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9月18日** (IT**認証**7171)
認証番号	C0157
認証申請者	**日本電気株式会社**
TOE**の名称**	WebOTX Application Server **高信頼実行ユニット**
TOE**のバージョン**	7.11
PP**適合**	**なし**
適合する保証パッケージ	EAL2**及び追加の保証コンポーネント**ALC_FLR.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

「WebOTX Application Server 高信頼実行ユニット」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 5
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 7
1.5.4 脅威 8
1.5.5 組織のセキュリティ方針 8
1.5.6 構成条件 8
1.5.7 操作環境の前提条件 9
1.5.8 製品添付ドキュメント 10
2 評価機関による評価実施及び結果 11
2.1 評価方法 11
2.2 評価実施概要 11
2.3 製品テスト 11
2.3.1 開発者テスト 11
2.3.2 評価者テスト 12
2.4 評価結果 15
3 認証実施 16
4 結論 17
4.1 認証結果 17
4.2 注意事項 21
5 用語 22
6 参照 25

1 全体要約

1.1 はじめに

この認証報告書は、「WebOTX Application Server 高信頼実行ユニット」（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「1.5.9 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：　WebOTX Application Server 高信頼実行ユニット
バージョン：　7.11
開発者：　日本電気株式会社

1.2.2 製品概要

本TOEが属する「WebOTX Application Server」は、J2EE1.4規格（JavaTM 2 platform Enterprise Edition Specification V1.4）に準拠したアプリケーションサーバである。TOEは「WebOTX Application Server」の一部であり、OLTPモニタ、J2EEコンテナ、管理機構、の3つのコンポーネントから成り、以下のサービス（機能）を利用者に対し提供している。

1）ユーザAP 実行サービス
ユーザAP 実行サービスは、J2EEコンテナによりユーザAPを利用可能にするサービス機能である。
2）利用者管理サービス

利用者管理サービスは、管理機構によりWebOTX 利用者の管理を可能にするサービス機能である。

3）ユーザAP 配備サービス

ユーザAP 配備サービスは、管理機構およびJ2EE コンテナによりユーザAPの配備を可能にするサービス機能である。

また、TOEは上記サービスに付随する以下のセキュリティ機能を提供している（各機能の詳細は「1.2.4　TOEの機能」を参照の事）。

1）一般利用者に対する識別認証機能
2）一般利用者に対するアクセス制御機能
3）WebOTX 管理者に対する識別認証機能
4）WebOTX 管理者に対する利用者管理機能
5）WebOTX 管理者に対するユーザAP 配備制御機能
6）ユーザAP に対するユーザAP 復旧機能

なお、本評価ではBASIC認証且つファイルレルムの構成のみ評価されており、それ以外の構成は評価対象外である。またJSPやServletからのJava API経由でのBASIC認証も評価対象外である。

1.2.3　TOEの範囲と動作概要

本TOE は以下の図1-1に示すとおり、点線で囲まれたOLTPモニタ、J2EEコンテナ、管理機構の3つのコンポーネントから構成される。

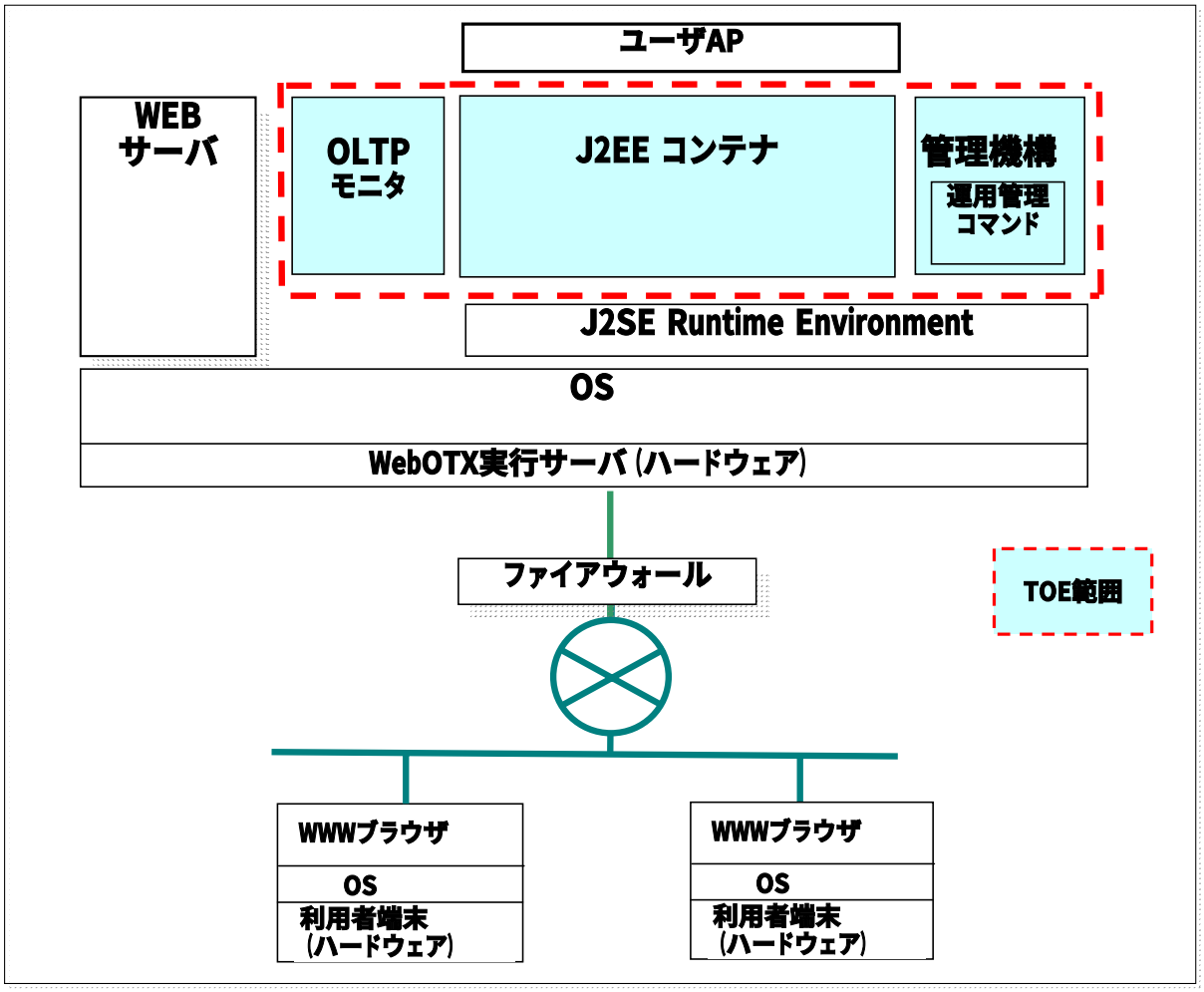

図1-1　TOEの物理的範囲

本評価はWindows、HP、Linuxにおいて実施され、図1-1に示されたプラットフォーム毎のTOE範囲外のコンポーネントの詳細は下記の通りとなる。

（1）Windows版

○ハードウェア

本体：NEC Express 5800シリーズ

メモリ：1GB以上（OS等の使用を含む）

CPU：Intel® Xeon®

ハードディスク：１GB以上（TOEのみでの使用量）

○ソフトウェア

OS：　Windows Server 2003 R2, Standard Edition（32ビット版）

その他：J2SE Development Kit 5.0

（2）HP版

○ハードウェア

本体：NEC NX7700iシリーズ
メモリ：2GB以上（OS等の使用を含む）
CPU：Intel® Itanium®
ハードディスク：１GB以上（TOEのみでの使用量）
○ソフトウェア
OS：HP-UX 11i v2
その他：J2SE Development Kit 5.0

（３）Linux版
○ハードウェア
本体：NEC Express 5800シリーズ
メモリ：1GB以上（OS等の使用を含む）
CPU：Intel® Xeon®
ハードディスク：１GB以上（TOEのみでの使用量）
○ソフトウェア
OS：Red Hat Enterprise Linux ES 4.0
その他：J2SE Development Kit 5.0

（４）OS共通
ソフトウェア：
Webサーバ：WebOTX　WebServer 2.0

（５）ファイアウォール
ハードウェア：
特定のポートおよび特定のプロトコル以外の通信を遮断する機能を有するもの。

（６）利用者端末
ハードウェア：Internet Explorer 6.0が動作するマシン
ソフトウェア： Internet Explorer 6.0

TOEの提供するサービス、及びセキュリティ機能は「1.2.2　製品概要」に記した通りであるが、基本的なサービスとセキュリティ機能の動作フローは以下の通りであり、図1-2で示した矢印の流れに従う。

・ユーザAP実行サービスは、一般利用者により呼び出され、一般利用者識別認証機能、ユーザAPアクセス制御機能が順に実行される。
・利用者管理サービスは、WebOTX管理者により呼び出され、WebOTX管理者識別認証機能、利用者管理機能が順に実行される。
・ユーザAP配備サービスは、WebOTX管理者により呼び出され、WebOTX管理

者識別認証機能、ユーザAP配備制御機能が順に実行される。

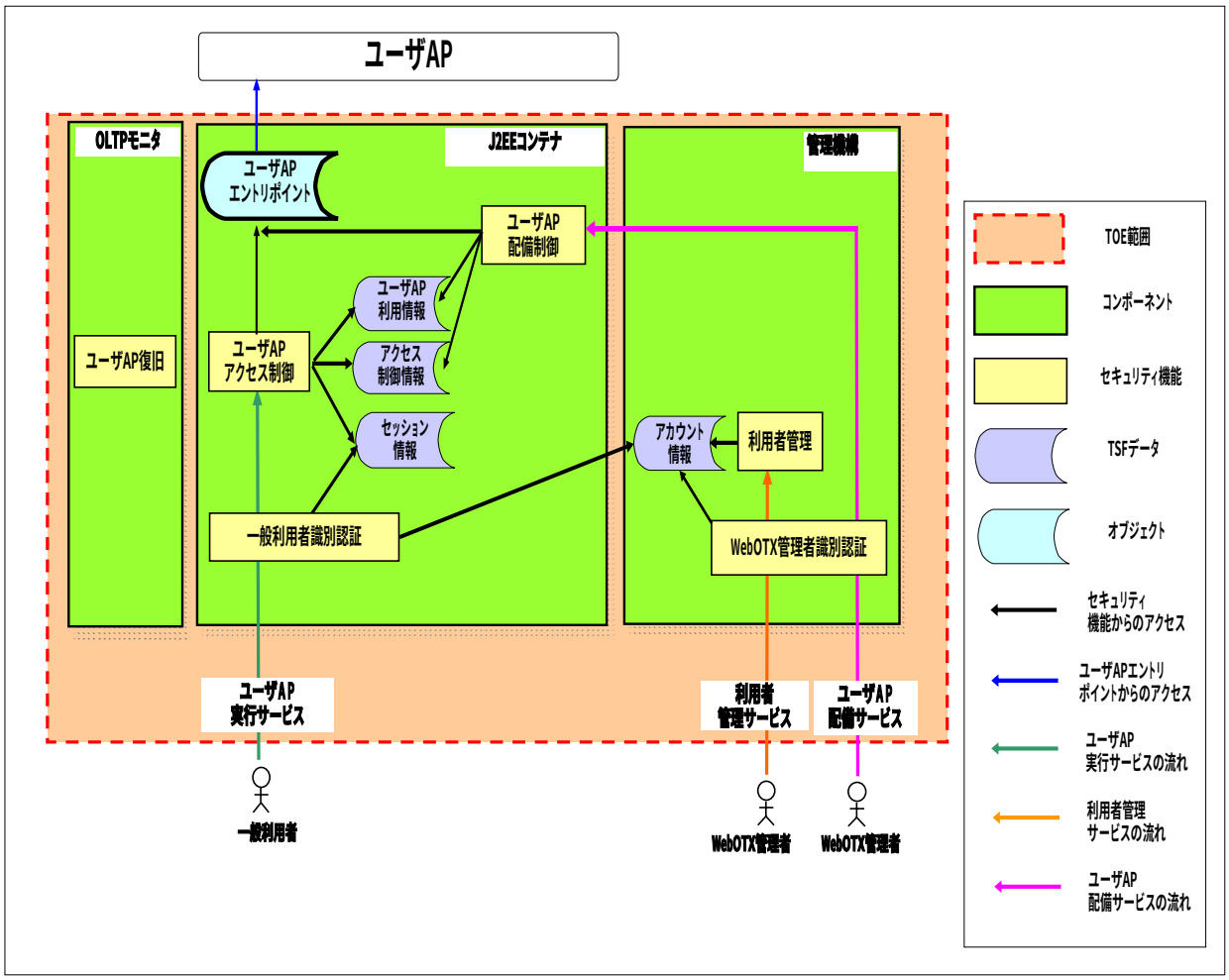

図1-2　TOEの論理的範囲

1.2.4　　TOEの機能

TOEの提供するサービスは「1.2.2　製品概要」に示した通りであるため、以下においてTOEが提供するセキュリティ機能詳細のみ示す。

1）一般利用者に対する識別認証機能
一般利用者がユーザAP実行サービスを利用する際に動作し、TOEに登録された一般利用者であるかのチェックを行い、認証に成功すれば一般利用者ロールを付与する。なお、本評価ではBASIC認証且つファイルレルムの構成のみ評価されており、それ以外の構成は評価対象外である。またJSPやServletからのJava API経由でのBASIC認証も評価対象外である。

2）一般利用者に対するアクセス制御機能
一般利用者がユーザAP実行サービスを利用する際に動作し、一般利用者ロー

ルとユーザAP許可利用者ロールを比較し、許可された場合にのみユーザAPエントリポイントへのアクセスを許可する。

3）WebOTX管理者に対する識別認証機能
WebOTX管理者が利用者管理サービスまたはユーザAP配備サービスを呼び出す際に最初に動作し、WebOTX管理者であるかのチェックを行う。

4）WebOTX管理者に対する利用者管理機能
WebOTX管理者が利用者管理サービスを利用する際に動作し、利用者情報の登録／更新／削除を行う。

5）WebOTX管理者に対するユーザAP配備制御機能
WebOTX管理者がユーザAP配備サービスを呼び出す際に動作し、使用中のユーザAPを誤って再配備、または配備解除しないようチェックを行う。

6）ユーザAPに対するユーザAP復旧機能
OLTPモニタにより、TOE上のJ2EEコンテナが異常終了していないかの確認を行う。OLTPモニタはユーザAP制御データを含むJ2EEコンテナが異常終了したことを検知した場合、自動的にJ2EEコンテナの再起動を行う。

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「WebOTX Application Server 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、「WebOTX Application Server 高信頼実行ユニット バージョン7.11 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、EAL2及び追加の保証コンポーネントALC_FLR.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、「1.2.4 TOE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。

・識別・認証
・セキュリティ管理
・アクセス制御
・セキュリティ機能保護

-

1.5.4 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

表1-1 想定する脅威

識別子	脅 威
T.ILLEGAL_LOGON（不正なログオン）	TOEに一般利用者として登録されていない者が、一般利用者になりまし、TOEが一般利用者に提供しているサービスを不正に利用するかもしれない。 または、TOEにWebOTX管理者として登録されていない者が、WebOTX管理者になりすまし、TOEがWebOTX管理者に提供しているサービスを不正に利用するかもしれない。その結果、不正に情報を取得したり改ざんしたりする可能性がある。
T.ILLEGAL_ACCESS（不正なユーザAP利用）	識別認証された一般利用者が、許可されていないユーザAP実行サービスを利用するかも知れない。その結果、ユーザAP実行サービスを利用して、許可されていない情報を取得する可能性がある。
T.MISTAKE（誤操作）	WebOTX管理者が、誤操作により動作中のユーザAPを配備解除または再配備するかもしれない。 その結果、一般利用者に提供していたユーザAP実行サービスが停止したり中断したりする。
T.PROCESSTERM（セキュリティ機能の長時間停止）	ユーザAPまたはJREの不具合等により、ユーザAP実行サービスを提供しているJ2EEコンテナのプロセスが異常終了するかもしれない。 その結果、J2EEコンテナの提供するユーザAP利用サービス及び一般利用者識別認証機能、ユーザAPアクセス制御機能、ユーザAP配備制御機能が停止し、一般利用者が長時間利用できない状態になる可能性がある。 停止中は一般利用者がTOEにアクセスする手段がないため、TOEはアンセキュアな状態にならない。

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はない。

1.5.6 構成条件

本TOEは、「1.2.3 TOEの範囲と動作概要」に示された各種ハードウェア、ソ

フトウェア構成で動作する。

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1-2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1-2 TOE使用の前提条件

識別子	前提条件
A.SECURECHANNEL（セキュア通信）	通信を秘匿する必要性がある場合、WebOTX管理者はHTTPSを使用するようWebサーバを設定するものとする。
A.OSJAVA（OS、JavaVMのセキュリティ）	システム管理者は、TOEが動作するOS及びJREに対し、適時必要なセキュリティパッチの適用を行うことにより、OS、JREのセキュリティに関する信頼性を維持するものとする。
A.WEBOTX_ADMIN（信頼できるWebOTX管理者）	WebOTX管理者は悪意を持たず、TOEの運用管理を適切に行える能力を持っている。 WebOTX管理者は、WebOTX管理者自身及び一般利用者に対し、推測されにくいパスワードを設定するものとする。 またWebOTX管理者は一般利用者に対し、設定したIDとパスワードを他人に漏れない方法で伝達するものとする。 WebOTX管理者はユーザAP許可利用者ロールが設定されているユーザAPを配備するものとする。
A.SYS_ADMIN（信頼できるシステム管理者）	システム管理者は悪意を持たず、内部ネットワーク、ファイアウォール及びAP実行サーバ上のTOE以外のSWの運用管理を行える能力を持っている。
A.ID_PASSWORD（IDとパスワードの適切な管理）	WebOTX管理者、一般利用者、システム管理者は、IDとパスワードを適切に管理し他人に漏らさないものとする。
A.FIREWALL（ファイアウォール）	システム管理者はTOEを導入するネットワークと他のネットワークとの境界にファイアウォールを設置し、ユーザAP実行サービスが使用するHTTPプロトコルおよびHTTPSプロトコルのポートのみ許可するようにする。
A.AREA（サーバエリア管理）	システム管理者は、サーバエリアを、WebOTX管理者を含む許可された者のみが入退出できるよう管理するものとする。

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1-3に示す。

表1-3 TOEのガイダンス文書

種類	ガイダンス文書名
利用者準備ガイダンス	WebOTX Application Server 利用者準備ガイダンス Ver1.7 （WebOTXAS-AGD_PRE-1.7）
利用者操作ガイダンス	WebOTX Application Server 利用者操作ガイダンス Ver1.7 （WebOTXAS-AGD_OPE-1.7）

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20年1月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、ライフサイクルの各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成20年2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 開発者テスト

1) 開発者テスト環境

「2.3.2 1)評価者テスト環境」を参照の事（厳密には評価者テスト環境とは利用者端末の台数が異なるが、利用者端末の台数はTSFの機能に影響しない）。

2) 開発者テスト概説

開発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

開発者が実施したテストの構成に関しては上記「1) 開発者テスト環境」を

参照の事。開発者テストは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クライアントのブラウザよりのテスト

②コンソールからのコマンドテスト

c.実施テストの範囲

テストは開発者によって1つのOS毎に63項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 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。

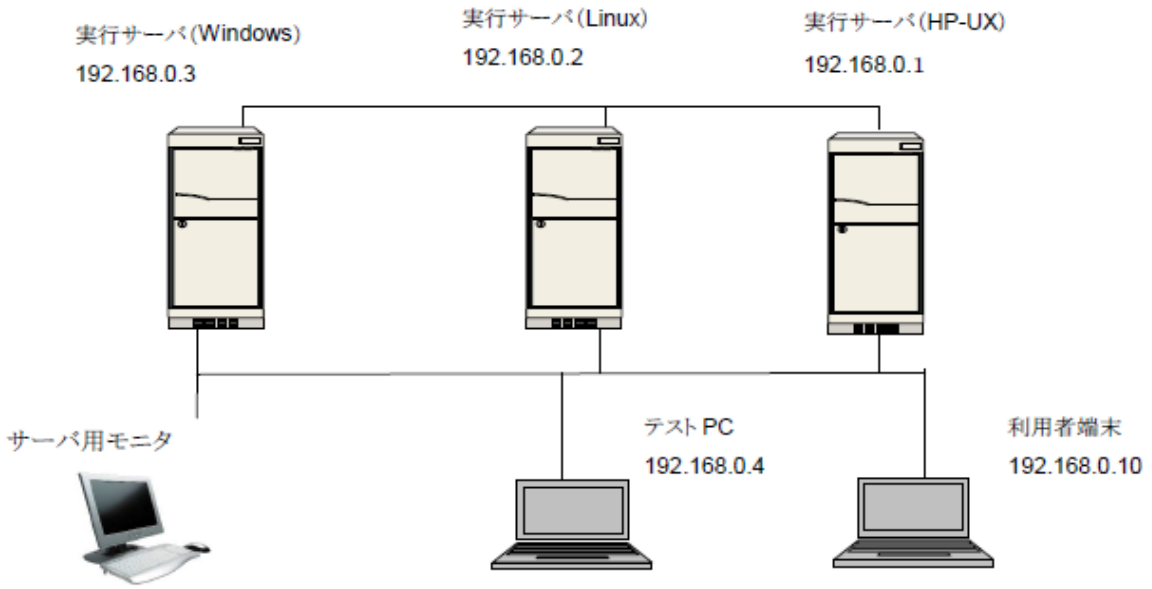

図2 -1　TOEの機器構成

各機器のハードウェア構成は、以下の表2-1の通りである。

表2 -1　ハードウェア構成

機器	種別	説明
TOE 実行サーバ（Windows 版）	本体	NEC Express 5800 シリーズ （型名：NEC Express 5800/120Rg-1）
	CPU	Intel(R) Xeon(R) 1.6GHz
	メモリ	3.25GB
	HDD	300GB
TOE 実行サーバ（HP-UX 版）	本体	NEC NX7700i シリーズ （型名：NEC NX7700i/3012E-2）
	CPU	Intel(R) Itenium 2 Family Processor 1.3GHz
	メモリ	2GB
	HDD	50GB
TOE 実行サーバ（Linux 版）	本体	NEC Express 5800 シリーズ （型名：NEC Express 5800/120Rg-1）
	CPU	Intel(R) Xeon(R) 1.6GHz
	メモリ	3.25GB
	HDD	300GB
利用者端末	Internet Explorer 6.0 が動作するマシン	
テスト用 PC	Internet Explorer 6.0 が動作するマシン	

各機器のソフトウェア構成は、以下の表2-2の通りである。

表2 -2　ソフトウェア構成

機器名	種別	製品名
TOE 実行サーバ（Windows 版）	TOE	WebOTX Application Server Standard Edition
	OS	Microsoft Windows Server 2003 R2, Standard Edition SP2
	AP	J2SE Development Kit 5.0 Update 13
	Webサーバ	WebOTX WebServer 2.0
TOE 実行サーバ（HP-UX版）	TOE	WebOTX Application Server Standard Edition
	OS	HP-UX 11i v2(B.11.23)
	AP	J2SE Development Kit 5.0 Update 7
	Webサーバ	WebOTX WebServer 2.0
TOE 実行サーバ（Linux版）	TOE	WebOTX Application Server Standard Edition
	OS	Red Hat Enterprise Linux ES release 4(Nahant Update 6)
	AP	J2SE Development Kit 5.0 Update 13

機器名	種別	製品名
	Webサーバ	WebOTX WebServer 2.0
利用者端末	AP	Internet Explorer 6.0
テスト用PC	AP	Internet Explorer 6.0、Teraterm 4.5.1、Wireshark 0.99.7

また、テスト時に評価者は以下の表2-3に示すツールを使用している。

表2 -3　使用ツール

種別	製品名
キャプチャツール	Wireshark-setup-0.99.7.exe
ターミナルエミュレーター（通信ソフト）	teraterm_utf8-4.51.exe

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 クライアントのブラウザよりのテスト
② コンソールからのコマンドテスト
③ ログ等によるTOE内部動作の観察

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13項目、侵入テストを4項目、開発者テストのサンプリングによるテストを36項目、計53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 開発者がテストしていないパラメタのテスト
② 複数同時処理に関するテスト
③ SFRを網羅する上で不足している部分をテスト

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 参考文献（IPA公開情報等）よりテスト項目を考案
③ 評価者独自の知見に基づき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。

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EAL2及び追加の保証コンポーネントALC_FLR.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.2.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ALC_CMS.2.1E	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。
ALC_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ALC_FLR.1.1E	評価はワークユニットに沿って行われ、欠陥修正手続き証拠資料がすべてのセキュリティ欠陥を追跡するために使用される手続き、及びTOE利用者に必要な情報を提供するための手段を含み、この手続きの適用により、欠陥訂正方法の調査状況と同時に各々のセキュリティ欠陥の性質と影響に関する記述が提供されることを確認している。また、当評価に至るまでになされた所見報告書による指摘も適切と判断される。
開発	**適切な評価が実施された**
ADV_FSP.2.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。

ADV_FSP.2.2E	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。
ADV_TDS.1.1E	評価はワークユニットに沿って行われ、TOE設計にてすべてのサブシステムが記述され、各サブシステムの特性が識別されていることを確認している。
ADV_TDS.1.2E	評価はワークユニットに沿って行われ、TOE設計にすべての機能要件が含まれ、具体化されていることを確認している。
ADV_ARC.1.1E	評価はワークユニットに沿って行われ、アーキテクチャ設計に自己保護、ドメイン分離、非バイパス性が記述され、TSFが保護されてい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_COV.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテスト項目が正確にTFSIと関連付けられていることを確認している。

ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	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、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、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、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、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、本評価時に行われた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.2.1E	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、開発者テストと同等の資源が提供されていることを確認している。
AVA_VAN.2.2E	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、関連する脆弱性が存在しないことを確認している。
AVA_VAN.2.3E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。

AVA_VAN.2.4E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

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
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

本報告書で使用された用語を以下に示す。

アプリケーションサーバ	サーバ上でJ2EEアプリケーションを動作させるためのソフトウェア。
WebOTX Application Server	NEC製のアプリケーションサーバ製品。 本STの対象であるTOEを含む。
プロセス	本STでは、OSによって管理されるプログラムの実行空間を指す。
Java	Sun Microsystems社が開発したプログラミング言語。
JavaVM	Java Virtual Machineの略。 Javaアプリケーションを動作させるための仮想マシン。様々なOS上でJavaアプリケーションを動作させるために、プラットフォームの差異を埋める機能を持つ。
JavaAPI	Java Application Program Interfaceの略。 Javaアプリケーションから利用できるソフトウェア部品の集まり。
J2EE	Java 2 Enterprise Editionの略。 企業用大規模 Web アプリケーションの機能を提供する Java API セット。
JDK	J2SE Development Kitの略。 Javaアプリケーションの開発環境。

JRE	J2SE Runtime Environmentの略。 Java アプリケーションを動作させるための実行環境。 Java VM と Java API から構成される。
J2EE アプリケーション	J2EE の仕様に基づいて作成されたアプリケーション。
J2EE コンテナ	J2EE アプリケーションを動作させる実行基盤としてのソフトウェア。J2SE Runtime Environment上で動作する。
EJB	Enterprise Java Beansの略。 業務ロジックの機能を提供する Javaアプリケーションをコンポーネント化（部品化）したもの。
HTTP	HyperText Transfer Protocol の略。 Web サーバと WWWブラウザ間の通信で利用するプロトコル。
HTTPS	Hypertext Transfer Protocol Security の略。 HTTP と SSL を組み合わせ、Web サーバと WWWブラウザ間でセキュアな通信をするプロトコル。
SSL	Secure Socket Layerの略。 インターネット上で情報を暗号化して通信を行うプロトコル。
WebOTX実行サーバ	TOEがインストールされ動作する、物理的なサーバマシン。
WebOTX利用者	TOEを利用する者。一般利用者およびWebOTX管理者を指す。
開発者	TOE上で動作するユーザAPを開発する者。
一般利用者	TOEが提供するユーザAP実行サービスを利用する者。
WebOTX管理者	TOEを管理する者。 TOE及びサーバエリア内の資産に対する十分なスキルを持つ。
システム管理者	サーバエリア内のHW、SW、ネットワークの管理責任者。 これらを適切に設定し、維持管理する責任を持つ。
配備	ユーザAPをアプリケーションサーバ上で使用可能にすること。 本STでは、ユーザAPエントリポイントを操作し、TOE上にユーザAP制御データを生成する操作を指す。
配備解除	ユーザAPをアプリケーションサーバ上から削除すること。 本STでは、TOE上からユーザAP制御データを削除する操作を指す。
運用	TOEが提供するサービスを維持する為に必要な定常時または異常時の作業全般を指す。
利用者端末	一般利用者がTOEを利用するために使用する端末。TOEへ

	の接続には、WWWブラウザまたはSOAPクライアントのいずれかの方法を取る。
クライアント	利用者端末上で動作し、TOE上のユーザAPに接続する機能を持つソフトウェア。
Webサーバ	WWWブラウザから一般利用者の要求を受付け、TOEが提供するユーザAPに接続する機能をもつ。
WWWブラウザ	利用者端末上で動作するクライアントであり、Webサーバを経由しTOEが提供するユーザAPに接続する機能を持つ。 本STではWWWブラウザを、SOAPクライアントと同様の機能として扱う。
ユーザAP	開発者によって作成され、一般利用者に対しサービスを提供する為のアプリケーション。
ユーザAPエントリポイント	TOEからユーザAPを制御する際に使用するオブジェクト。
ユーザAP制御データ	ユーザAPを利用する際に必要な利用者データ。
運用管理コマンド	TOEの利用者管理およびユーザAPの配備／配備解除を行うための専用コマンド。
コンソール画面	運用管理コマンドを実行する際に使用するOSが提供する入力画面。
ログイン要求画面	ユーザAP利用時に利用者ID、パスワードを入力する画面。 WWWブラウザの機能により表示される。
サーバエリア	WebOTX実行サーバが設置された部屋。
外部ネットワーク	サーバエリア外のイントラネットまたはインターネットを指す。内部ネットワークとの通信はファイアウォールによって制御される。

6 参照

[1] WebOTX Application Server セキュリティ ターゲット バージョン 1.6（2008年4月14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] WebOTX Application Server 高信頼実行ユニット バージョン7.11 評価報告書 第2版 2008年4月15日　株式会社電子商取引安全技術研究所　評価センター