすべての監査記録の読み出し方法と、個々の情報の記録形式がガイダンスに記載されていることを FAU_SAR.1.2 の要件とともに確認すべきである。

テスト：

評価者は、監査記録がいくつかの異なる形式や手法により格納されている場合、記録を読み出すためのすべてのインタフェースやファイルが暗黙的に管理者による読み出しアクセスを禁止されることがないか、他の機能や格納ファイルの属性の管理等を含め確認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。

適用上の注釈

監査記録が、可読かつ各情報の解釈が容易である形式で格納されている場合、本要件は FAU_GEN.1 により満たされていると ST 作成者は主張することができる。

監査にツール等を使用する場合、ST 作成者は FAU_GEN.1 で生成されたすべての監査記録が、どのようなツールを使用し、それらを管理者が使用であることを評価者が確認できる情報を ST に記載すべきである。

大量の情報が記録されるようなケースにおいては、重要な情報が埋没して監査のセキュリティ要件の目的を達成できないと判断したときは、ST 作成者は FAU_SAR.3 を要件として ST で定義することも検討すべきである。

保証アクティビティ

操作ガイダンス：

評価者は、FAU_GEN.1 で生成されたすべての監査記録の読み出し手順と情報について、利用者に解釈可能な説明がガイダンスで提供されていることを確認すべきである。

テスト：

評価者は、監査記録がいくつかの異なる形式や手法により格納されている場合、いくつかの適切なサンプルにより言語やタイムゾーンの設定等の変更によっても正しい形式で情報が利用者に提供されることを確認すべきである。

5.3.3.FAU_STG.1 保護された監査証跡格納

監査：　なし

依存性：　FAU_GEN.1　監査データ生成

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。

適用上の注釈

監査記録の削除について、直接監査証跡を削除する場合や監査用ツールを用いる場合など、多様な手段により不正な削除から保護しなければならない。

基本的に監査記録は形式変更以外の内容に関する変更は必要ないはずであり、監査記録の不正ではない改変というものを ST 作成者は慎重に検討すべきである。

保証アクティビティ

操作ガイダンス：

評価者は、それぞれの監査証跡について削除の方法と許可される操作者が明確にガイダンスに述べられていることを確認すべきである。

テスト：

評価者は、それぞれの監査証跡に対し削除を許可された又は許可されない利用者が操作を行った場合に成功又は失敗することを確認すべきである。特に監査ツールを用いて削除する手段が提供されている場合、監査証跡を直接編集・削除を行うことで、当該要件を逸脱することがないかを確認すべきである。

5.3.4.FAU_STG.4 監査データ損失の防止

監査： 監査格納失敗時にとられるアクション。

依存性： FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[選択：特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止, 最も古くに格納された監査記録への上書き：から 1 つのみ選択]及び[割付：*監査格納失敗時にとられるその他のアクション*]を行わなければならない。

適用上の注釈

監査証跡が満杯になり監査事象を抑止する場合でも、管理者操作が監査対象のため TOE の復旧や監査の確認等の操作ができない状況を起こしてはならない。新しい監査記録を残すために古い監査記録を上書きする場合、必ずしも最小レコード毎に上書きしていかなくてもよいが、上書きする単位（レコード群、日付、ファイル）については、過去の監査記録の維持という観点において極力妥当なものとしなければならない。

その他のアクションの例としては、管理者への通知やアラートの表示などがある。特段のアクションがない場合、割付は「なし」で完了させる。

保証アクティビティ

操作ガイダンス：

評価者は、監査証跡が満杯になった場合のアクションについて、利用者が明確に理解できるようにガイダンスに述べられていることを確認すべきである。たとえば、監査証跡が満杯になった状態で管理できる項目や方法、利用者を識別しているか、古い監査記録を上書きする場合、どこからが新たな記録であるかを認識可能か、監査格納失敗時にとられるすべてアクションが記述されているか等を確認すべきである。

テスト：

評価者は、監査証跡が満杯になった状態で、セキュリティ侵害につながるようなアクションが追跡不能のままなされることがないかという観点でテストを考案すべきである。たとえば、連続した試行による監査記録の生成により、TOE の動作停止や監査記録の上書きが仕様通りとなるか、監査格納失敗時における監査データのアクセス権が維持されるかを確認すべきである。

評価者は、古い監査記録が上書きされる場合、最も古い監査記録を上書きしているか、どこからが新たな記録であるかを認識できるかをすべての監査記録で確認すべきである。

5.4. 識別と認証（FIA）

5.4.1.FIA_AFL.1 認証失敗時の取り扱い

監査： 不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション。

依存性： FIA_UAU.1 認証のタイミング

FIA_AFL.1.1 TSF は、[割付：*認証事象のリスト*]に関して、[選択：[割付：*正の整数値*], [割付：*許容可能な値の範囲*]内における管理者設定可能な正の整数値]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2 不成功の認証試行が定義した回数[選択：に達する, を上回った]とき、TSF は、[割付：*アクションのリスト*]をしなければならない。

適用上の注釈

不成功の試行回数は時間的経過や再ログインなどリセットされる条件を明確にすべきである。閾値とその到達後のアクションは、認証事象毎に想定される攻撃に対抗し得ることを前提とし決定すべきである。その上で調達者のセキュリティ方針があれば、その方針を満たす値が設定可能である

必要がある。

アクションの例としては、該当する認証アカウントの一定時間無効化や管理者へのアラート通知などがある。また、管理者のアカウントをアクションにより無効とした場合、それ自体が攻撃の手段とならないよう、ロックの解除を含めた対応方法を管理者に提供すべきである。

保証アクティビティ

操作ガイダンス：

評価者は、不成功認証試行回数の累計やリセットの条件、閾値の管理及びアクションの管理（制限された事項の解除等）について、管理者が理解し管理可能である程度の詳細がガイダンス文書に記述されていることを確認すべきである。

テスト：

評価者は、連続したブルートフォース攻撃だけでなく、再ログインや製品のリセットを跨いだ試行により、不成功認証試行の閾値を超えた場合の仕様とテスト結果の整合を確認する。またその時の監査情報がふるまいを正確に記録していることも確認すべきである。

同一アカウントに対する異なるセッションやインタフェースでの誤ったパスワードによる試行の累計や異なるモダリティによる誤った認証の試行が、ガイダンスで規定された通りに不成功認証回数としてカウントされるか確認すべきである。同様に、同一アカウントによる異なるセッション等における認証試行の成功が、他の認証試行の状態に影響を与えないことも確認する。

5.4.2.FIA_UAU.1 認証のタイミング

監査： 不成功となった認証メカニズムの使用。

依存性： FIA_UID.1 識別のタイミング

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 **FMT_IPWD_EXT.1.1 を実現するアクション**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。

適用上の注釈

本要件及び FIA_UID.2.1 の TSF 仲介アクションとは、利用者の認証又は識別が完了する前に実施可能なセキュリティに係る機能であり、アクセス制御方針や TSF データに対し影響を与える操作等である。本 PP では[CC パート 2]に例示しているヘルプ表示のような一般的な機能を仲介アクションとは考えない。

FIA_UAU.1.1 では、製品導入時における初期管理者パスワードの設定を仲介アクションとして

許容する。これは運用に先駆けた設置・設定が安全な環境で行われることを想定している。この仲介アクションには、推測不能な初期管理者パスワードを提供するが、それらの変更を伴わない場合も含まれる。FIA_UAU.1.2 では、アップデート機能のようなセキュリティ上影響のある管理機能が必ず管理者の認証を経て実施されることを要求する。

本要件に関する監査において、未加工の認証情報（パスワード等）は不成功な場合であっても原則監査情報の対象としてはならない。

保証アクティビティ

操作ガイダンス：

評価者は、ガイダンス文書を確認し、利用者が認証されていない状態や認証を不要とするような不特定多数が使用できる（いわゆる”guest”）アカウントで実施可能となるセキュリティに影響を与えるような機能が明記されていないこと確認すること。

認証情報の秘密の品質尺度（パスワード強度等）について、本 PP では具体的な要件を求めていない。しかし評価者は、パスワードの文字数や文字種の他、文字列の複雑性や過去設定されたパスワードとの類似性など許容すべきパスワードの方針がガイダンスに明示されていることを確認すべきである。

テスト：

評価者は、利用者認証前に実施可能なアクションがガイダンスや実機等で識別された場合、それらのアクションによって TSF データやその他のセキュリティ方針に影響を及ぼさないアクションであることを確認すべきである。

評価者は、試行する認証情報のバリエーションを十分吟味すべきである。たとえば、不正なパスワードの例として、許可されていない文字種を用いた場合のふるまい、許可されたパスワード長付近でのパスワード設定や認証の実施など、確認すべき条件を明確にし、テストで代表的なパタンを網羅すべきである。

5.4.3.FIA_UID.2 アクション前の利用者識別

監査：　提供される利用者識別情報を含む、不成功となった利用者識別メカニズムの使用。

依存性：　なし

FIA_UID.2.1 TSF は、その利用者を代行する他の 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。

適用上の注釈

本要件は、利用者がセキュリティに係る仲介アクションを実施する場合、必ずその利用者が識別されていることである。

一般的に、攻撃者のヒントとなり得る情報の提供を制限するために、識別の失敗については認証

の試行完了後に認証の失敗と区別せずに利用者に伝える。監査記録に識別の失敗が認証試行に先駆けてあるいは認証の失敗とは別に記録すべき場合、ST 作成者は攻撃者による監査記録への読み出しアクセスを制限するために FAU_SAR.2 を ST に追記すべきである。

5.5. セキュリティ管理（FMT）

5.5.1.FMT_MOF.1 セキュリティ機能のふるまいの管理

監査： なし

依存性： FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MOF.1.1 TSF は、**TOE アップデート及び IP ネットワークサービス**を停止する, を動作させる能力を**管理者**に制限しなければならない。

適用上の注釈

本要件では、管理者のみが該当する管理機能を操作できることを要求する。FMT_SMF.1 で特定した管理機能の項目ごとに管理者が実施できる管理事項を規定する。ST 作成者は、調達者の要求により一般利用者に対するセキュリティ機能の管理を規定する必要があれば、要件の繰り返しを用いて追加することができる。

保証アクティビティ

操作ガイダンス：

評価者は、ガイダンス文書を確認し管理機能について操作方法が記述されていることを確認しなければならない。

テスト：

評価者は、管理者以外が当該管理機能の当該操作をすることが許可されていないことを確認すべきである。これらのテストは FMT_SMF.1 のテストと一緒に実施されるだろう。

5.5.2.FMT_MTD.1 TSF データの管理

監査： TSF データの値の改変。

依存性： FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 TSF は、**表３で特定した「TSF データ」**を表**３で特定した「操作」**する能力を**管理者**に制限しなければならない。

表３：TSF データの操作

TSF データ	操作	関連する機能コンポーネント
管理者パスワード	改変、削除（初期化）	FIA_UAU.1
時間	改変	FPT_STM.1

適用上の注釈

本要件では、管理者のみが識別された TSF データに特定された操作ができることを要求する。FMT_MTD.1.1 は、表 3 に示されている TSF データのリストについて、個別に管理者に制限する操作を規定する。ST 作成者は、調達者の要求等により表 3 を拡張し対象データや操作を記載してもよい。また、管理者以外の役割の操作を規定する必要があれば、要件の繰り返しを用いて追加することができる。

保証アクティビティ

操作ガイダンス：

評価者は、ガイダンス文書を確認し TSF データについて操作許可者や操作方法が記述されていることを確認しなければならない。

テスト：

評価者は、管理者以外が当該 TSF データの当該操作をすることが許可されていないことを確認すべきである。これらのテストは FMT_SMF.1 のテストと一緒に実施されるだろう。

5.5.3.FMT_IPWD_EXT.1 拡張：初期パスワードの設定

監査：　なし

依存性：　FMT_SMR.1　セキュリティの役割

FMT_SMF.1　管理機能の特定

FMT_IPWD_EXT.1.1 TSF は、TOE の管理者パスワードが初期状態で起動された場合、初期管理者パスワードについて[選択：[割付：*推測不能なパスワードを提供*], **設置者**による設定又は初期値変更を実施]しなければならない。

適用上の注釈

推測が可能な初期パスワードとは、機器個体に関わらず出荷時に一律に設定されたパスワードや、外部から獲得できる機器のプロファイルや出荷情報（時期や工場）に基づき設定されたパスワードなどである。推測不能なパスワードとは、例えば、機器の個体固有（一意でなくとも統計的に十分な分散を持つ）に付けられ、かつ出荷情報や固体番号などとの関連がないあるいは容易に推測されないパスワードである。

本要件は、出荷時に安易な初期パスワードが設定され、使用されることを防止するものであり、ブルートフォース攻撃に対抗するパスワードの強度（長さや文字種、組合わせの複雑さ等）は本要

件の範囲ではない。ST 作成者は、調達組織のセキュリティ方針等で強度を求められる場合は、秘密の品質尺度の検証のために FIA_SOS.1 を ST に追記すべきである。また、本 PP では、一般利用者が管理機能を操作することを想定していないが、一般利用者に対する初期パスワードの設定を規定する必要があれば、FMT_IPWD_EXT.1.1 に変えて FMT_IPWD_EXT.2.1 を要件として定義することができる。

保証アクティビティ

操作ガイダンス：

評価者は、ガイダンス文書を確認し、出荷時以外にパスワードが初期化される状況や手順が明記されているかを確認すること。

テスト：

評価者は、初期パスワードが提供される場合、開発者に初期パスワードと出荷情報等との関連を確認し、懸念があれば複数の出荷品を入手しそれらパスワードの相関について観察したりすべきである。これらの初期パスワードに関連性があると、製品が一括購入された場合、セキュリティ方針の異なる他部署が初期パスワードを知り得ることになる。

また、ガイダンスで識別された明示的なパスワード初期化の他にも、TOE のリセット時や電源断からの復帰などでパスワードが未設定となり得るパタンや初期パスワードが再設定される条件についても本要件が満たされることを確認すべきである。

5.5.4.FMT_SMF.1 管理機能の特定

監査： 特定された管理機能の実施。

依存性： なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない： **[**

1. **TOE アップデート ;**
2. **IP ネットワークサービス;**
3. **安全な初期パスワードの設定・提供 ;**
4. **表 3 に示した TSF データ管理機能]。**

適用上の注釈

本 PP が対象とする TOE はインターネットにつながっており、そのような状態で脆弱性が放置されることを防ぐため、１．では TOE のファームウェア及びソフトウェアのアップデートを管理機能として要求する。アップデートは管理者により明示的にあるいは TOE により自動的に開始されてもよいが、有効化されたアップデート機能を管理者以外が無効化できてはならない（FMT_MOF）。管理者が適切なタイミングでアップデートの実施を判断できるように指針を示す

ことは開発者の責任であり、アップデート適用の可否の判断は管理者の責任である。

また２．では、管理者がインターネットに対しオープンとなっているサービスポートを認識し管理できることを要求する。すべてのサービスを対象とすることが望ましいが、システム運用上停止することのできないサービスなどについては、本機能の対象外とすることができる。いずれの場合も評価において、独自サービスを含め脆弱性評定の対象とする。

ST 作成者は、TSF により提供される管理機能（セキュリティ属性管理、TSF データ管理、またはセキュリティ機能管理）を本 PP に追記し識別する。たとえば、監査格納失敗時や認証試行の閾値を超えての失敗時などにとられるアクションがいくつか規定され管理すべきであれば、FAU_STG.4 や FIA_AFL.1 の管理機能として特定すべきである。

保証アクティビティ

操作ガイダンス：

評価者は、ガイダンス文書を確認し管理機能について操作方法が記述されていることを確認しなければならない。

テスト：

新製品におけるアップデートの実施は、実際の顧客への配信準備が整っていない等の理由により困難な場合がある。評価者は、すくなくともガイダンス文書に示された手順に従って管理機能を実施できることは確認すべきである。

ここで識別されていない機能について、TSF に影響を与える操作や設定がないことは脆弱性評定での確認事項となる。

5.5.5.FMT_SMR.1 セキュリティの役割

監査：　　なし

依存性：　　FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、**管理者**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なければならない。

適用上の注釈

管理者のみを役割として特定しているが、セキュリティに関する役割が細分化されている場合（管理者と監査者の分離など）においても詳細化として本要件を満たすことができる。

5.6. TSF の保護（FPT）

5.6.1.FPT_ITI.1　TSF 間改変の検出

監査：　　送信 TSF データの改変の検出。

依存性：　　なし

FPT_ITI.1.1 TSF は、以下の尺度の範囲で、TSF と他の高信頼 IT 製品間で送出中のすべての TSF データの改変を検出する能力を提供しなければならない。: [割付: *定義された改変尺度*]

FPT_ITI.1.2 TSF は、TSF と他の高信頼 IT 製品間で送られるすべての TSF データの完全性を検証し、かつ改変が検出された場合には[割付：*とられるアクション*]を実行する能力を提供しなければならない。

適用上の注釈

本 PP で想定する主な「TSF データ」は TOE のアップデート用データ、「他の高信頼 IT 製品」はそのデータを送信する遠隔の管理されたサーバーである。また、「定義された改変尺度」は、改変を検出する際に使用するたとえばハッシュアルゴリズム等の強度である。改変検出のアルゴリズムにおいて暗号・電子署名のアルゴリズムを利用する場合、可能な限り「**電子政府推奨暗号リスト**」に記載されたアルゴリズムを使用する。

「とられるアクション」の例としては、改変を検出したアップデートデータの破棄などがある。この場合、アップデートの失敗を管理者に通知する又はアップデートデータの再送を要求するなどのアクションを伴うべきである。

保証アクティビティ

操作ガイダンス：

評価者は、「他の高信頼 IT 製品」から送信される TSF データの改変を検出し何らかのアクション（TSF データの破棄など）を行った場合、管理者が対処すべき事項あればそれらがガイダンス文書に記載されていることを確認する。

テスト：

評価者は、TSF データの送信相手である「他の高信頼 IT 製品」について実際にどのサイトやサーバーとコネクションを確立しているかを検証すべきである。特に高信頼 IT 製品に関して管理者による管理項目がない（つまり相手側情報がハードコーディングされている）場合、送信相手の特定についてどのような仕組みであるかを含め確認すべきである。

TSF データの改変を検出した際の TOE のふるまいを確認する際、ガイダンスの通り監査が記録されていること、管理者の対処が必要な場合はガイダンスに従い的確に対処できるかも確認すべきである。

5.6.2.FPT_STM.1 高信頼タイムスタンプ

監査： 変更前と変更後の時刻情報を含む時間の変更。

依存性： なし

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。

適用上の注釈

タイムスタンプは TOE 自身あるいは外部環境が提供してもよいが、[CC パート 2]にあるように「信頼できるタイムスタンプ」の意味及びどのように信頼に足ることを決定するかについて ST 作成者は明確にする必要がある。タイムスタンプは、たとえば世界時（UTC）とどれだけ厳密に同期する必要があるのか、システム系内での同期や経過時間を重視するのかなど信頼の意味を明確にする。また調達者に、たとえば世界時と同期する場合どのような NTP サーバーを用い、時刻の同期や確認についてどのように運用で担保すべきかなどをガイダンス文書等で理解させなければならない。

保証アクティビティ

操作ガイダンス：

管理者等が時刻の管理が必要な場合、評価者はガイダンス文書を確認し、その手順は無理がなくかつ明確に記載されていることを確認すべきである。

テスト：

評価者は、時刻の管理がガイダンス文書に記載されている場合、その手順に従って確実に実施できることを確認すべきである。外部環境から時刻が提供される場合は、意図しない入力やネットワーク遮断による時刻の変更が起こらないか、ネットワークや管理端末などいかなる入力経路を時刻情報が経由しても、時刻の変更は監査記録として残されるかを確認すべきである。

6. セキュリティ保証要件

本 PP への適合に必要なセキュリティ保証要件を表 4 に示す。これらの保証要件は[CC パート 3]の保証レベル EAL1 に相当する。

表 4：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評価（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)
	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)

表 4 に示された保証コンポーネントについて、評価機関は開発者から提供された TOE 及び関連する証拠資料を[CEM]に記述された保証コンポーネント用のワークユニットに基づいて評価し、合否を判定する。

ただし、本 PP では、[CEM]のワークユニットに、次節以降に記述する「適用上の注釈」を追加して適用する。本 PP の「適用上の注釈」に記述がない場合には、[CEM]のワークユニットがそのまま適用される。

本 PP への適合評価のために、開発者が評価機関に提供しなければならないものを以下に示す。

- 本 PP の要件を満足する ST
- 本 PP の要件を満足する TOE
- TOE 付属のガイダンス文書
- 基本機能仕様

「基本機能仕様」とは、ガイダンス文書とともに評価者のテストや脆弱性評定の項目作成のための入力となるセキュリティ機能のインタフェース（TSF インタフェース）を識別した仕様を記載したものをいう。本 PP の対象は、セキュリティ機能自体を他に提供するものではないため、評価者テスト等に必要とされるセキュリティ機能要件を実現する基本仕様は ST の TOE 要約仕様に示されており、インタフェー

スも管理者向けのガイダンス文書に記述されていることを想定する。開発において使用された機能仕様書を評価に提供することで、開発者にとって付加的な作業を軽減できるのであればそれも望ましい。ただし、評価のために（開発に使用されない）新たな資料を作成することは避けるべきである。セキュリティ機能のインタフェースやパラメタを識別できる基本仕様がどのような形にも文書化されてない場合は、セキュアな開発がなされていない可能性があるため本評価の対象とはならない。

通常 TOE のテスト環境やテストツールは評価機関にて準備するが、特殊な環境やツールを要する場合は評価機関からテスト環境構築支援を依頼されることがある。

6.1. ASE：セキュリティターゲット評価

適用上の注釈

開発者アクションエレメント：

本 PP は低保証のため厳密な根拠や正当化を必要としないが、開発者は基本機能仕様レベルで評価の指針が明確となる記述を提供しなければならない。

評価者アクションエレメント：

評価者は、ST において PP から追加・拡張された箇所について評価作業を集中することで、より効果的な作業が可能となるであろう。

6.2. ADV：開発

6.2.1. 基本機能仕様(ADV_FSP.1)

適用上の注釈

開発者アクションエレメント：

開発者が評価に提示する機能仕様としては、TOE のガイダンス文書を使用する。そのため ST の TOE 要約仕様には、セキュリティ機能要件がどのように実現されているかを具体的なコマンドや設定など評価者がガイダンス文書とのリンク付けが可能な程度に記述しなければならない。

ガイダンス文書には、管理コマンドのパラメタや電源入力ボタン、ネットワークを介しての制御データなどのセキュリティ機能に関するインタフェースが述べられている必要がある。セキュリティ事項にもかかわらず、機能仕様やインタフェースを記載していない場合、それらが評価対象となるセキュリティ機能に関与しない根拠を開発者は示す必要がある。

評価者アクションエレメント：

基本機能について、評価者は ST の TOE 要約仕様に示されたセキュリティ機能性の側面に焦点を当て、すべてのインタフェースの完全な仕様を求めるべきではない。本保証アクティビティの多くは、個々の機能要件のテストにおいて確認されるであろう。評価者は、TOE 要約仕様の基本機能の記述やガイダンス文書におけるインタフェースの識別が不十分で理解できない場合、開発資料を別途要求できるが SFR 実施及び SFR 支援、SFR 非干渉についての分離を文書化することは求めず、既存の開発証拠資料による説明を求めるべきである。

6.3. AGD：ガイダンス文書

6.3.1.利用者操作ガイダンス（AGD_OPE.1）

適用上の注釈

開発者アクションエレメント：

ガイダンス文書は、評価者による各セキュリティ機能要件の基本仕様の理解と評価者テストへの入力となる。開発者は、ガイダンス文書が本 PP のセキュリティ機能要件の保証アクティビティ実施に十分な情報を含むことを保証しなければならない。

評価者アクションエレメント：

評価者は、各セキュリティ機能要件の保証アクティビティを通じてガイダンス文書の情報を確認しているであろう。さらに、本 PP でセキュリティ管理の対象となっているアップデートや IP ネットワークサービス、機能コンポーネントの管理について手順が完全で正確であることを確認しなければならない。

6.3.2.準備手続き（AGD_PRE.1）

適用上の注釈

開発者アクションエレメント：

開発者は、ガイダンス文書が ST に述べられたすべての運用環境における設置・設定及びセキュリティ管理の説明を含んでいることを保証しなければならない。

評価者アクションエレメント：

評価者は、ガイダンス文書がアップデートサイトの設定や初期に立ち上がる IP ネットワークサービス、管理者パスワードの設定など、安全な運用環境準備のための手続きの説明を含み、それらが適用可能であることを確認しなければならない。

6.4. ALC クラス：ライフサイクルサポート

6.4.1. TOE のラベル付け(ALC_CMC.1)

適用上の注釈

開発者アクションエレメント：

開発者は、評価対象である製品と他のバージョンや類似製品と区別できる情報を利用者に提供しなければならない。それらは、製品自身の識別やガイダンス文書での記述、または利用者に向けた情報発信サイトなどがある。

評価者アクションエレメント：

評価者は、ST に記載されている TOE の識別が、ガイダンス文書やテスト用に入手した製品における識別（製品名称やバージョン番号等）に示されていることを確認する。また、利用者が参照する可能性のあるウェブ等に掲載されている製品情報についても、ST の情報と整合しており TOE を識別可能な状態

であることを確認すべきである。

6.4.2. TOE の CM 範囲(ALC_CMS.1)

適用上の注釈

本コンポーネントの目的は、開発過程において構成要素が管理されていることの保証である。しかし、本 PP の保証レベルでは、最終生産物である TOE とそのガイダンス文書の識別を確認する。また、これらは TOE やガイダンス文書の評価者テストへの適切な入力であることの識別となる。

開発者アクションエレメント：

開発者は、評価対象である製品及びガイダンス文書を識別する構成リストを維持していなければならない。また、製品パッケージに同梱リストがある場合、そこに記載された TOE とそのガイダンス文書の識別が構成リストと相違がないことを開発者は保証する。

評価者アクションエレメント：

評価者は、構成リストの内容が TOE やガイダンス文書及び ST 自身の識別の他、ST やガイダンス文書で言及されているそれぞれの識別と矛盾がないことを確認しなければならない。

6.5. ATE：テスト

6.5.1.独立テスト―適合(ATE_IND.1)

適用上の注釈

評価者アクションエレメント：

評価者は、テストのための環境やツールを使用する場合、それらがセキュリティ機能性に影響を与えないことをテスト報告書で論証しなければならない。特にそれらが開発者等から提供された場合には、客観性の観点から開発者の主張をそのまま受け入れるべきではない。

テスト結果が期待された結果と異なる場合、評価者はその要因を分析すべきである。その情報は、修正された TOE に対する同テストの再実施のみならず、他の機能要件に対する同様の観点でのテストの考慮や脆弱性評定における入力となり得る。

6.6. AVA クラス：脆弱性評定

6.6.1.脆弱性調査(AVA_VAN.1)

適用上の注釈

評価者アクションエレメント：

ここでは基本的な攻撃能力を持つ攻撃者に悪用される脆弱性を持つかを評定するが、非常に高度な攻撃ツールを必要とする攻撃であっても、そのツールが公知の場で攻撃者が入手可能であれば検査の対象となる。

また、攻撃の手法は主に公知の情報に基づくが、例えばプロトコルが非公開であることが、必ずしも基本的な攻撃能力に耐えうることの根拠にならないことに評価者は留意すべきである。
評価者が探索すべき公知の情報としては下記のようなものを含む：

- 一般的なウェブアプリケーションに関する脆弱性・攻撃手法の情報
- 一般的なウェルノウンポートや Bluetooth のサービスに関する脆弱性・攻撃手法の情報
- 製品独自の通信プロトコルの仕様・脆弱性の情報
- 類似製品に関する脆弱性情報のデータベースや検索サービス
- ベンダーサイトの製品サポート情報。

侵入テストの考案には、セッション管理の不備に起因するウェブページ移行時の認証スキップや動作している IP サービス・Bluetooth の脆弱性対応の確認のような公知の脆弱性に基づくものや、使用されている複数モダリティによる同時認証や負荷を与えながらの試行のように製品の仕様に依存するものなど、特殊なツールや専門的なスキル、膨大な資源などを必要としない基本的な攻撃能力で考え得るあらゆる攻撃手法を考慮すべきである。
評価者は、その脆弱性は潜在するが TOE の運用環境において顕在化しないと判断した場合、その理由を報告書に記載する。また、想定される攻撃者レベル（基本的な攻撃能力）においては顕在化しない潜在的脆弱性については、必要であれば侵入テストを実施し、残存脆弱性として報告書に記載する。

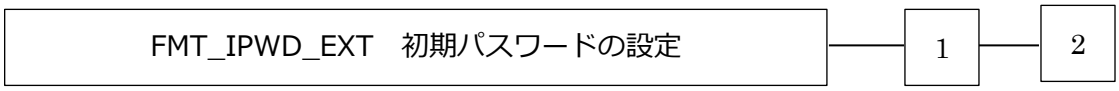
付属書 A　　拡張：コンポーネント定義

A.1. FMT_IPWD_EXT　拡張：初期パスワードの設定

ファミリのふるまい

このファミリは、TOE 設置時や初期化時に安易な初期パスワードが使用されないことを保証するため、初期パスワードの設定についての要件を定義する。

コンポーネントのレベル付け



FMT_IPWD_EXT.1　TSF は、管理機能のアクセスに必要な初期管理者パスワードについて、推測不能値を提供又は設置者による設定や提供値の変更を促すことを要求する。

FMT_IPWD_EXT.2　TSF は、利用者が TSF のアクセスに必要なすべての初期パスワードについて、推測不能値を提供又は利用者自身による設定や提供値の変更を促すことを要求する。

管理：FMT_IPWD_EXT.1、FMT_IPWD_EXT.2

予見される管理アクティビティはない。

監査：FMT_IPWD_EXT.1、FMT_IPWD_EXT.2

予見される監査対象事象はない。

FMT_IPWD_EXT.1　初期管理者パスワードの設定

下位階層：	なし
依存性：	FMT_SMF.1 管理機能の特定
	FMT_SMR.1 セキュリティの役割
FMT_IPWD_EXT.1.1	TSF は、TOE の管理者パスワードが初期状態で起動された場合、初期管理者パスワードについて[選択：[割付：*推測不能なパスワードを提供*], [割付：*許可された役割による設定又は変更*]を実施]しなければならない。

FMT_IPWD_EXT.2　初期利用者パスワードの設定

下位階層：	FMT_IPWD_EXT.1
依存性：	FMT_SMF.1 管理機能の特定
	FMT_SMR.1 セキュリティの役割

FMT_IPWD_EXT.2.1　TSF は、TOE の利用者パスワードが初期状態で起動された場合、すべての初期利用者パスワードについて[選択：[割付：*推測不能なパスワードを提供*], [割付：*許可された識別された役割による設定又は変更*]を実施]しなければならない。

根拠：

パスワードの初期値は、その後のパスワードによる TOE 保護を確実にするものである。コモンクライテリアでは、パスワード初期値設定に適した SFR を提供していない。本拡張コンポーネントは、セキュリティ属性や TSF データの管理であり、FMT クラスのコンポーネントとする。

付属書 B　　根拠

B.1. セキュリティ機能要件依存性分析

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。
FAU_STG.4	FAU_STG.1	FAU_STG.1 が対応し、依存性が満たされる。
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1 が対応し、依存性が満たされる。
FIA_UAU.1	FIA_UID.1	上位階層 FIA_UID.2 が対応し、依存性が満たされる。
FIA_UID.2	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_IPWD_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	上位階層 FIA_UID.2 が対応し、依存性が満たされる。
FPT_ITI.1	なし	不要
FPT_STM.1	なし	不要

B.2. セキュリティ保証要件根拠

保証要件は[CC パート 3]の EAL1 に相当する。本 PP の対象となる TOE は、TOE 概要で述べたように管理されたシステムの構成要素として設置されることを想定されており、TOE 自身がセキュリティを目的としていない。そのため、TOE は基本的な SFR を満たせば十分であり、セキュリティ対策方針を通じて脅威や前提条件から SFR を派生する必要はない。