# InfoCage PC セキュリティ　Ver.1.22

# セキュリティターゲット

バージョン 1.12

2008 年 6 月 3 日

日本電気株式会社

# 更新履歴

| バージョン | 変更箇所 | | 変更日 | 更新者 |
|---|---|---|---|---|
| | 章・節・項 | 更新内容（概要） | | |
| 1.00 | 全体 | 新規作成 | 2007/10/15 | 日本電気株式会社 |
| 1.01 | 全体 | 評価機関指摘事項に対応 | 2007/10/29 | 日本電気株式会社 |
| 1.02 | 全体 | 評価機関指摘事項に対応 | 2007/12/28 | 日本電気株式会社 |
| 1.03 | 全体 | 評価機関指摘事項に対応 | 2008/02/29 | 日本電気株式会社 |
| 1.04 | 全体 | 評価機関指摘事項に対応 | 2008/03/14 | 日本電気株式会社 |
| 1.05 | 全体 | 評価機関指摘事項に対応 | 2008/03/21 | 日本電気株式会社 |
| 1.06 | 全体 | 評価機関指摘事項に対応 | 2008/03/31 | 日本電気株式会社 |
| 1.07 | 全体 | 評価機関指摘事項に対応 | 2008/04/07 | 日本電気株式会社 |
| 1.08 | 1.5.3 | 動作環境の変更 | 2008/04/11 | 日本電気株式会社 |
| 1.09 | 全体 | 評価機関指摘事項に対応 | 2008/05/09 | 日本電気株式会社 |
| 1.10 | 全体 | 評価機関指摘事項に対応 | 2008/05/23 | 日本電気株式会社 |
| 1.11 | 全体 | 評価機関指摘事項に対応 | 2008/05/27 | 日本電気株式会社 |
| 1.12 | 全体 | 誤記・修正漏れに対応 | 2008/06/03 | 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

# 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

| | |
|---|---|
| ST タイトル： | InfoCage PC セキュリティ Ver.1.22 セキュリティターゲット |
| ST バージョン： | 1.12 |
| ST 作成者： | 日本電気株式会社 |
| ST 作成日： | 2008 年 6 月 3 日 |

## 1.2. TOE 参照

| | |
|---|---|
| TOE 名称： | InfoCage PC セキュリティ |
| TOE バージョン： | Ver.1.22 |
| TOE 開発者： | 日本電気株式会社、NEC システムテクノロジー株式会社 |

## 1.3. 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

## 1.4. 用語

### 1.4.1. 本 ST における用語

| 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一つで、OS の権限を変更できる権限 |
| InfoCage PC セキュリティ | 定義されたポリシー情報を基に識別認証、PC 制御、暗号化、及び監査を行い、情報漏えいを防止するソフトウェア製品 |
| InfoCage 認証 | InfoCage PC セキュリティが導入された PC を操作可能にする際の識別認証であり、Windows 認証の前に行われる |
| InfoCage ユーザ ID | InfoCage 認証で使用されるユーザ識別子（Windows ユーザとは異なる） |
| InfoCage パスワード | InfoCage 認証で使用されるパスワード |
| I/O ポート | デバイスを接続するため PC に備えられた接続コネクタ |
| LogViewer | ログサーバで動作する、操作ログの閲覧、検索機能 |
| LogViewer 起動制御情報 | LogViewer を使用するための制御情報 |
| Windows 認証 | OS である Windows へのログオン時に行う識別認証であり、InfoCage 認証の後に行われる |
| Windows ユーザ ID | Windows 認証で使用されるユーザ識別子（InfoCage ユーザとは異なる） |
| 暗号鍵入力制御情報 | ファイル暗号用共通鍵をクライアントにインポートするための情報 |
| 暗号化ドライブ | 管理者に指定され、TOE の暗号機能により暗号化されるドライブ |
| 一時ログフォルダ | クライアントの操作ログが、ログサーバに送信されるまで保管されるフォルダ |
| 一般 AP | クライアント上で使用される、TOE 以外の AP |
| イントラネット | インターネットで普及した技術を利用して、特定の組織内に構築されたネットワーク |
| 外部メディア | CD、DVD や USB メモリのように、PC 本体内にはない外部の記録媒体 |
| 管理者端末 | 管理者が使用する、InfoCage PC セキュリティ 管理者端末ソフトウェアがインストールされた PC |
| 許可外部メディア | 管理者によりクライアント上での使用が許可され、ファイルの入出 |

| 用語 | 定義内容 |
|---|---|
| | 力時に TOE が自動的に暗号化/復号を行うリムーバブルメディア |
| 禁止対象 I/O ポート | 制御対象 I/O ポートのうち、許可外部メディアが接続された I/O ポートと異なる種類の I/O ポート<br>(例:許可外部メディアが USB ポートに接続するものであった場合は、USB ポートを除く制御対象 I/O ポートを指す) |
| クライアント | 一般利用者が使用する、InfoCage PC セキュリティ クライアントソフトウェアがインストールされた PC |
| クライアントセットアップ | 管理者端末、又はクライアントに InfoCage PC セキュリティをインストールするためのセットアップ用ファイルであり、管理者がクライアントセットアップ作成ツールで作成する |
| 再認証 | TOE にログオンした利用者から一定時間アクセスがない場合に要求される InfoCage 認証 |
| システムドライブ | OS がインストールされたドライブ |
| 自動暗号化フォルダ | OS 上のフォルダであり、TOE の暗号機能により格納されたファイルを自動的に暗号化する |
| 制御対象 I/O ポート | TOE で制御することができる I/O ポートであり、USB、シリアル/パラレル、IEEE1394、赤外線、PCMCIA のポートを指す。 |
| 制御対象外 I/O ポート | TOE で制御することができない I/O ポートであり、制御対象 I/O ポート以外のポートを指す。 |
| 操作ログ | 一般利用者がクライアント、又は管理者が管理者端末を、いつどのように操作したか記録した電子データ |
| デバイス | I/O ポートに接続する機器であり、CD/DVD デバイス、FD デバイス、USB デバイス、プリンタ等がある |
| ファイル暗号用共通鍵 | 利用者がファイルを暗号化/復号する際に使用する暗号鍵 |
| ポリシー情報 | クライアント、及び管理者端末上で InfoCage ユーザに適用される制限の定義情報であり、管理者がポリシー作成ツールで作成する |
| リムーバブルメディア | 外部メディアの中で OS がリムーバブルメディアと判断するもの(CD、DVD、FD を除く) |
| ログサーバ | InfoCage PC セキュリティ サーバソフトウェアがインストールされ、クライアント、及び管理者端末の操作ログが保存されるサーバ |
| ログ抽出情報 | 操作ログをクライアントからエクスポート、及びログファイルから操作ログをインポートする際に使用する情報 |
| ログ抽出暗号用共通 | 一般利用者が操作ログをエクスポートする際、又は利用者が操作ロ |

| 用語 | 定義内容 |
|---|---|
| 鍵 | グをインポートする際に使用する暗号鍵 |
| ロックアウト | 管理者が設定したロックアウトの閾値を越えて InfoCage 認証に失敗した際の InfoCage 認証を実行できない状態 |
| ロックアウトの閾値 | 管理者が許容する連続した InfoCage 認証の失敗回数であり、この回数を越えて InfoCage 認証に失敗するとロックアウトされる |

### 1.4.2. 略語

＜CC 関連略語＞

CC　コモンクライテリア（Common Criteria）
EAL　評価保証レベル（Evaluation Assurance Level）
IT　情報技術（Information Technology）
PP　プロテクションプロファイル（Protection Profile）
SFR　セキュリティ機能要件（Security Functional Requirement）
SFP　セキュリティ機能方針（Security Function Policy）
ST　セキュリティターゲット（Security Target）
TOE　評価対象（Target Of Evaluation）
TSF　TOE セキュリティ機能（TOE Security Functions）

＜TOE 関連略語＞

AP　アプリケーションプログラム（Application Program）
CPU　中央処理装置（Central Processing Unit）
DB　データベース（Database）
DBMS　データベース管理システム（Database Management System）
GB　ギガバイト（Giga Byte）
GHz　ギガヘルツ（Gigahertz）
HDD　ハードディスクドライブ（Hard Disk Drive）
ID　識別情報（Identification）
IEEE　電気電子学会（The Institute of Electrical and Electronics Engineers, Inc.）
IP　インターネットプロトコル（Internet Protocol）
LAN　ローカルエリアネットワーク（Local Area Network）
MAC　メディアアクセスコントロール（Media Access Control）
MB　メガバイト（Mega Byte）
OS　オペレーティングシステム（Operation System）
PC　パーソナルコンピュータ（Personal Computer）
PCMCIA ピーシーエムシーアイエー（Personal Computer Memory Card International Association）
SSL　セキュアソケットレイヤ（Secure Socket Layer）
TCP　伝送制御プロトコル（Transport Control Protocol）
USB　ユニバーサルシリアルバス（Universal Serial Bus）

# 1.5. TOE 概要

## 1.5.1. TOE の使用方法及び主要なセキュリティ機能の特徴

TOEである「InfoCage PCセキュリティ Ver.1.22」は、管理者が定義する「ポリシー情報」に基づき、PCからの情報漏洩を防止するためのセキュリティ機能（表 1-1参照）を提供するソフトウェア製品である。

TOE は、一般利用者が使用する「クライアント」、管理者が使用する「管理者端末」、及び PC の操作ログが蓄積される「ログサーバ」にインストールされ、使用される。

**表 1-1 TOE の主要なセキュリティ機能**

| セキュリティ機能 | 概要 |
|---|---|
| 識別認証機能 | ・利用者を識別認証する(※) |
| PC 制御機能 | ・I/O ポート、及びプリンタの利用可否を制御する<br>・許可外部メディアへのファイル出力を制御する |
| 暗号機能 | ・ドライブ単位の暗号化/復号を行う<br>・ファイル単位の暗号化/復号を行う<br>・許可外部メディアへのファイル出力時に暗号化を行う<br>・操作ログをリムーバブルメディアへエクスポート/インポートする時に暗号化/復号を行う |
| 監査機能 | ・操作ログを生成し、ログサーバに転送する<br>・ログサーバに蓄積された操作ログの閲覧、検索を行う<br>・操作ログをリムーバブルメディアへエクスポート、リムーバブルメディアから操作ログのインポートを行う |
| ポリシー設定機能 | ・ポリシー情報の作成、適用、変更を行う |

※認証方式は、パスワードによる認証方式を対象とする。

## 1.5.2. TOE 種別

本 TOE は、OS 上で動作する、PC からの情報漏洩を防止するためのアプリケーションソフトウェアである。（OS は TOE 範囲外である）

## 1.5.3. 必要な TOE 以外のハードウェア／ソフトウェア

TOEを動作させるために必要となる、TOE以外のハードウェア／ソフトウェアを表 1-2、及び表 1-3に示す。

表 1-2　ハードウェア構成

| 端末名 | 種別 | 説明 |
|---|---|---|
| ログサーバ | CPU | 3.0GHz 以上の x86 互換アーキテクチャの CPU |
| | メモリ | 1.0GB 以上 |
| | HDD | 340MB 以上の空き容量<br>（追加で操作ログの量に応じた空き容量が必要） |
| 管理者端末 | CPU | 1.0GHz 以上の x86 互換アーキテクチャの CPU |
| | メモリ | 1 GB 以上(OS が Windows Vista の場合) |
| | | 512MB 以上(OS が Windows XP の場合) |
| | HDD | システムドライブに 800MB 以上の空き容量<br>(OS が Windows Vista の場合) |
| | | システムドライブに 500MB 以上の空き容量<br>(OS が Windows XP の場合) |
| クライアント | CPU | 1.0GHz 以上の x86 互換アーキテクチャの CPU |
| | メモリ | 1 GB 以上(OS が Windows Vista の場合) |
| | | 512MB 以上(OS が Windows XP の場合) |
| | HDD | システムドライブに 800MB 以上の空き容量<br>(OS が Windows Vista の場合) |
| | | システムドライブに 500MB 以上の空き容量<br>(OS が Windows XP の場合) |

表 1-3　ソフトウェア構成

| 端末名 | 種別 | 製品名 |
|---|---|---|
| ログサーバ | OS | Microsoft Windows Server 2003 R2 Enterprise Edition 日本語版 (SP2) |
| | DBMS | Microsoft SQL Server 2005 日本語版（SP2） |
| | Web サーバ | Apache Tomcat 6.0 |
| | | Apache Axis 1.4 |
| | Java ランタイム | J2SE Runtime Environment 5.0 Update 13 |
| | JDBC ドライバ | Microsoft SQL Server 2005 JDBC Driver Ver.1.1 |
| 管理者 | OS(※) | Microsoft Windows Vista Ultimate 日本語版 |

| 端末名 | 種別 | 製品名 |
|---|---|---|
| 端末 | | 又は Microsoft Windows XP Professional 日本語版（SP2） |
| | Web ブラウザ | Microsoft Internet Explorer 6.0(SP2)<br>又は Microsoft Internet Explorer 7.0 |
| | AP 実行環境 | (OS が Microsoft Windows XP Professional 日本語版（SP2）の場合)<br>Microsoft .NET Framework 2.0<br>Microsoft .NET Framework 2.0 日本語 Language Pack |
| | | (OS が Microsoft Windows Vista Ultimate 日本語版の場合)<br>Microsoft .NET Framework 3.0<br>Microsoft .NET Framework 3.0 日本語 Language Pack |
| クライアント | OS(※) | Microsoft Windows Vista Ultimate 日本語版<br>又は Microsoft Windows XP Professional 日本語版（SP2） |

※32bit 版の OS のみをサポートする。

# 1.6. TOE 記述

## 1.6.1. TOE 関連の利用者役割

TOE における、利用者の役割は以下のとおりである。利用者の役割は、組織の責任者、管理者、一般利用者の 3 種類に分類され、役割毎に定義された権限の範囲の業務を行うことができる。なお、組織の責任者、管理者、一般利用者を総称して「利用者」と呼ぶ。

(1) 組織の責任者

TOE の利用組織における責任者である。組織の責任者は、信頼できる管理者を選出し、その役割を理解させた上で任命する。また、組織の責任者は、自ら組織に損害を与えるような行為を行わないため、脅威エージェントとはならない。

(2) 管理者

ログサーバ、及び管理者端末の管理を行う利用者であり、ログサーバ、及び管理者端末にログオンできる権限を有する。管理者は、クライアントを利用することもあるが、その際は、一般利用者とは異なる権限での操作が行える。管理者は、組織の責任者に任命された信頼できる者であるため、脅威エージェントとはならない。管理者の役割、及び管理者端末で行うことを以下に示す。

- InfoCage ユーザ ID、InfoCage パスワードの設定
- クライアントセットアップの作成、配付
- ポリシー情報の作成、配付

- ファイル暗号用共通鍵の作成、配付(管理者が自らに権限を与えた場合)
- 暗号鍵入力制御情報の作成、配付(管理者が自らに権限を与えた場合)
- 一般利用者から配付されたファイル暗号用共通鍵のインポート(一般利用者にファイル暗号用共通鍵を作成する権限を与えた場合)
- 操作ログの閲覧、検索(管理者端末から Web ブラウザ経由でログサーバにアクセスすることで操作ログの閲覧、検索を行う)

管理者がクライアントにログオンする場合に行える役割を以下に示す。

- クライアントの利用
- クライアントに登録されている InfoCage ユーザに適用されるポリシーの確認/更新
- クライアントに登録されている InfoCage ユーザのパスワードを変更

(3) 一般利用者

管理者の定義したポリシー情報に基づきクライアントを利用する利用者である。一般利用者は、自らが所属する組織の情報を積極的に暴露することはないが、情報セキュリティに関する脅威への認識が十分でないために許可されない操作を実行する可能性があるため、脅威エージェントとなり得る。一般利用者の役割を以下に示す。

- クライアントの利用
- 管理者から配付されたポリシー情報の適用
- ファイル暗号用共通鍵の作成、配付(管理者から権限が与えられている場合)
- 暗号鍵入力制御情報の作成、配付(管理者から権限が与えられている場合)
- 管理者、又は一般利用者から配付されたファイル暗号用共通鍵のインポート

(4) 第三者

TOE を利用する組織の要員ではない、外部の者を指す。第三者は、主に金銭目的で、利用者が組織外に持ち出したクライアント、又は外部メディアを不正に使用する可能性があるため、脅威エージェントとなり得る。

### 1.6.2. TOE の利用方法

管理者は、まずログサーバに InfoCage PC セキュリティ Ver.1.22 ログサーバソフトウェアを、管理者端末に InfoCage PC セキュリティ Ver1.22 管理者端末ソフトウェア(InfoCage PC セキュリティ Ver.1.22 クライアントソフトウェアを除く)をインストールする。その後、管理者端末においてクライアントセットアップ、ポリシー情報、許可外部メディアを作成し、一般利用者に配付する。管理者は作成したクライアントセットアップを使用して管理者端末に InfoCage PC セキュリティ Ver.1.22 クライアントソフトウェアをインストールし、ポリシー情報を適用する。一般利用者も同様に、管理者から配付された

クライアントセットアップを用いてクライアントをセットアップする。

セットアップ完了後、一般利用者は、管理者から安全な方法で通知された InfoCage ユーザ ID、及び InfoCage パスワードを用いた InfoCage 認証を行ってクライアントにログオンし、ポリシー情報の制限の範囲内でクライアントを利用する。また、ファイル暗号用共通鍵を作成する権限を持った管理者、又は一般利用者はファイル暗号用共通鍵を作成し、ファイル暗号用共通鍵を配付する権限を持った管理者、又は一般利用者はファイル暗号用共通鍵を配付する。管理者端末、又はクライアント内から外部にファイルを持ち出す場合は、許可外部メディアを使用し、暗号化した状態で持ち出す。許可外部メディア、管理者端末、及びクライアントには管理者が許可外部メディア入出力制御情報を設定し、許可外部メディアに設定されている許可外部メディア入出力制御情報と同一の許可外部メディア入出力制御情報が設定されている管理者端末、又はクライアントでのみ許可外部メディア内の保護対象データを復号することができる。また、許可外部メディア入出力制御情報が設定されていないリムーバブルメディアの場合は読み込みのみができる。

プリンタへファイルを出力する場合は、ポリシー情報(プリンタ利用制御情報)により利用が許可されているプリンタのみに対して出力することができる。

管理者が管理者端末、及び一般利用者がクライアントを操作した履歴は操作ログとしてログサーバに転送・蓄積される。管理者は蓄積された操作ログを定期的に閲覧・検索することによって、一般利用者による不正な利用の有無を確認し、必要に応じてポリシー情報を更新して一般利用者に配付する。管理者、及び一般利用者は、管理者から更新されたポリシー情報を入手し、管理者端末、又はクライアントに適用することができる。ただし、スタンドアロンでクライアントを使用している間は、ログサーバへの操作ログの転送・蓄積は行えないため、スタンドアロンで使用しているクライアント内の操作ログをリムーバブルメディアへエクスポートし、当該リムーバブルメディアを管理者端末、又は組織内 LAN に接続されているクライアントに装着し、当該リムーバブルメディアから操作ログをインポートすることで、管理者端末、又は組織内 LAN に接続されているクライアントが代行して操作ログをログサーバに転送する。

なお、クライアントセットアップ、ポリシー情報、及びファイル暗号用共通鍵の配付は、「アクセス制御されたサーバ等に保存し、アクセスを許可された一般利用者のみがダウンロードする」、「CD-R 等の書き換え不可能なメディアに保存し、管理者が一般利用者に直接手渡す」等の安全な方法で行われる。また、エクスポートした操作ログを格納したリムーバブルメディアの受け渡しは、「一般利用者から、操作ログを代行してログサーバへ転送する利用者へ直接手渡しする」等の安全な方法で行われる。

また、InfoCage 認証には USB メディア、FeliCa、又は指紋を用いる方式がオプションとして提供されるが、標準設定では InfoCage ユーザ ID、及び InfoCage パスワードを用いる方式が選択される。

その他、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。

表 1-4にクライアントセットアップに添付される情報を、表 1-5にポリシー情報の詳細を示す。

**表 1-4　クライアントセットアップに添付される情報**

| 添付情報 | 概要 |
|---|---|
| ポリシー情報 | クライアント、及び管理者端末上で InfoCage ユーザに適用される制限の定義情報であり、管理者が管理者端末で作成する |
| ログ抽出情報 | 操作ログをクライアントからエクスポート、及びログファイルから操作ログをインポートする際に使用する情報 |
| ファイル暗号用共通鍵に関する権限情報 | ファイル暗号用共通鍵を作成、配付する権限を与えるか否かの情報 |

**表 1-5　ポリシー情報の詳細**

| 制御項目 | 概要 |
|---|---|
| InfoCage ユーザ ID | InfoCage 認証で使用されるユーザ識別子 |
| InfoCage パスワード | InfoCage 認証で使用されるパスワード |
| InfoCage パスワード桁数 | InfoCage パスワードの最小文字数 |
| InfoCage パスワード有効期限 | InfoCage パスワードの有効日数 |
| ロックアウトの閾値 | 管理者が許容する連続した InfoCage 認証の失敗回数であり、この回数を越えて失敗するとロックアウトされる |
| 再認証時間 | 再認証が要求されるまでの、連続した TOE の未操作時間 |
| I/O ポート利用制御情報 | 制御対象 I/O ポートの利用可否を制御する情報 |
| プリンタ利用制御情報 | プリンタの利用可否を制御する情報 |
| リムーバブルメディア出力制御情報 | リムーバブルメディアへのファイル出力可否を制御する情報 |
| 許可外部メディア入出力制御情報 | 許可外部メディアを識別する情報 |
| ログファイル抽出制御情報 | リムーバブルメディアへの操作ログのエクスポート可否を制御する情報 |
| ログ警告サイズ | 一時ログフォルダの使用割合がこの値を越えると、利用者に |

| 制御項目 | 概要 |
|---|---|
| | 対して警告が発せられる |

### 1.6.3. 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。

#### 1.6.3.1. TOE の動作環境

TOEが動作するログサーバ、管理者端末、クライアント、関連するIT機器、及びネットワークのモデル動作環境を図 1-1に示す。

なお、TOE の動作に必要な環境は、(2)組織内 LAN、(3)ログサーバ、(4)クライアント、及び(5)管理者端末である。

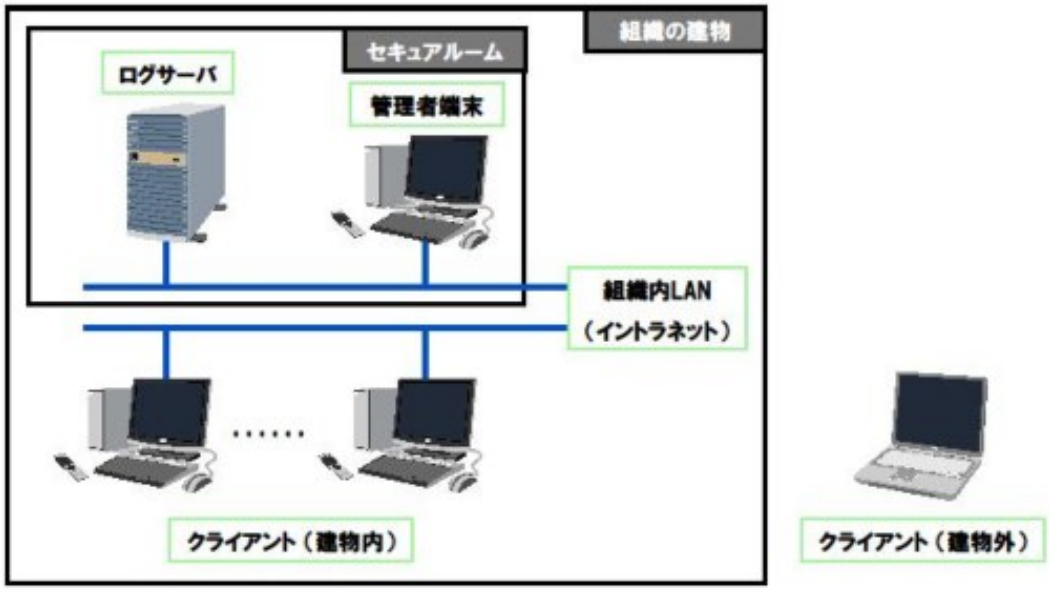


**図 1-1 TOE の動作環境**

(1) 物理的な配置

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、組織の建物内に設置され、組織内 LAN に接続される。ただし、クライアントは一時的に組織の建物外へ持ち出されることも考えられる。

また、ログサーバ、及び管理者端末は、組織の建物内の物理的に隔てられ、別途入室管理された部屋（以下、「セキュアルーム」という）に設置される。

(2)　組織内 LAN

組織内の機器を接続するイントラネットであり、ログサーバ、管理者端末及びクライアントは、通常この LAN に接続され運用される。

(3)　ログサーバ

ログサーバは、組織内 LAN に接続され、管理者に使用される。ログサーバには、管理者端末、及びクライアントから転送された操作ログが蓄積される。また、組織内 LAN を介しての管理者端末からの要求に応じて蓄積した操作ログを閲覧、及び検索することができる。

(4)　クライアント

クライアントは、組織内 LAN に接続され、管理者、又は一般利用者に使用される。管理者がクライアントを利用する場合は、一般利用者とは異なる権限での操作が行える。また、クライアントは一時的に組織の建物外へ持ち出されることも考えられるが、その際は組織内 LAN には接続されない。クライアントで生成された操作ログは、組織内 LAN を介してログサーバに転送される。

(5)　管理者端末

管理者端末は、組織内 LAN に接続され、管理者に使用される。管理者端末で生成された操作ログは、組織内 LAN を介してログサーバに転送される。また、管理者端末から組織内 LAN を介して、ログサーバに蓄積された操作ログを閲覧、及び検索する要求をログサーバに出すことができる。

#### 1.6.3.2. TOE のコンポーネント

図 1-2の破線内に示されるコンポーネントがTOEの物理的範囲である。

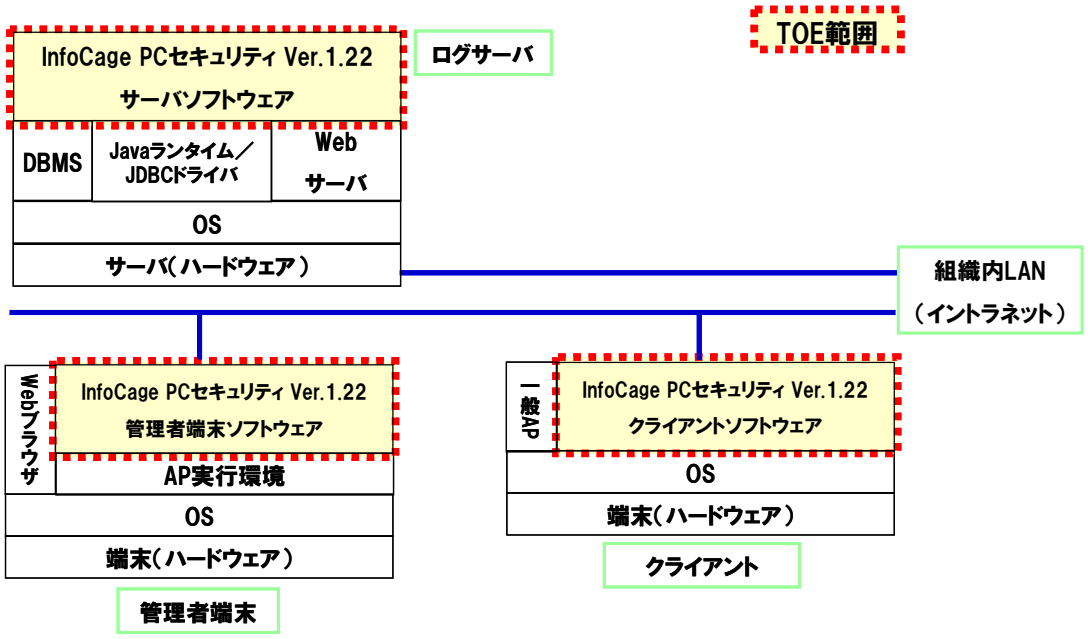


図 1-2　TOE のコンポーネント

TOEのソフトウェアコンポーネント名とバージョンを表 1-6に示す。

表 1-6　TOE のソフトウェアコンポーネント

| 機器名 | ソフトウェアコンポーネント名 |
|---|---|
| ログサーバ | InfoCage PC セキュリティ Ver.1.22 サーバソフトウェア<br>※ InfoCage PC セキュリティ Ver.1.22 サーバソフトウェアは、<br>以下のモジュールで構成されている<br>・InfoCage 簡易ログサーバ：バージョン 1.22.2525 |
| 管理者端末 | InfoCage PC セキュリティ Ver.1.22 管理者端末ソフトウェア(注)<br>※ InfoCage PC セキュリティ Ver.1.22 管理端末ソフトウェアは、<br>以下のモジュールで構成されている<br>・InfoCage PC セキュリティ(管理者ツール)：バージョン 1.2.2.3<br>上記以外のモジュールは、クライアントの項を参照のこと |
| クライアント | InfoCage PC セキュリティ Ver.1.22 クライアントソフトウェア<br>※ InfoCage PC セキュリティ Ver1.22 クライアントソフトウェアは、<br>以下のモジュールで構成されている<br>・InfoCage PC セキュリティ：バージョン 1.2.2.3<br>・InfoCage ファイル暗号：バージョン 2.00.0030<br>・InfoCage モバイル防御：バージョン 4.21.4000.0003 |

| 機器名 | ソフトウェアコンポーネント名 |
|---|---|
| | (OS が Microsoft Windows XP Professional 日本語版（SP2）の場合)<br>・InfoCage モバイル防御：バージョン 4.22.4000.0001<br>(OS が Microsoft Windows Vista Ultimate 日本語版の場合) |

注：InfoCage PC セキュリティ Ver.1.22 管理者端末ソフトウェアには、ポリシー作成ツール、クライアントセットアップ作成ツール、InfoCage PC セキュリティ Ver1.22 クライアントソフトウェアが含まれる。

図 1-2において、表 1-6で示したTOEの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（表 1-2、及び表 1-3参照）。

#### 1.6.3.3. 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 1-7に示す。

**表 1-7 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 | InfoCage PC セキュリティ Ver.1.22 インストールガイド (0122S06) |
| 利用者操作ガイダンス | InfoCage PC セキュリティ Ver.1.22 管理者ガイド (0122K06) |
| | InfoCage PC セキュリティ Ver.1.22 ユーザーズガイド (0122U06) |

### 1.6.4. TOE の論理的な範囲

図 1-3の「TOEのセキュリティ機能」に示される機能がTOEの論理的範囲となる。

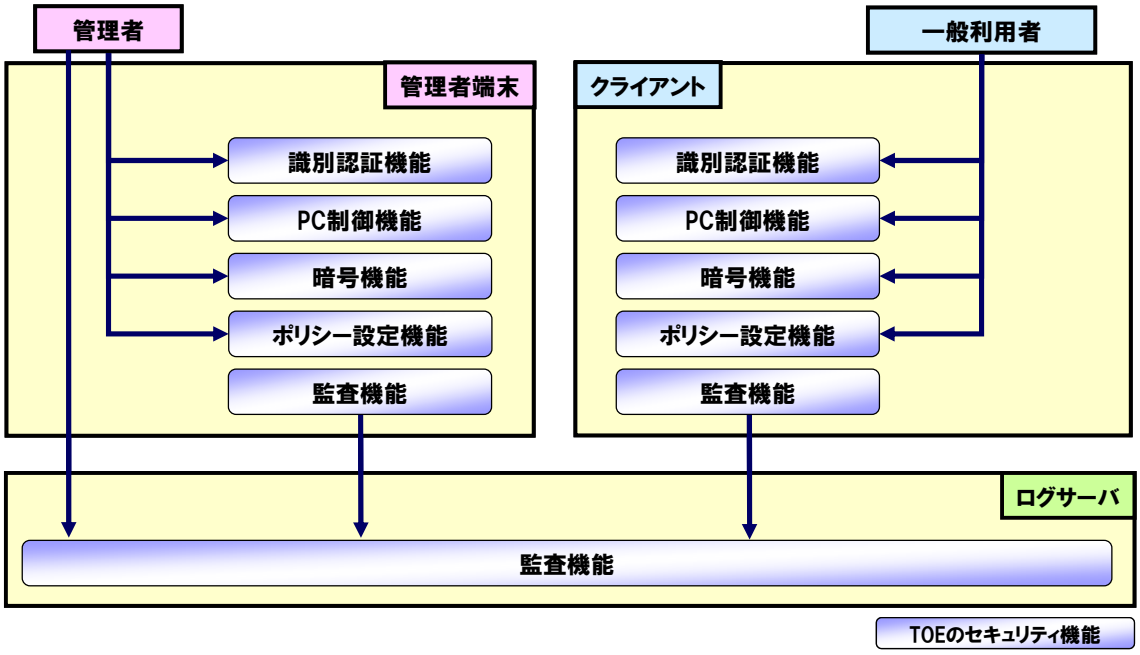


**図 1-3　TOE の論理構成図**

以下、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説明する。

(1)　識別認証機能

本機能は、一般利用者がクライアントを、管理者が管理者端末、又はクライアントを利用する前に識別認証（InfoCage 認証）を行い、一定時間管理者端末、又はクライアントの操作が行われない時に再認証を行う機能を提供する。機能の詳細を以下に示す。

＜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（InfoCage 認証）
- 管理者の InfoCage パスワードの変更
- ログオン後、一定時間管理者からアクセスがない場合の再認証

＜クライアント＞

- 一般利用者、又は管理者がクライアントにログオンする際の識別認証（InfoCage 認証）
- 一般利用者、又は管理者の InfoCage パスワードの変更
- ログオン後、一定時間一般利用者、又は管理者からアクセスがない場合の再認証

(2)　PC 制御機能

本機能は、管理者端末、又はクライアントに適用されたポリシー情報に基づき、PC の動作を制御する機能を提供する。機能の詳細を以下に示す。

＜管理者端末・クライアント共通＞

・　ポリシー情報に基づく以下の制御を行うように設定
  - 制御対象 I/O ポート、及びリムーバブルメディアへのデータ出力を制御するように設定
  - プリンタへの出力を制御するように設定

(3)　暗号機能

本機能は、暗号鍵ファイルの生成、及びファイルの暗号化/復号を行う機能を提供する。機能の詳細を以下に示す。

＜管理者端末・クライアント共通＞

・　TOE 導入時の内蔵 HDD をドライブ単位で暗号化
  ※　TOE のインストール時にドライブ単位で暗号化を行う。HDD からファイルの読み込みを行う際に自動的に復号を行い、HDD へファイルの書き込みを行う際に自動的に暗号化を行うので、利用者は暗号化/復号を意識することなく管理者端末、クライアントを使用することができる。
・　ファイルの暗号化／復号
  ※　利用者が指定したファイルの暗号化を行い、利用者が指定したタイミングで復号を行うので、ドライブ単位での暗号化のようにファイルを読み込む際に自動的に復号されることはない。
・　許可外部メディアにファイルを出力する際の自動暗号化
  ※　利用者がファイルを許可外部メディアに出力する際に自動的にファイルの暗号化を行い、許可外部メディアからファイルを読み込む際に自動的にファイルの復号を行う。
・　管理者端末、又はクライアントにおいてファイルを暗号化／復号する際に用いる、暗号鍵ファイルの生成、配付（※）
  ※　暗号鍵ファイルの生成、配付の機能の利用可否については、管理者によって指定された役割によって決められる。
・　ファイルを暗号化／復号する際に用いる暗号鍵ファイルのインポート

(4)　監査機能

本機能は、監査対象事象を操作ログとして取得し、ログサーバに転送した操作ログを検索、閲覧する機能を提供する。機能の詳細を以下に示す。

＜ログサーバ＞

・　管理者端末からの要求に応じて、ログサーバの DB に蓄積された操作ログの閲覧、検索を実行

＜管理者端末・クライアント共通＞
- 管理者端末、又はクライアントの操作ログの生成、及びログサーバへの送信
- ログサーバへ操作ログを送信する際の転送保護
- クライアントからリムーバブルメディアへエクスポートされた操作ログのインポート

＜管理者端末＞
- ログサーバへ操作ログの閲覧、検索要求を発行

＜クライアント＞
- 一時ログフォルダ内の操作ログをリムーバブルメディアへエクスポート

(5) ポリシー設定機能

本機能は、ポリシーの作成、変更、適用、及び参照の機能を提供する。機能の詳細を以下に示す。

＜管理者端末＞
- ポリシー情報の作成、変更

＜管理者端末・クライアント共通＞
- ポリシー情報の適用、参照

### 1.6.5. TOE 資産

本 TOE の保護資産は、以下に示す「保護対象データ」である。

＜保護対象データ＞
- 利用者が指定した任意のファイル
  ※ 盗難、紛失や PC 内部からの流出に対して保護することを想定
- 利用者が指定した自動暗号化フォルダ内のファイル
  ※ 盗難、紛失や PC 内部からの流出に対して保護することを想定
- 利用者が外部メディアに書き出したファイル
  ※ 盗難や紛失に対して保護することを想定
- 管理者の指定した暗号化ドライブ内のファイル
  ※ 盗難や紛失に対して保護することを想定

# 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 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

本 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ため、PP 適合根拠はない。

# 3. セキュリティ課題定義

本章では、脅威、組織のセキュリティ方針、及び前提条件について記述する。

## 3.1. 脅威

TOE に対する脅威を以下に示す。

**T.01**（不正なログオン）
第三者が、正当な利用者になりすまして TOE に不正にログオンし、保護対象データを搾取、暴露するかもしれない。

**T.02**（許可されていないプリンタへの出力）
一般利用者が、許可されていないプリンタに保護対象データを出力することにより、出力された保護対象データが第三者に搾取され、暴露されるかもしれない。

**T.03**（クライアントの盗難、紛失）
第三者にクライアントを盗難され、又は一般利用者が紛失したクライアントを第三者が入手し、当該クライアントに保存された保護対象データを暴露するかもしれない。

**T.04**（外部メディアの盗難、紛失）
第三者に外部メディアを盗難され、又は一般利用者が紛失した外部メディアを第三者が入手し、当該外部メディアに保存された保護対象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は無い。

## 3.3. 前提条件

前提条件を以下に示す。

**A.01**（セキュアルームへの機器設置）
ログサーバ、及び管理者端末は、管理者のみが入室できる室内（セキュアルーム）に設置される。

**A.02**（ログサーバの管理）
管理者以外は、ログサーバの OS、及び DBMS へログオンすることができない。また、管理者は定期的にログサーバ上に保存された操作ログのバックアップを取得し、ログサーバ上のディスクに十分な空き容量を確保する。

**A.03**（管理者の管理）
管理者は信頼できる者であり、不正な操作を行わない。
また､管理者から一般利用者への InfoCage ユーザ ID や InfoCage パスワードの通知、及びファイル(クライアントセットアップ、ポリシー情報、ファイル暗号用共通鍵、及

び暗号鍵入力制御情報)の配付については、管理者に許可された利用者のみが認識または入手できる、安全な方法で行う。また、管理者は、通知した InfoCage ユーザ ID、InfoCage パスワード、及び配付したファイルを確実にクライアントに設定するように、利用者に対して指導する。また、ファイル暗号用共通鍵、及び暗号鍵入力制御情報を配付する権限を一般利用者に与えた場合、管理者は、配付の権限を持った一般利用者が権限を持たない一般利用者へファイル暗号用共通鍵、及び暗号鍵入力制御情報を、安全な方法で配付するように指導する。

**A.04**（パスワードの管理）
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、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。
また、管理者は、上記に示したパスワードの管理を実施できるように、利用者に対して指導する。

**A.05**（操作ログをエクスポートしたリムーバブルメディアの管理）
スタンドアロンでクライアントを利用する利用者は、クライアント内の操作ログをエクスポートしたリムーバブルメディアを、同一組織内の利用者に渡す。外部メディアを受け取った利用者は、リムーバブルメディアからログをインポートし、操作ログをログサーバへ確実に転送する。
また、管理者は、上記に示したようにスタンドアロンで利用しているクライアントのログが確実にログサーバに転送されるように、利用者に対して指導する。

**A.06**（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は、ウイルス対策ソフトウェアを導入するとともに、常に最新のウイルス対策ソフトウェアのパターンファイルや、OS のセキュリティ対策用修正ソフトウェアを適用する。

# 4. セキュリティ対策方針

本章では、TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針、及びセキュリティ対策方針根拠について記述する。

## 4.1. TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を以下に示す。

**O.01**（利用者の識別認証）
TOE は、その利用開始時に利用者を識別認証しなければならない。

**O.02**（監査）
TOE は、TOE のセキュリティ機能に関連する事象を操作ログとして記録しなければならない。

**O.03**（I/O ポート制御）
TOE は、利用者毎に制御対象 I/O ポートの利用可否を制御するように OS に設定しなければならない。

**O.04**（プリンタ制御）
TOE は、利用者毎にプリンタの利用可否を制御するように OS に設定しなければならない。

**O.05**（許可外部メディア暗号化/復号）
TOE は、一般利用者がクライアント、又は管理者が管理者端末から許可外部メディアに保護対象データを入出力する際、当該データを暗号化/復号する機能を提供しなければならない。

**O.06**（ドライブ暗号化/復号）
TOE は、管理者の指定したドライブを暗号化/復号する機能を提供しなければならない。

**O.07**（ファイル暗号化/復号）
TOE は、利用者が指定したファイル、及び利用者が設定したフォルダ内のデータを暗号化/復号する機能を提供しなければならない。

**O.08**（リムーバブルメディア出力制御）
TOE は、リムーバブルメディアからのファイルの読み込みのみを許可し、リムーバブルメディアへの書き込みを制御する機能を提供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示す。

**OE.01**（セキュアルームへの機器設置）
管理者は、ログサーバ、及び管理者端末は、管理者のみが入室できる室内（セキュアルーム）に設置しなければならない。

**OE.02**（ログサーバの管理）
管理者は、管理者以外がログサーバの OS、及び DBMS にログオンできないよう、ログサーバの OS､及び DBMS には管理者のアカウントのみを登録しなければならない。また、管理者は、定期的にログサーバ上に保存された操作ログのバックアップを取ると共に、ログサーバ上のディスクに十分な空き容量を確保しなければならない。

**OE.03**（管理者の管理）
組織の責任者は、不正を行わない信頼できる管理者を任命し、管理者が不正を行わないよう監督し､管理者が適切に TOE を運用できるよう指導しなければならない｡また、管理者は、TOE の運用に必要な InfoCage ユーザ ID、InfoCage パスワード、及びファイル(クライアントセットアップ、ポリシー情報、ファイル暗号用共通鍵、及び暗号鍵入力制御情報)を管理者に許可された利用者のみが認識、又は入手できる方法で一般利用者に通知または配付しなければならない。また、管理者は、利用者に対して、通知した InfoCage ユーザ ID、InfoCage パスワード、及び配付したファイルを確実にクライアントに設定するように指導しなければならない。また、ファイル暗号用共通鍵、及び暗号鍵入力制御情報を配付する権限を一般利用者に与えた場合、管理者は、配付の権限を持った一般利用者が権限を持たない一般利用者へファイル暗号用共通鍵、及び暗号鍵入力制御情報を、安全な方法で配付するように指導しなければならない。

**OE.04**（パスワードの管理）
管理者は、利用者に対して、TOE にログオン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ことや、推測・解析されにくいパスワードを設定し、適切な間隔で定期的に変更することについて、指導しなければならない。

**OE.05**（接続機器の管理）
管理者は､利用者に対して､クライアントの制御対象外 I/O ポートに機器を接続しないよう指導しなければならない。

**OE.06**（操作ログをエクスポートしたリムーバブルメディアの管理）
管理者は､「スタンドアロンで利用されるクライアントからエクスポートされた操作ログ」を格納するリムーバブルメディアを、同一組織内の利用者に確実に渡すように、利用者に対して指導しなければならない。
また、管理者は、当該リムーバブルメディアを受け取った利用者が使用している管理者端末、又はクライアントに当該リムーバブルメディア内の操作ログをインポートし、ログサーバへ転送するよう当該リムーバブルメディアを受け取った利用者に対して指導しなければならない。

**OE.07**（外部メディアへの出力管理）
管理者は、一般利用者が平文のファイルを外部メディアへ出力する場合は外部メディアを適切に管理するように一般利用者に対して指導しなければならない。

**OE.08**（OS の動作）

OS は、TOE が OS 環境に設定した情報の通りに動作することで、管理者が許可した制御対象 I/O ポート、プリンタのみに出力を許可しなければならない。

**OE.09**（不正ソフトウェア対策）
管理者は、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、最新のウイルスパターンファイル、及び OS のセキュリティ対策修正ソフトウェアを適用しなければならない。また、管理者は、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、常に最新のウイルスパターンファイル、及び OS のセキュリティ対策修正ソフトウェアを適用するように一般利用者に対して指導しなければならない。

## 4.3. セキュリティ対策方針根拠

### 4.3.1. セキュリティ対策方針とセキュリティ課題定義の間の追跡

セキュリティ対策は、3 章で規定した脅威に対抗するためのもの、あるいはTOEの前提条件及び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 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**

| | T.01(不正なログオン) | T.02(許可されていないプリンタへの出力) | T.03(クライアントの盗難、紛失) | T.04(外部メディアの盗難、紛失) | A.01(セキュアルームへの機器設置) | A.02(ログサーバの管理) | A.03(管理者の管理) | A.04(パスワードの管理) | A.05(操作ログをエクスポートしたリムーバブルメディアの管理) | **A.06(不正ソフトウェア対策)** |
|---|---|---|---|---|---|---|---|---|---|---|
| O.01(利用者の識別認証) | × | | | | | | | | | |
| O.02(監査) | × | × | | | | | | | | |
| O.03(I/O ポート制御) | | | | × | | | | | | |
| O.04(プリンタ制御) | | × | | | | | | | | |
| O.05(許可外部メディア暗号化/復号) | | | | × | | | | | | |
| O.06(ドライブ暗号化/復号) | | | × | | | | | | | |
| O.07(ファイル暗号化/復号) | | | × | | | | | | | |
| O.08(リムーバブルメディア出力制御) | | | | × | | | | | | |

| | T.01(不正なログオン) | T.02(許可されていないプリンタへの出力) | T.03(クライアントの盗難、紛失) | T.04(外部メディアの盗難、紛失) | A.01(セキュアルームへの機器設置) | A.02(ログサーバの管理) | A.03(管理者の管理) | A.04(パスワードの管理) | A.05(操作ログをエクスポートしたリムーバブルメディアの管理) | **A.06(不正ソフトウェア対策)** |
|---|---|---|---|---|---|---|---|---|---|---|
| OE.01(セキュアルームへの機器設置) | | | | | × | | | | | |
| OE.02(ログサーバの管理) | | | | | | × | | | | |
| OE.03(管理者の管理) | | | | | | | × | | | |
| OE.04(パスワードの管理) | | | | | | | | × | | |
| OE.05(接続機器の管理) | | | | × | | | | | | |
| OE.06(操作ログをエクスポートしたリムーバブルメディアの管理) | | | | | | | | | × | |
| OE.07(外部メディアへの出力管理) | | | | × | | | | | | |
| OE.08(OS の動作) | | × | | × | | | | | | |
| OE.09(不正ソフトウェア対策) | | | | | | | | | | × |

### 4.3.2. 追跡の正当性

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、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＞

**T.01**（不正なログオン）
　この脅威は、第三者により実行される。第三者がとり得る具体的な不正ログオンの方法を示すと共に、有効な対抗策を示す。

a.　第三者が利用者になりすまし、保護対象データを搾取し、暴露する
　この攻撃に対しては、TOE の利用開始時に識別認証を行い、TOE の利用を正当な利用者のみに制限することで、脅威を軽減できる。
　また、識別認証の失敗に関する操作ログを記録することによって、不正なログオンの試行を検出し、脅威を緩和できる。
　**O.01**(利用者の識別認証)により利用を許可された TOE にログオンするための ID とパスワードを入力し、正しく識別認証されないと管理者端末またはクライアントを利用できないこととするとともに、**O.02**(監査)により識別認証の失敗の操作ログを採取することにより、上記の攻撃に対抗することができる。

　以上の攻撃方法に対抗することにより、第三者はクライアントを利用することができなくなるため、**T.01**(不正なログオン)に対抗することができる。従って、以上の攻撃方法への対抗策に該当する、**O.01**(利用者の識別認証)、**O.02**(監査)によって **T.01**(不正なログオン)に対抗できる。

**T.02**（許可されていないプリンタへの出力）
　この脅威は、一般利用者、及び第三者によって実行される。一般利用者、及び第三者がとり得る具体的な行動について示すと共に、有効な対抗策を示す。

a.　一般利用者が許可されていないプリンタに出力した保護対象データを、第三者が搾取し、暴露する
　この攻撃に対しては、クライアントで利用を許可するプリンタを明確に定め、保護対象データの出力を制御するように OS に設定し、OS は TOE が設定した情報の通りに利用を許可するプリンタのみに出力するように動作することで、脅威を軽減できる。
　また、管理者から許可されていないプリンタを追加しようとしたことに関する操作ログを記録することによって、許可されていないプリンタの追加の試行を検出し、脅威を緩和できる。
　**O.04**(プリンタ制御)、及び **OE.08**(OS の動作)により利用を許可するプリンタ以外には保護対象データに出力できないようにすることと、**O.02**(監査)により許可されていないプリンタの追加試行の操作ログを採取することにより、上記の攻撃に対抗することができる。

　以上の行動に対抗することにより、許可されていないプリンタへは保護対象データを出力することできず、第三者が保護対象データを入手することができなくなるため、**T.02**(許可されていないプリンタへの出力)に対抗することができる。従って、以上の攻撃方法への対抗策に該当する、**O.02**(監査)、**O.04**(プリンタ制御)、及び **OE.08**(OS の動作)によって **T.02**(許可されていないプリンタへの出力)に対抗できる。

**T.03**（クライアントの盗難、紛失）
　この脅威は、第三者によって実行される。第三者がとり得る具体的な攻撃方法を示すと

共に、有効な対抗策を示す。

a. 第三者が入手したクライアントから HDD を取り出し、保護対象データを暴露する
この攻撃に対しては、クライアント内の HDD に保存される保護対象データを暗号化し、許可された利用者のみが復号できるようにすることで、脅威を軽減できる。
**O.06**(ドライブ暗号化/復号)、及び **O.07**(ファイル暗号化/復号)により、クライアント内の HDD に保存される保護対象データを暗号化し、許可された利用者のみが復号できるようにすることにより、上記の攻撃に対抗することができる。

以上の攻撃方法に対抗することにより、第三者がクライアントを盗難しても保護対象データの内容を読み取ることができなくなるため、**T.03**(クライアントの盗難、紛失)に対抗することができる。従って、以上の攻撃方法への対抗策に該当する、**O.06**(ドライブ暗号化/復号)、**O.07**(ファイル暗号化/復号)によって **T.03**(クライアントの盗難、紛失)に対抗できる。

**T.04**（外部メディアの盗難、紛失）
この脅威は、第三者によって実行される。第三者がとり得る具体的な攻撃方法を示すと共に、有効な対抗策を示す。

a. 第三者が外部メディアを入手し、保護対象データを暴露する
この攻撃に対しては、許可外部メディアに保存される保護対象データを暗号化し、許可された利用者のみが復号できるようにすることで、脅威を軽減できる。
**O.05**(許可外部メディア暗号化/復号)により許可外部メディアに保存される保護対象データを暗号化し、許可された利用者のみが復号できるようにすることで、上記に対抗することができる。

また、許可外部メディア以外の外部メディアに保護対象データを暗号化せずに出力するには以下の 5 つのケースが考えられる。

1. 禁止対象 I/O ポートに接続した外部メディアに保護対象データを出力する。
このケースに対しては、禁止対象 I/O ポートを利用できないように OS に設定し、OS は TOE が設定した情報の通りに禁止対象 I/O ポートに接続された外部メディアに保護対象データを出力できないように動作することで、脅威を軽減できる。
このケースには、**O.03**(I/O ポート制御)、及び **OE.08**(OS の動作)により禁止対象 I/O ポートに接続した外部メディアに保護対象データを出力できないようにすることで対抗することができる。
2. 利用が許可された制御対象 I/O ポートに接続された外部メディア(リムーバブルメディアを除く)に保護対象データを出力する。
このケースに対しては、上記外部メディアへ保護対象データを出力する際は、必要最小限のファイルのみを出力することと、上記外部メディアを紛失しないように細心の注意を払うように管理者が一般利用者に対して指導を徹底することで、脅威を緩和できる。
このケースには、**OE.07**(外部メディアへの出力管理)により上記外部メディアに保護対象データを出力する場合は適切な管理を行うように利用者に指導することで対応することができる。
3. 利用が許可された制御対象 I/O ポートに接続されたリムーバブルメディア(許可外部メディア入出力制御情報が設定されていないリムーバブルメディア)に保護対象データを出力する。

このケースに対しては、上記リムーバブルメディアは読み込みのみを可能とし、保護対象データの出力を制御することによって、脅威を軽減できる。
このケースには、**O.08**(リムーバブルメディア出力制御)により上記リムーバブルメディアに保護対象データを出力できないようにすることで対抗することができる。

4. クライアントに既設されている機器(CD/DVD ドライブ、FD ドライブ等)に接続された外部メディアに保護対象データを出力する。
   このケースに対しては、上記外部メディアへ保護対象データを出力する際は、必要最小限のファイルのみを外部メディアに出力することと、外部メディアを紛失しないように細心の注意を払うように管理者が一般利用者に対して指導を徹底することで、脅威を緩和できる。
   このケースには、**OE.07**(外部メディアへの出力管理)により上記外部メディアに保護対象データを出力する場合は適切な管理を行うように利用者に指導することで対抗することができる。
5. 制御対象外 I/O ポート接続した外部メディアに保護対象データを出力する。
   このケースに対しては、管理者はクライアントの制御対象外 I/O ポートには外部メディアを接続しないように確認、指導を徹底し、制御対象外 I/O ポートに接続された外部メディアに保護対象データを出力できないようにすることによって、脅威を緩和できる。
   このケースには、**OE.05**(接続機器の管理)により制御対象外 I/O ポートには外部メディアを接続しないように利用者に指導することで対抗することができる。

以上の攻撃方法に対抗することにより、第三者が平文の状態で保護対象データを入手することができなくなるため **T.04**(外部メディアの盗難、紛失)に対抗することができる。従って、以上の攻撃方法への対抗策に該当する、**O.03**(I/O ポート制御)、**O.05**(許可外部メディア暗号化/復号)、**O.08**(リムーバブルメディア出力制御)、**OE.05**(接続機器の管理)、**OE.07**(外部メディアへの出力管理)、及び **OE.08**(OS の動作)によって **T.04**(外部メディアの盗難、紛失)に対抗できる。

＜前提条件＞

**A.01**（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、管理者端末）の設置に関するものである。それぞれに有効な対策方針を以下に示す。

a. ログサーバ、及び管理者端末を設置する部屋を制限する
   ログサーバ、及び管理者端末は、操作ログやポリシーを作成する機能等の TOE の運用に対して重要な情報を保持しているので、管理者以外は操作できないようにするために、ログサーバ、及び管理者端末は、組織の建物内の、物理的に隔てられ、別途入室管理された室内（セキュアルーム）に設置する。
   **OE.01**(セキュアルームへの機器設置)によりログサーバ、及び管理者端末を入室管理された室内(セキュアルーム)に設定することで上記を実現することができる。
b. 入室を許可する者を制限する
   a.と同様にログサーバ、及び管理者端末は、管理者以外は操作できないようにするために、ログサーバ、及び管理者端末が設置されるセキュアルームに入室を許可される者は、管理者のみとする。

**OE.01**(セキュアルームへの機器設置)により、セキュアルームに入室できる者を管理者のみに限定することで上記を実現することができる。

以上の対策を実施することにより、ログサーバ、及び管理者端末は、管理者のみが入室できるセキュアルームに設置されることになるため、**A.01**(セキュアルームへの機器設置)に応じることができる。従って、それぞれの要求に応じる対応策として該当する、**OE.01**(セキュアルームへの機器設置)の達成によって **A.01**(セキュアルームへの機器設置)が実現される。

**A.02**（ログサーバの管理）
この前提条件は、ログサーバの OS、及び DBMS の管理に関するものである。有効な対策方針を以下に示す。

a. ログサーバの OS、及び DBMS にログオンできる利用者を制限する
管理者以外にログを操作させないようにすることでログの正確性を保つために、ログサーバの OS、及び DBMS にログオンできる者を管理者のみに制限し、管理者がその設定を維持、管理する。
**OE.02**(ログサーバの管理)によりログサーバの OS、及び DBMS には管理者のみのアカウントを登録することにより上記を実現することができる。
b. ログサーバ上の操作ログの消失を防ぐ
管理者は、ログサーバ上の操作ログの消失を防ぐために、定期的にログサーバに保存されている操作ログのバックアップを取る。また、管理者は、ログサーバのディスク容量不足による操作ログの消失を防ぐために、DBMS のディスク使用量やログサーバのディスク残容量を定期的に確認し、ログサーバ上のディスクに十分な空き容量を確保する。
**OE.02**(ログサーバの管理)によりログサーバ上の操作ログのバックアップを取り、ディスク容量を確保することにより上記を実現することが出来る。

以上の対策を実施することにより、管理者以外は、ログサーバの OS、及び DBMS へログオンすることができなくなり、ログサーバ上の操作ログの消失を防ぐことができるため、**A.02**(ログサーバの管理)に応じることができる。従って、以上の要求に応じる対応策として該当する、**OE.02**(ログサーバの管理)の達成によって **A.02**(ログサーバの管理)が実現される。

**A.03**（管理者の管理）
この前提条件は、管理者の管理に関するものである。それぞれに有効な対策方針を以下に示す。

a. 信頼できる管理者の選任
管理者は、TOE の運用に関しての決定権を持っており、TOE をセキュアに運用するために重要な役割を持っている。そのため、管理者は組織の責任者により選任され、その役割、及び責任を十分に理解し、職務に忠実で決して悪意を抱かない者とする。
**OE.03**(管理者の管理)により不正を行わない信頼のできる者を管理者に任命することで上記を実現することができる。
b. 組織の責任者による監督
組織の責任者は、管理者が TOE をセキュアに運用するために、管理者に TOE の管理

状況を報告させ、不正を行わないよう監督すると共に、TOE を適切に運用できるよう指導する。
**OE.03**(管理者の管理)により組織の責任者が管理者に対して適切に TOE を運用できるように指導することで上記を実現することができる。

c. 管理者によるファイルの安全な方法での配付
管理者は、TOE の運用に関わる重要な情報を外部に漏らさないようにするために、一般利用者に対して InfoCage ユーザ ID、InfoCage パスワード、許可外部メディア及びファイル（クライアントセットアップ、ポリシー情報、ファイル暗号用共通鍵、及び暗号鍵入力制御情報）を通知または配付する場合は、「一般利用者に直接通知する」、「アクセス制御されたサーバ等に保存し、アクセスを許可された一般利用者のみがダウンロードする」、「CD-R 等の書き換え不可能なメディアに保存し、管理者が一般利用者に直接手渡す」等の安全な方法で管理者に許可された利用者のみに通知又は配付する。
**OE.03**(管理者の管理)により TOE の運用に関わる重要な情報を許可された一般利用者のみに通知又は配付することで上記を実現することができる。

d. 配付したファイルをクライアントに設定
管理者は、利用者に通知した InfoCage ユーザ ID、InfoCage パスワード、及び配付したファイル(クライアントセットアップ、ポリシー情報、ファイル暗号用共通鍵、及び暗号鍵入力制御情報)をクライアントに設定するように利用者に対して指導する。
**OE.03**(管理者の管理)により通知した InfoCage ユーザ ID、InfoCage パスワード、及び配付したファイルをクライアントに設定するように管理者が利用者を指導することで上記を実現することができる。

e. 一般利用者によるファイルの安全な方法での配付
管理者は、ファイル暗号用共通鍵、及び暗号鍵入力制御情報を配付する権限を一般利用者に与えた場合、ファイル暗号用共通鍵を外部に漏らさないようするために、配付の権限を持った一般利用者に対して、ファイル暗号用共通鍵、及び暗号鍵入力制御情報を通知、又は配付する場合は、「一般利用者に直接通知する」、「アクセス制御されたサーバ等に保存し、アクセスを許可された一般利用者のみがダウンロードする」、「CD-R 等の書き換え不可能なメディアに保存し、配付の権限を持った一般利用者が権限を持たない一般利用者に直接手渡す」等の安全な方法で管理者に許可された一般利用者のみに通知又は配付するように、配付の権限を持った一般利用者に対して指導する。
**OE.03**(管理者の管理)により、ファイル暗号用共通鍵、及び暗号鍵入力制御情報を配付する権限を持った一般利用者にファイル暗号用共通鍵、暗号鍵入力制御情報を安全に配付するように管理者が指導することで上記を実現することが出来る。

以上の対策を実施することにより、管理者は不正な操作を行わないことを保証でき、管理者が通知した InfoCage ユーザ ID、InfoCage パスワード、及び配付したファイルがクラ

イアントに設定されるため、**A.03**(管理者の管理)に応じることができる。従って、それぞれの要求に応じる対応策として該当する、**OE.03**(管理者の管理)の達成によって **A.03**(管理者の管理)が実現される。

**A.04**（パスワードの管理）
この前提条件は、利用者が TOE ログオン時に使用するパスワードの管理に関するものである。それぞれに有効な対策方針を以下に示す。

a. パスワードの安全な管理
利用者は、第三者によるクライアントへの不正なログオンを防ぐために、TOE にログオン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、管理者はパスワードを他人に漏らさないように利用者に対して指導する。
**OE.04**(パスワードの管理)によりパスワードを他人に漏らさないように管理者が利用者を指導することで上記を実現することができる。
b. パスワードの定期的な変更
利用者は、第三者によるクライアントへの不正なログオンを防ぐために、TOE にログオン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。また、管理者は、パスワードを定期的に変更するように利用者に対して指導する。
**OE.04**(パスワードの管理)によりパスワードを定期的に変更するように管理者が利用者を指導することで上記を実現することができる。

以上の対策を実施することにより、利用者はパスワードを他人に漏れないように管理することができるため、**A.04**(パスワードの管理)に応じることができる。従って、それぞれの要求に応じる対応策として該当する、**OE.04**(パスワードの管理)の達成によって **A.04**(パスワードの管理)が実現される。

**A.05**（操作ログをエクスポートしたリムーバブルメディアの管理）
この前提条件は、利用者がスタンドアロンで TOE を使用する際の操作ログの管理に関するものである。それぞれに有効な対策方針を以下に示す。

a. リムーバブルメディアの安全な配送
利用者は、スタンドアロンで利用するクライアントのログを紛失しないようにするために、スタンドアロンで利用されるクライアントからエクスポートされた操作ログを格納するリムーバブルメディアを「操作ログをエクスポートした一般利用者から、操作ログを代行して転送する利用者へ直接手渡しする」等の安全な方法で、第三者に当該リムーバブルメディアが渡らないように受け渡す。また、管理者は、第三者に当該リムーバブルメディアが渡らないよう、利用者に指導する。
**OE.06**(操作ログをエクスポートしたリムーバブルメディアの管理)により操作ログをエクスポートしたリムーバブルメディアは同一組織内の利用者へ確実に渡すように管理者が利用者に指導することで上記を実現することができる。
b. 操作ログの代行転送
スタンドアロンで利用されるクライアントからエクスポートされた操作ログを格納するリムーバブルメディアを受け取った利用者は、スタンドアロンで利用したクライアントのログが確実にログサーバに転送されるようにするために、当該リムーバブルメディアを管理者端末、又は組織内 LAN に接続されているクライアントにインポートすることによって、操作ログを代行してログサーバへ転送する。また、管理者は、当該リムーバブルメディアを受けとった利用者がログを確実にログサーバに転送するよう

に指導する。
**OE.06**(操作ログをエクスポートしたリムーバブルメディアの管理)により操作ログをエクスポートしたリムーバブルメディアを受け取った利用者に確実にログサーバへ操作ログを転送するように管理者が指導することで上記を実現することができる。

以上の対策を実施することにより、スタンドアロンで利用しているクライアントのログが確実にログサーバへ転送されるようになるため、**A.05**(操作ログをエクスポートしたリムーバブルメディアの管理)に応じることができる。従って、それぞれの要求に応じる対応策として該当する、**OE.06**(操作ログをエクスポートしたリムーバブルメディアの管理)の達成によって **A.05**(操作ログをエクスポートしたリムーバブルメディアの管理)が実現される。

**A.06**（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。それぞれに有効な対策方針を以下に示す。

a. ウイルス対策ソフトウェアの導入
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する。また、インストールしたウイルス対策ソフトウェアについて、常に最新のパターンファイルを適用する。
**OE.09**(不正ソフトウェア対策)により、管理者が、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常に最新のパターンファイルを適用する。また、一般利用者が使用するクライアントについては、一般利用者が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、常に最新のパターンファイルを適用するように管理者が指導することで上記を実現することができる。
b. OS のセキュリティ対策用修正ソフトウェアの更新
ログサーバ、管理者端末、及びクライアントにインストールされている OS に対して、常に最新のセキュリティ対策用修正ソフトウェアを適用する。
**OE.09**(不正ソフトウェア対策)により、管理者が、ログサーバ、管理者端末、及びクライアントの OS に対して、常に最新のセキュリティ対策用修正ソフトウェアを適用し、一般利用者が使用するクライアントについては、一般利用者がクライアントの OS に対して常に最新のセキュリティ対策用修正ソフトウェアを適用するように管理者が指導することで上記を実現することができる。

以上の対策を実施することにより、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、パターンファイル、及び OS のセキュリティ対策用修正ソフトウェアを最新の状態に保つことができるため、**A.06**(不正ソフトウェア対策)に応じることができる。従って、それぞれの要求に応じる対応策として該当する、**OE.09**(不正ソフトウェア対策)の達成によって **A.06**(不正ソフトウェア対策)が実現される。

# 5. 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 に適合しているため、拡張コンポーネントは無い。

# 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。本章で使用する用語の定義を以下に示す。

＜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 |
|---|---|
| 制御対象 I/O ポートのレジストリ | OS が保持しているレジストリであり、制御対象 I/O ポートの利用可否に関する情報 |
| プリンタのレジストリ | OS が保持しているレジストリであり、プリンタの利用可否に関する情報 |
| 暗号鍵ファイル | ファイル暗号用共通鍵を格納するファイル |
| リムーバブルメディア | OS がリムーバブルメディアと判断する外部の記録媒体であり、CD、DVD、FD を除いたもの |
| ログファイル | エクスポートした操作ログを格納するファイル |

＜操作＞

| 操作 | 定義 |
|---|---|
| データの出力 | 制御対象 I/O ポートへのデータの出力 |
| 印刷 | データの印刷 |
| 書き出し | 管理者端末から暗号鍵ファイルへの、ファイル暗号用共通鍵の書き出し、又はクライアントからログファイルへの操作ログの書き出し |
| 読み込み | 暗号鍵ファイルからクライアントへの、ファイル暗号用共通鍵の読み込み、又はログファイルから管理者端末、又はクライアントへの操作ログの読み込み |
| 設定 | OS のレジストリへのプリンタの利用可否情報の設定、又は OS への制御対象 I/O ポートの利用可否情報の設定 |
| 削除 | OS のプリンタのレジストリを削除 |
| 出力制御 | リムーバブルメディアへの出力を禁止する |

＜セキュリティ属性＞

| セキュリティ属性名 | 属性の内容 | 取り得る値 |
|---|---|---|
| I/O ポート利用制御情報 | USB、IEEE1394、シリアル/パラレル、赤外線、PCMCIA の各ポートの利用可否を指定する情報 | 「有効」、又は「無効」 |
| リムーバブルメディア出力制御情報 | リムーバブル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」、「すべてのリムーバブルメディアを利用禁止」、又は「すべてのリムーバブルメディアを許可」 |
| 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」 |
| 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 | メーカーID、製品 ID、シリアル番号 |
| 外部メディア情報 | OS が判定したメディアの種類の情報 | リムーバブルメディア、その他 |
| ポート名 | ポリシー情報に基づき利用の可否が制御されるポートの名称 | 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 |
| プリンタ利用制御情報 | プリンタの利用範囲を指定する情報 | 「一部許可」、「すべて許可」、「すべて拒否」 |
| 許可されたプリンタ情報 | ポリシー情報に基づき利用の可否を制御するプリンタを、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 |
| プリンタ登録情報 | プリンタのレジストリに登録されているプリンタの情報 | 登録されたプリンタ固有のレジストリキーの値 |
| ファイル暗号タイプ | ファイル暗号用共通鍵の利用範囲を指定する情報 | 「管理者」、「リーダ」、「メンバ」 |
| ファイル暗号利用許可情報 | ファイル暗号用共通鍵を利用してファイルの暗号化を許可する情報 | 「許可」、「禁止」 |
| 暗号鍵入力制御情報 | ファイル暗号用共通鍵をエク | 8 文字以上、32 文字以下の半 |

| セキュリティ属性名 | 属性の内容 | 取り得る値 |
|---|---|---|
| | スポート、インポートするための情報 | 角英数字記号 |
| ログ抽出情報 | 操作ログをエクスポート、インポートする際に使用する情報 | 1 文字以上、256 文字以下の半角英数字記号 |
| ログファイル抽出制御情報 | 操作ログのエクスポートの許可／禁止を指定するための情報 | 「ログファイルのエクスポートを許可する」、「ログファイルのエクスポートを禁止する」 |
| InfoCage ユーザ ID | InfoCage 認証で使用されるユーザ識別子 | 1 文字以上、127 文字以下の任意の文字列 |

＜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 | 監査対象事象の種別であり、エラー、警告、情報の 3 種類が存在する |
| メッセージ | 監査事象の結果であり、事象の詳細な内容を表す |
| ログ警告サイズ | 管理者端末、又はクライアントのログ保存領域に対する使用割合の閾値であり、使用割合がこの値を越えると、利用者に対して警告が発せられる |
| 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 | 利用者の指定したファイルを暗号化、及び復号する際に使用する暗号鍵 |
| ドライブ暗号用共通鍵 | 管理者の指定した暗号化ドライブを暗号化、及び復号する際に使用する暗号鍵 |
| ログ抽出暗号用共通鍵 | 利用者がエクスポート、又はインポートした操作ログを暗号化、及び復号する際に使用する暗号鍵 |
| 再認証時間 | 利用者が TOE にログオンした後の、連続した TOE 未操作時間 |

## 6.1. セキュリティ機能要件

本節では、TOE が提供するセキュリティ機能要件を記述する。なお、本節では 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]。

[詳細化]：監査記録を生成 → 監査記録を管理者端末、又はクライアント上で生成

[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.1b | ・禁止されたプリンタの追加、プリンタの利用禁止 |
| FIA_AFL.1 | ・ロックアウトの閾値を越えた InfoCage 認証失敗、及びそれに続いてとられるアクション（ロックアウト） |
| FIA_UAU.2a | ・InfoCage 認証の成功、失敗 |
| FIA_UID.2 | ・InfoCage 認証の成功、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]

[詳細化]：監査記録 → 管理者端末、又はクライアント上の監査記録

[割付：その他の監査関連情報]：

・イベント ID

・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。

[詳細化]：各監査対象事象 → 管理者端末、又はクライアント上の各監査対象事象

**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]：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、PC 名、IP アドレス、MAC アドレス}

[詳細化]：監査記録 → ログサーバ上に格納してある監査記録

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

[詳細化]：監査記録 → ログサーバ上に格納してある監査記録

**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
- InfoCage ユーザ ID
- PC 名
- IP アドレス
- MAC アドレス
- イベントタイプ
- イベント ID

[詳細化]：監査データ → ログサーバ上に格納してある監査データ

[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。

[詳細化]：監査証跡 → 管理者端末、又はクライアント上の監査証跡

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。

[詳細化]：監査証跡 → 管理者端末、又はクライアント上の監査証跡

[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。

[詳細化]：監査証跡 → 管理者端末、又はクライアント上の監査証跡

[割付：事前に定義された限界]：管理者の設定したログ警告サイズ

[割付：監査格納失敗の恐れ発生時のアクション]：監査データ消失の恐れが発生した PC を使用している利用者へ通知する。

**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。

[詳細化]：監査証跡 → 管理者端末、又はクライアント上の監査証跡

[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、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 | ANSI X9.17 | 擬似乱数生成アルゴリズム | 128bit |
| ファイル暗号用共通鍵 | ANSI X9.17 | 擬似乱数生成アルゴリズム | 168bit |
| | ANSI X9.17 | 擬似乱数生成アルゴリズム | 128/192/256bit から選択 |
| ドライブ暗号用共通鍵 | ANSI X9.17 | 擬似乱数生成アルゴリズム | 128bit |
| ログ抽出暗号用共通鍵 | ANSI X9.17 | 擬似乱数生成アルゴリズム | 256bit |

### 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、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 197 | AES | 128bit | 許可外部メディアへファイルを書き出す際の暗号化、読み込む際の復号 |
| ファイル暗号用共通鍵 | SP800-67 | 3DES | 168bit | 一般利用者の指定したファイルの暗号化、及び復号 |
| | FIPS 197 | AES | 128/192/256bit | |
| ドライブ暗号用共通鍵 | FIPS 197 | AES | 128bit | 管理者の指定したドライブの暗号化、及び復号 |
| ログ抽出暗号用共通鍵 | FIPS 197 | AES | 256bit | クライアントから操作ログをエクスポートする際の暗号化、エクスポートした操作ログをインポートする際の復号 |

## ○利用者データ保護（FDP）

### FDP_ACC.1a サブセットアクセス制御（制御対象 I/O ポートへの出力制御）

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＞

・管理者プロセス

・一般利用者プロセス

＜オブジェクト＞

・制御対象 I/O ポートのレジストリ

＜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 |
|---|---|---|
| 管理者プロセス<br>一般利用者プロセス | 制御対象 I/O ポートのレジストリ | 設定 |

[割付：アクセス制御 SFP]：I/O ポート制御方針

**FDP_ACC.1b サブセットアクセス制御（プリンタへの出力制御）**

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.1.1b 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＞

・管理者プロセス

・一般利用者プロセス

＜オブジェクト＞

・プリンタのレジストリ

＜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 |
|---|---|---|
| 管理者プロセス<br>一般利用者プロセス | プリンタのレジストリ | 設定、削除 |

[割付：アクセス制御 SFP]：プリンタ制御方針

**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＞

・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<br>一般利用者プロセス | 暗号鍵ファイル | 書き出し、読み込み |

[割付：アクセス制御 SFP]：暗号鍵ファイル入出力制御方針

**FDP_ACC.1d サブセットアクセス制御（リムーバブルメディア出力制御）**

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.1.1d 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＞

・リムーバブルメディア

＜SFPで扱われるサブジェクトとオブジェクト間の操作＞：表 6-7に示す。

**表 6-7 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<br>一般利用者プロセス | リムーバブルメディア | 出力制御 |

[割付：アクセス制御 SFP]：リムーバブルメディア出力制御方針

**FDP_ACC.1e サブセットアクセス制御（ログ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.1.1e 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＞

・ログファイル

＜SFPで扱われるサブジェクトとオブジェクト間の操作＞：表 6-8に示す。

**表 6-8 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 | ログファイル | 書き出し |
| 管理者プロセス<br>一般利用者プロセス | ログファイル | 読み込み |

[割付：アクセス制御 SFP]：ログ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（制御対象 I/O ポートの出力制御）**
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 6-9に示す。

表 6-9 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 |
|---|---|
| 管理者プロセス<br>一般利用者プロセス | I/O ポート利用制御情報<br>許可 USB デバイス入出力制御情報<br>許可外部メディア入出力制御情報<br>リムーバブルメディア出力制御情報 |

＜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 6-10に示す。

表 6-10 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 |
|---|---|
| 制御対象 I/O ポートのレジストリ | 外部メディア情報<br>ポート名 |

[割付：アクセス制御 SFP]：I/O ポート制御方針

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]：

制御されたサブジェクトは制御されたサブジェクトに対応するSFP関連セキュリティ属性(表 6-9)、及び制御されたオブジェクトに対応するSFP関連セキュリティ属性(表 6-10)が取る値に基づき、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。

＜制御されたサブジェクト＞：管理者プロセス、一般利用者プロセス

＜制御されたオブジェクト＞：制御対象 I/O ポートのレジストリ

＜制御された操作＞：設定

＜アクセスを管理する規則＞：表 7-2～表 7-7を参照

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（プリンタへの出力制御）**
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.1.1b 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 6-11に示す。

**表 6-11 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<br>一般利用者プロセス | プリンタ利用制御情報<br>許可されたプリンタ情報 |

＜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 6-12に示す。

**表 6-12 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 |
|---|---|
| プリンタのレジストリ | プリンタ登録情報 |

[割付：アクセス制御 SFP]：プリンタ制御方針

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]：

制御されたサブジェクトは制御されたサブジェクトに対応するSFP関連セキュリティ属性(表 6-11)、及び制御されたオブジェクトに対応するSFP関連セキュリティ属性(表 6-12)が取る値に基づき、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。

＜制御されたサブジェクト＞：管理者プロセス、一般利用者プロセス

＜制御されたオブジェクト＞：プリンタのレジストリ

＜制御された操作＞：設定、削除

＜アクセスを管理する規則＞：表 7-11を参照

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<br>一般利用者プロセス | ファイル暗号タイプ |

＜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 |
|---|---|
| 暗号鍵ファイル | 暗号鍵入力制御情報 |

[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]：

表 6-15に示す、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。

**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<br>一般利用者プロセス | 暗号鍵ファイル | 書き出し | 管理者プロセス、又は一般利用者プロセスが、「ファイル暗号タイプ」として「管理者」又は「リーダ」の権限を保有している場合、暗号鍵入力制御情報を入力した時にファイル暗号用共通鍵を暗号鍵ファイルに書き出す |
| 管理者プロセス<br>一般利用者プロセス | 暗号鍵ファイル | 読み込み | 管理者プロセス、又は一般利用者プロセスは、暗号鍵入力制御情報を入力した時、暗号鍵ファイルからファイル暗号用共通鍵を読み込む |

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_ACF.1d セキュリティ属性によるアクセス制御（リムーバブルメディア出力制御）**
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.1.1d 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 6-16に示す。

**表 6-16 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<br>一般利用者プロセス | リムーバブルメディア出力制御情報 |

＜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 6-17に示す。

**表 6-17 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 |
|---|---|
| リムーバブルメディア | 許可外部メディア入出力制御情報 |

[割付：アクセス制御 SFP]：リムーバブルメディア出力制御方針

FDP_ACF.1.2d 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]：

制御されたサブジェクトは制御されたサブジェクトに対応するSFP関連セキュリティ属性(表 6-16)、及び制御されたオブジェクトに対応するSFP関連セキュリティ属性(表 6-17)が取る値に基づき、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。

＜制御されたサブジェクト＞：管理者プロセス、一般利用者プロセス

＜制御されたオブジェクト＞：リムーバブルメディア

＜制御された操作＞：出力制御

＜アクセスを管理する規則＞：表 7-15を参照

FDP_ACF.1.3d 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.1.4d 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.1e セキュリティ属性によるアクセス制御（ログ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.1.1e 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 6-18に示す。

**表 6-18 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<br>一般利用者プロセス | ログファイル抽出制御情報 |

＜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 6-19に示す。

**表 6-19 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 |
|---|---|
| ログファイル | ログ抽出情報 |

[割付：アクセス制御 SFP]：ログファイル入出力制御方針

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

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

表 6-20に示す、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。

**表 6-20 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 | ログファイル | 書き出し | 一般利用者プロセスは、ログファイル抽出制御情報が「ログファイルのエクスポートを許可する」のとき、ログ抽出情報と共に操作ログをログファイルに書き出す |
| 管理者プロセス<br>一般利用者プロセス | ログファイル | 読み込み | 管理者プロセス、又は一般利用者プロセスは、管理者端末、又はクライアントに登録されているログ抽出情報が、ログファイル内に登録されているログ抽出情報と一致したとき、ログファ |

| | | | |
|---|---|---|---|
| | | | イルから操作ログを読み込む |

FDP_ACF.1.3e 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.1.4e 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.2a 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.2.1a 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.2.2a 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。

[詳細化]：利用者データ　→　暗号鍵ファイル

[詳細化]：セキュリティ属性　→　暗号鍵入力制御情報

FDP_ETC.2.3a 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.2.4a 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]：なし

**FDP_ETC.2b セキュリティ属性を伴う利用者データのエクスポート（操作ログのエクスポ**

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.2.1b 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]：ログファイル入出力制御方針

FDP_ETC.2.2b 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。

[詳細化]：利用者データ　→　ログファイル

[詳細化]：セキュリティ属性　→　ログ抽出情報

FDP_ETC.2.3b 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.2.4b 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]：なし

**FDP_ITC.2a セキュリティ属性を伴う利用者データのインポート（暗号鍵ファイルのインポート）**
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.2.1a 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.2.2a 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。

[詳細化]：利用者データ　→　暗号鍵ファイル

[詳細化]：セキュリティ属性　→　暗号鍵入力制御情報

FDP_ITC.2.3a 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.2.4a 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.2.5a 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]：なし

**FDP_ITC.2b セキュリティ属性を伴う利用者データのインポート（ログファイルのインポート）**

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.2.1b 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]：ログファイル入出力制御方針

FDP_ITC.2.2b 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。

[詳細化]：利用者データ　→　ログファイル

[詳細化]：セキュリティ属性　→　ログ抽出情報

FDP_ITC.2.3b 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.2.4b 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.2.5b 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]：なし

## ○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] ：InfoCage 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

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 6-21に示す。

**表 6-21 認証失敗時のアクションのリスト**

| 認証事象 | アクション |
|---|---|
| InfoCage 認証 | TOE は 3 分～3 分 30 秒の間のランダムな時間、PC をロックアウトする。その後、不成功の認証試行回数の値を 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、許可 USB デバイス入出力制御情報、許可外部メディア入出力制御情報、リムーバブルメディア出力制御情報、プリンタ利用制御情報、許可されたプリンタ情報、ファイル暗号タイプ、ログファイル抽出制

御情報

**FIA_SOS.1 秘密の検証**
下位階層：なし
依存性：なし

FIA_SOS.1.1 TSF は、秘密が[割付：定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付：定義された品質尺度]：表 6-22に示す。

**表 6-22 定義された品質尺度のリスト**

| 秘密情報 | 品質尺度 |
|---|---|
| InfoCage 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。<br>- 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<br>- 数字は、[0-9]の合計 10 文字<br>- 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{\|}~ 、及び半角スペースの 33 文字<br>・管理者の設定したパスワード桁数の設定に従う。<br>・管理者の設定したパスワードの有効期限の設定に従う。 |
| LogViewer 起動制御情報 | ・ASCII 文字であり、以下の範囲の文字が使用できる。<br>- アルファベットは、大文字[A-Z]の 26 文字、小文字[a-z]の 26 文字の合計 52 文字<br>- 数字は、[0-9]の合計 10 文字<br>- 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{\|}~ の 32 文字、及び半角の空白<br>・桁数は、8 文字以上 127 文字以下。 |
| 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。<br>- 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<br>- 数字は、[0-9]の合計 10 文字<br>- 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{\|}~ の 32 文字、及び半角の空白<br>・桁数は、8 文字以上 32 文字以下。 |

**FIA_UAU.2a アクション前の利用者認証（InfoCage 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.2.1a 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、一般利用者

[詳細化]：認証　→　InfoCage 認証

**FIA_UAU.2b アクション前の利用者認証（LogViewer 起動制御情報）**
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.2.1b 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、各利用者に認証が成功することを要求しなければならない。

[詳細化]：その利用者を代行する他の TSF 仲介アクション　→　LogViewer の起動

[詳細化]：利用者 → 管理者

[詳細化]：認証　→　LogViewer 起動制御情報による認証

**FIA_UAU.2c アクション前の利用者認証（暗号鍵入力制御情報）**
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.2.1c 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、各利用者に認証が成功することを要求しなければならない。

[詳細化]：その利用者を代行する他の TSF 仲介アクション　→　ファイル暗号用共通鍵のインポート

[詳細化]：利用者 → 管理者、一般利用者

[詳細化]：認証　→　暗号鍵入力制御情報による認証

**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**
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 → 一般利用者、管理者

**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、許可 USB デバイス入出力制御情報、許可外部メディア入出力制御情報、リムーバブルメディア出力制御情報、プリンタ利用制御情報、許可されたプリンタ情報、ファイル暗号タイプ、ログファイル抽出制御情報

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

[割付：属性の最初の関連付けの規則]：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（制御対象 I/O ポートへの出力制御）**
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 6-23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 6-23の列「操作」に示す。

[割付：許可された識別された役割]：表 6-23の列「役割」に示す。

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：I/O ポート制御方針、リムーバブルメディア出力制御方針

**表 6-23 セキュリティ属性の管理**

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| I/Oポート利用制御情報 | 作成、問い合わせ、改変 | 管理者 |
| 一般利用者本人の「I/Oポート利用制御情報」 | 問い合わせ | 一般利用者本人 |
| リムーバブルメディア出力制御情報 | 作成、問い合わせ、改変 | 管理者 |
| 一般利用者本人の「リムーバブルメディア出力制御情報」 | 問い合わせ | 一般利用者本人 |
| 許可外部メディア入出力制御情報 | 作成、問い合わせ、改変 | 管理者 |
| 許可USBデバイス入出力制御情報 | 作成、問い合わせ、改変 | 管理者 |

**FMT_MSA.1b セキュリティ属性の管理（プリンタへの出力制御）**
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.1.1b 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 6-24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 6-24の列「操作」に示す。

[割付：許可された識別された役割]：表 6-24の列「役割」に示す。

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：プリンタ制御方針

表 6-24 セキュリティ属性の管理

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| プリンタ利用制御情報 | 作成、問い合わせ、改変 | 管理者 |
| 許可されたプリンタ情報 | 作成、問い合わせ、改変 | 管理者 |
| 一般利用者本人の「プリンタ利用制御情報」 | 問い合わせ | 一般利用者本人 |
| 一般利用者本人の「許可されたプリンタ情報」 | 問い合わせ | 一般利用者本人 |

**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 6-25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 6-25の列「操作」に示す。

[割付：許可された識別された役割]：表 6-25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 6-25 セキュリティ属性の管理

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| 暗号鍵入力制御情報 | 作成 | 「ファイル暗号タイプ」として「管理者」、又は「リーダ」の権限を保有している管理者、又は一般利用者 |
| ファイル暗号タイプ | 作成、問い合わせ、改変 | 管理者 |
| 一般利用者本人の「ファイル暗号タイプ」 | 問い合わせ | 一般利用者本人 |

**FMT_MSA.1d セキュリティ属性の管理（ログ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.1.1d 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 6-26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 6-26 の列「操作」に示す。

[割付：許可された識別された役割]：表 6-26の列「役割」に示す。

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

**表 6-26 セキュリティ属性の管理**

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| ログファイル抽出制御情報 | 作成、問い合わせ、改変 | 管理者 |

**FMT_MSA.3a 静的属性初期化（制御対象 I/O ポートへの出力制御）**
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]：許可的

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：I/O ポート制御方針、リムーバブルメディア出力制御方針

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（プリンタへの出力制御）**
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.3.1b 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]：許可的

[割付：アクセス制御 SFP、情報フロー制御 SFP] ：プリンタ制御方針

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（ログ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] ：ログ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 6-27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 6-27の列「操作」に示す。

[割付：許可された識別された役割]：表 6-27の列「役割」に示す。

**表 6-27 TSF データの管理**

| TSF データ | 操作 | 役割 |
|---|---|---|
| InfoCage ユーザ ID | 作成、問い合わせ、削除 | 管理者 |
| | 問い合わせ | 一般利用者本人 |
| InfoCage パスワード | 作成、改変 | 管理者 |
| 一般利用者本人の InfoCage パスワード | 改変 | 一般利用者本人 |
| InfoCage パスワード桁数 | 作成、問い合わせ、改変 | 管理者 |
| InfoCage パスワード有効期限 | 作成、問い合わせ、改変 | 管理者 |
| ログ警告サイズ | 作成、問い合わせ、改変 | 管理者 |
| ロックアウトの閾値 | 作成、問い合わせ、改変 | 管理者 |
| 再認証時間 | 作成、問い合わせ、改変 | 管理者 |
| LogViewer 起動制御情報 | 改変 | 管理者 |
| ファイル暗号利用許可情報 | 作成、問い合わせ、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 6-28に示す。

**表 6-28 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 | 管理機能 |
|---|---|---|
| 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) | ・なし(利用者グループは固定であり、管理対象とはならない) |
| 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<br>・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） | ・ログ警告サイズ<br>・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(アクションは固定であり、管理対象とはならない) |
| 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（暗号鍵属性は固定であり、管理対象とはならない） |

| 機能要件 | CC パート 2 に規定された管理要件 | 管理機能 |
|---|---|---|
| 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_ACC.1d | ・なし | ・なし |
| FDP_ACC.1e | ・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 | ・なし(属性は固定であり、管理対象とはならない) |
| FDP_ACF.1b | ・明示的なアクセスまたは拒否に基づく決定に使われる属性の管理 | ・なし(属性は固定であり、管理対象とはならない) |
| 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 | ・なし(属性は固定であり、管理対象とはならない) |
| FDP_ACF.1d | ・明示的なアクセスまたは拒否に基づく決定に使われる属性の管理 | ・なし(属性は固定であり、管理対象とはならない) |
| FDP_ACF.1e | ・明示的なアクセスまたは拒否に基づく決定に使われる属性の管理 | ・なし(属性は固定であり、管理対象とはならない) |
| FDP_ETC.2a | ・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 | ・なし(エクスポート制御規則は固定であり、管理対象とはならない) |
| FDP_ETC.2b | ・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。 | ・なし(エクスポート制御規則は固定であり、管理対象とはならない) |
| FDP_ITC.2a | ・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(制御規則は固定であり、管理対象とはならない) |
| FDP_ITC.2b | ・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（制御規則は固定であり、管理対象とはならない） |
| FIA_AFL.1 | ・不成功の認証試行に対する閾値の管理<br>・認証失敗の事象においてとられるアクションの管理 | ・ロックアウトの閾値<br>・なし(アクションは固定であり、管理対象とはならない) |
| FIA_ATD.1 | ・もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる | ・I/O ポート利用制御情報<br>・許可 USB デバイス入出力制御情報<br>・許可外部メディア入出力制御情報<br>・リムーバブルメディア出力制御情報<br>・プリンタ利用制御情報<br>・許可されたプリンタ情報<br>・ファイル暗号タイプ<br>・ログファイル抽出制御情報 |
| FIA_SOS.1 | ・秘密の検証に使用される尺度の管理 | ・InfoCage パスワードの桁数<br>・InfoCage パスワードの有効期限 |
| FIA_UAU.2a | ・管理者による認証データの管理;<br>このデータに関係する利用者による認証データの管理 | ・InfoCage パスワード |
| FIA_UAU.2b | ・管理者による認証データの管理;<br>このデータに関係する利用者による認証データの管理 | ・LogViewer 起動制御情報 |
| FIA_UAU.2c | ・管理者による認証データの管理;<br>このデータに関係する利用者による認証データの管理 | ・暗号鍵入力制御情報 |
| 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 | ・InfoCage ユーザ ID |
| FIA_USB.1 | ・許可管理者は、デフォルトのサブジェクトの | ・なし(セキュリティ属性は固定であ |

| 機能要件 | CC パート 2 に規定された管理要件 | 管理機能 |
|---|---|---|
| | セキュリ属性を定義できる<br>・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 | り、管理対象とはならない)<br>・なし(セキュリティ属性は固定であり、管理対象とはならない) |
| 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（グループは固定であり、管理対象とはならない） |
| 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（グループは固定であり、管理対象とはならない） |
| 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（グループは固定であり、管理対象とはならない） |
| FMT_MSA.1d | ・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（グループは固定であり、管理対象とはならない） |
| 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;<br>・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（グループは固定であり、管理対象とはならない）<br>・なし（デフォルト値は固定であり、管理対象とはならない） |
| 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;<br>・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（グループは固定であり、管理対象とはならない）<br>・なし（デフォルト値は固定であり、管理対象とはならない） |
| 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<br>・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（グループは固定であり、管理対象とはならない）<br>・なし（デフォルト値は固定であり、管理対象とはならない） |
| FMT_MTD.1 | ・TSF データと相互に影響を及ぼし得る役割のグループを管理すること | ・なし（グループは固定であり、管理対象とはならない） |
| FMT_SMF.1 | ・なし | ・なし |
| FMT_SMR.1 | ・役割の一部をなす利用者のグループの管理 | ・なし（グループは固定であり、管理対象とはならない） |
| FPT_ITT.1 | ・TSF が(その改変から)保護すべき改変の種別の管理<br>・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（アクションは固定であり、管理対象とはならない）<br>・なし（アクションは固定であり、管理対象とはならない） |
| FPT_STM.1 | ・時間の管理 | ・なし(OS の機能を利用するため、管理対象とはならない) |

**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
・一般利用者本人

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。全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 EAL1 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 6-29に示す。

**表 6-29 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**

| 機能要件 | O.01(利用者の識別認証) | O.02(監査) | O.03(I/O ポート制御) | O.04(プリンタ制御) | O.05(許可外部メディア暗号化/復号) | O.06(ドライブ暗号化/復号) | O.07(ファイル暗号化/復号) | O.08(リムーバブルメディア出力制御) |
|---|---|---|---|---|---|---|---|---|
| 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_COP.1 | | | | | × | × | × | |
| FDP_ACC.1a | | | × | | | | | |
| FDP_ACC.1b | | | | × | | | | |
| FDP_ACC.1c | | | | | | | × | |
| FDP_ACC.1d | | | | | | | | × |
| FDP_ACC.1e | | × | | | | | | |
| FDP_ACF.1a | | | × | | | | | |
| FDP_ACF.1b | | | | × | | | | |
| FDP_ACF.1c | | | | | | | × | |
| FDP_ACF.1d | | | | | | | | × |
| FDP_ACF.1e | | × | | | | | | |
| FDP_ETC.2a | | | | | | | × | |
| FDP_ETC.2b | | × | | | | | | |
| FDP_ITC.2a | | | | | | | × | |
| FDP_ITC.2b | | × | | | | | | |
| FIA_AFL.1 | × | | | | | | | |
| FIA_ATD.1 | | × | × | × | | | × | × |
| FIA_SOS.1 | × | × | | | | | × | |
| FIA_UAU.2a | × | | | | | | | |
| FIA_UAU.2b | | × | | | | | | |
| FIA_UAU.2c | | | | | | | × | |
| FIA_UAU.6 | × | | | | | | | |
| FIA_UAU.7 | × | × | | | | | × | |
| FIA_UID.2 | × | | | | | | | |
| FIA_USB.1 | × | × | × | × | | | × | × |
| FMT_MSA.1a | | | × | | | | | × |
| FMT_MSA.1b | | | | × | | | | |

| 機能要件 | O.01(利用者の識別認証) | O.02(監査) | O.03(I/O ポート制御) | O.04(プリンタ制御) | O.05(許可外部メディア暗号化/復号) | O.06(ドライブ暗号化/復号) | O.07(ファイル暗号化/復号) | O.08(リムーバブルメディア出力制御) |
|---|---|---|---|---|---|---|---|---|
| FMT_MSA.1c | | | | | | | × | |
| FMT_MSA.1d | | × | | | | | | |
| 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 6-29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 TOE のセキュリティ機能要件により実現できることを説明し、各セキュリティ対策方針に対して必要な対策の詳細を分析する。また、それぞれの対策に対して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、要求する機能については、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.01**（利用者の識別認証）

この TOE セキュリティ対策方針は、正当な利用者のみに TOE の利用を許可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通りである。

a. 指定回数以内に認証成功しない場合、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「ロックアウトの閾値」を越えて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。
b. 推測困難な認証情報を用いる
　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。
c. 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.2a である。

d. 再認証を要求する
　利用者が PC の側を離れた際など、TOE が操作可能な状態で放置されると、正当な利用者以外の者に TOE を操作される恐れがある。そのため、TOE は管理者が設定した「再認証時間」が経過した場合、再認証を要求する。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。
e. 認証時の入力内容はダミー表示とする
　認証時に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、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。
f. 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。
g. 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、TOE を利用できる。TOE の利用に際し、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_USB.1 である。
h. 識別認証機能の管理機能を提供する
　TOE は、識別認証を実施するための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_MTD.1、及び FMT_SMF.1 である。
i. 識別認証機能に必要な役割を管理する
　TOE は、識別認証を実施するために必要な役割を利用者と関連付け、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、i すべての対策を満たすことは、O.01(利用者の識別認証)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_SOS.1、FIA_UAU.2a、FIA_UAU.6、FIA_UAU.7、FIA_UID.2、FIA_USB.1、FMT_MTD.1、FMT_SMF.1、及び FMT_SMR.1 の達成により、O.01(利用者の識別認証)を実現できる。

**O.02**（監査）
この TOE セキュリティ対策方針は、TOE のセキュリティ機能に関連する事象を操作ログとして記録することを求めている。操作ログは、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。また、操作ログは正確である必要があるため、不正に削除、又は改変されてはならない。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通りである。

a. 操作ログとして必要な情報を記録する
　TOEは、**T.01**(不正なログオン)、及び**T.02**(許可されていないプリンタ)の脅威に対抗するために必要な情報を記録しなければならない。そのため、表 6-1で示した監査対象事象を、正確な時刻と共に利用者と関連付けて記録する必要がある。この要件に該当するセキュリティ機能要件は、FAU_GEN.1、FAU_GEN.2、及びFPT_STM.1 である。
b. 取得した操作ログの利用を制限する
　取得した操作ログは、許可された利用者のみが、許可された範囲で利用できるよう、その利用を制限する必要がある。そのため TOE は、ログサーバに転送される前の管理

者端末、又はクライアント上に存在する操作ログを参照させず、ログサーバへ転送された操作ログの参照のみを、LogViewer 起動制御情報による認証に成功した管理者に許可する。また、LogViewer 起動制御情報による認証の際の入力情報をそのまま表示すると、管理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、ダミー表示にする必要がある。また、ログサーバ上の操作ログ参照においては、許可された条件に基づき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、FAU_SAR.3、FIA_UAU.7、及び FIA_UAU.2b である。

c. 推測困難な認証情報を用いる

認証を行うためには、LogViewer 起動制御情報が、管理者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、LogViewer 起動制御情報に対し、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。この機能要件に該当するセキュリティ属性は、FIA_SOS.1 である。

d. 取得した操作ログを保護する

取得した操作ログは、不正な削除、又は不正な改変から保護する必要がある。そのため TOE は、管理者端末、及びクライアントに格納された操作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、管理者端末、又はクライアント上の操作ログが管理者の設定した「ログ警告サイズ」を越えた場合、管理者、又は一般利用者に対し操作ログ消失の恐れがあることを通知する。更に、操作ログが満杯になった場合は、操作ログの消失を防止するアクションを実行する。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。

e. 操作ログを確実に転送する

管理者端末、又は組織内 LAN に接続されたクライアントにおいて生成された操作ログは、確実にログサーバへ転送される必要がある。そのため TOE は、操作ログを転送時の暴露、改変から保護しなければならない。

また、スタンドアロンで使用しているクライアントにおいて生成された操作ログについても、確実にログサーバへ転送される必要がある。そのため、スタンドアロンで使用しているクライアントの操作ログをリムーバブルメディアにセキュリティ属性(ログ抽出情報)と共にエクスポートする。操作ログをエクスポートしたリムーバブルメディアを、エクスポートしたセキュリティ属性(ログ抽出情報)と同一のセキュリティ属性(ログ抽出情報)を持った管理者端末、又は組織内 LAN に接続されたクライアントに接続し、操作ログをインポートする。これによって、管理者端末、又は組織内 LAN に接続されたクライアントが代行してインポートした操作ログをログサーバへ転送する。

この要件に該当するセキュリティ機能要件は、FDP_ACC.1e、FDP_ACF.1e、FDP_ETC.2b、FDP_ITC.2b、及び FPT_ITT.1 である。

f. 監査機能の管理機能を提供する

TOE は、監査を実施するための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_MTD.1、及び FMT_SMF.1 である。

g. 監査機能に必要な役割を管理する

TOE は、監査を実施するために必要な役割を利用者と関連付け、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。

h. 制御に必要となるセキュリティ属性を管理する

TOE は、ログファイル入出力制御に必要となるセキュリティ属性(ログファイ抽出制御情報)の操作の権限を、利用者の役割に応じて関連付ける。セキュリティ属性を操作

できるのは操作権限が与えられた利用者のみである。この要件に該当するセキュリティ機能要件は、FMT_MSA.1d、FMT_MSA.3c、及び FMT_SMR.1 である。

i. 利用者とプロセスの結合

TOE は、管理者、及び一般利用者に関連するセキュリティ属性(ログファイル抽出制御情報)と管理者、及び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。

以上、a、b、c、d、e、f、g、h、i すべての対策を満たすことは、O.02(監査)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、FDP_ACC.1e、FDP_ACF.1e、FDP_ETC.2b、FDP_ITC.2b、FIA_ATD.1、FIA_SOS.1、FIA_UAU.2b、FIA_UAU.7、FIA_USB.1、FMT_MSA.1d、FMT_MSA.3c、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_ITT.1、及び FPT_STM.1 の達成により、O.02(監査)を実現できる。

O.03（I/O ポート制御）

この TOE セキュリティ対策方針は、利用者を代行するプロセスが、あらかじめ設定された制御対象 I/O ポートに対するアクセス権限に応じて制御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通りである。

a. 制御対象 I/O ポートの出力制御に対する設定を行う

TOE は、制御対象 I/O ポートに対して、データ出力の可否を定義し制御する必要がある。TOE は、管理者プロセス及び一般利用者プロセスと制御対象 I/O ポートの操作リストを対応付け、それに従って制御対象 I/O ポートへのデータ出力を制御するように OS(制御対象 I/O ポートのレジストリ)に設定する。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、管理者、及び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、許可 USB デバイス入出力制御情報、許可外部メディア入出力制御情報、リムーバブルメディア出力制御情報）と管理者、及び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. 制御に必要となるセキュリティ属性を管理する

TOE は、I/O ポート制御に必要となるセキュリティ属性（I/O ポート利用制御情報、一般利用者本人の「I/O ポート利用制御情報」、リムーバブルメディア出力制御情報、一般利用者本人の「リムーバブル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、許可 USB デバイス入出力制御情報）の操作権限を、利用者の役割に応じて関連付ける。セキュリティ属性を操作できるのは、操作権限が与えられた利用者のみである。この要件に該当するセキュリティ機能要件は、FMT_MSA.1a、FMT_MSA.3a、及び FMT_SMR.1 である。

d. TSF データを管理する

TOE は、I/O ポート制御に関係する TSF データ（InfoCage ユーザ ID）に対する操作、及びその操作を実行できる役割を管理する。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。

以上、a、b、c、d すべての対策を満たすことは、O.03(I/O ポート制御)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.1a、FDP_ACF.1a、FIA_ATD.1、FIA_USB.1、FMT_MSA.1a、FMT_MSA.3a、FMT_MTD.1、及び FMT_SMR.1 の達成により、O.03(I/O ポート制御)を実現できる。

**O.04**（プリンタ制御）

この TOE セキュリティ対策方針は、利用者を代行するプロセスが、あらかじめ設定されたプリンタに対するアクセス権限に応じて制御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通りである。

a. プリンタの出力制御に対する設定を行う
   TOE は、プリンタに対して、印刷の可否を定義し制御する必要がある。TOE は、管理者プロセス及び一般利用者プロセスとプリンタの操作リストを対応付け、それに従って、プリンタの利用可否を制御するように OS(プリンタのレジストリ)に設定する。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. 利用者とプロセスの結合
   TOE は、管理者、及び一般利用者に関連するセキュリティ属性（プリンタ利用制御情報、許可されたプリンタ情報）と管理者、及び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. 制御に必要となるセキュリティ属性を管理する
   TOE は、プリンタ制御に必要となるセキュリティ属性（プリンタ利用制御情報、許可されたプリンタ情報、一般利用者本人の「プリンタ利用制御情報」、一般利用者本人の「許可されたプリンタ情報」）の操作権限を、利用者の役割に応じて関連付ける。セキュリティ属性を操作できるのは操作権限が与えられた利用者のみである。この要件に該当するセキュリティ機能要件は、FMT_MSA.1b、FMT_MSA.3b 及び FMT_SMR.1 である。
d. TSF データを管理する
   TOE は､プリンタ制御に関係する TSF データ(InfoCage ユーザ ID)に対する操作、及びその操作を実行できる役割を管理する。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。

以上、a、b、c、d すべての対策を満たすことは、O.04(プリンタ制御)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.1b、FDP_ACF.1b、FIA_ATD.1、FIA_USB.1、FMT_MSA.1b、FMT_MSA.3b、FMT_MTD.1、及び FMT_SMR.1 の達成により、O.04(プリンタ制御)を実現できる。

**O.05**（許可外部メディア暗号化/復号）

この TOE セキュリティ対策方針は、利用者が許可外部メディアに保護対象データを入出力する際、暗号化/復号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通りである。

a. 標準に基づく暗号鍵を生成する
   TOE は、国際標準により規格化された暗号鍵生成メカニズムによって暗号鍵を生成する。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 の機能により生成された暗号鍵を使用し、許可外部メディアへファイルを書き出す際に暗号化を行い、許可外部メディアからファイルを読み込む際に復号を行う。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。

以上、a、b すべての対策を満たすことは、O.05(許可外部メディア暗号化/復号)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、及び FCS_COP.1 の達成により、O.05(許可外部メディア暗号化/復号)を実現できる。

O.06（ドライブ暗号化/復号）
この TOE セキュリティ対策方針は、管理者の指定した暗号化ドライブ内のファイルを暗号化/復号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通りである。

a. 標準に基づく暗号鍵を生成する
TOE は、国際標準により規格化された暗号鍵生成メカニズムによって暗号鍵を生成する。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 の機能により生成された暗号鍵を使用し、管理者の指定した暗号化ドライブ内のファイルを暗号化/復号する。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。

以上、a、b すべての対策を満たすことは、O.06(ドライブ暗号化/復号)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、及び FCS_COP.1 の達成により、O.06(ドライブ暗号化/復号)を実現できる。

O.07（ファイル暗号化/復号）
この TOE セキュリティ対策方針は、利用者が指定した任意のファイル、及び利用者が設定した自動暗号化フォルダ内のファイルを暗号化/復号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通りである。

a. 標準に基づく暗号鍵を生成する
TOE は、国際標準により規格化された暗号鍵生成メカニズムによって暗号鍵を生成する。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 の機能により生成された暗号鍵を使用し、利用者の指定した任意のファイル、及び利用者が設定した自動暗号化フォルダ内のファイルを暗号化/復号する。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. 暗号鍵のインポート、及びエクスポート
TOE は、暗号鍵のインポート/エクスポートの実行について、許可する操作、及び規則に基づき、アクセス制御を実行する。また、暗号鍵をエクスポートする場合、セキュリティ属性（暗号鍵入力制御情報）と共にエクスポートする。また、TOE は、暗号鍵をインポートする場合、セキュリティ属性（暗号鍵入力制御情報）を入力して認証に成功した場合のみインポートする。また、セキュリティ属性(暗号鍵入力制御情報)を入力する際、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、ダミー表示にする必要がある。これらの要件に該当するセキュリティ機能要件は、FDP_ACC.1c、ADP_ACF.1c、FDP_ETC.2a、FDP_ITC.2a、FIA_UAU.2c、及び FIA_UAU.7 である。

d. 推測困難な認証情報を用いる

認証を行うためには、暗号鍵入力制御情報が、第三者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、暗号鍵入力制御情報に対し、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。

e. 制御に必要となるセキュリティ属性を管理する

TOE は、暗号鍵の入力制御に必要となるセキュリティ属性（暗号鍵入力制御情報、ファイル暗号タイプ、一般利用者本人の「ファイル暗号タイプ」）の操作権限を、利用者の役割に応じて関連付ける。セキュリティ属性を操作できるのは操作権限が与えられた利用者のみである。この要件に該当するセキュリティ機能要件は、FMT_MSA.1c、及び FMT_SMR.1 である。

f. ファイル暗号化/復号機能の管理機能を提供する

TOE は、ファイル暗号化/復号を実施するための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。

g. 利用者とプロセスの結合

TOE は、管理者、及び一般利用者に関連するセキュリティ属性(ファイル暗号タイプ)と管理者、及び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。

以上、a、b、c、d、e、f、g すべての対策を満たすことは、O.07(ファイル暗号化/復号)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_COP.1、FDP_ACC.1c、ADP_ACF.1c、FDP_ETC.2a、FDP_ITC.2a、FIA_ATD.1、FIA_SOS.1、FIA_UAU.2c、FIA_UAU.7、FIA_USB.1、FMT_MSA.1c、FMT_SMF.1、及び FMT_SMR.1 の達成により、O.07(ファイル暗号化/復号)を実現できる。

O.08（リムーバブルメディア出力制御）

この TOE セキュリティ対策方針は、利用者を代行するプロセスが、あらかじめ設定されたリムーバブルメディアに対するアクセス権限に応じて制御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通りである。

a. リムーバブルメディアに対するアクセス制御を実施する

TOE は、リムーバブルメディアに対して、出力の可否を定義し制御する必要がある。TOE は、管理者プロセス及び一般利用者プロセスとリムーバブルメディアの操作リストを対応付け、それに従ってリムーバブルメディアへの出力を制御する。この要件に該当するセキュリティ機能要件は、FDP_ACC.1d、及び FDP_ACF.1d である。

b. 利用者とプロセスの結合

TOE は、管理者、及び一般利用者に関連するセキュリティ属性（許可外部メディア入出力制御情報、リムーバブルメディア出力制御情報）と管理者、及び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. 制御に必要となるセキュリティ属性を管理する

TOE は、リムーバブルメディア出力制御に必要となるセキュリティ属性（許可外部

メディア入出力制御情報、リムーバブルメディア出力制御情報、一般利用者本人の許可外部メディア入出力制御情報）の操作権限を、利用者の役割に応じて関連付ける。セキュリティ属性を操作できるのは操作権限が与えられた利用者のみである。この要件に該当するセキュリティ機能要件は、FMT_MSA.1a、FMT_MSA.3a 及び FMT_SMR.1 である。

d. TSF データを管理する

TOE は、リムーバブルメディア出力制御に関係する TSF データ（InfoCage ユーザ ID）に対する操作、及びその操作を実行できる役割を管理する。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。

以上、a、b、c、d すべての対策を満たすことは、O.08(リムーバブルメディア出力制御)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.1d、FDP_ACF.1d、FIA_ATD.1、FIA_USB.1、FMT_MSA.1a、FMT_MSA.3a、FMT_MTD.1、及び FMT_SMR.1 の達成により、O.08(リムーバブルメディア出力制御)を実現できる。

### 6.3.2. セキュリティ機能要件依存性

セキュリティ機能要件のコンポーネントの依存性を表 6-30に示す。

**表 6-30 セキュリティ機能要件のコンポーネントの依存性**

| 機能要件 | CC パート 2 で規定されている依存先コンポーネント | 依存性を満たすコンポーネント | 依存性が満たされないコンポーネント |
|---|---|---|---|
| FAU_GEN.1 | FPT_STM.1 | FPT_STM.1 | なし |
| FAU_GEN.2 | FAU_GEN.1 | FAU_GEN.1 | なし |
| | FIA_UID.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 |
| FAU_STG.1 | FAU_GEN.1 | FAU_GEN.1 | なし |
| FAU_STG.3 | FAU_STG.1 | FAU_STG.1 | なし |
| FAU_STG.4 | FAU_STG.1 | FAU_STG.1 | なし |
| FCS_CKM.1 | FCS_CKM.2<br>または　FCS_COP.1 | FCS_COP.1 | FCS_CKM.2　(*1) |
| | FCS_CKM.4 | なし | FCS_CKM.4　(*2) |
| | FMT_MSA.2 | なし | FMT_MSA.2　(*3) |
| FCS_COP.1 | FDP_ITC.1<br>または　FDP_ITC.2<br>または　FCS_CKM.1 | FCS_CKM.1 | なし |
| | FCS_CKM.4 | なし | FCS_CKM.4　(*2) |
| | FMT_MSA.2 | なし | FMT_MSA.2　(*3) |
| FDP_ACC.1a | FDP_ACF.1 | FDP_ACF.1a | なし |
| FDP_ACC.1b | FDP_ACF.1 | FDP_ACF.1b | なし |
| FDP_ACC.1c | FDP_ACF.1 | FDP_ACF.1c | なし |
| FDP_ACC.1d | FDP_ACF.1 | FDP_ACF.1d | なし |
| FDP_ACC.1e | FDP_ACF.1 | FDP_ACF.1e | なし |
| FDP_ACF.1a | FDP_ACC.1 | FDP_ACC.1a | なし |
| | FMT_MSA.3 | FMT_MSA.3a | なし |
| FDP_ACF.1b | FDP_ACC.1 | FDP_ACC.1b | なし |
| | FMT_MSA.3 | FMT_MSA.3b | なし |
| FDP_ACF.1c | FDP_ACC.1 | FDP_ACC.1c | なし |
| | FMT_MSA.3 | なし | FMT_MSA.3　(*4) |
| FDP_ACF.1d | FDP_ACC.1 | FDP_ACC.1d | なし |
| | FMT_MSA.3 | FMT_MSA.3a | なし |
| FDP_ACF.1e | FDP_ACC.1 | FDP_ACC.1e | なし |
| | FMT_MSA.3 | FMT_MSA.3c | なし |
| FDP_ETC.2a | FDP_ACC.1<br>または　FDP_IFC.1 | FDP_ACC.1c | なし |
| FDP_ETC.2b | FDP_ACC.1<br>または、FDP_IFC.1 | FDP_ACC.1e | なし |
| FDP_ITC.2a | FDP_ACC.1<br>または FDP_IFC.1 | FDP_ACC.1 c | なし |
| | FDP_ITC.1<br>または　FTP_TRP.1 | なし | FTP_ITC.1<br>または FTP_TRP.1　(*5) |
| | FPT_TDC.1 | なし | FPT_TDC.1　(*6) |
| FDP_ITC.2b | FDP_ACC.1 | FDP_ACC.1e | なし |

| 機能要件 | CC パート 2 で規定されている依存先コンポーネント | 依存性を満たすコンポーネント | 依存性が満たされないコンポーネント |
|---|---|---|---|
| | または　FDP_IFC.1 | | |
| | FTP_ITC.1<br>または　FTP_TRP.1 | なし | FTP_ITC.1<br>または FTP_TRP.1　(*5) |
| | FPT_TDC.1 | なし | FPT_TDC.1　(*6) |
| FIA_AFL.1 | FIA_UAU.1 | FIA_UAU.2a | なし |
| FIA_ATD.1 | なし | なし | なし |
| FIA_SOS.1 | なし | なし | なし |
| FIA_UAU.2a | FIA_UID.1 | FIA_UID.2 | なし |
| FIA_UAU.2b | FIA_UID.1 | なし | FIA_UID.1　(*7) |
| FIA_UAU.2c | FIA_UID.1 | なし | FIA_UID.1　(*8) |
| FIA_UAU.6 | なし | なし | なし |
| FIA_UAU.7 | FIA_UAU.1 | FIA_UAU.2a<br>FIA_UAU.2b<br>FIA_UAU.2c | なし |
| FIA_UID.2 | なし | なし | なし |
| FIA_USB.1 | FIA_ATD.1 | FIA_ATD.1 | なし |
| FMT_MSA.1a | FDP_ACC.1<br>または　FDP_IFC.1 | FDP_ACC.1a、<br>FDP_ACC.1d | なし |
| | FMT_SMR.1 | FMT_SMR.1 | なし |
| | FMT_SMF.1 | FMT_SMF.1 | なし |
| FMT_MSA.1b | FDP_ACC.1<br>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 |
| FMT_MSA.1c | FDP_ACC.1<br>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 |
| FMT_MSA.1d | FDP_ACC.1<br>または、FDP_IFC.1 | FDP_ACC.1e | なし |
| | FMT_SMR.1 | FMT_SMR.1 | なし |
| | FMT_SMF.1 | FMT_SMF.1 | なし |
| FMT_MSA.3a | FMT_MSA.1 | FMT_MSA.1a | なし |
| | FMT_SMR.1 | FMT_SMR.1 | なし |
| FMT_MSA.3b | FMT_MSA.1 | FMT_MSA.1b | なし |
| | FMT_SMR.1 | FMT_SMR.1 | なし |
| FMT_MSA.3c | FMT_MSA.1 | FMT_MSA.1d | なし |
| | FMT_SMR.1 | FMT_SMR.1 | なし |
| FMT_MTD.1 | FMT_SMR.1 | FMT_SMR.1 | なし |
| | FMT_SMF.1 | FMT_SMF.1 | なし |
| FMT_SMF.1 | なし | なし | なし |
| FMT_SMR.1 | FIA_UID.1 | FIA_UID.2 | なし |
| FPT_ITT.1 | なし | なし | なし |
| FPT_STM.1 | なし | なし | なし |

表 6.11 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満たしている。例外について、依存関係が満たされなくとも問題が無い根拠を示す。

*1　FCS_CKM.1　→　FCS_CKM.2

FCS_CKM.1 の対象となる暗号鍵のうち、許可外部メディア用共通鍵は許可外部メディア内に、ドライブ暗号用共通鍵、及びログ抽出暗号用共通鍵はクライアント内に保存され、配付されることはない。

また、ファイル暗号用共通鍵は、4.2の**OE.03**(管理者の管理)に記載した通りTOEの機能を用いることなく、安全な方法で配付される。

よって、この依存関係は不要である。

*2　FCS_CKM.1、FCS_COP.1　→　FCS_CKM.4

FCS_CKM.1、及び FCS_COP.1 の対象となる暗号鍵のうち、許可外部メディア用共通鍵、ドライブ暗号用共通鍵、及びログ抽出暗号用共通鍵は、それぞれ許可外部メディア内、クライアント内に暗号化された状態で保存され、許可外部メディアのフォーマットまたは TOE のアンインストールを行わない限り、最初に生成した鍵を更新することなく使用するため、破棄されることはない。

また、ファイル暗号用共通鍵は、クライアントの暗号化されたドライブ内に存在するため、破棄する必要は無い。

よって、これらの依存関係は不要である。

*3　FCS_CKM.1、FCS_COP.1　→　FMT_MSA.2

FCS_CKM.1、及び FCS_COP.1 で取り扱う暗号鍵は管理されるセキュリティ属性を持たないため、何らかの値をセキュリティ属性として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。

*4　FDP_ACF.1c　→　FMT_MSA.3

FDP_ACF.1c で取り扱うセキュリティ属性(暗号鍵入力制御情報)は、作成時に管理者、又は管理者に指定された一般利用者がセキュリティ属性の値を直接入力するため、デフォルト値を持たない。

よって、この依存関係は不要である。

*5　FDP_ITC.2a、FDP_ITC.2b　→　FTP_ITC.1　または　FTP_TRP.1

暗号鍵ファイル、及びログファイルのインポートに際して、利用者が直接 TOE にセキュリティ属性を入力、及び TOE 内部でセキュリティ属性の値を設定するため、高信頼パス/チャネルを介した通信を使用する必要がない。

よって、この依存関係は不要である。

*6　FDP_ITC.2a、FDP_ITC.2b　→　FPT_TDC.1

暗号鍵ファイル、及びログファイルのインポート時に使用するセキュリティ属性である暗号鍵入力制御情報、及びログ抽出情報は、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がない。

よって、この依存関係は不要である。

*7　FIA_UAU.2b　→　FIA_UID.1

FIA_UAU.2b の対象となる LogViewer の起動については、管理者しか LogViewer への URL と起動のパスワードを知らないため、改めて利用者を識別する必要はない。

よって、これらの依存関係は不要である。

*8　FIA_UAU.2c　→　FIA_UID.1

FIA_UAU.2c の対象となるファイル暗号用共通鍵のインポートは、FIA_UAU.2a の InfoCage 認証に成功した正当な管理者、又は一般利用者のみが実行できるため、改めて利用者を識別する必要はない。

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、PC からの情報漏洩を防止する製品であるため、セキュリティ機能に対する信頼性が要求される。一方、高い保証レベルの評価では相応の評価期間、及びコストを要するため、本 TOE の開発サイクル、製品価格へ影響を及ぼすことも事実である。

以上を考慮すると、EAL1 は独立した第三者機関によるガイダンス文書の評価や独立テストが実施されるため、一定の信頼性を確保することができ、評価期間、及びコストが与える影響も妥当である。

ただし、PC からの情報漏洩を防止するという製品特性を鑑み、脅威分析を含めた完全なセキュリティターゲット評価を実施するため、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 のセキュリティ機能の要約仕様を記述する。

## 7.1. 識別認証機能

TOE のセキュリティ機能である「識別認証機能」は、利用者がローカル、又はリモートからクライアント、又はローカルから管理者端末を利用する前に識別認証（InfoCage 認証）を行い、一定時間クライアント、又は管理者端末の操作が行われない時に再認証を行う。また、識別認証機能は InfoCage パスワードを変更する機能を提供する。以下に、識別認証機能の要約仕様を示す。

[FIA_AFL.1]、[FIA_ATD.1]、[FIA_UAU.2a]、[FIA_UAU.7] 、[FIA_UID.2]、[FIA_USB.1]、[FMT_SMR.1]

TOE は、利用者がローカル、又はリモートからクライアント、又はローカルから管理者端末を利用する前に、InfoCage ユーザ ID、及び InfoCage パスワードを入力することを要求する。また、利用者が入力した InfoCage ユーザ ID、及び InfoCage パスワードと、TOE が保持する InfoCage ユーザ ID、及び InfoCage パスワードを照合することで識別認証を行い、正当な利用者のみに利用を許可する。

TOE は、利用者が入力した InfoCage ユーザ ID、InfoCage パスワードと、TOE 内部で保持している InfoCage ユーザ ID、InfoCage パスワードの照合結果が不一致の場合、InfoCage ユーザ ID 毎に連続した不成功認証試行の回数をカウントアップする。その値が「ロックアウトの閾値」を越えた時、TOE は 3 分～3 分 30 秒のランダムな時間 PC をロックアウトし、その後、カウントアップしていた不成功認証試行の回数の値を 0 にする。なお、本機能は再認証時には機能しない。

TOE は、利用者が InfoCage パスワードの入力を行っている間は、入力データを直接表示せず、入力された文字の数だけダミーとして「＊」を表示する。

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、及び一般利用者という役割を関連付ける。

TOE は、InfoCage 認証に成功した利用者を代行して動作するサブジェクト（管理者プロセス、一般利用者プロセス）に対して、以下のセキュリティ属性を対応付ける。

＜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
- 許可外部メディア入出力制御情報
- リムーバブルメディア出力制御情報
- ファイル暗号タイプ
- ログファイル抽出制御情報

また、TOE は、個々の利用者に対して、以下の<セキュリティ属性>を「ポリシー情報」として対応付けて保持する。また、TOE にログオンした利用者の操作を代行するプロセス(管理者プロセス、一般利用者プロセス)に対して、以下の<セキュリティ属性>を対応付ける。

<セキュリティ属性>

- I/O ポート利用制御情報
- 許可 USB デバイス入出力制御情報
- 許可外部メディア入出力制御情報
- リムーバブルメディア出力制御情報
- プリンタ利用制御情報
- 許可されたプリンタ情報
- ファイル暗号タイプ
- ログファイル抽出制御情報

[FIA_UAU.6]

TOE は、利用者が TOE にログオンした後、管理者の設定した「再認証時間」を越えて無操作の状態が続いた場合、再度 InfoCage ユーザ ID、及び InfoCage パスワードの入力を要求する。なお、本機能が動作する時は、連続した不成功認証試行の回数が「ロックアウトの閾値」を越えた場合でも、PC のロックアウトは行わない。

[FIA_SOS.1] 、[FMT_MTD.1]、[FMT_SMF.1]

TOEは、管理者に利用者のInfoCageパスワードを変更する機能、及び利用者に利用者本人のInfoCage パスワードを変更する機能を提供する。変更時には、表 7-1に示す品質尺度を満たすInfoCage パスワードのみを受け入れる。

**表 7-1 定義された品質尺度のリスト**

| 秘密情報 | 品質尺度 |
|---|---|

| 秘密情報 | 品質尺度 |
|---|---|
| InfoCage 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。<br>- 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<br>- 数字は、[0-9]の合計 10 文字<br>- 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{\|}~ の 32 文字<br>・管理者の設定したパスワード桁数の設定に従う。<br>・管理者の設定したパスワードの有効期限の設定に従う。 |

## 7.2. PC 制御機能

TOE のセキュリティ機能である「PC 制御機能」は、管理者端末、又はクライアントに適用されたポリシー情報に基づき、制御対象 I/O ポートに対応するレジストリへの利用可否情報の書き込み、制御対象のプリンタに対応するレジストリへの利用可否情報の書き込み、及び制御対象プリンタが追加された時の削除を行う。以下に、PC 制御機能の要約仕様を示す。

[FDP_ACC.1a]、[FDP_ACF.1a]

TOEは、管理者が管理者端末、又は一般利用者がクライアントにログオンした時に適用されるポリシー情報に基づき、管理者端末、又はクライアントの制御対象I/Oポートに機器が接続された時、又はログオン時に制御対象I/Oポートに機器が接続されていた時に、表 7-2～表 7-7に示すI/Oポート制御方針に従い、管理者がポリシー情報に設定した「I/Oポート利用制御情報」、「許可USBデバイス入出力制御情報」、「許可外部メディア入出力制御情報」、及び「リムーバブルメディア出力制御情報」に基づき、OS(制御対象I/Oポートのレジストリ)に利用情報(利用許可、利用禁止のいずれかの情報)を設定する。OSはTOEによって設定されたレジストリの情報に従って動作するため、レジストリを設定することによって、制御対象I/Oポートの利用可否が制御される。

また、I/Oポート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表 7-8に、サブジェクトと対応するセキュリティ属性を表 7-9に、オブジェクトと対応するセキュリティ属性を表 7-10にそれぞれ示す。

なお、OS の制御対象 I/O ポートのレジストリは、制御対象 I/O ポートに接続される機器毎に持っており、制御対象 I/O ポートに機器が接続されたタイミングで生成される。

判定条件①

TSFは、機器が接続された制御対象I/Oポートの「I/Oポート利用制御情報」を確認し、表 7-2に基づく判定を行う。

**表 7-2 判定条件①**

| サブジェクトに対 | セキュリテ | 操作 | 判定結果 |
|---|---|---|---|

| 応するSFP関連セキュリティ属性 | ィ属性の取る値 | | (操作内容、又は次の判定条件) |
|---|---|---|---|
| I/O ポート利用制御情報 | 有効 | なし | 判定条件②へ |
| | 無効 | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用禁止」に設定する |

判定条件②

TSFは、制御対象I/Oポートのレジストリより「ポート名」を確認し、表 7-3に基づく判定を行う。

**表 7-3 判定条件②**

| オブジェクトに対応するSFP関連セキュリティ属性 | セキュリティ属性の取る値 | 操作 | 判定結果 (操作内容、又は次の判定条件) |
|---|---|---|---|
| ポート名 | USB ポート | なし | 判定条件③へ |
| | 上記以外 | なし | 判定条件④へ |

判定条件③

TSFは、接続された機器のメーカーID、製品ID、シリアルIDと、サブジェクトに対応するSFP関連セキュリティ属性の「許可USBデバイス入出力制御情報」を比較し、比較結果によって、表 7-4に基づく判定を行う。

**表 7-4 判定条件③**

| 比較結果 | 操作 | 判定結果 (操作内容、又は次の判定条件) |
|---|---|---|
| 一致 | なし | 判定条件④へ |
| 不一致 | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用禁止」に設定する |

判定条件④

TSFは、制御対象I/Oポートのレジストリより「外部メディア情報」を確認し、表 7-5に基づく判定を行う。

**表 7-5 判定条件④**

| オブジェクトに対応するSFP関連セキュリティ属性 | セキュリティ属性の取る値 | 操作 | 規則 |
|---|---|---|---|
| 外部メディア情報 | リムーバブルメディア | なし | 判定条件⑤へ |
| | その他 | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用許可」に設定する |

判定条件⑤

TSFは、サブジェクトに対応するSFP関連セキュリティ属性の「リムーバブルメディア

出力制御情報」を確認し、表 7-6に基づく判定を行う。

**表 7-6 判定条件⑤**

| オブジェクトに対応するSFP関連セキュリティ属性 | セキュリティ属性の取る値 | 操作 | 規則 |
|---|---|---|---|
| リムーバブルメディア出力制御情報 | 許可外部メディアのみ利用可能 | なし | 判定条件⑥へ |
| | すべてのリムーバブルメディアを利用禁止 | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用許可」に設定する |
| | すべてのリムーバブルメディアを許可 | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用許可」に設定する |

判定条件⑥

TSFは、接続されたリムーバブルメディアの「許可外部メディア入出力制御情報」と、管理者プロセス、及び一般利用者プロセスに関連するセキュリティ属性の「許可外部メディア入出力制御情報」を比較し、比較結果によって、表 7-7に基づく判定を行う。

**表 7-7 判定条件⑥**

| 比較結果 | 操作 | 判定結果<br>(操作内容、又は次の判定条件) |
|---|---|---|
| 一致 | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用許可」に設定する |
| 不一致 | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用禁止」に設定する |
| 接続されたリムーバブルメディアに「許可外部メディア入出力制御情報」がない | 設定 | 当該制御対象 I/O ポートのレジストリに対して「利用許可」に設定する。 |

**表 7-8 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<br>一般利用者プロセス | 制御対象 I/O ポートのレジストリ | 設定 |

**表 7-9 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 |
|---|---|
| 管理者プロセス<br>一般利用者プロセス | I/O ポート利用制御情報<br>許可 USB デバイス入出力制御情報<br>許可外部メディア入出力制御情報<br>リムーバブルメディア出力制御情報 |

**表 7-10 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 |
|---|---|
| OS(制御対象 I/O ポートのレジストリ) | 外部メディア情報<br>ポート名 |

[FDP_ACC.1b]、[FDP_ACF.1b]

TOEは、利用者が管理者端末、又はクライアントにログオンした時に適用されるポリシー情報に基づき、「表 7-11 アクセスを管理する規則」に示すプリンタ制御方針に従い、管理者がポリシー情報に設定した「プリンタ利用制御情報」に基づき、OS(プリンタのレジストリ)にプリンタ利用情報(利用許可、利用禁止のいずれかの情報)を設定、又はOS(プリンタのレジストリ)からプリンタ情報を削除する。OSはTOEによって設定されたレジストリの情報に従って動作するため、レジストリを設定することによって、プリンタの利用が制御される。また、レジストリからプリンタ情報を削除することによって、OSはプリンタを認識できなくなるため、プリンタの追加が制御される。

また、プリンタ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表 7-12に、サブジェクトと対応するセキュリティ属性を
表 7-13に、オブジェクトと対応するセキュリティ属性を表 7-14にそれぞれ示す。

**表 7-11 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<br>一般利用者プロセス | プリンタのレジストリ | 設定、削除 | ・ 管理者プロセス、及び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」に指定されたプリンタのレジストリ対して利用許可に設定する。また、この設定の時、許可されたプリンタ以外のプリンタが追加された場合は、そのプリンタのレジストリを削除する。<br>・ 管理者プロセス、及び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」のときすべてのプリンタのレジストリに対して利用許可に設定する。<br>・ 管理者プロセス、及び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」のときすべてのプリンタのレジストリに対して利用禁止に設定する。また、この設定の時、追加されたプリンタのレジストリを削除する。 |

**表 7-12 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<br>一般利用者プロセス | プリンタのレジストリ | 設定、削除 |

**表 7-13 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<br>一般利用者プロセス | プリンタ利用制御情報<br>許可されたプリンタ情報 |

**表 7-14 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 |
|---|---|
| OS(プリンタのレジストリ) | プリンタ登録情報 |

[FDP_ACC.1d]、[FDP_ACF.1d]

TOEは、利用者が管理者端末、又はクライアントにログオンした時に適用されるポリシー情報、管理者端末、又はクライアントに接続されたリムーバブルメディアの許可外部メディア入出力制御情報の有無に基づき、利用者がリムーバブルメディアへファイルの出力を行った場合に、「表 7-15 アクセスを管理する規則」に示すリムーバブルメディア出力制御方針に従い、管理者がポリシー情報に設定した「リムーバブルメディア出力制御情報」と、利用者が接続したリムーバブルメディアに許可外部メディア入出力制御情報が設定されているか否かに基き、接続したリムーバブルメディアへの出力を制御する。リムーバブルメディアへの出力を拒否することにより、リムーバブルメディアへファイルの書き込みをできないようにする。また、リムーバブルメディアからの入力については制御を行わないため、リムーバブルメディアからファイルの読み込みはできるようにする。

また、リムーバブルメディア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表 7-16に、サブジェクトと対応するセキュリティ属性を表 7-17に、オブジェクトと対応するセキュリティ属性を表 7-18にそれぞれ示す。

**表 7-15 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<br>一般利用者プロセス | リムーバブルメディア | 出力制御 | ・ 管理者プロセス、及び一般利用者プロセスは、リムーバブル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」で、接続されたリムーバブルメディアに「許可外部メディア入出力 |

| サブジェクト | オブジェクト | 操作 | 規則 |
|---|---|---|---|
| | | | 制御情報」が設定されていない場合は、そのリムーバブルメディアへの出力を拒否する。<br>・ 管理者プロセス、及び一般利用者プロセスは、リムーバブルメディア出力制御情報が「すべてのリムーバブルメディアを利用禁止」の場合は、リムーバブルメディアへの出力を拒否する。 |

**表 7-16 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<br>一般利用者プロセス | リムーバブルメディア | 出力制御 |

**表 7-17 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<br>一般利用者プロセス | リムーバブルメディア出力制御情報 |

**表 7-18 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 |
|---|---|
| リムーバブルメディア | 許可外部メディア入出力制御情報 |

## 7.3. 暗号機能

TOE のセキュリティ機能である「暗号機能」は、「管理者の指定したドライブ内のファイル」、「利用者が指定したファイル、又は利用者が指定した自動暗号化フォルダ内のファイル」、及び「許可外部メディアに保存されるファイル」の暗号化/復号を行う。また、暗号機能は、それぞれの暗号鍵を生成し、ファイル暗号のみ暗号化/復号に使用する暗号鍵を管理する機能を提供する。以下に、暗号機能の要約仕様を示す。

[FCS_CKM.1]

TOEは、管理者が許可外部メディアを登録する際に「許可外部メディア用共通鍵」を、管理者が必要とした時に「ファイル暗号用共通鍵」を、利用者が管理者端末、又はクライアントにTOEをインストールする際に「ドライブ暗号用共通鍵」を、スタンドアロンで使用しているクライアントから操作ログをエクスポートする際、及びエクスポートした操作ログを管理者端末、又は組織内LANに接続されているクライアントにインポートする際に

「ログ抽出暗号用共通鍵」をそれぞれ生成する。暗号鍵は、表 7-19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って生成される。

**表 7-19 暗号鍵生成のための標準、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 | ANSI X9.17 | 乱数生成アルゴリズム | 128bit |
| ファイル暗号用共通鍵 | ANSI X9.17 | 擬似乱数生成アルゴリズム | 168bit |
| | ANSI X9.17 | 擬似乱数生成アルゴリズム | 128/192/256bit から選択 |
| ドライブ暗号用共通鍵 | ANSI X9.17 | 乱数生成アルゴリズム | 128bit |
| ログ抽出暗号用共通鍵 | ANSI X9.17 | 擬似乱数生成アルゴリズム | 256bit |

[FDP_ACC.1c]、[FDP_ACF.1c]

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、及び一般利用者という役割、及び役割に応じた操作を代行するプロセス(管理者プロセス、一般利用者プロセス)を関連付ける。なお、ファイル暗号タイプについては、クライアントセットアップ作成時に、管理者が設定を行う。

管理者プロセス、又は一般利用者プロセスは、「表 7-20アクセスを管理する規則」に示す暗号鍵ファイル入出力制御方針に従って、「ファイル暗号タイプ」として「管理者」、又は「リーダ」の権限を保有している場合に、ファイル暗号用共通鍵に暗号鍵入力制御情報を付与し、暗号鍵ファイルとして書き出すことができる。一般利用者プロセスは、「表 7-20アクセスを管理する規則」に示す暗号鍵ファイル入出力制御方針に従って、暗号鍵ファイルの読み込み時に暗号鍵入力制御情報を入力することで、暗号鍵ファイルからファイル暗号用共通鍵を読み込むことができる。これらの規則をまとめ、表 7-20に示す。

**表 7-20 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<br>一般利用者プロセス | 暗号鍵ファイル | 書き出し | 管理者プロセス、又は一般利用者プロセスが「ファイル暗号タイプ」として「管理者」又は「リーダ」の権限を保有している場合、暗号鍵入力制御情報を入力した時にファイル暗号用共通鍵を暗号鍵ファイルに書き出す |
| 管理者プロセス | 暗号鍵ファイル | 読み込み | 管理者プロセス、又は一般利用 |

| 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 | | | 者プロセスは、暗号鍵入力制御情報を入力した時、暗号鍵ファイルからファイル暗号用共通鍵を読み込む |

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表 7-21に、サブジェクトと対応するセキュリティ属性を表 7-22に、オブジェクトと対応するセキュリティ属性を表 7-23にそれぞれ示す。

**表 7-21 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<br>一般利用者プロセス | 暗号鍵ファイル | 書き出し、読み込み |

**表 7-22 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<br>一般利用者プロセス | ファイル暗号タイプ |

**表 7-23 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 |
|---|---|
| 暗号鍵ファイル | 暗号鍵入力制御情報 |

[FDP_ETC.2a] 、 [FDP_ITC.2a] 、 [FIA_SOS.1] 、 [FIA_UAU.2c] 、 [FIA_UAU.7] 、 [FMT_MSA.1c]、[FMT_SMF.1]

TOEは、「表 7-20アクセスを管理する規則」に示す暗号鍵ファイル入出力制御方針に従い、管理者によってファイル暗号タイプが「管理者」「リーダ」に設定された利用者のみに暗号鍵入力制御情報を作成するインタフェースを提供する。また、TOEは、暗号鍵ファイルをエクスポートする場合は、必ず暗号鍵入力制御情報の付与を要求し、その設定をファイル暗号タイプが「管理者」「リーダ」に設定された利用者にのみ許可する。

TOEは、「表 7-20アクセスを管理する規則」に示す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、この書き出しはファイル暗号タイプが「管理者」「リーダ」に設定された利用者のみが実行できる。

TOEは、「表 7-20アクセスを管理する規則」に示す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の読み込み時に暗号鍵入力制御情報の照合を行い、暗号鍵ファイル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用共通鍵の読み込みを許可する。なお、TOEは利用者が文字列の入力を行っている間は、入力データを直接表示せず、入力された文字の数だけダミーとして「＊」を表示する。

なお、TOEは、表 7-24に示す品質尺度を満たす文字列のみを暗号鍵入力制御情報として受け入れる。

**表 7-24 定義された品質尺度のリスト**

| 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。<br>- 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<br>- 数字は、[0-9]の合計 10 文字<br>- 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{\|}~ の 32 文字、及び半角の空白<br>・桁数は、8 文字以上 32 文字以下。 |

[FCS_COP.1]

TOE は、許可外部メディアへファイルを書き出す際に許可外部メディア用共通鍵を用いて当該ファイルを暗号化し、許可外部メディアからファイルを読み出す際に許可外部メディア用共通鍵を用いて当該ファイルを復号する。

TOE は、ファイル暗号用共通鍵を用いて、利用者が指定した任意のファイルを利用者の要求に応じて暗号化/復号する。また、ファイル暗号用共通鍵を用いて、利用者が設定した自動暗号化フォルダ内にファイルを書き込むときに暗号化し、自動暗号化フォルダから読み出すときに復号する。

TOE は、管理者端末、又はクライアントへインストールされると、ドライブ暗号用共通鍵を用いて、管理者が指定した暗号化ドライブ内のファイルを暗号化する。また、ドライブ構成が変更となり、管理者が指定したドライブが暗号化されていないことを検出した場合は、利用者がログオンした時に暗号化されていないドライブを暗号化する。その他、暗号化ドライブと非暗号化ドライブ間でフォルダ/ファイルをコピー又は移動する場合、フォルダ/ファイルの読み込み/書き込み時に自動的に暗号化/復号を行い、管理者端末、又はクライアントから TOE をアンインストールする際には、暗号化ドライブ内のファイルを復号する。

TOE は、スタンドアロンで使用しているクライアントから操作ログがリムーバブルメディアへエクスポートされると、ログ抽出暗号用共通鍵を用いて、エクスポートした操作ログを暗号化する。また、エクスポートしたログが管理者端末、又は組織内 LAN に接続されているクライアントにインポートされると、ログ抽出暗号用共通鍵を用いて、操作ログを復号する。

表 7-25にそれぞれの暗号操作と、暗号操作に用いる暗号鍵を示す。

**表 7-25 暗号操作のための標準、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 197 | AES | 128bit | 許可外部メディアへファイルを書き出す際の暗号化、読み込む際の復号 |
| ファイル暗号用共通鍵 | SP800-67 | 3DES | 168bit | 一般利用者の指定したファイルの暗号化、及び復号 |
| | FIPS 197 | AES | 128/192/256bit | |
| ドライブ暗号用共通鍵 | FIPS 197 | AES | 128bit | 管理者の指定したドライブの暗号化、及び復号 |
| ログ抽出暗号用共通鍵 | FIPS 197 | AES | 256bit | クライアントから操作ログをエクスポートする際の暗号化、エクスポートした操作ログをインポートする際の復号 |

## 7.4. 監査機能

TOE のセキュリティ機能である「監査機能」は、管理者端末、及びクライアントにおける監査対象事象を操作ログとして取得し、ログサーバに転送する。また、監査機能は、取得した操作ログを暴露、改ざんから保護し、管理者のみに操作ログの閲覧、検索、削除を実行する機能を提供する。以下に、監査機能の要約仕様を示す。

[FAU_GEN.1]、[FAU_GEN.2]、[FPT_STM.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操作ログの生成、及び生成した情報の管理を行う。そのため、あらかじめ定められた監査の対象となる事象を検出した際、当該事象とその原因となった InfoCage ユーザ ID、及び OS から取得した正確な日付、時刻を関連付けた上で操作ログとして生成する。生成した操作ログは、管理者端末、又はクライアントの一時ログフォルダに保存する。以下に、監査対象事象、及び操作ログの構成を示す。

＜監査対象事象＞

- 禁止されたプリンタの追加、プリンタの利用禁止
- ロックアウトの閾値を越えた InfoCage 認証失敗、及びそれに続いてとられるアクション（ロックアウト）
- InfoCage 認証の成功、失敗
- OS のシャットダウン

＜操作ログの構成＞

- 操作ログ出力の日付、時刻（事象の日付・時刻）
- イベントタイプ（事象の種別）
- InfoCage ユーザ ID（サブジェクト識別情報）
- メッセージ（事象の結果）
- イベント ID（その他の監査関連情報）
- 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）

なお、監査対象事象が発生するのは、利用者の TOE へのログオン完了から OS のシャットダウンの実行までの間であるため、それぞれを監査機能の起動、終了とする。

また、監査機能は **T.01**(不正なログオン)、及び **T.02**(許可されていないプリンタ)の脅威に対抗する機能であるため、上記監査対象事象に示した操作ログを取得すれば十分である。

[FPT_ITT.1]

TOE は、管理者端末、又はクライアントが組織内 LAN に接続されている場合、管理者がポリシー情報に設定した間隔で、管理者端末、又はクライアントの一時ログフォルダに保存された操作ログ、及びログファイルから読み込んだ操作ログを SSL により暗号化してログサーバへ転送する。

[FAU_SAR.1]、[FAU_SAR.2]、[FAU_SAR.3] 、[FIA_SOS.1]、[FIA_UAU.2b]、[FIA_UAU.7]、[FMT_MTD.1]、[FMT_SMF.1]

TOE は、ログサーバ上の DB に蓄積された操作ログの閲覧、検索を行うインタフェースとして「LogViewer」を提供し、管理者のみにその使用を許可する。(「LogViewer」はログサーバにインストールされる TOE のソフトウェアコンポーネントである「InfoCage PC セキュリティ Ver1.22 サーバソフトウェア」により提供される。)

管理者は、管理者端末からブラウザを使ってログサーバにアクセスし、「LogViewer」を起動することにより、操作ログの閲覧、検索を行う。

TOEは、管理者にLogViewerの使用を許可する前にLogViewer起動制御情報の入力を要求する。TOEは、入力されたLogViewer起動制御情報と、TOE内部に保持しているLogViewer起動制御情報を比較し、一致した場合のみLogViewerの使用を許可する。なお、TOEは、表 7-26に示す品質尺度を満たす文字列のみをLogViewer起動制御情報として受け入れる。なお、LogViewer起動制御情報の改変は、管理者のみが実行できる。なお、管理者がLogViewer起動制御情報の入力を行っている間は、入力データを直接表示せず、入力された文字の数だけダミーとして「●」を表示する。

**表 7-26 定義された品質尺度のリスト**

| 秘密情報 | 品質尺度 |
|---|---|
| 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。<br>- 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<br>- 数字は、[0-9]の合計 10 文字<br>- 記号は、!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ の 32 文字、及び半角の空白<br>・桁数は、8 文字以上 127 文字以下。 |

TOE は LogViewer において、以下に示す＜監査情報＞を、監査対象事象ごとに参照できる機能を提供する。また、管理者が以下に示す＜検索条件＞の一つ、又は複数を組み合わせた条件を指定し、参照したい操作ログのみを抽出して表示する機能を提供する。

＜監査情報＞

- 日付、時刻
- イベントタイプ
- InfoCage ユーザ ID
- メッセージ
- イベント ID
- PC 名
- IP アドレス
- MAC アドレス

＜検索条件＞

- 期間、時間帯
- InfoCage ユーザ ID
- PC 名
- IP アドレス
- MAC アドレス
- イベントタイプ
- イベント ID

[FDP_ACC.1e]、[FDP_ACF.1e]、[FDP_ETC.2b]、[FDP _ITC.2b]

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、及び一般利用者という役割、及び役割に応じた操作を代行するプロセス(管理者プロセス、一般利用者プロセス)

を関連付ける。なお、ログ抽出情報については「InfoCage PC セキュリティ Ver1.22 管理者端末ソフトウェア(InfoCage PC セキュリティ Ver.1.22 クライアントソフトウェアを除く)」を管理者端末にインストールする際に管理者が設定を行い、ログ抽出情報はクライアントセットアップをインストールする際にクライアントセットアップをインストールした管理者端末、及びクライアントに登録される。

一般利用者プロセスは、「表 7-27 アクセスを管理する規則」に示すログファイル入出力制御方針に従って、操作ログにログ抽出情報を付与し、ログファイルとして書き出すことができる。管理者プロセス、又は一般利用者プロセスは、「表 7-27 アクセスを管理する規則」に示すログファイル入出力制御方針に従って、ログファイルの読み込み時に、ログファイルを読み込む管理者端末、又はクライアントに登録されているログ抽出情報とログファイルに登録されているログ抽出情報を比較し、一致していた場合はログファイルから操作ログを読み込むことができる。これらの規則をまとめ、「表 7-27」に示す。

**表 7-27 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 | ログファイル | 書き出し | 一般利用者プロセスが、ログファイル抽出制御情報が「ログファイルのエクスポートを許可する」のとき、ログ抽出情報と共に操作ログをログファイルに書き出す |
| 管理者プロセス<br>一般利用者プロセス | ログファイル | 読み込み | ログファイルを読み込む PC に登録されているログ抽出情報が、ログファイル内に登録されているログ抽出情報と一致したとき、ログファイルから操作ログを読み込む |

ログ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表 7-28に、サブジェクトと対応するセキュリティ属性を表 7-29に、オブジェクトと対応するセキュリティ属性を表 7-30にそれぞれ示す。

**表 7-28 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 | ログファイル | 書き出し |
| 管理者プロセス<br>一般利用者プロセス | ログファイル | 読み込み |

**表 7-29 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<br>一般利用者プロセス | ログファイル抽出制御情報 |

**表 7-30 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 |
|---|---|
| ログファイル | ログ抽出情報 |

[FAU_STG.1]、[FAU_STG.3]、[FAU_STG.4]

TOE は、ログサーバへ転送される前の、管理者端末、又はクライアントの一時ログフォルダに保存された操作ログを不正な改変から保護するため、操作ログの登録、及びログサーバへの転送のための読み出しプロセス以外に、一時ログフォルダへのアクセスを許可しない。

TOE は、ログサーバへ転送される前の、管理者端末、又はクライアントの一時ログフォルダに保存された操作ログの容量が、管理者の設定した「ログ警告サイズ」を越えた場合、操作ログ消失の恐れが発生したことを示すメッセージを、当該管理者端末、又は当該クライアントの画面に表示する。

TOE は、管理者端末、又はクライアントにおいて、あらかじめ確保された操作ログの保存領域が満杯になった場合、最も古くに格納された操作ログへの上書きを行う。

## 7.5. ポリシー設定機能

TOE のセキュリティ機能である「ポリシー設定機能」は、「管理者端末においてポリシー情報を作成、変更する機能」、及び「管理者端末、及びクライアントにおいてポリシー情報を適用、参照する機能」を提供する。以下に、ポリシー設定機能の要約仕様を示す。

[FMT_MSA.1a]、[FMT_MSA.3a]、[FMT_SMF.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、及び一般利用者という役割を関連付ける。

TOEは、I/Oポート制御方針に従い、表 7-31に示す通り許可された役割のみに、セキュリティ属性に対する操作を実行するインタフェースを提供する。また、TOEは、表 7-31に示したセキュリティ属性に対して、設定しなければ利用や出力を制御しない許可的なデフォルト値を与え、管理者のみにその設定を許可する。

**表 7-31 セキュリティ属性の管理**

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| I/Oポート利用制御情報 | 作成、問い合わせ、改変 | 管理者 |

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| 一般利用者本人の「I/Oポート利用制御情報」 | 問い合わせ | 一般利用者本人 |
| リムーバブルメディア出力制御情報 | 作成、問い合わせ、改変 | 管理者 |
| 一般利用者本人の「リムーバブルメディア出力制御情報」 | 問い合わせ | 一般利用者本人 |
| 許可外部メディア入出力制御情報 | 作成、問い合わせ、改変 | 管理者 |
| 許可USBデバイス入出力制御情報 | 作成、問い合わせ、改変 | 管理者 |

[FMT_MSA.1b]、[FMT_MSA.3b]、[FMT_SMF.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、及び一般利用者という役割を関連付ける。

TOEは、プリンタ制御方針に従い、表 7-32に示す通り許可された役割のみに、セキュリティ属性に対する操作を実行するインタフェースを提供する。また、TOEは、表 7-32に示したセキュリティ属性に対して、設定しなければプリンタの利用を制御しない許可的なデフォルト値を与え、管理者のみにその設定を許可する。

**表 7-32 セキュリティ属性の管理**

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| プリンタ利用制御情報 | 作成、問い合わせ、改変 | 管理者 |
| 許可されたプリンタ情報 | 作成、問い合わせ、改変 | 管理者 |
| 一般利用者本人の「プリンタ利用制御情報」 | 問い合わせ | 一般利用者本人 |
| 一般利用者本人の「許可されたプリンタ情報」 | 問い合わせ | 一般利用者本人 |

[FMT_MSA.1c]、[FMT_SMF.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、及び一般利用者という役割を関連付ける。

TOEは、暗号鍵ファイル入出力制御方針に従い、表 7-33に示す通り許可された役割のみに、セキュリティ属性に対する操作を実行するインタフェースを提供する。

**表 7-33 セキュリティ属性の管理**

| 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、管理者に指定された一般利用者 |
| ファイル暗号タイプ | 作成、問い合わせ、改変 | 管理者 |

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| 一般利用者本人の「ファイル暗号タイプ」 | 問い合わせ | 一般利用者本人 |

[FMT_MSA.1d]、[FMT_MSA.3c]、[FMT_SMF.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、及び一般利用者という役割を関連付ける。

TOEは、ログファイル入出力制御方針に従い、表 7-34に示す通り許可された役割のみに、セキュリティ属性に対する操作を実行するインタフェースを提供する。また、TOEは、表 7-34に示したセキュリティ属性に対して、設定しなければログのエクスポートを制御する制限的なデフォルト値を与え、管理者のみにその設定を許可する。

**表 7-34 セキュリティ属性の管理**

| セキュリティ属性 | 操作 | 役割 |
|---|---|---|
| ログファイル抽出制御情報 | 作成、問い合わせ、改変 | 管理者 |

[FMT_MTD.1]、[FMT_SMF.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、及び一般利用者という役割を関連付ける。

TOEは、ポリシー情報に含まれるTSFデータを操作するインタフェースの使用を、表 7-35 に示す役割に対してのみ許可する。

また、ファイル暗号利用許可情報のデフォルト値では「許可」であり、管理者のみが設定値を変更することができるが、本 TOE の運用ではファイル暗号利用許可情報は常に「許可」とする。

**表 7-35 TSF データの管理**

| TSF データ | 操作 | 役割 |
|---|---|---|
| InfoCage ユーザ ID | 作成、問い合わせ、削除 | 管理者 |
| | 問い合わせ | 一般利用者本人 |
| InfoCage パスワード桁数 | 作成、問い合わせ、改変 | 管理者 |
| InfoCage パスワード有効期限 | 作成、問い合わせ、改変 | 管理者 |
| ログ警告サイズ | 作成、問い合わせ、改変 | 管理者 |
| ロックアウトの閾値 | 作成、問い合わせ、改変 | 管理者 |
| 再認証時間 | 作成、問い合わせ、改変 | 管理者 |
| ファイル暗号利用許可情報 | 作成、問い合わせ、改変 | 管理者 |

以上