# 認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

| | |
|---|---|
| **申請受付日（受付番号）** | **平成20年8月26日** (IT**認証**8236) |
| **認証番号** | C0221 |
| **認証申請者** | **日本電気株式会社** |
| TOE**の名称** | StarOffice X V1.5 |
| TOE**のバージョン** | 1.5.02 |
| PP**適合** | **なし** |
| **適合する保証パッケージ** | EAL2 |
| **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21年6月29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　山里　拓己

**評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。**

① 情報技術セキュリティ評価のためのコモンクライテリア バージョン3.1 改訂第2版 (翻訳第2.0版)
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 改訂第2版　(翻訳第2.0版)

**評価結果：合格**

「StarOffice X V1.5」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

# 目次

# 1 全体要約

## 1.1 はじめに

この認証報告書は、「StarOffice X V1.5」（以下「本TOE」という。）について、みずほ情報総研株式会社　情報セキュリティ評価室（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である日本電気株式会社に報告するとともに、本TOEに関心を持つ利用者や運用者に対しセキュリティ情報を提供するものである。

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

本認証報告書は、本TOEの運用に携わる運用管理責任者、システム管理者及びオフィス責任者を読者と想定している。本認証報告書は、本TOEに対して適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

### 1.1.1 評価保証レベル

本TOEが適合を主張する評価保証レベルは、EAL2適合である。

### 1.1.2 PP適合

適合するPPはない。

## 1.2 評価製品

### 1.2.1 製品名称

本TOEは、以下の製品のセキュリティ機能である。

| | |
|---|---|
| 製品名称： | StarOffice X Standard V1.5<br>StarOffice X Enterprise V1.5 |
| バージョン： | 1.5.02 |
| 開発者： | 日本電気株式会社 |

### 1.2.2 製品概要

StarOffice X Enterprise V1.5 及び StarOffice X Standard V1.5 は会社組織内のネットワーク環境で使用するグループウェアであり、利用するユーザ規模が 1000 ユーザ以

上の場合には StarOffice X Enterprise V1.5 を、1000 ユーザ未満の場合には StarOffice X Standard V1.5 を使用する。

本製品（StarOffice X Enterprise V1.5 または StarOffice X Standard V1.5）を運用する前に、会社内の組織に対応付けられたオフィスを、システム管理者が本製品に登録する。本製品の利用者（オフィス責任者、一般利用者）は、自身が登録されているオフィスのキャビネット配下に、付与されたアクセス権限にしたがって文書データを登録することができる。キャビネット配下に登録された文書データは、キャビネットを使用する利用者の所属組織、利用者種別、職位などに基づいて、利用者同士で共有し、相互に参照することができる。

本製品は、利用目的に合わせて複数のキャビネットを登録することができる。キャビネット配下には、複数の文書データをまとめる単位としてフォルダを登録することができる（例：オフィスを会社内の事業本部に対応付けた場合、キャビネットとして当該事業本部の中の事業部等を登録し、フォルダとして当該事業部等の中の部等を登録）。また、キャビネットやフォルダ、文書データに対するリンクとなるショートカットを登録することができる。なお、キャビネット配下に格納された文書データは、本製品が提供するメールや掲示板から、ショートカットにより連携して利用することができる。

本製品は、サービス機能として、キャビネットサービス機能、メールサービス機能、掲示板サービス機能、スケジュールサービス機能、施設予約機能、電話帳機能を提供している。さらに、メンテナンスのためのサービス機能として、運用機能を提供している。

### 1.2.3 TOE範囲とセキュリティ機能

TOEは、StarOffice X Enterprise V1.5及びStarOffice X Standard V1.5に共通するコンポーネントであり、一般機能として、1.2.2に記載した7つのサービス機能を提供している。TOEは、上記サービス機能の一つであるキャビネットサービス機能が提供する、オフィスのキャビネット配下のフォルダや文書データ、及びショートカットに対して不正アクセス（破壊・改ざん・暴露）を防止するために、セキュリティ機能として、識別認証機能とアクセス制御機能を提供している。

TOEの構成を図1-1に示す。TOEはWebサーバ上及びリソースサーバ上に配置され、TOEの利用において、利用者（オフィス責任者、一般利用者）は、利用者クライアントよりWebサーバを介し、リソースサーバ上のTOEのサービス機能（運用機能以外）を使用することができる。また、システム管理者は、Webサーバ及びリソースサーバのローカルコンソールより、各サーバ上のTOEの運用機能を使用することができる。

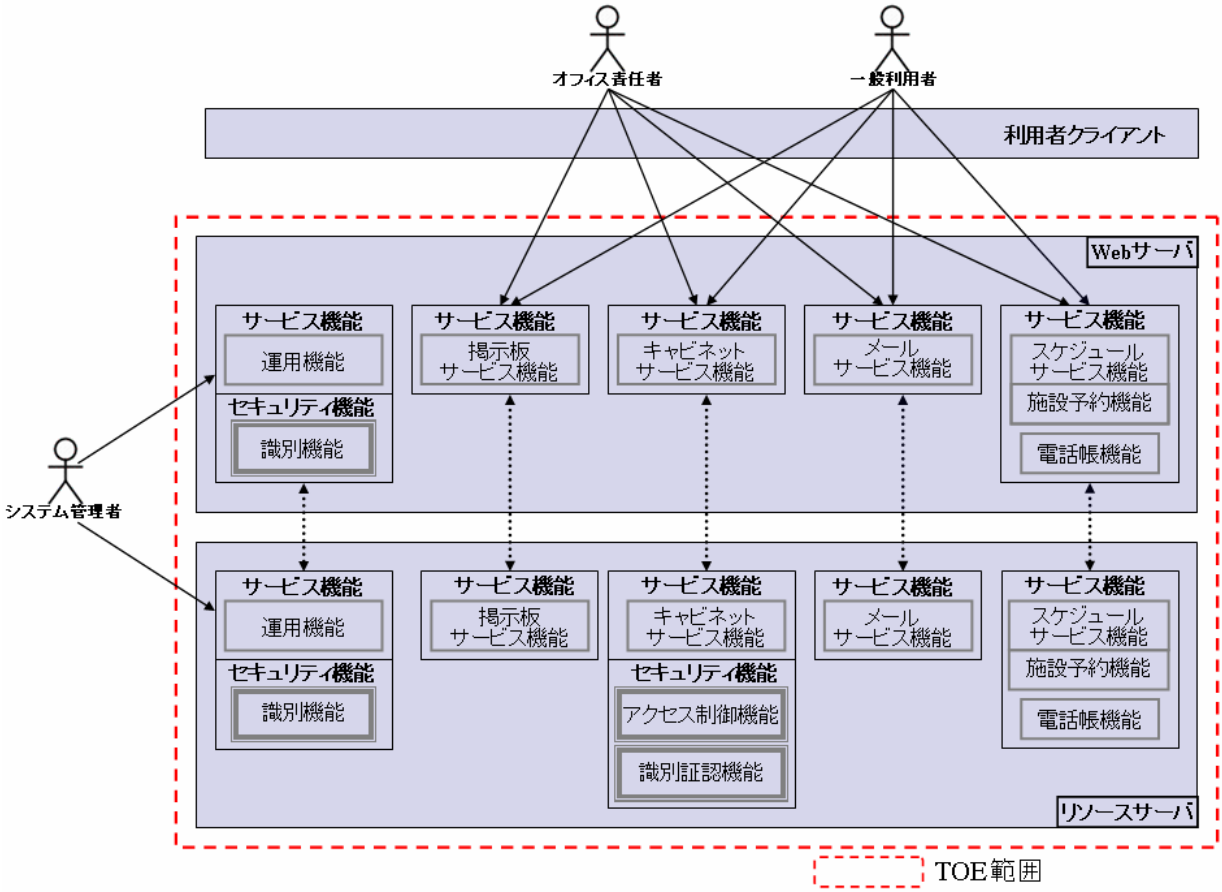


**図1-1 TOEの構成**

利用者（オフィス責任者、一般利用者）がTOEのキャビネットサービス機能を使用する際に、TOEのセキュリティ機能である識別認証機能及びアクセス制御機能により、適切な本人確認がなされた上で、権限が付与されているオブジェクト（フォルダ、文書データ等）のみへのアクセスが許可されるように制御される。

また、システム管理者がTOEの運用機能を使用する際に、TOEのセキュリティ機能である識別認証機能に含まれる識別の機能が使用される（ローカルコンソールからの操作がシステム管理者に限定されることについては、TOE運用の前提条件として要請され、実現される。TOEのセキュリティ機能としては、アカウントにより、システム管理者を識別するだけである）。

なお、運用機能は、システム管理者に対して、以下の機能を提供する。

・一般利用者、オフィス責任者の登録先となるオフィスの作成や、利用者の登録、更新、削除、パスワードポリシーの設定を行う、ディレクトリサービスメンテナンス機能

・キャビネットの初期設定や管理を行う、キャビネットサービスメンテナンス機能

## 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「StarOffice X V1.5 セキュリティターゲット」（以下「本ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、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・製造・出荷環境が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、「StarOffice X V1.5 評価報告書」（以下「評価報告書」という。）[13]に示されている。なお、評価方法は、CEM（[11][12]のいずれか）に準拠する。

## 1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成21年6月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

# 2 TOE概要

## 2.1 セキュリティ課題と前提

TOEが解決すべき課題と、必要とする前提を以下に示す。

### 2.1.1 脅威

本TOEは、表2-1に示す脅威を想定し、これに対抗する機能を備える。

**表2-1 想定する脅威**

| 識別子 | 脅　威 |
|---|---|
| T.SPOOFING<br>(なりすまし) | 悪意のある第三者、及び TOE の利用者が、TOE の正当な利用者になりすまして TOE の操作を行う、または利用中の正当な TOE 利用者の離席時に TOE の操作を行うことにより、利用者データを破壊・改ざん・暴露するかもしれない。 |
| T.ILLEGAL_ACCESS<br>(不正なアクセス) | TOEの正当な利用者が、故意に許可されていない操作を行うことにより、利用者データを破壊・改ざん・暴露するかもしれない。 |

### 2.1.2 組織のセキュリティ方針

本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存在しない。

### 2.1.3 操作環境の前提条件

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

| 識別子 | 前提条件 |
|---|---|
| A.SAFE_PLACE<br>(安全な場所) | TOEが稼動するWebサーバ、及びリソースサーバに関連するハードウェアは、入退室が管理された物理的セキュリティを確保した部屋に設置する。この部屋への入室は、許可された人のみに限定する。 |
| A.NETWORK | TOEが稼動するWebサーバ、及びリソース |

| | |
|---|---|
| (ネットワーク環境) | サーバは、ファイアウォールにより、イントラネットからのアクセスを制限した保護されたネットワークに接続している。 |
| A.SECURE_CHANNEL<br>(セキュアな通信) | TOEの通信路は、暗号化による通信内容の秘匿を行う。 |
| A.SYSTEM_ADMIN<br>(システム管理者の運用操作) | システム管理者による TOE の運用操作は、Web サーバ上、及びリソースサーバ上のコンソールのみから実行する。<br>（補足）ガイダンスで、A.NETWORK の実現も含めポートの制限をすることが要請され、クライアントからの TOE 運用操作はできない。 |
| A.SERVER_USER<br>(サーバユーザ) | TOEが稼動するWebサーバ、及びリソースサーバのコンソールからの操作は、システム管理者のみ、利用することができる。<br>（補足）ガイダンスで、Webサーバ及びリソースサーバのOSの識別認証機能により、システム管理者のみが利用できるようにすることが要請されている。 |
| A.ADMINISTRATOR<br>(信頼できる管理者) | TOE の運用管理責任者、システム管理者、オフィス責任者は、役割に付与された行為のみを行い、悪意のある行為を行わない。 |
| A.PASSWORD_MANAGEMENT<br>(パスワード管理) | TOEの利用者は、TOEにアクセスするための認証情報(パスワード)を、第三者に知られないように管理する。 |
| A.PASSWORD<br>(パスワード) | システム管理者は、TOE にアクセスするための認証情報(パスワード)の最小文字数を、8 文字以上の長さに設定する。<br>（補足）ガイダンスで、パスワードポリシー設定の詳細が要請されている。設定されたパスワードポリシーに従い、TOE のセキュリティ機能により、パスワードの品質チェックが行われる。 |
| A.UNLOCK_ACCOUNT<br>(アカウントロック解除) | システム管理者は、オフィス責任者、一般利用者が認証に失敗してアカウントロックになったときのロック解除を、システム管理者のみが行うように設定する。 |
| A.SESSION_TIMEOUT | 利用者クライアントからTOEへのアクセスが |

| | |
|---|---|
| (セションタイムアウト時間) | ないときのタイムアウト時間は、20分から60分の間で値を設定する。 |
| A.CLIENT<br>(利用者クライアント) | 利用者クライアントでは、StarOffice X V1.5 ビジネスナビゲータを利用しないものとする。<br>（補足）ガイダンスで、上記ビジネスナビゲータをインストールしないように要請されている。サーバ側でシステム管理者が介在しない限り、クライアントのみで勝手なインストールはできない。 |
| A.ACCESS_PRIVILEGE<br>(アクセス権変更権の付与) | TOE のアクセス権変更権は、オフィス責任者にのみ付与する。 |

### 2.1.4 製品添付ドキュメント

本TOEに添付されるドキュメントの識別を以下に示す。読者は、上記表2-2の内容、及び上記表2-2には記載されていない注意喚起事項を実施するために、下記ドキュメントの十分な理解と遵守が要求される。

- StarOffice X Standard V1.5　－運用管理者編－　スタートアップガイド　第 2 版
- StarOffice X Enterprise V1.5　－運用管理者編－　スタートアップガイド　第 2 版
- StarOffice X V1.5　－運用管理者編－　コンフィグレーションガイド　第 2 版
- StarOffice X V1.5　－運用管理者編－　利用者環境構築・運用ガイド　第 2 版
- StarOffice X V1.5　－運用管理者編－　リファレンスガイド　第 2 版
- StarOffice X V1.5　－運用管理者編－　セキュリティ設定ガイド　初版
- StarOffice X V1.5　－利用者編－　スタートアップガイド　第 2 版
- StarOffice X V1.5　－利用者編－　リファレンスガイド　第 2 版
- Enterprise Directory Server V5.0 運用の手引き 第 9 版

### 2.1.5 構成条件

本TOEは、StarOffice X V1.5である。本評価は以下のハードウェア及びソフトウェア上での動作を対象とする。なお、本構成に示されるハードウェア及びソフトウェアの信頼性は本評価の範囲外である。

（1） TOE動作に必要なハードウェアの評価構成

| 端末・装置名 | | | |
|---|---|---|---|
| | ベンダ名 | 種別 | 説明 |
| Webサーバ | | | |
| | NEC,<br>その他 | 本体 | Express5800シリーズ<br>PC/AT互換機 |
| | | メモリ | 4GB以上 |
| | | HDD | 空き容量： 0.7 GB以上 |
| リソースサーバ | | | |
| | NEC | 本体 | Express5800シリーズ |
| | | メモリ | 4GB以上(6GB以上を推奨) |
| | | HDD | 空き容量： 1.6 GB以上 |
| 利用者クライアント | | | |
| | NEC,<br>その他 | 本体 | PC/AT互換機 |
| | | メモリ | 512MB以上を推奨 |
| | | HDD | 空き容量： 300MB以上を推奨 |

（2）TOE動作に必要なソフトウェアの評価構成

[Web サーバ]

・Windows Server 2003 Standard Edition SP2 (OS)
・Internet Information Services 6.0 (Web サーバソフトウェア)
・.NET Framework 2.0 SP1、及び
.NET Framework 2.0 日本語 Language Pack SP1 (アプリケーション実行環境)
・ASP.NET 2.0 AJAX Extension 1.0 (AJAX 実行環境)
・J2SDK 5.0 update 16、及び JDBC ドライバ (Java 実行環境)
・WebOTX Web Edition Ver. 7.11 (アプリケーションサーバソフトウェア)

[リソースサーバ]

・Windows Server 2003 Standard Edition SP2 (OS)
・Internet Information Services 6.0 (Web サーバソフトウェア)
・.NET Framework 2.0 SP1、及び
.NET Framework 2.0 日本語 Language Pack SP1 (アプリケーション実行環境)
・J2SDK 5.0 update 16 (Java 実行環境)
・WebOTX Web Edition Ver. 7.11 (アプリケーションサーバソフトウェア)
・SQL Server 2005 Express Edition (DBMS)

[利用者クライアント]

・Windows XP Professional Edition SP2、または Windows XP Professional Edition SP3、または Windows Vista Business Edition SP1 のいずれか (OS)
・Internet Explorer 6.0 SP2、または Internet Explorer 7.0 のいずれか (Web ブラウザ)
ただし、OS が Windows Vista の場合は Internet Explorer 7.0 のみ

## 2.2 セキュリティ対策

TOEは、具備したセキュリティ機能（識別認証機能、アクセス制御機能）により以下のように2.1.1の脅威に対抗する。

TOEは、2.1.1の脅威に対抗するために、識別認証機能により、TOEの許可された利用者をユーザIDとパスワードにより役割（オフィス責任者、一般利用者）も含め識別認証（本人確認）し、さらに、アクセス制御機能により、各役割の各許可利用者に付与されている権限の範囲内で、キャビネットサービス機能が管理するオブジェクト（オフィス、キャビネット、フォルダ、文書、ショートカット）へのアクセスを許可する制御を行う。

TOEの識別認証機能は、TOEの許可利用者（オフィス責任者、一般利用者）のパスワード作成・変更における品質尺度の検証の機能、認証失敗の累積時のアカウントロック機能、及び利用者クライアントからの無操作状態が一定時間経過した場合のセッションタイムアウト（セッションを切断）の機能も提供している。

また、TOEのアクセス制御機能は、識別認証された一般利用者が、キャビネットサービス機能が管理するオブジェクトの操作を行うときに、当該一般利用者に対応付けられた一般利用者プロセスが保持する利用者所属組織情報、利用者職位情報、及び利用者識別情報と、操作対象となるオブジェクトの利用許可者情報に指定されている利用者所属組織、利用者職位、及び利用者識別とが一致したとき、操作を許可する。これらの条件が一致しないときには、一般利用者への操作を許可しない。

また、TOEのアクセス制御機能は、識別認証されたオフィス責任者が、自身の所属組織において、キャビネットサービス機能が管理するオブジェクトの操作を行うときに、オフィス責任者に対応付けられたオフィス責任者プロセスが保持する利用者識別情報と、操作対象となるオブジェクトが保持するオフィス責任者情報とが一致したとき、操作を許可する。自身の所属組織でない場合（操作対象となるオブジェクトが保持するオフィス責任者情報と一致しないとき）には、オフィス責任者は一般利用者扱いとなり、オフィス責任者プロセスが保持する利用者所属組織情報、利用者職位情報、及び利用者識別情報と、操作対象となるオブジェクトの利用許可者情報に指定されている利用者所属組織、利用者職位、及び利用者識別とが一致したとき、操作を許可する。これらの条件が一致しないときには、オフィス責任者への操作を許可しない。

なお、TOEのアクセス制御機能により、各オフィスに対して、当該オフィスのオフィス責任者のみがキャビネットの登録と管理を行うことができ、さらに、キャビネット配下の各フォルダ、各文書、各ショートカットに利用者ごとのアクセス権（登録、参照、更新、削除、コピー等）を設定することができる。

また、システム管理者がTOEの運用機能を使用する際に、上記識別認証機能に含

まれる識別の機能が使用され、Webサーバ上、及びリソースサーバ上のOSに登録されているアカウントによる識別が行われる（ローカルコンソールからの操作がシステム管理者に限定されることについては、TOE運用の前提条件として要請され、上記OSの識別認証機能により実現される）。

システム管理者は、TOEの運用機能以外に、TOEのアクセス制御機能の一部として、TOEの識別認証機能に関わる設定（利用者のユーザID及びパスワードの作成等、パスワード最小長、アカウントロックを行う閾値、アカウントロックの解除、セッションタイムアウトを行う時間等の設定）を行う機能が提供されている。利用者（オフィス責任者、一般利用者）は、システム管理者が初期設定を行った自身のパスワードを変更することができる機能を提供されている。

# 3 評価機関による評価実施及び結果

## 3.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

## 3.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年9月に始まり、平成21年6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21年2月に製造・配送現場へ赴き、記録、現物及びスタッフへのヒアリングにより、配付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21年3月及び4月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

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

## 3.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

### 3.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価した開発者テストの概要を以下に示す。

1) 開発者テスト環境

開発者が実施したテストの構成を図3-1に示す。

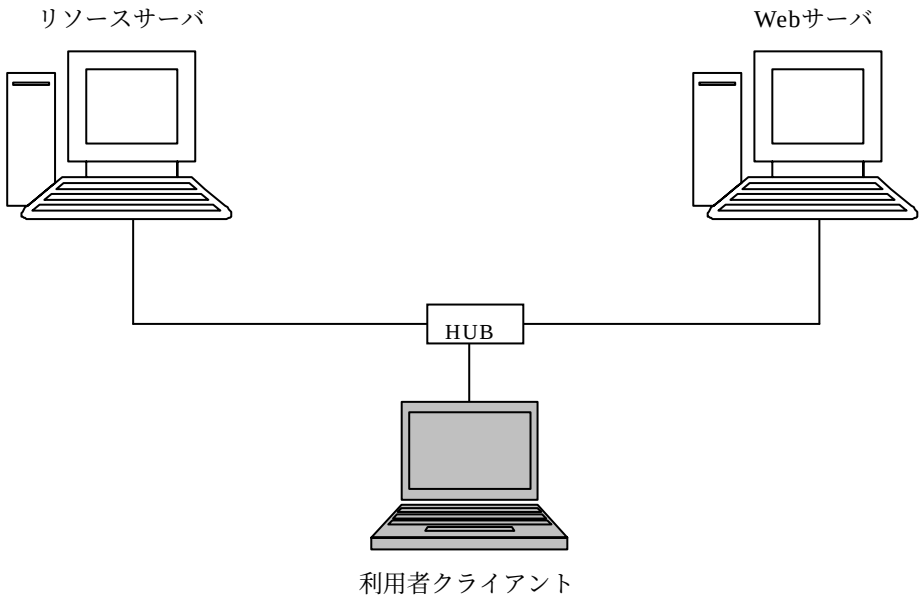


**図3-1　開発者テストの構成**

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。開発者テストで使用されたソフトウェア構成、及びハードウェア構成を表3-1に示す。

**表3-1　開発者テストのソフトウェア構成、及びハードウェア構成**

| ハードウェア | | ソフトウェア |
|---|---|---|
| Webサーバ(1台) | 本体：PC/AT互換機<br>メモリ：2GB<br>HDD:98GB | ・StarOffice X V1.5 1.5.02（Webサーバに設置されるべきコンポーネント一式）<br>・Windows Server 2003 Standard Edition SP2 (OS)<br>・Internet Information Services 6.0 (Webサーバソフトウェア)<br>・.NET Framework 2.0 SP1、及び<br>.NET Framework 2.0 日本語 Language Pack SP1 (アプリケーション実行環境)<br>・ASP.NET 2.0 AJAX Extension 1.0 (AJAX実行環境)<br>・J2SDK 5.0 update 16、及びJDBCドライバ (Java実行環境)<br>・WebOTX Web Edition Ver. 7.11 (アプリケーションサーバソフトウェア) |
| リソースサーバ(1台) | 本体：Express5800シリーズ<br>メモリ：2.5GB<br>HDD：26GB | ・StarOffice X V1.5 1.5.02（リソースサーバに設置されるべきコンポーネント一式）<br>・Windows Server 2003 Standard Edition SP2 (OS)<br>・Internet Information Services 6.0 (Webサーバソフトウェア)<br>・.NET Framework 2.0 SP1、及び<br>.NET Framework 2.0 日本語 Language Pack SP1 (アプリケーション実行環境)<br>・J2SDK 5.0 update 16 (Java実行環境)<br>・WebOTX Web Edition Ver. 7.11 (アプリケーションサーバソフトウェア)<br>・SQL Server 2005 Express Edition (DBMS) |
| 利用者クライアント(1台) | 本体：PC/AT互換機<br>メモリ：512MB以上<br>HDD：300MB以上 | ・Windows XP Professional Edition SP2、Windows XP Professional Edition SP3、Windows Vista Business Edition SP1 (OS)<br>・Internet Explorer 6.0 SP2、Internet Explorer 7.0 (Webブラウザ)<br>※ただし、OSがWindows Vistaの場合はInternet Explorer 7.0のみ<br>※利用者クライアントは1台であるが、開発者テストではOS及びブラウザ |

| ハードウェア | | ソフトウェア |
|---|---|---|
| | | についての組み合わせのすべてのパタンについてテストを実施し確認。 |

2) 開発者テスト概説

開発者の実施したテストは以下のとおり。

a. テスト概要

開発者テストで実施されたテストの概要は以下のとおり。

（1）テスト手法は、開発者の手動操作によるリソースサーバからのコマンド及び GUI ツールの操作、及び利用者クライアントからの Web 画面の操作により実施している。前者は、TOE を使用するシステム管理者向けの TSFI を刺激し、後者は TOE を使用するオフィス責任者及び一般利用者向けの TSFI を刺激する。

（2）各テストの実際のテスト結果は、メッセージ表示、画面表示、テスト結果ファイル等により、確認がなされた。

b. 実施テストの範囲

テストは開発者によって206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。

c. 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。

### 3.3.2 評価者独立テスト

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

1) 評価者独立テスト環境

評価者が実施したテストの構成は、図3-1に示した開発者テストの構成と同一の構成である。

ただし、STにおいて識別されているTOE評価構成の中の利用者クライアントにおけるソフトウェア構成については、表3-1に示されたもののうち、Windows XP SP2 - Internet Explorer 6.0とWindows Vista - Internet Explorer 7.0の組み合わせでのみ評価者テストが実施された。

TSFIはサーバ側のインタフェースであり、クライアントからサーバへ送信するhttpリクエストに関して、OSやブラウザの組み合わせに依存する差異はヘッダ部分（User-Agentに記述されるバージョン情報等）のみであり、TOEがその情報を参照してふるまいを変えることはないため、Windows XPとInternet Explorerの組み合わせについては、表3-1に示された4種類のうち、上記1種類のみで十分であると判断された。

2) 評価者独立テスト概説

評価者の実施した独立テストは以下のとおり。

a. 独立テストの観点

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点での独立テストを考案した。

（1）開発者テストのサンプリングという観点では、SFR（サブジェクト、オブジェクト、操作）の網羅性、TSFの網羅性、及びインタフェースタイプ（クライアントのWebブラウザ画面が起動元となるインタフェース、サーバのコマンド及びGUIツールが起動元となるインタフェース）の網羅性を考慮した。

（2）開発者テストの厳密性及び十分性を補足するために、下記の観点を考慮した。

－開発者テストでは考慮されていないインタフェースの正しいふるまいの確認（セッションタイムアウト発生時のTOE動作の確認；オフィス責任者は自オフィス以外では一般利用者権限のみとなることの確認；フォルダ内の当該利用者に何らかの権限が付与されている文書に対してのみ、取りまとめ機能であるクリップ操作が可能であることの確認）

－パスワードのパラメタ（入力可能・不可能文字）のバリエーションをテストすることによる、正しいふるまいの確認

－インタフェース起動法を拡張し、ショートカットを介した文書アクセスにおけるアクセス制御機能の正しいふるまいの確認

－インタフェースタイプを拡張し、GUIのインタフェースによるシステム管理者のサーバ操作の正しいふるまいの確認（開発者テストでは、コマンドのインタフェースによるサーバ操作しか確認されていない場合）

－テストの条件を変えて、一般利用者がフォルダの削除権限はあるが、当該フォルダ内のオブジェクトに削除権限がない場合のアクセス制御機能の正しいふるまいの確認

b. テスト概要

評価者が実施した独立テストの概要は以下のとおり。

（1）開発者テストの全206項目のうち、54項目をサンプリングし、実施した。
（2）開発者テストを補足する独立テストは、17項目実施し、評価者の手動操作により行った。テスト結果は、画面確認、メッセージ確認、文書ファイルへのアクセス可能性等により行った。

c. 結果

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

### 3.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性の可能性について、必要と思われる侵入テストを考案し実施した。評価者侵入テストの概要を以下に示す。

1) 評価者侵入テスト概説

評価者の実施した侵入テストは以下のとおり。

a. 懸念される脆弱性

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

(1) オープンポートに関係する公知の脆弱性
(2) 公開されている攻撃コードの悪用可能性
(3) Webインタフェースにおける入力値（範囲外のパラメタ値等）による脆弱性
(4) httpsコマンドの改ざん送付による不正アクセスの可能性
(5) Webアプリケーションの脆弱性（クエリストリング、hiddenパラメタ）
(6) セッションIDの推測の脆弱性
(7) Webサービスに対する脆弱性（不要なスクリプトファイルやファイルの残存）
(8) Webアプリケーションの脆弱性2（クロスサイトスクリプティング、SQLインジェクション）
(9) 実行可能ファイルのキャビネット登録による脆弱性
(10) セキュリティ機能実行中のケーブル取り外しによる脆弱性
(11) 同時アクセスによる処理の混乱の脆弱性
(12) システム管理者による設置・生成・立ち上げ時の誤操作の脆弱性
(13) ディレクトリサービス停止状態におけるキャビネットサービスへのア

クセスの脆弱性（TOE初期化時の脆弱性）

評価者は、上記(1)～(13)の脆弱性の識別において、TOEがWebアプリケーションである特性を考慮し、公知の脆弱性DB、及びWebプログラミングに関する公開脆弱性情報を活用すると同時に、開発者から提出された証拠資料（機能仕様、セキュリティアーキテクチャ証拠資料、ガイダンス等）に基づき、バイパス、改ざん、直接攻撃、監視、及び誤使用の観点で脆弱性の探索を行った。

b. 実施テストの範囲

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

(1) 侵入検査ツールにより、オープンポートに関係する公知の脆弱性を探索した。
(2) 公知の脆弱性DBの探索結果を踏まえ、TOEが利用しているアプリケーションに対する公開攻撃コードを探索し、悪用可能な攻撃コードが存在しないことを確認した。
(3) Webインタフェースからのパラメタ値を不適切（範囲外等）に入力（一部送信データをキャプチャし、改ざんできるツールを活用）し、TOEのふるまいを確認した。
(4) 許可されない役割等のページで実行可能なコマンドをツールで送付し、キャビネット内のデータへの許可されないアクセスができないことを確認した。
(5) 保護が必要な認証画面ページを対象に、クエリストリングやhiddenパラメタの使用時の安全性を確認した。
(6) Cookieに含まれるtoken（セッションIDの値）をツールによりキャプチャし、ランダムで推測しにくい値になっていることを確認した。
(7) ディレクトリ洗い出しツールにより、Webサーバに不要なスクリプトファイルが含まれる設定ファイルやフォルダの残存がないことを確認した。
(8) Web脆弱性検査ツールにより、Webアプリケーションの脆弱性（クロスサイトスクリプティング、SQLインジェクション）を探索した。
(9) 実行可能ファイル（exeファイル、マクロを含むファイル）がキャビネットに登録できても、問題ないことを確認した。
(10) セキュリティ機能実行中のケーブル取り外しが、セキュリティに影響しないことを確認した。
(11) 同時アクセス操作が発生した場合に、処理が混乱して許可されないアクセス操作が可能になるようなことがないことを確認した。
(12) システム管理者の誤操作（再インストール）があっても確認手段があり、

初期化状態が維持されることを確認した。

(13) TOE初期化時に識別認証機能が実行されない状況下でも、キャビネットのオブジェクトへのアクセスが保護される仕組みが適切に動作することを確認した。

c. 結果

実施した評価者侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

## 3.4 評価結果

### 3.4.1 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

### 3.4.2 評価者コメント/勧告

特になし。

# 4 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。
② 所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、本ST及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

# 5 結論

## 5.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL2に対する保証要件を満たすものと判断する。

## 5.2 注意事項

なし。

# 6 用語

本報告書で使用されたCCに関する略語を以下に示す。

| | |
|---|---|
| CC | Common Criteria for Information Technology Security Evaluation(セキュリティ評価基準) |
| CEM | Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法） |
| EAL | Evaluation Assurance Level（評価保証レベル） |
| PP | Protection Profile（プロテクションプロファイル） |
| ST | Security Target（セキュリティターゲット） |
| TOE | Target of Evaluation（評価対象） |
| TSF | TOE Security Functionality（TOEセキュリティ機能） |
| TSFI | TSF Interface（TSFインタフェース） |

本報告書で使用された用語の定義を以下に示す（順不同）。

| | |
|---|---|
| 運用管理責任者 | TOEの運用管理全般に責任を持つ人物である。<br>・システム管理者の任命を行う。<br>・TOEを利用しない。 |
| システム管理者 | TOEの初期設定業務、運用管理業務を行う人物である。<br>・運用管理責任者により任命される。<br>・TOEへのオフィスの登録とその管理を行う。<br>・オフィス責任者の任命とTOEへの登録、管理を行う。<br>・一般利用者のTOEへの登録、管理を行う。 |
| オフィス責任者 | 自身の所属するオフィスの管理業務を行う人物である。<br>・各オフィスに1名、システム管理者により、一般利用者のなかから選出される。<br>・所属するオフィスにおいてキャビネットの登録と管理を行う。<br>・キャビネット配下のフォルダ、文書、ショートカットに、アクセス権を設定する。 |
| 一般利用者 | TOEにおける利用操作を行う人物である。<br>・「所属組織」、「職位」が決定している。<br>・付与された権限に基づいて、TOEの操作権限を持つ。 |
| リソースサーバ | TOEが管理するリソースデータを配置するサーバ。 |
| Webサーバ | TOEの利用者要求を受け付けるアプリケーションを配置するサーバ。 |
| ビジネスナビゲー | TOEの機能を利用するためのクライアントアプリケーション。 |

| | |
|---|---|
| タ | ポータルと同等の機能（キャビネット機能、メール機能、スケジュール/施設予約機能、電話帳機能等）を利用可能（本評価では、標準的であるブラウザからのポータルの利用を想定し、ビジネスナビゲータは評価構成から外れている）。 |
| キャビネットサービス | 文書データの登録・更新の管理、保管を行うサービス機能。 |
| オフィス | TOEの利用者が所属している組織を表現する単位。<br>システム管理者により、オフィスが作成される。<br>オフィスの直下には、キャビネットが複数格納できる。 |
| キャビネット | 文書データを階層構造で保管する最上位の単位。<br>キャビネットの配下には、複数のフォルダや文書、及びショートカットを格納できる。 |
| フォルダ | 文書データを階層構造で管理する単位。<br>フォルダの配下には、複数のフォルダや文書、及びショートカットを格納できる。 |
| 文書 | 文書データを表現する単位。<br>単一の文書ファイル、または複数の文書ファイルを関連付けて管理する。 |
| ショートカット | キャビネットやフォルダ、文書へのリンクを表現する単位。<br>ショートカットは、キャビネットやフォルダの配下に作成できる。<br>なお、ショートカットをメールに添付したとき、ショートカット自体はキャビネットやフォルダによるアクセス制御の影響を受けない。<br>(ショートカットのリンク先は、アクセス制御が行われる) |
| クリップ | 文書をまとめて管理するオブジェクト。複数の文書を1つのオブジェクトとして扱えるようになる。クリップされた各文書へのアクセス権は、各文書に付与されている権限に依存し、クリップには無関係。 |
| パスワードポリシー | TOEの認証に関するセキュリティポリシー。<br>パスワード最小長、パスワード制約条件、認証失敗最大回数、アカウントロック設定についての設定を保持する。 |

# 7 参照


[1] StarOffice X V1.5 セキュリティターゲット バージョン 1.10 2009年5月27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 2 September 2007 CCMB-2007-09-002

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

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル バージョン3.1 改訂第1版 2006年9月 CCMB-2006-09-001 (平成19年3月翻訳第1.2版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-002 (平成20年3月翻訳第2.0版)

[10] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-003 (平成20年3月翻訳第2.0版)

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

[12] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン3.1 改訂第2版 2007年9月 CCMB-2007-09-04 (平成20年3月翻訳第2.0版)

[13] StarOffice X V1.5 評価報告書 08000753-R003-02 みずほ情報総研株式会社 情報セキュリティ評価室 2009年6月15日