WebOTX Application Server
セキュリティ ターゲット

バージョン: 1.6

WebOTXAS-ST-1.6

2008 年 04 月 14 日

日本電気株式会社

NEC

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		
1.0	初版	-	-	2007/09/03	日本電気株式会社
1.1		1.4.6 7.1.1	文言修正 ・ユーザ AP に対応づけられた→ユーザ AP 毎に決められた	2007/09/06	日本電気株式会社
1.1		6.1.3	文言修正・ FDP_ACF.1.2a および FDP_ACF.1.3a	2007/09/06	日本電気株式会社
1.1		1.4.7	文言修正 ・利用者アクセス制御方針→利用者データアクセス制御方針 a ・利用者管理機能の説明 ・ユーザ AP 配備制御機能の説明 ・ログイン要求画面→ログイン要求画面	2007/09/06	日本電気株式会社
1.1		1.4.7	文言追加 用語にログイン要求画面を追加	2007/09/06	日本電気株式会社
1.1		1.4.5 1.4.7	文言修正 1.4.5 の表 5 におけるオブジェクトの説明を修正。	2007/10/28	日本電気株式会社
1.1		3.3.3 4.2 4.3.1	VAW-EOR-0001-00 の指摘に対する反映 ・A.USERAP を削除 ・OM.USERAP を削除 表 6 を修正	2007/10/31	日本電気株式会社
1.1		3.3.1 4.2	VAW-EOR-0002-00 および VAW-EOR-0008-00 の指摘に対する反映 ・A.OSJAVA の文言修正 ・OM.OSJAVA の文言修正	2007/10/31	日本電気株式会社

1.1		1.3.2 1.4.7 3.1 4.1 4.3.2 6.3.1 7.1.6	VAW-EOR-0003-00 の指摘に対する反映 ・文言修正	2007/10/31	日本電気株式会社
1.1		6.1.4	VAW-EOR-0004-00 の指摘に対する反映 ・FPT_FLS.1 を削除	2007/10/31	日本電気株式会社
1.1		1.4.2 1.4.6	VAW-EOR-0005-00 の指摘に対する反映 ・ 表 5 の文言修正 ・用語統一	2007/10/31	日本電気株式会社
1.1		3.2 4.3.2	VAW-EOR-0006-00 の指摘に対する反映 ・ 説明追加および文言修正	2007/10/31	日本電気株式会社
1.1		4.3.1 4.3.2	VAW-EOR-0007-00 の指摘に対する反映 ・ A.WEBOTX_ADMIN への対応関係を修正 ・表 6 の対応関係を修正	2007/10/31	日本電気株式会社
1.1		4.3.2	VAW-EOR-0009-00 の指摘に対する反映 ・文言修正	2007/10/31	日本電気株式会社
1.1		6.3.1	VAW-EOR-0010-00 の指摘に対する反映 ・文言修正	2007/10/31	日本電気株式会社
1.1		6.3.1	VAW-EOR-0011-00 の指摘に対する反映 ・文言修正	2007/10/31	日本電気株式会社
1.1		6.1.2 6.3.1 6.3.2 7.1 7.1.4	VAW-EOR-0012-00 の指摘に対する反映 ・ FMT_MOF.1 を削除 ・ FMT_MSA.1a を削除 ・ FMT_MSA.3a を削除 ・FMT_MSA.1、FMT_MSA.3、FMT_MTD の割り当てを変更	2007/10/31	日本電気株式会社

1.1		6.1.2	VAW-EOR-0013-00 の指摘に対する反映 ・表 15 および 7.1.4 の文言を修正	2007/10/31	日本電気株式会社
1.1		6.3.1	VAW-EOR-0014-00 の指摘に対する反映 3.1 および 4.3.2 の文言を修正	2007/10/31	日本電気株式会社
1.1		7.1.3	VAW-EOR-0015-00 の指摘に対する反映 7.1.3 の文言修正 表 16 修正 用語追加	2007/10/31	日本電気株式会社
1.1		6.1.3	VAW-EOR-0016-00 の指摘に対する反映 6.1.3 の表 19 修正	2007/10/31	日本電気株式会社
1.1		6.1.3	VAW-EOR-0017-00 の指摘に対する反映 6.1.3 の文言修正	2007/10/31	日本電気株式会社
1.1		7.1.2	VAW-EOR-0017-00 の指摘に対する反映 7.1.2 の文言追加	2007/10/31	日本電気株式会社
1.1		7.1.2	VAW-EOR-0018-00 の指摘に対する反映 ・文言追加	2007/10/31	日本電気株式会社
1.2		4.1 6.3.1	VAW-EOR-0014-01 の指摘に対する反映 ・文言修正 ・OM.OSDETECT 追加	2007/11/15	日本電気株式会社
1.2		6.1.3	VAW-EOR-0016-01 の指摘に対する反映 ・文言修正	2007/11/15	日本電気株式会社
1.2		6.3.1	VAW-EOR-0019-01 の指摘に対する反映 6.3.1 の文言修正 FMT_MSA.3 の削除および注釈追加	2007/11/15	日本電気株式会社
1.2		6.1.2	VAW-EOR-0020-01 の指摘に対する反映 ・文言修正	2007/11/15	日本電気株式会社
1.3		6.1.3	VAW-EOR-0015-01 およ	2007/11/30	日本電気株式会社

			び VAW-EOR-0016-03 の指摘に対する反映 ・表 16 修正		
1.3		6.1.2	VAW-EOR-0020-01 の指摘に対する反映 ・表 13 修正	2007/11/30	日本電気株式会社
1.3		4.2 4.3.2	VAW-EOR-0021-00 の指摘に対する反映 OM.WEBOTX_ADMIN を修正 表 6 および 4.3.2 の文言を修正 表 19 の注釈を修正	2007/11/30	日本電気株式会社
1.4		6.1.1	VAW-EOR-0024-00 の指摘に対する反映 FIA_UID.1.2 の記述を追加	2008/01/23	日本電気株式会社
1.4		6.1.1	VAW-EOR-0025-00 の指摘に対する反映 FIA_USB.1.2a/b、FIA_USB.1.3a/b の割付を修正	2008/01/23	日本電気株式会社
1.4		6..3.2	VAW-EOR-0026-00 の指摘に対する反映 表 18 中の FMT_SMR.1、FMT_MSA.1 の依存性割付を修正	2008/01/23	日本電気株式会社
1.4		6..1.1 7.1.4	パスワードの設定条件の修正	2008/01/24	日本電気株式会社
1.5		1.4.6 7.1.6	ユーザ AP 復旧機能における説明を修正 ・ユーザ AP 再起動失敗時における説明を追加	2008/02/21	日本電気株式会社
1.5		1.4.6 7.1.3 7.1.6	ユーザ AP 利用者数の増減に関する表記を修正 ・ユーザ AP アクセス制御機能の説明を修正	2008/02/21	日本電気株式会社
1.5		1.2	TOE 参照を修正 ・バージョン表記修正	2008/02/21	日本電気株式会社
1.5		4.3.2	A.USERAP を削除	2008/02/21	日本電気株式会社
1.6		1.4.7	認証方式について追記	2008/04/14	日本電気株式会社

■登録商標・商標について

本書に記載されている商品名、会社名などの固有名詞は、各社の商標または登録商標です。

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 Version 3.1

・Common Criteria for Information Technology Security Evaluation
Part2: Security functional components Version 3.1

・Common Criteria for Information Technology Security Evaluation
Part3: Security assurance components Version 3.1

・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 2006 年 9 月バージョン 3.1 改訂第 1 版 CCMB-2006-09-002
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 3:
セキュリティ保証コンポーネント 2006 年 9 月バージョン 3.1 改訂第 1 版 CCMB-2006-09-003
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

・Java™ 2 platform Enterprise Edition Specification V1.4

略語・用語

本 ST における記号と略語

CC	コモンクライテリア（Common Criteria）
EAL	評価保証レベル（Evaluation Assurance Level）
OSP	組織のセキュリティ方針（Organizational Security Policy）
PP	プロテクションプロファイル（Protection Profile）
SAR	セキュリティ保証要件（Security Assurance Requirement）
SFR	セキュリティ機能要件（Security Functional Requirement）
SFP	セキュリティ機能方針（Security Function Policy）
ST	セキュリティターゲット（Security Target）
TOE	評価対象（Target of Evaluation）
TSF	TOE セキュリティ機能（TOE Security Functionality）
TSFI	TSF インタフェース（TSF Interface）
PC	パーソナルコンピュータ（Personal Computer）
AP	アプリケーション（Application）
API	アプリケーションインタフェース(Application Program Interface)
OS	オペレーティングシステム（Operating System）
HW	ハードフェア(Hardware)
SW	ソフトウェア(Software)
NW	ネットワーク(Network)

本 ST で使用している用語とその定義

用語	定義内容
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。
J2SE	Java 2 Standard Edition の略。 ワークステーション用の機能を持つ 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。
再配備	既にアプリケーションサーバ上で動作しているユーザ AP を置換した後に使用可能にすること。 本 ST では、TOE 上のユーザ AP 制御データを削除した後、新たにユーザ 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 ブラウザを利用する。
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。
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。
内部ネットワーク	サーバエリア内に存在し、WebOTX 実行サーバと接続されたネットワーク。
OLTP モニタ	On-Line Transaction Processing　Monitor の略。 ユーザ AP の実行状態を監視するソフトウェア。
利用者 ID	TOE が TOE 利用者を一意に特定するために払い出す ID。

ロール	TOE 上の各保護資産に対する操作に対して割り当てられる権限の集まり。
ユーザ AP 許可利用者ロール	ユーザ AP に対して単一に割り当てられるロールであり、一般利用者がユーザ AP を利用する際に必要な権限を表す。
一般利用者代行手続	TOE 上で一般利用者の権限で動作する手続。
WebOTX 管理者代行手続	TOE 上で WebOTX 管理者の権限で動作する手続。
障害ログ	TOE の運用中に発生した障害を WebOTX 管理者が検知、確認するために TOE が出力するファイル。

1. ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、および 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: WebOTX Application Server セキュリティターゲット
ST バージョン: 1.6
ST 発行日: 2008 年 04 月 14 日
ST 作成者: 日本電気株式会社

1.2. TOE 参照

TOE の識別情報は、以下の通りである。

TOE 名称: WebOTX Application Server 高信頼実行ユニット
TOE バージョン: 7.11
TOE 開発者: 日本電気株式会社

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 範囲外のハードウェア/ソフトウェアについて記述する。

1.3.1. TOE 種別

「WebOTX Application Server」は J2EE1.4 規格（Java™ 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。本製品は、一般利用者が、利用者端末からアプリケーションサーバ上で動作するユーザ AP を利用可能とするための機能として、ユーザ AP 実行サービスを提供している。

本 ST における TOE はアプリケーションサーバ「WebOTX Application Server」の根幹をなす、WebOTX Application Server 高信頼実行ユニット（以降、高信頼実行ユニットと略称）である。

対象となる製品は「WebOTX Application Server Enterprise Edition」および「WebOTX Application Server Standard Edition」であり、この2製品には同一の TOE が含まれている。

1.3.2. TOE の使用方法と主要なセキュリティ機能

WebOTX が提供する本質的かつ主要なサービス機能は一般利用者に対しユーザ AP 実行サービスを安定して提供することである。ここで、ユーザ AP 実行サービスのセキュリティにとっての主要な脅威は以下が想定される。

（1）TOE に一般利用者として登録されていない者による、ユーザ AP 実行サービスの利用
（2）TOE に登録された一般利用者による、利用権限のないユーザ AP 実行サービスの利用
（3）WebOTX 管理者の誤操作による、ユーザ AP 実行サービスの停止
（4）ユーザ AP の異常終了による、セキュリティ機能の長時間の停止

（1）に対しては管理機構の利用者管理機能および J2EE コンテナの一般利用者識別認証機能、（2）に対しては J2EE コンテナのユーザ AP アクセス制御機能、（3）に対しては管理機構の WebOTX 管理者識別認証機能、利用者管理機能および J2EE コンテナのユーザ AP 配備制御機能、（4）に対しては OLTP モニタのユーザ AP 復旧機能により対抗すれば、十分である。

よって本 ST では、「WebOTX Application Server」に含まれる、J2EE コンテナ、管理機構および OLTP モニタの3コンポーネントから構成される「高信頼実行ユニット」を TOE とする。

TOE の主な使用法を以下に示す。

- 利用者管理サービスにより、WebOTX 管理者は WebOTX 利用者を管理する。
- ユーザ AP 配備サービスにより、WebOTX 管理者は予め開発者が作成したユーザ AP を TOE に配備する。
- ユーザ AP 実行サービスにより、一般利用者は利用者端末上のクライアントからユーザ AP を利用する。

TOE の主要なセキュリティ機能は、以下の通りである。

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。

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。

1.3.3. TOE 以外のハードウェア/ソフトウェア

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

（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

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 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 1 に示す。

表 1 TOE 関連の役割定義一覧

役割	内容
WebOTX 管理者	WebOTX 管理者は、TOE を管理する者である。 WebOTX 管理者は、TOE の管理者権限を有する。WebOTX 管理者は TOE の設定および運用管理についての十分な知識を有する。 WebOTX 管理者は、WebOTX 実行サーバ上から運用管理コマンドを用いて以下の作業を行う。 (1)TOE の構築、設定 (2)TOE の運用管理（TOE 起動停止、サービス起動停止、性能改善） (3)TOE の障害監視（障害ログの監視） (3)WebOTX 利用者の登録、更新、削除 (4)ユーザ AP 許可利用者ロールの確認、配備、再配備、配備解除
一般利用者	一般利用者は、TOE が提供するユーザ AP 実行サービスを利用する者である。 一般利用者は、利用者端末から WWW ブラウザを使用し、外部ネットワークから TOE に接続する。
システム管理者	システム管理者は、TOE が動作する内部ネットワーク上の HW、SW、NW を管理する者である。 システム管理者の作業は具体的には以下のようになる。 (1)WebOTX 実行サーバの HW の設定 (2) WebOTX 実行サーバの TOE 以外の SW である OS、JRE の設定、維持管理 (3)ファイアウォールの設定 (4)内部ネットワークの維持管理

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)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のネットワーク構成を 図 1 に示す。
図中の TOE 稼働マシン枠で示した部分が、TOE が稼働する WebOTX 実行サーバであり、内部ネットワーク上に設置される。外部ネットワークから内部ネットワークに通信する場合は、ファイアウォールを経由する必要がある。
一般利用者は、外部ネットワーク上の利用者端末から、TOE にアクセスする。
WebOTX 管理者は、WebOTX 実行サーバを直接操作し運用管理を行う。

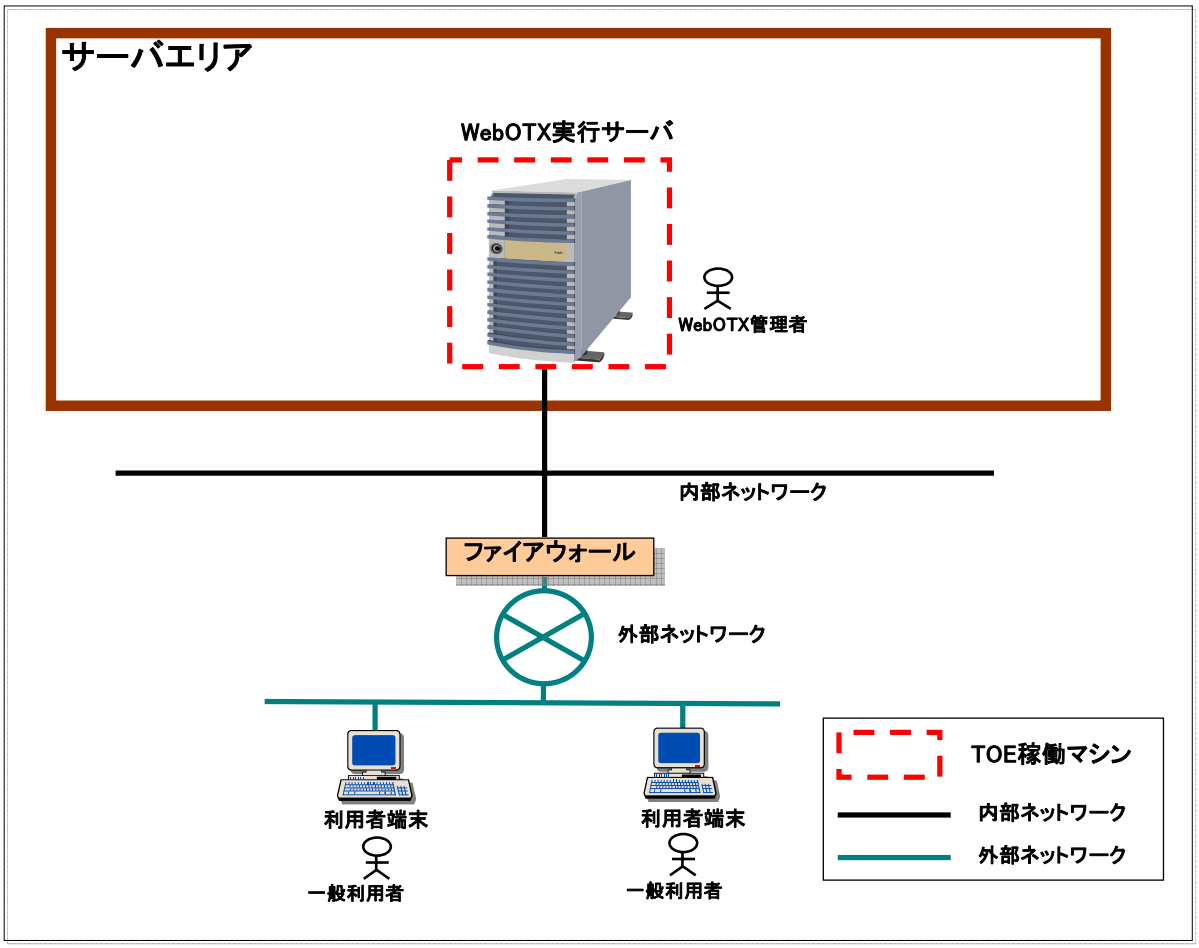

図 1　TOE のネットワーク構成

1.4.2.2.TOE の物理的範囲(コンポーネント)

TOEのコンポーネント構成図を 図 2 に示す。
図中の TOE 範囲枠で示したコンポーネントが TOE の物理的な範囲内である。
TOE が動作する WebOTX 実行サーバは、HW、OS、JRE、Web サーバおよび TOE を含んでいる。

TOE は WebOTX 実行サーバで動作するソフトウェアであり、J2EE コンテナ、管理機構、OLTP モニタの3つのコンポーネントから構成される。
これらのコンポーネントは、相互に独立したプロセスとして動作する。

以下 TOE のコンポーネントについて説明する。
J2EE コンテナ:
J2EE コンテナは、J2EE 仕様で作成されたユーザ AP を配備、再配備、配備解除、実行するコンポーネントであり、JRE 上で動作する。
J2EE コンテナは一般利用者に対し、ユーザ AP 実行サービスを実行するための外部インタフェースを提供する。
一般利用者がユーザ AP 実行サービスを利用する場合は、利用者端末で WWW ブラウザを起動し、ファイアウォールを経由し J2EE コンテナ上のユーザ AP エントリポイントにアクセスする。

管理機構:
管理機構は、WebOTX 利用者の管理を行うコンポーネントであり、JRE 上で動作する。
管理機構は WebOTX 管理者に対し、利用者管理サービスとユーザ AP 配備サービスを実行するための運用管理コマンドを提供する。
OLTP モニタ:
OLTP モニタは、ユーザ AP 実行サービスを維持するコンポーネントである。
OLTP モニタはユーザ AP 実行サービスを提供する J2EE コンテナの異常終了の際に、J2EE コンテナの再起動を行う。

TOE 外のコンポーネントについて以下に説明する。

WebOTX 実行サーバ:
WebOTX 実行サーバは TOE が動作するマシンである。
WebOTX 実行サーバ上では、OS が動作し、さらに OS 上で JRE および Web サーバが動作する。

ファイアウォール:
ファイアウォールは、WebOTX 実行サーバが存在する内部ネットワークと、利用者端末が存在する外部ネットワークの境界に設置される。

Web サーバ:
Web サーバは、WebOTX 実行サーバ上で動作し、ファイアウォールを経由して TOE に伝達される一般利用者からの要求および一般利用者への応答を中継する機能を有する。

利用者端末:
利用者端末は、一般利用者が使用するマシンである。
利用者端末上では、OS が動作し、さらに OS 上で WWW ブラウザが動作する。

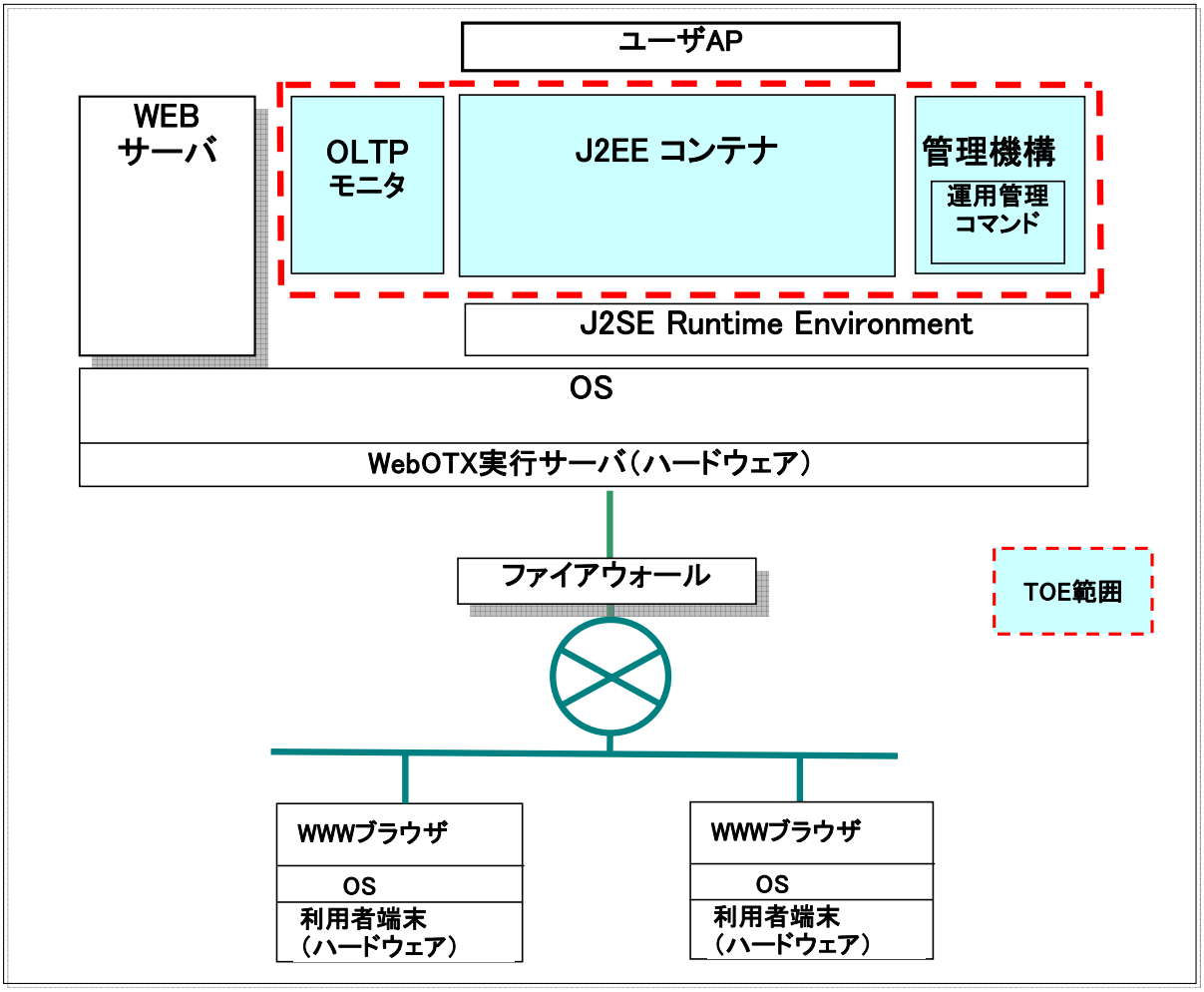

図 2　TOE の物理的範囲(コンポーネント)

1.4.3. ガイダンス

TOE のガイダンスは、以下の通りである。

・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）

1.4.4. TOE の論理的範囲

TOEの論理範囲図を 図 3 に示す。

図中の TOE 範囲枠で示した部分が TOE の論理的な範囲内である。

TOE は J2EE コンテナ、OLTP モニタおよび管理機構の3コンポーネントにより構成されており、これらが提供するサービス機能およびセキュリティ機能が、TOE の論理範囲のすべてとなる。

・J2EE コンテナは、「一般利用者識別認証機能」、「ユーザ AP アクセス制御機能」および「ユーザ AP 配備制御機能」を提供する。

・管理機構は、「WebOTX 管理者識別認証機能」および「利用者管理機能」を提供する。

・OLTP モニタは、「ユーザ AP 復旧機能」を提供する。

TOE は WebOTX 利用者に「ユーザ AP 実行サービス」、「利用者管理サービス」および「ユーザ AP 配備サービス」を提供しており、各サービスは以下の機能から構成されている。

・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。

・ユーザ AP 利用情報、アクセス制御情報、セッション情報は、J2EE コンテナに含まれる TSF データである。
・アカウント情報は、管理機構に含まれる TSF データである。
・ユーザ AP エントリポイントは、J2EE コンテナに含まれるオブジェクトである。
・ユーザ AP は、TOE 範囲外であり、ユーザ AP エントリポイントから制御する。

利用者データと TSF データ、TOE のサブジェクトとオブジェクト及び、TOE サービス機能とセキュリティ機能についての詳細は後述する。

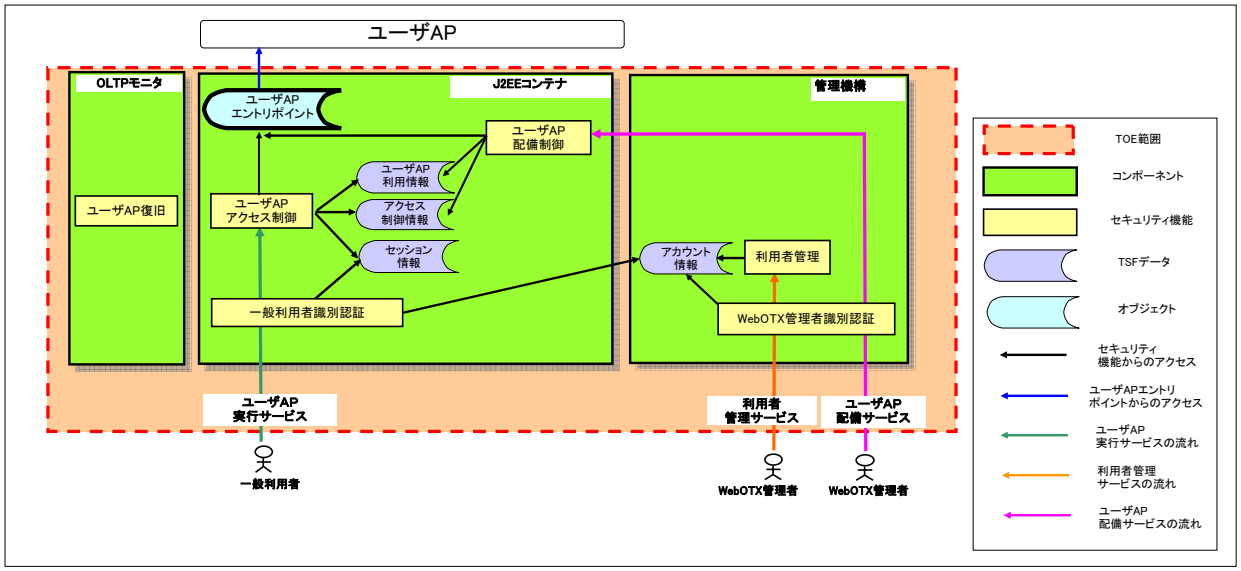

図 3　TOE の論理範囲

1.4.5. 利用者データと TSF データ

TOEの利用者データを 表 2 に示す。

表 2 利用者データ

利用者データ名	内容
ユーザ AP 制御データ	ユーザ AP 制御データは、TOE からユーザ AP を呼び出すために用いられる利用者データである。

TOEのTSFデータを 表 3 に示す。

表 3 TSF データ

TSF データ名	内容
アカウント情報	アカウント情報は、TOE を利用する WebOTX 管理者または一般利用者を識別する為に用いられる。 アカウント情報には、利用者 ID、パスワードおよびロールが格納される。
セッション情報	セッション情報は、認証済みの一般利用者を一意に識別する為に用いられる。 セッション情報は一般利用者毎に生成され、識別認証された一般利用者に割り当てられたロールを格納する。
アクセス制御情報	アクセス制御情報はユーザ AP の利用権限を確認する際に用いられる。 アクセス制御情報はユーザ AP 毎に存在し、以下の情報を含む。 ・一般利用者に対する利用者権限ロール
ユーザ AP 利用情報	ユーザ AP 利用情報は、ユーザ AP を利用している一般利用者数を確認する際に用いられる。 ユーザ AP 利用情報はユーザ AP 毎に存在し、以下の情報を含む。 ・ユーザ AP 利用者数 ユーザ AP 実行サービス利用中の一般利用者数

1.4.6. TOE のサブジェクトとオブジェクト

TOE のセキュリティ機能を記述する上で必要となる、サブジェクトおよびオブジェクトについて示す。

サブジェクトを 表 4、オブジェクトを 表 5 に示す。

表 4 サブジェクト一覧

サブジェクト名	内容
一般利用者代行手続	TOE 内で一般利用者を代行し、セキュリティ機能を実行する手続。
WebOTX 管理者代行手続	TOE 内で WebOTX 管理者を代行し、セキュリティ機能を実行する手続。

表 5 オブジェクト一覧

データ名	内容
ユーザ AP エントリポイント	ユーザ AP エントリポイントは、J2EE コンテナ内に存在し、TOE からユーザ AP の利用を行なうためのユーザ AP 制御データへのリンクを保持する。

1.4.7. TOE サービス機能とセキュリティ機能

本 ST では、TOE 利用者が TOE を利用する際の機能を、「サービス機能」として定義する。また、TOE の維持およびサービス機能の維持に必要な機能を、「セキュリティ機能」として定義する。

TOE は WebOTX 利用者に対し、「ユーザ AP 実行サービス」、「利用者管理サービス」および「ユーザ AP 配備サービス」を提供している。

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。

TOE サービス機能を維持するためのセキュリティ機能を以下に記述する。

【一般利用者識別認証機能】

一般利用者識別認証機能は、一般利用者がユーザ AP 実行サービスを利用する際に最初に動作し、一般利用者を識別認証する機能である。
一般利用者は、TOE 上のユーザ AP を利用する際に、利用者端末から WWW ブラウザを実行し、ユーザ AP 毎に決められた URL をアクセスして TOE にユーザ AP 利用要求を送信する。
TOE はこの要求を、ファイアウォール、Web サーバを経由し J2EE コンテナで受信する。この際ファイアウォールは、HTTP プロトコルもしくは HTTPS プロトコルのみを通過させ、それ以外を遮断するよう設定

されているものとする。
TOE は一般利用者識別認証機能を実行し、一般利用者に対する識別認証を行う。TOE は一般利用者から受信した利用者 ID、パスワードを TOE が管理するアカウント情報と照合する。利用者 ID、パスワードの両方が一致する場合、識別認証成功と判断しアカウント情報からこの一般利用者に割り当てられたロールを取得する。識別認証に失敗した場合、WWW ブラウザに認証エラーを通知する。識別認証成功後、TOE はセッション情報を生成し、一般利用者ロールを格納する。HTTP の認証方式としては BASIC 認証のみを対象とする。

【ユーザ AP アクセス制御機能】
ユーザ AP アクセス制御機能は、一般利用者がユーザ AP 実行サービスを利用する際に、ユーザ AP エントリポイントの利用権限があるかを確認する機能である。
一般利用者の識別認証成功後、TOE はユーザ AP アクセス制御機能を呼び出す。TOE は認証済みの一般利用者に割り当てられたロールをセッション情報から取得するとともに、アクセス制御情報から該当のユーザ AP に割り当てられたロールを取得する。
TOE は利用者アクセス制御方針に従い、一般利用者ロールとユーザ AP 許可利用者ロールの内容が一致するかを調べる。ロールの内容が一致する場合のみユーザ AP エントリポイントへのアクセスを許可する。一致しない場合、TOE は一般利用者の利用要求を拒否し利用者端末にアクセスエラーを通知する。

【WebOTX 管理者識別認証機能】
WebOTX 管理者識別認証機能は、WebOTX 管理者が利用者管理サービスまたはユーザ AP 配備サービスを利用する際に最初に動作し、WebOTX 管理者を識別認証する機能である。
WebOTX 管理者は、WebOTX 利用者の管理またはユーザ AP の配備／配備解除を行う際に、利用者管理サービスまたはユーザ AP 配備サービスを利用する。いずれのサービスを利用する場合でも、WebOTX 管理者はまず TOE が動作するマシンの OS にログオンする。その後、コンソール画面を起動し、目的のサービスを実行するための運用管理コマンドを実行する。運用管理コマンドでは、WebOTX 管理者である利用者 ID、パスワードをコマンドのパラメタとして指定すると共にコマンドの実行に必要な情報を指定する。
TOE は運用管理コマンドを実行後、コマンドラインで指定された内容を解析し、利用者 ID、パスワードを取得し、TOE の管理するアカウント情報から取得した利用者 ID、パスワードをアカウント情報と照合する。利用者 ID、パスワードの両方が一致する場合、さらにアカウント情報からこの WebOTX 管理者に割り当てられたロールを取得し、それが WebOTX 管理者のロールの値を有している場合に識別認証成功と判断する。識別認証に失敗した場合、TOE は運用管理コマンドに認証エラーを表示する。TOE は WebOTX 管理者の識別認証に成功後、運用管理コマンドの内容により利用者管理機能またはユーザ AP 配備制御機能のいずれかを実行する。

【利用者管理機能】
利用者管理機能は、WebOTX 管理者が WebOTX 利用者を事前に登録し、管理する機能である。
WebOTX 管理者識別認証機能による WebOTX 管理者の識別認証に成功後、TOE は利用者管理機能を呼び出す。TOE は運用管理コマンドにより指定された内容により、WebOTX 利用者の登録／更新／削除の操作を行う。

【ユーザ AP 配備制御機能】
ユーザ AP 配備制御機能は、WebOTX 管理者がユーザ AP の配備、再配備または配備解除を行う際にユーザ AP の動作状態を事前確認することにより、ユーザ AP 実行サービスに影響を与えることなく

配備、再配備、配備解除のいずれかを行う機能である。
WebOTX 管理者識別認証機能による WebOTX 管理者の識別認証に成功後、TOE はユーザ AP 配備制御機能を呼び出す。TOE は運用管理コマンドから指定された内容により、ユーザ AP の配備／再配備／配備解除のいずれかの処理を行う。
ユーザ AP の配備の場合、TOE はユーザ AP 制御データおよびアクセス制御情報を TOE 上に生成する。
ユーザ AP の再配備の場合、 TOE は指定されたユーザ AP を利用中の一般利用者が存在するかを、各ユーザ AP に対応するユーザ AP 利用情報に格納されたユーザ AP 利用者数により確認する。ユーザ AP を利用中の一般利用者が存在した場合、TOE はすべての一般利用者の利用完了を待ちあわせる。一般利用者の利用完了後、TOE はユーザ AP 制御データおよびアクセス制御情報を TOE から削除した後、新たなユーザ AP 制御データおよびアクセス制御情報を生成する。
ユーザ AP の配備解除の場合、TOE は再配備の処理と同様、指定されたユーザ AP が一般利用者による利用中かどうかを確認し、実行中の場合は処理を待ち合わせる。一般利用者の利用完了後、TOE はユーザ AP 制御データおよびアクセス制御情報を TOE から削除する。

【ユーザ AP 復旧機能】
ユーザ AP 復旧機能は、J2EE コンテナの予期せぬ停止を確認し、J2EE コンテナを再起動することにより、J2EE コンテナ内のセキュリティ機能およびユーザ AP 実行サービスを復旧する機能である。
J2EE コンテナが異常終了した場合、TOE は J2EE コンテナが動作するプロセスの異常終了を OS からの通知を受け取ることにより検出すると、対象の J2EE コンテナの再起動を行う。もし J2EE コンテナの再起動に失敗した場合、ユーザ AP 復旧機能は J2EE コンテナの再起動を予め設定された回数の範囲内で繰り返し試みる。
所定回数繰り返しても J2EE コンテナの再起動が成功しない場合、ユーザ AP 復旧機能は自動復旧不能と判断し、J2EE コンテナの再起動に失敗した旨の内容を障害ログに出力し WebOTX 管理者の介入を要求する。
WebOTX 管理者は、障害ログにより J2EE コンテナの再起動失敗を検出した場合、障害の原因を取り除いた後、手動で TOE を再起動し正常な状態に復旧させる。
これにより J2EE コンテナが提供する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 配備制御機能を復旧することで、使用できない時間を最小限とする。

WebOTX Application Server の機能のうち、TOE 範囲外の主要機能を以下に記述する。

【Web サーバ機能】
利用者端末からの HTTP リクエストを受信し応答を返却する機能。

【CORBA サービス機能】
Object Management Group (OMG)が制定している Common Object Request Broker Architecture (CORBA)仕様に基づいた分散オブジェクトを動作させる機能。

【流量制御機能】
利用者端末からの処理要求の受付を制限することにより、高負荷状態においても一定の処理能力を維持する機能

【性能計測機能】

WebOTX Application Server の”各種性能値”を収集し、統計情報をまとめる機能。

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 および TOE の CC 適合主張は、以下のとおりである。
ST と TOE が適合を主張する CC のバージョン:

パート 1:概説と一般モデル 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 2:セキュリティコンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 3:セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版

CC パート 2 に対する ST の適合 : CC パート 2 適合
CC パート 3 に対する ST の適合 : CC パート 3 適合

2.2. PP 主張

本 ST には適合している PP はない。

2.3. パッケージ主張

本 TOE は、EAL2 追加である。追加する要件は ALC_FLR.1 である。

2.4. 適合主張根拠

本 ST に適合している PP 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を行う。

3.1. 脅威

TOE に対する脅威を以下に記述する。

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 利用サービスおよ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。

3.2. 組織のセキュリティ方針

TOE および TOE の運用環境に適用する組織のセキュリティ方針を以下に記述する。

TOE が想定する組織のセキュリティ方針はない。

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を行う。

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。

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 および 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。

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.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 管理者自身およ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、ファイアウォールおよび 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。

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.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。

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および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.USERMANAGE（利用者管理）
TOE は、WebOTX 管理者に対し、WebOTX 利用者を管理するための情報である利用者 ID、パスワード、ロールを TOE に登録する機能を提供しなければならない。

O.ID_AUTH（TOE 利用者の識別認証）
TOE は、利用者が TOE を利用する時は必ず識別認証されることを保証し、識別認証に成功した利用者のみ TOE の利用を許可しなければならない。

O. ACCESSCONTROL（ユーザ AP のアクセス制御）
TOE は、一般利用者のユーザ AP に対する利用権限を確認し、対象の一般利用者に許可されたユーザ AP のみサービスの利用を許可するようアクセスを制御しなければならない。

O.DEPLOYCONTROL（配備制御）
TOE は、TOE 上にユーザ AP を再配備する場合、あるいは TOE からユーザ AP を配備解除する場合に、対象のユーザ AP が一般利用者の利用中でないかを確認し、利用中の場合は一般利用者の利用完了を待ち合わせた後、再配備または配備解除しなければならない。

O.PROCESSALIVE（セキュリティ機能の生存チェック）
TOE は、OS からの通知により J2EE コンテナの異常終了を確認し、もし異常終了していれば速やかに再起動するよう動作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。

OM.SECURECHANNEL（セキュア通信）
WebOTX 管理者は、通信を秘匿する必要性があるユーザ AP の場合、システム管理者に対し HTTPS の設定を依頼する。

OM.OSJAVA(OS、JavaVM によるセキュリティ)
システム管理者は、TOE が動作する OS および 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。

OM.WEBOTX_ADMIN（信頼できる WebOTX 管理者）
信頼できる WebOTX 管理者を設置し、TOE に対する十分なトレーニングを行う。
WebOTX 管理者は、WebOTX 管理者自身およ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。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。
WebOTX 管理者は、ユーザ AP にユーザ AP 許可利用者ロールが設定されていることを、配備する前に確認する。

OM.SYS_ADMIN（信頼できるシステム管理者）
信頼できるシステム管理者を設置する。
システム管理者は、内部ネットワーク、ファイアウォールおよび AP 実行サーバ上の TOE 以外の SW である OS、JRE の維持管理を行う。
システム管理者は TOE が必要とするシステム管理について十分なトレーニングを受ける。

OM.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ようにする。

OM.FIREWALL（ファイアウォールの設置）
システム管理者は、内部ネットワークと外部ネットワークの間にファイアウォールを設置する。
ファイアウォールには、ユーザ AP 実行サービスで使用する HTTP および HTTPS のみのプロトコルおよびポートを許可する設定を行う。

OM.AREA（サーバエリアの保護）
システム管理者は、TOE が設置されるサーバエリアを、WebOTX 管理者を含む許可された者のみが入退室できるよう管理する。

OM.OSDETECT（OS によるプロセス終了検知）
システム管理者は、TOE が動作する WebOTX 実行サーバに、プロセス終了を検知しこれを通知する機能を持つ OS を導入する。

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 6 に示す。表中の「×」は対応関係にあることを示している。

表 6 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.ILLEGAL_LOGON	T.ILLEGAL_ACCESS	T.MISTAKE	T.PROCESSTERM	A.SECURECHANNEL	A.OSJAVA	A.WEBOTX_ADMIN	A.SYS_ADMIN	A.ID_PASSWORD	A.FIREWALL	A.AREA
O.USERMANAGE	×	×									
O.ID_AUTH	×										
O.ACCESSCONTROL		×									
O.DEPLOYCONTROL			×								
O.PROCESSALIVE				×							
OM.SECURECHANNEL					×						
OM.OSJAVA						×					
OM.WEBOTX_ADMIN		×					×				
OM.SYS_ADMIN								×			
OM.ID_PASSWORD									×		
OM.FIREWALL	×									×	
OM.AREA	×										×
OM.OSDETECT				×							

上記より各セキュリティ対策方針は一つ以上の脅威、および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.ILLEGAL_LOGON（不正なログオン）
この脅威は、一般利用者に対するなりすましの脅威と、WebOTX管理者に対するなりすましの脅威が想定される。それぞれの場合の具体的な不正ログオンの方法を示すとともに、有効な対抗策について以下に述べる。

a)WebOTX 利用者でない攻撃者が、一般利用者になりすましユーザ AP 実行サービスの利用を試みる。
この脅威に対しては、O.USERMANAGE により、あらかじめ WebOTX 管理者がユーザ AP 実行サービスの利用者を TOE に登録しIDとパスワードを設定しておく。一般利用者にユーザ AP 実行サービスを提供する際には、O.ID_AUTH により必ず利用者 ID とパスワードによる識別認証を行う。これにより TOE の利用を登録された一般利用者のみに制限することで、この脅威に対抗できる。
以上、この対抗策に該当するセキュリティ対策方針は、O.ID_AUTH、O.USERMANAGE である。

b) WebOTX 管理者でない者が、WebOTX 管理者になりすまし利用者管理サービス、ユーザ AP 配備サービスの利用を試みる。
この脅威に対しては、OM.AREA によりシステム管理者がサーバエリア内への入室を管理する。また外部ネットワークからはサービスを利用するための運用管理コマンドを実行できないよう、ファイアウォールを設置し、OM.FIREWALL により WebOTX 実行サーバ以外の利用者端末からコンソールが使用できないよう抑止する。WebOTX 利用者が利用者管理サービス、ユーザ AP 配備サービスを利用する際は、O.USERMANAGE により事前に WebOTX 管理者を TOE に登録しID、パスワードを設定しておき、これらのサービスを利用する前に、O.ID_AUTH により利用者IDとパスワードによる識別認証を行う。WebOTX 利用者が WebOTX 管理者権限を持つ場合にのみこれらサービスの利用を許可することで、この脅威に対抗できる。
以上、この対抗策に対するセキュリティ対策方針は、O.ID_AUTH、O.USERMANAGE、OM.AREA、OM.FIREWALL である。
よっていずれの場合にもこの脅威に対するセキュリティ対策は十分である。

T.ILLEGAL_ACCESS（不正なユーザ AP 利用）
この脅威は、識別認証された一般利用者による、許可されていないユーザ AP 実行サービスの利用が考えられる。
この脅威に対しては、O.USERMANAGE により、WebOTX 管理者が一般利用者を TOE に登録する際に、この一般利用者に対しユーザ AP の利用を許可する為の一般利用者ロールを登録しておく。
また OM.WEBOTX_ADMIN により、WebOTX 管理者はユーザ AP を配備する前に、ユーザ AP にユーザ AP 許可利用者ロールが設定されていることを確認しておく。
TOE は、識別認証された一般利用者がユーザ AP を利用する際に、O.ACCESSCONTROL により一般利用者ロールとユーザ AP 許可利用者ロールを照合し、ロールの内容が一致する場合にのみ対象のユーザ AP 実行サービスを許可することで、この脅威に対抗できる。
以上、この対抗策に対するセキュリティ対策方針は、O.USERMANAGE、O.ACCESSCONTROL、OM.WEBOTX_ADMIN である。
よってこの脅威に対するセキュリティ対策は十分である。

T.MISTAKE（誤操作）
この脅威は、サーバエリア内に存在する WebOTX 管理者による誤操作が考えられる。この脅威に有効な対抗策について以下に述べる。
サーバエリア内に存在する WebOTX 管理者が、ユーザ AP 配備サービスを利用しユーザ AP を再配

備または配備解除する場合において、一般利用者が利用中のユーザ AP を誤って置換もしくは停止してしまうことにより、ユーザ AP 実行サービスが提供できなくなる脅威が想定される。
この脅威に対しては、O.DEPLOYCONTROL により対象のユーザ AP が一般利用者の利用中であるかどうかを TOE が判断し、未使用の場合のみユーザ AP 配備サービスの処理を実行する事でこの脅威に対抗できる。
この対抗策に対するセキュリティ対策方針は、O.DEPLOYCONTROL である。
よって、この脅威に対するセキュリティ対策は十分である。

T.PROCESSTERM（セキュリティ機能の長時間停止）
この脅威は、利用中のユーザ AP が動作中の J2EE コンテナが、プログラムの不具合や JRE の不具合等により異常終了することで、J2EE コンテナのセキュリティ機能が停止し、長時間提供できないことが考えられる。この脅威に有効な対抗策について以下に述べる。
この脅威に対しては、OM.OSDETECT により J2EE コンテナの異常終了を OS が検知し、TOE に通知すると、 O.PROCESSALIVE により TOE が J2EE コンテナを再起動し速やかにセキュリティ機能を復旧することでこの脅威に対抗できる。
この対抗策に対するセキュリティ対策は、OM.OSDETECT 、O.PROCESSALIVE である。
よって、この脅威に対するセキュリティ対策は十分である。

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

組織のセキュリティ方針がないので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はない。

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.FIREWALL（ファイアウォール）
セキュリティ対策方針 OM.FIREWALL は前提条件 A.FIREWALL を直接充足する。

A.AREA（サーバエリア管理）
セキュリティ対策方針 OM.AREA は前提条件 A. AREA を直接充足する。

A.OSJAVA（OS、JavaVM のセキュリティ）
セキュリティ対策方針 OM. OSJAVA は前提条件 A. OSJAVA を直接充足する。

A. ID_PASSWORD（ID とパスワードの適切な管理）
セキュリティ対策方針 OM. ID_PASSWORD は前提条件 A. ID_PASSWORD を直接充足する。

A.WEBOTX_ADMIN（信頼できる WebOTX 管理者）
セキュリティ対策方針 OM. WEBOTX_ADMIN により、前提条件 A.WEBOTX_ADMIN を充足する。

A.SYS_ADMIN（信頼できるシステム管理者）
セキュリティ対策方針 OM. SYS_ADMIN は前提条件 A.SYS_ADMIN を直接充足する。

A.SECURECHANNEL（セキュア通信）
セキュリティ対策方針 OM.SECURECHANNEL は前提条件 A. SECURECHANNEL を直接充足する。

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を行う。

本 ST では拡張コンポーネントは使用しない。

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を行う。

6.1. セキュリティ機能要件

セキュリティ機能のクラス毎に以下で、機能要件の記述を行う。

6.1.1. FIA クラス:識別と認証

FIA_ATD.1 利用者属性定義

下位階層: なし
依存性: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。:[割付: セキュリティ属性のリスト]

[割付: セキュリティ属性のリスト]
・一般利用者ロール
・WebOTX 管理者ロール

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]
パスワードは 8 文字以上の英数記号で構成される文字列。

FIA_UAU.1 認証のタイミング

下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる[割付: TSF 仲介アクションのリスト]を許可しなければならない。

[割付: TSF 仲介アクションのリスト]
・ ユーザ AP 利用時の利用者 ID およびパスワード入力要求(一般利用者の識別認証)

FIA_UAU.1.2 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_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.1 識別のタイミング

下位階層: なし
依存性: なし

FIA_UID.1.1 TSF は、利用者が識別される前に利用者を代行して実行される[割付: TSF 仲介アクションのリスト]を許可しなければならない。

[割付: TSF 仲介アクションのリスト]
・ ユーザ AP 利用時の利用者 ID およびパスワード入力要求（一般利用者の識別認証）

FIA_UID.1.2 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。

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。

FIA_USB.1a J2EE コンテナの利用者-サブジェクト結合

下位階層: なし
依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1a TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: 利用者セキュリティ属性のリスト]

[割付: 利用者セキュリティ属性のリスト]
・一般利用者ロール

FIA_USB.1.2a TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の最初の関連付けの規則]

[割付: 属性の最初の関連付けの規則]

なし。

FIA_USB.1.3a TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の変更の規則]

[割付: 属性の変更の規則]
なし。

FIA_USB.1b 管理機構の利用者-サブジェクト結合

下位階層: なし
依存性: FIA_ATD.1 利用者属性定義

FIA_USB.1.1b TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: 利用者セキュリティ属性のリスト]

[割付: 利用者セキュリティ属性のリスト]
・WebOTX 管理者ロール

FIA_USB.1.2b TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の最初の関連付けの規則]

[割付: 属性の最初の関連付けの規則]
なし。

FIA_USB.1.3b TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の変更の規則]

[割付: 属性の変更の規則]
なし。

6.1.2. FMT クラス:セキュリティ管理

FMT_MSA.1 管理機構のセキュリティ属性の管理

下位階層: なし
依存性: [FDP_ACC.1 サブセットアクセス制御、または FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MSA.1.1 TSF は、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を

[割付: 許可された識別された役割]に制限する[割付: アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

上記の割付、選択を **表 7** に示す。

表 7 管理機構のセキュリティ属性の管理

［割付:セキュリティ属性のリスト］	［選択:その他の操作］	［割付:許可された識別された役割］
一般利用者ロール	参照	WebOTX 管理者
	更新	WebOTX 管理者
	削除	WebOTX 管理者
WebOTX 管理者ロール	参照	WebOTX 管理者
	更新	WebOTX 管理者
	削除	WebOTX 管理者

[割付: アクセス制御 SFP、情報フロー制御 SFP]:
利用者データアクセス制御方針b

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。

上記の割付、選択を 表 8 に示す。

表 8 TSF データの管理

［割付:TSF データのリスト］	［選択:その他の操作］	[割付: 許可された識別された役割]
アカウント情報	登録	WebOTX 管理者
	更新	WebOTX 管理者
	削除	WebOTX 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]
上記の割付を 表 9 に示す。

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_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし（利用者に対する追加のセキュリティ属性はないため、管理対象とならない）
FIA_SOS.1	秘密の検証に使用される尺度の管理。	なし（アクションは固定であり、管理対象とならない）
FIA_UAU.1	管理者による認証データの管理。	運用管理コマンドによる、利用者情報（パスワード）の登録・更新・削除
	関係する利用者による認証データの管理	なし（一般利用者には認証データに対する権限はないため、管理対象とならない）
	利用者が認証される前にとられるアクションのリストを管理すること	なし（アクションは固定であり、管理対象とならない）
FIA_UAU.2	管理者による認証データの管理。	運用管理コマンドによる、利用者情報（パスワード）の登録・更新・削除
	このデータに関係する利用者による認証データの管理。	なし（一般利用者には認証データに対する権限はないため、管理対象とならない）
FIA_UID.1	利用者識別情報の管理;	運用管理コマンドによる、利用者情報（利用者 ID）の登録・更新・削除
	許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。	なし（アクションは固定であり、管理対象とならない）
FIA_UID.2	利用者識別情報の管理;	運用管理コマンドによる、利用者情報（利用者 ID）の登録・更新・削除
FIA_USB.1a	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。	なし（アクションは固定であり、管理対象とならない）
	許可管理者は、サブジェクトのセキュリティ属性を変更できる。	なし（サブジェクトのセキュリティ属性は固定であり、管理対象とならない）
FIA_USB.1b	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。	なし（アクションは固定であり、管理対象とならない）
	許可管理者は、サブジェクトのセキュリティ属性を変更できる。	なし（サブジェクトのセキュリティ属性は固定であり、管理対象とならない）
FMT_MSA.1	セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	なし（サブジェクトのセキュリティ属性は固定であり、管理対象とならない）
FMT_MTD.1	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	なし（TSF データと利用者の権限の関係は固定であり、管理対象とならない）

FMT_SMF.1	なし	なし
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	なし(役割は固定であり、管理対象とならない)
FDP_ACC.1a	なし	なし
FDP_ACC.1b	なし	なし
FDP_ACF.1a	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	運用管理コマンドによる、利用者情報(ロール)の登録・更新・削除
FDP_ACF.1b	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	なし(アクセス制御方針は固定であり、管理対象とならない)
FPT_RCV.2	なし	なし

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]
WebOTX 管理者
一般利用者

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。

6.1.3. FDP クラス:利用者データ保護

FDP_ACC.1a ユーザ AP 実行サービス時のサブセットアクセス制御

下位階層: なし
依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1a TSF は、[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御 SFP]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]
＜サブジェクトのリスト＞
- 一般利用者代行手続

＜オブジェクトのリスト＞
- ユーザ AP エントリポイント

＜SFP で扱われるサブジェクトとオブジェクト間の操作のリスト＞
- 実行

[割付: アクセス制御 SFP]

利用者データアクセス制御方針 a

FDP_ACC.1b ユーザ AP 配備サービス時のサブセットアクセス制御

下位階層: なし
依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1b TSF は、[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付: アクセス制御 SFP]を実施しなければならない。

[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]
＜サブジェクトのリスト＞
- WebOTX 管理者代行手続

＜オブジェクトのリスト＞
- ユーザ AP エントリポイント

＜SFP で扱われるサブジェクトとオブジェクト間の操作のリスト＞
- 配備
- 再配備
- 配備解除

[割付: アクセス制御 SFP]
利用者データアクセス制御方針 b

FDP_ACF.1a セキュリティ属性によるユーザ AP 実行サービス時のアクセス制御

下位階層: なし
依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1a TSF は、以下の[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 SFP]を実施しなければならない。

割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]
上記割付を 表 10 に示す。

表 10　ユーザ AP 実行サービス時におけるアクセス制御

「割付:サブジェクト」	[割付: サブジェクトの SFP 関連セキュリティ属性]	［割付:オブジェクト］	[割付: オブジェクトの SFP 関連セキュリティ属性]
一般利用者代行手続	一般利用者ロール	ユーザ AP エントリポイント	ユーザ AP 許可利用者ロール

[割付: アクセス制御 SFP]:利用者データアクセス制御方針 a

FDP_ACF.1.2a　TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]
上記割付を 表 11 に示す。

表 11　ユーザ AP 実行サービス時における
制御されたサブジェクトと制御されたオブジェクト間での操作規則

「割付:制御されたサブジェクト」	［割付:制御されたオブジェクト］	［割付:制御された操作］
一般利用者代行手続	ユーザ AP エントリポイント	一般利用者ロールがユーザ AP に割り付けられたユーザ AP 許可利用者ロールの内容と一致すれば実行を許可

FDP_ACF.1.3a　TSF は、次の追加規則、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]:なし

FDP_ACF.1.4a　TSF は、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]:なし

FDP_ACF.1b セキュリティ属性によるユーザ AP 配備サービス時のアクセス制御

下位階層: なし
依存性: FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1b TSF は、以下の[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付: アクセス制御 SFP]を実施しなければならない。

[割付: 示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、および各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]
上記割付を 表 12 に示す。

表 12 ユーザ AP 配備サービス時におけるアクセス制御

「割付:サブジェクト」	[割付: サブジェクトの SFP 関連セキュリティ属性]	[割付:オブジェクト]	[割付: オブジェクトの SFP 関連セキュリティ属性]
WebOTX 管理者代行手続	WebOTX 管理者ロール	ユーザ AP エントリポイント	ユーザ AP 利用情報に格納されたユーザ AP 利用者数

[割付: アクセス制御 SFP]:利用者データアクセス制御方針b

FDP_ACF.1.2b TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうかを決定するために、次の規則を実施しなければならない: [割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]

1)WebOTX 管理者代行手続がユーザ AP エントリポイントに対し再配備の操作を行なう場合、対象のユーザ AP のユーザ AP 利用情報を確認し、ユーザ AP の利用者が0でなければ、再配備を許可しない。
2)WebOTX 管理者代行手続がユーザ AP エントリポイントに対し配備解除の操作を行なう場合、対象のユーザ AP のユーザ AP 利用情報を確認し、ユーザ AP の利用者が0でなければ、配備解除を許可しない。

FDP_ACF.1.3b TSF は、次の追加規則、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]:なし

FDP_ACF.1.4b TSF は、[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付: セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]なし。

補足説明
FDP_ACF.1.1b、 FDP_ACF.1.2b、FDP_ACF.1.3b、FDP_ACF.1.4b の規則を合わせたものが利用者データアクセス制御方針bのアクセス制御規則である。

6.1.4. FPT クラス：TSF の保護

FPT_RCV.2 自動回復

下位階層: FPT_RCV.1 手動回復
依存性: AGD_OPE.1 利用者操作ガイダンス

FPT_RCV.2.1 [割付: 障害/サービス中断のリスト]からの自動回復が不可能な場合、TSF はセキュアな状態に戻す能力が提供されるメンテナンスモードに移らなければならない。

[割付: 障害/サービス中断のリスト]
ユーザ AP 実行サービスの異常終了時かつユーザ AP の再起動に問題がある場合

FPT_RCV.2.2 [割付: 障害/サービス中断のリスト]に対し、TSF は、自動化された手順による TOE のセキュアな状態への復帰を保証しなければならない。

[割付: 障害/サービス中断のリスト]
ユーザ AP 実行サービスの異常終了時かつユーザ AP の再起動に問題がない場合

6.2. セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 であり、追加する保証コンポーネントは ALC_FLR.1 である。
すべての保証要件コンポーネントは、CC パート 3 で規定されているコンポーネントを直接使用する。

6.2.1. ADV クラス: 開発

ADV_ARC.1:セキュリティアーキテクチャ記述
ADV_FSP.2:セキュリティ実施機能仕様
ADV_TDS.1:基本設計

6.2.2. AGD クラス: ガイダンス文書

AGD_OPE.1:利用者操作ガイダンス
AGD_PRE.1:準備手続き

6.2.3. ALC クラス :ライフサイクルサポート

ALC_CMC.2:CM システムの使用
ALC_CMS.2: TOE の一部の CM 範囲
ALC_DEL.1:配付手続き
ALC_FLR.1:基本的な欠陥修正

6.2.4. ASE クラス :セキュリティターゲット評価

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. ATE クラス :テスト

ATE_COV.1 カバレージの証拠
ATE_FUN.1 機能テスト
ATE_IND.2 独立テスト - サンプル

6.2.6. AVA: 脆弱性評定

AVA_VAN.2:脆弱性分析

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 表 13 に示す。
表中の「×」は対応関係にあることを示している。

表 13 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.ID_AUTH	O.ACCESSCONTROL.	O.USER MANAGE	O.DEPLOYCONTROL	O.PROCESSALIVE
FIA_ATD.1			×		
FIA_SOS.1			×		
FIA_UAU.1	×				
FIA_UAU.2	×				
FIA_UID.1	×				
FIA_UID.2	×				
FIA_USB.1a	×				
FIA_USB.1b	×				
FMT_MSA.1			×		
FMT_MTD.1			×		
FMT_SMF.1			×		
FMT_SMR.1			×		
FDP_ACC.1a		×			
FDP_ACC.1b				×	
FDP_ACF.1a		×			
FDP_ACF.1b				×	
FPT_RCV.2					×

表 13 より、各TOE セキュリティ機能要件が1つ以上のTOE セキュリティ対策方針に対応している。
次に、各セキュリティ対策方針が、TOE のセキュリティ機能要件により実現できることを説明する。

各セキュリティ対策方針に対応するセキュリティ機能要件根拠について、以下に記述する。

O.ID_AUTH（TOE 利用者の識別認証）
このセキュリティ対策方針は、正当な利用者が TOE を利用するための、利用者の制限を求めている。利用者が TOE の提供する各サービスを利用する際は、TOE によって対象のサービスの利用を許可された者であることが確認されなければならない。このため TOE は他の TSF 実行に先立ち、FIA_UID.1、FIA_UAU.1 により一般利用者の識別認証を実行し、FIA_UID.2、FIA_UAU.2 により WebOTX 管理者の識別認証を実行する。
識別認証に成功した利用者に対して、TOE はサービスの利用を終了するまで認証状態を継続する必要がある。一般利用者の識別認証の場合は、FIA_USB.1a により、WebOTX 管理者の識別認証の場合は FIA_USB.1b により、利用者を代行するサブジェクトに対しロールを割り当てる。

以上、これらの対策に必要な機能要件に該当する、FIA_UAU.1、FIA_UAU.2、FIA_UID.1、FIA_UID.2、FIA_USB.1a、FIA_USB.1b の達成により、O.ID_AUTH を実現できる。

O.ACCESSCONTROL（ユーザ AP のアクセス制御）
このセキュリティ対策方針は、利用者を代行する TOE 内のサブジェクトが、一般利用者ロールに基づくアクセス制御方針に従って許可されたユーザ AP エントリポイントにアクセスすることを求めている。
TOE は「利用者データアクセス制御方針 a」に従いユーザ AP エントリポイントへのアクセスを管理する。
TOE は FDP_ACC.1a、FDP_ACF.1a により、一般利用者ロールとユーザ AP 許可利用者ロールの内容が一致していれば利用権限を満たしていると判定し、ユーザ AP エントリポイントへのアクセスを許可する。
以上、上記の対策に必要な機能要件に該当する、FDP_ACC.1a、FDP_ACF.1a の達成により、O.ACCESSCONTROL を実現できる。

O.USERMANAGE（利用者管理）
このセキュリティ対策方針は、TOE の利用者を予め登録し、TOE が提供するサービス及び保護資産に対する権限を設定しておくことを求めている。

WebOTX 管理者は、「利用者データアクセス制御方針 b」に従い、WebOTX 利用者をあらかじめ TOE に登録し管理する。
FIA_ATD.1 により、TOE は WebOTX 利用者として WebOTX 管理者と一般利用者の2種類のロールを想定し動作する。
WebOTX 利用者の登録／更新／削除の操作は、FMT_MTD.1 により WebOTX 管理者のみ可能とする。WebOTX 管理者は FMT_SMF.1 により、WebOTX 利用者の利用者 ID、パスワード、ロールをアカウント情報に登録する。登録の際に TOE は、パスワードが FIA_SOS.1 により必要な品質尺度を満たしていることの確認を行う。また登録されたロールの内容により、WebOTX 利用者の役割は WebOTX 管理者もしくは一般利用者のいずれかとなるため、利用者 ID に対し割り当てられる役割は、FMT_SMR.1 により維持される。
WebOTX 管理者は FMT_MSA.1 により、アカウント情報に登録された WebOTX 利用者のロールを参照／更新／削除することが可能である。
以上、上記の対策に必要な機能要件に該当する FIA_ATD.1、FMT_MTD.1、FMT_SMF.1、FIA_SOS.1、FMT_SMR.1、 FMT_MSA.1 の達成により、O.USERMANAGE を実現できる。

O.DEPLOYCONTROL（ユーザ AP 配備制御）
このセキュリティ対策方針は、WebOTX 管理者によるユーザ AP 配備サービス実行時における、ユーザ AP 実行サービスの保護について求めている。
TOE は一般利用者に対し継続してユーザ AP 実行サービスを利用可能とするため、「利用者データアクセス制御方針 b」に従い、ユーザ AP 実行サービスを提供するユーザ AP の配備および配備解除のタイミングに配慮する必要がある。TOE はユーザ AP 配備サービス実行時、FDP_ACC.1b および FDP_ACF.1b によるアクセス制御を実行し、稼動中のユーザ AP を再配備もしくは配備解除することによりユーザ AP 実行サービスが停止するのを防ぐ。
以上、上記の対策に必要な機能要件に該当する、FDP_ACC.1b、FDP_ACF.1b の達成により、O.DEPLOYCONTROL を実現できる。

O.PROCESSALIVE（セキュリティ機能の生存チェック）
このセキュリティ対策方針は、ユーザ AP 実行サービス提供中の J2EE コンテナが異常終了した場合に、セキュリティ機能の停止時間を最小にするため、速やかに J2EE コンテナを再開することを求めている。
TOE は、ユーザ AP 実行サービスの提供中に J2EE コンテナの異常終了を確認すると、FPT_RCV.2 により対象の J2EE コンテナの再起動を行う。これにより J2EE コンテナが提供する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 配備制御機能が長時間使用不能になることを防ぐ。
以上、上記の対策に必要な機能要件に該当する、FPT_RCV.2 により O.PROCESSALIVE 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 表 14 に示す。

表 14 セキュリティ要件依存性根拠

コンポーネント	CC Part2 における依存コンポーネント	TOE における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
FIA_ATD.1	なし	なし	なし
FIA_SOS.1	なし	なし	なし
FIA_UAU.1	FIA_UID.1	FIA_UID.1	なし
FIA_UAU.2	FIA_UID.1	FIA_UID.1	なし
FIA_UID.1	なし	なし	なし
FIA_UID.2	なし	なし	なし
FIA_USB.1a	FIA_ATD.1	FIA_ATD.1	なし
FIA_USB.1b	FIA_ATD.1	FIA_ATD.1	なし
FMT_MSA.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	FDP_ACC.1a FDP_ACC.1b FMT_SMR.1 FMT_SMF.1	なし
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	なし
FMT_SMF.1	なし	なし	なし
FMT_SMR.1	FIA_UID.1	FIA_UID.1 FIA_UID.2	なし
FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a	なし
FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a	FMT_MSA.3
FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b	なし
FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1b	FMT_MSA.3
FPT_RCV.2	AGD_OPE.1	AGD_OPE.1	なし

FDP_ACF.1a、FDP_ACF1b において、それぞれ依存関係にある FMT_MSA.3 を対象外としている理由を以下に示す。

1）FDP_ACF.1a

一般利用者代行手続のセキュリティ属性である一般利用者ロールについては、運用管理コマンドで一般利用者を登録または更新する際に明示的に指定される。従って一般利用者ロールの初期値を TOE が設定する必要はない。

ユーザ AP エントリポイントのセキュリティ属性であるユーザ AP 許可利用者ロールについては、WebOTX 管理者がユーザ AP 配備前に設定されていることを確認する運用となっている。従ってユーザ AP 許可利用者ロールの初期値を TOE が設定する必要はない。

2）FDP_ACF.1b

WebOTX 管理者代行手続のセキュリティ属性である WebOTX 管理者ロールについては、運用管理コマンドで WebOTX 管理者を登録または更新する際に明示的に指定される。従って WebOTX 管理者ロールの初期値を TOE が設定する必要はない。

ユーザ AP エントリポイントのセキュリティ属性である、ユーザ AP 利用情報に格納されたユーザ AP 利用者数については、TOE の内部で制御される TSF データであり、外部から内容を操作する手段を持たない。従ってユーザAP利用情報の初期値を TOE が設定する必要はない。

表 14 と上記の理由により必要な依存関係を満たしている。

6.3.3. セキュリティ保証要件根拠

TOE を含む製品である WebOTX Application Server は、多数の一般利用者に対し安定してユーザ AP を利用できる環境を提供することを製品の目的としている。EAL2は TOE の開発段階のセキュリティ対策の分析（系統立ったテストの実施と分析、開発環境や開発生産物の管理状況の評価）を含むので必要十分な選択であるといえる。
また、TOE 製品の特性として、セキュリティ欠陥に対する迅速な対応が求められる。製品の安全性を確保するには継続してセキュリティパッチを提供する必要がある。
よって本セキュリティ機能に対する保証レベルとして EAL2 +ALC_FLR.1 を選択する。

7. TOE 要約仕様

この章では、TOE の要約仕様について記述する。

7.1. TOE の要約仕様

この節では、6．1節で記述したセキュリティ機能要件に対応する TOE の要約仕様について説明する。**表 15** にセキュリティ機能とセキュリティ機能要件の対応表を示す。

表 15 TOE セキュリティ機能とセキュリティ機能要件の対応関係

	一般利用者識別認証機能	WebOTX 管理者識別認証機能	ユーザ AP アクセス制御機能	利用者管理機能	ユーザ AP 配備制御機能	ユーザ AP 復旧機能
FIA_ATD.1				×		
FIA_SOS.1				×		
FIA_UAU.1	×					
FIA_UAU.2		×				
FIA_UID.1	×					
FIA_UID.2		×				
FIA_USB.1a	×					
FIA_USB.1b		×				
FMT_MSA.1				×		
FMT_MTD.1				×		
FMT_SMF.1				×		
FMT_SMR.1				×		
FDP_ACC.1a			×			
FDP_ACC.1b					×	
FDP_ACF.1a			×			
FDP_ACF.1b					×	
FPT_RCV.2						×

7.1.1. 一般利用者識別認証機能

FIA_UID.1
一般利用者識別認証機能は、ユーザ AP 実行サービスの利用を要求する一般利用者に対し、事前に識別を要求する。

一般利用者は、TOE 上のユーザ AP を利用する際に、利用者端末から WWW ブラウザを実行し、ユーザ AP 毎に決められた URL をアクセスして TOE にユーザ AP 利用要求を送信する。
TOE は一般利用者からの要求を J2EE コンテナで受信し、一般利用者識別認証機能を実行する。一般利用者識別認証機能は、利用者 ID、パスワードが存在しない場合、WWW ブラウザに対し利用者 ID、パスワードを要求するコードを返却する。そのコードを受け取った WWW ブラウザはログイン要求画面を表示し、一般利用者は利用者 ID、パスワードを送信する。

FIA_UAU.1
一般利用者識別認証機能は、ユーザ AP 実行サービスの利用を要求する一般利用者に対し、利用者 ID、パスワードによる認証を行う。

一般利用者識別認証機能は、一般利用者から受信した利用者 ID、パスワードを TOE が管理するアカウント情報と照合する。アカウント情報には、WebOTX 利用者の利用者 ID、パスワード、ロールの情報が格納されている。一般利用者識別認証機能は一般利用者から入力された利用者 ID が、アカウント情報内に存在するかを確認する。
入力された利用者 ID が存在しない場合、一般利用者識別認証機能は認証失敗と判断し、WWW ブラウザに対し認証エラーを返却する。
次に一般利用者識別認証機能は、アカウント情報に格納されたパスワードと、一般利用者より送信されたパスワードが合致するかを判断する。合致すれば正当な一般利用者として認証する。
入力されたパスワードが合致しない場合、一般利用者識別認証機能は認証失敗と判断し、WWW ブラウザに対し認証エラーを返却する。

FIA_USB.1a
一般利用者識別認証機能は、識別認証された一般利用者に対し、一般利用者ロールを付与する。

一般利用者識別認証機能はアカウント情報から、利用者 ID に対応する一般利用者ロールを取得し、この一般利用者に割り当てたセッション情報に一般利用者ロールを格納する。
一般利用者ロールは、WebOTX 管理者によりあらかじめ一般利用者に割り当てられる権限を示す値であり、一般利用者が変更することはできない。

7.1.2. WebOTX 管理者識別認証機能

FIA_UID.2
WebOTX 管理者識別認証機能は、利用者管理サービスまたはユーザ AP 配備サービスの利用を要求する WebOTX 管理者に対し、識別を行う。

TOE は、WebOTX 管理者による運用管理コマンド操作の際に、利用者 ID およびパスワードの入力を要求する。これはサービス利用時に必ず最初に実行されるため、迂回は不可能である。管理機構は、WebOTX 管理者識別認証機能を実行し、以下の内容を受信する。
・コマンド内容
・利用者 ID
・パスワード

FIA_UAU.2b
WebOTX 管理者識別認証機能は、識別された WebOTX 管理者に対し、パスワードによる認証を行う。

WebOTX 管理者識別認証機能は受信したコマンドデータを解析し、利用者 ID、パスワード、コマンド内容を取得する。
WebOTX 管理者識別認証機能は、WebOTX 管理者より入力された利用者 ID、パスワードを、TOE が管理するアカウント情報と照合する。アカウント情報には、WebOTX 利用者の利用者 ID、パスワード、ロールの情報が格納されている。WebOTX 管理者識別認証機能は WebOTX 管理者から送信された利用者 ID が、アカウント情報内に存在するかを確認する。
入力された利用者 ID が存在しない場合、WebOTX 管理者識別認証機能は認証失敗と判断し、運用管理コマンドに対し認証エラーを返却する。
次に WebOTX 管理者識別認証機能は、アカウント情報に格納されたパスワードと、WebOTX 管理者より送信されたパスワードが合致するかを判断する。
入力されたパスワードが合致しない場合、WebOTX 管理者識別認証機能は認証失敗と判断し、運用管理コマンドに対し認証エラーを返却する。
次に WebOTX 管理者識別認証機能は、アカウント情報に格納されたロールが、WebOTX 管理者のロールと合致するかを判断する。
以上のチェックが全て合致すれば、正当な WebOTX 管理者として認証する。

FIA_USB.1b
WebOTX 管理者識別認証機能は、識別認証された WebOTX 管理者に対し、WebOTX 管理者ロールを付与する。

WebOTX 管理者識別認証機能はアカウント情報から、利用者 ID に対応する WebOTX 管理者ロールを取得する。WebOTX 管理者ロールは、あらかじめ TOE により割り当てられる値であり、WebOTX 利用者が変更することはできない。

7.1.3. ユーザ AP アクセス制御機能

FDP_ACC.1a
ユーザAPアクセス制御機能は、一般利用者がユーザAPエントリポイントに対しアクセスする場合に許可する操作の方針を「利用者データアクセス制御方針」として予め定義する。ユーザAPアクセス制御機能におけるサブジェクトとオブジェクト間の操作について、表 16 に示す。

表 16　ユーザ AP アクセス制御機能におけるサブジェクトとオブジェクト間での操作規則

サブジェクト	オブジェクト	制御された操作	制御における条件
一般利用者代行手続	ユーザ AP エントリポイント	実行	ユーザ AP に割り当てられたユーザ AP 許可利用者ロールと一般利用者に割り当てられた一般利用者ロールの内容が一致すれば実行

FDP_ACF.1a
ユーザ AP アクセス制御機能は、一般利用者ロールに設定された利用者権限を確認しユーザ AP エントリポイントへのアクセスを制限する。

WebOTX 管理者は、配備前のユーザ AP に対し、ユーザ AP 許可利用者ロールが設定されていることを確認する。J2EE コンテナはユーザ AP 配備の際、ユーザ AP 許可利用者ロールをアクセス制御情報に格納する。
ユーザ AP アクセス制御機能は、識別認証された一般利用者がユーザ AP の利用を要求する際、この一般利用者に割り当てられた一般利用者ロールと、アクセス制御情報から取得したユーザ AP 許可利用者ロールの比較を行う。ユーザ AP アクセス制御機能は利用者データアクセス制御方針 a に従い、一般利用者ロールとユーザ AP 許可利用者ロールの内容が合致するかを調べ、合致した場合にのみ一般利用者に対しユーザ AP エントリポイントへのアクセスを許可する。一致しない場合、ユーザ AP アクセス制御機能は一般利用者の利用要求を拒否し WWW ブラウザにアクセスエラーを通知する。

7.1.4. 利用者管理機能

FIA_ATD.1
利用者管理機能は、WebOTX 利用者のロールをあらかじめ定義する。

TOE は、WebOTX 利用者として、TOE を運用する WebOTX 管理者、ユーザ AP を利用する一般利用者の二種類を想定する。利用者管理機能は、これらの役割に対応する、WebOTX 管理者ロール、一般利用者ロールを定義する。

FIA_SOS.1
利用者管理機能は、WebOTX 利用者のパスワードが以下の条件を満たすことを保証する。

・8 文字以上の英数記号で構成される文字列
利用者管理機能は、利用者管理サービスにおける WebOTX 利用者の登録時及びパスワードの変更時において、新たなパスワードの候補として入力された文字列が上記の基準を満たさない場合には、エラーを返却する。

FMT_MSA.1
利用者管理機能 WebOTX 管理者が WebOTX 利用者を登録する際に、一般利用者ロールと WebOTX 管理者ロールに対する操作を許可する。

利用者管理機能は、利用者データアクセス制御方針 b に基づき、識別認証された WebOTX 管理者に対し、以下の操作を許可する。

・一般利用者ロールの参照
・一般利用者ロールの更新
・一般利用者ロールの削除
・WebOTX 管理者ロールの参照
・WebOTX 管理者ロールの更新
・WebOTX 管理者ロールの削除

FMT_MTD.1
利用者管理機能は WebOTX 利用者に対し、TSF データの操作を制限する。

利用者管理機能は、J2EEコンテナおよび管理機構により、WebOTX利用者のTSFデータに対する操作を制限する。利用者管理機能によるTSFデータ管理について 表 17 に示す。

表 17 TSF データの管理

TSF データのリスト	操作	許可された識別された役割
アカウント情報	登録	WebOTX 管理者
	更新	WebOTX 管理者
	削除	WebOTX 管理者

FMT_SMR.1
利用者管理機能は、WebOTX 利用者の役割を維持する。

利用者管理機能は、WebOTX 利用者に対し、一般利用者ロールまたは WebOTX 管理者ロールのいずれかを設定する。それぞれのロールに対する更新の権限は、FIA_MSA.1 により WebOTX 管理者に限定される。

FMT_SMF.1
利用者管理機能は、WebOTX 管理者に対し管理機能を提供する。

利用者管理機能は、WebOTX 管理者に対し、利用者管理サービスを提供することにより以下のセキュリティ管理機能を提供する。

・利用者情報（利用者 ID、パスワード、ロール）の登録
・利用者情報（利用者 ID、パスワード、ロール）の更新
・利用者情報（利用者 ID、パスワード、ロール）の削除
・利用者情報（利用者 ID、パスワード、ロール）の参照

7.1.5. ユーザ AP 配備制御機能

FDP_ACC.1b
TOEは、WebOTX管理者がユーザAP配備サービスを実行する際に許可する操作の方針を「利用者デ

ータアクセス制御方針」として予め定義する。ユーザAP配備制御機能におけるサブジェクトとオブジェクト間の操作について 表 18 に示す。

表 18 ユーザ AP 配備制御機能におけるサブジェクトとオブジェクト間での操作規則

サブジェクト	オブジェクト	制御された操作	制御における条件
WebOTX 管理者代行手続	ユーザ AP エントリポイント	配備	なし
		再配備	ユーザ AP 利用情報に格納されたユーザAP利用者数が0でなければ操作を待ち合わせる。
		配備解除	ユーザ AP 利用情報に格納されたユーザAP利用者数が0でなければ操作を待ち合わせる。

FDP_ACF.1b
ユーザ AP 配備制御機能は、ユーザ AP 配備サービスの操作を制限する。

ユーザ AP 配備制御機能は運用管理コマンドからユーザ AP の再配備／配備解除の要求を受け付けた際、以下を実行する。
・ユーザ AP の再配備の場合
ユーザ AP 配備制御機能は指定されたユーザ AP を利用中の一般利用者が存在するかをユーザ AP 利用情報のユーザ AP 利用者数により確認する。ユーザ AP 利用者数が0でない場合、ユーザ AP 配備制御機能すべての一般利用者の利用完了を待ちあわせる。一般利用者の利用完了後、ユーザ AP 配備制御機能は実行中のユーザ AP 制御データおよびアクセス制御情報をTOE から削除した後、新たなユーザ AP 制御データおよびアクセス制御情報を生成する。
・ユーザ AP の配備解除の場合
ユーザ AP 配備制御機能は再配備の処理と同様、指定されたユーザ AP を利用中の一般利用者が存在するかをユーザ AP 利用情報のユーザ AP 利用者数により確認し、実行中の場合は処理を待ち合わせる。次にユーザ AP 配備制御機能はユーザ AP 制御データおよびアクセス制御情報をTOE から削除する。これにより TOE はユーザ AP 実行サービス提供不可の状態になる。

7.1.6. ユーザ AP 復旧機能

FPT_RCV.2
ユーザ AP 復旧機能は、J2EE コンテナの異常終了時に自動回復を行う。

ユーザ AP 復旧機能は、ユーザ AP 実行サービスを提供している J2EE コンテナの稼動状態を監視する。J2EE コンテナが異常終了した場合、TOE は J2EE コンテナが動作するプロセスの異常終了を OS から通知を受け取ることにより検出すると、対象のユーザ AP エントリポイントが含まれる J2EE コンテナの再起動を行う。
もし J2EE コンテナの再起動に失敗した場合、ユーザ AP 復旧機能は J2EE コンテナの再起動を予め設定された回数の範囲内で繰り返し試みる。
所定回数繰り返しても J2EE コンテナの再起動が成功しない場合、ユーザ AP 復旧機能は自動復旧不

能と判断し、J2EE コンテナの再起動に失敗した旨の内容を障害ログに出力し WebOTX 管理者の介入を要求する。
WebOTX 管理者は、障害ログにより J2EE コンテナの再起動失敗を検出した場合、障害の原因を取り除いた後、手動で TOE を再起動し正常な状態に復旧させる。

これにより J2EE コンテナが提供する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 配備制御機能が使用できない時間を最小限にする。

以上