DeviceProtector AE Version 2.5

セキュリティターゲット

バージョン: 1.12

2009 年 02 月 06 日

NEC ソフト株式会社

更新履歴

バージョン	変更概要	変更箇所		変更日	変更者
		章・節・項	内容		
1.00	初版		新規作成	2008/05/29	NEC ソフト(株)
1.01	全体見直し	全章		2008/06/13	NEC ソフト(株)
1.02	TOE 物理的範囲を変更	1.4.2 章	TOE 物理的範囲に OS 機能を含めるように変更。	2008/06/18	NEC ソフト(株)
1.03	脅威と対策を変更	全章	脅威およびセキュリティ対策を変更。 全章を見直し。	2008/07/18	NEC ソフト(株)
1.04	セキュリティ要件および概要を変更	全章	脅威およびセキュリティ対策を見直し、セキュリティ要件および TOE 要約仕様を修正。	2008/07/30	NEC ソフト(株)
1.05	全体見直し	全章	全体の文章を見直し、間違った表現を修正した。	2008/08/19	NEC ソフト(株)
1,06	SFR の見直し	6 章、7 章	FIA_ATD.1 および FIA_USB.1 を削除。文章を見直し修正した。	2008/09/01	NEC ソフト(株)
1.07	脅威とセキュリティ機能を変更	全章	脅威を詳細化し、セキュリティ機能に管理者パスワード変更機能を追加。全体の文章を見直し、修正した。	2008/10/02	NEC ソフト(株)
1.08	文章の修正	1章、4章	1章および4章の文章を見直し、修正した。	2008/10/16	NEC ソフト(株)
1.09	文章の修正	1章	1.3.1 TOE 種別の文章を見直し、修正した。	2008/12/16	NEC ソフト(株)
1.10	文章の修正	1章	1.4.2.5 ガイダンスにリリースノートの記述を追加。	2009/01/16	NEC ソフト(株)
1.11	前提条件見直し	3 章	前提条件の表現を見直し、修正した。	2009/01/22	NEC ソフト(株)
1.12	セキュリティ課題定義部分の記述修正	1 章、3 章、4 章	1 章、3 章及び 4 章の文章を見直し、修正した。	2009/02/06	NEC ソフト(株)

目次

参考資料

本 ST における参考資料は、以下の通りである

・Common Criteria for Information Technology Security Evaluation Part1:
Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001

・Common Criteria for Information Technology Security Evaluation Part2:
Security functional components September 2007 Version 3.1 Revision 2 CCMB-2007-09-002

・Common Criteria for Information Technology Security Evaluation Part3:
Security assurance components September 2007 Version 3.1 Revision 2 CCMB-2007-09-003

・Common Methodology for Information Technology Security Evaluation:
Evaluation Methodology September 2007 Version 3.1 Revision 2 CCMB-2007-09-004

・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 2006 年 9 月バージョン 3.1 改訂第 1 版 CCMB-2006-09-001
平成 19 年 3 月翻訳第 1.2 版
独立行政法人 情報処理推進機構セキュリティセンター 情報セキュリティ認証室

・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 2007年 9 月バージョン 3.1 改訂第2版 CCMB-2007-09-002
平成 20 年 3 月翻訳第 2.0 版
独立行政法人 情報処理推進機構セキュリティセンター情報セキュリティ認証室

・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 2007 年 9 月バージョン 3.1 改訂第2版 CCMB-2007-09-003
平成 20 年 3 月翻訳第 2.0 版
独立行政法人 情報処理推進機構セキュリティセンター 情報セキュリティ認証室

・情報技術セキュリティ評価のための共通方法
評価方法 2007 年 9 月 バージョン 3.1 改訂第2版 CCMB-2007-09-004
平成 20 年 3 月翻訳第 2.0 版
独立行政法人 情報処理推進機構セキュリティセンター 情報セキュリティ認証室

用語

本STで使用している用語・略語の意味を、表 1 用語集に示す。

表 1 用語集

用語・略語	定義内容
デバイス	端末に搭載された装置、および接続された周辺装置。
管理者用設定ツール	デバイス使用制限設定、各パスワードの変更などを行うことができるツール。管理者のみが利用することができる。
TOE ポリシー	各デバイスの使用制限（有効/無効/ReadOnly）設定情報。
有効/無効	デバイスの使用制限のパラメータ。 有効:デバイスの使用制限なし。 無効:デバイスを使用不可にする。
ReadOnly	デバイスの使用制限のパラメータ。デバイスに対し、読み込みのみを許可し、書き出しを禁止する。
管理者パスワード	管理者を識別するためのパスワード。
ロック解除用パスワード	スクリーンセーバーを解除する時に利用するパスワード。
使用許可リスト	使用することが許可されたデバイスの情報。
Class Installers	.NET Framework におけるカスタム インストーラすべての基本クラス。アプリケーションのインストールを支援するコンポーネント。
デバイス一時解放用キーデバイス	USB 機器および IDE 機器に対し、一時的に有効にするためのデバイス。指定されたデバイスが端末に接続されている間は、USB 機器および IDE 機器を有効にする。
ユーザ・モードセットアップモジュール	ユーザ・モードで実行されるインストール用の実行プログラム。

1. ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、TOE 記述について記述する。

1.1. ST 参照

ST の識別情報は、以下の通りである。

ST タイトル: DeviceProtector AE Version 2.5 セキュリティターゲット
ST バージョン: 1.12
ST 発行日: 2009 年 02 月 06 日
ST 作成者: NEC ソフト株式会社

1.2. TOE 参照

TOE の識別情報は、以下の通りである。

TOE 名称: DeviceProtector AE
TOE バージョン: Version 2.5
TOE 開発者: NEC ソフト株式会社

1.3. TOE 概要

本節では、TOE の概要について、TOE 種別、TOE の使用方法と主要なセキュリティ機能、TOE 以外のハードウェア/ソフトウェア/ファームウェアについて記述する。

1.3.1. TOE 種別

TOE は、「DeviceProtector AE Version2.5」というソフトウェア製品である。「DeviceProtector AE Version 2.5」は、端末に接続されている各デバイスの使用を制限して、USB キー等のデバイスによる情報の不正持ち出しを防止する機能を提供する。
TOEは、デバイスによる情報の不正持ち出しを防止するために、各デバイスに対する設定情報を保護する。
TOE の主要なセキュリティ機能は「1.3.2 TOEの使用方法と主要なセキュリティ機能」に示す通り、各デバイスに対する設定情報を保護する機能である。

1.3.2. TOE の使用方法と主要なセキュリティ機能

TOE の使用方法は、以下の通りである。
TOE は、端末毎に各デバイスの使用許可、読込みのみ許可の制御を行うことにより、制限した USB 機器、DVD 装置等の各デバイスのルートでの情報漏えいを防止する。
TOE が制御対象とするデバイスは、USB 機器、IDE 機器、PC カード、シリアル／パラレル機器、フロッピーディスクドライブ、CD/DVD ドライブ、赤外線通信機器である。
TOE を利用するには、対象となる端末に TOE をインストールし、各デバイスに対して、無効/有効/ReadOnly の使用制限をデバイス毎に設定する。
TOEは、各デバイスに対する設定情報を以下で記述するセキュリティ機能により保護する。
TOE の主要なセキュリティ機能は、以下の通りである。

- 管理者認証機能
  TOE は、管理者パスワードにより、管理者の識別認証を行う。
- 管理者パスワード変更機能

TOE は、管理者パスワードの変更機能を提供する。

・ 管理者パスワード保護機能
TOE は、管理者パスワードを暗号化し、改ざんされたかどうかの検出を行う。

・ TOE ポリシー保護機能
TOE は、TOE ポリシーが改ざんされたどうかの検出を行う。

1.3.3. TOE 以外のハードウェア/ファームウェア/ソフトウェア

TOE が必要とする TOE 以外のハードウェア/ソフトウェア/ファームウェアを、以下に記述する。

1.3.3.1. 必要なハードウェア

TOEの動作に必要なハードウェア構成を、表 2に示す。
TOEは、表 2を満たす動作環境で、正しく確実に動作する。ただし、RAIDコントローラが搭載されているパソコン、NEC製以外のAHCIコントローラが搭載されているパソコン、および、WindowsがCドライブ以外にインストールされているパソコンでは、TOEを使用することができない。

表 2 ハードウェア構成

端末・装置名		種別	説明
端末			
	本体	CPU	32bit（x86）プロセッサ 800MHz 以上の CPU を搭載した PC/AT 互換機
		メモリ	512MB 以上
		HDD	50MB 以上の空き容量

1.3.3.2. 必要なソフトウェア

TOEの動作に必要なソフトウェアの構成を、表 3に示す。TOEは、表 3に識別されたソフトウェア構成によって、正しく確実に動作する

表 3 ソフトウェア構成

端末名			
	ベンダ名	製品名	備考
端末			
	Microsoft 社	Microsoft Windows XP Professional operating system 日本語版（Service Pack 2）、 または Microsoft Windows XP Home Edition operating system 日本語版(Service Pack 2)	オペレーティングシステム

1.4. TOE 記述

本節では、TOE 機能の詳細説明として、TOE 関連の役割定義、TOE の物理的範囲、TOE の論理的範囲、TOE 保護資産、TOE のサブジェクトとオブジェクト、TOE サービス機能とセキュリティ機能について記述する。

1.4.1. TOE 関連の役割定義

TOEに関連する役割定義を、表 4に示す。

表 4 TOE 関連の役割定義一覧

役割	内容
利用者	利用者は、TOE のデバイス使用制限機能により、持ち出し等の制限された環境で業務を行う人物である。 尚、OS の管理者権限は持たせない。
管理者	管理者は、OS の管理者権限を有し、管理者用設定ツールを使用して TOE の運用管理を行う人物である。

1.4.2. TOE の物理的範囲

TOE の物理的範囲(ネットワーク、コンポーネント)、ハードウェア構成、ソフトウェア構成を、以下に記述する。

1.4.2.1. TOE の物理的範囲(ネットワーク)

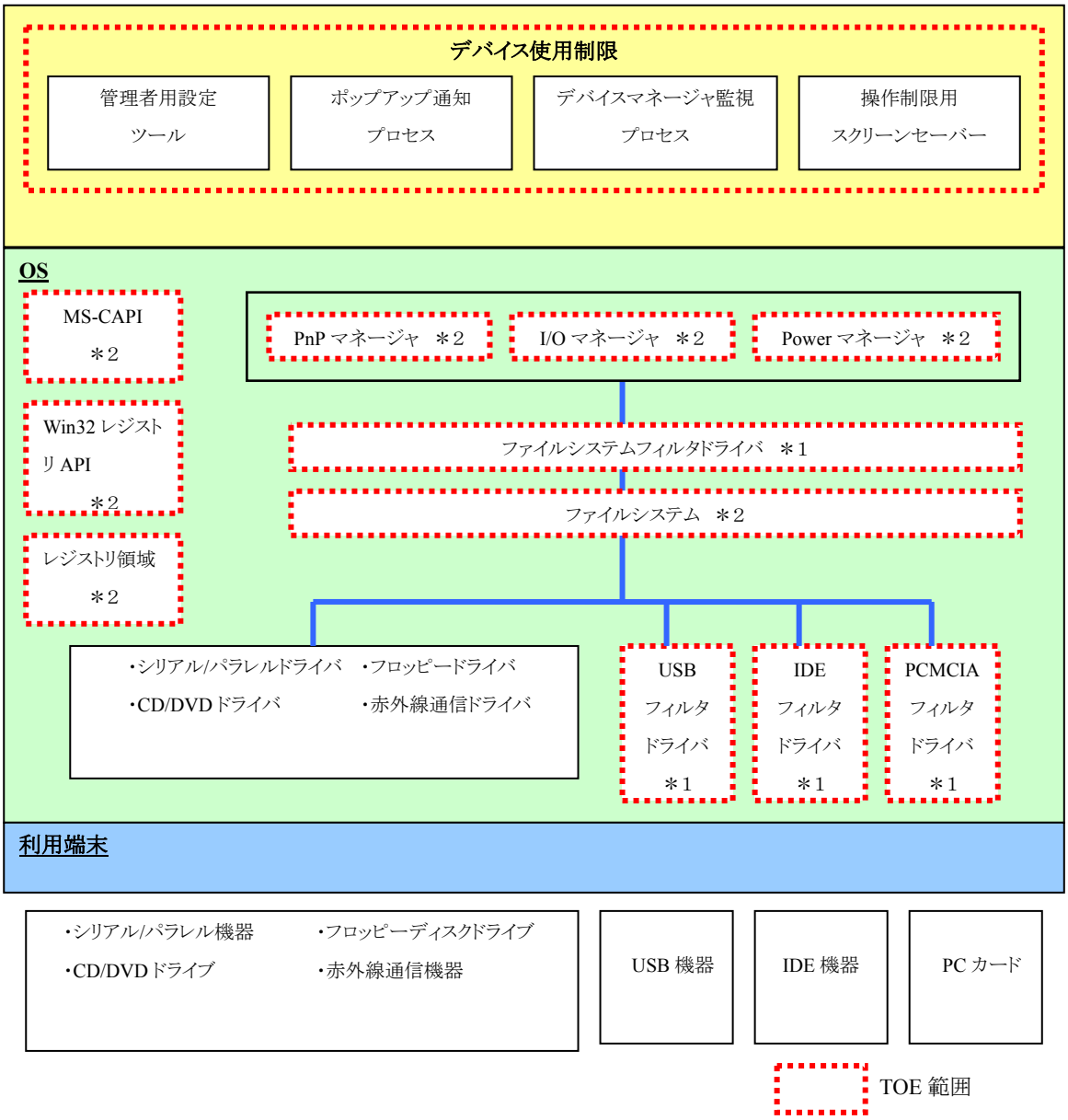
TOE は端末内で動作するため、特にネットワークを構成する必要はない。

1.4.2.2. ハードウェア構成

TOE は、ソフトウェアであるため、ハードウェアを含まない。

1.4.2.3. TOE の物理的範囲(コンポーネント)

TOEが動作するために必要となるコンポーネントの構成は、以下の図 1の通りである。



*1　TOE の OS 組み込みモジュール
*2　OS 標準モジュール

図 1　TOE の物理的範囲

TOE を稼動させ、利用するためには、OS が必要となる。
TOE が使用制限の対象とするデバイスは、USB 機器、IDE 機器、シリアル／パラレル機器、PC カード、フロッピーディスクドライブ、CD/DVD ドライブ、赤外線通信機器である。

(1)管理者用設定ツール
以下の機能を持つ管理者用のツール。
・デバイス設定機能
TOE ポリシーであるデバイスの有効・無効の設定、および ReadOnly の設定を行う。
USB、および IDE に関してはデバイスの個別登録などの詳細な設定ができる。

・管理者パスワード設定機能
管理者パスワードの変更ができる。
・ロック解除用パスワード設定機能
ロック解除用パスワードの変更ができる。

(2)ポップアップ通知プロセス
フィルタドライバからの通知を受け取り、各種メッセージを表示する機能を持つ。

(3)デバイスマネージャ監視プロセス
デバイス、プロセスの状態の監視を行なうサービスで以下の機能を持つ。
・デバイスの状態監視機能
図1の USB、IDE、PC カード以外のデバイスの有効・無効の状態を監視する。TOE ポリシーの設定と異なることを検出すると、スクリーンセーバーを起動する。
・USB フィルタドライバの状態監視機能
USB フィルタドライバの稼動状態を監視する。USB フィルタドライバからエラーの通知を受け取った場合、スクリーンセーバーを起動する。
・IDE フィルタドライバの状態監視機能
IDE フィルタドライバの稼動状態を監視する。IDE フィルタドライバからエラーの通知を受け取った場合、スクリーンセーバーを起動する。
・PCMCIA フィルタドライバの状態監視機能
PCMCIA フィルタドライバの稼動状態を監視する。PCMCIA フィルタドライバからエラーの通知を受け取った場合、スクリーンセーバーを起動する。
・ポップアップ通知プロセスの状態監視機能
ポップアップ通知プロセスの起動状態を監視し、不在の場合スクリーンセーバーを起動する。
・ファイルシステムフィルタドライバへの各状態通知
上記の監視においてエラーの通知を受け取った場合、ファイルシステムフィルタドライバにエラーを通知する。
・ロック解除用キーデバイスの状態監視機能
ロック解除用キーデバイスの接続状況を監視する。キーデバイス接続時はスクリーンセーバーを解除する。
・デバイス一時解放用キーデバイスの状態監視機能
デバイス一時解放用キーデバイスの接続状況を監視する。キーデバイス接続時は USB と IDE の設定を有効にし、切断時は USB と IDE の設定を TOE ポリシーの設定に戻す。

(4)操作制限用スクリーンセーバー
デバイスマネージャ監視プロセス、各フィルタドライバから起動されるスクリーンセーバー。

(5)ファイルシステムフィルタドライバ
ドライブへの書込みを制御するドライバで以下の機能を持つ。
・ReadOnly 時の書込み禁止機能
ReadOnly 時のドライブへのデータの書き出しをブロックする。

(6)USB フィルタドライバ
USB デバイス制御を行なうドライバで以下の機能を持つ。
・デバイス情報の取得機能(プロダクト ID、ベンダ ID、シリアルナンバーなど)

これらの情報をもとに、使用許可リストとの比較を行なう。

・使用許可リスト登録済デバイスの選別機能
デバイスから取得した情報と使用許可リストで比較を行い、リストに登録されていれば、そのまま OS へ開示する。リストに登録されていないデバイスは、OS から隠蔽する。

・デバイス情報取得用 API 機能
管理者用設定ツールが接続しているデバイスやリストに登録しているデバイスの情報を表示するために用いられる。

・使用許可リスト設定用 API 機能
管理者用設定ツールが使用許可リストへデバイスを登録するために用いられる。

・ストレージデバイスの ReadOnly 機能
ストレージデバイスについて、デバイスからの読込みは可能だが、デバイスへの書き出しをブロックする。

・ロック解除用キーデバイス識別機能
スクリーンセーバー解除用のキーとなるデバイスを選別する。

・デバイス一時解放機能用キーデバイス識別機能
デバイス一時解放機能のキーとなるデバイスを選別する。

(7)IDE フィルタドライバ

IDE デバイス制御を行なうドライバで以下の機能を持つ。

・デバイス情報の取得機能(ハードウェア ID、シリアルナンバーなど)
これらの情報をもとに、使用許可リストとの比較を行なう。

・使用許可リスト登録済デバイスの選別機能
デバイスから取得した情報と使用許可リストで比較を行い、リストに登録されていれば、そのまま OS へ開示する。リストに登録されていないデバイスは、OS から隠蔽する。また C ドライブが存在する物理ディスクは常に OS へ開示する。

・デバイス情報取得用 API 機能
管理者用設定ツールが接続しているデバイスやリストに登録しているデバイスの情報を表示するために用いられる。

・使用許可リスト設定用 API 機能
管理者用設定ツールが使用許可リストへデバイスを登録するために用いられる。

・ストレージデバイスの ReadOnly 機能
ストレージデバイスについて、デバイスからの読込みは可能だが、デバイスへの書き出しをブロックする。

(8)PCMCIA フィルタドライバ

PCMCIA デバイス制御を行うドライバで以下の機能を持つ。

・デバイスの有効・無効を制御する。

(9)PnP マネージャ

カーネルモード PnP マネージャは、オペレーティングシステムのモジュールやドライバと連携して、デバイスの構成、管理、維持を行う。

ユーザ・モード PnP マネージャは、ユーザ・モードセットアップモジュールや、Class Installers などと連携して、デバイスの構成、インストールを行う。

また、登録されたアプリケーションに対して、デバイスの状態が変化したこと通知します。

(10)Power マネージャ

パワーマネージャはシステム全体の電源ポリシーを管理しており、システムを通してデバイスなどの電源管理も行う。

(11)IO マネージャ

IO マネージャは最下層、中間層、およびファイルシステムを含む、全てのカーネルモードドライバに、入出力のための統一したインタフェースを提供する。

IO マネージャは、IO システムサービスを提供する。IO システムサービスを使用することにより、ユーザ・モードからのリクエストをドライバ向けに IRP というリクエストに変更し、最終的にデバイスへ通知する。

(12)ファイルシステム

ファイルの一元管理機能と，個々のファイルに対する操作の一貫性を保障する機能を提供する。

(13)MS-CAPI

Windows が提供する暗号化ライブラリ。

(14)Win32 レジストリ API

レジストリ情報をアクセスするための Windows API。

(15)レジストリ領域

Windows が提供するレジストリ領域、TOE はレジストリ領域に TOE ポリシーを保存する。

1.4.2.4. ソフトウェア構成

TOEを構成するコンポーネントのソフトウェア構成を、表 5に示す。TOEは、表 5に識別されたソフトウェアによって、正しく確実に動作する

表 5 ソフトウェア構成

端末名		
ベンダ名	コンポーネント名	備考
端末		
NEC ソフト株式会社	管理者用設定ツール	DPTool.exe
NEC ソフト株式会社	ポップアップ通知プロセス	DPServ.exe
NEC ソフト株式会社	デバイスマネージャ監視プロセス	DPServ1.exe
NEC ソフト株式会社	操作制限用スクリーンセーバー	DPScr.scr
NEC ソフト株式会社	ファイルシステムフィルタドライバ	Hdrfs.sys
NEC ソフト株式会社	IDE フィルタドライバ	DPidefil.sys
NEC ソフト株式会社	USB フィルタドライバ	DPfilter.sys
NEC ソフト株式会社	PCMCIA フィルタドライバ	DPpcmfilter.sys
MicroSoft	MS-CAPI	
MicroSoft	Win32 レジストリ API	
MicroSoft	PnP マネージャ	
MicroSoft	I/O マネージャ	

端末名			
	ベンダ名	コンポーネント名	備考
	MicroSoft	Power マネージャ	
	MicroSoft	ファイルシステム	

1.4.2.5. ガイダンス

TOE のガイダンスは、以下の通りである。

・DeviceProtector AE Version 2.5 インストールガイド V1.00

・DeviceProtector AE Version 2.5 管理者ガイド V1.00

・DeviceProtector AE Version 2.5.0.0 リリースノート（WindowsXP 用）

1.4.3. TOE の論理的範囲

TOEの論理的範囲は、以下の図 2の通りである。

TOE は、各デバイスの設定機能、ロック解除用パスワード変更機能を有する管理者用設定ツールを提供する。

TOE はセキュリティ機能として、管理者認証機能、管理者パスワード変更機能、管理者パスワード保護機能、TOE ポリシー保護機能を提供する。

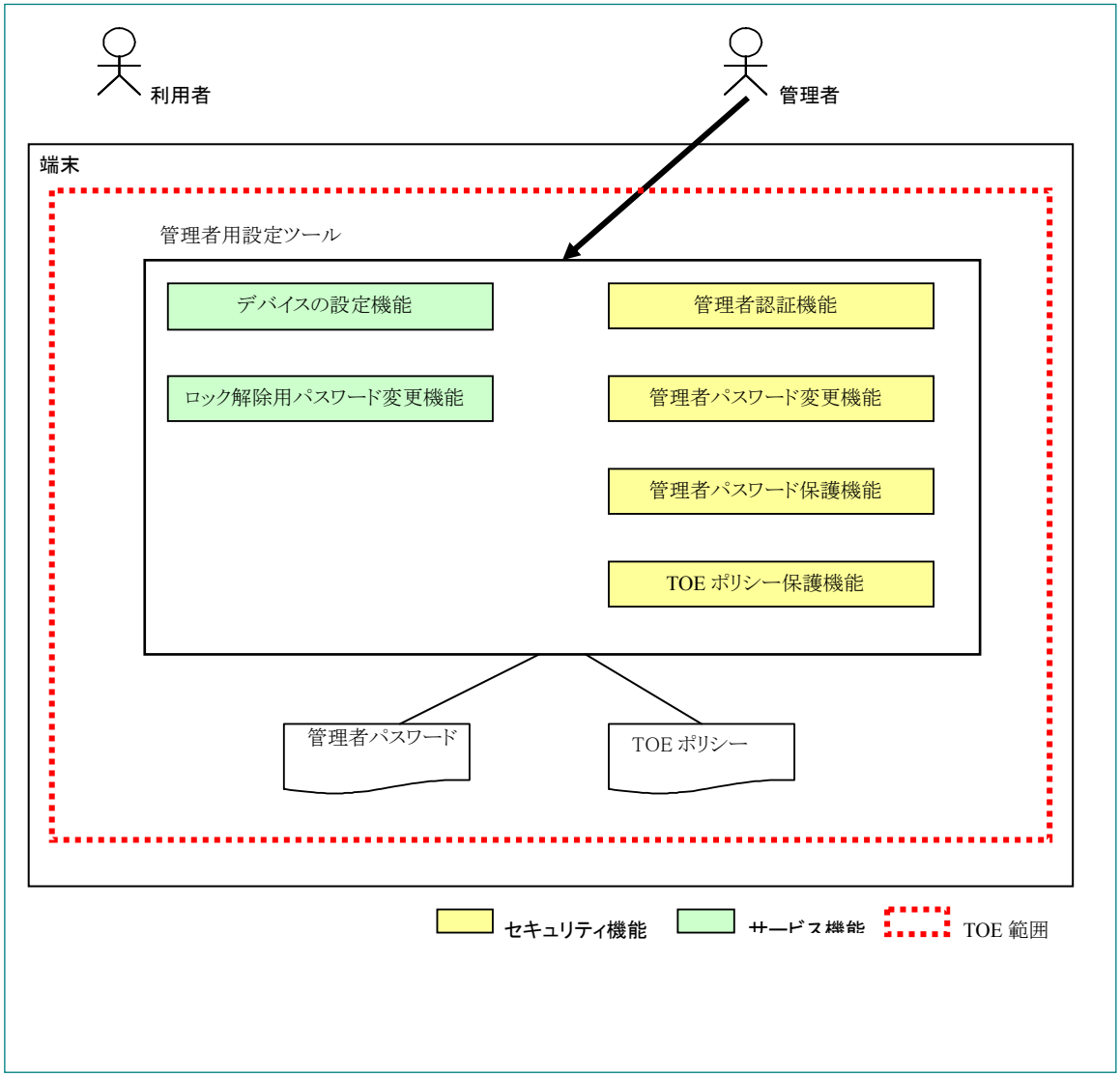


図 2 TOE の論理範囲

1.4.4. TOE 保護資産

TOE は、各デバイスに対する設定情報を定義した TOE ポリシーが改竄されることで、禁止されたデバイスが利用され、情報が不正に持ち出されることを防止することを目的としており、以下の利用者データを保護資産とする。

表 6 利用者データ一覧

データ名	内容
TOE ポリシー	各デバイスの使用制限を設定した情報。

1.4.5. TOE サービス機能とセキュリティ機能

TOE は、以下の機能を有する管理者用設定ツールを提供する。

- デバイスの設定機能

TOE が制御するデバイスに対し、TOE ポリシーである有効/無効/ReadOnly などの使用制限を設定する機能である。

TOE が制御対象とするデバイスは、USB 機器、IDE 機器、シリアル／パラレル機器、PC カード、フロッピーディスクドライブ、CD/DVD ドライブ、赤外線通信機器である。

また、シリアル／パラレル機器、PC カード、フロッピーディスクドライブ、CD/DVD ドライブ、赤外線通信機器の場合、OS 標準付属の対応するデバイスマネージャの状態を指定された使用制限に対応して、有効または無効に設定する。

- ロック解除用パスワード変更機能
  ロック解除用パスワードを変更する機能。

TOE が提供するセキュリティ機能を、以下に記述する。

- 管理者認証機能
  TOE は、管理者パスワードにより、管理者の識別認証を行う。
- 管理者パスワード変更機能
  TOE は、管理者パスワードの変更機能を提供する。
- 管理者パスワード保護機能
  TOE は、管理者パスワードを暗号化し、改ざんされたかどうかの検出を行う。
- TOE ポリシー保護機能
  TOE は、TOE ポリシーが改ざんされたどうかの検出を行う。

2. 適合主張

本章では、CC 適合主張、PP 主張、パッケージ主張、適合主張根拠について記述する。

2.1. CC 適合主張

本 ST は、以下の通り、CC 適合を主張する。
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 2006 年 9 月 バージョン 3.1 改訂第 1 版 翻訳第 1.2 版
・パート 2: セキュリティ機能コンポーネント 2007 年 9 月 バージョン 3.1 改訂第2版 翻訳第 2.0 版
・パート 3: セキュリティ保証コンポーネント 2007 年 9 月 バージョン 3.1 改訂第2版 翻訳第 2.0 版
CC パート 2 適合性:CC パート 2 適合
CC パート 3 適合性:CC パート 3 適合

2.2. PP 主張

本 ST が適合している PP はない。

2.3. パッケージ主張

本 ST は、パッケージ EAL1 追加である。
追加コンポーネントは ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 である。

2.4. 適合主張根拠

本 ST は、PP 適合を主張しないため、PP 適合根拠はない。

3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、前提条件について記述する。

3.1. 脅威

TOE に対する脅威を以下に記述する。
T.MODIFY_POLICY_DATA(ポリシーファイルの変更)
TOE の利用者が、端末に格納されている TOE ポリシーを直接変更しようとするかもしれない。

3.2. 組織のセキュリティ方針

TOE の運用環境、または TOE に適用する組織のセキュリティ方針を以下に記述する。
P.ADMIN_AUTHORITY(管理者認証)
TOE は、管理者用設定ツールの利用を管理者のみに制限し、管理者パスワードの変更を識別認証された管理者のみに制限しなければならない。また、一定の品質を満たす管理者パスワードのみ登録を許可し、認証試行回数を制限しなければならない。

P.PASSWORD_POLICY(管理者パスワードのポリシー)
TOE の管理者は、管理者パスワードを設定し他人に知られないように管理する。管理者は、推測されにくい管理者パスワードを設定して適切な頻度(6ヶ月以内)で変更する。

P.PASSWORD_PROTECTION(管理者パスワードの保護)
TOE は、端末に保存する管理者パスワードを秘匿し、改ざんを検出しなければならない。

3.3. 前提条件

本節では、TOE 運用環境の物理的セキュリティ、人的セキュリティ、TOE 利用環境に関する前提条件について記述する。

3.3.1. 物理的セキュリティに関する前提条件

物理的セキュリティに関する前提条件を以下に記述する。
「なし」

3.3.2. 人的セキュリティに関する前提条件

人的セキュリティに関する前提条件を以下に記述する。
A.ADMIN(信頼できる管理者)
TOE の管理者は、TOE の運用管理を適切に行える者であり、悪意ある行為を行わない。

3.3.3. TOE 利用環境における前提条件

TOE 利用環境における前提条件を以下に記述する。
A.OSADMIN_AUTH(管理者権限)
OS の管理者権限は、管理者のみに与え、利用者は限定ユーザで、運用させる。

4. セキュリティ対策方針

本章では、TOE 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、セキュリティ対策方針根拠について記述する。

4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を以下に記述する。

O.ADMIN_AUTHORITY(管理者権限)
TOE は、管理者の識別認証を行い、管理者用設定ツールの利用を管理者のみに制限しなければならない。

O.PASSWORD_AUTHORITY(管理者パスワード変更権限)
TOE は、管理者パスワードの変更を識別認証した管理者に制限しなければならない。

O.PASSWORD_POLICY(管理者パスワードのポリシー)
TOE は、管理者パスワードに対し、以下のポリシーを実現しなければならない。

- パスワード品質
  8文字より短い、全て同一文字、英字のみ、および数字のみのパスワードは登録させない。
- 認証試行回数制限
  管理者パスワードの認証の認証試行回数を3回に制限し、認証不成功回数が3回に達したときは管理者用設定ツールを10分間使用禁止にしなければならない。

O.PASSWORD_PROTECTION(管理者パスワードの保護)
TOE は、端末に格納される管理者パスワードを秘匿し、改ざんを検出することで、管理者パスワードが暴露または改ざんされないように保護しなければならない。

O.POLICY_PROTECTION(TOE ポリシーの保護)
TOE は、端末に格納された TOE ポリシーの改ざんを検出し、端末に格納される TOE ポリシーが改ざんされないように保護しなければならない。

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を以下に記述する。

OE.PASSWORD_MANAGEMENT(パスワードの管理)
TOE の管理者は、管理者パスワードを記憶し、他人に漏らしてはならない。また、推測されにくいパスワードを設定し、適切な頻度（6ヶ月以内）で変更しなければならない。

OE.TRUSTED_ROLE（信頼される役割）
TOE を利用する職場または現場におけるセキュリティに関する権限、および責任を有する者。または、権限を委任でき、管理業務を代行させることができる者を TOE の管理者に選定しなければならない。

OE.OS_AUTHORITY（OS の権限）
Windows の管理者権限を管理者のみに与え、利用者は制限ユーザで運用させなければならい。

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とセキュリティ課題定義との関係、セキュリティ対策方針の正当性について以下に記述する。

4.3.1. セキュリティ対策方針とセキュリティ課題定義との関係

セキュリティ対策方針とセキュリティ課題定義(脅威、組織のセキュリティ方針、前提条件)の対応関係を、表 8に示す。表中の「×」は、対応関係を示している。

表 7 セキュリティ対策方針とセキュリティ課題定義対応表

	T.MODIFY_POLICY_DATA	P.ADMIN_AUTHORITY	P.PASSWORD_POLICY	P.PASSWORD_PROTECTION	A.ADMIN	A. OSADMIN_AUTH
O.ADMIN_AUTHORITY		×				
O.PASSWORD_AUTHORITY		×				
O.PASSWORD_POLICY		×				
O.PASSWORD_PROTECTION				×		
O.POLICY_PROTECTION	×					
OE.PASSWORD_MANAGEMENT			×			
OE.TRUSTED_ROLE					×	
OE.OS_AUTHORITY						×

表 8により、各セキュリティ対策方針は一つ以上の脅威、組織のセキュリティ方針、前提条件に対応している。

4.3.2. セキュリティ対策方針の正当性

各セキュリティ課題に対するセキュリティ対策方針の根拠を記述する。

4.3.2.1. 脅威に対するセキュリティ対策方針の根拠

脅威に対してセキュリティ対策方針が対抗できることを以下で説明する。

T.MODIFY_POLICY_DATA(TOE ポリシーの改ざん)

この脅威は、利用者が端末に格納された TOE ポリシーを直接変更することが考えられる。

この攻撃に対しては、TOE ポリシーに改ざんを検知するためのハッシュ値を付与し、暗号化することで

脅威を軽減できる。この対抗策に該当するセキュリティ方針は、O.POLICY_PROTECTION である。以上より、O.POLICY_PROTECTION の対抗策により T.MODIFY_POLICY_DATA に対抗できる。

4.3.2.2. 組織のセキュリティ方針に対するセキュリティ対策方針の根拠

P.ADMIN_AUTHORITY
この運用環境のセキュリティ対策方針は、管理者認証に関するものである。有効な対策を以下に記述する。
・管理者用設定ツールを実行する前に、管理者パスワードによる識別認証を行い、管理者用設定ツールの利用を TOE の管理者のみに制限する。また、管理者パスワードによる識別認証試行は制限される。
これに対する運用環境のセキュリティ対策方針は、O.ADMIN_AUTHORITY、及び O.PASSWORD_POLICY である。
・管理者パスワードの変更は、管理者のみを可能にする。
これに対するセキュリティ対策方針は、O.PASSWORD_AUTHORITY である。
以上より、O.ADMIN_AUTHORITY、O.PASSWORD_POLICY、 及び O.PASSWORD_AUTHORITY の対策により、P.ADMIN_AUTHORITY が実現できる。

P.PASSWORD_POLICY
この運用環境のセキュリティ対策方針は、パスワードの管理に関するものである。有効な対策を以下に記述する。
・管理者は管理者パスワードを他人に漏らさず、また他人に推測されやすいパスワードを設定しない。また、定期的(6ヶ月以内)に管理者パスワードを変更することで、管理者パスワードが漏洩する可能性を軽減する。
これに対する運用環境のセキュリティ対策方針は、OE.PASSWORD_MANAGEMENT である。
以上より、OE.PASSWORD_MANAGEMENT の対策により、P.PASSWORD_POLICY が実現できる。

P.PASSWORD_PROTECTION
この運用環境のセキュリティ対策方針は、管理者パスワードの保護に関するものである。有効な対策を以下に記述する。
・端末に格納する管理者パスワードに対してハッシュ値を付与し、暗号化して管理者パスワードを秘匿することで、脅威を軽減できる。
この対抗策に該当するセキュリティ方針は、O.PASSWORD_PROTECTION である。
以上より、O.PASSWORD_PROTECTION の対抗策により P.PASSWORD_PROTECTION に対抗できる。

4.3.2.3. 前提条件に対するセキュリティ対策方針の根拠

A.ADMIN(信頼できる管理者)
この前提条件は、信頼できる管理者に関するものである。有効な対策を以下に記述する。
・TOE の管理者には、信頼できる人物を任命しなければならない。
これに対する運用環境のセキュリティ対策方針は、OE.TRUSTED_ROLE である。
以上により、OE.TRUSTED_ROLE の対策により、A.ADMIN が実現できる。

A.OSADMIN_AUTH(管理者権限)

この運用環境のセキュリティ対策方針は、OS の権限に関するものである。有効な対策を以下に記述する。

・OS の管理者権限を管理者のみに与え、利用者は制限ユーザで運用する。

これに対する運用環境のセキュリティ対策方針は、OE.OS_AUTHORITY である。

以上より、OE.OS_AUTHORITY の対策により、A.OSADMIN_AUTH が実現できる。

5. 拡張コンポーネント定義

本章では、拡張コンポーネント定義について記述する。

5.1. 拡張コンポーネント定義

本 ST では、拡張コンポーネントを使用しない。

6. セキュリティ要件

本章では、セキュリティ要件について記述する。
尚、TOE のセキュリティ機能要件で使用するサブジェクト、およびオブジェクトは無い。

6.1. セキュリティ機能要件

本節では、TOE のセキュリティ機能要件を記述する。

6.1.1. 暗号サポート(FCS)

FCS_CKM.1 暗号鍵生成

下位階層: なし
依存性: [FCS_CKM.2 暗号鍵配付、または FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1 TSF は、以下の[割付: 標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付: 暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付: 暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付: 標準のリスト] : DeviceProtector AE 暗号方式
[割付: 暗号鍵生成アルゴリズム] : DeviceProtector AE 共通鍵生成アルゴリズム
[割付: 暗号鍵長さ] : 192ビット

FCS_COP.1a 暗号操作(ハッシュ)

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1a TSF は、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

上述の割付および選択を下表に示す。

[割付: 標準のリスト]	FIPS-PUB180-2	FIPS-PUB180-2
[割付: 暗号アルゴリズム]	SHA-1	SHA-1
[割付: 暗号鍵長]	160 ビット	160 ビット
[割付: 暗号操作のリスト]	管理者パスワードのハッシュ値の生成と検証	TOE ポリシーのハッシュ値の生成と検証

FCS_COP.1b 暗号操作(暗号化)

下位階層: なし
依存性: [FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄

FCS_COP.1.1b TSF は、[割付: 標準のリスト]に合致する、特定された暗号アルゴリズム[割付: 暗号アルゴリズム]と暗号鍵長[割付: 暗号鍵長]に従って、[割付: 暗号操作のリスト]を実行しなければならない。

上述の割付および選択を下表に示す。

[割付: 標準のリスト]	FIPS-SUB46-3	FIPS-SUB46-3
[割付: 暗号アルゴリズム]	3-key Triple DES	3-key Triple DES
[割付: 暗号鍵長]	192 ビット	192 ビット
[割付: 暗号操作のリスト]	管理者パスワードおよび管理者パスワードのハッシュ値の暗号化	TOE ポリシーのハッシュ値の暗号化

6.1.2. 識別と認証(FIA)

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし
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時を検出しなければならない。

[割付: 認証事象のリスト]:管理者の認証
[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]:[割付: 正の整数値]
[割付: 正の整数値] : 3

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]時、TSF は、[割付: アクションのリスト]をしなければならない。

[選択:に達する、を上回った] : に達する
[割付: アクションのリスト]:管理者用設定ツールを10分間、使用禁止。

FIA_SOS.1 秘密の検証

下位階層: なし
依存性: なし

FIA_SOS.1.1 TSF は、秘密が[割付: 定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付: 定義された品質尺度] :

- 管理者パスワードは 8 文字以上 246 文字以下の、以下の範囲の ASCII 文字が使用できる。
- アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字。
- 数字は、[0-9]の合計 10 文字。
- 記号は、 !"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字。
- 管理者パスワードに指定された全ての文字が、同一文字のみ、英字のみ、および数字

のみを禁止する。

FIA_UAU.2 アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング

依存性: FIA_UID.1 識別のタイミング

FIA_UAU.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、各利用者に認証が成功することを要求しなければならない。

FIA_UID.2 アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

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。

6.1.3. セキュリティ管理(FMT)

FMT_MTD.1 TSF データの管理

下位階層: 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_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[割付: 許可された識別された役割]に制限しなければならない。

[割付: TSF データのリスト] : 以下の TSF データ

[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]] : 以下の操作

[割付: 許可された識別された役割] : 以下の役割

表 8 TSF データの管理

TSF データ	操作	許可された識別された役割
管理者パスワード	改変	管理者

FMT_SMF.1 管理機能の特定

下位階層: なし

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。:[割付: TSF によって提供される管理機能のリスト]

[割付: TSF によって提供される管理機能のリスト] :

表 9 セキュリティ管理機能の特定

機能要件	管理要件	管理項目
FIA_AFL.1	1)不成功の認証試行に対する閾値の管理 2)認証失敗の事象においてとられるアクションの管理	1)閾値は固定のため、管理不要 2)アクションは固定のため、管理不要

機能要件	管理要件	管理項目
FIA_SOS.1	1)秘密の検証に使用される尺度の管理	1)尺度は固定のため、管理不要
FIA_UAU.2	1)管理者による認証データの管理 2)このデータに関係する利用者による認証データの管理。	1) 管理者パスワードの改変
FIA_UID.2	1)利用者識別情報の管理	1)利用者識別情報はないため、管理不要

FMT_SMR.1 セキュリティの役割

下位階層: なし

依存性: FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、役割[割付: 許可された識別された役割]を維持しなければならない。

[割付: 許可された識別された役割] :管理者

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。

6.2. セキュリティ保証要件

本節では、TOE のセキュリティ保証要件を記述する。

6.2.1. 開発(ADV)

ADV_FSP.1: 基本機能仕様

6.2.2. ガイダンス文書(AGD)

AGD_OPE.1: 利用者操作ガイダンス
AGD_PRE.1: 準備手続き

6.2.3. ライフサイクルサポート(ALC)

ALC_CMC.1: TOE のラベル付け
ALC_CMS.1: TOE の CM 範囲

6.2.4. セキュリティターゲット評価(ASE)

ASE_CCL.1: 適合主張
ASE_ECD.1: 拡張コンポーネント定義
ASE_INT.1: ST 概説
ASE_OBJ.2: セキュリティ対策方針
ASE_REQ.2: 派生したセキュリティ要件
ASE_SPD.1: セキュリティ課題定義
ASE_TSS.1: TOE 要約仕様

6.2.5. テスト(ATE)

ATE_IND.1: 独立テスト-準拠

6.2.6. 脆弱性評価（AVA）

AVA_VAN.1: 脆弱性調査

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

セキュリティ機能要件とセキュリティ対策方針の対応関係を以下の表 11 に示す。

表 10 セキュリティ機能要件とセキュリティ対策方針の対応関係

	O.ADMIN_AUTHORITY	O.PASSWORD_AUTHORITY	O.PASSWORD_POLICY	O.PASSWORD_PROTECTION	O.POLICY_PROTECTION
FCS_CKM.1				×	×
FCS_COP.1a				×	×
FCS_COP.1b				×	×
FIA_AFL.1			×		
FIA_SOS.1			×		
FIA_UAU.2	×	×			
FIA_UID.2	×	×			
FMT_MTD.1		×			
FMT_SMF.1		×			
FMT_SMR.1		×			

セキュリティ機能要件根拠について、以下に記述する。

O.ADMIN_AUTHORITY(管理者権限)
この TOE セキュリティ対策方針は、管理者用設定ツールの利用を管理者のみが行うことができるようにすることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下の通りである。
管理者用設定ツール利用前に、管理者を識別する。この要件に該当するセキュリティ機能要件は、FIA_UID.2 である。
管理者用設定ツール利用前に、管理者であることを識別認証するためにパスワードを利用する。この要件に該当するセキュリティ機能要件は、FIA_UAU.2 である。
以上より、FIA_UAU.2、FIA_UID.2 の達成により、O.ADMIN_AUTHORITY を実現できる。

O.PASSWORD_AUTHORITY(管理者パスワード変更権限)
この TOE セキュリティ対策方針は、管理者パスワードの変更は管理者のみが行うことができるようにすることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下の通りである。
管理者用設定ツール利用前に、管理者を識別する。この要件に該当するセキュリティ機能要件は、FIA_UID.2 である。
管理者用設定ツール利用前に、管理者であることを識別認証するためにパスワードを利用する。この

要件に該当するセキュリティ機能要件は、FIA_UAU.2 である。
管理者のみが管理者用設定ツールを使用して、管理者パスワードを変更することができる。この要件に該当するセキュリティ機能要件は、FMT_MTD.1、FMT_SMF.1 である。
管理者用設定ツールの利用は、識別認証された管理者のみがおこなうことができる。この要件に該当するセキュリティ機能要件は、FMT_SMR.1 である。
以上より、FIA_UAU.2、FIA_UID.2、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1 の達成により、O.PASSWORD_AUTHORITY を実現できる。

O.PASSWORD_POLICY(管理者パスワードのポリシー)
この TOE セキュリティ対策方針は、管理者パスワードに8文字より短い、全て同一文字、英字のみ、および数字のみのパスワードを登録させないこと、および管理者パスワードの試行回数を3回に制限することを求めている。この要求に対し、必要な対策の詳細と、求められる機能は、以下の通りである。
TOE は管理者パスワードを登録または変更する時、容易に推測されないパスワードであることを確認しなければならない。この要件に対するセキュリティ機能要件は FIA_SOS.1 である。
TOE は管理者パスワードを識別認証時、試行回数を3回に制限しなければならない。この要件に対するセキュリティ機能要件は FIA_AFL.1 である。
以上より、FIA_SOS.1、FIA_AFL.1 の達成により O.PASSWORD_POLICY を実現できる。

O.PASSWORD_PROTECTION(管理者パスワードの保護)
この TOE セキュリティ対策方針は、利用者に管理者パスワードが漏れないように、端末に登録する管理者パスワードを暗号化し、端末に登録する管理者パスワードにハッシュ値を付与し、付与したハッシュ値を暗号化して、改ざんを検出することを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下の通りである。
TOE は管理者パスワードを端末に保存する時、管理者パスワードに改ざんを検出するためのハッシュ値を付与し、管理者パスワードと付与したハッシュ値を暗号化しなければならない。この要件に対するセキュリティ機能要件は、FCS_CKM.1、FCS_COP.1a および FCS_COP.1b である。
以上より、FCS_CKM.1、FCS_COP.1a および FCS_COP.1b の達成により、O.PASSWORD_PROTECTION を実現できる。

O.POLICY_PROTECTION(TOE ポリシーの保護)
TOE は端末に登録されている TOE ポリシーの改ざんを検出する必要がある。この要求に対し、必要な対策の詳細と、求められる機能は以下の通りである。
TOE は、端末に登録する TOE ポリシーにハッシュ値を付与し、付与したハッシュ値を暗号化しなければならない。この要件に対するセキュリティ機能要件は、FCS_CKM.1、FCS_COP.1a および FCS_COP.1b である。
以上より、FCS_CKM.1、FCS_COP.1a および FCS_COP.1b の達成により O.PROFILE_PROTECTION を実現できる。

6.3.2. セキュリティ機能要件の依存性根拠

セキュリティ要件のコンポーネントの依存性を、以下の表 18 に示す。

表 11 セキュリティ要件のコンポーネントの依存性

項番	セキュリティ要件	CC パート 2 で規定されている依存コンポーネント	TOE の依存コンポーネント	依存性が満たされないコンポーネント	妥当性
1	FCS_CKM.1	FCS_CKM.2 または FCS_COP.1 FCS_CKM.4	FCS_COP.1b	FCS_CKM.4	*1
2	FCS_COP.1a	FCS_CKM.1 FCS_CKM.4		FCS_CKM.1 FCS_CKM.4	*2
3	FCS_COP.1b	FCS_CKM.1 FCS_CKM.4	FCS_CKM.1	FCS_CKM.4	*1
4	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 （左記の下位階層）	なし	
5	FIA_SOS.1	なし	なし	なし	
6	FIA_UAU.2	FIA_UID.1	FIA_UID.2 （左記の下位階層）	なし	
7	FIA_UID.2	なし	なし	なし	
8	FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	なし	
9	FMT_SMF.1	なし	なし	なし	
10	FMT_SMR.1	FIA_UID.1	FIA_UID.1	なし	

表 16 より、TOE セキュリティ機能要件は後述する例外を除きそれぞれの必要な依存関係を全て満たしている。全ての例外について、依存関係は満たされなくても問題がない根拠を以下に示す。

*1) FCS_CKM.4、FCS_COP.1b

TOE は、端末固有の値を独自な方法で一意に変換して共通鍵に使用しており、端末に保存していない。このため、共通鍵の削除は行わない。

*2) FCS_COP.1a

FCS_COP.1a は、ハッシュ値の生成と検証であるため、共通鍵は不要である。このため、共通鍵の生成と削除は行わない。

6.3.3. セキュリティ保証要件根拠

本製品は、端末格納データを外部デバイスに持ち出すことにより、情報漏えいすることを防止し、また不正なプログラムを持ち込むことを防止する製品である。情報漏えいの 7 割以上は組織内部から起こり、従業員のミスや故意による持ち出しが主な原因となっている。このような環境で、セキュリティ製品として高い信頼性が要求される。
しかし、本製品は、信頼された管理者の管理下で、一般従業員の脅威にさらされている状況を想定していることから、低レベルな攻撃を想定している。
このため、保証レベルとして EAL1+の選択は妥当であると言える。

7. TOE 要約仕様

7.1. 管理者認証機能

TOE は、管理者用設定ツールを実行できるのは、管理者のみに制限している。
管理者かどうかの識別は、管理者パスワードを入力させ、端末に登録されている管理者パスワードと一致しているかどうか確認することにより、管理者であることを認証する。

（FIA_AFL.1）
TOE は、管理者用設定ツールの起動時、管理者パスワードを入力させ、端末に登録されている管理者パスワードと一致しない場合、管理者パスワードを再度入力させる。
管理者パスワードの入力を3回まで行い、かつ、3回とも、管理者パスワードが一致しなかった場合、管理者用設定ツールを直ちに終了し、以降、10分間、管理者用設定ツールが起動しないようにする。

（FIA_UAU.2、FIA_UID.2）
TOE は、管理者用設定ツールの起動時に、管理者用設定ツールの実行者が管理者であることを確認するために、管理者パスワードによる認証を実行し、管理者に対して、管理者用設定ツールの利用を許可する。

（FDP_SOS.1）
TOE は、管理者パスワードを新規に登録する場合、および管理者用設定ツールで管理者パスワードを変更する場合、入力された管理者パスワードが以下の条件を満足していることを確認し、条件を満足していない場合は、管理者パスワードを再入力させる。

- 管理者パスワードは 8 文字以上 246 文字以下の、以下の範囲の ASCII 文字である。
- アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字。
- 数字は、[0-9]の合計 10 文字。
- 記号は、 !”#$%&’()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字。
- 全て同一文字、英字のみ、および数字のみではない。

7.2. 管理者パスワード変更機能

TOE は、管理者パスワードを変更する機能を提供する。

（FMT_MTD.1、FMT_SMF.1、FMT_SMR.1）
管理者パスワードの変更は、管理者用設定ツールのパスワード変更機能により行う。また、管理者用設定ツールの起動時に、管理者の識別認証を実行するため、管理者用設定ツールを操作できるのは管理者のみである。

7.3. 管理者パスワード保護機能

TOE は、管理者パスワードを端末に登録する時、管理者パスワードを暗号化して秘匿する。また、暗号化する際に、ハッシュ値を付与し、ハッシュ値を確認することにより、改ざんされたかどうかを判断する。

（FCS_CKM.1）

TOE は、端末固有の数値を使用して、独自の変更方法により、一意に変換した値を共通鍵として使用する。

（FCS_COP.1a）
TOE は、端末に保存する管理者パスワードの情報に SHI-1 のハッシュ値を付与する。

（FCS_COP.1b）
TOE は、上記のハッシュ値が付与された管理者パスワードの情報を端末に保存する時、前述の共通鍵を使用して、3-key Triple DES で暗号化を行い、暗号化した管理者パスワードの情報を端末に保存する。

TOE は、管理者パスワードによる管理者の識別認証を行う時、付与したハッシュ値が正しいかどうかを判断し、ハッシュ値が不正だった場合、管理者の識別認証を失敗させる。

7.4. TOE ポリシー保護機能

TOE は、TOE ポリシーにハッシュ値を付与してから暗号化し、付与したハッシュ値を検証することにより、改ざんされたかどうかを判断する。

（FCS_CKM.1）
TOE は、端末固有の数値を使用して、独自の変更方法により、一意に変換した数値を共通鍵として使用する。

（FCS_COP.1a）
TOE は、端末に保存する TOE ポリシーに SHI-1 のハッシュ値を付与する。

（FCS_COP.1b）
TOE は、上記のハッシュ値が付与された TOE ポリシーを端末に保存する時、前述の共通鍵を使用して、3-key Triple DES で暗号化を行い、暗号化した TOE ポリシーを端末に保存する。

TOE は、定期的にハッシュ値が正しいかどうかを判断し、ハッシュ値が不正だった場合、スクリーンセーバーを起動し、利用者に TOE ポリシーが改ざんされたことを通知する。

