認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	**平成**20**年**6**月**25**日** (IT**認証**8227)
認証番号	C0204
認証申請者	NEC**ソフト株式会社**
TOE**の名称**	DeviceProtector AE
TOE**のバージョン**	Version 2.5
PP**適合**	**なし**
適合する保証パッケージ	EAL1**及び追加の保証コンポーネント**ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1
開発者	NEC**ソフト株式会社**
評価機関の名称	**みずほ情報総研株式会社　情報セキュリティ評価室**

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。
平成21年2月24日

セキュリティセンター 情報セキュリティ認証室
技術管理者　鈴木　秀二

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 改訂第2版 (翻訳第2.0版)
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 改訂第2版 (翻訳第2.0版)

評価結果：合格

「DeviceProtector AE Version 2.5」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、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

1.1 はじめに

この認証報告書は、「DeviceProtector AE Version 2.5」（以下「本TOE」という。）について、みずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が行った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NECソフト株式会社に報告するとともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書と共に、対応するSTを併読されたい。本TOEの動作条件や運用のための前提についての詳細、本TOEが対抗する脅威へのセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件、及びセキュリティ仕様の概要と十分性の根拠は、STにおいて詳述されている。

本認証報告書は、情報漏えい対策ソフトウェアを運用する管理者を読者と想定している。本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL1追加である。
追加の保証コンポーネントは、ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1である。

1.1.2 PP適合

適合するPPはない。

1.2 評価製品

1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

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

1.2.2 製品概要

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ことを目的としたソフトウェアである。

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は、各デバイスに対する設定情報をTOEのセキュリティ機能により保護する。

TOEを利用するには、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。

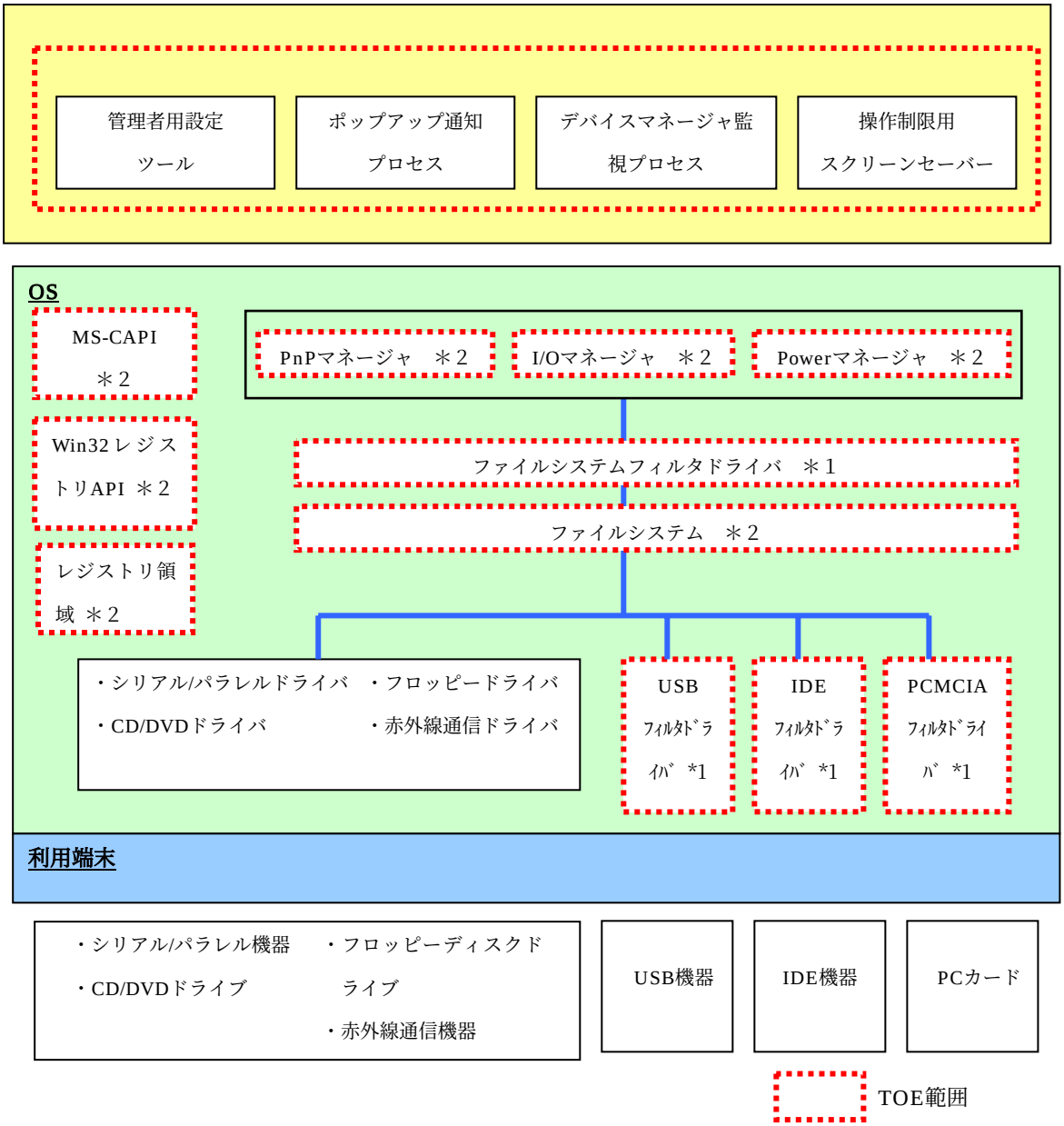
- 管理者認証機能
- 管理者パスワード変更機能
- 管理者パスワード保護機能
- TOEポリシー保護機能

保護された各デバイスの設定情報に従いデバイスの使用は制限されるものとする。

1.2.3 TOE範囲とセキュリティ機能

(1) TOEの範囲

TOEのコンポーネントの構成は、以下の図1-1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1-1　TOEのコンポーネントの構成

TOEは、デバイスの使用制限に必要な以下の図1-2に示す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。

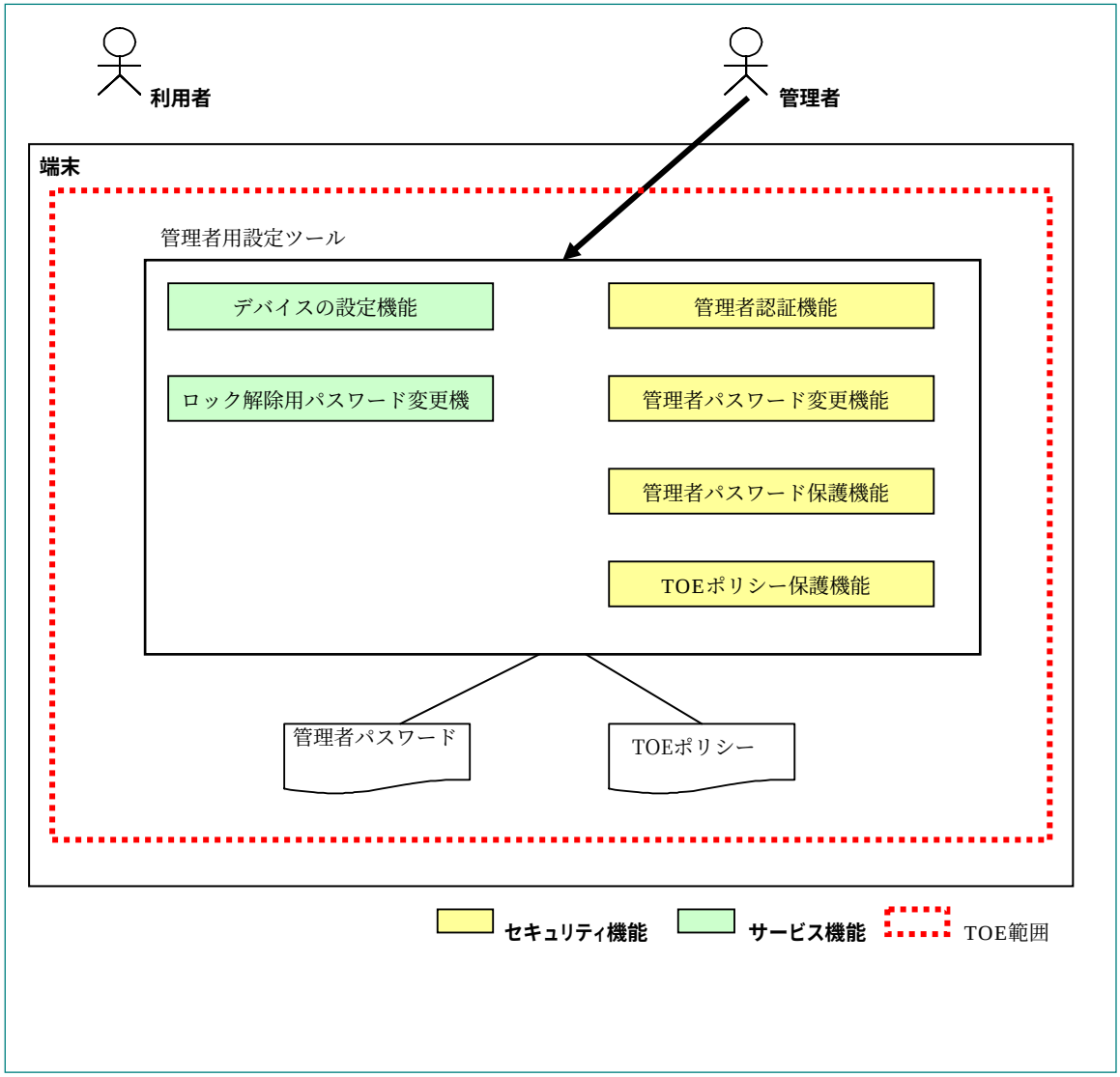


図1-2　管理者用設定ツール

(2) TOEの関係者

表1-1にTOEの関係者を示す。

表1-1　TOEの関係者

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。

(3) 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ポリシーが改ざんされることで、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、表1-2の利用者データを保護資産とする。

表1-2　保護資産

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。

(4) セキュリティ機能

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。

本セキュリティ機能により保護された設定情報に基づくデバイスの制御は本評価の範囲外である。

1.3　評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

①　本TOEのセキュリティ設計が適切であること。

② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「DeviceProtector AE Version 2.5　セキュリティターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件を調査し、本TOEがCCパート1 ([5][8]のいずれか) 附属書A、CCパート2（[6][9]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発がCCパート3（[7][10]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「DeviceProtector AE Version 2.5 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE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。評価は、平成21年2月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEM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概要

2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

表2-1 想定する脅威

識別子	脅　威
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。 （注）直接変更とは、TOEポリシーが格納されている情報をTOE以外の手段で変更することである。

2.1.2 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表2-2に示す。

表2-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
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。

2.1.3 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表2-3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2-3 TOE使用の前提条件

識別子	前提条件
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。
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。

2.1.4 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以下に示す。

- 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）

2.1.5 構成条件

本TOEは、DeviceProtector AEである。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。

（1） TOEの動作に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2-4に示す。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、及び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2-4　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

（2） TOEの動作に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2-5に示す。

表2-5　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

2.2　セキュリティ対策

TOEは、具備したセキュリティ機能により以下のように2.1.1の脅威に対抗し、2.1.2の組織のセキュリティ方針を満たす。

（1） 管理者認証機能

本機能は、P.ADMIN_AUTHORITY（管理者認証）の組織のセキュリティ方針を満たす機能である。

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。

（2） 管理者パスワード変更機能

本機能は、P.ADMIN_AUTHORITY（管理者認証）の組織のセキュリティ方針を満たす機能である。

TOEは、管理者パスワードを変更する機能を提供する。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。

（3） 管理者パスワード保護機能

本機能は、P.PASSWORD_PROTECTION（管理者パスワードの保護）の組織のセキュリティ方針を満たす機能である。

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。

（4） TOEポリシー保護機能

本機能は、T.MODIFY_POLICY_DATA(ポリシーファイルの変更)の脅威に対抗する機能である。

TOEは、TOEポリシーにハッシュ値を付与してから暗号化し、定期的に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。

3 評価機関による評価実施及び結果

3.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

3.2 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、平成20年7月に始まり、平成21年2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、平成20年12月に評価機関で本STにおいて識別されているTOE構成と同様の構成で評価者テストを実施した。

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。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

3.3 製品テスト

評価者は、評価の過程で示された証拠から、必要と判断した独立テスト及び脆弱性評定に基づく侵入テストを実行した。

3.3.1 評価者独立テスト

評価者は、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることの再確認のための独立テストを実施した。評価者が実施した独立テストの概要を以下に示す。

1) 評価者独立テスト環境

評価者が実施したテストの構成を以下に示す。評価者テストは本STにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

PC/AT互換機を一台用意し、TOEをインストールしてテスト環境を構築する。

TOEがインストールされる端末以外のIT環境は存在しない。

表3-1　ソフトウェア構成

構成要素	概要説明
DeviceProtector AE	TOE
OS	TOEが動作するために必要なOS。

表3-2　Professional版 テスト構成

端末	ベンダ名	ソフトウェア/バージョン	備考
IBM ThinkPad R52	NECソフト	DeviceProtector AE 2.5	TOE
	Microsoft	Microsoft Windows XP Professional operating system 日本語版（Service Pack 2）	OS

表3-3　Home Edition版　テスト構成

端末	ベンダ名	ソフトウェア/バージョン	備考
NEC VersaPro	NECソフト	DeviceProtector AE 2.5	TOE
	Microsoft	Microsoft Windows XP Home Edition operating system 日本語版（Service Pack 2）	OS

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

提供された評価証拠資料から、全てのTSFIは管理者用設定ツール上に存在しており、全てのセキュリティ機能が管理者用設定ツール上のインタフェースを介して実施される。評価者は、セキュリティ機能及びTSFIは数が限定的であることから、以下の観点での独立テストを考案した。

・ 全てのセキュリティ機能を網羅する

TOEの4つのセキュリティ機能（「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」）をすべて網羅する。

・ 利用者が操作可能なインタフェースを網羅する

管理者用設定ツール上のインタフェースを全てテスト対象とする。

・ 暗号操作（ハッシュ値計算、暗号化）については、内部インタフェース間でデータの受け渡しを行っており、TSFIを介してデータやパラメータを取得することができないため、ログ出力ツール（テスト用ツール）を用いてデータ及びパラメータを取得して確認を行う。パスワード情報から生成されるハッシュ値を別ツール（OpenSSL）により算出し、算出された値がログデータに表示されるハッシュ値と等しいことを確認する。

b. 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。

テストは、管理者用設定ツールを介した操作及びファイル、レジストリエディタを用いたレジストリに格納される値の参照、変更、及びログ出力ツールの出力結果の検証により実施された。

OSとしてWindows“ XP Home Edition ”及び“ XP Professional Edition ”を対象としていることから、独立テストにおいてはそれぞれのOSがインストールされた環境において、同一内容の16件（管理者認証機能:8件、管理者パスワード変更機能:2件、管理者パスワード保護機能:3件、TOEポリシー保護機能:3件）のテストを実施した。

c. 結果

実施したすべての評価者独立テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

3.3.2 評価者侵入テスト

評価者は、評価の過程で示された証拠から、懸念される脆弱性の可能性について必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、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。

- TOEポリシー、管理者パスワード、の探索、またTOEポリシー、管理者パスワード改ざん可能性に関する脆弱性

TOEポリシー及び管理者パスワード格納領域として一般利用者がアクセス可能なレジストリ領域が存在している。

- TOEポリシー改ざん検出機能の脆弱性

  改ざん検出機能の起動が時間情報に関連して起動しており、かつ、一般利用者がOSのシステム時間情報を変更可能である。

b. 実施テストの範囲

評価者は、潜在的な脆弱性が悪用される可能性があるかを決定するため、以下の侵入テストを実施した。

侵入テストは、上記懸念される脆弱性の結果から、保護資産改ざん可能性、改ざん検知機能の脆弱性検証の2件のテストが行われた。

- 保護資産改ざん可能性

  OS内の全てのフォルダ、レジストリを対象として管理者パスワード、TOEポリシーの探索を行う。また、管理者パスワード、TOEポリシー改ざん、破壊及びそれらがセキュリティ機能に与える影響について検証する。

- 改ざん検知機能の脆弱性検証

  TOEポリシー改ざん検出時に端末の利用制限（スクリーンセーバーの起動）が実施されるが、TOEの管理者以外の利用者がPower User権限などOSの時刻情報を変更する権限を有する状況を想定し、OSの時刻情報の改ざんがポリシー改ざん検出のタイミングに与える影響について検証する。

c. 結果

実施した評価者侵入テストでは、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。

3.4 評価結果

3.4.1 評価結果

評価報告書をもって、評価者は本TOE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。

3.4.2 評価者コメント/勧告

消費者に喚起すべき評価者勧告は特にない。

4 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正しく反映されていること。
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。

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。

5 結論

5.1 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TOEがCCパート3のEAL1及び保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1に対する保証要件を満たすものと判断する。

5.2 注意事項

特にない。

6 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）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
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用語の定義を以下に示す。

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。
デバイス	端末に搭載された装置、及び接続された周辺装置。

7 参照

[1] 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2月6日 NECソフト株式会社

[2] ITセキュリティ評価及び認証制度の基本規程 平成19年5月 独立行政法人 情報処理推進機構 CCS-01

[3] ITセキュリティ認証申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程 平成19年5月 独立行政法人 情報処理推進機構 CCM-03

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

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

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

[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1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2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2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0版)

[10] 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2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

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

[12] 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2版 2007年9月 CCMB-2007-09-004 (平成20年3月翻訳第2.0版)

[13] DeviceProtector AE Version2.5 評価報告書 07003427-01-R003-05 2009年2月6日 みずほ情報総研株式会社 情報セキュリティ評価室