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19年8月31日** (IT**認証**7168)
認証番号	C0156
認証申請者	**日本電気株式会社**
TOE**の名称**	NEC**グループ セキュア情報交換サイト**
TOE**のバージョン**	1.0
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	**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20年4月25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 セキュア情報交換サイト」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
1.1 はじめに 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 1
1.2.3 TOEの範囲と動作概要 2
1.2.4 TOEの機能 6
1.3 評価の実施 6
1.4 評価の認証 7
1.5 報告概要 7
1.5.1 PP適合 7
1.5.2 EAL 7
1.5.3 セキュリティ機能 8
1.5.4 脅威 9
1.5.5 組織のセキュリティ方針 10
1.5.6 構成条件 10
1.5.7 操作環境の前提条件 12
1.5.8 製品添付ドキュメント 13
2 評価機関による評価実施及び結果 14
2.1 評価方法 14
2.2 評価実施概要 14
2.3 製品テスト 14
2.3.1 評価者テスト 14
2.4 評価結果 16
3 認証実施 17
4 結論 18
4.1 認証結果 18
4.2 注意事項 20
5 用語 21
6 参照 23

1 全体要約

1.1 はじめに

この認証報告書は、「NECグループ セキュア情報交換サイト バージョン1.0」（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 セキュア情報交換サイト
バージョン： 1.0
開発者： 日本電気株式会社

1.2.2 製品概要

本TOEは、NECグループ社内利用者とその顧客間で、業務データの交換における誤配信と、情報漏洩を防止するためのサービスを提供している業務データ交換システムである。

TOEの使用方法は、まずNECグループ社員がエリアを作成し、作成したエリア内にフォルダを作成する。作成したフォルダ内に、社内利用者や顧客が業務データをアップロードする。アップロードされた業務データは、社内利用者や顧客がダウンロードして使用する。

サービス機能として、業務データのアップロード機能、ダウンロード機能、エリ

アメンテナンス機能、利用者メンテナンス機能、個人設定機能、運用管理を行う機能を提供している。

セキュリティ機能として、TOEで交換する業務データに対して、不正アクセスや誤配信、情報漏洩の防止を行うための機能を提供している。TOEが提供する主要なセキュリティ機能の概要を以下に示す。

・識別認証機能
　本TOEの利用者に対する識別と認証を行う機能。
・アクセス制御機能
　本TOEの利用者役割に基づいて、業務データへのアクセス制御を行う機能。
・監査機能
　本TOEの監査証跡の生成、参照を行う機能。
・暗号機能
　本TOEと利用者との間の通信データの暗号化、復号を行う機能。

1.2.3　TOEの範囲と動作概要

1) TOEの動作環境と範囲

TOEは、NECグループ社内とその顧客で使用されるシステムである。TOEの動作環境を図1-1に示す。

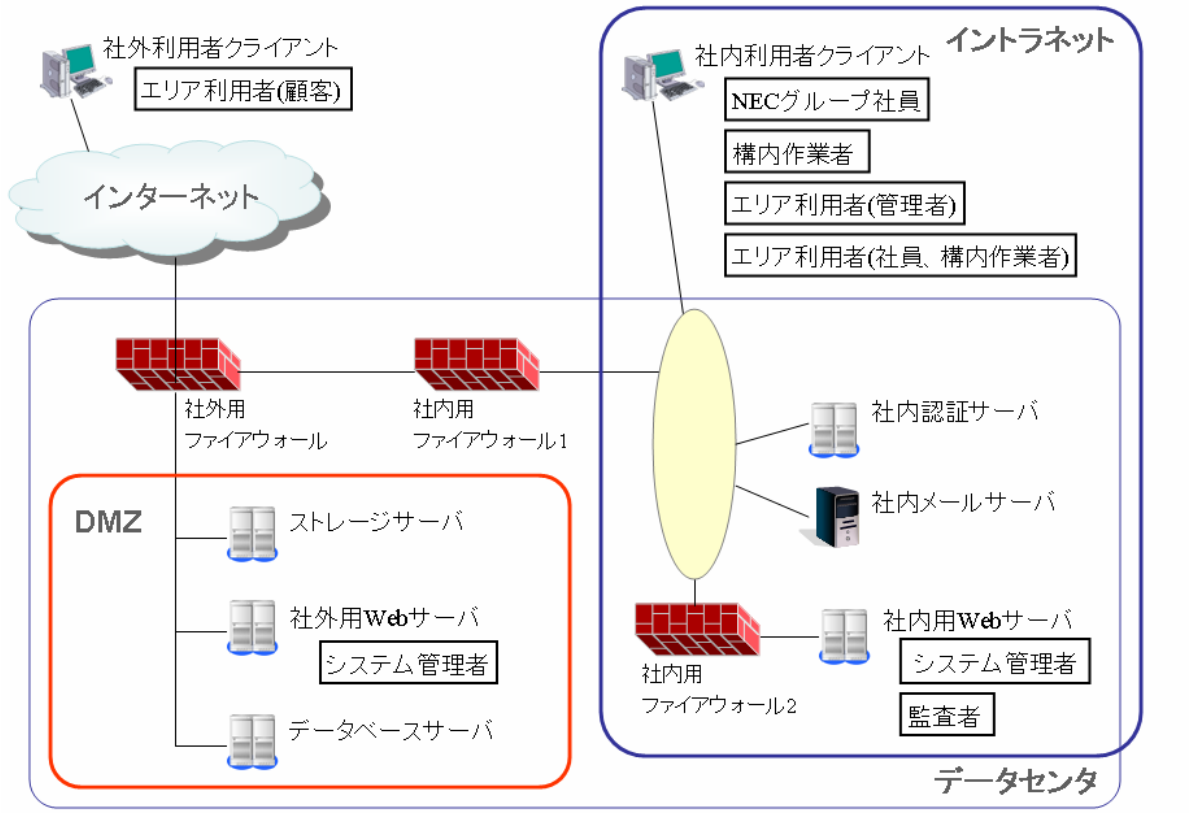

図1-1　TOEの動作環境

TOEの範囲は、社内用Webサーバ、社外用Webサーバ、社内利用者クライアント及び社外利用者クライアントで動作するソフトウェア群である。TOEを構成するソフトウェアを表1-1に示す。

表1-1　TOEのソフトウェア構成（TOEの範囲）

端末名			
	ベンダ名	名称	種別
社内用Webサーバ			
	NEC	NECグループ セキュア情報交換サイト V1.0 社内用サーバアプリケーションソフトウェア V1.0	アプリケーションソフトウェア
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Webブラウザ
	Microsoft	.NET Framework 3.0	アプリケーション実行環境
	Microsoft	Internet Information Server 6.0	Webサーバ
社外用Webサーバ			
	NEC	NECグループ セキュア情報交換サイト V1.0 社外用サーバアプリケーションソフトウェア V1.0	アプリケーションソフトウェア
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Webブラウザ
	Microsoft	.NET Framework 3.0	アプリケーション実行環境
	Microsoft	Internet Information Server 6.0	Webサーバ
社内利用者クライアント			
	NEC	NECグループ セキュア情報交換サイト V1.0 Webブラウザライブラリ V1.0	ActiveX Control
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Webブラウザ
	Microsoft	OS暗号処理ライブラリ	OSライブラリ
社外利用者クライアント			
	NEC	NECグループ セキュア情報交換サイト V1.0 Webブラウザライブラリ V1.0	ActiveX Control
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Webブラウザ
	Microsoft	OS暗号処理ライブラリ	OSライブラリ

2) TOEの動作概要

従来、業務データの交換手段として、メールの利用が一般的であるが、この場合、誤配信や、情報漏洩の危険性が少なくない。本TOEは、NECグループ社内利用者と顧客との間で取り交わす業務データに対して、その交換可能な社内利用者を限定すると共に顧客にURLとPINを別送することで誤配信を防止し、交換するデータを暗号化することで情報漏洩の防止を行うシステムである。

図1-1において、交換する業務データ及びその関連情報は、それぞれ、TOE外のストレージサーバ、データベースサーバに格納される。NECグループ社内利用者は、社内利用者クライアントを操作し、社内用Webサーバを経由して業務データにアクセスする。顧客は、社外利用者クライアントを操作し、社外用Webサーバを経由して業務データにアクセスする。

業務データの交換は以下のように行われる。

①まず、業務データの交換を行うために、その格納場所となるエリア、及びフォルダを作成しておく。エリアの作成者は、作成したエリア内のフォルダ単位に、そのフォルダを使用する社内利用者、顧客を登録しておく。

②フォルダに登録された社内利用者、顧客は、業務データをアップロードする。業務データのアップロードは登録されたフォルダに対してのみ可能である。この時、業務データを格納するフォルダに対して、ダウンロードを行える社内利用者、顧客を指定する。ダウンロード者の指定は、あらかじめ登録された社内利用者、顧客から選択することで行う。

③TOEは、ダウンロードのためのワンタイムURL、及び、顧客がワンタイムURLを利用するときに必要となるPINを生成する。生成されたワンタイムURLは、ダウンロードを行う社内利用者、顧客に対して、メールで通知する。メールはTOE外の社内メールサーバを経由して配信される。一方、PINは、ワンタイムURLとは別の方法で顧客に通知する。

④ワンタイムURLを利用するときに、社内利用者は、TOE外の社内認証サーバによる認証を行う。また、顧客は、PINによる認証を行う。これにより、フォルダ内の業務データに対して、ダウンロードを指定された社内利用者、顧客のみが、ダウンロードを行える。

3) TOEの利用者役割

TOEにおける利用者の役割は以下のとおりである。

TOEが提供するサービスの利用者は、システム管理者、監査者、NECグループ社員、構内作業者、顧客である。NECグループ社員の利用者役割は、NECグループ社員、エリア利用者(管理者)、エリア利用者(社員、構内作業)のいずれかに分類される。構内作業者の利用者役割は、構内作業者、エリア利用者(社員、構内作業者)のいずれかに分類される。顧客の利用者役割は、エリア利用者(顧客)となる。

□NECグループ社員

社内利用者クライアントより、エリアの作成、更新、削除、及びエリア、フォルダの選択による参照操作を行うことができる。

□構内作業者

社内利用者クライアントより、エリア、フォルダの選択による参照操作を行うことができる。

□エリア利用者(管理者)

NECグループ社員がエリアを作成すると、そのエリア内におけるエリア利用者(管理者)となる。社内利用者クライアントより、業務データに関連する以下の操作と管理を行うことができる。

・フォルダの作成、更新、削除。
・フォルダの利用者となる社内作業者、及び顧客の登録、更新、削除。
・エリア利用者(社員、構内作業者)の操作権限を付与。
・フォルダの利用者として登録されたNECグループ社員に対しては、エリア利用者(管理者)権限を付与することができる。

□エリア利用者(社員、構内作業者)

エリア利用者(管理者)により、フォルダの利用者として登録されたNECグループ社員、構内作業者は、そのフォルダ内においてエリア利用者(社員、構内作業者)となる。社内利用者クライアントより、業務データに関連する操作を行うことができる。

構内作業者の場合は、エリア利用者(管理者)になることはできない。

□エリア利用者(顧客)

エリア利用者(管理者)により、フォルダの利用者として登録された顧客は、そのフォルダ内においてエリア利用者(顧客)となる。社外利用者クライアントより、業務データに関連する操作を行うことができる。

エリア利用者(管理者)になることはできない。

□システム管理者

社内用Webサーバ、社外用Webサーバのコンソールより、以下のTOEの運用管理を行うことができる。

・TOEの初期設定。
・TOEの起動と停止。

□監査者

社内用Webサーバのコンソールより、TOEの監査証跡の参照を行うことができる。

1.2.4 TOEの機能

本TOEが提供するサービス機能は、以下のとおりである。

【エリアメンテナンス機能】

エリアメンテナンス機能は、エリアの作成、更新、削除、及びフォルダの作成、更新、削除、フォルダ内のファイルの削除、エリアログの表示、出力を行う機能である。

【利用者メンテナンス機能】

利用者メンテナンス機能は、社内利用者と顧客の登録、更新、削除を行う機能である。

【アップロード依頼機能】

アップロード依頼機能は、エリア利用者(顧客)に対して、アップロードが行えるようにする機能である。アップロード依頼機能の処理の流れは以下のとおりである。

①エリア利用者(顧客)は、エリア利用者(社員、構内作業者)にアップロード依頼を要求。

②エリア利用者(社員、構内作業者)は、アップロード先のエリアとフォルダを決定し、ダウンロード許可者を指定。

③エリア利用者(顧客)に、アップロード依頼メールを通知。

【アップロード機能】

アップロード機能は、業務データのアップロードを行う機能である。業務データのアップロード後、ダウンロード依頼メールを通知する。

【ダウンロード機能】

ダウンロード機能は、業務データのダウンロードを行う機能である。業務データは、1度のみダウンロードすることが可能である。ダウンロードを許可された利用者全員が、ダウンロードを行うと、業務データは削除される。

【個人設定機能】

個人設定機能は、メールアドレスの変更を行う機能である。

【運用機能】

運用機能は、TOEの起動、停止、監査者の登録、削除、監査者パスワードの初期化、すべてのエリアログの表示・出力が行える機能である。

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「NECグループ セキュア情報交換サイト バージョン1.0 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 セキュア情報交換サイト バージョン1.0 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20年4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。

1.5.3 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

【識別認証機能】

TOEは、TOEへのアクセスに対する識別認証機能を提供する。

・エリア利用者(顧客)

ワンタイム URL による識別、PIN による認証が成功しなければならない。同一のワンタイム URL に対する PIN が異なる場合は、ワンタイム URL 毎に PIN の誤り回数をカウントするとともに、ワンタイム URL を失効とする。

・エリア利用者(社員、構内作業者)

ワンタイム URL による識別が成功しなければならない。ワンタイム URL 経由で TOE にアクセスし、社内認証サービスの認証に失敗した場合は、誤り回数をカウントするとともに、ワンタイム URL を失効とする。

・NECグループ社員、構内作業者

ユーザ ID による識別が成功しなければならない。

・システム管理者

URL による識別が成功しなければならない。

・監査者

URL による識別が成功しなければならない。

【監査機能】

TOEは、監査対象となる事象が発生した場合、監査記録を生成する。監査者は、監査機能を使用して、監査記録の参照、及び検索を行う。

【アクセス制御機能】

TOEは、TOEのすべての利用者に対して、その利用者役割毎に付与した権限に基づき、業務データと、その業務データを格納するエリア、フォルダに対して、アクセスの許可、不許可を行う機能を提供する。

【暗号機能】

TOEは、TOEのすべての利用者に対して、WebサーバとWebブラウザ間の通信データをSSL通信による、暗号化、復号するしくみにより、WebサーバとWebブラウザ間の通信データを保護する機能を提供する。

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
・アクセス制御
・識別・認証
・セキュリティ管理
・高信頼パス/チャネル

1.5.4 脅威

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2 想定する脅威

識別子	脅 威
T.SPOOFING(なりすまし)	インターネット上からアクセスする専門知識を持たない悪意のある第三者や、NECのイントラネット上からアクセスするTOEの利用者が、TOEの正当な利用者になりすまして、業務データを破壊、暴露するかもしれない。
T.ILLEGAL_ACCESS(不正なアクセス)	TOEの正当な利用者である、NECグループ社員、構内作業者、エリア利用者(管理者)、エリア利用者(社員、構内作業者)、エリア利用者(顧客)が、その利用者役割に対し、許可をしていない以下の操作を行うことで、業務データ、アップロードエリア情報、エリア利用者情報を破壊、暴露するかもしれない。 ・NECグループ社員ではないTOE利用者による、エリアの作成、更新、削除 ・エリア利用者(管理者)ではないTOE利用者による、フォルダの作成、更新、削除 ・エリア利用者(管理者)ではないTOE利用者による、フォルダ内への、利用者(NECグループ社員、構内作業者、顧客)の登録、更新、削除 ・エリア利用者(社員、構内作業者)ではなく、エリア利用者(顧客)でもないTOE利用者による、業務データのダウンロード、アップロード、削除
T. LISTEN-IN_NW_DATA (ネットワークデータ盗聴)	専門知識を持たない悪意のある第三者が、Webサーバとネットワーク上でやり取りされる業務データを盗聴したり、改ざんしたりすることで、業務データを暴露、破壊、改ざんするかもしれない。
T.MISDELIVERY (誤送信)	TOEの正当な利用者が、誤って違う顧客にTOEのURLの送信を行うことで、業務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1-3に示す。

表1-3 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_IDENTIFY (管理者識別)	TOEを利用するシステム管理者、監査者について、TOEにおける操作の記録を残すため、TOEによる識別を義務付ける。
P. AUDIT_LOG (監査記録)	TOEが生成する監査記録は、TOEの保護資産に対する不正操作の追跡を行うため、監査者のみが参照可能とする制限を行う。

1.5.6 構成条件

表1-4に、TOEの動作環境としてのハードウェア構成を示す。TOEは、表1-4を満たす動作環境で、正しく確実に動作する。

表1-5に、TOEの動作環境としてのソフトウェア構成を示す。TOEは表1-5に識別されたソフトウェア構成により、正しく動作する。

表1-4 TOE動作環境のハードウェア構成

端末・装置名	種別	説明
ストレージサーバ		
本体	ベンダ名	NEC
	製品名	iStorage NS460
	型名	NF8100-145A
	CPU	デュアルコアIntel Xeonプロセッサ 3GHz
	メモリ	3GB(2GB+1GB)
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(標準)
	増設ディスク	物理容量2100GB(300GB×7)RAID5
社内用Webサーバ		
本体	ベンダ名	NEC
	製品名	Express5800/120Ri-2 (XD2/3G(4))
	型名	N8100-1318
	CPU	デュアルコアIntel Xeonプロセッサ 3GHz × 2CPU
	メモリ	4GB(2GB×2)

端末・装置名	種別	説明
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(標準)
社外用Webサーバ		
本体	ベンダ名	NEC
	製品名	Express5800/120Ri-2 (XD2/3G(4))
	型名	N8100-1318
	CPU	デュアルコアIntel Xeonプロセッサ 3GHz × 2CPU
	メモリ	4GB(2GB×2)
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(標準)
データベースサーバ		
本体	ベンダ名	NEC
	製品名	Express5800/140Re-4(XMPD/3.40G(16))
	型名	N8100-1276
	CPU	デュアルコアIntel Xeon　プロセッサ 3.40GHz×4
	メモリ	4GB(2GB×2)
	LAN	1000BASE-T×2(標準)
	外部ストレージ	1148GB
社内利用者クライアント		
本体	表1-5の社内利用者クライアントで定義されたOSが動作可能な本体	
社外利用者クライアント		
本体	表1-5の社外利用者クライアントで定義されたOSが動作可能な本体	

表1-5　TOE動作環境のソフトウェア構成

端末名		
ベンダ名	製品名	種別
ストレージサーバ		
Microsoft	Windows Storage Server 2003 R2	OS
社内用Webサーバ		
Microsoft	Windows Server 2003 R2 _Standard Edition	OS
社外用Webサーバ		
Microsoft	Windows Server 2003 R2 _Standard Edition	OS
データベースサーバ		
Microsoft	Windows Server 2003 R2_Standard Edition	OS

端末名		
ベンダ名	製品名	種別
Oracle	Oracle Database 10g Standard Edition 1 Processor	DBMS
社内利用者クライアント		
Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS
社外利用者クライアント		
Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS

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1-6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1-6 TOE使用の前提条件

識別子	前提条件
A. DATACENTER (データセンタ)	社内用Webサーバ、社外用Webサーバ、データベースサーバ、ストレージサーバ、社内認証サーバ、社内メールサーバは、入退出管理を実施した許可のない者の入室を禁止し、入室者の行動を監視しているデータセンタに設置する。
A.NETWORK (ネットワーク)	社内用Webサーバは、適切に設定した社内用ファイアウォール2によってイントラネットからのアクセスを制限されている。 社外用Webサーバは、適切に設定した社外用ファイアウォールによってインターネットからのアクセスを制限されている。
A.SYSTEM_ADMIN (システム管理者の利用制限)	システム管理者の操作は、社内用Webサーバ上、及び社外用Webサーバ上のコンソールのみで行う。
A.AUDIT_ADMIN (監査者の利用制限)	監査者の操作は、社内用Webサーバ上のコンソールのみで行う。
A.ADMINISTRATO	TOEの運用責任者、システム管理者、監査者、ストレージ

R(信頼できる管理者)	管理者、データベース管理者は、それぞれの役割に付与した行為のみを行い、悪意のある行為を行わない。

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に示す。

・NECグループ セキュア情報交換サイト バージョン1.0 運用マニュアル バージョン1.04　2008年1月8日

・NECグループ セキュア情報交換サイト バージョン1.0　利用マニュアル 第1.03版　2008年2月28日

・NECグループ セキュア情報交換サイト バージョン1.0　利用マニュアル (NECグループ利用者版) 第1.03版　2008年2月28日

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9月に始まり、平成20年4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12月に開発者サイトで開発者のテスト環境を使用し、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構成を図2-1に示す。

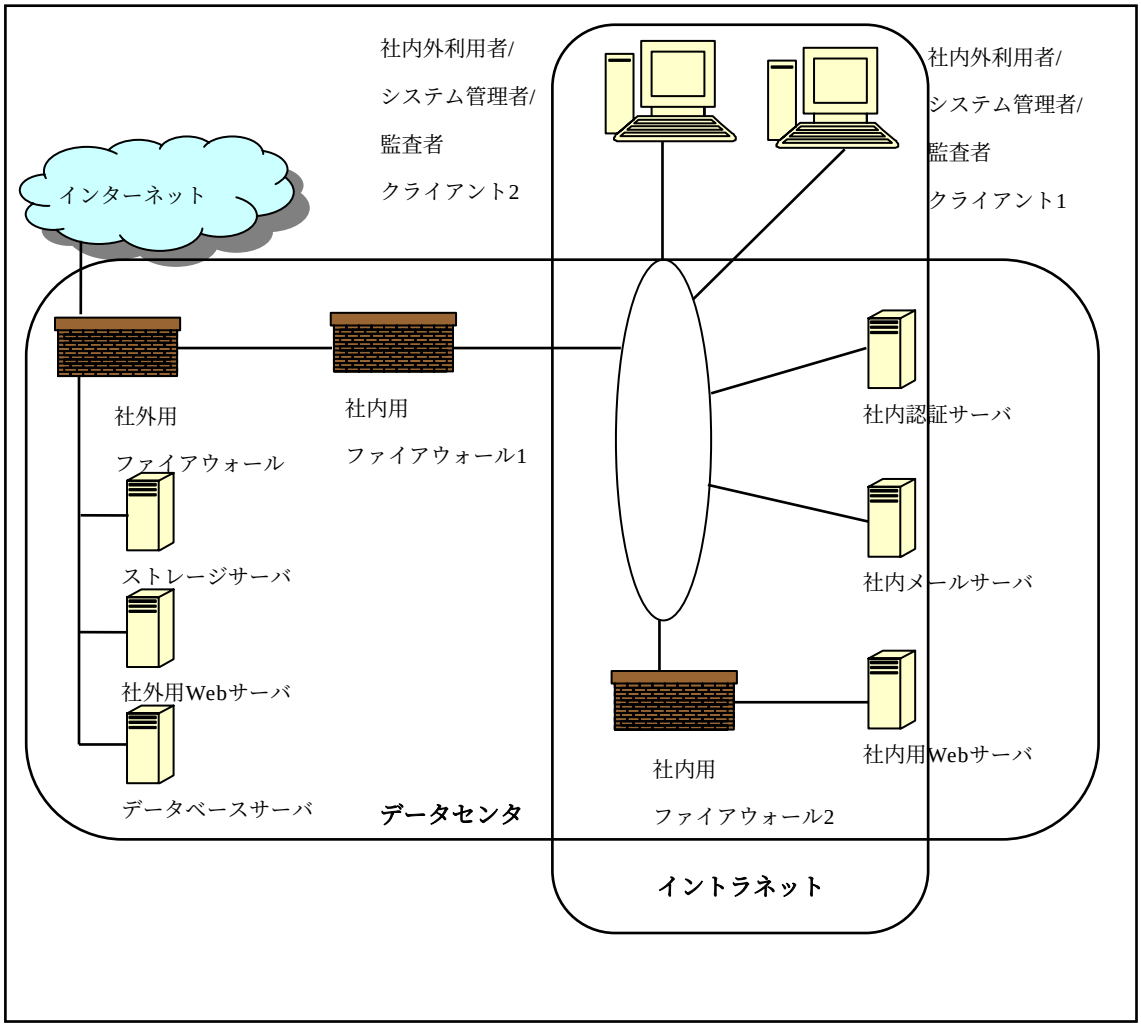

図2-1　評価者テストの構成図

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の構成を図2-1に示す。評価者テストはSTにおいて識別されているTOE構成と同等のTOEテスト環境で実施されている。

なお、社外利用者、システム管理者、監査者の端末の接続形態が実際の適用環境と異なるが､評価を行う上で同等であることを評価者が確認している。

b.テスト手法

テストには、以下の手法が使用された。

①利用者役割毎に端末を操作し、画面及びログ情報を検査。

②送受信データを取得し､その内容及び不正な入力値に対する応答を検査。

③脆弱性検査ツールによりOSやWebサーバの公知の脆弱性を検査。

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30項目､侵入テストを19項目、計49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 主要な役割を果たしているセキュリティ機能
② 新規性のあるセキュリティ機能
③ 異なるインタフェース種別から利用される機能
④ 公知の情報源から類似の脆弱性の存在が疑われるセキュリティ機能

d.結果

実施したすべての評価者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。

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を確認している。
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明確に定義されてい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の必要性を確認している。
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が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
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSFI	TOE Security Functionality Interface

本報告書で使用された用語を以下に示す。

エリア	業務データを管理する最上位の単位。エリアの配下に複数のフォルダを持つ。エリアは複数作成が可能。
エリア利用者	特定のエリア内のフォルダを利用する許可を得ている人物(NECグループ社員、構内作業者、顧客)。
顧客	NECのイントラネットの利用が許可されていない取引先の会社社員。
構内作業者	NECのイントラネットの利用を許可された協力会社社員。
社内認証サーバ	社内認証サービスが稼動するサーバ。
社内認証サービス	NEC社内利用者のユーザID、パスワードを一元管理し、NECグループの各種システムに認証情報を提供するサービス。
社内利用者	NECグループ社員と構内作業者。
フォルダ	エリア内に業務データを保管するための単位。フォルダは複数作成が可能。

ワンタイムURL	一定時間、利用可能なURL。フォルダに対する宛先となる。ワンタイムURLには、識別情報を含む。

6 参照

[1] NECグループ セキュア情報交換サイト バージョン1.0 セキュリティターゲット バージョン 1.14（2008年4月3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 Revision 1 September 2006 CCMB-2006-09-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional components Version 3.1 Revision 1 September 2006 CCMB-2006-09-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components Version 3.1 Revision 1 September 2006 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 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: セキュリティ保証コンポーネント バージョン3.1 改訂第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 Revision 1 September 2006 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 改訂第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 セキュア情報交換サイト 評価報告書 第2版 2008年4月4日 みずほ情報総研株式会社 情報セキュリティ評価室