NEC グループ セキュア情報交換サイト

バージョン 1.0

セキュリティターゲット

バージョン：1. 14

2008 **年** 4 **月** 3 **日**

日本電気株式会社

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	-	-	2007/9/19	日本電気株式会社
1.01	内部レビュー反映	1 章	TOE 記述の修正	2007/10/12	日本電気株式会社
		3 章	脅威、前提条件の見直し	2007/10/12	
		4 章	対策方針根拠の修正	2007/10/12	
		6 章	SFR の見直しと追加	2007/10/12	
		7 章	SFR の見直しに伴う修正	2007/10/12	
1.02	評価確認事項、ST 対応分析の反映	1 章 3 章～4 章 6 章～7 章	各章の対応関係の見直し	2007/11/14	日本電気株式会社
		2 章、5 章	拡張機能コンポーネント定義追加	2007/11/14	
1.03	評価指摘事項の反映	1 章	TOE 概要の修正 TOE 記述の修正	2007/12/7	日本電気株式会社
		3 章	脅威の表記の見直し	2007/12/7	
		4 章	対策方針の修正	2007/12/7	
		5 章	拡張機能コンポーネント定義修正	2007/12/7	
		6 章	SFR の記述の見直し	2007/12/7	
		7 章	SFR の見直しに伴う修正	2007/12/7	
1.04	評価指摘事項の反映	1 章	TOE 記述の修正	2007/12/21	日本電気株式会社
		4 章	不要な対策方針の削除	2007/12/21	
		6 章	不要な SFR の削除	2007/12/21	
		7 章	SFR の見直しに伴う修正	2007/12/21	
1.05	評価指摘事項の反映	3 章	脅威の表記の見直し	2008/1/15	日本電気株式会社
		4 章	対策方針の修正	2008/1/15	
		6 章	SFR の定義の見直し	2008/1/15	
1.06	評価指摘事項の反映	1 章	ソフトウェア構成の説明修正	2008/1/18	日本電気株式会社
		3 章	脅威の表記の見直し	2008/1/18	
		4 章	不要な対策方針の削除	2008/1/18	
		5 章	拡張機能コンポーネント説明修正	2008/1/18	
		6 章	SFR の見直し	2008/1/18	
		7 章	SFR の見直しに伴う修正	2008/1/18	
1.07	評価指摘事項の反映	6 章	SFR の記述見直し	2008/1/25	日本電気株式会社
		7 章	SFR の見直しに伴う修正	2008/1/25	
1.08	評価指摘事項の反映	6 章	SFR の記述見直し	2008/1/30	日本電気株式会社
1.09	評価指摘事項の反映	6 章	SFR の記述見直し	2008/1/31	日本電気株式会社
1.10	評価指摘事項の反映	4 章	対策方針の追加 対策方針の説明追記 対策方針根拠の修正	2008/2/14	日本電気株式会社

バージョン	変更概要	変更箇所		変更日	変更者
		章･節･項	内容		
		5 章	表記誤り修正	2008/2/14	
		6 章	SFR の記述見直し 要件根拠の修正	2008/2/14	
		7 章	要約仕様の説明追記	2008/2/14	
1.11	評価指摘事項の反映	1 章	TOE ソフトウェア構成への追記	2008/2/22	日本電気株式会社
		6 章	SFR の不要な記述の削除	2008/2/22	
		7 章	要約仕様の説明を見直し	2008/2/22	
1.12	評価指摘事項の反映	1 章	TOE ガイダンスの表記修正	2008/3/7	日本電気株式会社
		6 章	SFR の不要な記述の削除	2008/3/7	
			要件根拠の修正	2008/3/7	
		7 章	SFR の見直しに伴う修正	2008/3/7	
1.13	評価指摘事項の反映	4 章 6～7 章	利用者の表記修正	2008/3/31	日本電気株式会社
		6 章	保証要件の表記修正	2008/3/31	
		7 章	ワンタイム URL の説明を見直し	2008/3/31	
1.14	評価指摘事項の反映	1 章	セキュリティ機能の表記修正	2008/4/3	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 2006 Version 3.1 Revision 1 CCMB-2006-09-002
・Common Criteria for Information Technology Security Evaluation Part3：
Security assurance components September 2006 Version 3.1 Revision 1 CCMB-2006-09-003
・Common Methodology for Information Technology Security Evaluation：
Evaluation Methodology September 2006 Version 3.1 Revision 1 CCMB-2006-09-004
・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 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
・情報技術セキュリティ評価のための共通方法
評価方法 2006 年 9 月 バージョン 3.1 改定第 1 版 CCMB-2006-09-004
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

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、以下の表 1 に示す。

表 1 用語集

用語・略語	定義内容
.NET Framework	Microsoft 社のアプリケーションの開発、実行環境
ActiveX Control	Microsoft 社の Internet Explorer を拡張するためのソフトウェア
DBMS	Database Management System データベースを管理するソフトウェア
DMZ	DeMilitarized Zone 「非武装地帯」。インターネットなどのネットワークと、社内のネットワークなどからも隔離された区域
GB	Giga Bytes ギガバイト 情報の大きさを表す単位
Internet Explorer	Microsoft 社の Web ページを閲覧するためのアプリケーションソフト
Internet Information Server	Microsoft 社のインターネットサーバソフトウェア
NEC	日本電気株式会社
NEC グループ	NEC を含む、NEC に関連する会社の総称
OS	Operating System 入出力機能やメモリの管理など、共通して利用される基本機能を提供するソフトウェア
PIN	Personal Identification Number 個人を識別する暗証番号
RAID1	Redundant Arrays of Inexpensive Disks 1 複数台のハードディスクに、同時に同じ内容を書き込む技術
SSL	Secure Socket Layer Netscape Communications 社が開発した、インターネット上で情報を暗号化して送受信する通信規約
インターネット	国際的に相互接続されているネットワーク
イントラネット	企業内などの限定した施設内のネットワーク
エリア	業務データを管理する最上位の単位。エリアは複数作成が可能
エリア利用者	特定のエリア内のフォルダを利用する許可を得ている人物(NEC グループ社員、構内作業者、顧客)
ストレージサーバ	データやプログラムを記憶する外部記憶装置
ストレージシステム	ストレージを管理するためのソフトウェア

用語･略語	定義内容
セキュリティパッチ	OS に保安上の弱点が発覚したときに配布される修正プログラム
データベースサーバ	DBMS が稼動するサーバ
ファイアウォール	ネットワークから不正侵入、不正アクセスを防ぐシステム
フォルダ	エリア内に業務データを保管するための単位。フォルダは複数作成が可能
ユーザ ID	ユーザの識別コード
ワンタイム URL	一定時間、利用可能な URL。フォルダに対する宛先となる。ワンタイム URL には、識別情報を含む。
ワンタイム URL 有効期間	ワンタイム URL を利用することができる期間
業務データ	社内利用者同士、社内利用者と顧客間で、取り扱う業務に関する、文書データ
顧客	NEC のイントラネットの利用が許可されていない取引先の会社社員
構内作業者	NEC のイントラネットの利用を許可された協力会社社員
社外用 Web サーバ	NEC グループ セキュア情報交換サイト 社外 Web サーバ
社外利用者クライアント	インターネット上から TOE を利用する、顧客のクライアント端末
社内認証サーバ	社内認証サービスが稼動するサーバ
社内認証サービス	社内利用者のユーザ ID、パスワードを一元管理し、NEC グループの各種システムに認証情報を提供するサービス
社内用 Web サーバ	NEC グループ セキュア情報交換サイト 社内 Web サーバ
社内利用者	NEC グループ社員と構内作業者
社内利用者クライアント	NEC イントラネット上で TOE を利用する、社内利用者のクライアント端末

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: NEC グループ セキュア情報交換サイト バージョン 1.0 セキュリティターゲット
ST バージョン: 1.14
ST 発行日: 2008 年 4 月 3 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: NEC グループ セキュア情報交換サイト
TOE バージョン: 1.0

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、及び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、業務データのセキュアな交換を実現するための業務ソフトウェアシステムである。

1.3.2. TOE の使用方法、及び主要なセキュリティ機能

本 TOE は、社内利用者と顧客間で、業務データの交換における誤配信、情報漏洩を防止するためのサービスを提供している業務データ交換システムである。
TOE の使用方法は、まず NEC グループ社員がエリアを作成し、作成したエリア内にフォルダを作成する。作成したフォルダ内に、社内利用者や顧客が業務データをアップロードする。アップロードされた業務データは、社内利用者や顧客がダウンロードして使用する。
サービス機能として、業務データのアップロード機能、ダウンロード機能、エリアメンテナンス機能、利用者メンテナンス機能、個人設定機能、運用管理を行う機能を提供している。
セキュリティ機能として、TOE で交換する業務データに対して、不正アクセスや誤配信、情報漏洩の防止を行う。また、監査記録の採取を行う。
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
本 TOE の利用者に対する識別と認証を行う機能
アクセス制御機能
本 TOE の利用者役割に基づいて、業務データへのアクセス制御を行う機能
監査機能
本 TOE の監査証跡を生成、参照を行う機能
暗号機能
本 TOE と利用者との間の通信データの暗号化、復号を行う機能

1.3.3. 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

表 2 に、TOE の動作環境としてのハードウェア構成を示す。TOE は、表 2 を満たす動作環境で、正しく確実に動作する。

表 2 ハードウェア構成

端末･装置名	種別	説明
ストレージサーバ		
本体	ベンダ名	NEC
	製品名	iStorage NS460
	型名	NF8100-145A
	CPU	デュアルコア Intel Xeon プロセッサ 3GHz
	メモリ	3GB(2GB+1GB)
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(標準)
	増設ディスク	物理容量 2100GB(300GB×7)RAID5
社内用 Web サーバ		
本体	ベンダ名	NEC
	製品名	Express5800/120Ri-2 (XD2/3G(4))
	型名	N8100-1318
	CPU	デュアルコア Intel Xeon プロセッサ 3GHz × 2CPU
	メモリ	4GB(2GB×2)
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(標準)
社外用 Web サーバ		
本体	ベンダ名	NEC
	製品名	Express5800/120Ri-2 (XD2/3G(4))
	型名	N8100-1318
	CPU	デュアルコア Intel Xeon プロセッサ 3GHz × 2CPU
	メモリ	4GB(2GB×2)
	HDD	73GB×2(15000rpm, RAID1)
	LAN	1000BASE-T×2(標準)
データベースサーバ		
本体	ベンダ名	NEC
	製品名	Express5800/140Re-4(XMPD/3.40G(16))
	型名	N8100-1276
	CPU	デュアルコア Intel Xeon プロセッサ 3.40GHz×4
	メモリ	4GB(2GB×2)
	LAN	1000BASE-T×2(標準)
	外部ストレージ	1148GB
社内利用者クライアント		

端末･装置名		種別	説明
	本体	表 3 ソフトウェア構成の社内利用者クライアントで定義されたOSが動作可能な本体	
社外利用者クライアント			
	本体	表 3 ソフトウェア構成の社外利用者クライアントで定義されたOSが動作可能な本体	

1.3.3.2. 必要なソフトウェア

表 3 に、TOE の動作環境としてのソフトウェア構成を示す。TOE は表 3 に識別されたソフトウェア構成により、正しく動作する

表 3 ソフトウェア構成

端末名			
	ベンダ名	製品名	種別
ストレージサーバ			
	Microsoft	Windows Storage Server 2003 R2	OS
社内用 Web サーバ			
	Microsoft	Windows Server 2003 R2 _Standard Edition	OS
社外用 Web サーバ			
	Microsoft	Windows Server 2003 R2 _Standard Edition	OS
データベースサーバ			
	Microsoft	Windows Server 2003 R2_Standard Edition	OS
	Oracle	Oracle Database 10g Standard Edition 1 Processor	DBMS
社内利用者クライアント			
	Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS
社外利用者クライアント			
	Microsoft	Windows 2000 Professional SP4, Windows XP Professional SP2, Windows Vista Business, Windows Vista Enterprise	OS

1.4. TOE 記述

本節では、システム概要、TOE 関連の役割定義、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. システム概要

従来、業務データの交換手段として、メールの利用が一般的であるが、この場合、誤配信や、情報漏洩の危険性が少なくない。本 TOE は、社内利用者と顧客との間で取り交わす業務データに対して、その交換可能な社内利用者を限定し、顧客に PIN を別送することで、誤配信を防止し、交換するデータを暗号化することで、情報漏洩の防止を行うシステムである。
TOE では、業務データの交換を行うために、その格納場所となるエリア、及びフォルダを作成する。

エリアは、配下に複数のフォルダ構造を持つ、業務データを管理するための最上位の単位で、複数、作成することができる。
フォルダは、各エリア内に複数、作成することができる、業務データを保管するための単位となる。
エリアの作成者は、作成したエリア内のフォルダ単位に、そのフォルダを使用する社内利用者、顧客を登録する。
フォルダに登録された社内利用者、顧客は、そのフォルダに対してのみ、業務データをアップロードすることができる。この時、業務データを格納するフォルダに対して、ダウンロードを行える社内利用者、顧客を指定しておく。
TOE は、ダウンロードを行う社内利用者、顧客に対して、ダウンロードを行うワンタイム URL をメールで通知する。
ワンタイム URL を利用するときに、社内利用者は、TOE 外の社内認証サービスによる認証を行う。また、顧客は、PIN による認証を行う。なお、ワンタイム URL を利用するときに、必要となる PIN は、顧客に対して、安全な方法で通知する。
これにより、フォルダ内の業務データに対して、ダウンロードを指定された社内利用者、顧客のみが、ダウンロードを行える。

1.4.2. TOE 関連の役割定義

TOE における利用者の役割は、以下のとおりである。
TOE に関連する利用者は、運用責任者、データベース管理者、ストレージ管理者に分類され、付与された権限範囲の業務を行う。
TOE が提供するサービスの利用者は、システム管理者、監査者、NEC グループ社員、構内作業者、顧客である。
NEC グループ社員の利用者役割は、NEC グループ社員、エリア利用者(管理者)、エリア利用者(社員、構内作業)のいずれかに分類される。
構内作業者の利用者役割は、構内作業者、エリア利用者(社員、構内作業者)のいずれかに分類される。
顧客の利用者役割は、エリア利用者(顧客)となる。
いずれの利用者についても、利用者役割に付与された権限範囲の業務を行う。
NEC グループ社員、構内作業者、エリア利用者(管理者)、エリア利用者(社員、構内作業者)、エリア利用者(顧客)について、TOE の利用役割と権限を以下の表 4 に示す。

表 4 TOE 利用者の役割と権限の関連図

		NEC グループ社員	構内作業者	エリア利用者(管理者)	エリア利用者(社員、構内作業者)	エリア利用者(顧客)
運用準備フェーズ	エリアの作成	○	―			
	作成エリアの参照、更新、削除	○	―			
運用フェーズ	フォルダの作成、更新、削除			○	―	―
	ファルダを利用する社内利用者、顧客の登録、更新、削除			○	―	―
	フォルダ内のファイルの削除			○	―	―
	エリア利用者(管理者)権限の付与			○	―	―
利用フェーズ	利用できるエリア一覧の参照	○	○			
	フォルダの利用者に登録されたファルダ一覧の参照			○	○	―
	フォルダの利用者に登録されたファルダの参照			○	○	○
	アップロード			○	○	○
	自身がアップロードしたファイルの削除			○	○	○
	アップロード依頼			○	○	―
	ダウンロード			○	○	○
	個人メールアドレス設定			○	○	―

TOE に関連する利用者は、TOE の利用許可はなく、以下の業務を行う。

□運用責任者

TOE の運用管理全般に責任を持つ人物

・システム管理者、データベース管理者、ストレージ管理者、及び監査者の任命

・システム管理者、データベース管理者、ストレージ管理者、及び監査者に対して、システムの運用に関する規則を遵守させ、情報セキュリティ教育を実施

・TOE の利用者に対して、セキュリティ意識の向上、及び維持

□データベース管理者

TOE 外の DBMS 管理を行う人物

・TOE の初期設定前の準備段階で、DBMS 設定

□ストレージ管理者

TOE 外のストレージシステムの管理を行う人物

・TOE の初期設定前の準備段階で、ストレージシステムの設定

TOE の利用者は、以下の権限を有し、TOE 内の業務を行う。

□NEC グループ社員

社内利用者クライアントより、エリアの作成、更新、削除の操作を行う人物

・エリアの作成、更新、削除

・エリア、フォルダの選択による参照

□構内作業者

社内利用者クライアントより、エリア、フォルダの選択操作を行う人物

・エリア、フォルダの選択による参照

□エリア利用者(管理者)

社内利用者クライアントより、業務データに関連する操作と管理を行う人物

・NEC グループ社員がエリアを作成すると、そのエリア内におけるエリア利用者(管理者)となる

・フォルダの作成、更新、削除

・フォルダの利用者となる社内作業者、及び顧客の登録、更新、削除

・エリア利用者(社員、構内作業者)の操作権限を付与

・フォルダの利用者として登録された NEC グループ社員に対しては、エリア利用者(管理者)権限を付与することができる

□エリア利用者(社員、構内作業者)

社内利用者クライアントより、業務データに関連する操作を行う人物

・エリア利用者(管理者)により、フォルダの利用者として登録された NEC グループ社員、構内作業者は、そのフォルダ内においてエリア利用者(社員、構内作業者)となる

・構内作業者の場合は、エリア利用者(管理者)になることはできない

□エリア利用者(顧客)

社外利用者クライアントより、業務データに関連する操作を行う人物

・エリア利用者(管理者)により、フォルダの利用者として登録された顧客は、そのフォルダ内においてエリア利用者(顧客)となる

・エリア利用者(管理者)になることはできない

□システム管理者

社内用 Web サーバ、社外用 Web サーバより、TOE の運用管理を行う人物

・TOE の初期設定の業務

・TOE の起動と停止

□監査者

社内用 Web サーバより、TOE の監査証跡の参照を行う人物

・TOE の監査の実施

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、図 1 に示す。

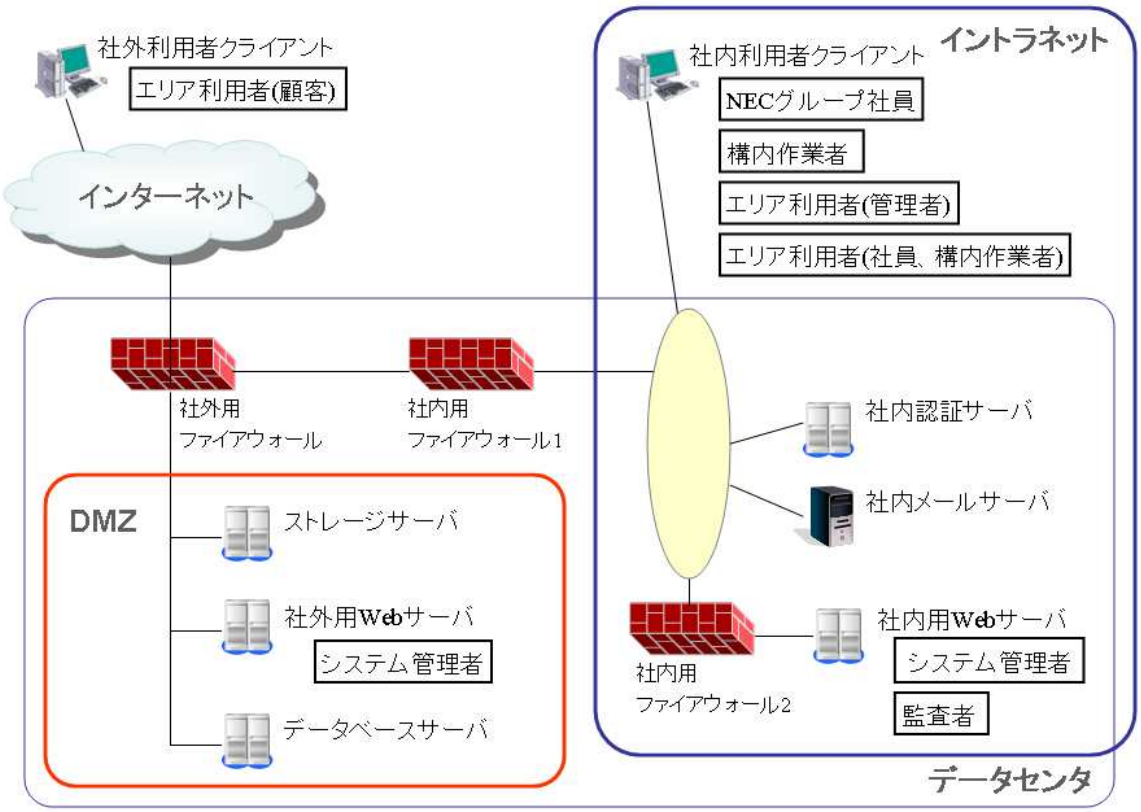

図 1 TOE の動作環境

⑴ **物理的配置、及びネットワーク**

TOE を利用する社内のクライアントは、イントラネット上にある社内利用者クライアントである。また、TOE を利用する社外のクライアントは、インターネット上にある社外利用者クライアントである。

TOE を利用するための社内利用者クライアントは、NEC グループ社員、構内作業者のみが入館できる、入退出が管理された建物内で利用される。

TOE を設置するデータセンタには、社内用 Web サーバ、社内認証サーバ、社内メールサーバ、社内用ファイアウォール 1、社内用ファイアウォール 2、社外用ファイアウォールが配置される。データセンタ内に DMZ が置かれ、社外用 Web サーバ、ストレージサーバ、データベースサーバが配置される。データセンタは、入退室が管理され、データセンタへの入室は、許可を受けた者に限定し、入室の行動は監視されている。

DMZ は、社外用ファイアウォールにより保護され、SSL 通信を利用することで、安全な通信状態を確保している。

また、社内用 Web サーバ、社内認証サーバ、社内メールサーバについては、社内用ファイアウォール 1 により保護され、さらに社内用 Web サーバは社内用ファイアウォール 2 により必要なアクセスに限定され、SSL 通信を利用することで、安全な通信状態を確保している。

⑵ **社外用 Web サーバ**

社外用 Web サーバへのアクセスは、インターネット、社外用ファイアウォールを経由して社外利用者クライアントからの業務データに関する要求を受け付け、DMZ 上のデータベースサーバ、ストレージサーバへのアクセスを行う。

また、システム管理者は、社外用 Web サーバをローカルに使用してアクセスを行う。

⑶ **社内用 Web サーバ**

社内用 Web サーバへのアクセスは、イントラネット、社内用ファイアウォール 2 を経由して社内利用者クライアントからの認証要求を受け付け、社内認証サーバへのアクセスを行う。

社内用 Web サーバは、イントラネット、社内用ファイアウォール 2 を経由して社内利用者クライアントからの業務データに関する要求を受け付け、DMZ 上のデータベースサーバ、ストレージサーバへのアクセスを行う。
また、システム管理者、及び監査者は、社内用 Web サーバをローカルに使用してアクセスを行う。

⑷ ストレージサーバ
ストレージサーバへのアクセスは、社外用 Web サーバ、社内用 Web サーバから行う。ストレージサーバには、社内利用者、顧客がアップロードした業務データを格納している。

⑸ データベースサーバ
データベースサーバへのアクセスは、社外用 Web サーバ、社内用 Web サーバから行う。データベースサーバには、社内利用者、顧客がアップロードした業務データに関する情報を格納している。

⑹ 社外利用者クライアント
社外利用者クライアントは、顧客のみ利用でき、インターネット、社外用ファイアウォールを経由して、社外用 Web サーバへのアクセスを行う。

⑺ 社内利用者クライアント
社内利用者クライアントは、社内利用者のみが利用でき、イントラネット、社内用ファイアウォール 2 を経由して社内用 Web サーバへのアクセスを行う。

⑻ 社外用ファイアウォール
インターネットからデータセンタ内の DMZ までのネットワークに流れる通信を制御している。
ストレージサーバ、データベース、社外用 Web サーバへのアクセスに対しては、パケットを監視して、決められたルールに基づきアクセスの制限を行っている。

⑼ 社内用ファイアウォール 1
イントラネットからデータセンタ内の DMZ、社内用 Web サーバへまでのネットワークに流れる通信を制御している。

⑽ 社内用ファイアウォール 2
社内用 Web サーバへのアクセスに対しては、パケットを監視し、決められたルールに基づきアクセスの制限を行っている。

⑾ 社内認証サーバ
社内認証サーバは、データセンタ内のネットワークに接続され、社内認証サービスを提供している。
社内認証サーバは、社内用 Web サーバからアクセスされる。

⑿ 社内メールサーバ
社内メールサーバは、データセンタ内のネットワークに接続され、電子メールの配送をするための機能を提供している。
社内メールサーバは、社内用 Web サーバからアクセスされる。

1.4.3.2. TOE の物理的範囲(コンポーネント)

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

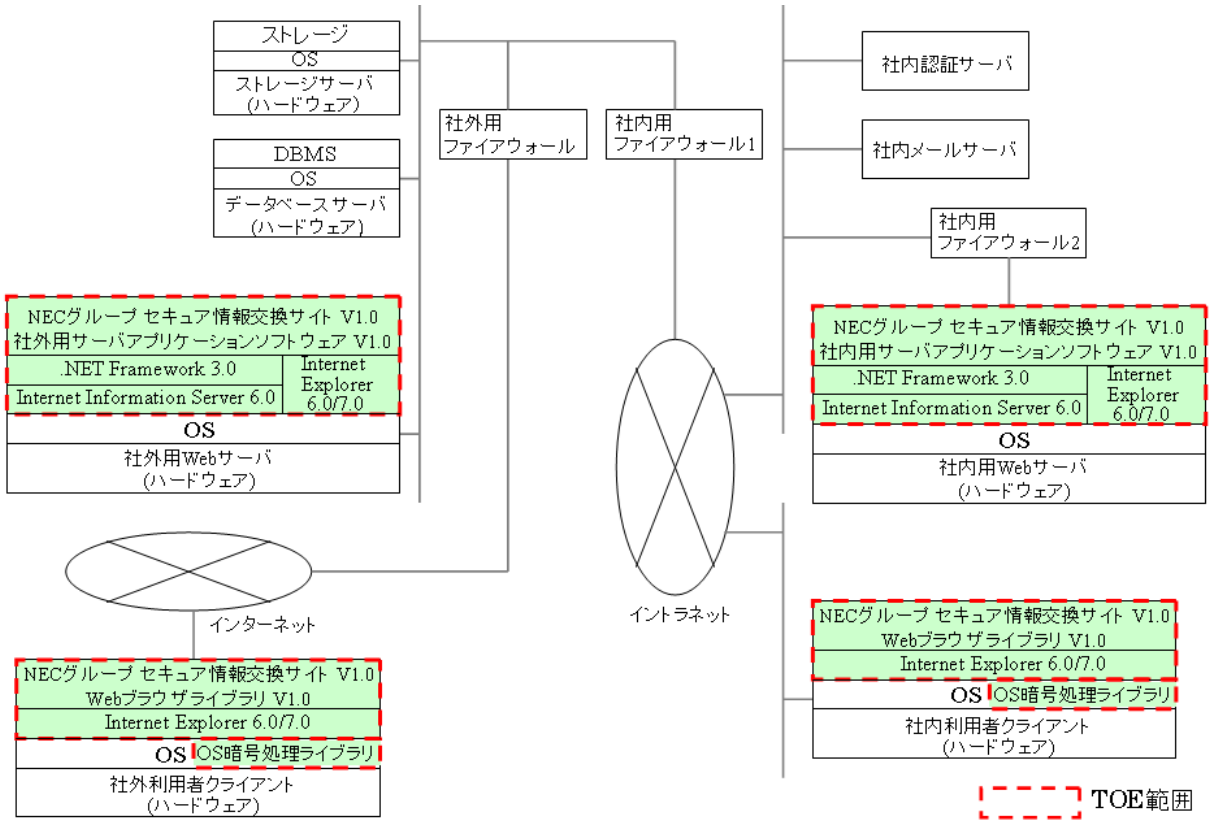

図 2 TOE の物理的範囲(コンポーネント)

TOE のソフトウェア構成を以下に示す。TOE は表 5 に識別されたソフトウェア構成によって、正しく確実に動作する。

表 5 TOE のソフトウェア構成

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

端末名			
	ベンダ名	名称	種別
社外利用者クライアント			
	NEC	NEC グループ セキュア情報交換サイト V1.0 Web ブラウザライブラリ V1.0	ActiveX Control
	Microsoft	Internet Explorer 6.0/Internet Explorer 7.0	Web ブラウザ
	Microsoft	OS 暗号処理ライブラリ	OS ライブラリ

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。

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

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

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

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。

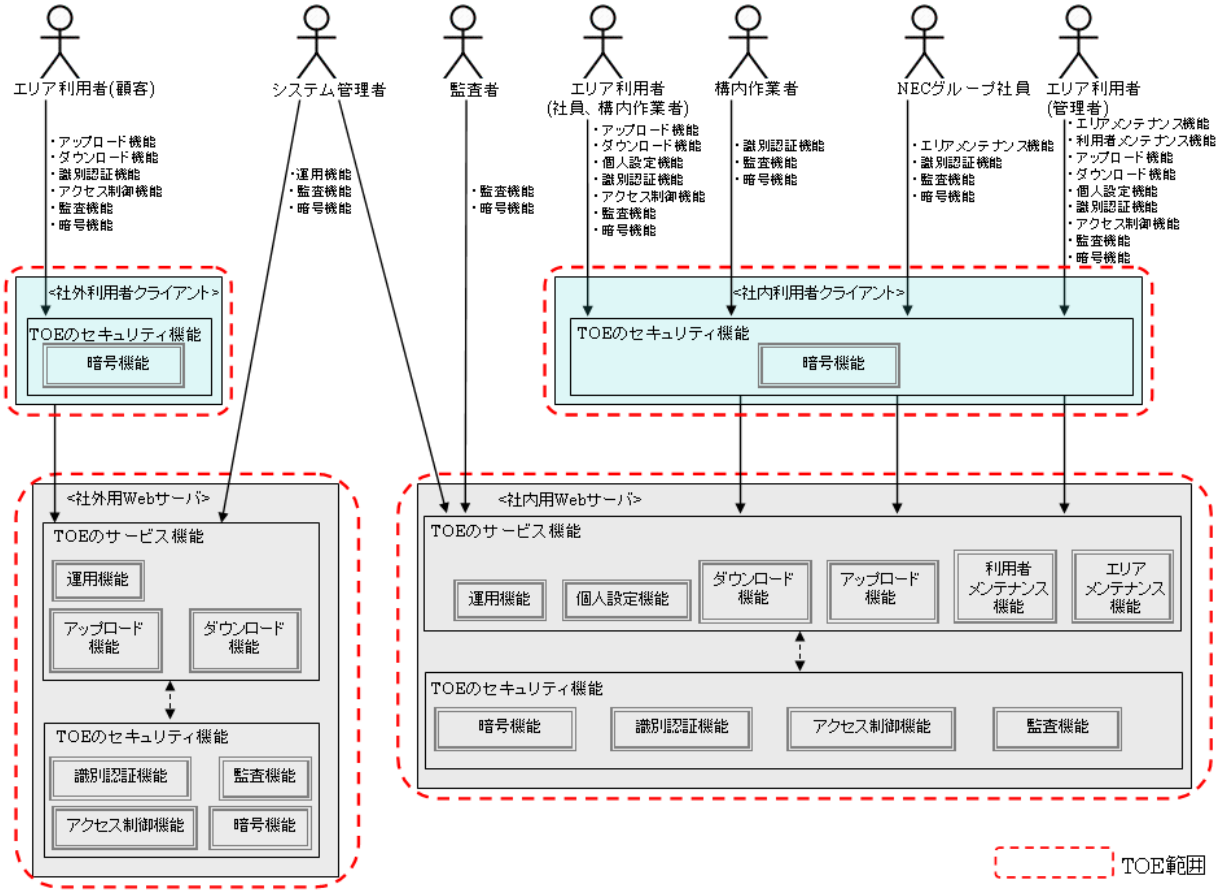

図 3 TOE の論理的構成

TOE の論理的構成は、TOE 提供機能について、サービス機能とセキュリティ機能に分けて、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の詳細を以下に記述する。

【エリアメンテナンス機能】

エリアメンテナンス機能について、以下の図 4 に示す。

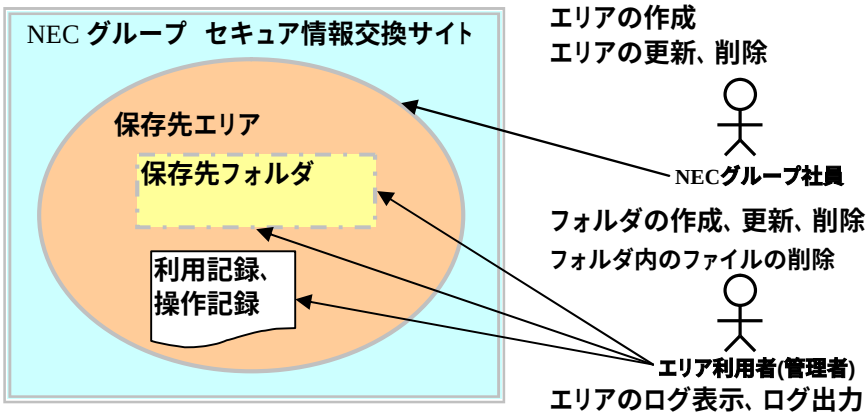

図 4 エリアメンテナンス

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

エリアの更新では、エリアの名称の変更を行う。フォルダの更新では、フォルダ名称の更新を行う。

【利用者メンテナンス機能】

利用者メンテナンス機能について、図 5 に示す。

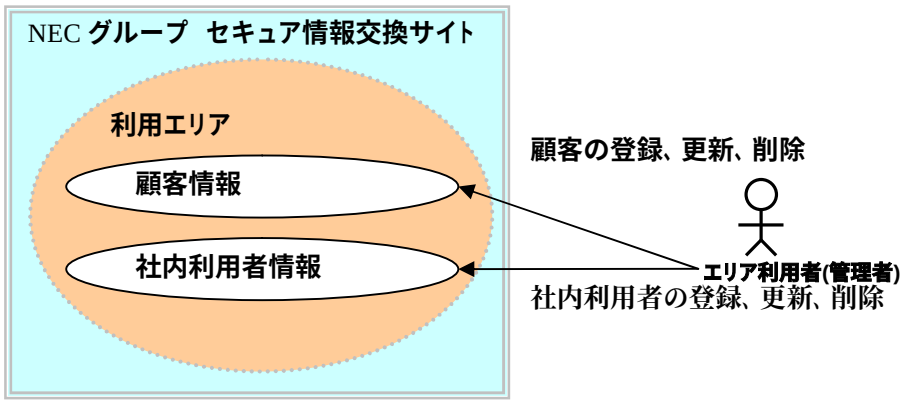

図 5 利用者メンテナンス

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

社内利用者、顧客の更新では、社内利用者情報、顧客の情報の更新を行う。

【アップロード依頼機能】

アップロード依頼機能について、図 6 に示す。

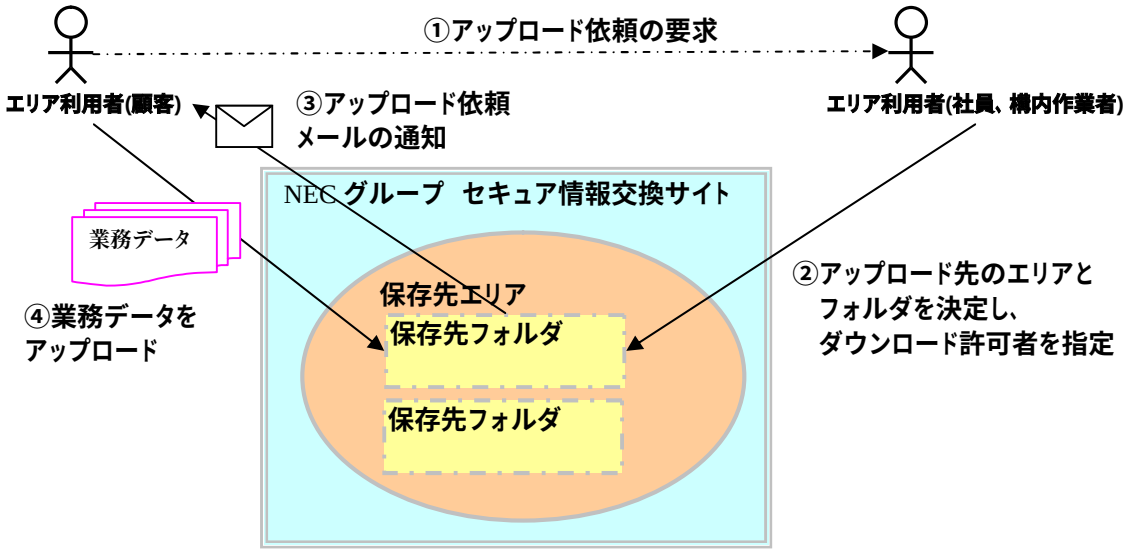

図 6 アップロード依頼

アップロード依頼機能は、エリア利用者(顧客)に対して、アップロードが行えるようにする機能である。

【アップロード機能】
アップロード機能について、図 7 に示す。

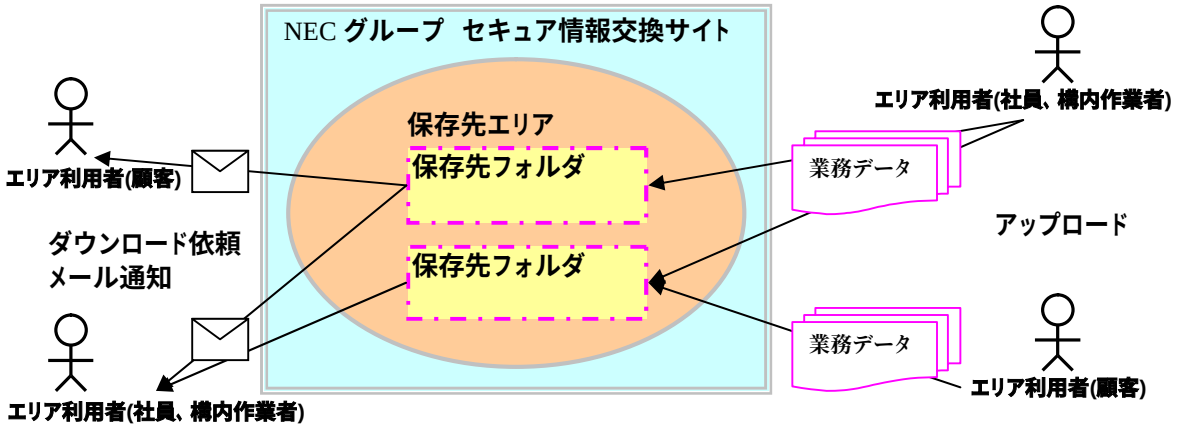

図 7 アップロード

アップロード機能は、業務データのアップロードを行う機能である。

【ダウンロード機能】
ダウンロード機能について、図 8 に示す。

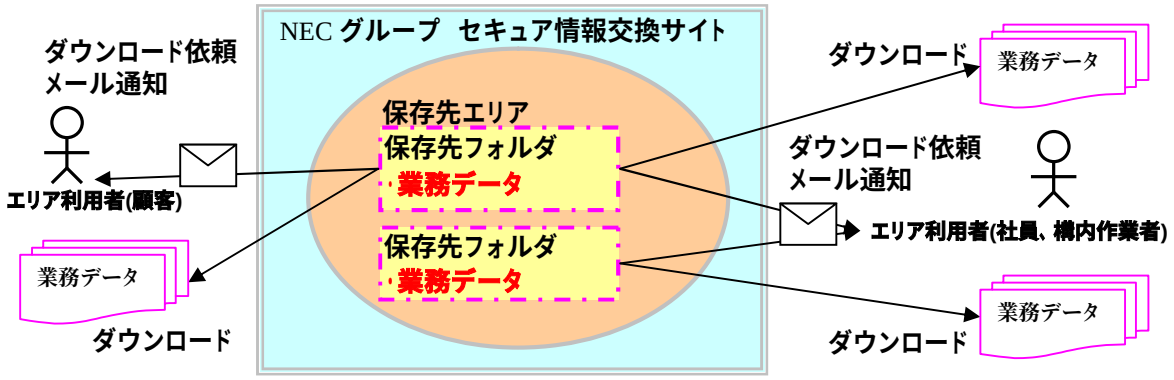

図 8 ダウンロード

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

【個人設定機能】
個人設定機能について、以下の図 9 に示す。

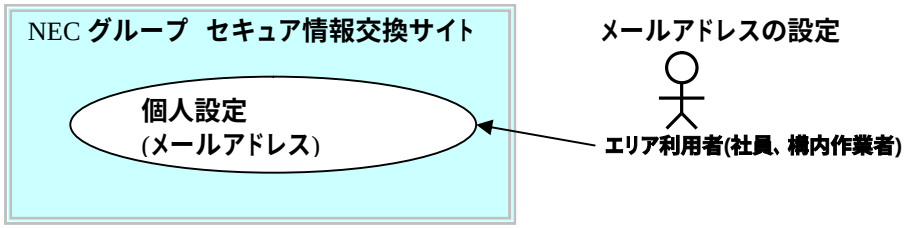

図 9 個人設定

個人設定機能は、メールアドレスの変更を行う機能である。

【運用機能】
運用機能について、以下の図 10 に示す。

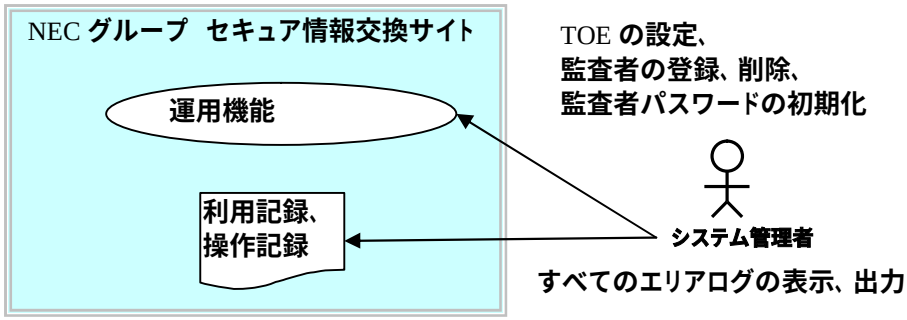

図 10 運用

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

1.4.4.2. 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を以下に記述する。

・TOE セキュリティ機能

【識別認証機能】

TOE は、TOE へのアクセスに対する識別認証機能を提供する。

□エリア利用者(顧客)

・ワンタイム URL による識別、PIN による認証が成功しなければならない

・同一のワンタイム URL に対する PIN が異なる場合は、ワンタイム URL 毎に PIN の誤り回数をカウントするとともに、ワンタイム URL を失効とする。

□エリア利用者(社員、構内作業者)

・ワンタイム URL による識別が成功しなければならない。

・ワンタイム URL 経由で TOE にアクセスし、社内認証サービスの認証に失敗した場合は、誤り回数をカウントするとともに、ワンタイム URL を失効とする。

□NEC グループ社員、構内作業者

・ユーザ ID による識別が成功しなければならない。

□システム管理者

・URL による識別が成功しなければならない。

□監査者

・URL による識別が成功しなければならない。

【監査機能】

TOE は、監査対象となる事象が発生した場合、監査記録を生成する。

監査者は、監査機能を使用して、監査記録の参照、及び検索を行う。

【アクセス制御機能】

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

【暗号機能】

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

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

CC 適合主張は、以下とおりである。
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 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 適合性: CC パート 2 拡張
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

この ST のパッケージ適合主張は、以下のとおりである。
・パッケージ: EAL1 追加
・追加コンポーネント:ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1

2.4. 適合根拠

この ST は PP 適合を主張していないので、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、及び脅威について以下に記述する。

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
業務データ	エリア利用者(管理者)、エリア利用者(社員、構内作業者)、エリア利用者(顧客)が、アップロードしたデータ
アップロードエリア情報	業務データのアップロード先となるエリア内のフォルダ情報、アップロード依頼を行った顧客情報、アップロードを行った利用者情報、ダウンロードを許可した利用者情報
エリア利用者情報	エリア利用者(管理者)が登録した、エリア利用者の情報(社員･構内作業者･顧客)

3.1.2. 脅威

TOE に対する脅威を以下に記述する。

T.SPOOFING(なりすまし)
インターネット上からアクセスする専門知識を持たない悪意のある第三者や、NEC のイントラネット上からアクセスする TOE の利用者が、TOE の正当な利用者になりすまして、業務データを破壊、暴露するかもしれない。

T.ILLEGAL_ACCESS(不正なアクセス)
TOE の正当な利用者である、NEC グループ社員、構内作業者、エリア利用者(管理者)、エリア利用者(社員、構内作業者)、エリア利用者(顧客)が、その利用者役割に対し、許可をしていない以下の操作を行うことで、業務データ、アップロードエリア情報、エリア利用者情報を破壊、暴露するかもしれない。

- ･NEC グループ社員ではない TOE 利用者による、エリアの作成、更新、削除
- ･エリア利用者(管理者)ではない TOE 利用者による、フォルダの作成、更新、削除
- ･エリア利用者(管理者)ではない TOE 利用者による、フォルダ内への、利用者(NEC グループ社員、構内作業者、顧客)の登録、更新、削除
- ･エリア利用者(社員、構内作業者)ではなく、エリア利用者(顧客)でもない TOE 利用者による、業務データのダウンロード、アップロード、削除

T. LISTEN-IN_NW_DATA (ネットワークデータ盗聴)
専門知識を持たない悪意のある第三者が、Web サーバとネットワーク上でやり取りされる業務データを盗聴したり、改ざんしたりすることで、業務データを暴露、破壊、改ざんするかもしれない。

T.MISDELIVERY(誤送信)

TOE の正当な利用者が、誤って違う顧客に TOE の URL の送信を行うことで、業務データを暴露するかもしれない。

3.2. 組織のセキュリティ方針

本節では、TOE、及び 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。

P. ADMIN_IDENTIFY (管理者識別)
TOE を利用するシステム管理者、監査者について、TOE における操作の記録を残すため、TOE による識別を義務付ける。

P. AUDIT_LOG (監査記録)
TOE が生成する監査記録は、TOE の保護資産に対する不正操作の追跡を行うため、監査者のみが参照可能とする制限を行う。

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. DATACENTER (データセンタ)
社内用 Web サーバ、社外用 Web サーバ、データベースサーバ、ストレージサーバ、社内認証サーバ、社内メールサーバは、入退出管理を実施した許可のない者の入室を禁止し、入室者の行動を監視しているデータセンタに設置する。

A.NETWORK(ネットワーク)
社内用 Web サーバは、適切に設定した社内用ファイアウォール 2 によってイントラネットからのアクセスを制限されている。
社外用 Web サーバは、適切に設定した社外用ファイアウォールによってインターネットからのアクセスを制限されている。

A.SYSTEM_ADMIN (システム管理者の利用制限)
システム管理者の操作は、社内用 Web サーバ上、及び社外用 Web サーバ上のコンソールのみで行う。

A.AUDIT_ADMIN (監査者の利用制限)
監査者の操作は、社内用 Web サーバ上のコンソールのみで行う。

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 の運用責任者、システム管理者、監査者、ストレージ管理者、データベース管理者は、それぞれの役割に付与した行為のみを行い、悪意のある行為を行わない。

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はない。

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、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(顧客の識別認証)
TOE は、エリア利用者(顧客)の TOE 利用には、ワンタイム URL と、対応する PIN を生成する。エリア利用者(顧客)が TOE を利用するとき、ワンタイム URL による識別と PIN による認証を行うことを保証し、指定された回数以内に識別認証に成功したエリア利用者(顧客)のみ、TOE の利用を許可しなければならない。

O.IDENTIFY (社内利用者の識別)
TOE は、NEC グループ社員、構内作業者が TOE を利用するとき、必ず識別することを保証する。

O.ADMIN_IDENTIFY (管理者の識別)
TOE は、システム管理者、監査者が TOE を利用するとき、必ず識別することを保証する。

O.ACCESS_CONTROL(アクセス制御)
TOE は、TOE の利用者に対して利用者役割種別に応じた、以下に示す必要機能のみを提供することにより、利用者データへの不正なアクセスを防止しなければならない。

- NEC グループ社員のみ、エリアを作成、更新、削除できる。
  (作成エリア内では、NEC グループ社員が、そのエリアのエリア利用者(管理者)となる)
- エリア利用者(管理者)のみ、作成したエリア内に、フォルダを作成、更新、削除できる。
- エリア利用者(管理者)のみ、作成したフォルダ内に、利用者(NEC グループ社員、構内作業者、顧客)を登録、更新、削除できる。
  (フォルダに登録した利用者が、エリア利用者(社員、構内作業者)、エリア利用者(顧客)となる)
- エリア利用者(社員、構内作業者)、エリア利用者(顧客)は、エリア利用者(管理者)が指定したフォルダでのみ、業務データをダウンロード、アップロード、削除できる。

O.AUDIT(監査)
TOE は、アクセス制御機能、及び識別認証機能に関連するセキュリティ関連事象を監査記録として、管理しなければならない。なお、暗号機能に関しては、SSL 通信に対する攻撃を想定しないため、監査の対象外とする。また、監査記録の読出しを監査者のみに限定しなければならない。また、監査記録は、事象の日付・時刻、事象箇所、及び事象の結果を含まなければならない。

O.ENCRYPT(暗号化)
TOE は、利用者と TOE 間の通信方式を SSL 通信で行い、利用者データを秘匿し、改ざん、暴露を防止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。

OE.TRUSTED_ROLE(信頼される役割)
運用責任者は、システム管理者、ストレージ管理者、データベース管理者、監査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、各役割についての重要性を理解させ、悪意を持った行為を行わないように、管理を実施しなければならない。

OE.NETWORK(ネットワーク環境)
社内用 Web サーバ、社外用 Web サーバが接続するネットワークは、適切に設定したファイアウォールによって外部から隔離しなければならない。

OE.ADMIN_TRAINING(管理者の教育、訓練)
データベース管理者、ストレージ管理者、システム管理者、監査者は、TOE の資産、及び TOE の安全管理に関する教育･訓練を受けなければならない。また、監査者は、TOE が生成した監査記録の確認方法、及び、対処方法について理解していなければならない。

OE.DATACENTER(データセンタ環境)
データセンタへの入退出においては、入退室管理が行われ、許可された運用責任者、監査者、システム管理者、ストレージ管理者、データベース管理者だけが入退室可能に制限し、入室者の行動を監視していなければならない。

OE.AUTHENTICATION(社内認証サービス)
TOE を利用する NEC グループ社員、構内作業者は、社内認証サービスによる認証を利用しなければならない。

OE.SEND_PIN(PIN の送付方法)
TOE で利用する PIN は、TOE の正当な利用者である、エリア利用者(顧客)に対し、電話や別アドレスの電子メールなどにより、TOE が送付するワンタイム URL とは別の経路で、送付しなければならない。

OE.SYSTEM_ADMIN (システム管理者の利用制限)
システム管理者による TOE の操作は、社内用 Web サーバ上、及び社外用 Web サーバ上のコンソールのみで行わなければならない。

OE.AUDIT_ADMIN (監査者の利用制限)
監査者による TOE の操作は、社内用 Web サーバ上のコンソールのみで行わなければならない。

OE.OS_TIMESTAMP (OS 環境タイムスタンプ)
TOE が稼動する OS は、高信頼のタイムスタンプを提供できなければならない。

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「×」は対応関係にあることを示している。

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

	T.SPOOFING	T.ILLEGAL_ACCESS	T.LISTEN-IN_NW_DATA	T.MISDELIVERY	P. ADMIN_IDENTIFY	P. AUDIT_LOG	A. DATACENTER	A.NETWORK	A.ADMINISTRATOR	A.SYSTEM_ADMIN	A.AUDIT_ADMIN
O.I&A	×			×							
O.IDENTIFY	×										
O.ADMIN_IDENTIFY					×						
O.AUDIT	×	×				×					
O.ACCESS_CONTROL		×									
O.ENCRYPT			×								
OE.TRUSTED_ROLE									×		
OE.NETWORK								×			
OE.ADMIN_TRAINING	×	×							×		
OE.DATACENTER							×				
OE.AUTHENTICATION	×										
OE.SEND_PIN	×			×							
OE.SYSTEM_ADMIN										×	
OE.AUDIT_ADMIN											×
OE.OS_TIMESTAMP	×	×									

表 7により、各セキュリティ対策方針は、1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、インターネット上からアクセスする高度な専門知識を持たない悪意のある第三者や、NEC のイントラネット上からアクセスする TOE の利用者によって実行される。このような者が取り得る具体的な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. 高度な専門知識を持たない悪意のある第三者による TOE へのアクセス

この攻撃は、高度な専門知識を持たない悪意のある第三者が、TOE にアクセスして業務データを操作してしまうことが考えられる。よって、O.I&A により、ワンタイム URL による識別情報の利用可能時間の制限、誤った PIN による認証の連続試行を制限することで、脅威を軽減できる。また、OE.SEND_PIN により、ワンタイム URL の連絡とは別の経路で PIN を伝達するため、インターネット上で盗聴される可能性が低くなり、脅威を軽減することができる。また、O.AUDIT、及び OE.OS_TIMESTAMP により、信頼できる時刻を含む監査記録を採取し、OE.ADMIN_TRAINING により、採取された監査記録を監査者が確認し、攻撃の可能性がみられたときに監査者が適切な処置を行うことで、脅威の緩和ができる。

b. TOE 利用者の役割を逸脱して TOE を利用

この攻撃は、TOE の利用者に付与された役割を逸脱した利用を試みるものである。よって、OE.AUTHENTICATION により、NEC グループ社員、構内作業者について社内認証サービスの認証を実施すること、及び O.IDENTIFY により利用者の役割を識別することで、脅威を軽減できる。また、O.AUDIT、及び OE.OS_TIMESTAMP により、信頼できる時刻を含む監査記録を採取し、OE.ADMIN_TRAINING により、採取された監査記録を監査者が確認し、攻撃の可能性がみられたときに監査者が適切な処置を行うことで、脅威の緩和ができる。

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.IDENTIFY、O.AUDIT、OE.ADMIN_TRAINING、OE.AUTHENTICATION、OE.OS_TIMESTAMP 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、不正アクセスの方法を示すとともに、それぞれに有効な対抗策について述べる。

a. 許可を得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で、脅威を除去できる。

また、O.AUDIT、及び OE.OS_TIMESTAMP により、信頼できる時刻を含む監査記録を採取し、OE.ADMIN_TRAINING により、採取された監査記録を監査者が確認し、攻撃の可能性がみられたときに監査者が適切な処置を行うことで、脅威の緩和ができる。

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.AUDIT、O.ACCESS_CONTROL、OE.ADMIN_TRAINING、OE.OS_TIMESTAMP である。

T.LISTEN-IN_NW_DATA (ネットワークデータ盗聴)

この脅威は、専門知識を持たない悪意のある第三者によって実行される。このような者が取り得るネットワークデータの不正利用の方法を示すとともに、それぞれに有効な対抗策について以下に述べる。

a. 社外用 Web サーバと社外利用者クライアント間、社内用 Web サーバと社内利用者クライアント間の通信データを傍受、破壊、改ざん

この攻撃は、社外用 Web サーバと社外利用者クライアント間、社内用 Web サーバと社内利用者クライアント間の通信データに対し、通信中のデータの不正取得や、破壊、改ざんされた通信データを送信することが考えられる。

よって、O.ENCRYPT により、社外用 Web サーバと社外利用者クライアント間、社内用 Web サーバと社内利用者クライアント間の通信に、SSL 通信を使用して、通信中のデータを秘匿することで、脅威を軽減できる。

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.ENCRYPT である。

T. MISDELIVERY (誤送信)

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、誤送信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. 誤った顧客への送信を実行

この脅威は、TOE に誤ったメールアドレスを登録したとき、業務データのアクセス先となる URL を、その誤ったメールアドレスに対して送信してしまうことが考えられる。

よって、O.I&A により、業務データにアクセスするためには、URL だけではなく、PIN の認証を必要とすることで、脅威を軽減できる。また、OE.SEND_PIN により、予めエリア利用者(顧客)に対し、PIN を電話や別アドレスの電子メールなどで別送しておくことで、脅威を軽減できる。

以上より、この攻撃に対抗するセキュリティ対策方針は、OE.SEND_PIN、O.I&A 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。

P. ADMIN_IDENTIFY (管理者識別)

この組織のセキュリティ方針は、TOE を利用するシステム管理者、監査者の識別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、及び監査者を識別

TOE は、システム管理者、及び監査者を識別する機能を提供する。

この方針に対応するセキュリティ対策方針は、O. ADMIN_IDENTIFY である。

以上より、O. ADMIN_IDENTIFY の達成により、P.ADMIN_IDENTIFY が実行される。

P. AUDIT_LOG (監査記録)

この組織のセキュリティ方針は、監査記録の参照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. 監査記録の参照を監査者のみに制限

監査記録に対して、監査者のみが記録内容の参照を可能とする機能を提供する。

この方針に対応するセキュリティ対策方針は、O.AUDIT である。

以上より、O.AUDIT の達成により、P.AUDIT_LOG が実行される。

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抗できることを以下で説明する。

A. DATACENTER (データセンタ)

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建物を制限

入退出管理を実施した建物内のフロアに TOE、TOE に関連するハードウェアを設置して、許可のない者の入室を禁止し、入室者の行動を監視しているデータセンタに設置する。

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.DATACENTER である。

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

A.NETWORK(ネットワーク)

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 が稼動する社内用 Web サーバへの接続は、適切に設定した社内用ファイアウォール 2 を用いて、必要な通信のみに制限する。
インターネットから、社外用 Web サーバへの接続は、適切に設定した社外用ファイアウォールを用いて必要な通信のみに制限する。
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.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.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. 教育･訓練の受講
データベース管理者、ストレージ管理者、システム管理者、監査者は、TOE の資産、及び TOE の安全管理に関する教育･訓練を受講するものとする。
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.ADMIN_TRAINING である。
b. 厳重な人選と適切な管理
運用責任者は、システム管理者、ストレージ管理者、データベース管理者、監査者の役割に適した者を厳重に人選し、それぞれの役割を理解させ、悪意を持った行為を行わないように管理を行う。
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。
以上の a、b に応じることが、A.ADMINISTRATOR に応じることである。したがって、
OE. ADMIN_TRAINING、OE.TRUSTED_ROLE、の達成により、A. ADMINISTRATOR が実行される。

A.SYSTEM_ADMIN (システム管理者の利用制限)
この前提条件は、システム管理者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. システム管理者の利用制限
システム管理者の TOE 利用は、社内用 Web サーバ上、及び社外用 Web サーバ上のコンソールのみに制限する。
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。
以上の a の達成により、A.SYSTEM_ADNIN が実行される。

A.AUDIT_ADMIN (監査者の利用制限)
この前提条件は、監査者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. 監査者の利用制限
監査者の TOE 利用は、社内用 Web 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.AUDIT_ADMIN である。
以上の a の達成により、A.AUDIT_ADMIN が実行される。

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する。

5.1. 拡張機能コンポーネント

CC パート 2 に定義された、セキュリティ機能コンポーネントの拡張コンポーネントとして、FTP_ITC_EX「TOE 内高信頼チャネル」を定義する。拡張コンポーネントを定義した理由を、以下に説明する。

[拡張の必要性]

・TOE の異なるパーツ間のデータ転送における保護(高信頼チャネル)に対する要件を規定する必要があるが、CC パート 2 のセキュリティ機能要件には、本要求を正確に満たす要件が存在していない。

[拡張機能コンポーネントに適用したクラスの理由]

・高信頼通信に関する要求事項であるため、既存の FTP クラスを適用した。

[拡張機能コンポーネントに適用したファミリの理由]

・新規に規定する要求事項は、TOE の異なるパーツ間における高信頼チャネルに関する規定であるため、FTP クラス内の既存ファミリである、TSF と高信頼 IT 製品(FTP_ITC)、TSF と利用者(FTP_TRP)に当てはまらない。このため、ITC_EX を新しいファミリとして識別し、定義した。

5.1.1. TOE 内高信頼チャネル(FTP_ITC_EX)

ファミリのふるまい

このファミリは、セキュリティ上の重要な操作のために、TOE の異なるパーツ間に高信頼チャネルを生成するための要件を定義する。このファミリは、TOE の異なるパーツ間で利用者あるいは TSF データのセキュアな通信に対する要求があるときは、含まれるべきである。

コンポーネントのレベル付け

FTP_ITC_EX：TOE 内高信頼チャネル	1

FTP_ITC_EX.1 TOE 内高信頼チャネルは、TSF が、TOE の異なるパーツ間に高信頼通信チャネルを提供することを要求する。

管理：FTP_ITC_EX.1

以下のアクションは FMT における管理機能と考えられる：

・もしサポートされていれば、高信頼チャネルを要求するアクションの構成。

監査：FTP_ITC_EX.1

セキュリティ監査データ生成(FAU_GEN)が PP/ST に含まれていれば、以下のアクションを監査対象にすべきである：

・最小：高信頼チャネル機能の失敗。

・基本：高信頼チャネル機能のすべての使用の試み。

FTP_ITC_EX.1 TOE 内高信頼チャネル

下位階層： なし

依存性： なし

FTP_ITC_EX.1.1

TSF は、TOE の異なるパーツ間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

FTP_ITC_EX.1.2
TSF は、[割付：*高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。

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以下に記述する。

6.1. TOE のサブジェクトとオブジェクトに関する定義

TOE の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、以下の表 8、表 9、表 10、表 11 に、説明を記述する。

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	NEC グループ社員プロセス	NEC グループ社員を代行するプロセスである。セキュリティ属性として、利用者種別、利用者識別情報、利用 URL を持つ。
	構内作業者プロセス	構内作業者を代行するプロセスである。セキュリティ属性として、利用者種別、利用者識別情報、利用 URL を持つ。
	顧客プロセス	顧客を代行するプロセスである。セキュリティ属性として、利用者種別、利用者識別情報、利用 URL を持つ。

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	エリア	業務データファイルのアップロード先のエリアに関連する情報を格納する。セキュリティ属性として、エリア利用許可者情報を持つ。
	フォルダ	業務データファイルのアップロード先のフォルダに関連する情報を格納する。セキュリティ属性として、フォルダ利用許可者情報、利用許可 URL を持つ。
	業務データファイル	アップロードされた業務データファイルに関連する情報を格納する。セキュリティ属性として、アップロード者情報、ダウンロード者情報、利用許可 URL を持つ。

表 10 操作一覧

使用される SFR	操作	内容
FDP_ACC.1 FDP_ACF.1	エリア作成	エリアの作成を行う。
	エリア名参照、 エリア名更新	エリア名の参照、更新を行う。
	エリア削除	エリアの削除を行う。
	フォルダ作成	フォルダの作成を行う。
	フォルダ名参照	フォルダ名の参照を行う。
	フォルダ名更新	フォルダ名の更新を行う。
	メールアドレス(エリア内)参照、 メールアドレス(エリア内)更新	エリア内に登録された利用者のメールアドレスの参照、更新を行う。
	メールアドレス(本人)参照、 メールアドレス(本人)更新	利用者自身のメールアドレスの参照、更新を行う。
	フォルダ削除	フォルダの削除を行う。
	アップロード依頼	アップロード依頼の登録を行う。

使用される SFR	操作	内容
	アップロード	業務データファイルのアップロードを行う。
	アップロード(ワンタイム URL)	ワンタイム URL から、業務データファイルのアップロードを行う。
	アップロードファイル削除 (ワンタイム URL)	アップロードされた業務データファイルの削除を行う。
	アップロードファイル削除	アップロードされた業務データファイルの削除を行う。
	ダウンロード、 ファイル存在確認	業務データファイルのアップロード、ファイルの存在確認を行う。
	ダウンロード(ワンタイム URL)、 ファイル存在確認(ワンタイム URL)	ワンタイム URL から、業務データファイルのアップロード、ファイルの存在確認を行う。

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	エリア利用者の種別を特定する属性	・NEC グループ社員 ・構内作業者 ・顧客
	利用者識別情報	エリア利用者を一意に特定する属性	利用者識別子の値
	利用 URL	ワンタイム URL 経由の利用者を特定する属性	ワンタイム URL の値
	エリア利用許可者情報	エリア利用を許可された利用者を特定する属性	利用者識別子の値のリスト
	フォルダ利用許可者情報	フォルダ利用を許可された利用者を特定する属性	利用者識別子の値のリスト
	アップロード者情報	業務データファイルをアップロードした利用者を特定する属性	利用者識別子の値、 または ワンタイム URL の値
	ダウンロード者情報	業務データファイルのダウンロードを許可された利用者を特定する属性	利用者識別子の値のリスト
	利用許可 URL	ワンタイム URL 経由でフォルダ、業務データファイルの利用を許可された利用者を特定する属性	ワンタイム URL の値のリスト

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、以下、機能要件を記述する。

6.2.1. FAU：セキュリティ監査

FAU_GEN.1 監査データ生成
下位階層： なし
依存性： FPT_STM.1 高信頼タイムスタンプ
FAU_GEN.1.1
TSF は、以下の監査対象事象の監査記録を生成できなければならない：
・監査機能の起動と終了；
・監査の[選択：*最小*, *基本*, *詳細*, *指定なし*：から 1 つのみ選択]レベルのすべての監査対象事象；
及び
・[割付：上記以外の個別に定義した監査対象事象]。
[選択：最小、基本、詳細、指定なし：から 1 つのみ選択]
指定なし
選択した各機能要件の監査対象とすべき最小レベルのアクション(CC における規定)と、それに関連する TOE の監査対象事象(表 12)と、個別に定義した監査対象事象を示す。

表 12 監査対象とすべき基本レベル以下のアクション(CC における規定)と関連する監査対象事象

機能要件	監査対象とすべきアクション	監査対象事象
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAR.1	・基本：監査記録からの情報の読み出し。	・監査記録の参照
FAU_SAR.2	・基本：監査記録からの成功しなかった情報読み出し	・監査記録の参照失敗
FAU_SAR.3	・詳細：閲覧に使用されるパラメタ	なし
FDP_ACC.1	なし	なし
FDP_ACF.1	・最小：SFP で扱われるオブジェクトに対する操作の実行における成功した要求 ・基本：SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求 ・詳細：アクセスチェック時に用いられる特定のセキュリティ属性	・NEC グループ社員によるエリアの作成の成功、失敗 ・NEC グループ社員によるエリアの更新、削除の成功、失敗 ・エリア利用者(管理者)によるフォルダの作成、更新、削除の成功、失敗 ・エリア利用者(社員、構内作業者)によるアップロード依頼の登録の成功、失敗 ・エリア利用者(管理者)によるアップロード依頼の登録の成功、失敗 ・エリア利用者(社員、構内作業者)による業務データのアップロードの成功、失敗 ・エリア利用者(顧客)による業務データのアップロードの成功、失敗 ・エリア利用者(管理者)による業務データのアップロードの成功、失敗 ・エリア利用者(社員、構内作業者)によるアップロードファイルの削除の成功、失敗 ・エリア利用者(顧客)によるアップロードファイルの削除の成功、失敗

機能要件	監査対象とすべきアクション	監査対象事象
		・エリア利用者(管理者)によるフォルダ内ファイルの削除の成功、失敗 ・エリア利用者(社員、構内作業者)による業務データのダウンロードの成功、失敗 ・エリア利用者(顧客)による業務データのダウンロードの成功、失敗 ・エリア利用者(管理者)による業務データのダウンロードの成功、失敗
FIA_AFL.1a	・最小：不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	・累積認証失敗回数が閾値に達した場合のワンタイム URL の失効
FIA_AFL.1b	・最小：不成功の認証試行に対する閾値への到達及びそれに続いてとられるアクション(例えば端末の停止)、もし適切であれば、正常状態への復帰(例えば端末の再稼動)。	・累積認証失敗回数が閾値に達した場合のワンタイム URL の失効
FIA_ATD.1	なし	なし
FIA_SOS.2a	・最小：TSF による、テストされた秘密の拒否； ・基本：TSF による、テストされた秘密の拒否または受け入れ； ・詳細：定義された品質尺度に対する変更の識別。	・ワンタイム URL の品質尺度の検証(成功と失敗)
FIA_SOS.2b	・最小：TSF による、テストされた秘密の拒否； ・基本：TSF による、テストされた秘密の拒否または受け入れ； ・詳細：定義された品質尺度に対する変更の識別。	・PIN の品質尺度の検証(成功と失敗)
FIA_UAU.2	・最小：認証メカニズムの不成功になった使用； ・基本：認証メカニズムのすべての使用； ・詳細：利用者認証以前に行われたすべての TSF 仲介アクション。	・エリア利用者(顧客)の認証の成功と失敗
FIA_UID.2a	・最小：提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用； ・基本：提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	・エリア利用者(顧客)の識別の成功と失敗 ・ワンタイム URL 経由による、エリア利用者(社員、構内作業者)の識別の成功と失敗
FIA_UID.2b	・最小：提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用；	なし

機能要件	監査対象とすべきアクション	監査対象事象
	・基本：提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	
FIA_UID.2c	・最小：提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用； ・基本：提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	なし
FIA_USB.1	・最小：利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 ・基本：利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの成功または失敗)。	なし
FMT_MSA.1	・基本：セキュリティ属性の値の改変すべて。	・エリア利用許可者情報の改変 ・フォルダ利用許可者情報の改変
FMT_MSA.3a	・基本：許可的あるいは制限的規則のデフォルト設定の改変。 ・基本：セキュリティ属性の初期値の改変すべて。	なし
FMT_MSA.3b	・基本：許可的あるいは制限的規則のデフォルト設定の改変。 ・基本：セキュリティ属性の初期値の改変すべて。	なし
FMT_SAE.1	・基本：属性に対する有効期限の時間の特定； ・基本：属性の有効期限切れによってとられるアクション。	なし
FMT_SMF.1	・管理機能の使用。	なし
FMT_SMR.1	・最小：役割の一部をなす利用者のグループに対する改変； ・詳細：役割の権限の使用すべて。	なし
FTP_ITC_EX.1	・最小：高信頼チャネル機能の失敗 ・基本：高信頼チャネル機能のすべての使用の試み	なし

[割付：上記以外の個別に定義した監査対象事象]

なし

FAU_GEN.1.2

TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

・事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)；及び

・各監査事象種別に対して、PP/ST 機能コンポーネントの監査対象事象の定義に基づいた、[割付：*その他の監査関連情報*]

[割付：その他の監査関連情報]
・会社コード
・部門コード

FAU_GEN.2 利用者識別情報の関連付け
下位階層： なし
依存性： FAU_GEN.1 監査データ生成
FIA_UID.1 識別のタイミング
FAU_GEN.2.1
TSF は、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

FAU_SAR.1 監査レビュー
下位階層： なし
依存性： FAU_GEN.1 監査データ生成
FAU_SAR.1.1
TSF は、[割付：*許可利用者*]が、[割付：*監査情報のリスト*]を監査記録から読み出せるようにしなければならない。
[割付：許可利用者]
監査者
[割付：監査情報のリスト]
{事象の日付・時刻、事象の種別、利用者コード、事象の結果(成功または失敗)、会社コード、部門コード}

FAU_SAR.1.2
TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

FAU_SAR.2 限定監査レビュー
下位階層： なし
依存性 ： FAU_SAR1 監査レビュー
FAU_SAR.2.1
TSF は、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

FAU_SAR.3 選択可能監査レビュー
下位階層： なし
依存性： FAU_SAR.1 監査レビュー
FAU_SAR.3.1
TSF は、[割付：*論理的な関連の基準*]に基づいて、監査データを[選択：*検索, 分類, 並べ替え*]する能力を提供しなければならない。
[割付：論理的な関連の基準]
検索対象日付範囲
[選択：検索、分類、並べ替え]
検索

6.2.2. 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＞
・NEC グループ社員プロセス
・構内作業者プロセス
・顧客プロセス
＜オブジェクト＞
・エリア
・フォルダ
・業務データファイル
＜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＞
・NEC グループ社員によるエリアの作成
・NEC グループ社員によるエリア名の参照、更新
・NEC グループ社員によるエリアの削除
・NEC グループ社員によるフォルダの作成
・NEC グループ社員によるフォルダ名の参照
・NEC グループ社員によるフォルダ名の更新
・NEC グループ社員によるメールアドレス(エリア内)の参照、更新
・NEC グループ社員によるメールアドレス(本人)の参照、更新
・NEC グループ社員によるフォルダの削除
・NEC グループ社員によるアップロード依頼の登録
・NEC グループ社員による業務データファイルのアップロード
・NEC グループ社員によるアップロードファイルの削除
・NEC グループ社員による業務データファイルのダウンロード、ファイルの存在確認
・NEC グループ社員による業務データファイルのダウンロード、ファイルの存在確認(ワンタイム URL 経由)
・構内作業者によるフォルダ名の参照
・構内作業者によるメールアドレス(本人)の参照、更新
・構内作業者によるアップロード依頼の登録
・構内作業者による業務データファイルのアップロード
・構内作業者によるアップロードファイルの削除
・構内作業者による業務データファイルのダウンロード、ファイルの存在確認
・構内作業者による業務データファイルのダウンロード、ファイルの存在確認(ワンタイム URL 経由)
・顧客によるフォルダの参照
・顧客による業務データファイルのアップロード(ワンタイム URL 経由)
・顧客によるアップロードファイルの削除(ワンタイム URL 経由)
・顧客による業務データのダウンロード(ワンタイム URL 経由)

[割付：アクセス制御 SFP]

＜業務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]

以下のとおり、各表に示す。

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表 13 に示す。

表 13 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
NEC グループ社員プロセス 構内作業者プロセス 顧客プロセス	利用者種別
	利用者識別情報
	利用 URL

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表 14 に示す。

表 14 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
エリア フォルダ 業務データファイル	エリア利用許可者情報
	フォルダ利用許可者情報
	アップロード者情報
	ダウンロード者情報
	利用許可 URL

[割付: アクセス制御 SFP]
＜業務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]

以下の表 15 に示す。

表 15 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	制御された操作	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
NEC グループ社員プロ	・利用者種別: NEC グループ社員	エリア作成	エリア	なし

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	制御された操作	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
セス	・利用者種別： NEC グループ社員 ・利用者識別情報： エリア利用許可者情報と一致	エリア名参照、 エリア名更新	エリア	・エリア利用許可者情報： 利用者識別情報と一致
		エリア削除	エリア	・エリア利用許可者情報： 利用者識別情報と一致
		フォルダ作成	エリア	・エリア利用許可者情報： 利用者識別情報と一致
		フォルダ名参照	フォルダ	・エリア利用許可者情報： 利用者識別情報と一致
		フォルダ名更新	フォルダ	・エリア利用許可者情報： 利用者識別情報と一致
		メールアドレス (エリア内)参照、 メールアドレス (エリア内)更新	フォルダ	・エリア利用許可者情報： 利用者識別情報と一致
		フォルダ削除	フォルダ	・エリア利用許可者情報： 利用者識別情報と一致
		アップロード依頼	フォルダ	・エリア利用許可者情報： 利用者識別情報と一致
		業務データアップロード	フォルダ	・エリア利用許可者情報： 利用者識別情報と一致
		アップロードファイル削除	業務データファイル	・エリア利用許可者情報： 利用者識別情報と一致
		ダウンロード、 ファイル存在確認	業務データファイル	・エリア利用許可者情報： 利用者識別情報と一致
	・利用者種別： NEC グループ社員 ・利用者識別情報： フォルダ利用許可者情報と一致	フォルダ名参照	フォルダ	・フォルダ利用許可者情報： 利用者識別情報と一致
		メールアドレス (本人)参照、 メールアドレス (本人)更新	フォルダ	・フォルダ利用許可者情報： 利用者識別情報と一致
		アップロード依頼	フォルダ	・フォルダ利用許可者情報： 利用者識別情報と一致
		アップロード	フォルダ	・フォルダ利用許可者情報： 利用者識別情報と一致
	・利用者種別： NEC グループ社員 ・利用者識別情報： アップロード者情報と一致	アップロードファイル削除	業務データファイル	・アップロード者情報： 利用者識別情報と一致
	・利用者種別： NEC グループ社員 ・利用者識別情報： ダウンロード者情報と一致	ダウンロード、 ファイル存在確認	業務データファイル	・ダウンロード者情報： 利用者識別情報と一致
	・利用者種別： NEC グループ社員 ・利用 URL：	ダウンロード (ワンタイム URL)、 ファイル存在確認	業務データファイル	・利用許可 URL： 利用 URL と一致

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	制御された操作	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
	利用許可 URL と一致	(ワンタイム URL)		
構内作業者プロセス	・利用者種別： 構内作業者 ・利用者識別情報： フォルダ利用許可者情報と一致	フォルダ名参照	フォルダ	・フォルダ利用許可者情報： 利用者識別情報と一致
		メールアドレス(本人)参照、 メールアドレス(本人)更新	フォルダ	・フォルダ利用許可者情報： 利用者識別情報と一致
		アップロード依頼	フォルダ	・フォルダ利用許可者情報： 利用者識別情報と一致
		業務データアップロード	フォルダ	・エリア利用許可者情報： 利用者識別情報と一致
	・利用者種別： 構内作業者 ・利用者識別情報： アップロード者情報と一致	アップロードファイル削除	業務データファイル	・アップロード者情報： 利用者識別情報と一致
	・利用者種別： 構内作業者 ・利用者識別情報： ダウンロード者情報と一致	ダウンロード、 ファイル存在確認	業務データファイル	・ダウンロード者情報： 利用者識別情報と一致
	・利用者種別： 構内作業者 ・利用 URL： 利用許可 URL と一致	ダウンロード(ワンタイム URL)、 ファイル存在確認(ワンタイム URL)	業務データファイル	・利用許可 URL： 利用 URL と一致
顧客プロセス	・利用者種別： 顧客 ・利用 URL： 利用許可 URL と一致	業務データアップロード(ワンタイム URL)	フォルダ	・利用許可 URL： 利用 URL と一致
	・利用者種別： 顧客 ・利用 URL： アップロード者情報と一致	アップロードファイル削除(ワンタイム URL)	業務データファイル	・アップロード者情報： 利用 URL と一致
	・利用者種別： 顧客 ・利用 URL： 利用許可 URL と一致	ダウンロード(ワンタイム URL)、 ファイル存在確認(ワンタイム URL)	業務データファイル	・利用許可 URL： 利用 URL と一致

※表 15 に示す、サブジェクトのセキュリティ属性とオブジェクトのセキュリティ属性の値が一致した場合に、サービスの利用が許可される。

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

6.2.3. FIA：識別認証

FIA_AFL.1a 認証失敗時の取り扱い { エリア利用者(顧客) }
下位階層： なし
依存性： FIA_UAU.1 認証のタイミング
FIA_AFL.1.1a
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]
・エリア利用者(顧客)の PIN による認証
[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]
[割付：正の整数値]
3

FIA_AFL.1.2a
不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：*アクションのリスト*]をしなければならない。
[割付：アクションのリスト]
ワンタイム URL の失効化

FIA_AFL.1b 認証失敗時の取り扱い {エリア利用者(社員、構内作業者) }
下位階層： なし
依存性： FIA_UAU.1 認証のタイミング
FIA_AFL.1.1b
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]
・ワンタイム URL 経由による、エリア利用者(社員、構内作業者)の社内認証サービスによる認証

[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]
[割付：正の整数値]
3

FIA_AFL.1.2b
不成功の認証試行が定義した回数に達するか上回ったとき、TSF は、[割付：*アクションのリスト*]をしなければならない。
[割付：アクションのリスト]
ワンタイム URL の失効化

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]
・利用者種別(NEC グループ社員、構内作業者、顧客)
・利用者識別情報
・利用 URL

FIA_SOS.2a TSF 秘密生成 { ワンタイム URL }
下位階層： なし
依存性： なし
FIA_SOS.2.1a
TSF は、[割付：*定義された品質尺度*]に合致する秘密を生成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＞
・ワンタイム URL は、利用者の利用毎に異なる、乱数を元に生成された 27 桁固定長の文字列
・ワンタイム URL に使用する文字は、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 2 文字

FIA_SOS.2.2a
TSF は、[割付：TSF 機能のリスト]に対し、TSF 生成の秘密の使用を実施できなければならない。
[割付：TSF 機能のリスト]
・識別認証機能におけるワンタイム URL

FIA_SOS.2b TSF 秘密生成 { PIN }
下位階層： なし
依存性： なし
FIA_SOS.2.1b

TSF は、[割付：*定義された品質尺度*]に合致する秘密を生成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＞
・PIN は、乱数を元に生成された 16 桁固定長の文字列
・PIN に使用する文字は、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 2 文字

FIA_SOS.2.2b
TSF は、[割付：TSF 機能のリスト]に対し、TSF 生成の秘密の使用を実施できなければならない。
[割付：TSF 機能のリスト]
・識別認証機能における PIN

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→エリア利用者(顧客)
認証 →PIN による認証

FIA_UID.2a アクション前の利用者識別 { ワンタイム URL による識別 }
下位階層：なし
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→エリア利用者(顧客)、エリア利用者(社員、構内作業者)
識別 →ワンタイム URL による識別

FIA_UID.2b アクション前の利用者識別 { 社内認証サービスのユーザ ID による識別 }
下位階層：なし
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：利用者→NEC グループ社員、構内作業者
識別 →社内認証サービスのユーザ ID による識別

FIA_UID.2c アクション前の利用者識別 { URL による識別 }
下位階層：なし

依存性: なし

FIA_UID.2.1c

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→システム管理者、監査者**
識別 →URL 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**
- **利用者識別情報**
- **利用 URL**

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]

以下の表 16 に示す。

表 16 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
NEC グループ社員	NEC グループ社員プロセス	利用者種別	NEC グループ社員
		利用者識別情報	利用者識別子の値
		利用 URL	ワンタイム URL の値
構内作業者	構内作業者プロセス	利用者種別	構内作業者
		利用者識別情報	利用者識別子の値
		利用 URL	ワンタイム URL の値
顧客	顧客プロセス	利用者種別	顧客
		利用 URL	ワンタイム URL 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

6.2.4. 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]
以下の表 17 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]]
以下の表 17 に示す。
[割付：その他の操作]
登録
[割付：許可された識別された役割]
以下の表 17 に示す。
[割付：アクセス制御 SFP、情報フロー制御 SFP]
業務操作アクセス制御方針

表 17 セキュリティ属性の管理

セキュリティ属性	選択：デフォルト値変更、問い合わせ、改変、削除、登録	許可された識別された役割
エリア利用許可者情報	問い合わせ、削除、登録	エリア利用者(管理者)
フォルダ利用許可者情報	問い合わせ、改変、削除、登録	エリア利用者(管理者)

FMT_MSA.3a 静的属性初期化 { エリア利用許可者情報 }
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.3.1a
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。
詳細化：セキュリティ属性→セキュリティ属性(エリア利用許可者情報)
[選択：制限的、許可的、[割付：その他の特性]：から 1 つのみ選択]
[割付：その他の特性]
エリアを作成した NEC グループ社員の利用者識別情報を特定する
[割付：アクセス制御 SFP、情報フロー制御 SFP]
業務操作アクセス制御方針

FMT_MSA.3.2a
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_MSA.3b 静的属性初期化 { 利用許可 URL、アップロード者情報、ダウンロード者情報 }
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.3.1b

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。

詳細化: セキュリティ属性→セキュリティ属性(利用許可 URL、アップロード者情報、ダウンロード者情報)

[選択: 制限的、許可的、[割付: その他の特性]: から 1 つのみ選択]

[割付: その他の特性]

・アップロード依頼を行ったフォルダにアクセスする URL と、アップロード者を特定する

・業務データファイルのダウンロード者と、業務データファイルにアクセスする URL を特定する

[割付: アクセス制御 SFP、情報フロー制御 SFP]

業務操作アクセス制御方針

FMT_MSA.3.2b

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_SAE.1 時限付き許可

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割
FPT_STM.1 高信頼タイムスタンプ

FMT_SAE.1.1

TSF は、[割付: *有効期限がサポートされるはずのセキュリティ属性のリスト*]に対する有効期限の時間を特定する能力を、[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: 有効期限がサポートされるはずのセキュリティ属性のリスト]

以下の表 18 に示す。

[割付: 許可された識別された役割]

以下の表 18 に示す。

FMT_SAE.1.2

これらセキュリティ属性の各々について、TSF は、示されたセキュリティ属性に対する有効期限の時間後、[割付: *各々のセキュリティ属性に対してとられるアクションのリスト*]を行えなければならない。

[割付: 各々のセキュリティ属性に対してとられるアクションのリスト]

以下の表 18 に示す。

表 18 有効期限をサポートするセキュリティ属性と許可役割

セキュリティ属性	許可された識別された役割	各々のセキュリティ属性に対してとられるアクション
ワンタイム URL 有効期間	システム管理者	・有効期間を過ぎたワンタイム URL を失効とする。

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]
- エリア利用者(管理者)による、エリア利用許可者情報の問い合わせ、削除、登録機能
- エリア利用者(管理者)による、フォルダ利用許可者情報の問い合わせ、改変、削除、登録機能

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]
- エリア利用者(管理者)
- システム管理者

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。

6.2.5. FTP:高信頼パス/チャネル

FTP_ITC_EX.1 TOE 内高信頼チャネル
下位階層: なし
依存性: なし
FTP_ITC_EX.1.1
TSF は、TOE の異なるパーツ間に、他の通信チャネルと論理的に区別され、その端点の保証された識別及び改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。
詳細化: TOE の異なるパーツ→Web サーバ、Web ブラウザ

FTP_ITC_EX.1.2
TSF は、[**割付**: *高信頼チャネルが要求される機能のリスト*]のために、高信頼チャネルを介して通信を開始しなければならない。
[**割付**: 高信頼チャネルが要求される機能のリスト]
- エリアメンテナンス機能
- 利用者メンテナンス機能
- アップロード依頼機能
- アップロード機能
- ダウンロード機能
- 個人設定機能

6.3. セキュリティ保証要件

保証要件のクラス毎に以下で保証要件を記述する。

6.3.1. 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

6.3.2. ADV :開発

ADV_FSP.1:基本機能仕様

6.3.3. 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

6.3.4. ALC :ライフサイクルサポート

AGD_CMC.1:TOE のラベル付け
AGD_CMS.1:TOE の CM 範囲

6.3.5. ATE :テスト

ATE_IND.1 独立テスト・準拠

6.3.6. AVA:脆弱性評定

AVA_VAN.1 脆弱性調査

6.4. セキュリティ要件根拠

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、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

	O.I&A	O.IDENTIFY	O.ADMIN_IDENTIFY	O.ACCESS_CONTROL	O.AUDIT	O.ENCRYPT
FAU_GEN.1					×	
FAU_GEN.2					×	
FAU_SAR.1					×	
FAU_SAR.2					×	
FAU_SAR.3					×	
FDP_ACC.1				×		
FDP_ACF.1				×		
FIA_AFL.1a	×					
FIA_AFL.1b		×				
FIA_ATD.1				×		
FIA_SOS.2a	×	×				
FIA_SOS.2b	×					
FIA_UAU.2	×					
FIA_UID.2a	×	×				
FIA_UID.2b		×				
FIA_UID.2c			×			
FIA_USB.1				×		
FMT_MSA.1				×		
FMT_MSA.3a				×		
FMT_MSA.3b				×		
FMT_SAE.1	×	×				
FMT_SMF.1				×		
FMT_SMR.1	×	×		×		
FTP_ITC_EX.1						×

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(顧客の識別認証)

この TOE セキュリティ対策方針は、正当な TOE の利用者である、エリア利用者(顧客)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、正当なエリア利用者(顧客)であることの判断を行う。この対策の詳細、必要機能は以下のとおりである。

a. TOE のサービス機能利用前に、エリア利用者(顧客)を識別認証

エリア利用者(顧客)が、TOE のサービス機能の操作前に、利用許可者であることを、識別されなければならない。また、エリア利用者(顧客)の識別認証は、ワンタイム URL による識別と PIN による認証が成功しなければならない。なお、ワンタイム URL にはシステム管理者が設定した有効期限があり、有効期限が切れたワンタイム URL は失効となり、識別に失敗する。

このため、識別認証する前にエリア利用者(顧客)は、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、FIA_UAU.2、FMT_SAE.1、FMT_SMR.1 である。

b. 指定回数以内の識別認証に失敗したときに、TOE 利用の失効化

識別認証に失敗したエリア利用者(顧客)は、TOE の正当な利用者でないとみなす必要がある。TOE は、指定した回数内の識別認証に失敗したエリア利用者(顧客)に対し、予め定義したアクション(ワンタイム URL 失効化)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.1a である。

c. 利用毎に異なるワンタイム URL の生成

識別を行うためのワンタイム URL は、一時に生成されるものとし、同一利用者に対しても、毎回異なる URL でなければならない。よって、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生成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_SOS.2a である。

d. 一定品質規準を満たす PIN の生成

識別認証を行う際に必要な PIN は、本人以外に予測することが困難でなければならない。よって、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生成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_SOS.2b 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、FIA_AFL.1a、FIA_SOS.2a、FIA_SOS.2b、FIA_UAU.2、FIA.UID.2a、FMT_SAE.1、FMT_SMR.1 の達成により、O.I&A を実現できる。

O.IDENTIFY (社内利用者の識別)

この TOE セキュリティ対策方針は、正当な TOE の利用者である、NEC グループ社員、構内作業者の識別を求めている。この対策の詳細、必要機能は以下のとおりである。

a. TOE のサービス機能利用前に、NEC グループ社員、構内作業者を識別

NEC グループ社員、構内作業者が TOE のサービス機能を利用する前に、利用許可者であることを、識別されなければならない。

このため、NEC グループ社員、構内作業者を識別する前に、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、FIA_UID.2b である。

b. 指定回数以内の識別認証に失敗したときに、TOE 利用の失効化

エリア利用者(社員、構内作業者)が、ワンタイム URL を利用して TOE へアクセスした場合、TOE は指定した回数内の認証に失敗したエリア利用者(社員、構内作業者)に対して、予め指定したアクション(ワンタイム URL 失効化)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.1b である。

c. 利用毎に異なるワンタイム URL を生成

識別を行うためのワンタイム URL は、一時に生成されるものとし、同一利用者に対しても、毎回異なる URL でなければならない。よって、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生成するしくみを提供する。なお、ワンタイム URL にはシステム管理者が設定した有効期限があり、有効期限が切れたワンタイム URL は失効となり、識別に失敗する。

この要件に該当するセキュリティ機能要件は、FIA_SOS.2a、FMT_SAE.1、FMT_SMR.1 である。

以上、a、b、c のすべての対策を満たすことは、O.IDENTIFY 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、FIA_AFL.1b、FIA_SOS.2a、FIA.UID.2a、FIA_UID.2b、FMT_SAE.1、FMT_SMR.1 の達成により、O.IDENTIFY を実現できる。

O.ADMIN_IDENTIFY (管理者の識別)

この TOE セキュリティ対策方針は、正当な TOE の利用者である、システム管理者、監査者の識別を求めている。この対策の詳細、必要機能は以下のとおりである。

a. TOE のサービス機能利用前に、システム管理者、監査者を識別

システム管理者、監査者が、TOE のサービス機能を利用する前に、URL により利用許可者であることを、識別されなければならない。

このため、システム管理者、監査者を識別する前に、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.2c である。

以上、a の対策を満たすことは、O.ADMIN_IDENTIFY 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、FIA_UID.2c、の達成により、O.ADMIN_IDENTIFY 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では、NEC グループ社員、構内作業者、エリア利用者(管理者)、エリア利用者(社員、構内作業者)、エリア利用者(顧客)は、許可された保護資産のみのアクセスを実施するため、アクセス制御方針を定義し、保護資産に対する操作を制御することを求める。この対策の詳細、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

NEC グループ社員、構内作業者、エリア利用者(管理者)、エリア利用者(社員、構内作業者)、エリア利用者(顧客)に対して許可操作と操作対象を決定する。また、許可がない者が操作できないように、操作を実施しなければならない。

このため、NEC グループ社員、構内作業者、顧客について、その利用者役割に基づき、エリア、フォルダ、業務データファイルに対する、以下の操作のアクセス制御を実施する。

・NEC グループ社員によるエリアの作成
・NEC グループ社員{エリア利用者(管理者)}によるエリア名の参照、更新
・NEC グループ社員{エリア利用者(管理者)}によるエリアの削除
・NEC グループ社員{エリア利用者(管理者)}によるフォルダの作成
・NEC グループ社員{エリア利用者(管理者)}によるフォルダ名の参照
・NEC グループ社員{エリア利用者(社員、構内作業者)}によるフォルダ名の参照
・NEC グループ社員{エリア利用者(管理者)}によるフォルダ名の更新
・NEC グループ社員{エリア利用者(管理者)}によるフォルダの削除
・NEC グループ社員{エリア利用者(管理者)}によるアップロード依頼の登録
・NEC グループ社員{エリア利用者(社員、構内作業者)}によるアップロード依頼の登録
・NEC グループ社員{エリア利用者(管理者)}による業務データファイルのアップロード
・NEC グループ社員{エリア利用者(社員、構内作業者)}による業務データファイルのアップロード
・NEC グループ社員{エリア利用者(管理者)}によるアップロードファイルの削除
・NEC グループ社員{エリア利用者(社員、構内作業者)}によるアップロードファイルの削除

・NEC グループ社員{エリア利用者(管理者)}による業務データファイルのダウンロード、ファイルの存在確認
・NEC グループ社員{エリア利用者(社員、構内作業者)}による業務データファイルのダウンロード、ファイルの存在確認(ワンタイム URL 経由)
・構内作業者{エリア利用者(社員、構内作業者)}によるフォルダ名の参照
・構内作業者{エリア利用者(社員、構内作業者)}によるアップロード依頼の登録
・構内作業者{エリア利用者(社員、構内作業者)}による業務データファイルのアップロード
・構内作業者{エリア利用者(社員、構内作業者)}によるアップロードファイルの削除
・構内作業者{エリア利用者(社員、構内作業者)}による業務データファイルのダウンロード、ファイルの存在確認
・構内作業者{エリア利用者(社員、構内作業者)}による業務データファイルのダウンロード、ファイルの存在確認(ワンタイム URL 経由)
・顧客{エリア利用者(顧客)}によるフォルダの参照
・顧客{エリア利用者(顧客)}による業務データファイルのアップロード(ワンタイム URL 経由)
・顧客{エリア利用者(顧客)}によるアップロードファイルの削除(ワンタイム URL 経由)
・顧客{エリア利用者(顧客)}による業務データのダウンロード(ワンタイム URL 経由)
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
利用者に応じてアクセスを制限するためには、TOE を利用するとき、各利用者が持つ利用者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。このため、利用者は、それぞれの利用者セキュリティ属性である利用者種別を持ち、利用者を代行して動作するサブジェクトに利用者種別を関連付け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、FIA_USB.1 である。

c. 利用者役割に応じたアクセス制御
エリア、フォルダへのアクセスを制御するために、セキュリティ属性である、エリア利用許可者情報、フォルダ利用許可者情報を適切に設定しなければならない。エリア利用許可者情報に対する問い合わせ、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、削除は、エリア利用者(管理者)により行うことができる。なお、セキュリティ属性である、エリア利用許可者情報は、NEC グループ社員がエリアを作成するとき、その NEC グループ社員を特定するデフォルト値が設定される。また、セキュリティ属性である、利用許可 URL は、エリア利用者(社員、構内作業者)が指定したフォルダへのアップロード依頼、または業務データのアップロードを行うとき、そのファルダ、または業務データファイルへのアクセス URL を特定するデフォルト値が設定される。なお、アップロードを行うとき、ダウンロードを許可された利用者が、セキュリティ属性である、ダウンロード者情報に設定される。このとき、アップロードを実行した利用者が、セキュリティ属性である、アップロード者情報に設定される。
これに該当するセキュリティ機能要件は、FMT_MSA.1、FMT_MSA.3a、FMT_MSA.3b、FMT_SMR.1 である。

d. 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 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.3a、FMT_MSA.3b、FMT_SMF.1、FMT_SMR.1 の達成により、O_ACCESS_CONTROL が実現できる。

O.AUDIT(監査)

この TOE セキュリティ対策方針は、監査記録の取得とその保護について求める。監査記録は、TOE の動作状況を後日確認するための証拠となる情報であり、必要となった時点で利用できなければならない。このため、監査記録の保護では、監査記録の確実な取得、監査記録の改ざんを考慮する。この対策の詳細と、必要機能は、以下のとおりである。

a. 監査記録に必要な情報を取得

TOE の動作で、監査対象とすべき事象について、必要な情報を記録しなければならない。識別認証、及びアクセス制御に関連する試みについて、事象の日付、時刻、ユーザ ID、会社コード、部門コードを含む監査記録を生成する。このとき、セキュリティメカニズムの使用について、監査(監査レベル:指定なし)を求める。監査記録の取得において、その監査事象が発生した正確な日付・時刻を取得する。なお、監査レベルの「指定なし」については、監査対策がセキュリティ事象への事後対策手段であり、TOE のセキュリティ対策として、識別認証、及びアクセス制御により保証しているため、これで十分と考える。

これに該当するセキュリティ機能要件は、FAU_GEN.1 である。

また、監査記録の取得において、事象を起こした主体を明らかにしなければならない。このため、監査対象事象を、その原因となった識別情報に関連付ける。

これに該当するセキュリティ機能要件は、FAU_GEN.2 である。

b. 監査記録の利用者、及び利用内容の制限

監査記録の読み出しを、許可した者のみに制限する。監査記録を読み出して利用することは、監査者のみに利用を許可し、それ以外の者の利用を禁止する。

これに該当するセキュリティ機能要件は、FAU_SAR.1、FAU_SAR.2 である。

監査記録の利用においては、検索ができなければならない。監査記録の利用にあたっては、指定した条件を用いた検索を提供する。

これに該当するセキュリティ機能要件は、FAU_SAR.3 である。

以上、a、b のすべての対策を満たすことは、O_AUDIT 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、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_SAR.3 の達成により、O.AUDIT が実現できる。

O.ENCRYPT(暗号化)

この TOE セキュリティ対策方針は、通信データの保護について求める。その対策として、通信データを暗号化、復号する必要がある。この対策の詳細と、必要機能は以下のとおりである。

a. 通信データの暗号化、復号

社外利用者クライアントと社外 Web サーバ間、社内利用者クライアントと社内用 Web サーバ間の通信は SSL 通信を行うことで、他の通信チャネルと区別され、通信データの改ざん、暴露されないように保護する。

これに該当するセキュリティ機能要件は、FTP_ITC_EX.1 である。

以上、a の対策を満たすことは、O_ENCRYPT 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、FTP_ITC_EX.1 の達成により、O.ENCRYPT が実現できる。

6.4.2. 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 20 に示す。

表 20 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	根拠
FAU_GEN.1	FPT_STM.1	なし	FPT_STM.1	*1

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	根拠
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2	なし	
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし	
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	なし	
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	なし	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3a FMT_MSA.3b	なし*2	
FIA_AFL.1a	FIA_UAU.1	FIA_UAU.2 (左記の上位階層)	なし	
FIA_AFL.1b	FIA_UAU.1	なし	FIA_UAU.1	*3
FIA_ATD.1	なし	なし	なし	
FIA_SOS.2a	なし	なし	なし	
FIA_SOS.2b	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_UID.2c	なし	なし	なし	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし	
FMT_MSA.1	[FDP_ACC.1、 FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	なし	
FMT_MSA.3a	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1	FMT_SMR.1	*4
FMT_MSA.3b	FMT_MSA.1 FMT_SMR.1	なし	FMT_MSA.1	*5
			FMT_SMR.1	*6
FMT_SAE.1	FMT_SMR.1 FPT_STM.1	FMT_SMR.1	FPT_STM.1	*7
FMT_SMF.1	なし	なし	なし	
FMT_SMR.1	FIA_UID.1	FIA_UID.2a FIA_UID.2b FIA_UID.2c (左記の上位階層)	なし	
FTP_ITC_EX.1	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。すべての例外について、依存関係は満たさなくても問題がない根拠を以下に示す。

*1) FAU_GEN.1 →FPT_STM.1

本 TOE では、システム内の時刻は、OE.OS_TIMESTAMP により、TOE 外となる OS 機能を使用することから、依存関係は不要である。

*2)セキュリティ属性(フォルダ利用許可者情報)について

本 TOE では、FDP_ACF.1 のオブジェクトのセキュリティ属性(フォルダ利用許可者情報)については、フォルダの作成時に初期値を設定する必要がないため、FMT_MSA.3 のセキュリティ属性としての依存関係は不要である。

*3) FIA_AFL.1b → FIA_UAU.1

本 TOE では、エリア利用者(社員、構内作業者)の認証については、OE.AUTHENTICATION により、TOE 外の社内認証サービスを利用することから、依存関係は不要である。

*4) FMT_MSA.3a →FMT_SMR.1

本 TOE では、FMT_MSA.3a のセキュリティ属性(エリア利用許可者情報)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。

*5) FMT_MSA.3b →FMT_MSA.1

本 TOE では、FMT_MSA.3b のセキュリティ属性(利用許可 URL)については、ワンタイム URL として、一時的に生成されるのみで、管理を行う必要がないため、依存関係は不要である。

*6) FMT_MSA.3b →FMT_SMR.1

本 TOE では、FMT_MSA.3b のセキュリティ属性(利用許可 URL、アップロード者情報、ダウンロード者情報)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。

*7) FMT_SAE.1 →FPT_STM.1

本 TOE では、システム内の時刻は、OE.OS_TIMESTAMP により、TOE 外となる OS 機能を使用することから、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 TOE は、想定する脅威から、攻撃者のレベルを低レベルとしており、また、NEC グループ内で顧客との情報交換に利用する社内システムでもあることから、公知の脆弱性に対するレベルの保証で十分と考えている。このため、EAL1+ ASE_SPD.1、ASE_OBJ.2、ASE_REQ.2 を選択する。

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、正当な利用者であり、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、認証に利用する PIN は、品質尺度の検証のしくみも提供する。以下では、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

⑴ 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、FMT_SAE.1 時限付き許可

TOE は、TOE のサービス機能を利用させる前に、エリア利用者(顧客)を識別認証する。識別認証は、ワンタイム URL による識別と PIN による認証を行う。このとき、下記(7)に示す秘密生成に基づいたワンタイム URL と、下記(8)に示す秘密生成に基づいた PIN を使用する。なお、ワンタイム URL は、システム管理者が設定した有効期限日数を経過すると自動的に失効する。

・下記処理が 1→3 の順番ですべて成功した場合に、エリア利用者(顧客)の識別認証が成功となる。

1. ワンタイム URL よる識別
2. ワンタイム URL の有効期限の検証
3. 顧客に通知した PIN と入力された PIN が一致することを確認して認証

上記より、FIA_UID.2a、FIA_UAU.2、FIA_SOS.2a、FIA_SOS.2b、FMT_SAE.1 を実現する。

⑵ FIA_UID.2a アクション前の利用者識別、FMT_SAE.1 時限付き許可

TOE は、TOE のサービス機能を利用させる前に、エリア利用者(社員、構内作業者)を識別する。識別は、ワンタイム URL による識別を行う。このとき、下記(7)に示す秘密生成に基づいたワンタイム URL を使用する。なお、ワンタイム URL は、システム管理者が設定した有効期限日数を経過すると自動的に失効する。

・下記の処理が成功した場合に、エリア利用者(社員、構内作業者)の識別が成功となる。

1. ワンタイム URL よる識別
2. ワンタイム URL の有効期限の検証

上記より、FIA_UID.2a、FIA_SOS.2a、FMT_SAE.1 を実現する。

⑶ FIA_UID.2b アクション前の利用者識別

TOE は、TOE のサービス機能を利用させる前に、NEC グループ社員、構内作業者を識別する。識別は、ユーザ ID による識別を行う。

・下記の処理が成功した場合に、NEC グループ社員、構内作業者の識別が成功となる。

1. ユーザ ID による識別

上記より、FIA_UID.2b を実現する。

⑷ FIA_UID.2c アクション前の利用者識別

TOE は、TOE のサービス機能を利用させる前に、システム管理者、監査者を識別する。識別は、システム管理者画面、監査者画面の URL による検証を行う。

・下記の処理が成功した場合のみ、システム管理者、監査者の識別が成功となる。

1. URL による識別

上記より、FIA_UID.2c を実現する。

⑸ FIA_AFL.1a 認証失敗時の取り扱い

TOE は、エリア利用者(顧客)の識別認証に関して、以下の機能を提供する。

・エリア利用者(顧客)が使用するワンタイム URL に対する PIN が異なる場合、ワンタイム URL 毎に PIN の誤り回数をカウントする。累積誤り回数が不成功認証試行回数(3 回固定)に達すると、そのワンタイム URL を失効とする。

上記より、FIA_AFL.1a を実現する。

⑹ FIA_AFL.1b 認証失敗時の取り扱い

TOE は、エリア利用者(社員、構内作業者)の識別に関して以下の機能を提供する。

・エリア利用者(社員、構内作業者)が、ワンタイム URL 経由で、社内認証サービスの認証に失敗した場合は、社内認証サービスの認証誤り回数をカウントする。累積誤り回数が不成功認証試行回数(3 回固定)に達すると、そのワンタイム URL を失効とする。

上記より、FIA_AFL.1b を実現する。

⑺ FIA_SOS.2a TSF 秘密生成

TOE は、識別認証に使用する、以下の条件を満たす、ワンタイム URL を生成する。

1. 乱数を元に生成し、27 桁固定長の文字列である
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 2 文字

上記より、FIA_SOS.2a を実現する。

⑻ FIA_SOS.2b TSF 秘密生成

TOE は、識別認証に使用する、以下の条件を満たす、PIN を生成する。

1. 乱数を元に生成し、16 桁固定長の文字列である
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 2 文字

上記より、FIA_SOS.2b を実現する。

⑼ FMT_SMR.1 セキュリティの役割

TOE は、上記(1)、及び上記(2)に示す、ワンタイム URL の有効期限の管理を許可されている役割と、許可された役割を維持する。

・システム管理者

上記より、FMT_SMR.1 を実現する。

7.2. 監査機能

監査機能は、TOE の安定的な稼動の記録を維持するために、監査記録を生成する機能、監査記録の参照、及び検索を行う機能を提供する。

監査機能は、監査者のみが利用できる。

以下では、監査機能について、SFR 実現方法という観点から説明する。

7.2.1. 監査機能に対応する SFR の実現方法

⑴ FAU_GEN.1 監査データ生成

TOE は、TOE がセキュアに運用されていることを監視するために必要な情報の採取、及び採取した情報の管理を行うために、監査の対象となる事象が発生した場合、当該事象の監査証跡として、監査記録を生成する。
監査記録は、以下の監査対象事象の発生時に採取する。

- 監査機能の起動と終了
- 監査記録の参照
- 監査記録の参照失敗
- NEC グループ社員によるエリアの作成の成功、失敗
- NEC グループ社員によるエリアの更新、削除の成功、失敗
- エリア利用者(管理者)によるフォルダの作成、更新、削除の成功、失敗
- エリア利用者(管理者)による社内利用者情報(エリア利用許可者情報、フォルダ利用許可者情報)の改変(登録、更新、削除)の成功、失敗
- エリア利用者(管理者)による顧客情報(フォルダ利用許可者情報)の改変(登録、更新、削除)の成功、失敗
- エリア利用者(社員、構内作業者)によるアップロード依頼の登録の成功、失敗
- エリア利用者(管理者)によるアップロード依頼の登録の成功、失敗
- エリア利用者(社員、構内作業者)による業務データのアップロードの成功、失敗
- エリア利用者(顧客)による業務データのアップロードの成功、失敗
- エリア利用者(管理者)による業務データのアップロードの成功、失敗
- エリア利用者(社員、構内作業者)によるアップロードファイルの削除の成功、失敗
- エリア利用者(顧客)によるアップロードファイルの削除の成功、失敗
- エリア利用者(管理者)によるフォルダ内のファイルの削除の成功、失敗
- エリア利用者(社員、構内作業者)による業務データのダウンロードの成功、失敗
- エリア利用者(顧客)による業務データのダウンロードの成功、失敗
- エリア利用者(管理者)による業務データのダウンロードの成功、失敗
- 累積認証失敗回数が閾値に達した場合のワンタイム URL の失効
- PIN の品質尺度の検証(成功と失敗)
- ワンタイム URL の品質尺度の検証(成功と失敗)
- エリア利用者(顧客)の認証の成功と失敗
- ワンタイム URL によるエリア利用者(社員、構内作業者)の識別の成功と失敗
- エリア利用者(顧客)の識別の成功と失敗
- 利用者種別の改変
- エリア利用者(管理者)のメールアドレス改変
- エリア利用者(社員、構内作業者)のメールアドレス改変

監査記録は、以下の項目で構成される。

- 事象の日付、時刻(OS から取得したタイムスタンプ情報を使用する)
- 事象の種別：事象の分類
- サブジェクト識別情報(利用者コード)
- 事象の結果(成功／失敗)
- 会社コード
- 部門コード

上記より、FAU_GEN.1 を実現する。

⑵ FAU_GEN.2 利用者識別情報の関連付け

TOE は、監査対象となる事象が発生した場合に、当該事象とその原因となった利用者の識別情報(サブジェクト識別情報)を、関連付けたうえで監査証跡としての監査記録を生成する。利用者の識別情報として、利用者コードをサブジェクト識別情報として記録する。
上記より、FAU_GEN.2 を実現する。

⑶ FAU_SAR.1 監査レビュー

TOE は、採取した情報を分かりやすい形式で出力し、監査者のみが参照できる機能を提供する。監査項目を下記とし、監査者を識別して監査記録から読み出す機能を提供する。

- サブジェクト識別情報(利用者コード)
- 事象の種別
- 事象の結果(成功･失敗)
- 事象の日付、時刻
- 会社コード
- 部門コード

上記より、FAU_SAR.1 を実現する。

⑷ FAU_SAR.2 限定監査レビュー

TOE は、監査者以外が監査記録の読出し機能の利用を禁止するしくみを提供するために、監査者を識別して、監査記録への操作を監査者のみに許可し、操作を制御する。
上記より、FAU_SAR.2 を実現する。

⑸ FAU_SAR.3 選択監査レビュー

TOE は、監査記録の参照機能として、事象の日付の範囲指定で検索を行う機能を提供する。
上記より、FAU_SAR.3 を実現する。

7.3. アクセス制御機能

TOE は、TOE の利用者役割毎に付与した権限に基づき、利用者データへの操作を制御する機能を提供する。
以下では、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。

7.3.1. アクセス制御機能に対応する SFR の実現方法

⑴ FIA_ATD.1 利用者属性定義

TOE は、利用者のセキュリティ属性と利用者を関連付けるための要件を定義し、以下に提供する。

1. 利用者種別(NEC グループ社員、構内作業者、顧客)
2. 利用者識別情報
3. 利用 URL

上記より、FIA_ATD.1 を実現する。

⑵ FIA_USB.1 利用者-サブジェクト結合

TOE は、認証された利用者が TOE を使用するために、以下の表 21 に示す、利用者のセキュリティ属性とその利用者を代行するサブジェクトとの関連付けを行う。

表 21 サブジェクトと利用者セキュリティ属性の関係

サブジェクト	利用者セキュリティ属性	セキュリティ属性項目
NEC グループ社員プロセス	利用者種別	NEC グループ社員
	利用者識別情報	利用者識別子の値
	利用 URL	ワンタイム URL の値
構内作業者プロセス	利用者種別	構内作業者

サブジェクト	利用者セキュリティ属性	セキュリティ属性項目
	利用者識別情報	利用者識別子の値
	利用 URL	ワンタイム URL の値
顧客プロセス	利用者種別	顧客
	利用 URL	ワンタイム URL の値

上記より、FIA_USB1 を実現する。

⑶ 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、以下の表 22 に示すサブジェクトとオブジェクトに対しての操作を行う、業務操作アクセス制御方針を実行する。

表 22 業務操作アクセス制御方針で扱われるサブジェクトとオブジェクト間の操作

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	制御された操作	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
NEC グループ社員プロセス	・利用者種別: NEC グループ社員	エリア作成	エリア	なし
	・利用者種別: NEC グループ社員 ・利用者識別情報: エリア利用許可者情報と一致	エリア名参照、エリア名更新	エリア	・エリア利用許可者情報: 利用者識別情報と一致
		エリア削除	エリア	・エリア利用許可者情報: 利用者識別情報と一致
		フォルダ作成	エリア	・エリア利用許可者情報: 利用者識別情報と一致
		フォルダ名参照	フォルダ	・エリア利用許可者情報: 利用者識別情報と一致
		フォルダ名更新	フォルダ	・エリア利用許可者情報: 利用者識別情報と一致
		メールアドレス(エリア内)参照、メールアドレス(エリア内)更新	フォルダ	・エリア利用許可者情報: 利用者識別情報と一致
		フォルダ削除	フォルダ	・エリア利用許可者情報: 利用者識別情報と一致
		アップロード依頼	フォルダ	・エリア利用許可者情報: 利用者識別情報と一致
		業務データアップロード	フォルダ	・エリア利用許可者情報: 利用者識別情報と一致
		アップロードファイル削除	業務データファイル	・エリア利用許可者情報: 利用者識別情報と一致
		ダウンロード、ファイル存在確認	業務データファイル	・エリア利用許可者情報: 利用者識別情報と一致
	・利用者種別: NEC グループ社員 ・利用者識別情報: フォルダ利用許可者情報と一致	フォルダ名参照	フォルダ	・フォルダ利用許可者情報: 利用者識別情報と一致
		メールアドレス(本人)参照、メールアドレス(本人)更新	フォルダ	・フォルダ利用許可者情報: 利用者識別情報と一致
		アップロード依頼	フォルダ	・フォルダ利用許可者情報: 利用者識別情報と一致

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	制御された操作	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
		アップロード	フォルダ	・フォルダ利用許可者情報：利用者識別情報と一致
	・利用者種別：NEC グループ社員 ・利用者識別情報：アップロード者情報と一致	アップロードファイル削除	業務データファイル	・アップロード者情報：利用者識別情報と一致
	・利用者種別：NEC グループ社員 ・利用者識別情報：ダウンロード者情報と一致	ダウンロード、ファイル存在確認	業務データファイル	・ダウンロード者情報：利用者識別情報と一致
	・利用者種別：NEC グループ社員 ・利用 URL：利用許可 URL と一致	ダウンロード(ワンタイム URL)、ファイル存在確認(ワンタイム URL)	業務データファイル	・利用許可 URL：利用 URL と一致
構内作業者プロセス	・利用者種別：構内作業者 ・利用者識別情報：フォルダ利用許可者情報と一致	フォルダ名参照	フォルダ	・フォルダ利用許可者情報：利用者識別情報と一致
		メールアドレス(本人)参照、メールアドレス(本人)更新	フォルダ	・フォルダ利用許可者情報：利用者識別情報と一致
		アップロード依頼	フォルダ	・フォルダ利用許可者情報：利用者識別情報と一致
		業務データアップロード	フォルダ	・エリア利用許可者情報：利用者識別情報と一致
	・利用者種別：構内作業者 ・利用者識別情報：アップロード者情報と一致	アップロードファイル削除	業務データファイル	・アップロード者情報：利用者識別情報と一致
	・利用者種別：構内作業者 ・利用者識別情報：ダウンロード者情報と一致	ダウンロード、ファイル存在確認	業務データファイル	・ダウンロード者情報：利用者識別情報と一致
	・利用者種別：構内作業者 ・利用 URL：利用許可 URL と一致	ダウンロード(ワンタイム URL)、ファイル存在確認(ワンタイム URL)	業務データファイル	・利用許可 URL：利用 URL と一致
顧客プロセス	・利用者種別：顧客 ・利用 URL：利用許可 URL と一致	業務データアップロード(ワンタイム URL)	フォルダ	・利用許可 URL：利用 URL と一致

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	制御された操作	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
	・利用者種別： 顧客 ・利用 URL： アップロード者情報 と一致	アップロードファイル削除 (ワンタイム URL)	業務データ ファイル	・アップロード者情報： 利用 URL と一致
	・利用者種別： 顧客 ・利用 URL： 利用許可 URL と一致	ダウンロード (ワンタイム URL)、 ファイル存在確認 (ワンタイム URL)	業務データ ファイル	・利用許可 URL： 利用 URL と一致

※サブジェクトのセキュリティ属性とオブジェクトのセキュリティ属性の値が一致した場合に、サービスの利用が許可される。

上記より、FDP_ACC.1、FDP_ACF.1 を実現する。

⑷ FMT_MSA.1 セキュリティ属性の管理、FMT_MSA.3a、FMT_MSA.3b 静的属性初期化

TOE は、利用者役割に応じたアクセス制御を行うためにセキュリティ属性の改変を、特定の利用者に限定する。以下に定義する。

1. エリア利用者(管理者)のみが、以下のセキュリティ属性の操作を行える。
   ・エリア利用許可者情報に対する、問い合わせ、削除、登録
   ・フォルダ利用許可者情報に対する、問い合わせ、改変、削除、登録
2. 以下のセキュリティ属性については、初期値が登録される
   ・エリア利用許可者情報に、作成した NEC グループ社員の利用者識別情報を設定
   ・利用許可 URL に、アップロード依頼を行ったフォルダにアクセスする URL を設定
   ・利用許可 URL に、アップロードを行った業務データにアクセスする URL を設定
   ・ダウンロード者情報に、ダウンロードの利用を許可する利用者識別情報を設定
   ・アップロード者情報に、アップロードを実行した利用者識別情報を設定

上記より、FMT_MSA.1、FMT_MSA.3a、FMT_MSA.3b を実現する。

⑸ FMT_SMF.1 管理機能の特定

TOE は、以下に示すセキュリティ管理機能を提供する。

・エリア利用者(管理者)による、エリア利用許可者情報の問い合わせ、削除、登録
・エリア利用者(管理者)による、フォルダ利用許可者情報の問い合わせ、改変、削除、登録

上記は、FMT_MSA.1 により、FMT_SMF.1 を実現する。

⑹ FMT_SMR.1 セキュリティの役割

TOE は、上記(4)に示すセキュリティ属性の管理、及び上記(5)に示すセキュリティ管理機能の使用を許可されている役割と、許可された役割を維持する。

・エリア利用者(管理者)

上記より、FMT_SMR.1 を実現する。

7.4. 暗号機能

TOE は、社外利用者クライアントと社外 Web サーバ間、社内利用者クライアントと社内用 Web サーバ間の通信データを暗号化、復号する機能を提供する。

以下では、暗号機能について、SFR 実現方法という観点から説明する。

7.4.1. 暗号機能に対応する SFR の実現方法

⑴ FTP_ITC_EX.1 TOE 内高信頼チャネル

TOE は、他の TOE との高信頼チャネルを生成するための要件を、以下に定義する。

1. 社外利用者クライアント、社内利用者クライアントの Internet Explorer6.0/7.0 と社外用 Web サーバ、社内用 Web サーバの Internet Information Server 6.0 間の通信には SSL 機能を使用し、サーバ証明書を基に、他の通信と区別する。
2. TOE は、以下の機能を利用するときに、SSL 通信を使用する。

- エリアメンテナンス機能
- 利用者メンテナンス機能
- アップロード依頼機能
- アップロード機能
- ダウンロード機能
- 個人設定機能

上記より、FTP_ITC_EX.1 を実現する。