NEC グループ 情報漏洩防止システム V1.0

セキュリティターゲット

バージョン 1.12

２００７年１２月１２日

日本電気株式会社

更新履歴

バージョン	更新日	変更内容	作成者
1.00	2007/04/23	新規作成	日本電気株式会社
1.01	2007/05/18	I/O ポート制御の記述を追記 追記に伴い、全体見直し	日本電気株式会社
1.02	2007/06/08	評価機関指摘事項に対応	日本電気株式会社
1.03	2007/07/13	評価機関指摘事項に対応	日本電気株式会社
1.04	2007/08/03	評価機関指摘事項に対応	日本電気株式会社
1.05	2007/08/15	評価機関指摘事項に対応	日本電気株式会社
1.06	2007/08/22	評価機関指摘事項に対応	日本電気株式会社
1.07	2007/08/31	評価機関指摘事項に対応	日本電気株式会社
1.08	2007/10/10	評価機関指摘事項に対応	日本電気株式会社
1.09	2007/10/15	評価機関指摘事項に対応	日本電気株式会社
1.10	2007/10/19	評価機関指摘事項に対応	日本電気株式会社
1.11	2007/11/14	評価機関指摘事項に対応	日本電気株式会社
1.12	2007/12/12	評価機関指摘事項に対応	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

本書は、以下のドキュメントを参照している。

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

・Common Criteria for Information Technology Security Evaluation Part 2: Security functional components September 2006 Version 3.1 Revision 1 CCMB-2006-09-002

・Common Criteria for Information Technology Security Evaluation Part 3: 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 改定第 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 改定第 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 改定第 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

略語・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

IT（Information Technology）：情報技術

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

SFR（Security Functional Requirement）：セキュリティ機能要件

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

＜TOE 関連略語＞

AP（Application Program）：アプリケーションプログラム

CPU（Central Processing Unit）：中央処理装置

DB（Database）：データベース

DBMS（Database Management System）：データベース管理システム

GB（Giga Byte）：ギガバイト

GHz（Gigahertz）：ギガヘルツ

HDD（Hard Disk Drive）：ハードディスクドライブ

ID（Identification）：識別情報

IEEE（The Institute of Electrical and Electronics Engineers, Inc.）：電気電子学会

IP（Internet Protocol）：インターネットプロトコル

LAN（Local Area Network）：ローカルエリアネットワーク

MAC（Media Access Control）：メディアアクセスコントロール

MB（Mega Byte）：メガバイト

OS（Operating System）：オペレーティングシステム

PC（Personal Computer）：パーソナルコンピュータ

PCMCIA（Personal Computer Memory Card International Association）：ピーシーエムシーアイエー

SSL（Secure Socket Layer）：セキュアソケットレイヤ

USB（Universal Serial Bus）：ユニバーサルシリアルバス

＜TOE 関連用語＞

用語	定義内容
Administrator 権限	Microsoft オペレーティングシステムのユーザ権限の種類のひとつで、ＯＳの設定を変更できる権限
NEC	日本電気株式会社
NEC グループ	NEC 及び NEC 関係会社
I/O ポート	PC と PC に接続される機器とのデータのやり取りに使用することができるポートで、USB ポート、IEEE1394 ポート、シリアルポート、パラレルポート、赤外線ポート、PCMCIA ポート及びプリンタポート
Java	オブジェクト指向プログラミング言語の一つ。プログラミング言語である Java の実行環境
JDBC	Java とデータベースの接続のための AP インタフェース
LogViewer	ログサーバアプリケーションソフトウェアで動作するログの閲覧・検索機能
LogViewer 起動制御情報	LogViewer を使用するための制御情報
USB デバイス	PC の USB ポートに接続される周辺機器の総称
Web	World Wide Web と同義。インターネット上で提供されるハイパーテキストシステム
Winny	ファイル共有ソフトウェアの一つ
Windows ネットワークのワークグループ	Microsoft オペレーティングシステムのネットワーク ID の種類のひとつで、ファイルやプリンタのようなリソースを共有することができるネットワーク上のコンピュータの論理グループ
暗号鍵入力制御情報	ファイル暗号用共通鍵を読み込むための情報
一般 AP ファイル	Microsoft Office Word/Excel/PowerPoint 等のクライアントの OS 上で動作するアプリケーションプログラムの総称で、ソースコードを含まない実行形式の利用者データ
管理者	管理者とクライアント管理者の利用者役割を持つ者
外部メディア	クライアントに接続され OS によりリムーバブルメディアと認識されたメディア（外付け HDD、USB メモリ、PCMCIA メモリ）
管理者端末	管理者がクライアント制御情報の作成やログの閲覧・検索を行う PC
許可 USB デバイス	管理者によりあらかじめ利用を許可された USB デバイス
許可外部メディア	クライアントに接続され OS によりリムーバブルメディアと認識

	されたメディア（外付け HDD、USB メモリ、PCMCIA メモリ）で、管理者によりあらかじめ許可外部メディア入出力制御情報が書き込まれたメディア
グループ名	各部署単位に決定する任意の名称
クライアント	NEC グループ内で利用する PC
クライアント制御情報	PC 制御方針であり、管理者により作成され、クライアントに設定され、クライアントの動作を制御する定義情報
クライアントセットアップイメージ	管理者により作成され、クライアントの動作環境をあらかじめ設定するための情報をまとめたファイルであり、クライアント制御情報も含む
再認証時間	ログオンした後、離席等した場合の TOE 未使用時間
資産管理システム	社有資産の管理を行う、TOE とは独立して運用されているシステム
プリンタポート	クライアントの印刷データをプリンタに出力するためのポート
保守モード	Microsoft Windows OS を保守するため、Windows 起動時に指定するモード（セーフモード）
利用者	管理者、クライアント管理者及び一般利用者の総称
レジストリ	クライアントの OS の制御に関わる設定項目が格納されている領域
ログ	監査証跡に記録された監査記録

1. ST 概説

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

1.1. ST 参照

タイトル：NEC グループ 情報漏洩防止システム V1.0 セキュリティターゲット
バージョン：1.12
作成者： 日本電気株式会社
発行日： 2007 年 12 月 12 日

1.2. TOE 参照

TOE 名：NEC グループ 情報漏洩防止システム
TOE のバージョン：V1.0

1.3. TOE 概要

1.3.1. TOE の使用法及び主要なセキュリティ機能の特徴

本TOEは、NECグループ全体に導入される情報漏洩防止システムである。管理者が利用者毎に付与する権限に従ったPC制御方針を作成し、これを利用者のPCに適用することにより、PCからの情報持ち出しにかかわる操作を制限し、情報漏洩を防止する。

本TOEの主要なセキュリティ機能は、識別認証機能、アクセス制御機能、暗号機能及び監査機能である。

・識別認証機能
　-利用者を識別認証する機能
・アクセス制御機能
　-I/O ポート、プリンタへの入出力を制御する機能
　-利用者プログラムの実行を制御する機能
　-許可外部メディアへのファイルの出力を制御する機能
　-許可 USB デバイスへのファイルの入出力を制御する機能
　-クライアント制御情報の作成及び変更を制御する機能
・暗号機能
　-ファイルの暗号化／復号を行う機能
　-暗号化／復号のための鍵の生成を行う機能
　-許可外部メディアおよび許可 USB デバイスへのファイル出入力時に暗号化／復号を行う機能

・監査機能
-ログを生成し、ログサーバに転送する機能
-ログサーバに蓄積されたログの閲覧・検索を行う機能

1.3.2. TOE 種別

TOE は、NEC グループ社員向けの情報漏洩防止のためのソフトウェアである。

1.3.3. 必要な TOE 以外のハードウェア/ソフトウェア/ファームウェア

TOE を動作させるためのハードウェア/ソフトウェアを表 1-1 と表 1-2 に示す。

表 1-1 ハードウェア構成

機器名	種別	説明
ログサーバ	CPU	Pentium 4　3.0GHz 以上
	メモリ	2GB 以上
	HDD	100GB 以上
	グラフィック	1024×768 ピクセル以上の解像度 256 色以上のカラー表示
管理者端末、クライアント共通	CPU	Pentium Ⅲ　1.0GHz 以上
	メモリ	512MB 以上
	HDD	40GB 以上
	グラフィック	1024×768 ピクセル以上の解像度 256 色以上のカラー表示

表 1-2 ソフトウェア構成

機器名	種別	製品名
ログサーバ	ウイルス対策	Networks Associates Technology VirusScan Enterprise 8.0i
管理者端末	ウイルス対策	Networks Associates Technology VirusScan Enterprise 8.0i
クライアント	ウイルス対策	Networks Associates Technology VirusScan Enterprise 8.0i
	AP	一般 AP ファイル※

(※一般 AP ファイルは、TOE を動作させるために必要ではないが、TOE のアクセス制御の対象となるため記載している)

1.4. TOE 記述

1.4.1. システム利用方法

管理者は、ログサーバと管理者端末のセットアップを行う。管理者は一般利用者用のクライアント制御情報の作成、クライアントセットアップイメージの作成、ファイル暗号用共通鍵の作成及び暗号鍵入力制御情報の作成を行うとともに、ログサーバに蓄積されたログの閲覧・検索を行い、必要に応じて個々に作成したクライアント制御情報の更新を行う。

また、クライアントに対して、パスワードの強制変更、及び NEC グループ情報漏洩防止システム V1.0 クライアントアプリケーションソフトウェア Ver1.0 のアンインストールを行うことができる。

なお、クライアント制御情報の作成は、表 1-5 TOE のガイダンス文書に基づき、各部署や各利用者のシステムの利用状況を考慮したセキュアな値を設定する。

一般利用者は、クライアントをセットアップする場合は、あらかじめ NEC グループ標準の禁止対象ソフトウェアリストに記載されているソフトウェアを削除しておき、管理者から配付されたクライアントセットアップイメージを使ってクライアントをセットアップする。そして配付された暗号鍵入力制御情報を使ってファイル暗号用共通鍵を取り込むことによりセットアップを終了する。セットアップ後、管理者から通知された一般利用者ＩＤ、一般利用者パスワードを使ってクライアントにログオンし、I/O ポート、利用者プログラム、プリンタ及び許可外部メディアをクライアント制御情報に基づき利用することができる。その他、管理者からの指示によりクライアント制御情報のみを入手し、個別に適用する。(ただし、一般利用者はクライアント制御情報の設定内容を変更することはできない。)

クライアント制御情報の詳細を、表 1-3 に示す。

表 1-3 クライアント制御情報の詳細

制御項目	概要
一般利用者ＩＤ	TOE の一般利用者を識別するための ID
一般利用者パスワード	TOE の一般利用者を認証するためのパスワード
パスワード桁数	認証するためのパスワードの最小文字数
パスワード有効期限	設定したパスワードの有効日数
監査証跡の警告サイズ	利用者に対して警告を発するための監査証跡容量に対するログの使用割合の値
連続認証失敗許容回数	PC ロックされるまでのログオン連続失敗回数
許可外部メディア入出力制御情報	許可外部メディアに対して利用の可否を制御する情報
許可 USB デバイス入出力制御情報	許可 USB デバイスに対して利用の可否を制御する情報

制御項目	概要
再認証時間	TOE 利用時、再認証が要求されるまでの TOE の連続した未操作時間
I/O ポート利用制御情報	I/O ポートに対して利用の可否を制御する情報
プリンタ利用制御情報	プリンタの利用の可否、一部利用の許可を制御する情報
許可されたプリンタ情報	プリンタの一部利用が許可された場合の許可されたプリンタの詳細情報
外部メディア出力制御情報	外部メディアへのファイル出力の可否を制御する情報
抑止される利用者プログラム情報	利用を禁止するプログラムの名称

本 TOE は、各部署単位で構成する Windows ネットワーク のワークグループで運用される。

また、ログサーバ及び管理者端末においては、Administrator 権限で運用するが、クライアントの通常利用においては、Administrator 権限以外の任意の OS のユーザ権限で運用するものとする。

なお、ログサーバ、管理者端末、クライアント及び外部メディアについては、私物の紛失及び盗難を管理できないため、社内規程や資産管理システムにより管理された社有品のみ利用が許可されており、クライアントについては管理者経由で一般利用者に貸与される。

1.4.2. TOE 関連の利用者役割

TOE に関連する者は、管理者、クライアント管理者、一般利用者、システム責任者及び社内 LAN 管理者である。TOE の直接の利用者は、管理者、クライアント管理者及び一般利用者のいずれかに分類され、それぞれ利用者毎に付与された権限の範囲の業務を行うことができる。TOE に関連する全ての利用者は、就業規則や社内規定に従う。

(1)管理者

TOE の利用にあたり、各部署において、システム責任者がその役割を理解させた上で任命する者であり、各部署のクライアント及びログサーバの管理を行う。また、以下の役割がある。

・利用者 ID／パスワードの設定
・クライアントセットアップイメージの作成、配付
・クライアント制御情報の作成、配付
・ファイル暗号用共通鍵の作成、配付
・暗号鍵入力制御情報の作成、配付
・許可外部メディアの登録、配付

・ログの閲覧検索

(2)クライアント管理者

管理者がその任を兼務し各部署のクライアントの管理を行う。また、以下の役割がある。

・クライアントのパスワードの強制変更
・クライアントからの NEC グループ情報漏洩防止システム V1.0 クライアントアプリケーションソフトウェア Ver1.0 のアンインストール

(3)一般利用者

管理者により作成されたクライアント制御情報に基づき、クライアントを利用する者である。一般利用者は、以下の役割がある。

・クライアントの利用
・管理者から配付されたクライアント制御情報の取り込み
・管理者から配付されたファイル暗号用共通鍵の取り込み

(4)システム責任者

NEC グループの各部署において、信頼できる管理者を厳選し、その役割を理解させた上で任命する者である。

(5)社内 LAN 管理者

NEC グループのイントラネットの運用・保守を行う者である。

1.4.3. TOE の物理的な範囲

TOE の動作環境、コンポーネント及びガイダンス文書の構成を示す。

1.4.3.1. TOE の動作環境

TOE が稼動するログサーバ､管理者端末及びクライアントと関連する IT 機器及びネットワーク構成を図 1-1 に示す。

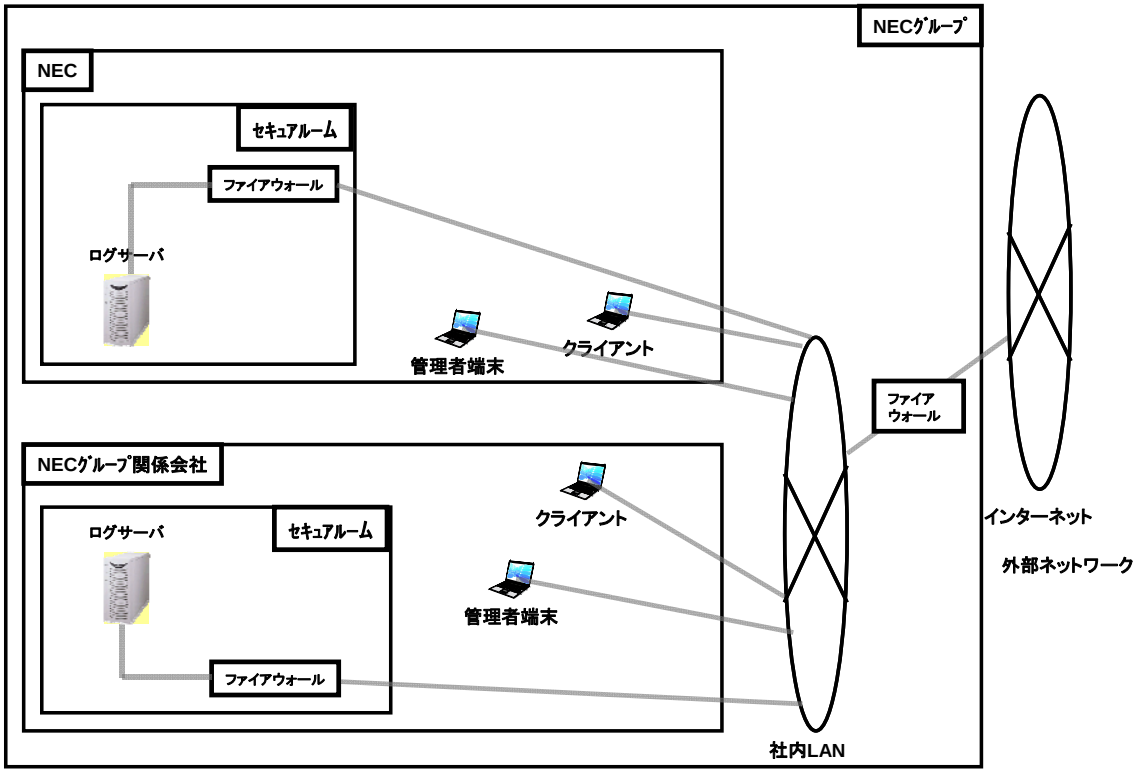

図 1-1 NEC グループ 情報漏洩防止システム動作環境

(1)物理的な配置とネットワーク

TOE が稼動するログサーバ、管理者端末及びクライアントは、社内 LAN に接続され、NEC グループ社員または NEC グループ社員に許可された者のみが入館できるよう入館管理された建物内に設置される。また、ログの保管されるログサーバは、物理的に隔てられ、別途入退室管理された部屋（以下、「セキュアルーム」という。）内の施錠可能なラック内で管理される。

セキュアルームは、管理者及び管理者が入室を許可した者の入室が許可される。管理者は、自らが入室を許可した者に対し、同行及び行動の監視を行う。

(2)社内 LAN

社内 LAN は、適切に設定されたファイアウォールを介して外部ネットワークと接続されている。また、セキュアルームのネットワークは、適切に設定されたファイアウォールを介してログサーバと管理者端末及びクライアントが通信できるように、社内 LAN に接続している。

(3)クライアント

クライアントは、一般利用者またはクライアント管理者により、社内 LAN に接続し利用される。クライアントで生成されたログは、社内 LAN を介して、ログサーバに転送される。

(4)管理者端末

管理者端末は、管理者により社内 LAN に接続し利用される。管理者端末で生成されたログはログサーバへ転送される。管理者端末は社内 LAN を介してログサーバ上のログを閲覧・検索する。

(5)ログサーバ

ログサーバは、NEC グループのセキュアルームに設置され、ファイアウォールを介して社内 LAN に接続される。管理者端末及びクライアントから転送されたログを蓄積する。

1.4.3.2. TOE のコンポーネント

図 1-2 の破線内に示されるソフトウェアが TOE の物理的範囲である。

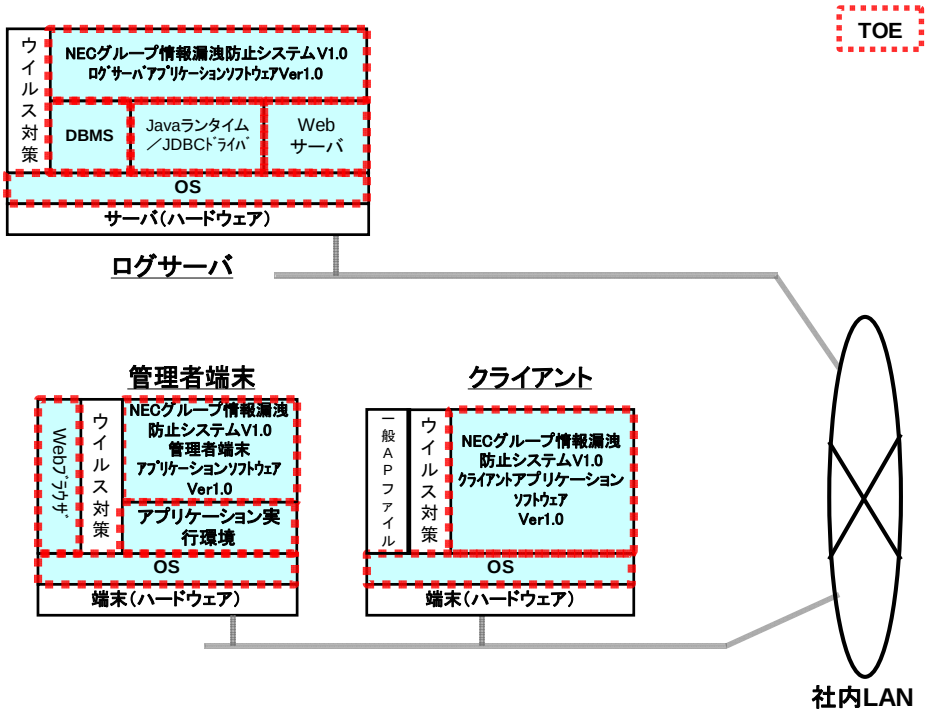

図 1-2 NEC グループ 情報漏洩防止システムのコンポーネント

TOE のソフトウェアコンポーネント名とバージョンを表 1-4 に示す。

表 1-4 TOE のソフトウェアコンポーネント

機器名	種別	ソフトウェアコンポーネント名
ログサーバ	AP	NEC グループ 情報漏洩防止システム V1.0 ログサーバアプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows Server 2003 Standard Edition（SP1）
	DBMS	Microsoft SQL Server 2005 Standard Edition（SP1）
	JDBC ドライバ	Microsoft SQL Server 2005 JDBC Driver Ver1.0
	Web サーバ	Apache Tomcat 5.5.17 Apache Axis 1.4
	Java ランタイム	Sun Java Runtime Environment (JRE) 5.0 Update 11
管理者端末	AP	NEC グループ 情報漏洩防止システム V1.0 管理者端末アプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows XP Professional（SP2）
	Web ブラウザ	Microsoft Internet Explorer 6.0（SP2）
	アプリケーション実行環境	Microsoft .NET Framework 2.0 Microsoft .NET Framework 2.0 日本語 Language Pack
クライアント	AP	NEC グループ 情報漏洩防止システム V1.0 クライアントアプリケーションソフトウェア Ver1.0
	OS	Microsoft Windows XP Professional（SP2）

図 1-2 において、表 1-4 で示した TOE ソフトウェアコンポーネント以外のハードウェア及びソフトウェアコンポーネントは TOE 範囲外である。TOE 範囲外のハードウェア及びソフトウェアコンポーネントについて、表 1-1 及び表 1-2 に示す。

1.4.3.3. TOE のガイダンス文書

TOE のインストール及び運用で利用するガイダンス文書を表 1-5 に示す。

表 1-5 TOE のガイダンス文書

種類	ガイダンス文書名
インストールガイダンス	NEC グループ 情報漏洩防止システム V1.0 インストールガイド
利用者操作ガイダンス	NEC グループ 情報漏洩防止システム V1.0 管理者ガイド
	NEC グループ 情報漏洩防止システム V1.0 利用者ガイド

1. 4. 4. TOE の論理的な範囲

図 1-3 の破線内に示される範囲が TOE の論理的範囲である。

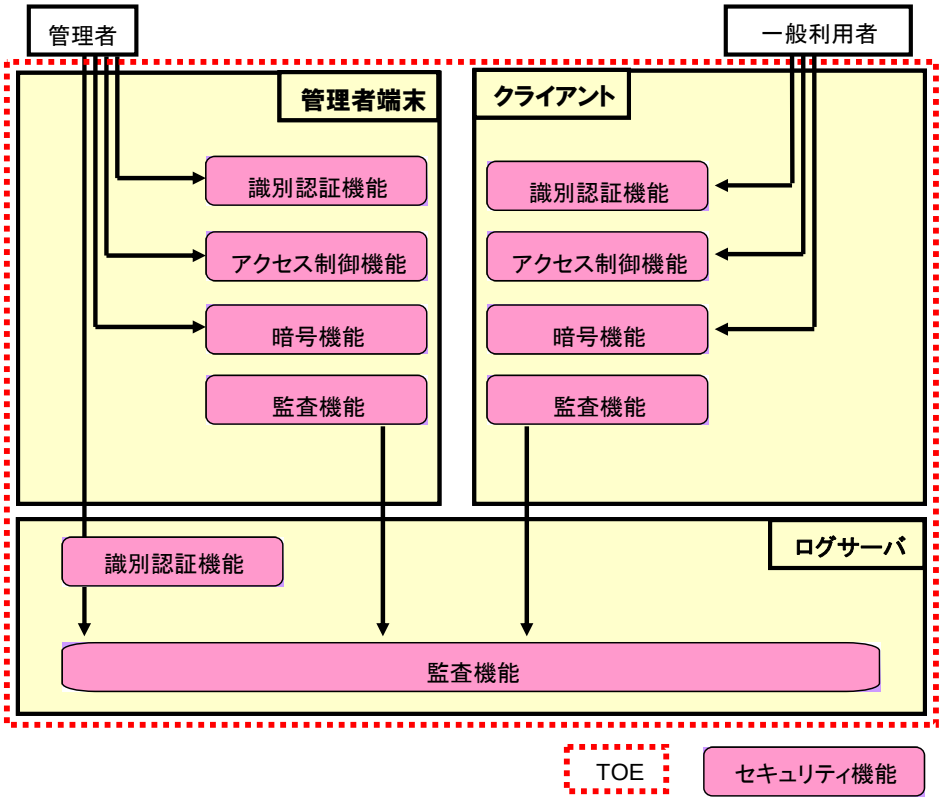

図 1-3 NEC グループ 情報漏洩防止システム論理構成図

図 1-3 に示した、TOE によって提供されるセキュリティ機能について次項で説明する。

1.4.4.1. TOE によって提供されるセキュリティ機能

(1) 監査機能

(管理者端末、クライアント)

・管理者端末及びクライアントのログの生成及びログサーバへの送信

・ログのログサーバへの送信時の転送保護

(ログサーバ)

・ログサーバの DB に蓄積されたログの閲覧・検索

(2) 識別認証機能

※本項で記述する識別認証機能は、管理者端末、クライアント及びログサーバ上の AP である「NEC グループ情報漏洩防止システム V1.0 管理者端末アプリケーションソフトウェア Ver1.0」、「NEC グループ情報漏洩防止システム V1.0 クライアントアプリケーションソフトウェア Ver1.0」及び「NEC グループ情報漏洩防止システム V1.0 ログサーバアプリケーションソフトウェア Ver1.0」によって提供される識別認証機能であり、OS により提供される識別認証機能ではない。

（管理者端末）
・管理者が管理者端末にログオンする際の識別認証
・一定時間管理者からのアクセスがない場合の PC ロックから復旧する際の識別認証
・管理者パスワードの変更

（クライアント）
・一般利用者またはクライアント管理者がクライアントにログオンする際の識別認証
・一定時間一般利用者からのアクセスがない場合の PC ロックから復旧する際の識別認証
・一般利用者パスワードの変更

（ログサーバ）
・管理者がログサーバに蓄積されたログを閲覧、検索する際の識別認証の実施

(3) アクセス制御機能
（管理者端末）
・クライアント制御情報の作成、変更

（クライアント）
・クライアント制御情報の参照
・クライアント制御情報に基づき以下を実施
　－I/O ポート及びプリンタの利用可否の設定の制御
　－一般 AP ファイルの実行及びファイル名称変更の制御
　－許可外部メディアへのファイル出力の制御
　－許可 USB デバイスへのファイル入出力の制御

(4) 暗号機能
（管理者端末）

・クライアントを利用する一般利用者が、入手、作成した任意のデータファイルを暗号化／復号するための暗号鍵ファイルの生成

（クライアント）

・クライアントを利用する一般利用者が、入手、作成した任意のデータファイルを暗号化／復号するための鍵の読み込み、削除

・クライアントを利用する一般利用者が、入手、作成した任意のデータファイルの暗号化／復号

・許可外部メディアへの出入力時のファイルの暗号化／復号

1.4.5. TOE 資産

本 TOE の資産は、以下の TSF データ及び利用者データである。

＜TSF データ＞

管理者端末及びクライアント上の TSF データには以下のものがある。

・管理者ＩＤ
・管理者パスワード
・LogViewer 起動制御情報
・クライアント制御情報（表 1-3 参照）
・ログ

＜利用者データ＞

クライアント上の利用者データには以下のものがある。

・一般 AP ファイル
・一般 AP ファイルにより作成され、クライアント上で管理されるデータ

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、以下の通り 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　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
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、以下の通りパッケージ適合を主張する。

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

本 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及び前提条件について記述する。

3.1. 脅威

TOE の脅威エージェントの考察は以下のとおりである。

第 1.4.2 節で識別された人物のうち、システム責任者、LAN 管理者及び TOE の管理者は信頼できる人物であり、TOE の利用に関して不正を行うことはない。一方、一般利用者は、就業規則や社内規定により悪意をもって TOE を攻撃することは考えられないが、興味本位で自分以外のクライアントの利用やクライアントに対する許可されない操作をすることが考えられる。

管理者端末は、社内のみでの使用に限定しており、社内 LAN に接続して使用する。一方クライアント及び外部メディアは、社内での使用以外に社外に持ち出されることもある。社外に持ち出されたクライアント及び外部メディアは、NEC グループ外の者（以下、「第三者」と呼ぶ）により不正に利用されることが考えられる。

T.INJUSTICE_LOGON（不正なログオン）
一般利用者及び第三者が、TOE の正当な利用者になりすまして、利用者データまたは TSF データを改ざん、暴露するかもしれない。

T.UNAUTHORIZED_ACCESS（許可されない操作）
一般利用者が、許可されない操作（許可されていないプリンタへの出力、許可されていないプログラムの実行、許可されていない I/O ポートの利用）を実行することで、クライアントに保存された利用者データを暴露するかもしれない。

T.INJUSTICE_CONNECT（不正な装置の接続）
第三者が、不正な装置に外部メディアまたはクライアントの HDD を接続することにより、外部メディアまたはクライアントの HDD に保存された利用者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

組織のセキュリティ方針を以下に示す。

P.LOG_COLLECT（ログの集約）
管理者端末及びクライアントで収集されたログは、ログサーバにセキュアに集約される。

P.RESTRICTED_MEDIA（許可外部メディアのみの使用）
クライアントから書き込みできる外部メディアは、許可された外部メディアのみとする。

P.SECURITY_PARAMETER（適切なセキュリティパラメータ設定）
管理者は、TOE のガイダンス文書に基づきクライアント制御情報を適切な値に設定する。

3.3. 前提条件

前提条件を以下に示す。

A.MANAGE_SAFE_PLACE（管理者端末の安全な設置）
管理者端末は、NEC グループ社員及び NEC グループ社員が許可した者のみが入館できる建物内に設置される。

A.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）
ログサーバ及びログのバックアップ媒体は、入退室管理された室内に設置されなければならない。

A.UNJUST_SOFTWARE（不正ソフトウェア対策）
TOE が動作するログサーバ、管理者端末及びクライアントには、ウイルス対策ソフトウェアが導入されるとともに、ウイルス対策ソフトウェアのパターンファイルや、TOE のコンポーネントの一部である OS のセキュリティ対策用修正ソフトウェアが適切に適用される。

A.PASSWORD_MANAGEMENT（パスワードの管理）
TOE の利用者は、TOE にアクセスするためのパスワードを他人に知られないよう管理する。また TOE の利用者は、推測されにくいパスワードを設定し、適切な頻度で変更する。

A.NETWORK（ネットワーク環境）
社内 LAN と外部ネットワークは、外部ネットワークからの不正な通信を防ぐ装置を介して接続される。またセキュアルームのネットワークは、ログサーバ、管理者端末及びクライアントとの通信に必要なプロトコルのみ許可する装置を介して社内 LAN に接続される。

A.OPERATOR_MANAGEMENT（管理者の管理）
管理者は、信頼できる者であり、不正な操作を行なわない。

A.LOG_BACKUP（ログのバックアップ）
ログサーバのログは、消失から防止されなければならない。

A.PC_STARTUP_SET（PC の起動制御設定）
一般利用者に貸与される PC は、保守モードでの起動ができないように設定されなければならない。

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示す。

O.I&A（利用者の識別認証）
TOE は、利用者が TOE を利用するときは、利用者を識別認証しなければならない。また、TOE は設定された回数以内に識別認証に成功した利用者のみ TOE の利用を許可しなければならない。

O.RE_AUTH（再認証）
TOE は、TOE にログオンした利用者からの一定時間 TOE へのアクセスがないとき、再認証を要求しなければならない。再認証を要求している間は、TOE の他の機能の利用を制限しなければならない。

O.ACCESS_CONTROL（アクセス制御）
TOE は、利用者に付与された設定・権限に従って、利用者を代行するプロセスによる操作を制御しなければならない。

O.AUDIT（監査）
TOE は、TOE のセキュリティ機能に関連する事象をログとして記録し、そのログを保護しなければならない。また、TOE は管理者のみにログの参照を制限しなければならない。

O.ACCESS_CONTROL_MEDIA（外部メディアのアクセス制御）
TOE は、一般利用者による外部メディアへの書き込みを制限しなければならない。

O.CRYPTOGRAPHY（暗号化）
TOE は、外部メディアまたはクライアントに利用者データを保存するときは、利用者データを暗号化しなければならない。

O.LOG_COLLECT（ログの集約）
TOE は、管理者端末、クライアントで生成されたログをログサーバにセキュアに転送する。

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示す。

OE.SECURITY_PARAMETER（適切なセキュリティパラメータ設定）

管理者は、TOE をセキュアに運用するために、ガイダンスの記述にしたがって、クライアント制御情報を適切な値に設定しなければならない。

OE.MANAGE_PC_PLACE（管理者端末の安全な設置）
管理者端末は、NEC グループ社員及び NEC グループ社員によって許可された者のみが入退館管理される建物内に設置され、管理者端末の操作及び運用は同所で行われなければならない。

OE.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）
ログサーバは、入退室管理された室内に設置し、管理者のみがアクセス可能な施錠されたラックに設置しなければならない。また、ログのバックアップ媒体は、入退室管理された室内の管理者のみがアクセス可能なキャビネットに保管しなければならない。なお、管理者は、自身が許可した者を入室させた場合は、その者の行動を監視しなければならない。

OE.UNJUST_SOFTWARE（不正ソフトウェア対策）
利用者は、ログサーバ、管理者端末及びクライアントにウイルス対策ソフトウェアをインストールし、ウイルスパターンファイルを常に最新に更新しなければならない。また、TOE のコンポーネントの一部である OS は、セキュリティ対策修正ソフトウェアを適切に適用しなければならない。

OE.PASSWORD_MANAGEMENT（パスワードの管理）
TOE の利用者は、TOE にアクセスするためのパスワードを記憶し、他人に漏らしてはならない。 また、TOE 利用者は、パスワードを推測・解析されにくい設定にし、適切な間隔で変更しなければならない。

OE.NETWORK（ネットワーク環境）
社内 LAN は、適切に設定されたファイアウォールを介して外部ネットワークと接続しなければならない。また、セキュアルームのネットワークは、適切に設定されたファイアウォールを介してログサーバと管理者端末及びクライアントが通信できるように、社内 LAN に接続しなければならない。

OE.OPERATOR_MANAGEMENT（管理者の管理）
システム責任者は、不正を行わない信頼できる管理者を任命しなければならない。また、システム責任者は、管理者が不正を行わないように監督し、管理者が適切に TOE を運用できるように指導しなければならない。

OE.LOG_BACKUP（ログのバックアップ）
ログサーバのログが消失しないように、定期的にバックアップをとらなければならない。

OE.LOG_COLLECT（ログの集約）
管理者端末及びクライアントのログは、集約するため定期的にログサーバに送信しなければならない。

OE.USERDATA_CRYPTOGRAPHY（利用者データの暗号化指定）
利用者は、管理者端末、クライアントまたは外部メディアに利用者データを保存する場合は、暗号用フォルダに保存するかまたはファイルを暗号化して保存しなければならない。

OE.PC_STARTUP_SET（PC の起動制御設定）
管理者は、一般利用者に貸与する PC において、保守モードで起動しないように設定を行わなければならない。

4.3. セキュリティ対策方針根拠

セキュリティ対策は、本章で規定した脅威に対抗するためのものである。あるいは、TOE の前提条件と組織のセキュリティ方針を実現するためのものである。 セキュリティ対策方針と対抗する脅威及び対応する組織のセキュリティ方針及び前提条件の対応関係を表 4-1 に示す。

表 4-1 セキュリティ対策方針とセキュリティ課題定義の対応関係

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.INJUSTICE_LOGON	T.UNAUTHORIZED_ACCESS	T.INJUSTICE_CONNECT	P.LOG_COLLECT	P.RESTRICTED_MEDIA	P.SECURITY_PARAMETER	A.MANAGE_SAFE_PLACE	A.FACILITIES_IN_SECURE_ROOM	A.UNJUST_SOFTWARE	A.PASSWORD_MANAGEMENT	A.NETWORK	A.OPERATOR_MANAGEMENT	A.LOG_BACKUP	A.PC_STARTUP_SET
O.I&A	×													
O.RE_AUTH	×													
O.ACCESS_CONTROL		×												
O.AUDIT		×												
O.ACCESS_CONTROL_MEDIA					×									

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.INJUSTICE_LOGON	T.UNAUTHORIZED_ACCESS	T.INJUSTICE_CONNECT	P.LOG_COLLECT	P.RESTRICTED_MEDIA	P.SECURITY_PARAMETER	A.MANAGE_SAFE_PLACE	A.FACILITIES_IN_SECURE_ROOM	A.UNJUST_SOFTWARE	A.PASSWORD_MANAGEMENT	A.NETWORK	A.OPERATOR_MANAGEMENT	A.LOG_BACKUP	A.PC_STARTUP_SET
O.CRYPTOGRAPHY			×											
O.LOG_COLLECT				×										
OE.SECURITY_PARAMETER						×								
OE.MANAGE_PC_PLACE							×							
OE.FACILITIES_IN_SECURE_ROOM								×						
OE.UNJUST_SOFTWARE									×					
OE.PASSWORD_MANAGEMENT										×				
OE.NETWORK											×			
OE.OPERATOR_MANAGEMENT												×		
OE.LOG_BACKUP													×	
OE.LOG_COLLECT				×										
OE.USERDATA_CRYPTOGRAPHY			×											
OE.PC_STARTUP_SET														×

表 4-1 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及び前提条件に対応している。
次に、各脅威がセキュリティ対策方針で対抗できること、また各組織のセキュリティ方針・前提条件がセキュリティ対策方針で実現できることを説明する。

○脅威

脅威に対して想定される全ての攻撃方法に対抗する対策方針の正当化を以下に示す。

T.INJUSTICE_LOGON（不正なログオン）

この脅威は、一般利用者及び第三者が、正当な利用者になりすましてクライアントや管理者端末を利用することである。この脅威に有効な対抗策について以下に述べる。

ａ．利用を許可されていない者が、正当な利用者になりすます。

この攻撃に対しては、利用者の利用において識別・認証を行い、TOE の利用を正当な利用者のみに制限することにより脅威を軽減できる。この対抗策に該当するセキュリティ対策方針は、O.I&A である。

b. 一般利用者が、正当な利用者の離席時に正当な利用者になりすます。

この攻撃に対して、一定時間 TOE が未操作の場合、TOE は再認証を要求し、要求している間は TOE の他の機能の利用を制限することにより脅威を軽減できる。この対抗策に該当するセキュリティ対策方針は、O.RE_AUTH である。

以上、a、b 全ての攻撃方法に対抗することは、T.INJUSTICE_LOGON に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.I&A、O.RE_AUTH によって、T.INJUSTICE_LOGON に対抗できる。

T.UNAUTHORIZED_ACCESS（許可されない操作）

この脅威は、一般利用者によって実行される。一般利用者がとり得る、故意または誤操作により許可されていない操作を行う脅威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行う。

この攻撃に対しては、TOE の各操作（プリンタへの出力、利用者プログラムの実行、I/O ポートへの入出力）に対して利用者毎に権限を設定し、許可／禁止される操作を明確にすることにより脅威を除去できる。この対抗策に該当するセキュリティ対策方針は、O.ACCESS_CONTROL である。さらに、正確な時刻をもって利用者プログラムの実行に関するログを記録することによって“ログを記録されていること”は、つまり“操作を監視されている”という利用者への意識付けにつながり、これによって許可されない操作（許可されていない利用者プログラムの実行）が抑止可能となり、結果的に脅威を軽減できる。この対抗策に該当するセキュリティ対策方針は、O.AUDIT である。

以上の攻撃方法に対抗することは､T.UNAUTHORIZED_ACCESS に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.ACCESS_CONTROL 及び O.AUDIT によって、T.UNAUTHORIZED_ACCESS に対抗できる。

T.INJUSTICE_CONNECT（不正な装置の接続）

外部メディアやクライアントの盗難や紛失により、第三者による利用者データの暴露に対する有効な対抗策について以下に述べる。

a. 第三者が外部メディアを入手し、利用者データを暴露する。

この攻撃に対しては、外部メディアに保存される利用者データを暗号化し、許可された者のみが利用者データを復号できるようにすることにより脅威を軽減できる。この対抗策に該当するセキュリティ対策方針は、O.CRYPTOGRAPHY である。

ｂ．第三者がクライアントを入手し、利用者データを暴露する。

この攻撃に対しては、クライアントに保存される利用者データを暗号化し、許可された者のみが利用者データを復号できるようにすることにより脅威を軽減できる。この対抗策に該当するセキュリティ対策方針は、O.CRYPTOGRAPHY 及び

OE.USERDATA_CRYPTOGRAPHY である。

以上の攻撃方法に対抗することは、T.INJUSTICE_CONNECT に対抗することである。したがって、それぞれの攻撃方法に対する対抗策として該当する、O.CRYPTOGRAPHY 及び OE.USERDATA_CRYPTOGRAPHY によって、T.INJUSTICE_CONNECT に対抗できる。

○組織のセキュリティ対策方針

P.LOG_COLLECT（ログの集約）

この組織のセキュリティ方針は、ログを保管するログ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. ログのログサーバへのセキュアな集約

管理者端末及びクライアントで生成されたログは、ログサーバのログ DB に秘匿化された通信方法を用いて集約される。この方針に応じるための TOE セキュリティ対策方針は、O.LOG_COLLECT である。

b. ログのログサーバへの定期的な集約

管理者端末及びクライアントで生成されたログは、管理者が一元管理できるようにするため、ログサーバのログ DB に定期的に集約される。この方針に応じるための TOE セキュリティ対策方針は、OE.LOG_COLLECT である。

以上、上記に応じることは、P.LOG_COLLECT に応じることである。したがって、それぞれの要求に応じる対応策として該当する O.LOG_COLLECT 及び OE.LOG_COLLECT の達成によって P.LOG_COLLECT が実現される。

P.RESTRICTED_MEDIA（許可外部メディアのみの使用）

この組織のセキュリティ方針は、TOE は許可された外部メディアのみ使用を許可するものである。有効な対策方針について以下に述べる。

a. 許可外部メディアへの書き込み制限

一般利用者の外部メディアへの書き込みを許可された外部メディアにのみ制限することにより、利用できる外部メディアを許可外部メディアのみに制限することができる。この方針に応じるための TOE セキュリティ対策方針は O.ACCESS_CONTROL_MEDIA である。

以上、上記に応じることは、P.RESTRICTED_MEDIA に応じることである。したがって、それぞれの要求に応じる対応策として該当する O.ACCESS_CONTROL_MEDIA の達成によって P.RESTRICTED_MEDIA が実現される。

P.SECURITY_PARAMETER（適切なセキュリティパラメータ設定）

この組織のセキュリティ方針は、管理者が設定するセキュリティパラメータに関するもの

である。有効な対策方針について以下に述べる。

a. セキュアな変数設定

管理者は TOE をセキュアに運用するためガイダンスの記述に従い、クライアント制御情報を適切な値に設定する。この方針に応じるための運用環境のセキュリティ対策方針は、OE.SECURITY_PARAMETER である。

以上、上記に応じることは、P.SECURITY_PARAMETER に応じることである。したがって、それぞれの要求に応じる対応策として該当する、OE.SECURITY_PARAMETER の達成によって P.SECURITY_PARAMETER が実現される

○前提条件

A.MANAGE_SAFE_PLACE（管理者端末の安全な設置）

この前提条件は、TOE に関連するハードウェア（管理者端末）の設置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. 管理者端末を設置する場所の制限。

クライアント制御情報の作成や利用者データファイルの暗号化／復号を行うための暗号鍵の作成、配付、管理を行う管理者端末は NEC グループ社員及び NEC グループ社員に許可された者のみが入館可能な建物内に設置する。この方針に応じるための運用環境のセキュリティ対策方針としては、OE.MANAGE_PC_PLACE である。

以上、上記に応じることは、A.MANAGE_SAFE_PLACE に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.MANAGE_PC_PLACE の達成によって A.MANAGE_SAFE_PLACE が実現される。

A.FACILITIES_IN_SECURE_ROOM（セキュアルームへの機器設置）

この前提条件は、TOE に関連するハードウェア（ログサーバ）の設置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. ログが格納される機器を設置する部屋を制限する。

ログが格納されるハードウェア（ログサーバ）は、管理者、及び管理者に許可された者のみが入室可能な室内に設置する。

また、ログサーバ及びログのバックアップ媒体は、セキュアルーム内設置された、管理者のみがアクセス可能なラックまたはキャビネットに保管する。この方針に応じるための運用環境のセキュリティ対策方針は、OE.FACILITIES_IN_SECURE_ROOM である。

b. 入室を許可する者を制限する。

入室が許可される者は、管理者として許可されている者、及び管理者に許可された者のみとする。この方針に応じるための運用環境のセキュリティ対策方針は、

OE.FACILITIES_IN_SECURE_ROOM である。

以上、a、b 全てに応じることは、A.FACILITIES_IN_SECURE_ROOM に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、
OE.FACILITIES_IN_SECURE_ROOM の達成によって
A.FACILITIES_IN_SECURE_ROOM が実現される。

A.UNJUST_SOFTWARE（不正ソフトウェア対策）

この前提条件は、コンピュータウイルス及びセキュリティ対策用修正ソフトウェア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 関連ハードウェアにウイルス対策ソフトウェアを導入する。
TOE 関連ハードウェア（ログサーバ、管理者端末、クライアント）に、ウイルス対策ソフトウェアを導入する。この方針に応じるための運用環境におけるセキュリティ対策方針は、OE.UNJUST_SOFTWARE である。

b. パターンファイル、及びセキュリティ対策用修正ソフトウェアを適切に適用する。
ウイルス対策ソフトウェアのパターンファイル、及びセキュリティ対策用修正ソフトウェアの適用について、常に最新のものが適用される。この方針に応じるための運用環境におけるセキュリティ対策方針は、OE.UNJUST_SOFTWARE である。

以上、上記 a、b 全てに応じることは、A.UNJUST_SOFTWARE に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.UNJUST_SOFTWARE の達成によって A.UNJUST_SOFTWARE が実現される。

A.PASSWORD_MANAGEMENT（パスワードの管理）

この前提条件は、管理者の管理するパスワード、クライアント管理者の管理するパスワード及び一般利用者の管理するパスワード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. パスワードの適切な管理。
管理者、クライアント管理者及び一般利用者は、TOE にアクセスするためのパスワードを自分以外の他人に知られないように秘匿する。この方針に応じるための運用環境のセキュリティ対策方針は、OE.PASSWORD_MANAGEMENT である。

b. パスワードの定期的な変更。
管理者、クライアント管理者及び一般利用者は、TOE にアクセスするためのパスワードを、適切な間隔で定期的に変更する。この方針に応じるための運用環境のセキュリティ対策方針は、OE.PASSWORD_MANAGEMENT である。

以上、上記 a、b 全てに応じることは、A.PASSWORD_MANAGEMENT に応じることで

ある。したがって、それぞれの要求に応じる対抗策として該当する、OE.PASSWORD_MANAGEMENT の達成によって A.PASSWORD_MANAGEMENT が実現される。

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. 社内 LAN と外部ネットワークとの接続を制限する。

社内 LAN と外部ネットワークとの接続は、外部ネットワークからの不正な通信を防ぐ装置（ファイアウォール）を介して接続する。この方針に応じるための運用環境のセキュリティ対策方針は、OE.NETWORK である。

b. セキュアルームのネットワークへの接続を制限する。

TOE（ログサーバ）が接続されるセキュアルーム内のネットワークと社内 LAN は、適切に設定されたファイアウォールを介してログサーバと管理者端末及びクライアントが通信できるように接続する。この方針に応じるための運用環境のセキュリティ対策方針は、OE.NETWORK である。

以上、上記の a、b 全てに応じることは、A.NETWORK に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.NETWORK の達成によって A.NETWORK が実現される。

A.OPERATOR_MANAGEMENT（管理者の管理）

この前提条件は、管理者の選任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. 信頼できる者の選任。

管理者については、システム責任者により、社員の中から選任され、その役割及び責任を良く理解し、職務に忠実で決して悪意を抱かない者とする。この方針に応じるための運用環境のセキュリティ対策方針は、OE.OPERATOR_MANAGEMENT である。

b. システム責任者による監督。

システム責任者は、管理者に日ごろの活動状況を報告させ、不正を行わないように監督するとともに、TOE を適切に運用できるように、教育を受けさせ指導する。この方針に応じるための運用環境のセキュリティ対策方針は、OE.OPERATOR_MANAGEMENT である。

以上、上記 a、b 全てに応じることは、A.OPERATOR_MANAGEMENT に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.OPERATOR_MANAGEMENT の達成によって A.OPERATOR_MANAGEMENT が

実現される。

A.LOG_BACKUP（ログのバックアップ）
この前提条件は、ログを格納するログサーバ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. DB に格納されたログの適切な保護。
ログサーバのログは、消失しないように定期的にバックアップされる。この方針に応じるための運用環境のセキュリティ対策方針は、OE.LOG_BACKUP である。
以上、上記に応じることは、A.LOG_BACKUP に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.LOG_BACKUP の達成によって A.LOG_BACKUP が実現される。

A.PC_STARTUP_SET（PC の起動制御設定）
この前提条件は、PC の起動設定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. PC の起動制御設定。
管理者は、一般利用者に PC を貸与する場合は、保守モードでの起動を抑止する設定を行ったうえで貸与する。これにより、保守モードよる PC の起動を防止することができる。この方針に応じるための運用環境のセキュリティ対策方針は、OE.PC_STARTUP_SET である。
以上、上記に応じることは、A.PC_STARTUP_SET に応じることである。したがって、それぞれの要求に応じる対抗策として該当する、OE.PC_STARTUP_SET の達成によって A.PC_STARTUP_SET が実現される。

5. 拡張コンポーネント定義

5.1. 拡張コンポーネント定義

本 ST は CC パート 2 及び CC パート 3 に適合しているので、拡張コンポーネントはない。

6. セキュリティ要件

本章では、セキュリティ機能要件、セキュリティ保証要件及びセキュリティ要件根拠について記述する。

なお、本章で使用する用語の定義は、以下のとおりである。

＜サブジェクト＞

サブジェクト	定義
管理者プロセス	管理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

＜オブジェクト＞

オブジェクト	定義
I/O ポート	クライアント制御情報に基づき、データの入出力に利用されるクライアントの I/O ポート
エクスポート暗号鍵ファイル	管理者端末からファイル暗号用共通鍵をエクスポートしたファイル
インポート暗号鍵ファイル	クライアントでファイル暗号用共通鍵をインポートするファイル
暗号鍵ファイル	クライアントでファイル暗号用共通鍵データを格納するファイル
一般 AP ファイル	クライアント制御情報に基づき、クライアント上で実行を制御されるプログラムファイル

＜操作＞

操作	定義
入力、出力	I/O ポートへのファイルの出力または I/O ポートからのファイルの入力
実行、ファイル名称変更	クライアント上での一般 AP ファイルの実行、ファイル名称の変更
書き出し、読み込み	エクスポート用暗号鍵ファイルへのデータの書き出し、インポート暗号鍵ファイルの読み込み及び暗号鍵ファイルの書き出し

＜セキュリティ属性＞

セキュリティ属性名	属性の内容	とり得る値
I/O ポート利用制御情報	USB ポート、IEEE1394 ポート、シリアル/パラレルポート、赤外線ポート、PCMCIA ポートの利用可否を指定する情報	有効、無効
プリンタ利用制御情報	プリンタの利用範囲を指	一部許可、すべてを許可、

セキュリティ属性名	属性の内容	とり得る値
	定する情報	すべてを拒否
許可されたプリンタ情報	プリンタを一意に特定する情報	ドライバ名、ポート名、サーバ名、プリンタ名、URL、IP アドレス
許可USBデバイス入出力制御情報	許可 USB デバイスの利用可否を制御する情報	メーカ ID、製品 ID、シリアル番号
外部メディア出力制御情報	外部メディアの利用範囲を指定する情報	許可外部メディアのみ利用可能、すべての外部メディアを利用禁止、すべての外部メディアを許可
許可外部メディア入出力制御情報	許可外部メディアの利用可否を制御する情報	グループ名、キーワード
ポート名	クライアント制御情報に基づき、データの入出力を制御するポートの名称	USB ポート、IEEE1394 ポート、シリアル/パラレルポート、赤外線ポート、PCMCIA ポート、プリンタポート
抑止される利用者プログラム情報	起動が抑止されるプログラム名称を指定する情報	プログラム名称を表す任意の文字列
ファイル名称	プログラムファイルに付与されたプログラムファイルの名称	255 文字以内の文字列
管理者ＩＤ	管理者に付与されたＩＤ	1 文字以上 127 文字以下の任意の文字列
一般利用者ＩＤ	一般利用者に付与されたＩＤ	1 文字以上 127 文字以下の任意の文字列
利用者ＩＤ	管理者ＩＤ及び一般利用者ＩＤの総称	1 文字以上 127 文字以下の任意の文字列
暗号鍵入力制御情報	ファイル暗号用共通鍵を読み込むための情報	8 文字以上 32 文字以下の半角英数字記号

＜その他の用語＞

用語	定義
イベントＩＤ	監査記録を識別する番号
イベントタイプ	監査記録の分類であり、エラー、警告、情報の 3 種類が存在
カテゴリ	監査記録の分類であり、管理者が監査記録を検索する際にキーワードとして使用できる
許可外部メディア用共通鍵	許可外部メディアへファイルを書き出す際の暗号化及び許可外部メディアからファイルを読み込む際の復号に使用する暗号鍵データ
ファイル暗号用共通鍵	利用者データを暗号化・復号する際に使用する暗号鍵データ
連続認証失敗許容回数	管理者端末及びクライアントの認証時に、連続し

用語	定義
	て失敗できる許容回数 この回数を超えると、一定時間 PC がロックされる
連続した不成功認証試行回数カウンタ	管理者端末及びクライアントの認証時に、連続した認証失敗回数を保持したカウンタ
再認証時間	ログオンした後、離席等した場合の TOE 未使用時間
メッセージ	監査記録に記録された事象の詳細な内容

6.1. セキュリティ機能要件

本章では、CC パート 2 で規定されている機能要件コンポーネントを直接使用する。

○セキュリティ監査（FAU）

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：から一つのみ選択]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：から一つのみ選択]：指定なし
[割付：上記以外の個別に定義した監査対象事象]：表 6-1 に示す。

表 6-1 個別に定義した監査対象事象

機能要件	監査対象事象
FDP_ACF.1a	・外部メディアへの書き込み成功、失敗
FDP_ACF.1b	・プログラムファイルの起動の成功、失敗 ・プログラムファイルの名称変更の失敗
FIA_AFL.1	・連続した不成功認証試行回数カウンタの閾値到達、それに続いてとられるアクション（PC の一定時間のロック）
FIA_UAU.2	・利用者の識別認証の成功、失敗
FIA_UAU.6	・利用者の識別認証の成功、失敗
FIA_UID.2	・利用者の識別認証の成功、失敗
FMT_MTD.1	・利用者 ID の登録、更新、削除の成功、失敗 ・利用者パスワードの登録、更新の成功、失敗

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 の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]：

・イベント ID

・カテゴリ（ログのカテゴリ分類を示すもの）

・PC 名

・IP アドレス

・MAC アドレス

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]：LogViewer 起動制御情報を入力した管理者

[割付：監査情報のリスト]：
{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、イベントＩＤ、メッセージ、PC 名、IP アドレス、MAC アドレス}

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_SAR.1 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。

[詳細化]：アクセスを承認された利用者 → アクセスを承認された管理者

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]：検索には以下の条件を指定できる。
・期間、時間帯
・利用者ＩＤ
・PC 名
・ＩＰアドレス
・ＭＡＣアドレス
・イベントタイプ
・カテゴリ
・イベントＩＤ

[選択：検索、分類、並べ替え]：検索

FAU_STG.1 保護された監査証跡格納
下位階層：なし
依存性：FAU_GEN.1 監査データ生成

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を[選択：防止、検出：から一つのみ選択]できなければならない。

[選択：防止、検出：から一つのみ選択]：防止

FAU_STG.3 監査データ消失の恐れ発生時のアクション
下位階層：なし
依存性：FAU_STG.1 保護された監査証跡格納

FAU_STG.3.1 TSF は、監査証跡が[割付：事前に定義された限界]を超えた場合、[割付：監査格納失敗の恐れ発生時のアクション]をとらなければならない。

[割付：事前に定義された限界]：管理者がクライアント制御情報に設定した監査証跡の警告サイズ

[割付：監査格納失敗の恐れ発生時のアクション]：管理者、一般利用者への通知を行う。

FAU_STG.4 監査データ損失の防止
下位階層：FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性：FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[選択：監査対象事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き、から 1 つのみ選択]及び[割付：監査格納失敗時にとられるその他のアクション]を行わなければならない。

[選択：監査対象事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査記録への上書き、から 1 つのみ選択]：最も古くに格納された監査記録への上書き

[割付：監査格納失敗時にとられるその他のアクション]：なし

○暗号サポート（FCS）

FCS_CKM.1 暗号鍵生成

下位階層：なし

依存性：[FCS_CKM.2 暗号鍵配付、または
FCS_COP.1 暗号操作]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.1.1 TSF は、[割付：標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付：暗号鍵長]に従って、暗号鍵を生成しなければならない。

[割付：標準のリスト]：表 6-2 の列「標準」に示す。

[割付：暗号鍵生成アルゴリズム]：表 6-2 の列「暗号鍵生成アルゴリズム」に示す。

[割付：暗号鍵長]：表 6-2 の列「暗号鍵長」に示す。

表 6-2 暗号鍵生成のための標準リスト、暗号鍵生成アルゴリズム及び暗号鍵長

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
許可外部メディア用共通鍵	FIPS PUB 197	AES	128bit
ファイル暗号用共通鍵	FIPS PUB 46-3	3DES	168bit
	FIPS PUB 197	AES	128/192/256bit

FCS_CKM.4 暗号鍵破棄

下位階層：なし

依存性：[FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4.1 TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵破棄方法[割付：暗号鍵破棄方法]に従って、暗号鍵を破棄しなければならない。

[割付：標準のリスト]：なし

[割付：暗号鍵破棄方法]：手動での削除

FCS_COP.1 暗号操作
下位階層：なし
依存性：[FDP_ITC.1 セキュリティ属性なし利用者データインポート、または
FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または
FCS_CKM.1 暗号鍵生成]
FCS_CKM.4 暗号鍵破棄
FMT_MSA.2 セキュアなセキュリティ属性

FCS_COP.1.1 TSF は、[割付：標準のリスト]に合致する、特定された暗号アルゴリズム[割付：暗号アルゴリズム]と暗号鍵長[割付：暗号鍵長]に従って、[割付：暗号操作のリスト]を実行しなければならない。

上述の割付を下表に示す。

[割付：標準のリスト]：表 6-3 の列「標準」に示す。

[割付：暗号アルゴリズム]：表 6-3 の列「暗号アルゴリズム」に示す。

[割付：暗号鍵長]：表 6-3 の列「暗号鍵長」に示す。

[割付：暗号操作のリスト]：表 6-3 の列「暗号操作」に示す。

表 6-3 暗号操作のための標準リスト、暗号アルゴリズム、暗号鍵長及び暗号操作

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
許可外部メディア用共通鍵	FIPS PUB 197	AES	128bit	許可外部メディアへのファイルの書き出し時の暗号化・読み込み時の復号
ファイル暗号用共通鍵	FIPS PUB 46-3	3DES	168bit	利用者データの暗号化・復号
	FIPS PUB 197	AES	128/192/256bit	

○利用者データ保護（FDP）

FDP_ACC.1a サブセットアクセス制御（I/O ポートの入出力制御）
下位階層：なし

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

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

[割付：サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]：以下に示す。

＜サブジェクト＞
・一般利用者プロセス

＜オブジェクト＞
・I/O ポート

＜SFP で扱われるサブジェクトとオブジェクト間の操作＞

表 6-4 に示す。

表 6-4 SFP で扱われるサブジェクトとオブジェクト間の操作

サブジェクト	オブジェクト	操作
一般利用者プロセス	I/O ポート	入力、出力

[割付：アクセス制御 SFP]：外部入出力アクセス制御方針

FDP_ACC.1b サブセットアクセス制御（プログラムファイルの操作制御）
下位階層：なし
依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

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

[割付：サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト]：以下に示す。

＜サブジェクト＞
・一般利用者プロセス

＜オブジェクト＞
・一般 AP 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＞

表 6-5 に示す。

表 6-5 SFP で扱われるサブジェクトとオブジェクト間の操作

サブジェクト	オブジェクト	操作
一般利用者プロセス	一般 AP ファイル	実行、ファイル名称変更

[割付：アクセス制御 SFP]：プログラムファイルアクセス制御方針

FDP_ACC.1c サブセットアクセス制御（暗号鍵ファイルの入出力制御）
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.1.1c 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]：以下に示す。

＜サブジェクト＞
- 管理者プロセス
- 一般利用者プロセス

＜オブジェクト＞
- エクスポート暗号鍵ファイル
- インポート暗号鍵ファイル
- 暗号鍵ファイル

＜SFP で扱われるサブジェクトとオブジェクト間の操作＞

表 6-6 に示す。

表 6-6 SFP で扱われるサブジェクトとオブジェクト間の操作

サブジェクト	オブジェクト	操作
管理者プロセス	エクスポート暗号鍵ファイル	書き出し
一般利用者プロセス	インポート暗号鍵ファイル	読み込み
一般利用者プロセス	暗号鍵ファイル	書き出し

[割付：アクセス制御 SFP]：暗号鍵ファイル入出力制御方針

FDP_ACF.1a セキュリティ属性によるアクセス制御（I/O ポートの入出力制御）
下位階層：なし
依存性：FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

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

[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、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、表に示す。

＜示された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＞

表 6-7 に示す。

表 6-7 サブジェクト及び対応する SFP 関連セキュリティ属性

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
一般利用者プロセス	I/O ポート利用制御情報 プリンタ利用制御情報 許可されたプリンタ情報 許可 USB デバイス入出力制御情報 外部メディア出力制御情報 許可外部メディア入出制御情報

＜示された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＞

表 6-8 に示す。

表 6-8 オブジェクト及び対応する SFP 関連セキュリティ属性

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
I/O ポート	ポート名

[割付：アクセス制御 SFP]：外部入出力アクセス制御方針

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

[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]：以下のとおり、表 6-9 に示す。

表 6-9 アクセスを管理する規則

サブジェクト	オブジェクト	操作	規則
一般利用者プロセス	I/O ポート	入力、出力	・ 一般利用者プロセスは、I/O ポート利用制御情報が「有効」に指定された I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、I/O ポート

サブジェクト	オブジェクト	操作	規則
			利用制御情報が「無効」のとき指定された I/O ポートに対して入力及び出力を実行しない ・ 一般利用者プロセスは、許可 USB デバイス入出力制御情報が接続された USB デバイスの持つ情報と一致したとき、USB デバイスで使用する I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、許可 USB デバイス入出力制御情報が接続された USB デバイスの持つ情報と一致しないとき、USB デバイスで使用する I/O ポートに対して入力及び出力を実行しない ・ 一般利用者プロセスは、外部メディア出力制御情報が「許可外部メディアのみ利用可能」のとき指定された外部メディアで使用する I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、外部メディア出力制御情報が「すべての外部メディアを許可」のとき、すべての外部メディアで使用する I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、外部メディア出力制御情報が「すべての外部メディアを利用禁止」のとき、外部メディアで使用する I/O ポートに対して入力及び出力を実行しない ・ 一般利用者プロセスは、許可外部メディア入出力制御情報が接続された外部メディアの持つ情報と一致したとき、外部メディアで使用する I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、許可外部メディア入出力制御情報が接続された外部メディアの持つ情報と一致しないとき、外部メディアで使用する I/O ポートに対して入力及び出力を実行しない

サブジェクト	オブジェクト	操作	規則
		出力	・ 一般利用者プロセスは、プリンタ利用制御情報が「一部許可」の場合、許可されたプリンタ情報に指定された I/O ポートに対して出力を実行する ・ 一般利用者プロセスは、プリンタ利用制御情報が「すべて許可」のとき、I/O ポートに対して出力を実行する ・ 一般利用者プロセスは、プリンタ利用制御情報が「すべて拒否」のとき、I/O ポートに対して出力を実行しない

表 6-9 で示された制御されたサブジェクトは、制御されたオブジェクトに対して、制御された操作のみを行うことができる。

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

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

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

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

FDP_ACF.1b セキュリティ属性によるアクセス制御（プログラムファイルの操作制御）
下位階層：なし
依存性：FDP_ACC.1 サブセットアクセス制御
　　FMT_MSA.3 静的属性初期化

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

[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、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、表に示す。

＜示された 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＞

表 6-10 に示す。

表 6-10 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
一般利用者プロセス	抑止される利用者プログラム情報

＜示された 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＞

表 6-11 に示す。

表 6-11 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
一般 AP ファイル	ファイル名称

[割付：アクセス制御 SFP]：プログラムファイルアクセス制御方針

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

[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]：以下のとおり、表 6-12 に示す。

表 6-12 アクセスを管理する規則

サブジェクト	オブジェクト	操作	規則
一般利用者プロセス	一般APファイル	実行、ファイル名称変更	一般利用者プロセスは、抑止される利用者プログラム情報で指定したファイル名称の一般 AP ファイルを実行しないまたはファイル名称を変更しない

表 6-12 で示された、制御されたサブジェクトは、制御されたオブジェクトに対して、制御された操作のみを行うことができる。

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

らない。

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

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

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

FDP_ACF.1c セキュリティ属性によるアクセス制御（暗号鍵ファイルの入出力制御）
下位階層：なし
依存性：FDP_ACC.1 サブセットアクセス制御
FMT_MSA.3 静的属性初期化

FDP_ACF.1.1c 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、表に示す。

＜示された 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＞

表 6-13 に示す。

表 6-13 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
管理者プロセス	なし
一般利用者プロセス	なし

＜示された 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＞

表 6-14 に示す。

表 6-14 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
エクスポート暗号鍵ファイル	なし
インポート暗号鍵ファイル	なし
暗号鍵ファイル	暗号鍵入力制御情報

表 6-14 で示された、制御されるオブジェクトは、セキュリティ属性である暗号鍵入力制御情報によってのみアクセス制御が実施される。

[割付：アクセス制御 SFP]：暗号鍵ファイル入出力制御方針

FDP_ACF.1.2c 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]：以下のとおり、表 6-15 に示す。

表 6-15 アクセスを管理する規則

サブジェクト	オブジェクト	操作	規則
管理者プロセス	エクスポート暗号鍵ファイル	書き出し	管理者プロセスは、ファイル暗号用共通鍵データ及び暗号鍵入力制御情報を書き出す
一般利用者プロセス	インポート暗号鍵ファイル	読み込み	一般利用者プロセスは暗号鍵入力制御情報を読み込む
	暗号鍵ファイル	書き出し	一般利用者プロセスは、ファイル暗号用共通鍵データに付与された暗号鍵入力制御情報を入力した時、ファイル暗号用共通鍵データを書き出す

表 6-15 で示された、制御されたサブジェクトは、制御されたオブジェクトに対して、制御された操作のみを行うことができる。

FDP_ACF.1.3c 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.1.4c TSF は、[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]に基づいて、オブジェクトに対

して、サブジェクトのアクセスを明示的に拒否しなければならない。

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

FDP_ETC.2 セキュリティ属性を伴う利用者データのエクスポート（ファイル暗号用共通鍵のエクスポート）

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]

FDP_ETC.2.1 TSF は、SFP 制御下にある利用者データを TOE の外部にエクスポートするとき、[割付：アクセス制御 SFP 及び/または情報フロー制御 SFP]を実施しなければならない。

[割付：アクセス制御 SFP 及び/または情報フロー制御 SFP]：暗号鍵ファイル入出力制御方針

FDP_ETC.2.2 TSF は、利用者データに関係したセキュリティ属性とともに利用者データをエクスポートしなければならない。

FDP_ETC.2.3 TSF は、セキュリティ属性が TOE の外部にエクスポートされるとき、それがエクスポートされる利用者データに曖昧さなく関係付けられることを保証しなければならない。

FDP_ETC.2.4 TSF は、利用者データが TOE からエクスポートされるとき、[割付：追加のエクスポート制御規則]の規則を実施しなければならない。

[割付：追加のエクスポート制御規則]：ファイル暗号用共通鍵に暗号鍵入力制御情報を付与する

FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート（ファイル暗号用共通鍵のインポート）

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]
[FTP_ITC.1 TSF 間高信頼チャネル、または
FTP_TRP.1 高信頼パス]
FPT_TDC.1 TSF 間基本 TSF データ一貫性

FDP_ITC.2.1 TSF は、SFP 制御下にある利用者データを TOE の外部からインポートするとき、[割付:アクセス制御 SFP 及び/または情報フロー制御 SFP]を実施しなければならない。

[割付：アクセス制御 SFP 及び/または情報フロー制御 SFP]：暗号鍵ファイル入出力制御

方針

FDP_ITC.2.2 TSF は、TOE 外からインポートされるとき、利用者データに関連付けられたセキュリティ属性を使用しなければならない。

FDP_ITC.2.3 TSF は、使用されるプロトコルが、受け取るセキュリティ属性と利用者データ間の曖昧さのない関連性を備えていることを保証しなければならない。

FDP_ITC.2.4 TSF は、インポートされる利用者データのセキュリティ属性の解釈が、利用者データの生成元によって意図されたとおりであることを保証しなければならない。

FDP_ITC.2.5 TSF は、TOE 外部から SFP の下で制御される利用者データをインポートするとき、[割付:追加のインポート制御規則]の規則を実施しなければならない。

[割付：追加のインポート制御規則]：ファイル暗号用共通鍵に暗号鍵入力制御情報を付与する

○識別と認証（FIA）

FIA_AFL. 1　認証失敗時の取り扱い
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管理者の認証
・最後に成功した認証以降の一般利用者の認証

[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]：「1～99 回内における管理者設定可能な正の整数値」

[詳細化]：不成功認証試行 → 最後に成功した認証以降の連続した不成功認証試行

FIA_AFL.1.2 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]：表 6-16 に示す。

表 6-16 認証失敗時のアクションのリスト

認証事象	アクション
管理者の認証	TOE は 3 分～3 分 30 秒の間のランダムな時間、PC をロックする。その後、連続した不成功認証試行回数カウンタのカウンタ値を 0 にする。
一般利用者の認証	TOE は 3 分～3 分 30 秒の間のランダムな時間、PC をロックする。その後、連続した不成功認証試行回数カウンタのカウンタ値を 0 にする。

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]：I/O ポート利用制御情報、プリンタ利用制御情報、許可されたプリンタ情報、許可 USB デバイス入出力制御情報、外部メディア出力制御情報、抑止される利用者プログラム情報、許可外部メディア入出力制御情報、利用者ＩＤ

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]：表 6-17 に示す。

表 6-17 定義された品質尺度のリスト

秘密情報	品質尺度
管理者パスワード 一般利用者パスワード	・ASCII 文字であり、以下の範囲の文字が使用できる。 - 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 ・管理者の設定したパスワード桁数の設定に従う。 ・管理者の設定したパスワードの有効期限の設定に従う。

秘密情報	品質尺度
暗号鍵入力制御情報	・ASCII 文字であり、以下の範囲の文字が使用できる。 - 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、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字、及び半角の空白 ・桁数は、8 文字以上 32 文字以下。
LogViewer 起動制御情報	・ASCII 文字であり、以下の範囲の文字が使用できる。 - アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字 - 数字は、[0-9]の合計 10 文字 - 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字、及び半角の空白 ・桁数は、8 文字以上 127 文字以下。

FIA_UAU.2 アクション前の利用者認証（管理者、クライアント管理者、一般利用者）
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 → 管理者、クライアント管理者、一般利用者

FIA_UAU.6 再認証
下位階層：なし
依存性：なし

FIA_UAU.6.1 TSF は、条件[割付： 再認証が要求される条件のリスト]のもとで利用者を再認証しなければならない。

[詳細化]：利用者 → 管理者、一般利用者

[割付：再認証が要求される条件のリスト]：
・管理者が設定した再認証時間が経過した場合

FIA_UAU.7 保証された認証フィードバック
下位階層：なし
依存性：FIA_UAU.1 認証のタイミング

FIA_UAU.7.1 TSF は、認証を行っている間、[割付： フィードバックのリスト]だけを利用者に提供しなければならない。

[割付：フィードバックのリスト]：
・入力された文字の数だけダミー（＊または●）を表示する

FIA_UID.2 アクション前の利用者識別（管理者、クライアント管理者、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.2.1 TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

[詳細化]：利用者 → 管理者、クライアント管理者、一般利用者

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]：I/O ポート利用制御情報、プリンタ利用制御情報、許可されたプリンタ情報、許可 USB デバイス入出力制御情報、外部メディア出力制御情報、許可外部メディア入出力制御情報、抑止される利用者プログラム情報、利用者ＩＤ

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]：なし

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

○セキュリティ管理（FMT）

FMT_MSA.1a セキュリティ属性の管理（I/O ポートの入出力制御）
下位階層：なし
依存性：[FDP_ACC.1 サブセットアクセス制御、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.1.1a 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 6-18 の列「セキュリティ属性」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 6-18 の列「操作」に示す。

[割付：許可された識別された役割]：表 6-18 の列「役割」に示す。

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：外部入出力アクセス制御方針

表 6-18 セキュリティ属性の管理（I/O ポートの入出力制御）

セキュリティ属性	操作	役割
I/Oポート利用制御情報	改変	管理者
プリンタ利用制御情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
許可USBデバイス入出力制御情報	改変	管理者
許可されたプリンタ情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
外部メディア出力制御情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
許可外部メディア入出力制御情報	改変	管理者

FMT_MSA.1b セキュリティ属性の管理（プログラムファイルの操作制御）
下位階層：なし
依存性：[FDP_ACC.1 サブセットアクセス制御、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.1.1b 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 6-19 の列「セキュリティ属性」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 6-19 の列「操作」に示す。

[割付：許可された識別された役割]：表 6-19 の列「役割」に示す。

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：プログラムファイルアクセス制御方針

表 6-19 セキュリティ属性の管理（プログラムファイルの操作制御）

セキュリティ属性	操作	役割
抑止される利用者プログラム情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者

FMT_MSA.1c セキュリティ属性の管理（暗号鍵ファイルの入出力制御）
下位階層：なし
依存性：[FDP_ACC.1 サブセットアクセス制御、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.1.1c 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 6-20 の列「セキュリティ属性」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 6-20 の列「操作」に示す。

[割付：許可された識別された役割]：表 6-20 の列「役割」に示す。

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：暗号鍵ファイル入出力制御方針

表 6-20 セキュリティ属性の管理（暗号鍵ファイルの入出力制御）

セキュリティ属性	操作	役割
暗号鍵入力制御情報	作成	管理者

FMT_MSA.3a 静的属性初期化（I/O ポートの入出力制御）
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。

[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] ：外部入出力アクセス制御方針

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]：管理者

FMT_MSA.3b 静的属性初期化（プログラムファイルの操作制御）
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。

[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] ：プログラムファイルアクセス制御方針

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]：管理者

FMT_MSA.3c 静的属性初期化（暗号鍵ファイルの入出力制御）
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.3.1c 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] ：暗号鍵ファイル入出力制御方針

FMT_MSA.3.2c 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]：管理者

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 6-21 の列「TSF データ」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 6-21 の列「操作」に示す。

[割付：許可された識別された役割]：表 6-21 の列「役割」に示す。

表 6-21 TSF データの管理

TSF データ	操作	役割
管理者ＩＤ	登録、問い合わせ	管理者
一般利用者ＩＤ	登録、問い合わせ	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
管理者パスワード	登録、改変	管理者
クライアント管理者パスワード	登録	管理者
	改変	クライアント管理者
一般利用者パスワード	登録	管理者
	改変	クライアント管理者
	改変	一般利用者
パスワード桁数	改変	管理者
パスワード有効期限	改変	管理者
監査証跡の警告サイズ	改変	管理者
連続認証失敗許容回数	改変	管理者
再認証時間	改変	管理者
LogViewer 起動制御情報	改変	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]：表 6-22 に示す。

表 6-22 TSF によって提供される管理機能のリスト

機能要件	CC パート 2 に規定された管理要件	管理項目
FAU_GEN.1	・なし	・なし
FAU_GEN.2	・なし	・なし
FAU_SAR.1	・監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)	・LogViewer 起動制御情報
FAU_SAR.2	・なし	・なし
FAU_SAR.3	・なし	・なし
FAU_STG.1	・なし	・なし
FAU_STG.3	・閾値の維持 ・監査格納失敗が切迫した時にとられるアクションの維持（削除、改変、追加）	・監査証跡の警告サイズ ・なし（アクションは固定であり、管理対象とはならない）
FAU_STG.4	・監査格納失敗時にとられるアクションの維持（削除、改変、追加）	・なし
FCS_CKM.1	・暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	・なし（固定）
FCS_CKM.4	・暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	・なし（固定）
FCS_COP.1	・なし	・なし
FDP_ACC.1a	・なし	・なし
FDP_ACC.1b	・なし	・なし
FDP_ACC.1c	・なし	・なし
FDP_ACF.1a	・明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	・以下のセキュリティ属性 –I/O ポート利用制御情報 –プリンタ利用制御情報 –許可されたプリンタ情報 –許可 USB デバイス入出力制御情報 –外部メディア出力制御情報 –許可外部メディア入出力制御情報 –ポート名
FDP_ACF.1b	・明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	・以下のセキュリティ属性 －抑止される利用者プログラム情報 －ファイル名称
FDP_ACF.1c	・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	・以下のセキュリティ属性 －暗号鍵入力制御情報
FDP_ETC.2	・追加のエクスポート制御規則は、定義された役割の利用者により、設定可能である	・暗号鍵入力制御情報
FDP_ITC.2	・インポートに対して使用される追加の制御規則の改変	・なし（固定）
FIA_AFL.1	・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	・連続認証失敗許容回数 ・なし(アクションは固定)
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
FIA_SOS.1	・秘密の検証に使用される尺度の管理	・利用者のパスワード桁数 ・利用者のパスワード有効期限
FIA_UAU.2	・管理者による認証データの管理;	・利用者のパスワード

機能要件	CC パート 2 に規定された管理要件	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	
FIA_UAU.6	・許可管理者が再認証を要求できる場合、管理に再認証要求を含める	・再認証時間
FIA_UAU.7	・なし	・なし
FIA_UID.2	・利用者識別情報の管理	・利用者ＩＤ
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属性を定義できる ・許可管理者は、サブジェクトのセキュリティ属性を変更できる	・なし ・なし
FMT_MSA.1a	・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（固定）
FMT_MSA.1b	・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（固定）
FMT_MSA.1c	・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（固定）
FMT_MSA.3a	・初期値を特定できる役割のグループを管理すること; ･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（固定） ・なし（固定）
FMT_MSA.3b	・初期値を特定できる役割のグループを管理すること; ･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（固定） ・なし（固定）
FMT_MSA.3c	・初期値を特定できる役割のグループを管理すること; ･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（固定） ・なし（固定）
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（固定）
FMT_SMF.1	・なし	・なし
FMT_SMR.1	・役割の一部をなす利用者のグループの管理	・なし（固定）
FPT_ITT.1	･TSF が(その改変から)保護すべき改変の種別の管理 ･TSF の異なるパーツ間の転送中にデータ保護を提供するために使われるメカニズムの管理	・なし（固定） ・なし（固定）
FPT_STM.1	・時間の管理	・なし

FMT_SMR.1 セキュリティの役割
下位階層：なし
依存性：FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、役割[割付：許可された識別された役割]を維持しなければならない。

[割付：許可された識別された役割]：
- ・管理者
- ・クライアント管理者
- ・一般利用者

FMT_SMR.1.2 TSF は、利用者を役割に関連付けなければならない。

○TSF の保護（FPT）

FPT_ITT.1 基本 TSF 内データ転送保護
下位階層：なし
依存性：なし

FPT_ITT.1.1 TSF は、TSF データが TOE の異なるパーツ間で送られる場合、TSF データを[選択: 暴露、改変]から保護しなければならない。

[選択: 暴露、改変]：暴露、改変

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. セキュリティ保証要件

セキュリティ保証要件を記述する。
本 TOE の評価保証レベルは EAL1＋ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 である。すべての保証要件コンポーネントは、CC パート 3 で規定されている EAL 1 のコンポーネント及び ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 を直接使用する。

EAL1＋ASE_OBJ.2、ASE_REQ.2、ASE_SPD.1 規定コンポーネント

(1) ADV.：開発
　ADV_FSP.1：基本機能仕様

(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

(3) ALC：ライフサイクルサポート
　ALC_CMC.1：TOE のラベル付け
　ALC_CMS.1：TOE の CM 範囲

(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

(5) ATE：テスト
　ATE_IND.1：独立テスト- 適合

(6) AVA：脆弱性評定
　AVA_VAN.1：脆弱性調査

6.3. セキュリティ要件根拠

6.3.1. セキュリティ機能要件根拠

セキュリティ機能要件と TOE のセキュリティ対策方針の対応関係を表 6-23 に示す。

表 6-23　セキュリティ機能要件と TOE のセキュリティ対策方針の対応関係

	O.I&A	O.ACCESS_CONTROL	O.ACCESS_CONTROL_MEDIA	O.RE_AUTH	O.AUDIT	O.CRYPTOGRAPHY	O.LOG_COLLECT
FAU_GEN.1					×		
FAU_GEN.2					×		
FAU_SAR.1					×		
FAU_SAR.2					×		
FAU_SAR.3					×		
FAU_STG.1					×		
FAU_STG.3					×		
FAU_STG.4					×		
FCS_CKM.1						×	
FCS_CKM.4						×	
FCS_COP.1						×	
FDP_ACC.1a		×	×				
FDP_ACC.1b		×					
FDP_ACC.1c						×	
FDP_ACF.1a		×	×				
FDP_ACF.1b		×					
FDP_ACF.1c						×	
FDP_ETC.2						×	
FDP_ITC.2						×	
FIA_AFL.1	×						
FIA_ATD.1	×	×	×				
FIA_SOS.1	×						
FIA_UAU.2	×						
FIA_UAU.6				×			
FIA_UAU.7	×			×			
FIA_UID.2	×						
FIA_USB.1	×	×	×				

	O.I&A	O.ACCESS_CONTROL	O.ACCESS_CONTROL_MEDIA	O.RE_AUTH	O.AUDIT	O.CRYPTOGRAPHY	O.LOG_COLLECT
FMT_MSA.1a		×	×				
FMT_MSA.1b		×					
FMT_MSA.1c						×	
FMT_MSA.3a		×	×				
FMT_MSA.3b		×					
FMT_MSA.3c						×	
FMT_MTD.1		×	×				
FMT_SMF.1	×	×	×			×	
FMT_SMR.1	×	×	×			×	
FPT_ITT.1							×
FPT_STM.1					×		

表 6-23 より、各セキュリティ機能要件が 1 つ以上のセキュリティ対策方針に対応している。次に、各セキュリティ対策方針が、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、要求される機能を示し、それがすべて満たされることでセキュリティ対策方針を実現することができることを示す。なお、要求される機能については、一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（利用者の識別認証）

このTOEセキュリティ対策方針は、正当な利用者がTOEを利用するための、利用者の制限を求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. TOE利用前に、利用者を識別する

利用者がTOEを利用する前には、利用を許可されている者であることが識別されなければならない。よって、利用者が識別される前に実行が許可されるTSFは、利用者を識別するためのTSFのみである。この要件に該当するセキュリティ機能要件は、FIA_UID.2である。

b. TOE利用前に、利用者を認証する

利用者がTOEを利用する前には、利用を許可されている者であることが認証されなけれ

ばならない。よって、利用者が認証される前に実行が許可されるTSFは、利用者を認証するためのTSFのみである。この要件に該当するセキュリティ機能要件は、FIA_UAU.2である。

c. 推測困難な認証情報

認証を行うためには、利用者認証情報が、利用者本人以外に予測されることが困難でなければならない。予測されることが困難であるためには、利用者認証情報に対し、必要なレベルの品質を明確に定義し、その品質が満たされていることを検証しなければならない。この要件に該当するセキュリティ機能要件は、FIA_SOS.1である。

d. 識別認証に成功した時に、TOEの利用を許可する

識別認証に成功した利用者は、同じく成功したクライアントを用いてTOEを利用できる。TOEの利用に際しては、TOEは利用者を代行するサブジェクトを生成し、利用者がTSFを利用するためのセキュリティ属性を維持及び関連付ける。この要件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. 指定回数以内に認証に成功しない場合、TOEの利用を無効とする

認証に失敗した利用者は、TOEの正当な利用者ではないとみなす必要がある。TOEは、管理者が指定した連続認証失敗許容回数以上、認証に失敗した利用者に対し、あらかじめ定義されたアクション(TOEの一定期間の無効化)を実施する。この要件に該当するセキュリティ機能要件は、FIA_AFL.1である。

f. 認証時の入力内容はダミー表示とする

認証時の認証情報は、入力情報をそのまま表示すると、認証を行っている利用者以外に認証情報を知られる恐れがあるため、入力していることのみが分かるようにダミー表示にする必要がある。この要件に該当するセキュリティ機能要件は、FIA_UAU.7である。

g. 認証結果に応じた管理機能の提供

TOEは、利用者が認証に成功した場合は、認証結果に応じた管理機能を提供する。この要件に該当するセキュリティ機能要件は、FMT_SMF.1である。

h. 認証結果に応じたセキュリティ役割の対応付け

TOEは、利用者が認証に成功した場合は、認証結果に応じたセキュリティ役割の対応付けを行ない、これを維持する。この要件に該当するセキュリティ機能要件は、FMT_SMR.1である。

以上、a、b、c、d、e、f、g、h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_SOS.1、FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FIA_USB.1、FMT_SMF.1及びFMT_SMR.1の達成により、O.I&Aを実現することができる。

O.ACCESS_CONTROL （アクセス制御）

このTOEセキュリティ対策方針は、一般利用者または一般利用者を代行するプロセスが、あらかじめ決定されたI/Oポート、ユーザプログラムファイル及びプリンタポートに対するアクセス権限に応じて、アクセスが許可されることを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. プログラムファイルに対するアクセス制御を実施する

プログラムファイルに対して許可しない操作と対象を決定し、そのとおりに実施しなければならない。よって、一般利用者プロセスとプログラムファイルの操作リストを対応づけ、その対応に従ってプログラムファイルの実行及びファイル名称変更時にアクセス制御を行う。この要件に該当するセキュリティ機能要件は、FDP_ACC.1b及びFDP_ACF.1bである。

b. I/Oポートに対するアクセス制御を実施する

I/Oポートに対して許可する操作と対象を決定し、そのとおりに実施しなければならない。よって、一般利用者プロセスとI/Oポートの操作リストを対応付けし、その対応に従ってI/Oポートへの入力及び出力の制御を行う。この要件に該当するセキュリティ機能要件は、FDP_ACC.1a及びFDP_ACF.1aである。

c. 利用者とプロセスの結合

TOEは、一般利用者に関連するセキュリティ属性（I/Oポート利用制御情報、プリンタ利用制御情報、許可されたプリンタ情報、許可USBデバイス入出力制御情報、外部メディア出力制御情報、抑止される利用者プログラム情報、利用者ＩＤ）と一般利用者を代行して動作するサブジェクトを結合する。この要件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。

d. 意図したとおりアクセス制御が行われるために、TOEの動作に重大な影響を及ぼす操作を管理者に制限し、一般利用者に必要な操作権限を与える

アクセス制御で用いられるセキュリティ属性（I/Oポート利用制御情報、プリンタ利用制御情報、許可されたプリンタ情報、許可USBデバイス入出力制御情報、外部メディア出力制御情報、抑止される利用者プログラム情報、利用者ＩＤ）は、利用者の役割に応じてアクセスの可否が決定される。この要件に該当するセキュリティ機能要件は、FMT_MSA.1a、FMT_MSA.1bである。このセキュリティ属性は、管理者によってのみ変更が許され、一般利用者には改変することは許されない。この要件に該当するセキュリティ機能要件は、FMT_MSA.3a、FMT_MSA.3bである。

その他、TOEの動作に影響を与える設定及びOSの各種制御の設定について、管理する権限を持つ者を制限するため、TSFデータの役割に応じたアクセスを行う。この要件に該当するセキュリティ機能要件は、FMT_MTD.1である。

また、TOEはセキュリティ機能に応じた管理機能を提供する。この要件に該当するセキ

ュリティ機能要件は、FMT_SMF.1である。
さらに、TOEは管理者及び一般利用者の役割の対応付けを行い、これを維持する。この要件に該当するセキュリティ機能要件は、FMT_SMR.1である。

以上、a、b、c、d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、FIA_ATD.1、FIA_USB.1、FDP_ACC.1a、FDP_ACF.1a 、FDP_ACC.1b、FDP_ACF.1b、FMT_MSA.1a、FMT_MSA.1b、FMT_MSA.3a、FMT_MSA.3b、FMT_MTD.1、FMT_SMF.1及びFMT_SMR.1の達成により、O.ACCESS_CONTROLを実現できる。

O. ACCESS_CONTROL_MEDIA （外部メディアのアクセス制御）

このTOEセキュリティ対策方針は、一般利用者または一般利用者を代行するプロセスが、許可外部メディアに対するアクセス権限に応じて、アクセスが許可されることを求めている、この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a.許可外部メディアに対する、アクセス制御を実施する
一般利用者の許可外部メディアに対して許可する操作と規則を決定し、アクセス制御を実施しなければならない。この要件に該当するセキュリティ機能要件は、FDP_ACC.1a及びFDP_ACF.1aである。

b. 利用者とプロセスの結合
TOEは、一般利用者に関連するセキュリティ属性（外部メディア出力制御情報、許可外部メディア入出力制御情報、利用者ＩＤ）と一般利用者を代行して動作するサブジェクトを結合する。この要件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。

c. 意図したとおりアクセス制御が行われるために、TOEの動作に重大な影響を及ぼす操作を管理者に制限し、一般利用者に必要な操作権限を与える
アクセス制御で用いられるセキュリティ属性（外部メディア出力制御情報、許可外部メディア入出力制御情報、利用者ＩＤ）は、利用者の役割に応じてアクセスの可否が決定される。この要件に該当するセキュリティ機能要件は、FMT_MSA.1aである。このセキュリティ属性は、管理者によってのみ変更が許され、一般利用者には改変することは許されない。この要件に該当するセキュリティ機能要件は、FMT_MSA.3aである。
その他、TOEの動作に影響を及ぼす設定について、管理する権限を持つ者を制限するため、TSFデータの役割に応じたアクセスを行う。この要件に該当するセキュリティ機能要件は、FMT_MTD.1である。
また、TOEはセキュリティ機能に応じた管理機能を提供する。この要件に該当するセキュリティ機能要件は、FMT_SMF.1である。
さらに、TOEは管理者及び一般利用者の役割の対応付けを行い、これを維持する。この

要件に該当するセキュリティ機能要件は、FMT_SMR.1である。

以上、a、b、cすべての対策を満たすことは、O.ACCESS_CONTROL_MEDIA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_ATD.1、FIA_USB.1、FDP_ACC.1a、FDP_ACF.1a、FMT_MSA.1a 、FMT_MSA.3a、FMT_MTD.1、FMT_SMF.1及びFMT_SMR.1の達成により、O.ACCESS_CONTROL_MEDIAを実現できる。

O. RE_AUTH （再認証）

このTOEセキュリティ対策方針は、TOEにログオンした管理者または一般利用者が、一定時間経過後TOEへのアクセスを行う場合は、正式な利用者であることを再認証することを求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 再認証の要求

管理者が設定した、TOEの無操作時間が経過した場合、再認証が要求される。この要件に該当するセキュリティ機能要件は、FIA_UAU.6である。

b. 認証情報の秘匿

再認証時のパスワード入力の画面表示は、ダミー文字で秘匿する。この要件に該当するセキュリティ機能要件は、FIA_UAU.7である。

以上、a、bすべての対策を満たすことは、O.RE_AUTH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_UAU.6及びFIA_UAU.7の達成により、O.RE_AUTHを実現できる。

O.AUDIT（監査）

このTOEセキュリティ対策方針は、ログの取得とその保護について求めている。ログは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、ログの保護では、ログの確実な取得、閲覧、検索を考慮する。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. ログとして必要な情報を取得する

TOEは、表6-1で示した監査要件に関して、ログを正確な時刻とともに利用者と関連付けて取得する。この要件に該当するセキュリティ機能要件は、ログの取得についてはFAU_GEN.1であり、正確な時刻の取得は、FPT_STM.1であり、利用者との関連付けは、FAU_GEN.2である。

b. すべてのログを取得する

TOEは、監査証跡に格納されたログに対して不正な削除の防止及び不正な改変の防止を行う。また、ログが事前に設定された監査証跡の警告サイズを超えた場合は、管理者また

は一般利用者に対しログの消失の恐れがあることを通知する。さらに監査証跡が満杯になった場合は、ログの消失を防止するアクションを実施する。この要件に該当するセキュリティ機能要件は、FAU_STG.1、FAU_STG.3及びFAU_STG.4である。

c. 取得したログの利用者及び利用内容の制限

TOEは、監査証跡からログを読み出すのに、管理者にのみ参照可能なように提供する。また、ログの参照においては、管理者にのみログサーバ上のログの参照を許可し、管理者端末及びクライアントで採取されたログについては参照することはできない。

その他、ログの利用においては、許可された条件に基づき、分類及び検索の機能を提供する。この要件に該当するセキュリティ機能要件は、FAU_SAR.1、FAU_SAR.2及びFAU_SAR.3である。

以上、a、b、c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該当する、FAU_GEN.1、FAU_GEN.2、FAU_SAR.1、FAU_SAR.2、FAU_SAR.3、FAU_STG.1、FAU_STG.3、FAU_STG.4及びFPT_STM.1の達成により、O.AUDITを実現できる。

O.CRYPTOGRAPHY（暗号化）

このTOEセキュリティ対策方針は、クライアントへの利用者データの格納時のファイルの暗号化及び許可外部メディアへの書き出し時の暗号化の実施について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. 暗号鍵の生成

TOEは、国際標準に基づき規格化された暗号鍵生成メカニズムにより暗号鍵を生成する。この要件に該当するセキュリティ機能要件は、FCS_CKM.1である。

b. 暗号操作

TOEは、FCS_CKM.1の機能で生成された暗号鍵を使って、許可外部メディアへのファイルの書き込み時、任意のファイルの暗号化または復号を行う。この要件に該当するセキュリティ機能要件は、FCS_COP.1である。

c. 暗号鍵の書き出し

TOEは、任意のファイルの暗号化または復号を行うための鍵の書き出しを、管理者のみが行えるようにする。この要件に該当するセキュリティ機能要件は、FDP_ETC.2である。

d. 暗号鍵の削除

TOEは、任意のファイルの暗号化または復号を行うための鍵の削除を、TOEの利用を許可された鍵の所有者である一般利用者のみがが行えるようにする。この要件に該当するセキュリティ機能要件は、FCS_CKM.4である。

e. 暗号鍵の入力制御

TOEは、暗号鍵の入力制御において用いられるセキュリティ属性（暗号鍵入力制御情報）を管理し、その属性の管理を、管理者のみが行えるようにする。この要件に該当するセキュリティ機能要件は、FMT_MSA.1c及びFMT_MSA.3cである。

また、任意のファイルの暗号化または復号を行うための鍵の読み込みにおいては、読み込む暗号鍵に対して許可する操作と規則を決定し、アクセス制御を実施しなければならない。この要件に該当するセキュリティ機能要件は、FDP_ACC.1c及びFDP_ACF.1c及びFDP_ITC.2である。

f. 暗号鍵の管理機能と役割の対応付け

TOEは暗号に関するセキュリティ機能に応じた管理機能を提供する。この要件に該当するセキュリティ機能要件は、FMT_SMF.1である。

また、TOEは管理者及び一般利用者の役割の対応付けを行い、これを維持する。この要件に該当するセキュリティ機能要件は、FMT_SMR.1である。

以上、a、b、c、d、e、fすべての対策を満たすことは、O.CRYPTOGRAPHY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、FCS_CKM.1、FCS_CKM.4、FCS_COP.1、FDP_ACC.1a、FDP_ACF.1a、FDP_ETC.2、FDP_ITC.2、FMT_MSA.1c、FMT_MSA.3c、FMT_SMF.1及びFMT_SMR.1の達成により、O.CRYPTOGRAPHYを実現できる。

O.LOG_COLLECT（ログの集約）

このTOEセキュリティ対策方針は、管理者端末及びクライアントからログサーバへのログのセキュアな集約について求めている。この要求に対し、必要な対策の詳細と、求められる機能は以下のとおりである。

a. ログの確実な転送

TOEは、管理者端末及びクライアントにより生成されたログを、ログサーバに確実に転送し、転送時の暴露、改変からログを保護しなければならない。この要件に該当するセキュリティ機能要件は、FPT_ITT.1である。

以上、上記aの対策を満たすことは、O.LOG_COLLECT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、FPT_ITT.1の達成により、O.LOG_COLLECTを実現できる。

6.3.2. 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 6-24 に示す。

表 6-24　セキュリティ要件のコンポーネントの依存性

項番	TOE で使用されているコンポーネント	CC パート 2 で規定されている依存コンポーネント	TOE の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
1	FAU_GEN.1	FPT_STM.1	FPT_STM.1	なし	
2	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1	なし	
		FIA_UID.1	FIA_UID.2	なし	
3	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1	なし	
4	FAU_SAR.2	FAU_SAR.1	FAU_SAR.1	なし	
5	FAU_SAR.3	FAU_SAR.1	FAU_SAR.1	なし	
6	FAU_STG.1	FAU_GEN.1	FAU_GEN.1	なし	
7	FAU_STG.3	FAU_STG.1	FAU_STG.1	なし	
8	FAU_STG.4	FAU_STG.1	FAU_STG.1	なし	
9	FCS_CKM.1	[FCS_CKM.2、または FCS_COP.1]	FCS_COP.1	なし	
		FCS_CKM.4	FCS_CKM.4		
		FMT_MSA.2	なし	FMT_MSA.2	*1
10	FCS_CKM.4	[FCS_CKM.2、または FCS_COP.1]	FCS_COP.1	なし	
		FCS_CKM.1	FCS_CKM.1		
		FMT_MSA.2	なし	FMT_MSA.2	*1
11	FCS_COP.1	[FDP_ITC.1、または FDP_ITC.2、または FCS_CKM.1]	FCS_CKM.1	なし	
		FCS_CKM.4	なし	FCS_CKM.4	
		FMT_MSA.2	なし	FMT_MSA.2	*1
12	FDP_ACC.1a	FDP_ACF.1	FDP_ACF.1a	なし	
13	FDP_ACC.1b	FDP_ACF.1	FDP_ACF.1b	なし	
14	FDP_ACC.1c	FDP_ACF.1	FDP_ACF.1c	なし	
15	FDP_ACF.1a	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1a FMT_MSA.3a	なし	
16	FDP_ACF.1b	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1b FMT_MSA.3b	なし	
17	FDP_ACF.1c	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1c FMT_MSA.3c	なし	
18	FDP_ETC.2	[FDP_ACC.1、または FDP_IFC.1]	FDP_ACC.1c	なし	
19	FDP_ITC.2	[FDP_ACC.1、または FDP_IFC.1]	FDP_ACC.1c	なし	
		[FTP_ITC.1、または FTP_TRP.1]	なし	[FTP_ITC.1、または FTP_TRP.1]	*2
		FPT_TDC.1	なし	FPT_TDC.1	*3
20	FIA_AFL.1	FIA_UAU.1	FIA_UAU.1	なし	
21	FIA_ATD.1	なし	なし	なし	
22	FIA_SOS.1	なし	なし	なし	

項番	TOE で使用されているコンポーネント	CC パート２で規定されている依存コンポーネント	TOE の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
23	FIA_UAU.2	FIA_UID.1	FIA_UID.2	なし	
24	FIA_UAU.6	なし	なし	なし	
25	FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	なし	
26	FIA_UID.2	なし	なし	なし	
27	FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし	
28	FMT_MSA.1a	[FDP_ACC.1、または FDP_IFC.1]	FDP_ACC.1a	なし	
		FMT_SMR.1	FMT_SMR.1	なし	
		FMT_SMF.1	FMT_SMF.1	なし	
29	FMT_MSA.1b	[FDP_ACC.1、または FDP_IFC.1]	FDP_ACC.1b	なし	
		FMT_SMR.1	FMT_SMR.1	なし	
		FMT_SMF.1	FMT_SMF.1	なし	
30	FMT_MSA.1c	[FDP_ACC.1、または FDP_IFC.1]	FDP_ACC.1c	なし	
		FMT_SMR.1	FMT_SMR.1	なし	
		FMT_SMF.1	FMT_SMF.1	なし	
31	FMT_MSA.3a	FMT_MSA.1	FMT_MSA.1a	なし	
		FMT_SMR.1	FMT_SMR.1	なし	
32	FMT_MSA.3b	FMT_MSA.1	FMT_MSA.1b	なし	
		FMT_SMR.1	FMT_SMR.1	なし	
33	FMT_MSA.3c	FMT_MSA.1	FMT_MSA.1c	なし	
		FMT_SMR.1	FMT_SMR.1	なし	
34	FMT_MTD.1	FMT_SMR.1	FMT_SMR.1	なし	
		FMT_SMF.1	FMT_SMF.1	なし	
35	FMT_SMF.1	なし	なし	なし	
36	FMT_SMR.1	FID_UID.1	FID_UID.2	なし	
37	FPT_ITT.1	なし	なし	なし	
38	FPT_STM.1	なし	なし	なし	

表 6-24 より、セキュリティ機能要件は後述する例外を除きそれぞれの必要な依存関係をすべて満たしている。全ての例外について、依存関係は満たされなくても問題がない根拠を以下に示す。

*1) FCS_CKM.1、FCS_COP.1 → FMT_MSA.2

FCS_CKM.1及びFCS_COP.1で取り扱うセキュリティ属性は、各暗号鍵に関するものであり、それぞれ標準化されたアルゴリズムに従って、属性の値が決定されており、利用者による属性値の設定・改変を受け入れることはない。よって、これらの依存関係は不要である。

*2) FDP_ITC.2 → FTP_ITC1またはFTP_TRP.1

管理者が鍵をエクスポートする際には、一般利用者に手渡す鍵に対して暗号鍵入力制

御情報を設定し媒体に保存し、直接その鍵を受け取る権利のある一般利用者に手渡しすることでセキュリティは保たれており、セキュアな通信チャネルを使う必要が無い。よって、これらの依存関係は不要である。

*3) FDP_ITC.2 → FPT_TDC.1

インポート時に使用するセキュリティ属性の暗号鍵入力制御情報は、TOE内で生成したものであり、別のIT製品との間でセキュリティ属性の一貫性を維持する必要はない。よって、これらの依存関係は不要である。

6.3.3. セキュリティ保証要件根拠

本 TOE は自社のシステムであり、顧客向けとは異なり、厳密な保証は不要であり、EAL 1 で十分である。ただし、情報漏洩防止のためのシステムであるため、脅威分析を実施した完全なセキュリティターゲットの評価は必要であるので、ASE_OBJ.2、ASE_REQ.2 及び ASE_SPD.1 を追加している。

7. TOE 要約仕様

本章では、TOE 要約仕様について記述する。

7.1. TOE 要約仕様

この節では、TOE のセキュリティ機能を説明する。

7.1.1. 監査機能

[FAU_GEN.1]

TOE は、TOE がセキュアに運用されていることを監査するために必要なログの生成及び生成した情報の管理を行うために、あらかじめ定められた監査の対象となる動作を行った場合及び動作の結果が期待される結果ではなかった場合に、当該事象をログとして生成する。

ログは以下の監査対象事象の発生時に生成する。
・外部メディアへの書き込み成功、失敗
・プログラムファイルの起動の成功、失敗
・プログラムファイルの名称変更の失敗
・連続した不成功認証試行回数カウンタの閾値到達、それに続いて取られるアクション（PC の一定時間のロック）
・利用者の識別認証の成功、失敗
・利用者 ID の登録、更新、削除の成功、失敗
・利用者パスワードの登録、更新の成功、失敗

なお、TOE 起動後の利用者のログイン完了からシャットダウンの実行までの間以外では監査対象事象は発生しないため、それぞれを監査機能の起動と終了とする。

ログは、以下の項目で構成される。
・日付・時刻（事象の日付・時刻）：ログ出力の日付・時刻
・イベントタイプ（事象の種別）：エラー、警告、情報のイベントタイプの分類を示す
・利用者ＩＤ（サブジェクト識別情報）
・メッセージ（事象の結果）：事象の詳細な内容を表すもの。
・イベントＩＤ（その他の監査関連情報）
・カテゴリ（その他の監査関連情報）：ログのカテゴリ分類を示す
・PC 名（その他の監査関連情報）
・ＩＰアドレス（その他の監査関連情報）
・ＭＡＣアドレス（その他の監査関連情報）

[FAU_GEN.2]
TOE は、TOE がセキュアに運用されていることを監査するために必要な情報の生成及び生成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に、当該事象とその原因となった利用者ＩＤを、関連付けた上でログとして生成する。

[FAU_SAR.1]
TOE は、LogViewer 起動制御情報を入力した管理者に対してのみ、下記の監査情報のリストに基づいてログサーバ上のログを提供する。

＜監査情報のリスト＞
・日付・時刻
・イベントタイプ
・利用者ＩＤ
・メッセージ
・イベントＩＤ
・カテゴリ
・PC 名
・ＩＰアドレス
・ＭＡＣアドレス

また、管理者が読み出すことのできるログについては、監査対象事象ごとに監査項目を表示できるようにしている。

[FAU_SAR.2]
TOE は、入力された LogViewer 起動制御情報と TOE 内部で保持している LogViewer 起動制御情報を比較し、一致した LogViewer 起動制御情報を入力した管理者以外には、ログサーバに格納されたログへのアクセスを禁止する。

[FAU_SAR.3]
TOE は、以下の項目での検索要求に対応する。

＜ログの検索条件としては、以下の条件を指定できる。＞
・期間、時間帯
・利用者ＩＤ
・PC 名
・ＩＰアドレス
・ＭＡＣアドレス
・イベントタイプ
・カテゴリ
・イベントＩＤ

[FAU_STG.3]
TOE は、監査証跡に格納されたログが、予め管理者がクライアント制御情報に設定した監査証跡の警告サイズの値を超えた場合、ログが損失する恐れが発生したことを示すメッセージをクライアントまたは管理者端末の画面に表示する。

[FAU_STG.4]
TOE は、監査証跡に格納されたログが、予め確保されたログを格納するための領域が満杯になった場合、ログの損失を防止するため、管理者端末およびクライアントにおいては最も古くに格納されたログへの上書きを行う。

[FPT_ITT.1]
TOE は、管理者端末及びクライアントからログサーバへのログの転送において、SSL により暗号化して通信を行うことによりログをログサーバに集約する。

[FPT_STM.1]
TOE は、監査証跡に格納するログ生成のための正確な日付・時刻を提供する。

7.1.2. アクセス制御機能

[FAU_STG.1]
TOE は、監査証跡に格納されたログに対して、ログの登録とログのログサーバへの転送のための読出し以外のインタフェースを提供しないことにより、不正な改変から保護する。また、OS の如何なる権限をもってしても監査証跡内のログを直接編集するインタフェースを提供しないことにより、不正な改変から保護する。

[FDP_ACC.1a] [FDP_ACF.1a]
TOE は、識別認証機能（クライアント）により許可された一般利用者と対応づけられた一般利用者プロセスが、I/O ポートへの入出力を実行する場合は、管理者により設定されクライアントにインポートされたクライアント制御情報に従って、一般利用者プロセスの I/O ポートへの入力、出力の制御を外部入出力アクセス制御方針に従って実行する。
外部入出力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を以下の表 7-1 に、外部入出力アクセス制御方針で扱われるサブジェクトとセキュリティ属性を以下の

表 7-2 に、オブジェクトとセキュリティ属性を以下の表 7-3 にそれぞれ示す。

表 7-1 外部入出力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

サブジェクト	オブジェクト	操作
一般利用者プロセス	I/O ポート	入力、出力

表 7-2 サブジェクト及び対応する SFP 関連セキュリティ属性

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

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
一般利用者プロセス	I/O ポート利用制御情報 プリンタ利用制御情報 許可されたプリンタ情報 許可 USB デバイス入出力制御情報 外部メディア出力制御情報 許可外部メディア入出制御情報

表 7-3 オブジェクト及び対応する SFP 関連セキュリティ属性

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
I/O ポート	ポート名

[割付：アクセス制御 SFP]：外部入出力アクセス制御方針

また、TOEは、クライアント制御情報に従って、制御されたサブジェクトとオブジェクト間での操作を以下の表7-4の規則に従って実施する。

表 7-4 アクセスを管理する規則

サブジェクト	オブジェクト	操作	規則
一般利用者プロセス	I/O ポート	入力、出力	・ 一般利用者プロセスは、I/O ポート利用制御情報が「有効」に指定された I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、I/O ポート利用制御情報が「無効」のとき指定された I/O ポートに対して入力及び出力を実行しない ・ 一般利用者プロセスは、許可 USB デバイス入出力制御情報が接続された USB デバイスの持つ情報と一致したとき、USB デバイスで使用する I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、許可 USB デバイス入出力制御情報が接続された USB デバイスの持つ情報と一致しないとき、USB デバイスで使用する I/O ポートに対して入力及び出力を実行しない ・ 一般利用者プロセスは、外部メディア出力制御情報が「許可外部メディアのみ利用可能」のとき指定された外部メディアで使用する I/O ポートに対して入力及び出力を実行する

サブジェクト	オブジェクト	操作	規則
			・ 一般利用者プロセスは、外部メディア出力制御情報が「すべての外部メディアを許可」のとき、すべての外部メディアで使用する I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、外部メディア出力制御情報が「すべての外部メディアを利用禁止」のとき、外部メディアで使用する I/O ポートに対して入力及び出力を実行しない ・ 一般利用者プロセスは、許可外部メディア入出力制御情報が接続された外部メディアの持つ情報と一致したとき、外部メディアで使用する I/O ポートに対して入力及び出力を実行する ・ 一般利用者プロセスは、許可外部メディア入出力制御情報が接続された外部メディアの持つ情報と一致しないとき、外部メディアで使用する I/O ポートに対して入力及び出力を実行しない
		出力	・ 一般利用者プロセスは、プリンタ利用制御情報が「一部許可」の場合、許可されたプリンタ情報に指定された I/O ポートに対して出力を実行する ・ 一般利用者プロセスは、プリンタ利用制御情報が「すべて許可」のとき、I/O ポートに対して出力を実行する ・ 一般利用者プロセスは、プリンタ利用制御情報が「すべて拒否」のとき、I/O ポートに対して出力を実行しない

[FDP_ACC.1b] [FDP_ACF.1b]

TOE は、識別認証機能（クライアント）により許可された一般利用者と TOE 内部で一般利用者のプログラム操作を代行する一般利用者プロセスを対応付け、一般利用者がクライアント上で一般 AP ファイルを実行またはファイル名称を変更する場合は、管理者により設定されクライアントにインポートされたクライアント制御情報に従って、一般利用者プロセスがプログラムファイルの実行またはファイル名称変更をプログラムファイルアクセス制御方針に従って実行する。

プログラムファイル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を

以下の表 7-5 に、外部入出力アクセス制御方針で扱われるサブジェクトとセキュリティ属性を以下の表 7-6 に、オブジェクトとセキュリティ属性を以下の表 7-7 にそれぞれ示す。

表 7-5 プログラムファイル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

サブジェクト	オブジェクト	操作
一般利用者プロセス	一般 AP ファイル	実行、ファイル名称変更

表 7-6 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
一般利用者プロセス	抑止される利用者プログラム情報

表 7-7 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
一般 AP ファイル	ファイル名称

また、TOEは、インポートされたクライアント制御情報に従って、制御されたサブジェクトとオブジェクト間での操作を以下の表7-8の規則に従って実施する。

表 7-8 アクセスを管理する規則

サブジェクト	オブジェクト	操作	規則
一般利用者プロセス	一般APファイル	実行、ファイル名称変更	一般利用者プロセスは、抑止される利用者プログラム情報で指定したファイル名称の一般 AP ファイルを実行しないまたはファイル名称を変更しない

[FDP_ACC.1c] [FDP_ACF.1c]

TOE は、識別認証機能（クライアント）により許可された管理者または一般利用者と TOE 内部で管理者または一般利用者の操作をそれぞれ代行する管理者プロセス、一般利用者プロセスを対応付ける。管理者プロセスは、暗号鍵入力制御情報を付与したファイル暗号用共通鍵を暗号鍵ファイル入出力制御方針に従ってセキュリティ属性無しでエクスポート暗号鍵ファイルに書き出し、一般利用者プロセスは、セキュリティ属性無しでインポート暗号鍵ファイルを読み込み、一般利用者が入力した入力文字列と暗号鍵入力制御情報に設定された文字列が一致した場合に、暗号鍵ファイル入出力制御方針に従ってファイル暗号用共通鍵を暗号鍵ファイルに書き出す。

ファイル暗号用共通鍵の暗号鍵ファイル入出力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を以下の表 7-9 に、暗号鍵ファイル入出力制御方針で扱われるサブジェクトとセキュリティ属性を以下の表 7-10 に、オブジェクトとセキュリティ属性を以下の表 7-11 にそれぞれ示す。

表 7-9 暗号鍵ファイル入出力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

サブジェクト	オブジェクト	操作
管理者プロセス	エクスポート暗号鍵ファイル	書き出し
一般利用者プロセス	インポート暗号鍵ファイル	読み込み
一般利用者プロセス	暗号鍵ファイル	書き出し

表 7-10 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
管理者プロセス	なし
一般利用者プロセス	なし

表 7-11 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
エクスポート暗号鍵ファイル	なし
インポート暗号鍵ファイル	なし
暗号鍵ファイル	暗号鍵入力制御情報

また、TOEは、暗号鍵入力制御情報に従って、制御されたサブジェクトとオブジェクト間での操作を以下の表7-12の規則に従って実施する。

表 7-12 アクセスを管理する規則

サブジェクト	オブジェクト	操作	規則
管理者プロセス	エクスポート暗号鍵ファイル	書き出し	管理者プロセスは、ファイル暗号用共通鍵データ及び暗号鍵入力制御情報を書き出す
一般利用者プロセス	インポート暗号鍵ファイル	読み込み	一般利用者プロセスはインポート暗号鍵ファイルを読み込む
	暗号鍵ファイル	書き出し	一般利用者プロセスは、ファイル暗号用共通鍵データに付与された暗号鍵入力制御情報を入力した時、ファイル暗号用共通鍵データを書き出す

[FDP_ETC.2]
TOEは、暗号機能（クライアント）により、[FDP_ACC.1c]にて定義された暗号鍵ファイル入出力制御方針に従って、ファイル暗号に使用する鍵に暗号鍵入力制御情報を付与して書き出す。なお、この書き出しについては管理者のみが実施することができる。

[FDP_ITC.2]
TOEは、暗号機能（クライアント）により、[FDP_ACC.1c]にて定義された暗号鍵ファイル入出力制御方針に従って、ファイル暗号に使用する鍵の読み込み時に文字列の照合を行い、読み込まれる鍵に付与された暗号鍵入力制御情報と、入力された文字列が一致した場合の

みファイル暗号に使用する鍵の読み込みを許可する。

[FIA_ATD.1]
TOEは、利用者に応じて、以下のセキュリティ属性を対応付けて保持する。

＜保持するセキュリティ属性のリスト＞
- I/Oポート利用制御情報
- プリンタ利用制御情報
- 許可されたプリンタ情報
- 許可USBデバイス入出力制御情報
- 外部メディア出力制御情報
- 許可外部メディア入出力制御情報
- 抑止される利用者プログラム情報
- 利用者ＩＤ

[FIA_USB.1]
TOEは、ログオンした利用者に応じて、TOEの内部で管理者または一般利用者を代行して動作するサブジェクトに対して以下の利用者セキュリティ属性のリストを対応付ける。

＜利用者セキュリティ属性のリスト＞
- I/Oポート利用制御情報
- プリンタ利用制御情報
- 許可されたプリンタ情報
- 許可USBデバイス入出力制御情報
- 外部メディア出力制御情報
- 許可外部メディア入出力制御情報
- 抑止される利用者プログラム情報
- 利用者ＩＤ

[FMT_MSA.1a]
TOE は、表 7-13 のとおり、外部入出力アクセス制御方針に従って識別認証機能（管理者端末、クライアント）により許可された役割（管理者または一般利用者）に対して、セキュリティ属性に対して許可された操作のインタフェース以外を提供しないことにより、操作を許可された識別された役割に制限する。

表 7-13 セキュリティ属性の管理（I/O ポートの入出力制御）

セキュリティ属性	操作	役割

セキュリティ属性	操作	役割
I/Oポート利用制御情報	改変	管理者
プリンタ利用制御情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
許可USBデバイス入出力制御情報	改変	管理者
許可されたプリンタ情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
外部メディア出力制御情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
許可外部メディア入出力制御情報	改変	管理者

[FMT_MSA.1b]
TOE は、プログラムファイルアクセス制御方針に従って識別認証機能（管理者端末、クライアント）により許可された管理者または一般利用者に対して、表 7-14 のとおり、セキュリティ属性に対して、役割に対して許可された操作のインタフェース以外を提供しないことにより、操作を許可された識別された役割に制限する。

表 7-14 セキュリティ属性の管理（プログラムの起動制御）

セキュリティ属性	操作	役割
抑止される利用者プログラム情報	改変	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者

[FMT_MSA.1c]
TOE は、暗号鍵ファイル入出力制御方針に従って識別認証機能（管理者端末）により許可された管理者に対して、表 7-15 のとおり、セキュリティ属性に対して、役割に対して許可された操作のインタフェース以外を提供しないことにより、操作を許可された識別された役割に制限する。

表 7-15 セキュリティ属性の管理（暗号鍵ファイル入出力制御）

セキュリティ属性	操作	役割
暗号鍵入力制御情報	作成	管理者

[FMT_MSA.3a]
TOEは、外部入出力アクセス制御方針を実施するために使われるセキュリティ属性（表 7-13）に対して、制限的なデフォルト値を設定する。なお、セキュリティ属性のデフォル

ト値については、管理者のみが設定することができる。

[FMT_MSA.3b]
TOEは、プログラムファイルアクセス制御方針を実施するために使われるセキュリティ属性（表7-14）に対して、制限的なデフォルト値を設定する。なお、セキュリティ属性のデフォルト値については、管理者のみが設定することができる。

[FMT_MSA.3c]
TOEは、暗号鍵ファイル入出力制御方針を実施するために使われるセキュリティ属性（表7-15）に対して、制限的なデフォルト値を設定する。なお、セキュリティ属性のデフォルト値については、管理者のみが設定することができる。

[FMT_MTD.1]
TOEは、TSFデータに対して、表7-16に示すとおり、役割に応じた操作が行えるインタフェース以外を提供しないことによりTSFデータの操作を制御する。

表 7-16 TSF データに対する役割と操作のリスト

TSF データ	操作	役割
管理者ＩＤ	登録、問い合わせ	管理者
一般利用者ＩＤ	登録、問い合わせ	管理者
	問い合わせ	クライアント管理者
	問い合わせ	一般利用者
管理者パスワード	登録、改変	管理者
クライアント管理者パスワード	登録	管理者
	改変	クライアント管理者
一般利用者パスワード	登録	管理者
	改変	クライアント管理者
	改変	一般利用者
パスワード桁数	改変	管理者
パスワード有効期限	改変	管理者
監査証跡の警告サイズ	改変	管理者
連続認証失敗許容回数	改変	管理者
再認証時間	改変	管理者
LogViewer 起動制御情報	改変	管理者

[FMT_SMF.1]
TOE は、セキュリティ機能を適切に維持するため、認証された管理者による以下の項目の管理機能を持つ。
・LogViewer 起動制御情報
・監査証跡の警告サイズ

・以下のセキュリティ属性
　–I/0 ポート利用制御情報
　–プリンタ利用制御情報
　–許可されたプリンタ情報
　–許可 USB デバイス入出力制御情報
　–外部メディア出力制御情報
　–許可外部メディア入出力制御情報
　–ポート名
　–抑止される利用者プログラム情報
　–ファイル名称
・暗号鍵入力制御情報
・連続認証失敗許容回数
・利用者のパスワード桁数
・利用者のパスワード有効期限
・利用者のパスワード
・再認証時間
・利用者ＩＤ

[FMT_SMR.1]
TOEは、識別認証機能による利用者の識別結果に応じて、管理者として識別された場合は管理者の役割が関連付けられ、クライアント管理者として識別された場合はクライアント管理者の役割が関連付けられ、一般利用者として識別された場合は一般利用者としての役割が関連付けられる。

7.1.3. 識別認証機能

[FIA_AFL.1]
TOEは、管理者及び一般利用者が入力した利用者ＩＤに対するパスワードとTOE内部で保持している利用者ＩＤ・パスワードの照合結果が不一致の場合、利用者ＩＤ毎に連続した不成功認証試行回数カウンタをカウントアップし、連続した不成功認証試行回数カウンタのカウンタ値が連続認証失敗許容回数を上回った時、ＰＣをロックする。
なお、連続認証失敗許容回数は一般利用者毎及び管理者毎に設定されており、管理者が1～99の範囲内で設定する。

[FIA_SOS.1]
TOEは、管理者パスワード、一般利用者パスワード及び暗号鍵入力制御情報が入力された場合、以下の表7-17の品質尺度を満たすことを保証する。

表 7-17 定義された品質尺度のリスト

秘密情報	品質尺度
管理者パスワード 一般利用者パスワード	・ASCII 文字であり、以下の範囲の文字が使用できる。 - 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、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字 ・管理者の設定したパスワード桁数の設定に従う。 ・管理者の設定したパスワードの有効期限の設定に従う。
暗号鍵入力制御情報	・ASCII 文字であり、以下の範囲の文字が使用できる。 - アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字 - 数字は、[0-9]の合計 10 文字 - 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字、及び半角の空白。 ・桁数は、8 文字以上 32 文字以下。
LogViewer 起動制御情報	・ASCII 文字であり、以下の範囲の文字が使用できる。 - 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、及び半角の空白 ・桁数は、8 文字以上 127 文字以下。

[FIA_UAU.2] [FIA_UID.2]

TOEは、一般利用者、クライアント管理者及び管理者がクライアント及び管理者端末を利用する前に、利用者が入力した利用者ＩＤ・パスワードとTOEが保持している利用者ＩＤ・パスワードを照合することにより、正当な利用者であることを識別認証し利用を許可する。ログサーバの利用については、管理者が入力したLogViewer起動制御情報を照合することにより、正当な利用者であることを識別認証し利用を許可する。

なお、TOEの提供する識別認証の機能は、管理者端末、クライアント及びログサーバ上のAPである「NECグループ情報漏洩防止システムV1.0 管理者端末アプリケーションソフトウェア Ver1.0」、「NECグループ情報漏洩防止システムV1.0 クライアントアプリケーションソフトウェア Ver1.0」及び「NECグループ情報漏洩防止システムV1.0 ログサーバアプリケーションソフトウェア Ver1.0」によって提供される識別認証の機能であり、OSにより提供される識別認証の機能ではない。

[FIA_UAU.6]

TOEは、管理者または一般利用者がTOEにログオンした後、TOEをまったく利用しない期間が、管理者が設定した再確認時間を超えた場合に、再度TOEを利用する場合は、TOEの正当な利用者であることを、利用者ＩＤ、パスワードにより再確認する。

[FIA_UAU.7]
TOEは、利用者が認証実施時のパスワード入力を行っている間は、実際の入力データを直接表示しないように、入力された文字の数だけ、予め定められたダミー（＊または●）を表示する機能を提供する。

7.1.4. 暗号機能

[FCS_CKM.1]
TOEは、表7-18に示す標準に合致した暗号鍵生成アルゴリズムと指定された暗号鍵長に従い暗号鍵を生成する。

表 7-18 暗号鍵と生成アルゴリズム

鍵の種類	標準	暗号鍵生成アルゴリズム	暗号鍵長
許可外部メディア用共通鍵	FIPS PUB 197	AES	128bit
ファイル暗号用共通鍵	FIPS PUB 46-3	3DES	168bit
	FIPS PUB 197	AES	128/192/256bit

TOEは、許可外部メディアの登録時、許可外部メディア用共通鍵を生成する。また、ファイル暗号用共通鍵については、管理者の作成した共通鍵を一般利用者が読み込み、利用者データファイルの暗号化に使用する。

[FCS_CKM.4]
TOEは、不要となった暗号鍵に対して、識別認証機能（クライアント）によりTOEの利用を許可された、鍵の所有者である一般利用者に対してのみ、暗号鍵ファイルを削除する機能を提供する。

[FCS_COP.1]
TOEは、表7-19で示される鍵を用いて、各暗号操作を行う。

表 7-19 暗号操作のための標準リスト、暗号アルゴリズム、暗号鍵長及び暗号操作

鍵の種類	標準	暗号アルゴリズム	暗号鍵長	暗号操作
許可外部メディア用共通鍵	FIPS PUB 197	AES	128bit	許可外部メディアへのファイルの書き出し時の暗号化・読み込み時の復号
ファイル暗号用共通鍵	FIPS PUB 46-3	3DES	168bit	利用者データの暗号化・復号
	FIPS PUB 197	AES	128/192/256bit	

これらの鍵を用いた各暗号操作については以下のとおり。
TOEは、許可外部メディアの登録時に、許可外部メディア用共通鍵を生成する。TOEは、許可外部メディアへのファイルの書き出し時には許可外部メディア用共通鍵を用いてファイルの暗号化を行う。また、ファイル暗号用共通鍵については、一般利用者が管理者の作成した共通鍵を読み込み、利用者データファイルの暗号化／復号に使用する。

以上