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

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		
1.00	初版	-		2008/8/20	日本電気株式会社
1.01	レビュー結果見直し事項の反映	1～6 章	表記誤りの修正、記述内容の見直し	2008/9/25	日本電気株式会社
1.02	レビュー結果見直し事項の反映	1～6 章	記述内容の見直し	2008/10/3	日本電気株式会社
1.03	評価指摘事項の反映	1～6 章	記述内容の見直し	2008/10/31	日本電気株式会社
1.04	評価指摘事項の反映	1～6 章	記述内容の見直し	2008/12/10	日本電気株式会社
1.05	評価指摘事項の反映	1～6 章	記述内容の見直し	2008/12/18	日本電気株式会社
1.06	評価指摘事項の反映	1～6 章	記述内容の見直し	2008/12/26	日本電気株式会社
1.07	評価指摘事項の反映	1～7 章	記述内容の見直し	2009/1/16	日本電気株式会社
1.08	評価指摘事項の反映	1～7 章	記述内容の見直し	2009/1/27	日本電気株式会社
1.09	評価指摘事項の反映	1～7 章	表記誤りの修正、記述内容の見直し	2009/3/18	日本電気株式会社
1.10	評価指摘事項の反映	1 章	表記誤りの修正、記述内容の見直し	2009/5/27	日本電気株式会社

目次

参考資料

本 ST における参考資料は、以下のとおりである。

・Common Criteria for Information Technology Security Evaluation Part1:
Introduction and general model September 2006 Version 3.1 Revision 1 CCMB-2006-09-001

・Common Criteria for Information Technology Security Evaluation Part2:
Security functional components September 2007 Version 3.1 Revision 2 CCMB-2007-09-002

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

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

・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 2007 年 9 月バージョン 3.1 改訂第 2 版 CCMB-2007-09-002
平成 20 年 3 月翻訳第 2.0 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 2007 年 9 月バージョン 3.1 改訂第 2 版 CCMB-2007-09-003
平成 20 年 3 月翻訳第 2.0 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共通方法
評価方法 2007 年 9 月 バージョン 3.1 改訂第 2 版 CCMB-2007-09-004
平成 20 年 3 月翻訳第 2.0 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

用語

＜CC 関連略語＞
CC(Common Criteria):コモンクライテリア
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
SFP(Security Function Policy):セキュリティ機能ポリシー
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

本STで使用している用語・略語の意味を、表 1 に示す。

表 1 用語集

用語・略語	定義内容
DBMS	Database Management System データベース管理ソフトウェア
OS	Operating System 入出力機能やメモリ管理など、共通して利用される基本機能を提供するソフトウェア
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
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。 システム管理者により、オフィスが作成される。 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。 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。 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。 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。 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。 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。 (ショートカットのリンク先は、アクセス制御が行われる)
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。 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。
アクセス権変更権	キャビネット、フォルダ、文書、ショートカットに設定されたアクセス権を変更する権限

1. ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、TOE 記述について記述する。

1.1. ST 参照

ST の識別情報は、以下のとおりである。

ST タイトル: StarOffice X V1.5 セキュリティターゲット
ST バージョン: 1.10
ST 発行日: 2009 年 5 月 27 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、以下のとおりである。

TOE 名称: StarOffice X V1.5
TOE バージョン: 1.5.02
TOE 開発者: 日本電気株式会社

TOE は、StarOffice X V1.5 の基本製品となる StarOffice X Standard V1.5 と、StarOffice X Enterprise V1.5 の両方である。

1.3. TOE 概要

本節では、TOE の概要について、TOE 種別と TOE の使用方法と主要なセキュリティ機能、TOE 以外のハードウェア/ソフトウェア/ファームウェアについて記述する。

1.3.1. TOE 種別

TOE は、会社組織における業務に関する情報の安全な共有と管理を支援するためのグループウェア・アプリケーションソフトウェアであり、文書データへのアクセスを制御するキャビネットサービスを提供する。

1.3.2. TOE の使用方法と主要なセキュリティ機能

TOE 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、TOE を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。

TOE 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 TOE に登録する。TOE の利用者は、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。

TOE 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。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やショートカットは、TOE が提供するメールや掲示板と連携して利用することができる。

TOE 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、運用機能を提供している。

TOE のセキュリティ機能は、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、ショートカットに対して、不正アクセスの防止を行う。
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。

[TOE が提供するセキュリティ機能]

識別認証機能
TOE 利用者に対する識別認証を行う機能
アクセス制御機能
TOE 利用者の所属組織、利用者種別、職位などに基づき、文書データへのアクセスを制御する機能

なお、TOE のセキュリティ機能として監査機能は提供していない。TOE は、会社組織内の利用者が使用するため、セキュリティインシデントの追跡までを必要としていない。

1.3.3. TOE 以外のハードウェア/ファームウェア/ソフトウェア

TOE が動作するための環境を、以下に記述する。

1.3.3.1. 必要なハードウェア

TOEの動作環境として必要なハードウェア構成を、以下の 表 2 に示す。

表 2 ハードウェア構成

端末・装置名		
ベンダ名	種別	説明
Web サーバ		
NEC, その他	本体	Express5800 シリーズ 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, 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

1.3.3.2. 必要なソフトウェア

TOEの動作環境として必要なソフトウェア構成を、以下の 表 3 に示す。なお、製品名欄に複数の製品の記載がある場合は、いずれか一つの製品を選択する。

表 3 ソフトウェア構成

端末名		
ベンダ名	製品名	種別
Web サーバ		

端末名		
ベンダ名	製品名	種別
Microsoft	Windows Server 2003 Standard Edition SP2, Windows Server 2003 Standard Edition R2 SP2, Windows Server 2003 Enterprise Edition SP2, Windows Server 2003 Enterprise Edition R2 SP2, Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition	OS
	Internet Information Services 6.0, (Windows Server 2003 の場合) Internet Information Services 7.0 (Windows Server 2008 の場合)	Web サーバ ソフトウェア
	.NET Framework 2.0 SP1, .NET Framework 2.0 SP2	アプリケーション実行 環境
	.NET Framework 2.0 日本語 Language Pack SP1, .NET Framework 2.0 日本語 Language Pack SP2	
	ASP.NET 2.0 AJAX Extension 1.0	AJAX 実行環境
Sun Microsystems	J2SDK 5.0 update 16	Java 実行環境
	JDBC ドライバ	
NEC	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		
Microsoft	Windows Server 2003 Standard Edition SP2, Windows Server 2003 Standard Edition R2 SP2, Windows Server 2003 Enterprise Edition SP2, Windows Server 2003 Enterprise Edition R2 SP2, Windows Server 2008 Standard Edition, Windows Server 2008 Enterprise Edition	OS
Microsoft	Internet Information Services 6.0, (Windows Server 2003 の場合) Internet Information Services 7.0 (Windows Server 2008 の場合)	Web サーバ ソフトウェア
	.NET Framework 2.0 SP1, .NET Framework 2.0 SP2	アプリケーション実行 環境
	.NET Framework 2.0 日本語 Language Pack SP1, .NET Framework 2.0 日本語 Language Pack SP2	
Sun Microsystems	J2SDK 5.0 update 16	Java 実行環境
NEC	WebOTX Web Edition Ver. 7.11	アプリケーションサーバ ソフトウェア
Microsoft, Oracle	SQL Server 2005 Express Edition, SQL Server 2005, Oracle10g R2	DBMS
利用者クライアント		
Microsoft	Windows 2000 Professional SP4, Windows XP Professional Edition SP2, Windows XP Professional Edition SP3, Windows Vista Business Edition SP1	OS
Microsoft	Internet Explorer 6.0 SP2, Internet Explorer 7.0	Web ブラウザ

1.3.3.3. 評価構成

TOE の動作環境のうち、本評価において検証した構成を以下に示す。

[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

1.4. TOE 記述

本節では、製品特徴、TOE 関連の利用者定義、TOE の物理的範囲、TOE の論理的範囲について記述する。

1.4.1. 製品特徴

TOE は、会社内の組織、または組織をまたがって、業務に関する情報の安全な共有と管理を支援する、グループウェア・アプリケーションソフトウェアである。
TOE は、利用者が登録する任意の文書データについての共有、及び管理を行うキャビネットサービス機能により、キャビネット、フォルダ、文書データ、ショートカットに対する基本操作(登録、更新、コピー、移動、削除、アクセス権設定)を提供している。
TOE は、各利用者の所属組織、利用者種別、職位などに基づいて、キャビネット、フォルダ、文書データ、ショートカットへのアクセスが可能な利用者を制限することで、安全な共有を実現することができる。
なお、日々の業務やコミュニケーションを支援する機能として、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。また、システム管理者によるメンテナンス作業のため、運用機能を提供している。

1.4.2. TOE 関連の利用者定義

TOE のキャビネットサービス機能に関連する利用者は、以下のとおりである。
利用者は、運用管理責任者、システム管理者、オフィス責任者、一般利用者のいずれかに分類され、付与された権限の範囲で業務を行う。
TOE関連の利用者定義を、表 4 に示す。

表 4 TOE 関連の利用者定義

利用者定義	内容
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。

利用者定義	内容
	・システム管理者の任命を行う。 ・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。 ・運用管理責任者により任命される。 ・TOE へのオフィスの登録とその管理を行う。 ・オフィス責任者の任命と TOE への登録、管理を行う。 ・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。 ・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。 ・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。 ・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。 ・「所属組織」、「職位」が決定している。 ・付与された権限に基づいて、TOE の操作権限を持つ。

1.4.3. TOE の物理的範囲

TOE の動作環境、ハードウェア構成、ソフトウェア構成を、以下に記述する。

1.4.3.1. TOE の動作環境

TOEが必要とする動作環境を、以下の 図 1 に示す。

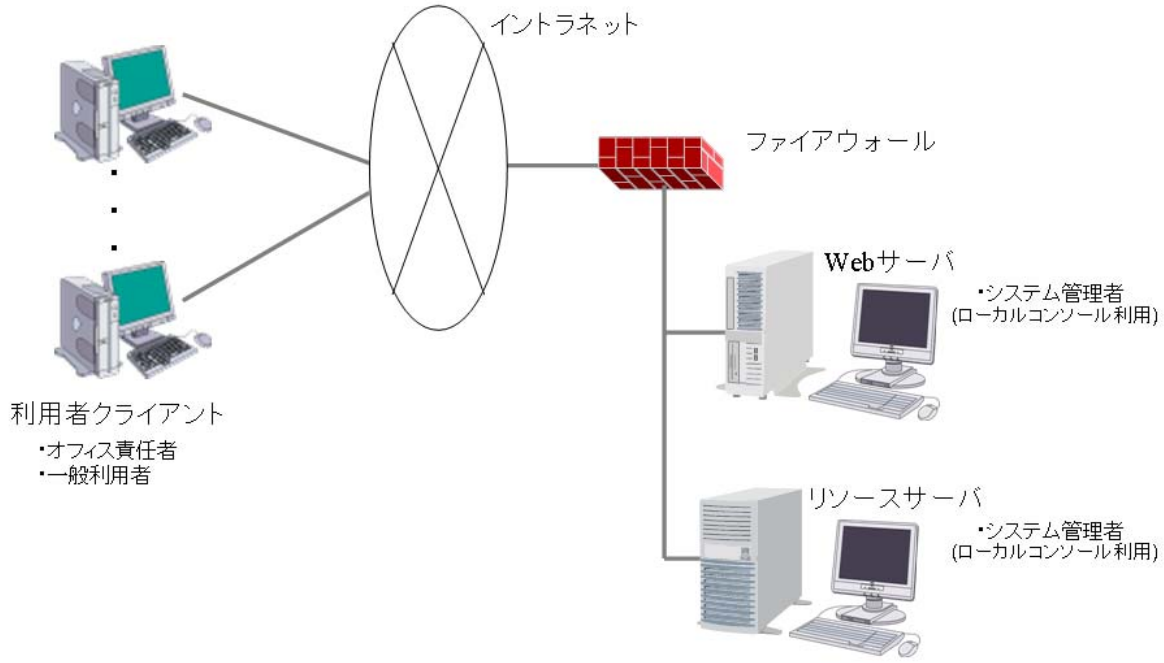

図 1 TOE の動作環境

(1) 物理的配置、及びネットワーク
TOEを利用する複数台の利用者クライアント、ファイアウォール経由でWebサーバ、及びリソースサーバが、イントラネットに接続される。

(2) Web サーバ

Web サーバは、利用者クライアントからの処理要求を受け付け、必要に応じてリソースサーバにアクセスし、処理結果を返却する。なお、システム管理者が行う運用操作は、ローカルコンソールを利用する。

(3) リソースサーバ

リソースサーバは、Web サーバからの処理要求を受け付け、TOE に登録された文書データ情報、メール情報、スケジュール情報、施設情報、及び管理情報とのアクセスを行う。なお、システム管理者が行う運用操作は、ローカルコンソールを利用する。

(4) 利用者クライアント

利用者クライアントは、オフィス責任者、一般利用者が使用し、Web サーバへのアクセスを行う。

1.4.3.2. TOE の物理的範囲(コンポーネント)

以下の 図 2 に示した破線内が、TOEが必要とするコンポーネント構成の物理的範囲である。

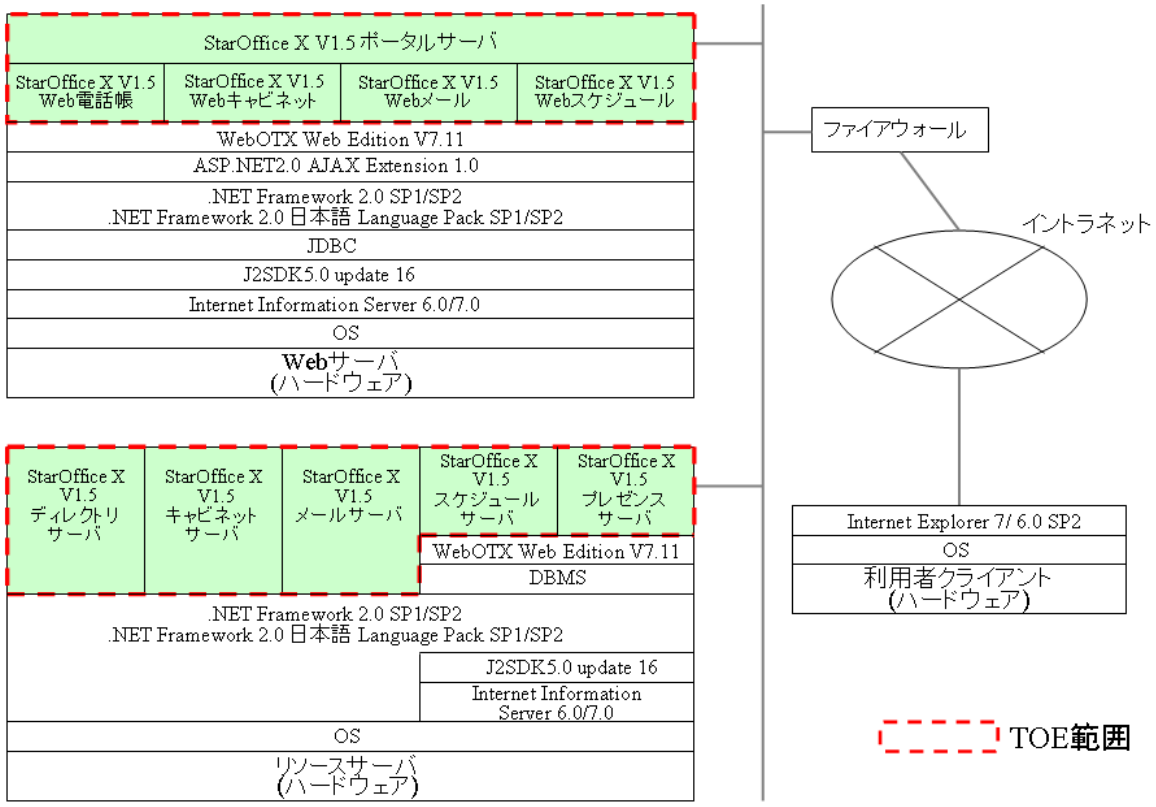

図 2 TOE の物理的範囲(コンポーネント)

[TOE のハードウェア構成]

TOE は、ソフトウェアのため、ハードウェアを含まない。

[TOE のソフトウェア構成]

TOEのソフトウェア構成を、以下の 表 5 に示す。

表 5 TOE のソフトウェア構成

端末名	
ベンダ名	製品名
Web サーバ	
NEC	StarOffice X V1.5 ポータルサーバ

端末名	
ベンダ名	製品名
NEC	StarOffice X V1.5 Web 電話帳
NEC	StarOffice X V1.5 Web キャビネット
NEC	StarOffice X V1.5 Web メール
NEC	StarOffice X V1.5 Web スケジュール
リソースサーバ	
NEC	StarOffice X V1.5 ディレクトリサーバ
NEC	StarOffice X V1.5 キャビネットサーバ
NEC	StarOffice X V1.5 メールサーバ
NEC	StarOffice X V1.5 スケジュールサーバ
NEC	StarOffice X V1.5 プレゼンスサーバ
利用者クライアント	
-	なし

表 5 において、StarOffice X V1.5 ディレクトリサーバには、NECのEnterprise Directory Serverが含まれる。また、StarOffice X V1.5 キャビネットサーバには、NECのPercioが含まれる。

各コンポーネントが提供しているサービス機能を、以下に記述する。

・StarOffice X V1.5 ディレクトリサーバ
運用機能を提供する。

・StarOffice X V1.5 Web キャビネット、StarOffice X V1.5 キャビネットサーバ
キャビネットサービス機能、掲示板サービス機能、運用機能を提供する。

・StarOffice X V1.5 Web メール、StarOffice X V1.5 メールサーバ
メールサービス機能を提供する。

・StarOffice X V1.5 Web スケジュール、StarOffice X V1.5 スケジュールサーバ
スケジュールサービス機能、施設予約機能を提供する。

・StarOffice X V1.5 Web 電話帳、StarOffice X V1.5 プレゼンスサーバ
電話帳機能を提供する。

なお、StarOffice X V1.5 ポータルサーバは、Web 上のインタフェースを提供する。

1.4.3.3. TOE の物理的範囲(ガイダンス)

TOE のガイダンスは、以下のとおりである。

・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

1.4.4. TOE の論理的範囲

TOEの論理的構成を、以下の 図 3 に示す。

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 サーバを仲介し、リソースサーバ上の以下の TOE サービス機能を使用することができる。

・キャビネットサービス機能
・掲示板サービス機能
・メールサービス機能
・スケジュールサービス機能
・施設予約機能
・電話帳機能

なお、TOE セキュリティ機能の識別認証機能、及びアクセス制御機能が、キャビネットサービス機能から使用される。

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、各サーバから以下の TOE サービス機能を使用することができる。

・運用機能

なお、TOE セキュリティ機能の識別機能が、運用機能から使用される。

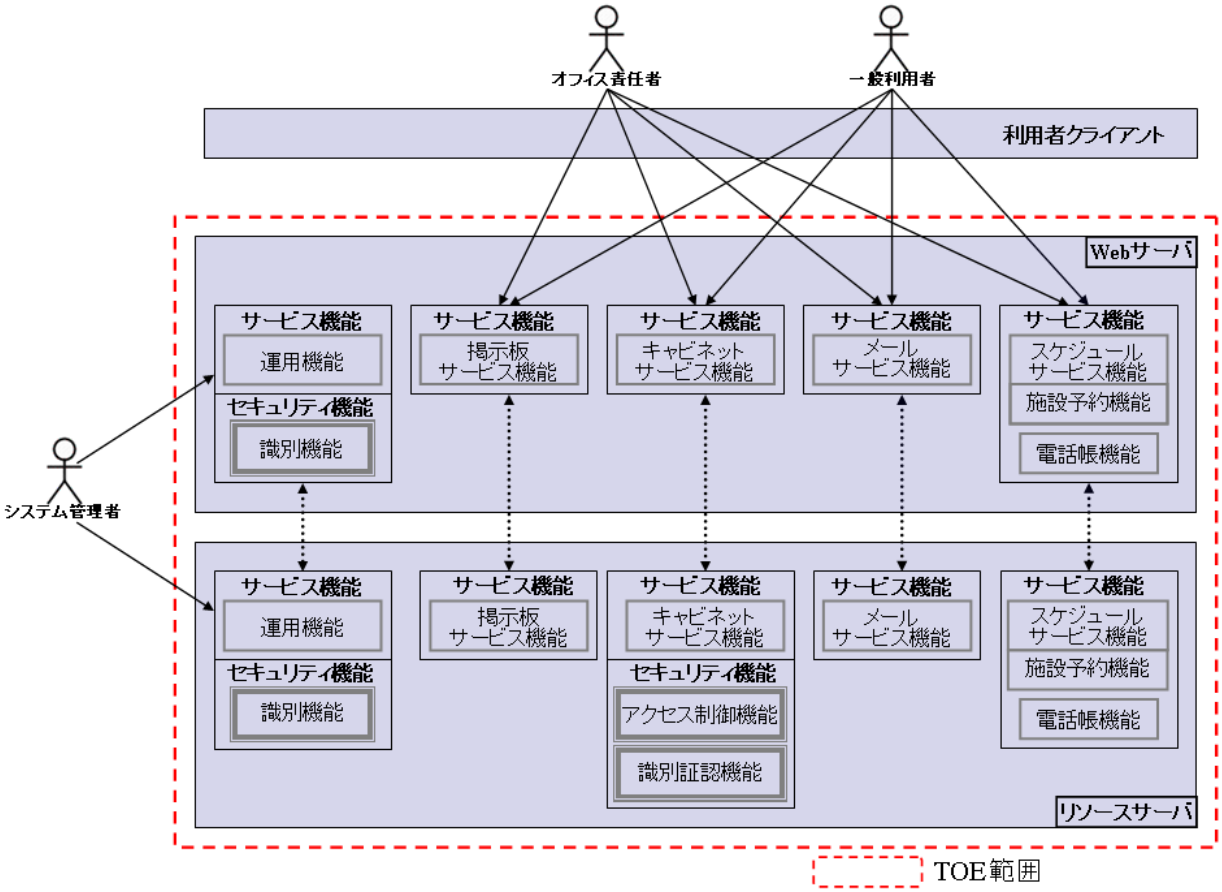

図 3 TOE の論理構成

TOE の論理的構成を、TOE が提供するサービス機能とセキュリティ機能について、以下に説明する。

1.4.4.1. TOE が提供するサービス機能

・TOE サービス機能

TOE が提供するサービス機能について、以下に記述する。

【キャビネットサービス機能】

キャビネットサービス機能について、以下の 図 4 に示す。

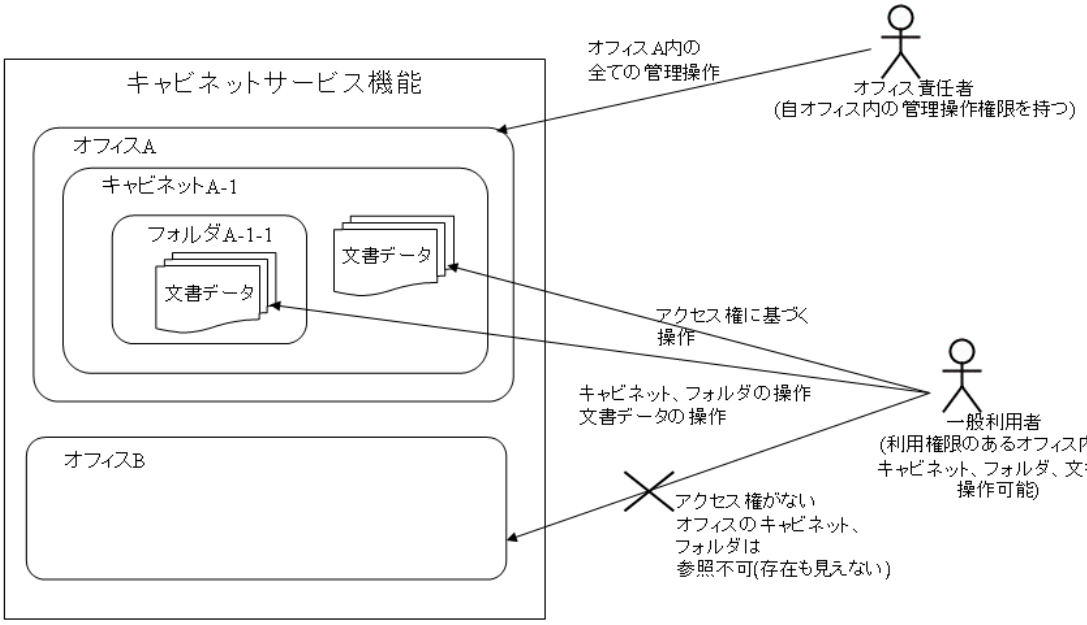

図 4 キャビネットサービス機能

キャビネットサービス機能は、TOE の利用者が所属するオフィスに対して、キャビネットの登録、更新、削除、コピー、移動、キャビネット内におけるフォルダの登録、更新、削除、コピー、移動、キャビネット内やフォルダ内に格納する文書データの登録、更新、削除、コピー、移動、履歴管理、文書番号採版、文書承認についての管理機能を提供する。
キャビネットやフォルダは、複数、登録することができる。キャビネット、フォルダ、文書データについて、それぞれ、利用者の所属組織、職位などの単位で、利用権限の設定が行える。

【メールサービス機能】
メールサービス機能について、以下の 図 5 に示す。

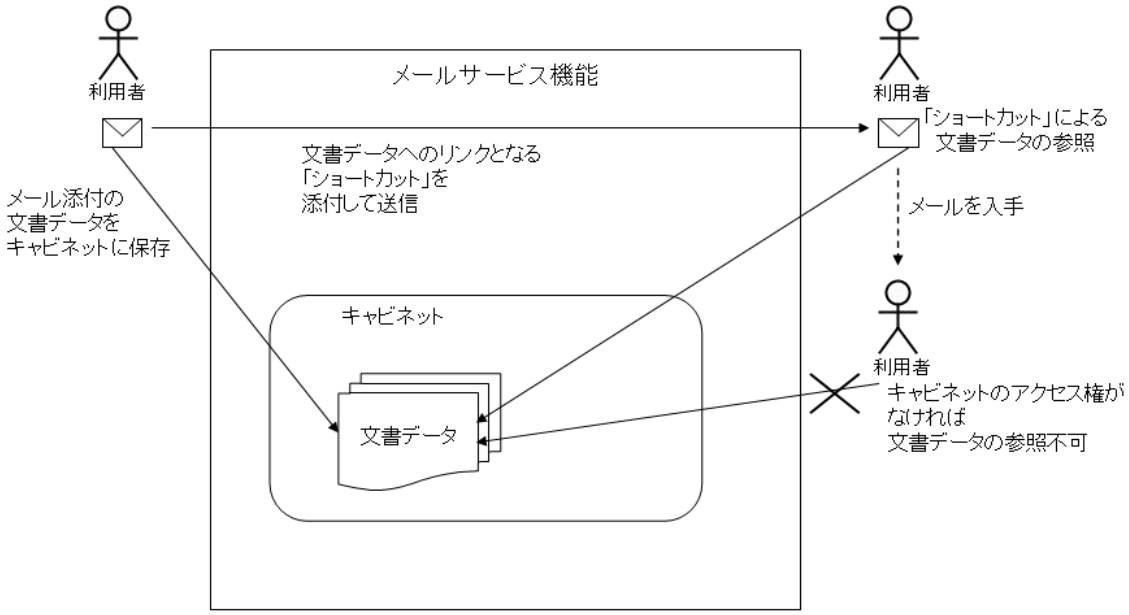

図 5 メールサービス機能

メールサービス機能は、TOEの利用者間のメール送受信、開封通知、発信取り消し、回覧メールの機能を提供する。
送信メールの添付文書に、キャビネットサービス機能が提供するキャビネットの配下に格納されているショートカットを指定した場合、そのショートカットを開くときに、キャビネットサービス機能が提供する、利用権限の設定が有効となる。図 5 のように、文書データへのリンクとなるショートカットを指定することで、キャビネット内の文書データに対する利用権限に基づいて、参照が行える。

【掲示板サービス機能】
掲示板サービス機能について、以下の 図 6 に示す。

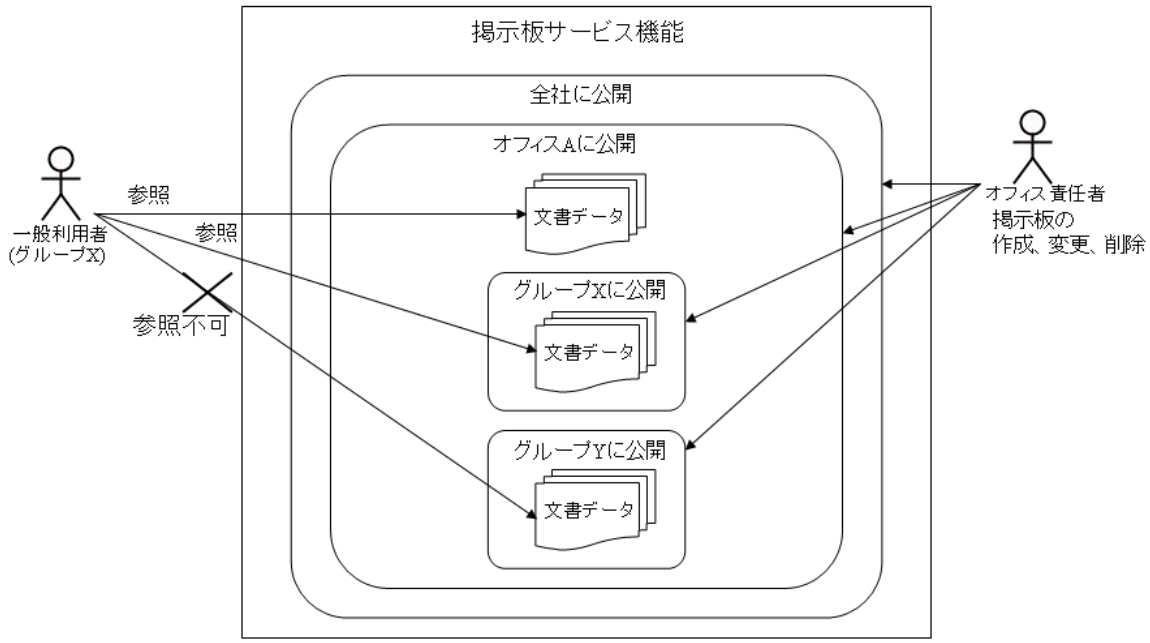

図 6 掲示板サービス機能

掲示板サービス機能は、掲示板として文書データを掲示し、公開範囲を限定して閲覧、検索を行う機能を提供する。公開範囲を限定した掲示板を複数、作成することができる。各掲示板の単位で、利用できる権限を設定することができる。
掲示板の文書データに、キャビネットサービス機能が提供するキャビネットの配下に格納されているショートカットを指定した場合、ショートカットを開くときに、キャビネットサービス機能が提供する、利用権限の設定が有効となる。

【スケジュールサービス機能】
スケジュールサービス機能は、以下の機能を提供する。
・利用者のスケジュールを全社、所属部門、グループ単位で共有するための表示、管理機能

【施設予約機能】
施設予約機能は、以下の機能を提供する。
・社内業務施設、設備の予約や予約状況を共有するための表示、管理機能

【電話帳機能】

電話帳機能は、以下の機能を提供する。
・利用者の電話番号、所属部門、メールアドレスの検索、表示、管理機能

【運用機能】
運用機能は、システム管理者に対し、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

1.4.4.2. TOE が提供するセキュリティ機能

TOE が提供するセキュリティ機能について、以下に記述する。
・TOE セキュリティ機能
【識別認証機能】
オフィス責任者、一般利用者について、以下の機能を提供する。
・ユーザ ID による識別、パスワードによる認証
・TOE 利用時に、ある一定時間の操作がなかった場合の対話セション終了
システム管理者について、以下の機能を提供する。
・OS に登録されたアカウントによる識別

【アクセス制御機能】
TOE は、キャビネットサービス機能における、オフィス責任者、及び一般利用者に付与された権限に基づいて、キャビネットサービス機能が提供する、文書データを格納するキャビネットやフォルダに対するアクセスの許可、文書データやショートカットに対するアクセスの許可を行う機能を提供する。

2. 適合主張

本章では、CC 適合主張、PP 主張、パッケージ主張、及び適合根拠について記述する。

2.1. CC 適合主張

本 ST は、以下のとおり、CC 適合を主張する。
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 翻訳第 1.2 版
・パート 2: セキュリティ機能コンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版 翻訳第 2.0 版
・パート 3: セキュリティ保証コンポーネント 2007 年 9 月 バージョン 3.1 改訂第 2 版 翻訳第 2.0 版
CC パート 2 適合性: CC パート 2 適合
CC パート 3 適合性: CC パート 3 適合

2.2. PP 主張

この ST が適合している PP はない。

2.3. パッケージ主張

本 ST は、EAL2 適合である。

2.4. 適合根拠

本 ST は、PP 適合を主張しないため、PP 適合根拠はない。

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する。

3.1. 脅威

本節では、TOE 保護資産、TOE に対する脅威を以下に記述する。

3.1.1. TOE 保護資産

TOEの保護資産である利用者データを 表 6 に記述する。

表 6 利用者データ一覧

データ名	内容
文書データ	キャビネット内、またはフォルダ内に登録された文書データ

3.1.2. 脅威

TOE に対する脅威を以下に記述する。
なお、TOE において想定する攻撃者のレベルは、専門知識を持たない者としている。

T.SPOOFING (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 (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。

3.2. 組織のセキュリティ方針

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を以下に記述する。

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.SAFE_PLACE (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 (ネットワーク環境)
TOE が稼動する Web サーバ、及びリソースサーバは、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 (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 (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。

A.SERVER_USER (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。

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.ADMINISTRATOR (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 (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。

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.PASSWORD (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。

A.UNLOCK_ACCOUNT (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 (セションタイムアウト時間)
利用者クライアントから TOE へのアクセスが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 (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。

A.ACCESS_PRIVILEGE (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。

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、及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.I&A (識別認証)
TOE は、オフィス責任者、及び一般利用者が TOE を利用するときに必ず識別認証を行うことを保証し、システム管理者により指定された認証失敗の最大回数以内に識別認証に成功したオフィス責任者、及び一般利用者のみに、TOE の利用を許可しなければならない。
また、システム管理者が TOE を利用するときに必ず識別を行うことを保証する。

O.CHECK_PASSWORD_POLICY (パスワードポリシーチェック)
TOE は、識別認証を行うときに、システム管理者により設定されたパスワードポリシーの維持をしなければならない。

O.ACCESS_CONTROL (アクセス制御)
TOE は、オフィス責任者、及び一般利用者を代行するプロセスに対し、組織のアクセス制御方針に基づいて、所属組織、利用者種別、職位、利用者識別と、その操作対象に設定、付与された権限にしたがった保護資産へのアクセスを保証しなければならない。

O.AUTO_LOGOUT (自動ログアウト)
TOE は、TOE にログインしたオフィス責任者、及び一般利用者から一定時間、TOE へのアクセスがないとき、自動的にログアウトを行わなければならない。

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。

OE.TRUSTED_ROLE (信頼される役割)
運用管理責任者は、システム管理者の役割に適した者を厳重に人選しなければならない。さらに、システム管理者は、オフィス責任者の役割に適した者を厳重に人選しなければならない。
運用管理責任者は、システム管理者、オフィス責任者に対して、管理者役割の重要性を理解させ、悪意を持った行為を行わないよう、監督しなければならない。

OE.PASSWORD_MANAGEMENT (パスワードの管理)
TOE 利用者は、TOE にアクセスするための認証情報(パスワード)を記憶し、他人に漏らしてはならない。また、パスワードの定期的な変更を行わなければならない。

OE.PASSWORD_POLICY_SET (パスワードポリシーの設定)
システム管理者は、TOE の認証に関するポリシーとして、TOE の運用開始前に、リソースサーバ上のディレクトリサーバに対して、以下のポリシー設定を行わなければならない。
・パスワード最小長に、8 文字以上の値を指定する。

・パスワード制約に、以下の条件を指定する。
  ・英字のみや、数字のみのパスワードを禁止
  ・直前に使用したパスワードの再使用を禁止
・認証失敗最大回数に、5～99999 回の間の任意の値を指定する。
・オフィス責任者、一般利用者の認証失敗時のアカウントロック設定を有効にする。
 (システム管理者がロック解除を行うまで、該当アカウントが使用不可となるように設定。)

OE.SESSION_TIMEOUT (セションタイムアウト時間)
システム管理者は、TOE の運用開始前に、利用者クライアントから TOE へのアクセスがないときのタイムアウト時間を、20 分から 60 分の間で安全な値に設定しなければならない。

OE.SAFE_PLACE (安全な場所)
TOE のサーバに関連するハードウェアは、入退室を管理している物理的セキュリティを確保した部屋に設置しなければならない。この部屋への入室は、許可を得た人のみに限定しなければならない。

OE.NETWORK (ネットワーク環境)
TOE のサーバは、適切に設定されたファイアウォールにより、TOE に必要な通信のみに制限し、アクセス保護をしなければならない。

OE.SECURE_CHANNEL (セキュアな通信)
TOE の Web サーバは、HTTPS 通信を使用する設定を維持しなければならない。

OE.SYSTEM_ADMIN (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の実行に制限しなければならない。

OE.SERVER_USER (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は、システム管理者のみに、利用を限定しなければならない。

OE.CLIENT (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のインストールを禁止しなければならない。

OE.ACCESS_PRIVILEGE (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、付与しなければならない。

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 7 に示す。表中の「×」は、対応関係を示している。

表 7 セキュリティ対策方針とセキュリティ課題定義対応表

脅威 組織のセキュリティ方針 前提条件 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	T.SPOOFING	T.ILLEGAL_ACCESS	A.SAFE_PLACE	A.NETWORK	A.SECURE_CHANNEL	A.SYSTEM_ADMIN	A.SERVER_USER	A.ADMINISTRATOR	A.PASSWORD	A.PASSWORD_MANAGEMENT	A.UNLOCK_ACCOUNT	A.SESSION_TIMEOUT	A.CLIENT	A.ACCESS_PRIVILEGE
O.I&A	×													
O.CHECK_PASSWORD_POLICY	×													
O.ACCESS_CONTROL		×												
O.AUTO_LOGOUT	×													
OE.TRUSTED_ROLE								×						
OE.PASSWORD_MANAGEMENT	×									×				
OE.PASSWORD_POLICY_SET	×								×		×			
OE.SESSION_TIMEOUT	×											×		
OE.SAFE_PLACE	×		×											
OE.NETWORK				×										
OE.SECURE_CHANNEL					×									
OE.SYSTEM_ADMIN	×					×								
OE.SERVER_USER	×						×							
OE.CLIENT													×	
OE.ACCESS_PRIVILEGE		×												×

以上の 表 7 より、各セキュリティ対策方針は、一つ以上の脅威、組織のセキュリティ方針、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以下に記述する。

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.SPOOFING (なりすまし)

この脅威は、高度な専門知識を持たない悪意のある第三者や他の利用者によって実行される。このような者が取り得る、なりすまし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. 正当な利用権限を持たない者が、認証情報を取得

この攻撃は、正当な利用者からの認証情報の取得、または類推により認証情報を取得することが考えられる。よって、OE.PASSWORD_MANAGEMENT により認証情報を他者に漏らさないこと、O.CHECK_PASSWORD_POLICY、及び OE.PASSWORD_POLICY_SET の最小パスワード長の

設定により類推されにくい認証情報を設定すること、さらに O.I&A、及び OE.PASSWORD_POLICY_SET により誤った識別認証の連続試行回数を制限し、アカウントロック設定によりアカウントをロックすることで、脅威を軽減できる。

b. 正当な利用権限を持たない者が、正当な利用者がログオンしたクライアントを使用
この攻撃は、正当な利用者が TOE にログオンしたまま離席し、長時間放置したとき、正当な利用権限を持たない者が、その正当な利用者権限を用いて、TOE を利用することが考えられる。
よって、ログオンしたまま長時間放置されたクライアントでは、OE.SESSION_TIMEOUT により設定された値に基づき、O.AUTO_LOGOUT により自動的にログアウトすることで、脅威を軽減できる。

c. TOE 利用者の役割を逸脱して TOE を使用
この攻撃は、TOE 利用者に付与された役割を逸脱して、TOE の利用を試みるものである。よって、O.I&A により、オフィス責任者、及び一般利用者について、その役割を識別認証すること、及びシステム管理者について、その役割を識別し、OE.SAFE_PLACE、OE.SERVER_USER、OE.SYSTEM_ADMIN により、許可された人のみが入室できる部屋のなかで Web サーバ、及びリソースサーバをシステム管理者のみがコンソールから利用することで、脅威を軽減できる。

以上より、この攻撃方法に対抗するセキュリティ対策方針は、O.I&A、O.CHECK_PASSWORD_POLICY、O.AUTO_LOGOUT、OE.PASSWORD_MANAGEMENT、OE.PASSWORD_POLICY_SET、OE.SESSION_TIMEOUT、OE.SAFE_PLACE、OE.SERVER_USER、OE.SYSTEM_ADMIN である。

T.ILLEGAL_ACCESS (不正なアクセス)

この脅威は、TOE の正当な利用者によって実行される。正当な利用者が取り得る、不正なアクセス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. 許可されていない操作を実行
この攻撃に対しては、O.ACCESS_CONTROL により、TOE の各操作における権限を設定し、利用者の操作を制限すること、及び OE.ACCESS_PRIVILEGE により、アクセス権変更の権限をオフィス責任者のみに制限することで、脅威を除去できる。

以上より、この攻撃に対抗するセキュリティ対策方針は、O.ACCESS_CONTROL、OE.ACCESS_PRIVILEGE 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ため、対応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

前提条件に対して、セキュリティ対策方針が対応していることを、以下で説明する。

A.SAFE_PLACE (安全な場所)

この前提条件は、TOE に関連するハードウェアが設置される場所に関するものである。有効な対策方針について以下に述べる。

a. TOE に関連するハードウェアを設置する場所を制限
入退出管理を実施した部屋に TOE、及び TOE に関連するハードウェアを設置し、許可のない人の入室を禁止する。
この条件に対応するための運用環境セキュリティ対策方針は、OE.SAFE_PLACE である。

以上より、OE.SAFE_PLACE の達成により、A.SAFE_PLACE が実行される。

A.NETWORK (ネットワーク環境)

この前提条件は、ネットワーク環境の構築に関するものである。有効な対策方針について以下に述べる。

a. 必要な通信のみに制限

イントラネットから、TOE が稼動する Web サーバ、リソースサーバへの接続は、適切に設定したファイアウォールを用いて、必要な通信のみにアクセスを制限する。

この条件に対応するための運用環境セキュリティ対策方針は、OE.NETWORK である。

以上より、OE.NETWORK の達成により、A.NETWORK が実行される。

A.SECURE_CHANNEL (セキュアな通信)

この前提条件は、通信路における通信の秘匿に関するものである。有効な対策方針について以下に述べる。

a. 暗号化通信

TOE の Web サーバは、HTTPS による通信を使用する設定を維持する。

この条件に対応するための運用環境セキュリティ対策方針は、OE.SECURE_CHANNERL である。

以上より、OE. SECURE_CHANNEL の達成により、A.SECURE_CHANNEL が実行される。

A.SYSTEM_ADMIN (システム管理者の運用操作)

この前提条件は、システム管理者の運用操作に関するものである。有効な対策方針について以下に述べる。

a. システム管理者による運用操作の制限

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に制限する。

この条件に対応するための運用環境セキュリティ対策方針は、OE.SYSTEM_ADMIN である。

以上より、OE.SYSTEM_ADMIN の達成により、A.SYSTEM_ADMIN が実行される。

A.SERVER_USER (サーバユーザ)

この前提条件は、TOE が稼動するサーバに関するものである。有効な対策方針について以下に述べる。

a. サーバの利用制限

TOE が稼動する Web サーバ、及びリソースサーバは、システム管理者のみが利用する。

この条件に対応するための運用環境セキュリティ対策方針は、OE.SERVER_USER である。

以上より、OE.SERVER_USER の達成により、A.SERVER USER が実行される。

A.ADMINISTRATOR (信頼できる管理者)

この前提条件は、信頼できる管理者に関するものである。有効な対策方針について以下に述べる。

a. 厳重な人選と適切な管理

運用管理責任者は、システム管理者の役割に適した者を厳重に人選する。さらに、システム管理者は、オフィス責任者の役割に適した者を厳重に人選する。

また、運用管理責任者は、システム管理者、オフィス責任者に対して、管理者役割の重要性を理解させ、悪意を持った行為を行わないよう、監督する。

この条件に対応するための運用環境セキュリティ対策方針は、OE.TRUSTED_ROLE である。

以上より、OE.TRUSTED_ROLE の達成により、A.ADMINISTRATOR が実行される。

A.PASSWORD_MANAGEMENT (パスワード管理)

この前提条件は、パスワードの管理に関するものである。有効な対策方針について以下に述べる。

a. パスワードの定期的な変更

TOE のパスワードは、他者に漏れたり、推測されたりすることがないように、定期的な変更を行う。

この方針に対応するための運用環境セキュリティ対策方針は、OE.PASSWORD_MANAGEMENT である。

以上より、OE.PASSWORD_MANAGEMENT の達成により、A.PASSWORD_MANAGEMENT が実行される。

A.PASSWORD (パスワード)

この前提条件は、パスワード長に関するものである。有効な対策方針について以下に述べる。

a. 最小パスワード長の設定

TOE の最小パスワード文字数は、8 文字以上の長さに設定する。

この方針に対応するための運用環境セキュリティ対策方針は、OE.PASSWORD_POLICY_SET である。

以上より、OE.PASSWORD_POLICY_SET の達成により、A.PASSWORD が実行される。

A.UNLOCK_ACCOUNT (アカウントロック解除)

この前提条件は、オフィス責任者、一般利用者のアカウントロックに関するものである。有効な対策方針について以下に述べる。

a. アカウントロック解除

オフィス責任者、一般利用者の認証失敗時のアカウントロックは、システム管理者のみが解除できる。

この方針に対応するための運用環境セキュリティ対策方針は、OE.PASSWORD_POLICY_SET である。

以上より、OE.PASSWORD_POLICY_SET の達成により、A.UNLOCK_ACCOUNT が実行される。

A.SESSION_TIMEOUT (セションタイムアウト時間)

この前提条件は、セションタイムアウト時間に関するものである。有効な対策方針について以下に述べる。

a. セションタイムアウト時間の設定

利用者クライアントから TOE へのアクセスがないときのタイムアウト時間は、20 分から 60 分の間の値を設定する。

この方針に対応するための運用環境セキュリティ対策方針は、OE.SESSION_TIMEOUT である。

以上より、OE.SESSION_TIMEOUT の達成により、A.SESSION_TIMEOUT が実行される。

A.CLIENT (利用者クライアント)

この前提条件は、利用者クライアントの環境に関するものである。有効な対策方針について以下に述べる。

a. クライアントソフトの制限

StarOffice X V1.5 ビジネスナビゲータの利用をさせない。

この方針に対応するための運用環境セキュリティ対策方針は、OE.CLIENT である。

以上より、OE.CLIENT の達成により、A.CLIENT が実行される。

A.ACCESS_PRIVILEGE (アクセス権変更権の付与)

この前提条件は、アクセス権変更権の利用に関するものである。有効な対策方針について以下に述べる。

a. アクセス権変更権の制限

TOE のアクセス権変更権の付与は、オフィス責任者のみに制限する。

この方針に対応するための運用環境セキュリティ対策方針は、OE. ACCESS_PRIVILEGE である。

以上より、OE. ACCESS_PRIVILEGE の達成により、A.ACCESS_PRIVILEGE が実行される。

5. 拡張コンポーネント定義

この ST では、拡張コンポーネントを使用しない。

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する。

6.1. TOE のサブジェクトとオブジェクトに関する定義

TOE セキュリティ機能において対象とするサブジェクト、オブジェクト、操作、セキュリティ属性について、それぞれの説明を以下に記述する。

6.1.1. サブジェクト

TOEセキュリティ機能において対象とするサブジェクトを、表 8 に記述する。

表 8 サブジェクト一覧

使用される SFR	サブジェクト	定義
FDP_ACC.1 FDP_ACF.1	オフィス責任者プロセス	オフィス責任者を代行するプロセス。
	一般利用者プロセス	一般利用者を代行するプロセス

6.1.2. オブジェクト

TOEセキュリティ機能において対象とするオブジェクトを、表 9 に記述する。

表 9 オブジェクト一覧

使用される SFR	オブジェクト	定義
FDP_ACC.1 FDP_ACF.1	オフィス	組織、所属利用者に関する情報が格納される。
	キャビネット	キャビネット階層に関する情報が格納される。 上位のオフィス情報を保持する。
	フォルダ	フォルダ階層に関する情報が格納される。 上位のキャビネット情報、フォルダ情報を保持する。
	文書	文書データに関する情報が格納される。 上位のキャビネット情報、フォルダ情報を保持する。 複数の文書データを保持することができる。
	ショートカット	他のオブジェクトへのリンク情報が格納される。 上位のキャビネット情報、フォルダ情報を保持する。

6.1.3. 操作

TOEセキュリティ機能において対象とする操作を、表 10 に記述する。

表 10 操作一覧

使用される SFR	操作	定義
FDP_ACC.1 FDP_ACF.1	オフィスの参照(一覧)	オフィスの参照(一覧)を行う。
	キャビネットの登録、参照(一覧)、更新、削除、コピー、移動、アクセス権設定、キャビネット選択	キャビネットの登録、参照(一覧)、更新、削除、コピー、移動、アクセス権設定、キャビネット選択を行う。
	フォルダの登録、検索、参照(一覧)、更新、削除、コピー、移動、アクセス権設定、フォルダ選択	フォルダの登録、検索、参照(一覧)、更新、削除、コピー、移動、アクセス権設定、フォルダ選択を行う。

使用される SFR	操作	定義
	文書の登録、検索、参照(一覧)、更新、削除、コピー、移動、ダウンロード、アクセス権設定、文書の内容表示	文書の登録、検索、参照(一覧)、更新、削除、コピー、移動、内容表示、ダウンロード、アクセス権設定、文書の内容表示を行う。
	ショートカットの登録、検索、参照(一覧)、更新、削除、コピー、移動、アクセス権設定、ショートカットの選択	ショートカットの登録、検索、参照(一覧)、更新、削除、コピー、移動、アクセス権設定、ショートカットの選択を行う。

6.1.4. セキュリティ属性

TOEセキュリティ機能において対象とするセキュリティ属性を、表 11 に記述する。

表 11 セキュリティ属性一覧

使用される SFR	セキュリティ属性	内容	値
FDP_ACC.1 FDP_ACF.1	利用者種別	利用者種別を特定する属性	・オフィス責任者 ・一般利用者
	利用者所属組織情報	利用者が所属している組織を特定する属性	所属オフィス識別子の値
	利用者職位情報	利用者の職位を特定する属性	・社長 ・役員 ・部長 ・課長 ・主任 ・担当
	利用者識別情報	利用者を一意に特定する属性	利用者識別子の値
	オフィス識別情報	オフィスを一意に特定する属性	オフィス識別子の値
	オフィス責任者情報	オフィス責任者を特定する属性	利用者識別子の値
	オフィス利用許可者情報	オフィスに登録された利用者を特定する属性	利用者識別子の値リスト
	キャビネット識別情報	キャビネットを一意に特定する属性	キャビネット識別子の値
	キャビネット利用許可者情報	キャビネットの操作を許可された利用者を特定する属性	利用者識別子の値リスト
	フォルダ識別情報	フォルダを一意に特定する属性	フォルダ識別子の値
	フォルダ利用許可者情報	フォルダの操作を許可された利用者を特定する属性	利用者識別子の値リスト
	文書識別情報	文書を一意に特定する属性	文書識別子の値
	文書利用許可者情報	文書の操作を許可された利用者を特定する属性	利用者識別子の値リスト
	ショートカット識別情報	ショートカットを一意に特定する属性	ショートカット識別子の値
	ショートカット利用許	ショートカットの操作を許可さ	利用者識別子の値リスト

使用される SFR	セキュリティ属性	内容	値
	可者情報	れた利用者を特定する属性	

6.2. セキュリティ機能要件

セキュリティ機能のクラス毎に、TOE が提供するセキュリティ機能要件を以下に記述する。

6.2.1. FDP:利用者データ保護

FDP_ACC.1 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.1.1

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リスト]

＜サブジェクト＞

- オフィス責任者プロセス
- 一般利用者プロセス

＜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

＜SFP で扱われるサブジェクトとオブジェクト間の操作リスト＞

- オフィスの参照(一覧)
- キャビネットの登録、参照(一覧)、更新、削除、コピー、移動
- キャビネットのアクセス権設定
- キャビネットの選択
- フォルダの登録、検索、参照(一覧)、更新、削除、コピー、移動
- フォルダのアクセス権設定
- フォルダの選択
- 文書の登録、検索、参照(一覧)、更新、削除、コピー、移動
- 文書のアクセス権設定
- 文書の内容表示
- 文書のダウンロード
- ショートカットの登録、検索、参照(一覧)、更新、削除、コピー、移動
- ショートカットのアクセス権設定
- ショートカットの選択

[割付:アクセス制御 SFP]

＜キャビネット操作アクセス制御方針＞

FDP_ACF.1 セキュリティ属性によるアクセス制御

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_ACF1.1
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、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]
以下の各表に示す。
表 12 に、SFP下において制御されるサブジェクト、及び対応するSFP関連セキュリティ属性を示す。

表 12 サブジェクト、及び対応するセキュリティ属性

制御されるサブジェクト	対応する SFP 関連セキュリティ属性
オフィス責任者プロセス 一般利用者プロセス	利用者種別 利用者所属組織情報 利用者職位情報 利用者識別情報

表 13 に、SFP下において制御されるオブジェクト、及び対応するSFP関連セキュリティ属性を示す。

表 13 オブジェクト、及び対応するセキュリティ属性

制御されるオブジェクト	対応する SFP 関連セキュリティ属性
オフィス	オフィス識別情報 オフィス責任者情報 オフィス利用許可者情報
キャビネット	キャビネット識別情報 キャビネット利用許可者情報
フォルダ	フォルダ識別情報 フォルダ利用許可者情報
文書	文書識別情報 文書利用許可者情報
ショートカット	ショートカット識別情報 ショートカット利用許可者情報

[割付: アクセス制御 SFP]
＜キャビネット操作アクセス制御方針＞

FDP_ACF.1.2
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]

表 14 に示す。

表 14 TOE へのアクセスを管理する規則

制御されたサブジェクト	サブジェクトのセキュリティ属性	制御されたオブジェクト	オブジェクトのセキュリティ属性	制御された操作
オフィス責任者プロセス	利用者種別 (オフィス責任者) 利用者所属組織情報 利用者識別情報	オフィス	オフィス識別情報 オフィス責任者情報	参照(一覧)
		キャビネット	[登録先]オフィス識別情報 [登録先]オフィス責任者情報	登録
			キャビネット識別情報 オフィス責任者情報	参照(一覧) 更新 削除 コピー 移動
			キャビネット識別情報 オフィス責任者情報	アクセス権設定
			キャビネット識別情報 オフィス責任者情報	キャビネット選択
		フォルダ	[登録先]キャビネット識別情報 [登録先]オフィス責任者情報 または [登録先]フォルダ識別情報 [登録先]オフィス責任者情報	登録
			フォルダ識別情報 オフィス責任者情報	参照(一覧) 更新 検索 削除 コピー 移動
			フォルダ識別情報 オフィス責任者情報	アクセス権設定
			フォルダ識別情報 オフィス責任者情報	フォルダ選択
		文書	キャビネット識別情報 オフィス責任者情報	登録
			文書識別情報 オフィス責任者情報	参照(一覧) 更新 検索 削除 コピー 移動
			文書識別情報 オフィス責任者情報	アクセス権設定
			文書識別情報 オフィス責任者情報	内容表示 ダウンロード
		ショートカット	[登録先]キャビネット識別情報 [登録先]オフィス責任者情報	登録

制御された サブジェクト	サブジェクトの セキュリティ属性	制御された オブジェクト	オブジェクトの セキュリティ属性	制御された 操作
			ショートカット識別情報 オフィス責任者情報	参照(一覧) 更新 検索 削除 コピー 移動
			ショートカット識別情報 オフィス責任者情報	アクセス権設定
			ショートカット識別情報 オフィス責任者情報	ショートカット選択
一般利用者 プロセス	利用者種別 (一般利用者) 利用者所属組織情報 利用者職位情報 利用者識別情報	オフィス	オフィス識別情報 オフィス利用許可者情報 (利用者所属組織)	参照(一覧)
		キャビネット	キャビネット識別情報 キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧)
			キャビネット識別情報 キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	キャビネット選択
		フォルダ	[登録先]キャビネット識別情報 [登録先]キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別) または [登録先]フォルダ識別情報 [登録先]フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	登録
			フォルダ識別情報 フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧) 更新 検索 削除 コピー 移動
			フォルダ識別情報 フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	フォルダ選択
		文書	[登録先]キャビネット識別情報 [登録先]キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別) または [登録先]フォルダ識別情報 [登録先]フォルダ利用許可者情報	登録

制御された サブジェクト	サブジェクトの セキュリティ属性	制御された オブジェクト	オブジェクトの セキュリティ属性	制御された 操作
			(利用者所属組織、利用者職位、利用者識別)	
			文書識別情報 文書利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧) 更新 検索 削除 コピー 移動
			文書識別情報 文書利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	内容表示 ダウンロード
		ショートカット	[登録先]キャビネット識別情報 [登録先]キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別) または [登録先]フォルダ識別情報 [登録先]フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	登録
			ショートカット識別情報 ショートカット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧) 更新 検索 削除 コピー 移動
			ショートカット識別情報 ショートカット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	ショートカット 選択

※オフィス責任者の場合、操作の対象となるオブジェクトの識別情報(オフィス識別情報、キャビネット識別情報、フォルダ識別情報、文書識別情報、ショートカット識別情報)を参照して特定し、該当するオブジェクトのオフィス責任者情報が、サブジェクトの利用者識別情報と一致したときに、操作が許可される。

※一般利用者の場合、操作の対象となるオブジェクトの識別情報(オフィス識別情報、キャビネット識別情報、フォルダ識別情報、文書識別情報、ショートカット識別情報)を参照して特定し、該当するオブジェクトのキャビネット利用許可者情報、フォルダ利用許可者情報、文書利用許可者情報、ショートカット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、利用者識別が、サブジェクトの利用者所属組織情報、利用者職位情報、利用者識別情報と一致したときに、操作が許可される。

※オフィス責任者の場合でも、自分が所属していないオフィスのなかで操作を行うときは、一般利用者として許可された操作に限定される。

FDP_ACF.1.3

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.1.4
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

6.2.2. FIA：識別認証

FIA_AFL.1 認証失敗時の取扱い
下位階層：　なし
依存性：　　FIA_UAU.1 認証のタイミング

FIA_AFL.1.1
TSF は、[割付：*認証事象のリスト*]に関して、[選択：[*割付：正の整数値*]、[*割付：許容可能な値の範囲*]*内における管理者設定可能な正の整数値*]回の不成功認証試行が生じたときを検出しなければならない。

[割付：認証事象のリスト]
　最後に成功した認証以降のオフィス責任者、及び一般利用者の認証

[選択：[割付：正の整数値]、「[割付：許容可能な値の範囲]内における管理者設定可能な正の整数値」]：
　「5 から 99999 回内におけるシステム管理者が設定可能な正の整数値」

FIA_AFL.1.2
不成功の認証試行が定義した回数[選択：*に達する、上回った*]とき、TSF は、[割付：*アクションのリスト*]をしなければならない。

[選択：に達する、上回った]
　に達する
[割付：アクションのリスト]
　システム管理者が解除するまで、アカウントのロック

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*]：
詳細化：　　利用者→オフィス責任者、及び一般利用者

[割付: セキュリティ属性のリスト]
{利用者種別、
利用者所属組織情報、
利用者職位情報、
利用者識別情報}

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]
以下の品質尺度
<品質尺度>
・パスワードは、パスワードポリシーに設定されたパスワード最小長の文字以上で 128 文字以下、以下の範囲の ASCII 文字が使用できる。
・アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字。
・数字は、 [0-9] の合計 10 文字。
・記号は、 !"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字。
・1 文字以上の数字または記号を含む。
・新しいパスワードは、直前のパスワードと同一であってはならない。

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。
詳細化: 利用者→オフィス責任者、及び一般利用者

FIA_UID.2a アクション前の利用者識別 (オフィス責任者、一般利用者)
下位階層: FIA_UID.1 識別のタイミング
依存性: なし

FIA_UID.2.1a
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。
詳細化: 利用者→オフィス責任者、及び一般利用者
識別 →ユーザ ID による識別

FIA_UID.2b アクション前の利用者識別 (システム管理者)
下位階層: FIA_UID.1 識別のタイミング

依存性: なし

FIA_UID.2.1b
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。
詳細化: 各利用者→システム管理者
識別 →OS アカウントによる識別

FIA_USB.1 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.1.1
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]
- 利用者種別
- 利用者所属組織情報
- 利用者職位情報
- 利用者識別情報

FIA_USB.1.2
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]
表 15 に示す。

表 15 属性の最初の関連付けの規則

利用者	利用者を代行して動作するサブジェクト	利用者セキュリティ属性	セキュリティ属性の値
オフィス責任者	オフィス責任者プロセス	利用者種別	オフィス責任者
		利用者所属組織情報	オフィス識別子の値
		利用者職位情報	職位コードの値
		利用者識別情報	利用者識別子の値
一般利用者	一般利用者プロセス	利用者種別	一般利用者
		利用者所属組織情報	オフィス識別子の値
		利用者職位情報	職位コードの値
		利用者識別情報	利用者識別子の値

FIA_USB.1.3
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

6.2.3. FMT:セキュリティ管理

FMT_MSA.1 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。

[割付: セキュリティ属性のリスト]
表 16 に示す。
[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]]
表 16 に示す。
[割付: その他の操作]
表 16 に示す。
[割付: 許可された識別された役割]
表 16 に示す。
[割付: アクセス制御 SFP、情報フロー制御 SFP]
キャビネット操作アクセス制御方針

表 16 セキュリティ属性の管理

セキュリティ属性	デフォルト値変更、問い合わせ、改変、削除、その他の操作	許可された識別された役割
キャビネット利用許可者情報 フォルダ利用許可者情報 文書利用許可者情報 ショートカット利用許可者情報	問い合わせ、改変、削除、登録	オフィス責任者

FMT_MSA.3 静的属性初期化

下位階層: なし

依存性: FMT_MSA.1 セキュリティ属性の管理
FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1

TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択: *制限的*、*許可的*、*[割付: その他の特性]*:から 1 つのみ選択]デフォルト値を与える[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。

[選択: 制限的、許可的、[割付: その他の特性]:から 1 つのみ選択]
制限的
[割付: アクセス制御 SFP、情報フロー制御 SFP]
キャビネット操作アクセス制御方針

FMT_MSA.3.2

TSF は、オブジェクトや情報が生成されるとき、[割付: *許可された識別された役割*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[割付: 許可された識別された役割]
　なし

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。

[割付: TSF データのリスト]
　表 17 に示す。
[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]]
　表 17 に示す。
[割付: その他の操作]
　表 17 に示す。
[割付: 許可された識別された役割]
　表 17 に示す。

表 17 TSF データの管理

TSF データ	デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
オフィス責任者のユーザ ID	問い合わせ、作成、削除	システム管理者
	問い合わせ	オフィス責任者
オフィス責任者のパスワード	作成、改変	システム管理者
	改変	オフィス責任者
一般利用者のユーザ ID	問い合わせ、作成、削除	システム管理者
	問い合わせ	一般利用者
一般利用者のパスワード	作成、改変	システム管理者
	改変	一般利用者
パスワード最小長	改変	システム管理者
オフィス責任者、一般利用者のアカウントロックの有効設定	改変	システム管理者
利用者の最後に成功した認証以降の不成功認証試行回数の閾値	改変	システム管理者
対話セション終了となる利用者が非アクティブである時間	改変	システム管理者
アカウントロック状態のユーザ(オフィス責任者、一般利用者)	改変	システム管理者

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]
以下の 表 18 に示す。

表 18 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
FDP_ACC.1	なし	なし
FDP_ACF.1	・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(変更不可のため管理項目はない)
FIA_AFL.1	・不成功の認証試行に対する閾値の管理	・不成功の認証試行に対する閾値の管理
	・認証失敗の事象においてとられるアクションの管理	なし(アクションは固定であり、管理対象とならない)
FIA_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(アクションは固定であり、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	・パスワード最小長の管理
FIA_UAU.2	・管理者による認証データの管理;	オフィス責任者、一般利用者のパスワードの登録
	・このデータに関係する利用者による認証データの管理。	オフィス責任者、一般利用者のパスワードの改変
FIA_UID.2a	・利用者識別情報の管理。	オフィス責任者、一般利用者のユーザ ID の作成、問い合わせ、削除
FIA_UID.2b	・利用者識別情報の管理。	なし(変更不可のため管理項目はない)
FIA_USB.1	・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。	
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(アクションは固定であり、管理対象とならない)
	・セキュリティ属性が特定の値を引き継ぐための規則を管理すること。	なし(アクションは固定であり、管理対象とならない)
FMT_MSA.3	・初期値を特定できる役割のグループを管理すること;	なし(初期値を特定できる役割のグループはない)
	・所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	なし(アクションは固定であり、管理対象とならない)
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 データと相互に影響を及ぼし得る役割のグループは固定であり、管理対象とならない)

機能要件	管理要件	管理項目
FMT_SMF.1	なし	なし
FMT_SMR.2	・役割の一部をなす利用者のグループを管理すること。	なし(役割の一部をなす利用者のグループは固定であり、管理対象とならない)
	・役割が満たさなければならない条件を管理すること。	なし(役割が満たさなければならない条件は固定であり、管理対象とならない)
FPT_STM.1	・時間の管理	なし(時刻の管理は、OS により行われるため、管理対象とならない)
FTA_SSL.3	・個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定;	・対話セションの終了を生じさせる利用者が非アクティブである時間の管理
	・対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定。	

FMT_SMR.2 セキュリティ役割における制限
下位階層: FMT_SMR.1 セキュリティの役割
依存性: FIA_UID.1 識別のタイミング

FMT_SMR.2.1
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]
・システム管理者
・オフィス責任者
・一般利用者

FMT_SMR.2.2
TSF は、利用者を役割に関連付けなければならない。

FMT_SMR.2.3
TSF は、条件[割付: *異なる役割に対する条件*]が満たされていることを保証しなければならない。

[割付: 異なる役割に対する条件]
・オフィス責任者は、自分が所属していないオフィスのなかで操作するときには、一般利用者となること

6.2.4. FPT:TSF データの保護

FPT_STM.1 高信頼タイムスタンプ
下位階層: なし
依存性: なし

FPT_STM.1.1
TSF は、高信頼タイムスタンプを提供できなければならない。

6.2.5. FTA:TOE アクセス

FTA_SSL.3 TSF 起動による終了

下位階層: なし
依存性: なし

FTA_SSL.3.1
TSF は、[割付: *利用者が非アクティブである時間間隔*]後に対話セションを終了しなければならない。

[割付: 利用者が非アクティブである時間間隔]
・最後の操作から、20 分から 60 分の初期設定時間

6.3. セキュリティ保証要件

TOE セキュリティ保証要件を以下に記述する。

6.3.1. ADV: 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

6.3.2. AGD: 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

6.3.3. ALC: 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

6.3.4. ASE: 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

6.3.5. ATE: 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

6.3.6. AVA: 脆弱性評定

AVA_VAN.2: 脆弱性分析

6.4. セキュリティ要件根拠

TOE セキュリティ保証要件を以下に記述する。

6.4.1. 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、以下の 表 19 に示す。
表中の「×」は対応関係にあることを示している。

表 19 セキュリティ機能要件とセキュリティ対策方針との関係

セキュリティ対策方針 / セキュリティ機能要件	O.I&A	O.CHECK_PASSWORD_POLICY	O.ACCESS_CONTROL	O.AUTO_LOGOUT
FDP_ACC.1			×	
FDP_ACF.1			×	
FIA_AFL.1	×	×		
FIA_ATD.1	×		×	
FIA_SOS.1		×		
FIA_UAU.2	×			
FIA_UID.2a	×			
FIA_UID.2b	×			
FIA_USB.1	×		×	
FMT_MSA.1			×	
FMT_MSA.3			×	
FMT_MTD.1			×	
FMT_SMF.1			×	
FMT_SMR.2			×	
FPT_STM.1				×
FTA_SSL.3				×

次に、各セキュリティ対策方針が、TOE 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し、必要な対策の詳細を分析する。次に、それぞれの対策に対し、要求機能を示し、それをすべて満たすことでセキュリティ対策方針を実現できることを示す。
なお、要求機能については、1 つ以上のセキュリティ機能要件がそれを満たし、セキュリティ対策方針に対する機能要件として必要であることを示す。

O.I&A(識別認証)
この TOE セキュリティ対策方針は、正当な TOE の利用者のみが TOE を利用できるように、利用者の制限を求めている。これにより、正当な TOE 利用者であることの判断を行う。この対策の詳細と、必要機能は以下のとおりである。

a. TOE サービス機能の利用前に、オフィス責任者、及び一般利用者を識別
TOE サービス機能の操作前に、ユーザ ID により、利用許可者であることが識別されなければならない。このため、識別前には、TOE サービス機能のいかなる操作も許可されない。
これに該当するセキュリティ機能要件は、FIA_UID.2a である。

b. TOE 運用機能の利用前に、システム管理者を識別

TOE 運用機能の操作前に、OS に登録されたアカウントにより、システム管理者であることが識別されなければならない。このため、識別前には、TOE 運用機能のいかなる操作も許可されない。
これに該当するセキュリティ機能要件は、FIA_UID.2b である。

c. TOE サービス機能の利用前に、オフィス責任者、及び一般利用者を認証
TOE サービス機能の操作前に、利用許可者であることが、認証されなければならない。
このため、認証前には、TOE サービス機能のいかなる操作も許可されない。
これに該当するセキュリティ機能要件は、FIA_UAU.2 である。

d. 識別認証成功時の TOE サービス機能の利用許可
識別認証に成功したオフィス責任者、及び一般利用者は、 TOE のサービス機能を利用できなければならない。
TOE は、TOE の利用者を代行するサブジェクトを生成、それぞれのセキュリティ属性を関連付けて、TOE を利用するしくみを提供する。
これに該当するセキュリティ機能要件は、FIA_ATD.1、及び FIA_USB.1 である。

e. 指定回数を超えた識別認証失敗時に、TOE 利用の無効化
識別認証に失敗したオフィス責任者、及び一般利用者は、TOE の正当な利用者でないとみなす必要がある。TOE は、指定した回数を越えて識別認証に失敗したオフィス責任者、及び一般利用者に対し、アカウントのロックを実施する。
これに該当するセキュリティ機能要件は、FIA_AFL.1 である。

以上、a、b、c、d のすべての対策を満たすことは、O.I&A を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FIA_AFL.1、FIA_ATD.1、FIA.UID.2a、FIA.UID.2b、FIA_UAU.2、FIA_USB.1 の達成により、O.I&A を実現できる。

O.CHECK_PASSWORD_POLICY(パスワードポリシーチェック)

この TOE セキュリティ対策方針は、TOE の正当な利用者の認証情報(パスワード)について、本人以外が利用できないように、パスワードポリシーに基づき、一定の品質基準を維持することを求めている。また、パスワードポリシーに基づき、認証失敗の指定回数を超えたときにアカウントをロックすることを求めている。この対策の詳細と、必要機能は以下のとおりである。

a. 一定品質基準のパスワードであることを確認
認証を行う際に必要なパスワードは、本人以外に予測することが困難でなければならない。予測することが困難であるために、TOE の利用者に対し、必要なレベルの品質を明確に定義し、その品質を満たしていることを検証する。
これに該当するセキュリティ機能要件は、FIA_SOS.1 である。

b. 指定回数を超えた認証失敗時のアカウントロック維持
パスワードポリシーに指定した回数を越えて、認証に失敗したオフィス責任者、及び一般利用者に対して、システム管理者が解除するまで、アカウントロックを維持する。
これに該当するセキュリティ機能要件は、FIA_AFL.1 である。

以上、a、b の対策を満たすことは、O.CHECK_PASSWORD_POLICY を満たすことである。したがって、その対策に必要な機能要件として該当する、FIA_SOS.1、FIA_AFL.1 の達成により、O.CHECK_PASSWORD_POLICY を実現できる。

O.ACCESS_CONTROL(アクセス制御)

この TOE セキュリティ対策方針は、TOE の利用者を代行するプロセスが、付与された権限により、許可操作による、保護資産に対するアクセス制御を求めている。この対策の詳細と、必要機能は以下のとおりである。

a. アクセス制御規定の実施

オフィス責任者、及び一般利用者に対して、許可操作と操作対象を決定する。このとおり、許可利用者のみが操作をできるように、実施しなければならない。
このため、TOE の利用者を代行して動作する各サブジェクトと、各操作対象(オブジェクト)の操作リストを定義し、その定義にしたがってアクセス制御を実施する。
これに該当するセキュリティ機能要件は、FDP_ACC.1、FDP_ACF.1 である。

b. 利用者をプロセスに関連付け
オフィス責任者、及び一般利用者に応じてアクセスを制限するため、TOE を利用するとき、各利用者が持つセキュリティ属性を、自分を代行して動作するプロセス(サブジェクト)に関連付ける必要がある。
これに該当するセキュリティ機能要件は、FIA_ATD.1、FIA_USB.1 である。

c. 利用者役割に応じたアクセス制御
意図したアクセス制御を行うために、利用者のセキュリティ属性である利用者種別を適切に設定し、各操作対象(オブジェクト)のセキュリティ属性である利用許可者情報の管理をオフィス責任者に制限しなければならない。このセキュリティ属性には、デフォルト値が存在せず、初期値を特定できる利用者は存在しない。
これに該当するセキュリティ機能要件は、FMT_MSA.1、FMT_MSA.3、FMT_SMR.2 である。

d. TOE の動作に影響する操作を制限
TOE の動作に影響を与える可能性のある TSF データの操作を、許可されている利用者に限定し、許可以外の操作を禁止する。
これに該当するセキュリティ機能要件は、FMT_MTD.1 である。

e. TOE の動作に影響する管理機能を特定
TOE は、TOE の動作に影響する管理機能を特定する。これにより、セキュリティ属性の管理を行う。
これに該当するセキュリティ機能要件は、FMT_SMF.1 である。

以上、a、b、c、d、e のすべての対策を満たすことは、O_ACCESS_CONTROL を満たすことである。したがって、それぞれの対策に必要な機能要件として該当する、FDP_ACC.1、FDP_ACF.1、FIA_ATD.1、FIA_USB.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1、FMT_SMR.2 の達成により、O_ACCESS_CONTROL が実現できる。

O.AUTO_LOGOUT(自動ログアウト)

この TOE セキュリティ対策方針は、TOE と TOE の利用者との対話セションの終了について求めている。この対策の詳細と、必要機能は以下のとおりである。

a. 対話セションを終了
TOE は、TOE を操作していない状態が、予め決定している時間間隔を超えた場合に、オフィス責任者、及び一般利用者との対話セションを切断する。
これに該当するセキュリティ機能要件は、FPT_STM.1、FTA_SSL.3 である。

以上、a の対策を満たすことは、O.AUTO_LOGOUT を満たすことである。したがって、その対策に必要な機能要件として該当する、FPT_STM.1、FTA_SSL.3 の達成により、O.AUTO_LOGOUT を実現できる。

6.4.2. セキュリティ機能要件依存性

セキュリティ要件のコンポーネントの依存性を、表 20 に示す。

表 20 セキュリティ要件コンポーネントの依存性

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	妥当性
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし	

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	妥当性
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1	なし	
	FMT_MSA.3	FMT_MSA.3	なし	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 (左記の上位階層)	なし	
FIA_ATD.1	なし	なし	なし	
FIA_SOS.1	なし	なし	なし	
FIA_UAU.2	FIA_UID.1	FIA_UID.2a (左記の上位階層)	なし	
FIA_UID.2a	なし	なし	なし	
FIA_UID.2b	なし	なし	なし	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし	
FMT_MSA.1	FDP_ACC.1 または FDP_IFC.1	FDP_ACC.1	なし	
	FMT_SMR.1	FMT_SMR.2 (左記の上位階層)	なし	
	FMT_SMF.1	FMT_SMF.1	なし	
FMT_MSA.3	FMT_MSA.1	FMT_MSA.1	なし	
	FMT_SMR.1	なし	FMT_SMR.1	※
FMT_MTD.1	FMT_SMF.1	FMT_SMF.1	なし	
	FMT_SMR.1	FMT_SMR.2 (左記の上位階層)	なし	
FMT_SMF.1	なし	なし	なし	
FMT_SMR.2	FIA_UID.1	FIA_UID.2a FIA_UID.2b (左記の上位階層)	なし	
FPT_STM.1	なし	なし	なし	
FTA_SSL.3	なし	なし	なし	

表 20 より、セキュリティ機能要件は、後述する例外を除いて必要な依存関係をすべて満たしている。例外について、依存関係を満たさなくても問題がない根拠を以下に示す。

※) FMT_MSA.3→FMT_SMR.1

本 TOE では、FMT_MSA.3 のセキュリティ属性の初期値を特定する、許可された識別された役割が存在しないため、依存関係は不要である。

6.4.3. セキュリティ保証要件根拠

本製品は、会社組織内の業務に関する情報を共有するものであり、そのセキュリティ機能には信頼性が要求されている。EAL2 では、TOE における開発段階のセキュリティ対策の分析(セキュリティアーキテクチャ設計の分析、詳細設計のサブシステムレベルでの分析、テストの実施)を含み、セキュリティ機能を安全に使用するための十分なガイダンス情報を必要としているため、妥当な選択といえる。

7. TOE 要約仕様

本章では、TOE のセキュリティ機能性について記述する。

7.1. 識別認証機能

識別認証機能は、TOE へアクセスする利用者を識別して、正当な利用者、かつ利用者本人であることを確認するための機能を提供する。また、認証に使用するパスワードにおける品質尺度の検証、TOE と利用者との対話セション終了のしくみも提供する。以下に、識別認証機能について、SFR 実現方法という観点から説明する。

7.1.1. 識別認証機能に対応する SFR の実現方法

(1) FIA_UID.2a アクション前の利用者識別、FIA_UAU.2 アクション前の利用者認証

TOE は、TOE のサービス機能を利用させる前に、オフィス責任者、及び一般利用者を識別認証する。識別認証は、ユーザ ID による識別とパスワードによる認証を行う。なお、パスワードについては、パスワード有効期間の検証を行う。

・以下の処理が、すべて成功した場合に、オフィス責任者、及び一般利用者の識別認証が成功となる。

1. ユーザ ID による識別
2. ユーザ ID に対応するパスワードによる認証

・ユーザ ID、またはパスワードのいずれかに誤りがある場合、またはパスワードの有効期限切れの場合には、識別認証の異常を通知する。

上記より、FIA_UID.2a、FIA_UAU.2 を実現する。

(2) FIA_UID.2b アクション前の利用者識別

TOE は、TOE の運用機能を利用させる前に、システム管理者を識別する。識別は、Web サーバ上、及びリソースサーバ上の OS に登録されたアカウントによる識別を行う。

上記より、FIA_UID.2b を実現する。

(3) FIA_AFL.1 認証失敗時の取り扱い

TOE は、オフィス責任者、及び一般利用者の識別認証に関して、以下の機能を提供する。

・オフィス責任者、及び一般利用者が使用するユーザ ID に対するパスワードに誤りがある場合、ユーザ ID 毎に、パスワードの誤り回数をカウントする。

・累積誤り回数が、システム管理者が設定した不成功認証試行回数(5 から 99999 回)に達すると、そのユーザ ID のアカウントをロックする。アカウントをロックされたオフィス責任者、及び一般利用者は、システム管理者がアカウントロック解除(アカウントロック状態のユーザを改変)するまで、TOE を使用できない。

・アカウントロック解除を行ったユーザ ID については、パスワードの誤り回数を 0 に戻す。

上記より、FIA_ AFL.1 を実現する。

(4) FIA_SOS.1 秘密の検証

TOE は、オフィス責任者、及び一般利用者のパスワードの作成、改変を行うとき、以下の条件を満たすことを検証し、検証に成功したパスワードのみを設定する。

1. パスワードは、パスワードポリシーに設定されたパスワード最小長の文字以上で 128 文字以下の文字列

2. 使用する文字は、以下の ASCII 文字を使用する
   英大文字: [A-Z]の 26 文字
   英小文字: [a-z]の 26 文字
   数字: [0-9]の 10 文字
   記号: [!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~]の 32 文字
   ・1 文字以上の数字または記号を含む。
   ・新しいパスワードは、直前のパスワードと同一であってはならない。

上記より、FIA_ SOS.1 を実現する。

(5) FTA_SSL.3 TSF 起動による終了、FPT_STM.1 高信頼タイムスタンプ

TOE は、TOE と利用者クライアント端末間に確立するセションに関して、以下の機能を提供する。
・TOE は、OS から取得した時刻に基づき、利用者クライアントが無操作状態のまま、システム管理者が設定した時間(利用者が非アクティブである時間)を経過したときに、セションの切断処理を実行する。
・初期設定時間(20 分から 60 分)は、システム管理者が設定。
上記より、FTA_SSL.3、FPT_STM.1 を実現する。

7.2. アクセス制御機能

アクセス制御機能は、TOE 利用者の役割毎に付与した権限に基づいて、利用者データへの操作を制御するための機能を提供する。
以下に、アクセス制御機能について、SFR 実現方法という観点から説明する。

7.2.1. アクセス制御機能に対応する SFR の実現方法

(1) FIA_ATD.1 利用者属性定義、FIA_USB.1 利用者-サブジェクト結合

TOE は、識別認証されたオフィス責任者、及び一般利用者について、以下のセキュリティ属性を定義し、TOE 内部でオフィス責任者、及び一般利用者を代行して動作する、オフィス責任者プロセス、及び一般利用者プロセスに対し、以下のセキュリティ属性を保持する。
・利用者種別(オフィス責任者、一般利用者)
・利用者所属組織情報
・利用者職位情報
・利用者識別情報
上記より、FIA_ATD.1、FIA_USB.1 を実現する。

(2) FMT_SMR.2 セキュリティ役割における制限

TOE は、識別認証の結果、オフィス責任者として識別された場合にはオフィス責任者の役割が付与され、一般利用者として識別された場合には一般利用者の役割が付与される。なお、オフィス責任者であっても、所属組織ではないオフィスで操作を行う場合は、一般利用者の役割となる。
また、Web サーバ上、及びリソースサーバ上の OS に登録されたアカウントによる識別の結果より、システム管理者として識別された場合はシステム管理者の役割が付与される。
上記より、FMT_SMR.2 を実現する。

(3) FDP_ACC.1 サブセットアクセス制御、FDP_ACF.1 セキュリティ属性によるアクセス制御

TOEは、システム管理者により登録されたキャビネットサービスのオフィスについて、その配下のオブジェクト操作に対する、以下の 表 21 に示す、キャビネット操作アクセス制御方針を定義する。

TOE は、識別認証された一般利用者が、キャビネットサービスのオブジェクトの操作を行うときに、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、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、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、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のオブジェクトの操作を行うときには、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が一致しないとき)は、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、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、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。

表 21 TOE へのアクセスを管理する規則

制御された サブジェクト	サブジェクトの セキュリティ属性	制御された オブジェクト	オブジェクトの セキュリティ属性	制御された 操作
オフィス責任者プロセス	利用者種別 (オフィス責任者) 利用者所属組織情報 利用者識別情報	オフィス	オフィス識別情報 オフィス責任者情報	参照(一覧)
		キャビネット	オフィス識別情報 オフィス責任者情報	登録
			キャビネット識別情報 オフィス責任者情報	参照(一覧) 更新 削除 コピー 移動
			キャビネット識別情報 オフィス責任者情報	アクセス権設定
			キャビネット識別情報 オフィス責任者情報	キャビネット選択
		フォルダ	[登録先]キャビネット識別情報 [登録先]オフィス責任者情報 または [登録先]フォルダ識別情報 [登録先]オフィス責任者情報	登録
			フォルダ識別情報 オフィス責任者情報	参照(一覧) 更新 検索 削除 コピー 移動
			フォルダ識別情報 オフィス責任者情報	アクセス権設定
			フォルダ識別情報 オフィス責任者情報	フォルダ選択
		文書	[登録先]キャビネット識別情報 [登録先]オフィス責任者情報	登録

制御された サブジェクト	サブジェクトの セキュリティ属性	制御された オブジェクト	オブジェクトの セキュリティ属性	制御された 操作
			文書識別情報 オフィス責任者情報	参照(一覧) 更新 検索 削除 コピー 移動
			文書識別情報 オフィス責任者情報	アクセス権設定
			文書識別情報 オフィス責任者情報	内容表示 ダウンロード
		ショートカット	[登録先]キャビネット識別情報) [登録先]オフィス責任者情報	登録
			ショートカット識別情報 オフィス責任者情報	参照(一覧) 更新 検索 削除 コピー 移動
			ショートカット識別情報 オフィス責任者情報	アクセス権設定
			ショートカット識別情報 オフィス責任者情報	ショートカット選択
一般利用者 プロセス	利用者種別 (一般利用者) 利用者所属組織情報 利用者職位情報 利用者識別情報	オフィス	オフィス識別情報 オフィス利用許可者情報 (利用者所属組織)	参照(一覧)
		キャビネット	キャビネット識別情報 キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧)
			キャビネット識別情報 キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	キャビネット選択
		フォルダ	[登録先]キャビネット識別情報 [登録先]キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別) または [登録先]フォルダ識別情報 [登録先]フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	登録
			フォルダ識別情報 フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧) 更新 検索 削除 コピー

制御された サブジェクト	サブジェクトの セキュリティ属性	制御された オブジェクト	オブジェクトの セキュリティ属性	制御された 操作
				移動
			フォルダ識別情報 フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	フォルダ選択
		文書	[登録先]キャビネット識別情報 [登録先]キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別) または [登録先]フォルダ識別情報 [登録先]フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	登録
			文書識別情報 文書利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧) 更新 検索 削除 コピー 移動
			文書識別情報 文書利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	内容表示 ダウンロード
		ショートカット	[登録先]キャビネット識別情報 [登録先]キャビネット利用許可者情報 (利用者所属組織、利用者職位、利用者識別) または [登録先]フォルダ識別情報 [登録先]フォルダ利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	登録
			ショートカット識別情報 ショートカット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	参照(一覧) 更新 検索 削除 コピー 移動
			ショートカット識別情報 ショートカット利用許可者情報 (利用者所属組織、利用者職位、利用者識別)	ショートカット 選択

上記より、FDP_ACC.1、FDP_ACF.1 を実現する。

(4) FMT_MSA.1 セキュリティ属性の管理、FMT_MSA.3 静的属性初期化

TOE は、識別認証の結果より、オフィス責任者の利用者役割に対してのみ、以下のセキュリティ属性の操作を許可する。
・キャビネット利用許可者情報に対する、問い合わせ、改変、登録、削除
・フォルダ利用許可者情報に対する、問い合わせ、改変、登録、削除
・文書利用許可者情報に対する、問い合わせ、改変、登録、削除
・ショートカット利用許可者情報に対する、問い合わせ、改変、登録、削除
なお、上記のセキュリティ属性のデフォルト値は、オブジェクトを登録したオフィスに所属している利用者に制限する。この値を上書きする、初期値を設定する利用者役割は存在しない。
上記より、FMT_MSA.1、FMT_MSA.3 を実現する。

(5) FMT_MTD.1 TSF データの管理
TOEは、TSFデータに対して、以下の 表 22 に示す、識別された役割に基づいて操作を行うインタフェース以外を提供しないことにより、TSFデータの操作を制限する。

表 22 TSF データの管理

TSF データ	デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
オフィス責任者のユーザ ID	問い合わせ、作成、削除	システム管理者
	問い合わせ	オフィス責任者
オフィス責任者のパスワード	作成、改変	システム管理者
	改変	オフィス責任者
一般利用者のユーザ ID	問い合わせ、作成、削除	システム管理者
	問い合わせ	一般利用者
一般利用者のパスワード	作成、改変	システム管理者
	改変	一般利用者
パスワード最小長	改変	システム管理者
オフィス責任者、一般利用者のアカウントロックの有効設定	改変	システム管理者
利用者の最後に成功した認証以降の不成功認証試行回数の閾値	改変	システム管理者
対話セション終了となる利用者が非アクティブである時間	改変	システム管理者
アカウントロック状態のユーザ(オフィス責任者、一般利用者)	改変	システム管理者

上記より、FMT_MTD.1 を実現する。

(6) FMT_SMF.1 管理機能の特定
TOEは、セキュリティ機能を維持するため、以下の 表 23 に示すセキュリティ管理機能を提供する。

表 23 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_AFL.1	・不成功の認証試行に対する閾値の管理	・不成功の認証試行に対する閾値の管理
FIA_SOS.1	・秘密の検証に使用される尺度の管理	・パスワード最小長の管理
FIA_UAU.2	・管理者による認証データの管理;	オフィス責任者、一般利用者のパスワードの登録

機能要件	管理要件	管理項目
	・このデータに関係する利用者による認証データの管理。	オフィス責任者、一般利用者のパスワードの改変
FIA_UID.2a	・利用者識別情報の管理。	オフィス責任者、一般利用者のユーザ ID の作成、問い合わせ、削除
FTA_SSL.3	・個々の利用者に対し対話セションの終了を生じさせる利用者が非アクティブである時間の特定;	・対話セションの終了を生じさせる利用者が非アクティブである時間の管理
	・対話セションの終了を生じさせる利用者が非アクティブであるデフォルト時間の特定。	

上記は、FMT_MTD.1 により、FMT_SMF.1 を実現する。