認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　藤原　武平太

原紙押印済

評価対象

申請受付日（受付番号）	**平成19年5月1日** (IT**認証**7148)
認証番号	C0134
認証申請者	**日本電気株式会社**
TOE**の名称**	NEC**グループ 情報漏洩防止システム**
TOE**のバージョン**	V1.0
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	**日本電気株式会社**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

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19年12月26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1版 (翻訳第1.2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1版　(翻訳第1.2版)

評価結果：合格

「NECグループ 情報漏洩防止システム」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、「NECグループ 情報漏洩防止システム V1.0」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所　評価センター（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日本電気株式会社に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.8 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応する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、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

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。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　NECグループ 情報漏洩防止システム
バージョン：　V1.0
開発者：　日本電気株式会社

1.2.2 製品概要

本TOEは、NECグループ全体に導入される情報漏洩防止システムである。管理者が利用者毎に付与する権限に従ったPC制御方針を作成し、これを利用者のPCに適用することにより、PCからの情報持ち出しにかかわる操作を制限し、情報漏洩を防止する。

本TOEの主要なセキュリティ機能は、識別認証機能、アクセス制御機能、暗号機能及び監査機能である。

・識別認証機能
　-利用者を識別認証する機能
・アクセス制御機能

-I/Oポート、プリンタへの入出力を制御する機能
-利用者プログラムの実行を制御する機能
-許可外部メディアへのファイルの出力を制御する機能
-許可USBデバイスへのファイルの入出力を制御する機能
-クライアント制御情報の作成及び変更を制御する機能

・暗号機能
-ファイルの暗号化／復号を行う機能
-暗号化／復号のための鍵の生成を行う機能
-許可外部メディア及び許可USBデバイスへのファイル出入力時に暗号化／復号を行う機能

・監査機能
-ログを生成し、ログサーバに転送する機能
-ログサーバに蓄積されたログの閲覧・検索を行う機能

1.2.3 TOEの範囲と動作概要

本TOEは、管理者端末及びクライアントから転送されたログを蓄積するログサーバ、識別認証機能やアクセス制御機能等の管理を実施する管理者が使用する管理者端末、NECグループ内の一般利用者が使用するクライアント、の3つの端末上で動作する分散TOEである。クライアントPCからの情報持ち出しにかかわる操作を制限するために、管理者は管理者端末においてPC制御方針を定めたクライアント制御情報を作成する。一般利用者は管理者から配布されたクライアント制御情報をクライアントに取り込むと、それ以降はそのクライアント制御情報に従ったI/Oポート、利用者プログラム、プリンタ及び許可外部メディアに対するアクセス制御機能がクライアント上で動作するようになる。また使用される許可外部メディアや入手したデータの暗号化も合わせて実施される。管理者端末及びクライアントにおける外部メディアの書き込み等の各種操作時には監査ログが生成され、それらの監査ログはログサーバに転送される。ログサーバに蓄積された監査ログは、管理者端末より閲覧・検索可能である。

本TOE動作概要は上記の通りであり、その物理的範囲は図1-1において赤い点線で囲まれたログサーバ、管理者端末、クライアント上のソフトウェア群である。TOEの各コンポーネントの詳細は表1-1に示されている。

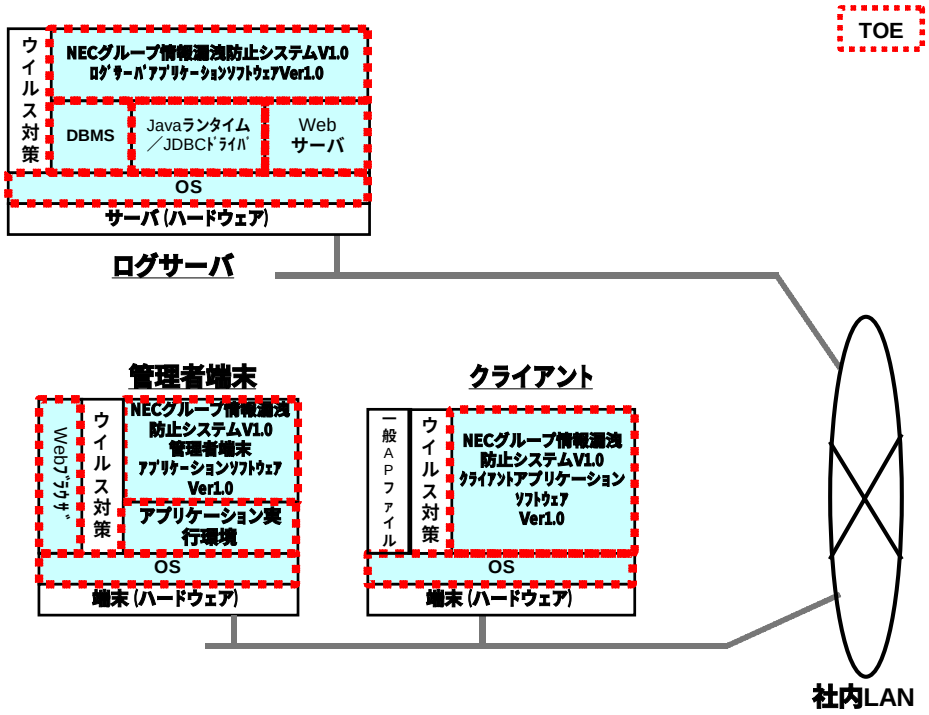

図1-1　TOEの構成

表1-1　TOEのソフトウェアコンポーネント

機器名	種別	ソフトウェアコンポーネント名
ログサーバ	AP	NECグループ 情報漏洩防止システム V1.0 ログサーバアプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows Server 2003 Standard Edition（SP1）
	DBMS	Microsoft SQL Server 2005 Standard Edition（SP1）
	JDBCドライバ	Microsoft SQL Server 2005 JDBC Driver Ver1.0
	Webサーバ	Apache Tomcat 5.5.17 Apache Axis 1.4
	Java ランタイム	Sun Java Runtime Environment (JRE) 5.0 Update 11
管理者端末	AP	NECグループ 情報漏洩防止システム V1.0 管理者端末アプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows XP Professional（SP2）
	Web ブラウザ	Microsoft Internet Explorer 6.0（SP2）

機器名	種別	ソフトウェアコンポーネント名
	アプリケーション実行環境	Microsoft .NET Framework 2.0 Microsoft .NET Framework 2.0 日本語Language Pack
クライアント	AP	NECグループ 情報漏洩防止システム V1.0 クライアントアプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows XP Professional（SP2）

なお、ログサーバ及び管理者端末においては、Administrator権限で運用するが、クライアントの通常利用においては、Administrator権限以外の任意のOSのユーザ権限で運用するものとする。

TOEが動作するハードウェアスペックは表1-2の通りである。

表1-2　ハードウェア構成

機器名	種別	説明
ログサーバ	CPU	Pentium 4　3.0GHz 以上
	メモリ	2GB以上
	HDD	100GB以上
	グラフィック	1024×768ピクセル以上の解像度 256色以上のカラー表示
管理者端末、クライアント共通	CPU	Pentium Ⅲ　1.0GHz 以上
	メモリ	512MB以上
	HDD	40GB以上
	グラフィック	1024×768ピクセル以上の解像度 256色以上のカラー表示

1.2.4　TOEの機能

以下にTOEのセキュリティ機能を、端末毎に示す。

1）監査機能

（管理者端末、クライアント）

・管理者端末及びクライアントのログの生成及びログサーバへの送信

・ログのログサーバへの送信時の転送保護

（ログサーバ）

・ログサーバのDBに蓄積されたログの閲覧・検索

2）識別認証機能

※本項で記述する識別認証機能は、管理者端末、クライアント及びログサーバ上のAPである「NECグループ情報漏洩防止システムV1.0 管理者端末アプリケーションソフトウェア Ver1.0」、「NECグループ情報漏洩防止システムV1.0 クライアントアプリケーションソフトウェア Ver1.0」及び「NECグループ情報漏洩防止システムV1.0 ログサーバアプリケーションソフトウェア Ver1.0」によって提供される識別認証機能であり、OSにより提供される識別認証機能ではない。

（管理者端末）

・管理者が管理者端末にログオンする際の識別認証

・一定時間管理者からのアクセスがない場合のPCロックから復旧する際の識別認証

・管理者パスワードの変更

（クライアント）

・一般利用者またはクライアント管理者がクライアントにログオンする際の識別認証

・一定時間一般利用者からのアクセスがない場合のPCロックから復旧する際の識別 認証

・一般利用者パスワードの変更

（ログサーバ）

・管理者がログサーバに蓄積されたログを閲覧、検索する際の識別認証の実施

3）アクセス制御機能

（管理者端末）

・クライアント制御情報の作成、変更

（クライアント）

・クライアント制御情報の参照

・クライアント制御情報に基づき以下を実施

－I/Oポート及びプリンタの利用可否の設定の制御

－一般APファイルの実行及びファイル名称変更の制御

－許可外部メディアへのファイル出力の制御

－許可USBデバイスへのファイル入出力の制御

4）暗号機能

（管理者端末）

・クライアントを利用する一般利用者が、入手、作成した任意のデータファイ

ルを暗号化／復号するための暗号鍵ファイルの生成

（クライアント）
・クライアントを利用する一般利用者が、入手、作成した任意のデータファイルを暗号化／復号するための鍵の読み込み、削除
・クライアントを利用する一般利用者が、入手、作成した任意のデータファイルの暗号化／復号
・許可外部メディアへの出入力時のファイルの暗号化／復号

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「NECグループ 情報漏洩防止システム V1.0 セキュリティターゲット」(以下「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、「NECグループ 情報漏洩防止システム V1.0 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19年12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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL1及び追加の保証コンポーネントASE_OBJ.2、ASE_REQ.2、ASE_SPD.1である。

1.5.3 セキュリティ機能

本TOEのセキュリティ機能は、「1.2.4TOEの機能」を参照のこと。

本TOEのセキュリティ機能は、以下に示すセキュリティ機能要件を実現している。

・セキュリティ監査
・暗号化機能
・アクセス制御
・送出データ保護
・入力データ保護
・識別と認証
・セキュリティ管理
・セキュリティ機能保護

1.5.4 脅威

本TOEは、表1-3に示す脅威を想定し、これに対抗する機能を備える。

表1-3 想定する脅威

識別子	脅 威
T.INJUSTICE_LOGON（不正なログオン）	一般利用者及び第三者が、TOEの正当な利用者になりすまして、利用者データまたはTSFデータを改ざん、暴露するかもしれない。
T.UNAUTHORIZED_ACCESS(許可されない操作)	一般利用者が、許可されない操作（許可されていないプリンタへの出力、許可されていないプログラムの実行、許可されていないI/Oポートの利用）を実行することで、クライアントに保存された利用者データを暴露するかもしれない。
T.INJUSTICE_CONNECT（不正な装置の接続）	第三者が、不正な装置に外部メディアまたはクライアントのHDDを接続することにより、外部メディアまたはクライアントのHDDに保存された利用者データを暴露するかもしれない。

1.5.5 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1-4に示す。

表1-4 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.LOG_COLLECT（ログの集約）	管理者端末及びクライアントで収集されたログは、ログサーバにセキュアに集約される。
P.RESTRICTED_MEDIA（許可外部メディアのみの使用）	クライアントから書き込みできる外部メディアは、許可された外部メディアのみとする。
P.SECURITY_PARAMETER（適切なセキュリティパラメータ設定）	管理者は、TOEのガイダンス文書に基づきクライアント制御情報を適切な値に設定する。

1.5.6 構成条件

本TOEは、「表1-1　TOEのソフトウェアコンポーネント」に示されたソフトウェアにより構成され、「表1-2　ハードウェア構成」で示されたスペックを満たすハードウェア上で動作する。

1.5.7 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1-5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1-5 TOE使用の前提条件

識別子	前提条件
A.MANAGE_SAFE_PLACE（管理者端末の安全な設置）	管理者端末は、NECグループ社員及びNECグループ社員が許可した者のみが入館できる建物内に設置される。
A.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）	ログサーバ及びログのバックアップ媒体は、入退室管理された室内に設置されなければならない。
A.UNJUST_SOFTWARE（不正ソフトウェア対策）	TOEが動作するログサーバ、管理者端末及びクライアントには、ウイルス対策ソフトウェアが導入されるとともに、ウイルス対策ソフトウェアのパターンファイルや、TOEのコンポーネントの一部であるOSのセキュリティ対策用修正ソフトウェアが適切に適用される。
A.PASSWORD_MANAGEMENT（パスワードの管理）	TOEの利用者は、TOEにアクセスするためのパスワードを他人に知られないよう管理する。またTOEの利用者は、推測されにくいパスワードを設定し、適切な頻度で変更する。
A.NETWORK（ネットワーク環境）	社内LANと外部ネットワークは、外部ネットワークからの不正な通信を防ぐ装置を介して接続される。またセキュアルームのネットワークは、ログサーバ、管理者端末及びクライアントとの通信に必要なプロトコルのみ許可する装置を介して社内LANに接続される。
A.OPERATOR_MANAGEMENT（管理者の管理）	管理者は、信頼できる者であり、不正な操作を行なわない。
A.LOG_BACKUP（ログのバックアップ）	ログサーバのログは、消失から防止されなければならない。
A.PC_STARTUP_SET（PCの起動制御設定）	一般利用者に貸与されるPCは、保守モードでの起動ができないように設定されなければならない。

1.5.8 製品添付ドキュメント

本TOEに添付されるドキュメントを以下の表1-6に示す。

表1-6 TOEのガイダンス文書

種類	ガイダンス文書名
インストールガイダンス	NECグループ 情報漏洩防止システム V1.0インストールガイド
利用者操作ガイダンス	NECグループ 情報漏洩防止システム V1.0管理者ガイド
	NECグループ 情報漏洩防止システム V1.0利用者ガイド

2 評価機関による評価実施及び結果

2.1 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。

2.2 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19年5月に始まり、平成19年12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19年10月に開発者サイトで開発者のテスト環境を借用し評価者テスト（評価者独立テストと侵入テスト）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。

2.3 製品テスト

評価者の実施した評価者テストの概要を以下に示す。

2.3.1 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの機器構成を以下の図2-1に示す。

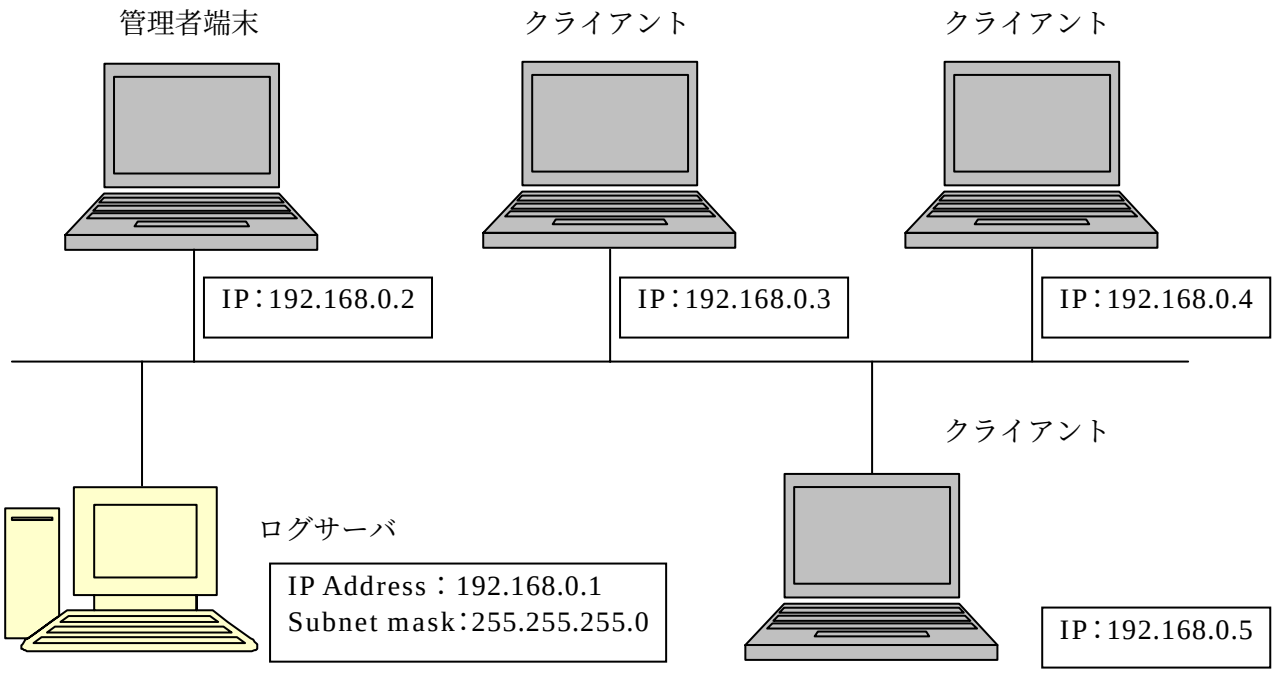

図2 -1　TOEの機器構成

各機器のハードウェア構成は、以下の通りである。

1）ログサーバ

・Express5800/120Re-1(X/3DG(1)) No.4Z01299 NEC Corporation

－ CPU Intel(R) Xeon(TM) CPU 3.00GHz

－ メモリ　2GB

－ HDD　100GB

2）管理者端末とクライアント

・VersaPro VY16F/RF-R NEC Corporation

－ CPU Intel(R) Pentium(R) M processor 1.60GHz

－ メモリ　496MB

－ HDD　40GB

各機器のソフトウェア構成は、以下の表2-1の通りである。

表2 -1　TOEのソフトウェア構成

機器名	種別	製品名
ログサーバ	AP	NECグループ　情報漏洩防止システム　V1.0 ログサーバアプリケーションソフトウェア　Ver1.0
	OS	Microsoft Windows Server 2003 Standard Edition（SP1）
	DBMS	Microsoft SQL Server 2005 Standard Edition（SP1）
	JDBCドライバ	Microsoft SQL Server 2005 JDBC Driver Ver1.0
	Webサーバ	Apache Tomcat 5.5.17 Apache Axis 1.4
	Javaランタイム	Sun Java Runtime Environment (JRE) 5.0 Update 11
	ウィルス対策	Networks Associates Technology VirusScan Enterprise 8.0i
管理者端末	AP	NEC グループ 情報漏洩防止システム V1.0 管理者端末アプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows XP Professional（SP2）
	Webブラウザ	Microsoft Internet Explorer 6.0（SP2）
	アプリケーション実行環境	Microsoft .NET Framework 2.0 Microsoft .NET Framework 2.0 日本語Language Pack
	ウィルス対策	Networks Associates Technology VirusScan Enterprise 8.0i
クライアント	AP	NEC グループ 情報漏洩防止システム V1.0 クライアントアプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows XP Professional（SP2）
	ウィルス対策	Networks Associates Technology VirusScan Enterprise 8.0i

また、テスト時に評価者は以下の表2-2に示すツールを使用している。

表2 -2　使用ツール

種別	製品名
レジストリエディタ	Microsoft(R) レジストリエディタ Version 5.1 （Build 2006.xpsp_sp2_gdr..070227 : Service Pack2）
Network Protocol Analyzer	WIRESHARK Version 0.99.6a (SVN Rev 22276)

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテスト構成は上記 1)評価者テスト環境に示した通りであり、評価者テストは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。

b.テスト手法

テストには、以下の手法が使用された。

① TOEが提供するインタフェース（TSFI）を利用しての機能テスト
② レジストリエディタによりレジストリを変更してのテスト
③ ネットワークプロトコルアナライザを利用しての通信テスト

c.実施テストの範囲

評価者が独自に考案した評価者独立テストを39項目（管理者端末におけるテスト：12項目、クライアントにおけるテスト：22項目、ログサーバにおけるテスト：5項目）、侵入テストを8項目、計47項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

1)評価者独立テスト

① テストサブセットに気が付いた問題と関連性のある少数のインタフェースを含め、これらのインタフェースを厳密にテストする
② SFR 実施インタフェースは必ずテスト項目に含める

2)侵入テスト

① 類似製品の公知の脆弱性情報よりテスト項目を考案
② 参考書籍および参考文献（IPA公開情報）よりテスト項目を考案
③ 他のテスト結果をベースに新たにテスト項目を考案

d.結果

実施したすべての評価者独立テストにおいて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。侵入テストに関しては1件のみ期待されたふるまいと一致していないものがあったが、CEMの規定に基づき検討した結果、本EAL1で想定される攻撃者のレベルでは悪用不可能である（即ち残存脆弱性である）と判定された。

2.4 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 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 当該所見報告書でなされた指摘内容が妥当であること。
② 当該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、ST及び評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された評価報告書、当該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及び追加の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していることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_INT.1.1E	評価はワークユニットに沿って行われ、TOE参照、TOE概要及びTOE記述が正しく記述されていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、TOE参照、TOE概要及びTOE記述が相互に一貫していること確認している。
ASE_CCL.1.1E	評価はワークユニットに沿って行われ、CCの適合主張の有効性を確認している。
ASE_SPD.1.1E	評価はワークユニットに沿って行われ、セキュリティ課題が明確に定義されていることを確認している。
ASE_OBJ.2.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針が明確に定義されていることを確認している。
ASE_ECD.1.1E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含まれていないため非適用であることを確認している。
ASE_ECD.1.2E	評価はワークユニットに沿って行われ、拡張セキュリティ要件が含まれていないため非適用であることを確認している。
ASE_REQ.2.1E	評価はワークユニットに沿って行われ、SFR、SARは明確に、曖昧さなく十分に定義され、また内部的に一貫していること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていることを確認している。

ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述がどのように各SFRを満たすかを示していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述がTOE概要及びTOE記述と一貫していることを確認している。
ライフサイクルサポート	**適切な評価が実施された**
ALC_CMC.1.1E	評価はワークユニットに沿って行われ、TOEは一意の参照でラベル付けされていることを確認している。
ALC_CMS.1.1E	評価はワークユニットに沿って行われ、TOEの構成リストが管理され、構成要素が一意に識別可能なことを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、SFR実施・SFR支援TSFIの目的と使用方法、パラメタが記載されていることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_OPE.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_PRE.1.1E	評価はワークユニットに沿って行われ、準備手続きがTOEのセキュアな準備を記述し、STの運用環境のITセキュリティ方針に従った環境が構築可能であることを確認している。

AGD_PRE.1.2E	評価はワークユニットに沿って行われ、準備手続きを元に評価者がセキュアにTOEと準備環境を構築可能なことを実行し確認している。
テスト	**適切な評価が実施された**
ATE_IND.1.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、提供されていることを確認している。
ATE_IND.1.2E	評価はワークユニットに沿って行われ、独立テストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_VAN.1.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、提供されていることを確認している。
AVA_VAN.1.2E	評価はワークユニットに沿って行われ、潜在的な脆弱性検出のために公知の資料を検査していることを確認している。
AVA_VAN.1.3E	評価はワークユニットに沿って行われ、識別された潜在的脆弱性が基本的な攻撃能力を持つ攻撃者からの攻撃に耐えられることを根拠とともに記述していることを確認している。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
IT	Information Technology
SFR	Security functional requirement
SAR	Security assurance requirement
TSFI	TOE Security Functionality interface

本報告書で使用されたTOE特有の略語を以下に示す。

AP	Application Program（アプリケーションプログラム）
DB	Database（データベース）
DBMS	Database Management System（データベース管理システム）
GB	Giga Byte（ギガバイト）
GHz	Gigahertz（ギガヘルツ）
HDD	Hard Disk Drive（ハードディスクドライブ）
LAN	Local Area Network（ローカルエリアネットワーク）
PC	Personal Computer（パーソナルコンピュータ）

本報告書で使用された用語を以下に示す。

Administrator権限	Microsoftオペレーティングシステムのユーザ権限の種類のひとつで、OSの設定を変更できる権限
NEC	日本電気株式会社
NECグループ	NEC及びNEC関係会社
I/Oポート	PCとPCに接続される機器とのデータのやり取りに使用することができるポートで、USBポート、IEEE1394ポート、シリアルポート、パラレルポート、赤外線ポート、PCMCIAポート及びプリンタポート
Java	オブジェクト指向プログラミング言語の一つ。プログラミング言語であるJavaの実行環境
JDBC	Javaとデータベースの接続のためのAPインタフェース
USBデバイス	PCのUSBポートに接続される周辺機器の総称
管理者	管理者とクライアント管理者の利用者役割を持つ者
外部メディア	クライアントに接続されOSによりリムーバブルメディアと認識されたメディア（外付けHDD、USBメモリ、PCMCIAメモリ）
管理者端末	管理者がクライアント制御情報の作成やログの閲覧・検索を行うPC
許可USBデバイス	管理者によりあらかじめ利用を許可されたUSBデバイス
許可外部メディア	クライアントに接続されOSによりリムーバブルメディアと認識されたメディア（外付けHDD、USBメモリ、PCMCIAメモリ）で、管理者によりあらかじめ許可外部メディア入出力制御情報が書き込まれたメディア
クライアント	NECグループ内で利用するPC
クライアント制御情報	PC制御方針であり、管理者により作成され、クライアントに設定され、クライアントの動作を制御する定義情報
プリンタポート	クライアントの印刷データをプリンタに出力するためのポート
保守モード	Microsoft Windows OSを保守するため、Windows起動時に指定するモード（セーフモード）

利用者	管理者、クライアント管理者及び一般利用者の総称
ログ	監査証跡に記録された監査記録

6 参照

[1] NECグループ 情報漏洩防止システム V1.0 セキュリティターゲット バージョン 1.12（2007年12月12日）日本電気株式会社

[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 September 2005 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version　3.1 September 2005 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version　3.1 September 2005 CCMB-2006-09-003

[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 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: セキュリティ機能要件 バージョン3.1 第1版　2006年9月 CCMB-2006-09-002　(平成19年3月翻訳第1.2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: セキュリティ保証要件 バージョン3.1 第1版　2006年9月 CCMB-2006-09-003　(平成19年3月翻訳第1.2版)

[11] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 3.1 September 2005 CCMB-2006-09-004

[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 第1版 2006年9月 CCMB-2006-09-00４　(平成19年3月翻訳第1.2版)

[13] NECグループ 情報漏洩防止システム V1.0 評価報告書 第1.3版 2007年12月13日 株式会社電子商取引安全技術研究所　評価センター