Systemwalker Centric Manager Enterprise Edition V13.2.0 Windows版 セキュリティターゲット

第1.25版

２００８/８/１

富士通株式会社

FUJITSU

－更新記録－

日付	版	更新箇所	更新内容	作成者
06/12/28	1.0 版	－	新規作成	富士通株式会社
07/02/14	1.1 版	2.2.2,2.2.3, 2.2.4,2.3,2.4,2.9 3,3.1,3.2 4.2 5.1.1 6.1.2,6.1.4,6.1.5 等	・保護資産、TOE ｾｷｭﾘﾃｨ環境の見直しと記事変更 ・TOE の関連者に一般利用者を追加 ・物理的環境に開発ｼｽﾃﾑ追加 ・ｺﾝｿｰﾙ操作制御、LiveHelp 認証及び監査ﾛｸﾞの記事修正など	富士通株式会社
07/02/27	1.2 版	2.2.2 2.2.4, 2.7.5 2.9	・保護資産に関する記述の修正 ・関連する記述に対する説明の追加や修正を実施	富士通株式会社
07/03/19	1.3 版	2,3,4,5,6,8 各章	・FDP_IFC.1 等を追加	富士通株式会社
07/04/23	1.4 版	全章	・記事修正	富士通株式会社
07/05/09	1.5 版	全章	・記事修正	富士通株式会社
07/06/15	1.6 版	全章	・所見報告書（No.1）に対する修正	富士通株式会社
07/07/12	1.7 版	全章	・記事修正	富士通株式会社
07/08/27	1.8 版	全章	・所見報告書（No.2）に対する修正	富士通株式会社
07/09/21	1.9 版	全章	・所見報告書（No.3）に対する修正	富士通株式会社
07/10/11	1.10 版	全章	・記事修正	富士通株式会社
07/10/15	1.11 版	5 章、6 章、8 章	・ACL ﾏﾈｰｼﾞｬｱｸｾｽ制御の記述修正	富士通株式会社
07/10/16	1.12 版	5 章、6 章、8 章	・要約仕様及び関連箇所の記事修正	富士通株式会社
07/10/22	1.13 版	5 章、6 章、8 章	・記事修正	富士通株式会社
07/11/02	1.14 版	5 章、6 章、8 章	・記事修正	富士通株式会社
07/11/22	1.15 版	2 章、5 章	・記事修正	富士通株式会社
07/11/29	1.16 版	5 章、6 章、8 章	・所見報告書（No.4）に対する修正	富士通株式会社
07/12/5	1.17 版	5 章、6 章、8 章	・記事修正	富士通株式会社
07/12/13	1.18 版	全章	・所見報告書（No.5）に対する修正	富士通株式会社
07/12/17	1.19 版	2 章、3 章、8 章	・所見報告書（No.6）に対する修正	富士通株式会社
08/ 1/15	1.20 版	2 章、5 章、6 章、8 章	・所見報告書（ADV）に絡む修正	富士通株式会社
08/ 2/22	1.21 版	全章	・Windows 版固有記事の修正	富士通株式会社
08/ 2/25	1.22 版	2 章、5 章、6 章、8 章	・記事修正	富士通株式会社
08/ 3/ 3	1.23 版	2 章、5 章、6 章、8 章	・記事修正	富士通株式会社
08/ 3/10	1.24 版	1 章、2 章、5 章、8 章	・記事修正	富士通株式会社
08/ 8/ 1	1.25 版	3 章、8 章	・所見報告書（ASE）に対する修正	富士通株式会社

FUJITSU

目次

FUJITSU

FUJITSU

図表目次

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、参考資料、及び表記規則、用語、略語について記述する。

1.1. ST 識別

1.1.1. ST の識別

名称　　：Systemwalker Centric Manager Enterprise Edition V13.2.0
　　Windows 版　セキュリティターゲット
バージョン　：第 1.25 版
作成日　　：2008 年 8 月 1 日
作成者　　：富士通株式会社

1.1.2. TOE の識別

名称　　：Systemwalker Centric Manager Enterprise Edition
バージョン　：V13.2.0（Windows）
なお、本 TOE は、以下のクライアント、サーバのソフトウェアで構成される。

- 運用管理クライアント
  Windows 版 Systemwalker Centric Manager Enterprise Edition V13.2.0 (Build-20070511) 運用管理クライアント
- 業務クライアント、(開発用クライアント)
  Windows 版 Systemwalker Centric Manager V13.2.0 (Build-20070511) クライアント
- 運用管理サーバ、(全体監視サーバ)
  Windows 版 Systemwalker Centric Manager Enterprise Edition V13.2.0 (Build-20070511) 運用管理サーバ
- 部門管理サーバ
  Windows 版 Systemwalker Centric Manager Agent Enterprise Edition V13.2.0 (Build-20070511) 部門管理サーバ
- 業務サーバ、(開発用サーバ)
  Windows 版 Systemwalker Centric Manager Agent Enterprise Edition V13.2.0 (Build-20070511) 業務サーバ

作成者　　：富士通株式会社

1.1.3. 適用する CC のバージョン

- ISO/IEC 15408:2005

- 補足-0512 適用

1.2. ST 概要

本 ST は、富士通株式会社が提供する業務システムの運用管理を支援するソフトウェア製品である「Systemwalker Centric Manager Enterprise Edition」のセキュリティ仕様を規定している。対象となる TOE のセキュリティ機能は以下のとおりである。

- ACL マネージャ機能
- コンソール操作制御機能
- LiveHelp 接続認証機能
- ACL マネージャ機能の監査ログ機能
- 運用管理クライアント操作の監査ログ機能
- 適用結果の自動通知機能
- サーバ上の TOE にログインするためのパスワードの保護機能

1.3. CC 適合

本 ST は、以下を満たしている。

パート 2 適合
パート 3 適合
EAL 1 適合
適合する PP は存在しない。

1.3.1. 参考資料

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August 2005 Version 2.3 CCMB-2005-08-001
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements August 2005 Version 2.3 CCMB-2005-08-002
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements August 2005 Version 2.3 CCMB-2005-08-003
- Common Methodology for Information Technology Security Evaluation Evaluation methodology Version 2.3 August 2005 CCMB-2005-08-004
- 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 2005 年 8 月 バージョン 2.3 CCMB-2005-08-001
  平成 17 年 12 月翻訳第 1.0 版 独立行政法人 情報処理推進機構セキュリティセンター 情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア パート 2：
  セキュリティ機能要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-002

平成 17 年 12 月翻訳第 1.0 版 独立行政法人 情報処理推進機構セキュリティセンター 情報セキュリティ認証室

- 情報技術セキュリティ評価のためのコモンクライテリア パート 3：
  セキュリティ保証要件 2005 年 8 月 バージョン 2.3 CCMB-2005-08-003
  平成 17 年 12 月翻訳第 1.0 版 独立行政法人 情報処理推進機構セキュリティセンター 情報セキュリティ認証室
- 情報技術セキュリティ評価のための共通方法 評価方法 2005 年 8 月 バージョン 2.3 CCMB-2005-08-004
  平成 17 年 12 月翻訳第 1.0 版 独立行政法人 情報処理推進機構セキュリティセンター 情報セキュリティ認証室
- 補足-0512　平成 17 年 12 月　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. 表記規則、用語、略語

1.4.1. 表記規則

必要の都度、各章の冒頭で明示する。

1.4.2. 用語

本 ST で定義する用語を以下に説明する。

用語	説明
アップロード	：開発システムの本 TOE に登録されている配付資源を開発システムから運用管理サーバに移すこと。
イベント	：運用管理を行う者に通知すべき業務システムで発生した重要な事象。イベントログや SNMP トラップにより通知される。
インベントリ情報	：運用管理を行う上で必要となる情報であり、ハードウェアに関する情報、導入されているソフトウェアに関する情報（名称など）および資産管理番号等のユーザが運用管理上設定するユーザ情報等からなる。
運用管理	：業務システムの円滑な稼動のための管理行為（業務）であり、ソフトウェアやデータの配付と適用、稼働状況の監視、トラブルの復旧、そして運用結果の査定からなる。
運用管理サーバ	：業務システム全体の監視、操作、資源配付を行なう専用サーバであり、運用管理クライアントから操作を行う。

用語	説明
運用管理クライアント	：運用管理サーバを操作するためのコンソール機能を持つクライアントである。
運用管理部門	：業務システムの運用管理を司る部門であり、運用管理方針の策定やシステム管理者の任命に責任をもつ。
運用管理方針	：業務システムの運用管理を行うに際して、その対象範囲や実施規則等を定めたもの
開発システム	：配付資源を開発するためのシステムであり、サーバ資源を開発するための開発用サーバと、クライアント資源を開発するための開発用クライアントから成る。
監視対象イベント	：サーバやネットワーク機器で発生するイベントの中で、本 TOE が運用管理のために監視対象とするイベント。
業務クライアント	：業務サーバと連携して業務処理を行うクライアント。
業務サーバ	：本 TOE が運用管理の対象とする業務処理を行うサーバ。
業務システム	：業務サーバ、業務クライアントおよびそれらをつなぐネットワーク機器から成る業務処理を行うシステム。
業務システム資産	：業務システムを構成するサーバ、クライアントおよびネットワーク機器であり、本 TOE が運用管理の対象とする資産。
ダウンロード	：配付資源を保持する業務サーバ上の本 TOE に対して、業務クライアントから資源のクライアントへの配付を要求すること。
適用	：目的の業務サーバまたは業務クライアントに配付された資源を指定されたディレクトリ配下に利用可能な形で格納すること。適用を行うに際しては、配付の延長で行う形態と、別途、人が介入して行う形態の二つがある。
登録	：運用管理サーバへの配付資源のアップロードに先立ち、開発完了した資源を開発システム上の本 TOE に配付資源の形で格納すること。
配付	：運用管理サーバ上の本 TOE が管理する配付資源を目的の業務サーバまたは業務クライアントに配ること。配付されたのちは、適用に備えて配付先の業務サーバまたは業務クライアントの本 TOE で保持される。
配付資源	：本 TOE を利用して業務サーバや業務クライアントに配付されるソフトウェアやデータであり、資源の種別や宛先等の必要な情報が付加された本 TOE が配付できる形式になっているもの。

用語	説明
リモートコマンド	：運用管理クライアントから運用管理サーバ経由で監視対象の業務サーバに対して発行するコマンド。
リモート操作	：運用管理クライアントから LiveHelp クライアントにアクセスして、環境設定やトラブル調査復旧を行う操作を示す。
LiveHelp クライアント	リモート操作の支援を受ける側の業務クライアント、運用管理クライアント、運用管理サーバ、業務サーバおよび部門管理サーバの総称。
OS コンソール	：運用管理サーバ、部門管理サーバまたは業務サーバの OS にリモートでログインし、OS 機能を使って操作を行うためのパソコン。
SNMP トラップ	：ネットワーク機器から非同期に通知される事象データ。

また、本 ST で使用する CC（Common Criteria）および IT 略語を以下に示す。

略語	説明
EAL	：Evaluation Assurance Level。評価保証レベル（CC 略語）
GUI	：Graphical User Interface。情報の表示にグラフィックを活用したユーザインタフェース。
MIB	：Management Information Base。SNMP で管理されるルータ等の機器が状態や構成等を外部に知らせるため公開する情報。
OS	：Operating System。オペレーティングシステム
PP	：Protection Profile。プロテクションプロファイル（CC 略語）
SFP	：Security Function Policy。セキュリティ機能方針（CC 略語）
SNMP	：Simple Network Management Protocol。TCP/IP において、ハブやルータ等の機器をネットワーク経由で監視・制御するためのプロトコル。
SOF	：Strength Of Function。機能強度（CC 略語）
ST	：Security Target。セキュリティターゲット（CC 略語）
TOE	：Target Of Evaluation。評価対象（CC 略語）
TSF	：TOE Security Functions。TOE セキュリティ機能（CC 略語）

2. TOE 記述

本章では、TOE 種別、TOE 概要、TOE の構成、TOE の機能および保護対象となる資産について記述する。

2.1. TOE 種別

本 TOE は、業務システムの安定稼動に必要な運用管理を支援するソフトウェア製品である。業務システムを構成するサーバ、クライアント、およびハブやルータ等のネットワーク機器（以降、これらを総称して業務システム資産と呼ぶ）に対して、本 TOE が定義するデプロイ（配付）、モニタリング（監視）、リカバリ（復旧）、そして、アセスメント（査定）の 4 つの運用管理フェーズにより、その運用管理をトータルに支援する。

- デプロイ（配付）は業務サーバや業務クライアントへのソフトウェアやデータの配備を行うフェーズであり、本 TOE はソフトウェアやデータの配付と適用を行う資源配付機能を提供する。
- モニタリング（監視）は業務システムの異常状態の監視を行うフェーズであり、本 TOE は稼動状況や性能等の監視のための事象監視機能を提供する。
- リカバリ（復旧）は業務システムがトラブルに陥った場合の原因調査や復旧を行うフェーズであり、本 TOE はサーバやクライアントに対するトラブル調査や復旧のための操作機能を提供する。
- そして、アセスメント（査定）は業務システムを定期的に評価・分析し、必要な予防処置を策定するフェーズであり、本 TOE は業務システムの稼動分析機能を提供する。

2.2. TOE 概要

2.2.1. TOE の利用目的

本 TOE は、業務システムの運用管理を、運用管理部門が定めた運用管理方針に従って行えるようにすることを目的とする。本 TOE を利用することで、以下のようなトラブルに対し、トラブルからの速やかな回復やトラブルの予防といったことを容易にかつ効率良く行うことができる。

- 業務の異常が長時間放置され処理が滞る
- 不当な誤った運用操作により業務が停止する
- 急なトラフィックの増加により処理遅延が発生する
- ソフトウェアの修正適用漏れにより誤動作を引き起こすなど

また、本 TOE は運用管理のための手段を提供する製品であり、業務システムの動作環境に合わせ、適切に利用することが必要である。

2.2.2. TOE の利用環境

本 TOE は図 2.1 に示したとおり分散システム環境で動作する。ここでは、本 TOE の利用環境として、本 TOE が関係する主要なサーバ、クライアント、および本 TOE が運用管理のために使用する資産について説明する。

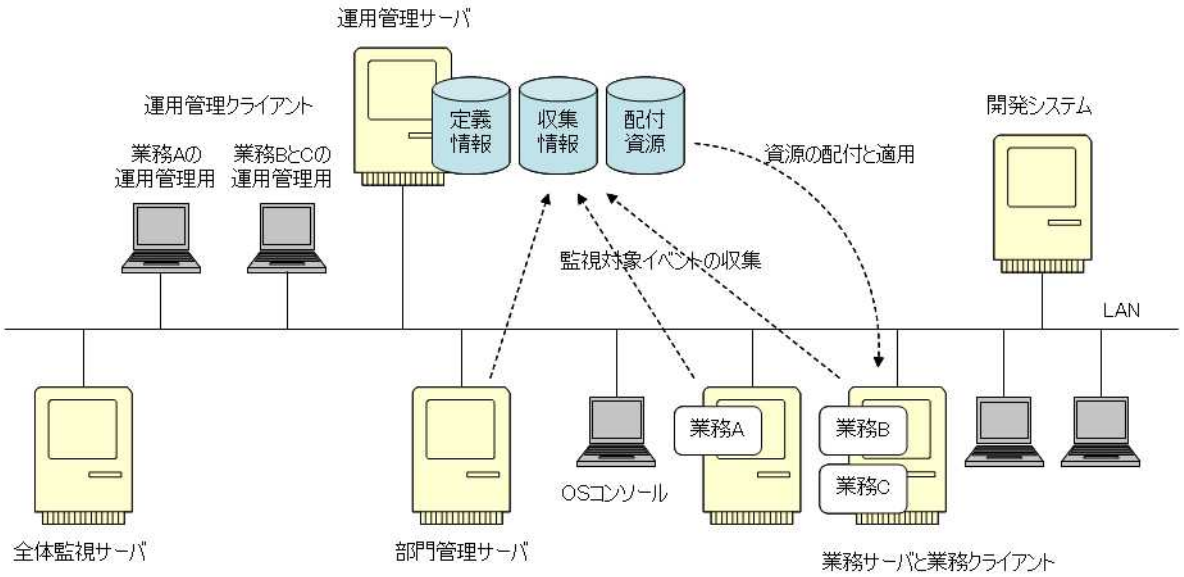

図 2.1　本 TOE に関係するサーバとクライアント

1) 運用管理サーバと運用管理クライアント

図 2.1 において、運用管理サーバおよび運用管理クライアントは、運用管理のための専用のサーバおよびクライアントであり、各々1 台は最低限必要である。

運用管理サーバは、運用管理に必要な情報を収集し管理することで、運用管理クライアントから、分散環境下のすべての業務システム資産を一元的に運用管理できる環境を実現する。収集する情報には以下のようなものがある。

- 業務サーバ、クライアントのハードウェア構成
- 導入されているソフトウェアの構成
- 導入されているソフトウェアの稼動状況（起動中、未起動など）
- サーバ、ネットワーク機器の性能情報、閾値を超えたことの通知など

運用管理クライアントは、運用管理サーバを使って運用操作を行うためのクライアントであり、以下のような操作が行える。

- 運用管理のための環境設定（動作環境、条件など）
- 運用管理サーバ上の情報を使った業務システムの監視やトラブルからの復旧操作
- ソフトウェアやデータの配付・適用の操作など

運用形態の異なる業務が共存するような場合は、図 2.1 に示したように、業務毎に運用管理クライアントを分けることができる。

2) 開発システム

開発システムは、業務サーバや業務クライアントで使用するソフトウェアや画面定義体等のデータを開発するシステムであり、サーバ資源を開発する開発用サーバ、クライアント資源を開発する開発用クライアントからなる。ここで開発されたものは、運用管理サーバにアップロードされ、該当するサーバ、クライアントに配付され適用される。

3) 業務サーバと業務クライアント

業務処理を行うサーバおよびクライアントである。本 TOE は、これらサーバ、クライアントで発生するイベントの監視や、業務処理に必要とされるソフトウェアやデータの配付・適用を行う。

なお、業務サーバにおける日常の業務操作（OS の立ち上げ、アプリケーションの起動や停止など）は、各業務サーバに割当てられたオペレータが OS コンソールから OS 機能を使って直接行う。

4) 部門管理サーバ

部門管理サーバは、運用管理サーバの負荷を分散させるためのサーバである。1 台の運用管理サーバでは能力的に無理な多数の業務サーバからなる大規模システムに対して、部門管理サーバはいくつかの業務サーバを束ねることで、運用管理サーバの負荷を軽減させる役割を果す。業務サーバが部門管理サーバを兼ねる。

5) 全体監視サーバ

全体監視サーバは、運用管理サーバの利用形態の一つである。例えば、地区毎に運用管理サーバを用意し、地区独立で運用管理しているようなシステムを全社レベルで監視するような場合に、業務サーバから運用管理サーバへ監視対象イベントを通知するのと同様に、全体監視サーバに位置づけた運用管理サーバに、配下の運用管理サーバから監視対象イベントを集めることで全体監視を実現する。

6) 運用管理で使用する資産

本 TOE が使用する資産には、定義情報、収集情報および配付資源がある。

定義情報は、運用管理部門が定めた運用管理方針を本 TOE に反映するためのものであり、本 TOE が定義する 4 つの運用管理フェーズ各々に対応して、以下のような内容から成る。

- 資源配付のための定義情報（資源の配付先や配付方法など、デプロイ（配付）に必要な動作環境を定義した情報）
- 事象監視のための定義情報（監視対象イベント、監視間隔および閾値など、モニタリング（監視）に必要な動作環境を定義した情報）
- 復旧のための定義情報（リモートコマンドやリモート操作のための定義など、リカバリ（復旧）に必要な動作環境を定義した情報）
- ログ収集のための定義情報（アセスメント（査定）の入力になるログファイルのフ

ァイル名や所在場所を定義した情報）

本 TOE は、これら定義情報をもとに、運用管理部門が期待する業務システムに最適化された運用管理環境を実現する。

収集情報は、監視のために業務システム資産から収集したイベント情報やインベントリ情報である。イベント情報には発生の都度収集される監視対象イベントと、一括して収集されるログファイルがある。これらの違いは、収集のタイミングと、ログファイルには監視対象から外れたイベント情報を含むことだけである。本 TOE はこれら情報から監視対象の稼動状況を認識する。本 TOE は業務システム資産が正しく動作することを前提としており、収集情報についても、その内容に関して誤りがないものとする。

配付資源は、配付のため本 TOE に登録されたソフトウェアやデータであり、その内容は信頼できるものとする。本 TOE は、定義情報および配付時の指定に従って配付を行う。また、クライアントへの配付は、利用者の業務都合に依存することから、本 TOE はサーバまでの配付を行い、それ以降はクライアント利用者に委ねている。そのサーバにログインできる利用者は、業務上必要な資源を自由にダウンロードできる。

2.2.3. TOE の関連者

本 TOE の関連者としては以下を想定する。TOE の関連者は、TOE が提供する GUI またはコマンドを使って TOE を操作する。

表 2.1　TOE の関連者

関連者	説明
システム管理者	administrator 権限を有する者であり、主に本 TOE を利用する者に対する利用者登録や権限設定等の操作を行う。加えて、本 TOE に関するすべての操作を行う権限をもつ。
運用管理者	ｼｽﾃﾑ管理者から管理者権限を与えられた者であり、与えられた管理者権限の範囲内で、本 TOE による運用管理に必要な環境の設定や変更を行う。また、運用担当者が行えるすべての操作を行う権限をもつ。
運用担当者	ｼｽﾃﾑ管理者または運用管理者から運用操作を行う権限を与えられた者であり、資源配付の操作および、許可された範囲内の特定業務ｻｰﾊﾞの特定業務に対する監視、復旧、査定のための操作を行う。
一般利用者	本 TOE が管理対象とする業務ｼｽﾃﾑを利用して業務処理を行う者であり、本 TOE を利用してｸﾗｲｱﾝﾄ資源のﾀﾞｳﾝﾛｰﾄﾞと適用を行う。

運用管理者、運用担当者の権限は、与えられたロールによって決定される。本 TOE が定義するロールと権限の関係は、表 2.2 のとおりである。なお、この表に示した監視機能に

は、“2.4.1 TOE の運用管理機能”に示すネットワーク管理、サーバ管理、LiveHelp、ヘルプデスク、レポーティング、およびログ収集管理の各機能が含まれる。以降、監視機能と云う用語は、これら機能をすべて指すものとする。

表 2.2　本 TOE が定義するロールと権限との関係

ロール名	説明	与えられる権限	
		運用管理者	運用担当者
DmAdmin	監視機能の管理系ﾛｰﾙ	✓	
DmOperation	監視機能の操作系ﾛｰﾙ		✓
DmReference	監視機能の参照系ﾛｰﾙ		✓
DistributionAdmin	資源配付の管理系ﾛｰﾙ	✓	
DistributionOperation	資源配付の操作系ﾛｰﾙ		✓
DistributionReference	資源配付の参照系ﾛｰﾙ		✓

運用管理者は最低一つの管理系ロールをもつ者であり、運用担当者は管理系以外のロールをもつ者である。

2.3. TOE の物理的構成

2.3.1. TOE の物理的構成要素

本 TOE は、表 2.3 に示す物理的構成要素からなる。

表 2.3 本 TOE の物理的構成要素の概要

構成要素	概要	本 ST での略称
運用管理ｻｰﾊﾞ向けｿﾌﾄｳｪｱ	業務ｼｽﾃﾑ全体の運用管理を行うためのｻｰﾊﾞ ｿﾌﾄｳｪｱであり、運用管理ｻｰﾊﾞに導入される。また、全体監視ｻｰﾊﾞを利用する場合には、全体監視ｻｰﾊﾞにも導入される。	CMGR/MGR
部門管理ｻｰﾊﾞ向けｿﾌﾄｳｪｱ	部門内の運用管理を行うためのｻｰﾊﾞ ｿﾌﾄｳｪｱであり、部門管理ｻｰﾊﾞに導入される。多数の業務ｻｰﾊﾞから成る大規模な業務ｼｽﾃﾑを対象に、部門内の運用管理を行うことで運用管理ｻｰﾊﾞの負荷分散を図る。 また、業務ｻｰﾊﾞが部門管理ｻｰﾊﾞを兼ねるため、当ｿﾌﾄｳｪｱは業務ｻｰﾊﾞ向けｿﾌﾄｳｪｱを包含する。	CMGR/Agent(S)
業務ｻｰﾊﾞ向けｿﾌﾄｳｪｱ	被管理対象のｻｰﾊﾞに導入されるｻｰﾊﾞ ｿﾌﾄｳｪｱである。業務ｻｰﾊﾞに導入される。また、開発用ｻｰﾊﾞに導入されて、ｻｰﾊﾞ資源の登録に利用される。	CMGR/Agent(J)
運用管理ｸﾗｲｱﾝﾄ向けｿﾌﾄｳｪｱ	運用管理者および運用担当者のためのｺﾝｿｰﾙ機能を提供するｸﾗｲｱﾝﾄｿﾌﾄｳｪｱである。運用管理ｸﾗｲｱﾝﾄに導入される。	CMGR/CL(M)
業務ｸﾗｲｱﾝﾄ向けｿﾌﾄｳｪｱ	被管理対象のｸﾗｲｱﾝﾄに導入されるｸﾗｲｱﾝﾄｿﾌﾄｳｪｱである。業務ｸﾗｲｱﾝﾄおよび開発ｼｽﾃﾑのｸﾗｲｱﾝﾄに導入される。	CMGR/CL(U)

注）以降、本 ST では、CMGR/MGR、CMGR/Agent(S)、CMGR/Agent(J)、CMGR/CL(M)および CMGR/CL(U)は本 TOE を表し、運用管理ｻｰﾊﾞ、運用管理ｸﾗｲｱﾝﾄ、業務ｻｰﾊﾞ等の用語は、本 TOE が動作するｻｰﾊﾞやｸﾗｲｱﾝﾄを表すものとする。

2.3.2. 物理的構成要素の物理的な配置

図 2.2 は、本 TOE の物理的構成要素が動作するサーバの物理的な配置と、TOE の関連者との関係を示したものである。

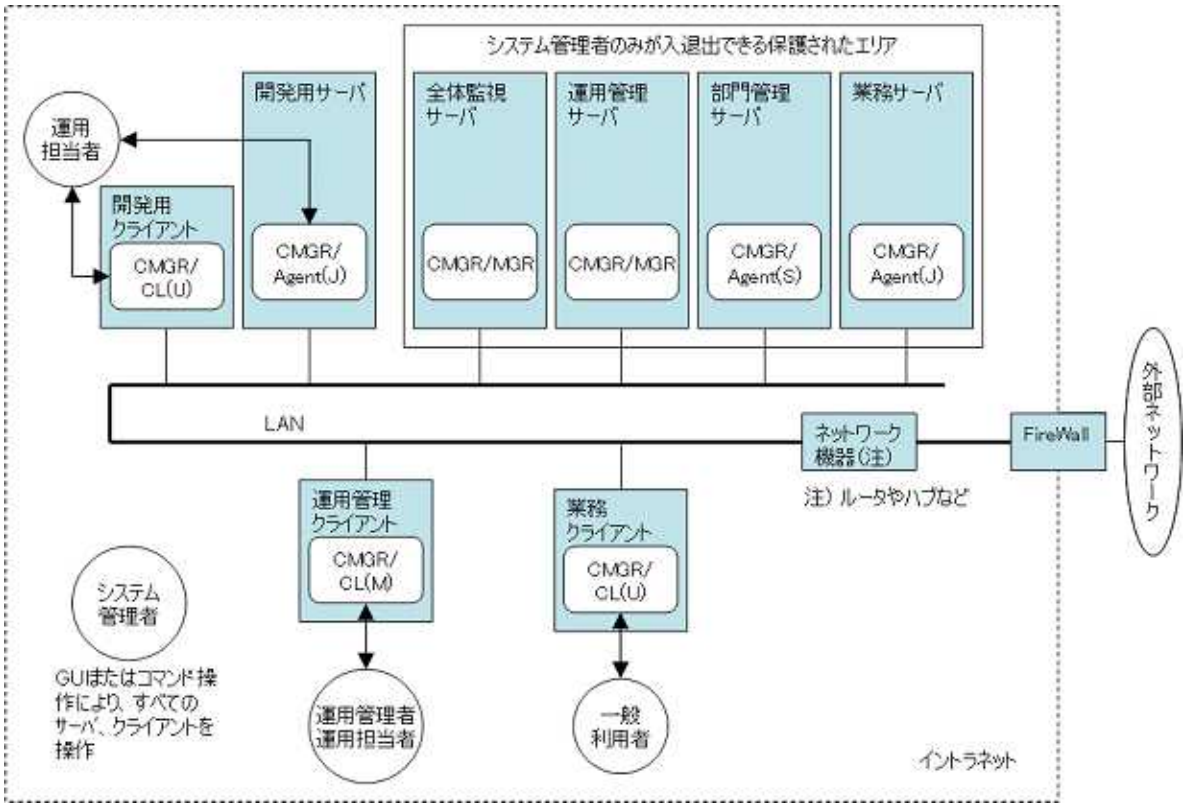

図 2.2　物理的構成要素の配置と TOE の関連者との関係

図 2.2 に示したとおり、関連するサーバ、クライアントはすべてファイアウォールで保護されたイントラネット内に置かれる。さらに、運用管理サーバ、全体監視サーバ、部門管理サーバおよび業務サーバについては、システム管理者のみが入退出できる物理的に保護されたエリアに設置される。

TOE の関連者については、GUI を使って操作する場合（運用管理者、運用担当者、システム管理者、一般利用者が該当)、CMGR/CL(M)、CMGR/CL(U)または CMGR/Agent(J)から必要な操作を行う。コマンドを使って操作する場合（運用管理者、運用担当者、システム管理者が該当)、各サーバ、クライアントの OS に直接ログインして操作を行う。

2.3.3.　動作に必要な資源

本 TOE に必要なハードウェアには以下のものがある。

- LAN カードが必須である。
- 最低一台の Pentium Ⅲ、500MHz 以上の CPU を搭載した PC 端末が運用管理クライアントとして必要である。

本 TOE に必要なディスク容量（選択機能すべて選択時、管理データ量に依存する部分は除く）と、メモリ容量（監視機能のみ使用時）は表 2.4 のとおりである。

表 2.4　本 TOE に必要なディスク容量とメモリ容量

区分	ディスク容量	メモリ容量
CMGR/MGR	4.15GB 以上	350MB 以上
CMGR/Agent(S)	1.3GB 以上	120MB 以上
CMGR/Agent(J)	1.17GB 以上	120MB 以上
CMGR/CL(M)	1.27MB 以上	80MB 以上
CMGR/CL(U)	800MB 以上	80MB 以上

本 TOE の動作に必要なソフトウェアは表 2.5 のとおりである。

表 2.5　本 TOE の動作に必要なソフトウェア

区分	動作 OS	ﾊﾟｯﾁ番号
CMGR/MGR CMGR/Agent(S) CMGR/Agent(J)	Microsoft(R) Windows Server(R) 2003 Enterprise Edition	SP2
CMGR/CL(M)	Windows(R) XP Professional	SP2
CMGR/CL(U)	Windows(R) XP Professional	SP2

SP: Service Pack

2.4. TOE の論理的構成

本TOEは表2.6に示す運用管理機能およびセキュリティ機能から成る。図中の○印は各々の機能が実装されている位置を示している。

表 2.6　本 TOE の論理的構成要素

機能名		CMGR/MGR	CMGR/Agent(S)	CMGR/Agent(J)	CMGR/CL(M)	CMGR/CL(U)
運用管理機能	Systemwalker ｺﾝｿｰﾙ	○			○	
	ﾈｯﾄﾜｰｸ管理	○	○		○	
	資源配付	○	○	○	○	○
	ｻｰﾊﾞ管理	○	○	○	○	
	LiveHelp	○	○	○	○	○
	ﾍﾙﾌﾟﾃﾞｽｸ	○			○	
	ﾚﾎﾟｰﾃｨﾝｸﾞ	○			○	
	ﾛｸﾞ収集管理	○	○	○		
	転送機能	○	○	○	○	○
セキュリティ機能	ACL ﾏﾈｰｼﾞｬ機能	○	○	○	○	
	ｺﾝｿｰﾙ操作制御機能	○			○	
	LiveHelp 接続認証機能	○	○	○	○	○
	ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能	○	○	○		
	運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能	○			○	
	適用結果の自動通知機能	○	○	○		○
	ｻｰﾊﾞ上の TOE にﾛｸﾞｲﾝするためのﾊﾟｽﾜｰﾄﾞの保護機能	○	○	○	○	○

2.4.1. TOE の運用管理機能

運用管理機能は、運用管理業務を直接支援する機能である。

機能名　　説明

Systemwalker ｺﾝｿｰﾙ　：運用管理ｸﾗｲｱﾝﾄから運用管理ｻｰﾊﾞを操作するためのｺﾝｿｰﾙ機能を提供する。当ｺﾝｿｰﾙ機能では、他の運用管理機能やｾｷｭﾘﾃｨ機能への操作ｲﾝﾀﾌｪｰｽを提供する。

ﾈｯﾄﾜｰｸ管理　：ﾈｯﾄﾜｰｸ機器に対する監視機能を提供する。事象監視のための定義情報をもとに、CMGR/MGR および CMGR/Agent(S)において、ﾈｯﾄﾜｰｸ機器からの SNMP ﾄﾗｯﾌﾟの受信や MIB 情報に対する閾値監視を行う。CMGR/CL(M)では、当機能に必要な定義手段を提供する。

機能名	説明
資源配付	：業務ｻｰﾊﾞや業務ｸﾗｲｱﾝﾄで使用する資源を運用管理ｻｰﾊﾞで集中管理し、指定されたｻｰﾊﾞへ資源をｵﾝﾗｲﾝで配付し適用する機能を提供する。ｸﾗｲｱﾝﾄに対しては、ｸﾗｲｱﾝﾄからのﾀﾞｳﾝﾛｰﾄﾞ要求を契機にｸﾗｲｱﾝﾄへの配付を行う。また、ｲﾝﾍﾞﾝﾄﾘ管理とｿﾌﾄｳｪｱ修正管理各機能を提供する。ｲﾝﾍﾞﾝﾄﾘ管理は、ｻｰﾊﾞやｸﾗｲｱﾝﾄの構成情報をｲﾝﾍﾞﾝﾄﾘ情報として収集し、一元管理する機能を提供する。ｿﾌﾄｳｪｱ修正管理は、ｿﾌﾄｳｪｱ修正情報を提供する富士通株式会社のｳｪﾌﾞｻｲﾄと連携し、その適用を管理する機能を提供する。ｳｪﾌﾞｻｲﾄとの接続は、本 TOE とは別のｿﾌﾄｳｪｱである UpdateAdvisor が行い、当機能は UpdateAdvisor を介して情報の入手を行うため、本 TOE がｳｪﾌﾞｻｲﾄと接続することはない。本 ST において、ｿﾌﾄｳｪｱ修正管理機能は評価対象であるが、UpdateAdvisor は評価対象外である。CMGR/MGR では、配付資源の管理と配付を行う。CMGR/Agent(J)では、配付されたｻｰﾊﾞ資源の適用、ｸﾗｲｱﾝﾄへの資源の配付を行う。MGR/Agent(S)では、CMGR/Agent(J)の機能に加え、配下の業務ｻｰﾊﾞに対する配付機能を提供する。CMGR/CL(M)では、当機能に必要な運用操作の手段を提供する。そして、CMGR/CL(U)では、資源のｱｯﾌﾟﾛｰﾄﾞおよび資源のﾀﾞｳﾝﾛｰﾄﾞと適用のための操作手段を提供する。
ｻｰﾊﾞ管理	：ｻｰﾊﾞに対する監視と操作機能を提供する。主な機能は、ｻｰﾊﾞの稼動監視、ｻｰﾊﾞの性能監視、ｱﾌﾟﾘｹｰｼｮﾝの稼動監視、およびﾘﾓｰﾄｺﾏﾝﾄﾞの各機能である。CMGR/Agent（S）および CMGR/Agent(J)では、監視対象ｲﾍﾞﾝﾄの収集や定義されたｱｸｼｮﾝ（運用管理ｸﾗｲｱﾝﾄへの表示や運用担当者への連絡など）の実行等を行う。CMGR/MGR では、収集された監視対象ｲﾍﾞﾝﾄの管理を行う。そして、CMGR/CL(M)では、監視対象ｲﾍﾞﾝﾄの発生を分かり易く表示する監視画面や、当機能を使った運用操作のための手段を提供する。

機能名	説明
LiveHelp	：ﾄﾗﾌﾞﾙの発生したｻｰﾊﾞ、ｸﾗｲｱﾝﾄ上の画面を運用管理ｸﾗｲｱﾝﾄで参照し、その利用者と画面を共有して復旧支援操作を行うための機能（ﾘﾓｰﾄ操作）を提供する。CMGR/CL(U)、CMGR/MGR、CMGR/Agent(J)およびCMGR/Agent(S)では、操作される側の機能を提供し、CMGR/CL(M)では、操作する側とされる側の機能を提供する。 注） ﾘﾓｰﾄ操作は操作される側の画面を使って行うことから、行える操作は操作される側でﾛｸﾞｲﾝしている利用者の権限に依存する。操作される側がCMGR/MGR、CMGR/Agent(J)、CMGR/Agent(S)またはCMGR/CL(M)の場合であっても、CMGR/CL(U)に対してﾘﾓｰﾄ操作を行う場合と比べ何ら差異はない。 よって、本STでのﾘﾓｰﾄ操作に関連する記述においては、操作される側の業務ｸﾗｲｱﾝﾄ、運用管理ｸﾗｲｱﾝﾄ、業務ｻｰﾊﾞ、部門管理ｻｰﾊﾞおよび運用管理ｻｰﾊﾞを“LiveHelpｸﾗｲｱﾝﾄ”と総称する。
ﾍﾙﾌﾟﾃﾞｽｸ	：運用中に発生するﾊｰﾄﾞｳｪｱやｿﾌﾄｳｪｱの障害、操作ﾐｽ等の情報をﾃﾞｰﾀﾍﾞｰｽ化して管理する機能を提供する。CMGR/MGRではﾄﾗﾌﾞﾙ情報の管理機能を提供し、CMGR/CL(M)では情報の登録や参照のための操作手段を提供する。
ﾚﾎﾟｰﾃｨﾝｸﾞ	：ﾛｸﾞ収集管理で収集されたﾛｸﾞﾌｧｲﾙをもとに、稼働状況等をｸﾞﾗﾌや表で表示する機能を提供する。CMGR/MGRがﾛｸﾞﾌｧｲﾙの管理を行い、CMGR/CL(M)においてﾚﾎﾟｰﾃｨﾝｸﾞのための操作手段を提供する。
ﾛｸﾞ収集管理	：ｻｰﾊﾞ毎に採取されるﾛｸﾞﾌｧｲﾙを運用管理ｻｰﾊﾞに転送し、運用管理ｻｰﾊﾞで一元管理するための機能を提供する。CMGR/MGR、CMGR/Agent(S)、およびCMGR/Agent(J)ではﾛｸﾞﾌｧｲﾙの収集機能を提供し、CMGR/MGRでは収集されたﾛｸﾞﾌｧｲﾙの管理機能を提供する。そして、CMGR/CL(M)では当機能に必要な操作手段を提供する。
転送機能	：転送機能を除く他の運用管理機能から呼び出されて、ﾈｯﾄﾜｰｸを介してﾃﾞｰﾀのやり取りを行うための機能を提供する。対象となるﾃﾞｰﾀは定義情報やﾛｸﾞ情報等であり、ﾕｰｻﾞ名やﾊﾟｽﾜｰﾄﾞは含まれない。CMGR/MGR、CMGR/Agent(S)、CMGR/Agent(J)、CMGR/CL(M)、およびCMGR/CL(U)各々において機能を提供する。

2.4.2. TOEのセキュリティ機能

本TOEのセキュリティ機能を以下に示す。

機能名	説明
ACL ﾏﾈｰｼﾞｬ機能	：IT 環境により識別認証された本 TOE の関連者に対して、その関連者のﾕｰｻﾞ名に割当てられた管理系/操作系/参照系の各ﾛｰﾙにより、その者が運用管理者であるか運用担当者であるかの識別を行い、識別結果に応じて運用管理ｸﾗｲｱﾝﾄから行える操作を制限する。また、CMGR/MGR、CMGR/Agent(S)および CMGR/Agent(J)が提供するｺﾏﾝﾄﾞを直接使った操作についても同様に制限を行う。CMGR/MGR、CMGR/Agent(S)および CMGR/Agent(J)においてﾛｰﾙに基づく権限の識別を行い、CMGR/CL(M)が識別結果に応じた操作画面（許可されないﾒﾆｭｰはｸﾞﾚｰｱｳﾄ）を提供することで、ﾛｰﾙに基づく操作の制限を実現する。当機能は常に動作する。
ｺﾝｿｰﾙ操作制御機能	：ﾛｰﾙで決められた操作内容をﾒﾆｭｰ単位でさらに細かく制限する機能を提供する。当機能により、同じﾛｰﾙをもつ運用担当者であっても、操作できる業務ｼｽﾃﾑ資産や操作内容を違えることができるため、大規模な業務ｼｽﾃﾑの運用管理を同じﾛｰﾙをもつ複数の運用担当者が互いに干渉なく手分けして行うことが可能になる。 当機能は ACL ﾏﾈｰｼﾞｬ機能が提供する運用管理ｸﾗｲｱﾝﾄに対するｱｸｾｽ制御機能を強化するものであり、その利用に対しては、有効（起動）と無効（停止）が選択できる。有効を選択した場合に当機能は動作する。CMGR/MGR および CMGR/CL(M)において、ACL ﾏﾈｰｼﾞｬ機能にｱﾄﾞｵﾝする形で動作する。
LiveHelp 接続認証機能	：LiveHelp ｸﾗｲｱﾝﾄにおいて、LiveHelp を使用してﾘﾓｰﾄ操作を行う者が許可された運用担当者であることを識別認証する機能を提供する。ﾊﾟｽﾜｰﾄﾞ認証方式と OS 認証方式の二つを用意しており、業務ｼｽﾃﾑの運用環境に応じて選択する。前者は LiveHelp ｸﾗｲｱﾝﾄに登録されたﾊﾟｽﾜｰﾄﾞを使って認証を行い、後者は LiveHelp ｸﾗｲｱﾝﾄの OS の識別認証機能を使って認証を行う。当機能は常に動作する。
ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能	：CMGR/MGR、CMGR/Agent(S)、および CMGR/Agent(J)において、ACL ﾏﾈｰｼﾞｬ機能の識別認証に係る監査事象（識別認証の実行、ﾛｰﾙの登録と削除）と、ｺﾏﾝﾄﾞ操作に対するﾛｰﾙによるｱｸｾｽ制御に係る監査事象を記録する。記録された監査ﾛｸﾞの照会は、流通する市販のｿﾌﾄ等を利用する（本 TOE は照会のための機能を提供しない）。当機能の利用に対しては、有効（起動）と無効（停止）が選択でき、有効を指定した場合に動作する。

機能名	説明
運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能	：CMGR/CL(M)において、運用管理ｸﾗｲｱﾝﾄからの操作に係る監査事象（ﾛｰﾙで許可された操作の実行、ｺﾝｿｰﾙ操作制御機能で定義された操作の実行、LiveHelp 識別認証の実行）を記録する。記録された監査ﾛｸﾞの照会は、流通する市販のｿﾌﾄ等を利用する（本 TOE は照会のための機能を提供しない）。当機能の利用に対しては、有効(起動）と無効（停止）が選択でき、有効を指定した場合に動作する。
適用結果の自動通知機能	：運用管理機能の資源配付を構成する機能要素の一つであり、配付資源の配付および適用の結果を上位ｼｽﾃﾑへ自動通知する機能を提供する。これにより、ｻｰﾊﾞ、ｸﾗｲｱﾝﾄにおける配付資源の適用状況を確実に把握することができる。CMGR/CL(U)では CMGR/Agent(S)または CMGR/Agent(J)への通知機能を提供し、CMGR/Agent(S)および CMGR/Agent(J)では CMGR/MGR への通知機能を提供する。当機能の利用に対しては、有効（起動）と無効（停止）が選択でき、有効を指定した場合に動作する。
ｻｰﾊﾞ上の TOE にﾛｸﾞｲﾝするためのﾊﾟｽﾜｰﾄﾞの保護機能	：ﾛｸﾞｲﾝする際のﾊﾟｽﾜｰﾄﾞが解読されないよう、独自のﾒｶﾆｽﾞﾑにより異なるﾃﾞｰﾀに変換および復元する機能を提供する。CMGR/CL(M)および CMGR/CL(U)でﾊﾟｽﾜｰﾄﾞの変換を行い、ﾛｸﾞｲﾝ先である CMGR/MGR、CMGR/Agent(J)および CMGR/Agent(S)でﾊﾟｽﾜｰﾄﾞの復元を行う。当機能は常に動作する。

2.4.3. TOE が依存する IT 環境

本 TOE が依存する IT 環境の機能には以下のものがある。

機能名	説明
利用者の識別認証機能	：本 TOE は、本 TOE の関連者を識別認証するために、OS が提供する識別認証機能を使用する。また、LiveHelp 接続認証機能で OS 認証方式を採用した場合も、本 TOE はﾘﾓｰﾄ操作を行う運用担当者を識別認証するために、当機能を使用する。
ﾘﾓｰﾄ操作時のﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞの保護機能	：本 TOE は、ﾘﾓｰﾄ操作時のﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞが解読されないよう異なったﾃﾞｰﾀに変換するため、運用管理ｸﾗｲｱﾝﾄおよび LiveHelp ｸﾗｲｱﾝﾄの OS が提供するﾃﾞｰﾀの変換/復元機能を使用する。
監査機能の起動と終了に係る監査ﾛｸﾞ機能	：本 TOE は、運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能の起動と終了事象に係る監査ﾛｸﾞをｲﾍﾞﾝﾄﾛｸﾞに出力するﾛｸﾞで代替するため、OS が提供するｲﾍﾞﾝﾄﾛｸﾞ機能を使用する。

機能名	説明
日付時刻の計時機能	：本 TOE は、監査ﾛｸﾞに設定する日付時刻の値、およびｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間の判定に使用する日付時刻の値を取得するために、OS が提供するﾀｲﾏ機能を使用する。

2.5. TOE の動作形態

図 2.3 は、本 TOE の論理的な接続形態を示したものである。互いに連携して動作することで、分散システム環境下における運用管理機能を実現する。

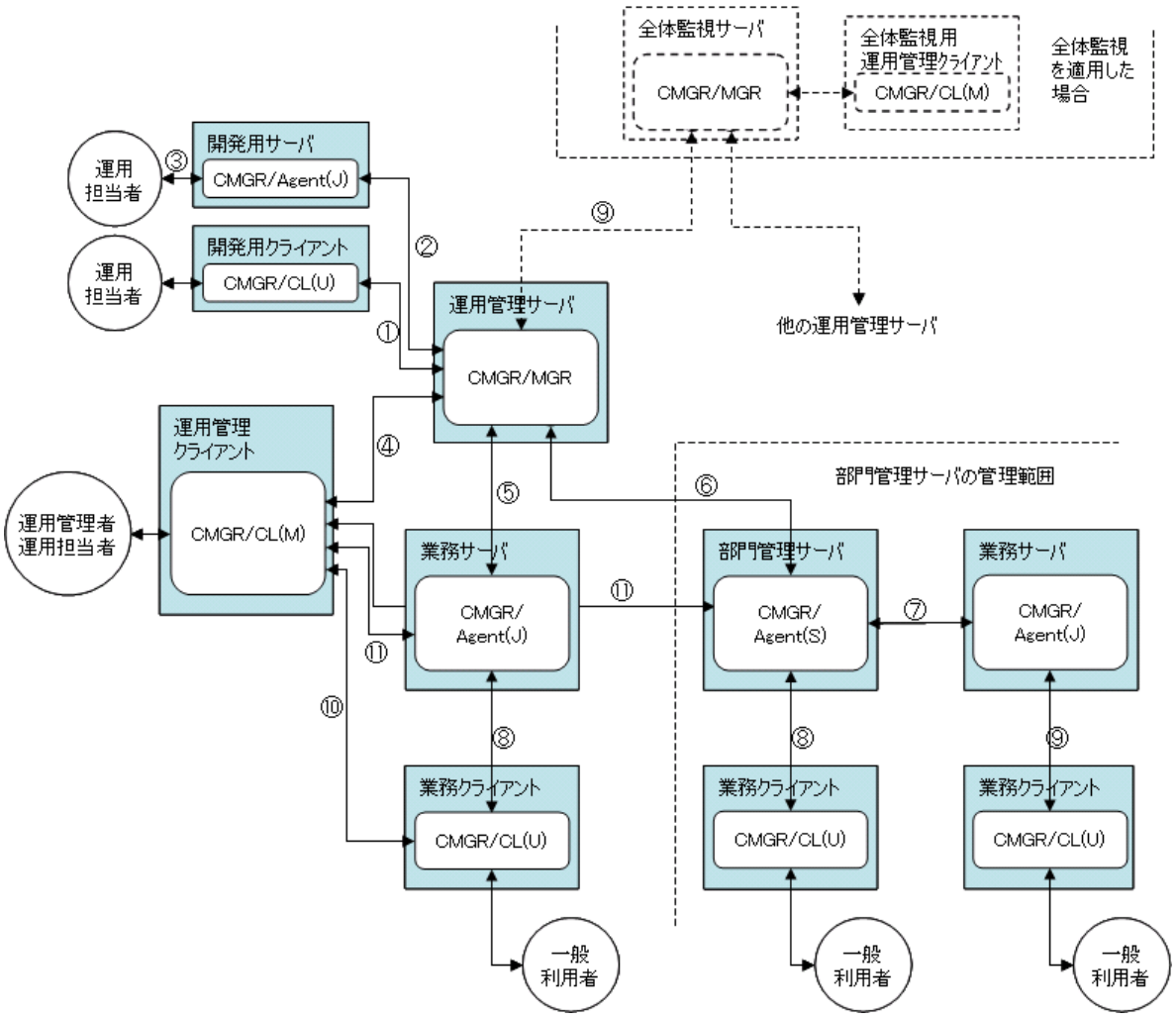

図 2.3　TOE の論理的な接続形態

資源配付の場合は以下のとおり動作する。

・ 配付資源の登録とアップロードは、開発用クライアントの CMGR/CL(U)（クライアント資源の場合）または開発用サーバの CMGR/Agent(J)（サーバ資源の場合）から、運

用管理サーバの CMGR/MGR に対して行う（図中①②③）。

- 資源の配付指示は、CMGR/CL(M)から CMGR/MGR に対して行う（図中④）。その結果、サーバ資源については、運用管理サーバの CMGR/MGR から CMGR/Agent(J)に配付され適用される（図中⑤）。CMGR/Agent(S)が存在する場合、運用管理サーバの CMGR/MGR は CMGR/Agent(S)まで配付を行い（図中⑥）、管理範囲内の CMGR/Agent(J)への配付は CMGR/Agent(S)が行う（図中⑦）。
- 資源が配付された後、サーバ毎に配付資源の適用を行う場合は、CMGR/Agent(J)または CMGR/Agent(S)に対して、CMGR/CL(M)から適用指示を行う（図中⑪）。
- クライアント資源については、CMGR/Agent(S)および CMGR/Agent(J)で保持され、業務クライアントの CMGR/CL(U)からのダウンロード要求を受けて、CMGR/CL(U)へ配付され適用される（図中⑧）。

監視の場合は以下のとおり動作する。

- CMGR/Agent(S)および CMGR/Agent(J)が監視対象イベントの収集を行い、運用管理サーバの CMGR/MGR へ通知する（図中⑤）。部門管理サーバが存在する場合は、CMGR/Agent(S)でいったん集約されたのち、運用管理サーバの CMGR/MGR へ送られる（図中⑦⑥）。
- 運用管理サーバの CMGR/MGR は、通知された監視対象イベントを CMGR/CL(M)に表示する（図中④）
- 全体監視サーバが存在する場合は、運用管理サーバの CMGR/MGR から全体監視サーバの CMGR/MGR に対して、全体監視に必要な監視対象イベントが通知（図中⑨）され、全体監視用に用意された CMGR/CL(M)に表示される。

CMGR/CL(M)からのリモートコマンドを使ったサーバ操作や、業務クライアントのリモート操作の場合は以下のとおり動作する。

- サーバ操作については、CMGR/CL(M)から運用管理サーバの CMGR/MGR にリモートコマンドが送られ（図中④）、CMGR/MGR により目的の CMGR/Agent(S)または CMGR/Agent(J)に送付され実行される。
- 業務クライアントがトラブル時のリモート操作については、CMGR/CL(M)から該当の業務クライアントの CMGR/CL(U)に接続し（図中⑩）、業務クライアントでの表示画面を運用管理クライアントに転送表示することで、トラブルの調査と復旧が行われる。CMGR/CL(U)以外の LiveHelp クライアントについても同様である。

そして、これらの動作がセキュアに行なわれるよう、TOE のセキュリティ機能は、TOE の関連者に対して、以下のとおりアクセス制御や識別認証を実施する。

- ACL マネージャ機能は、CMGR/CL(M)から運用管理サーバの CMGR/MGR を運用操作（図中④）する運用管理者および運用担当者に対して、その識別と識別結果に基づく操作制限を実施する。また、CMGR/MGR、CMGR/Agent(S)および CMGR/Agent(J)が提供するサーバ向けコマンドについても同様に制限する。

- コンソール操作制御機能は、CMGR/CL(M)から運用管理サーバの CMGR/MGR を運用操作（図中④）する運用担当者に対して、ACL マネージャ機能にアドオンする形で運用担当者毎の操作制限を実施する。
- LiveHelp 接続認証機能は、LiveHelp クライアントのリモート操作を行う運用担当者に対して、その識別認証を LiveHelp クライアントにおいて実施する（図中⑩）。
- 監査ログ機能は、CMGR/MGR、CMGR/Agent(S)、CMGR/Agent(J)、および CMGR/CL(M)において、監査ログの採取を行う。
- 業務クライアントおよび開発用クライアントからの操作に対しては､接続先サーバの OS が提供する識別認証機能を使って利用者を識別する。

また、表 2.7 は、サーバ、クライアントの接続関係を示したものである（サーバの OS にログインし直接操作する形態は除く）。前述のとおり、部門管理サーバが導入されても、やり取りされるデータの種類には違いはなく、ネットワーク接続の方式も同一である。運用操作の仕組みについても、運用管理サーバと同じである。そのため、部門管理サーバの導入による新たな不正利用の脅威は存在しない。全体監視サーバについても、扱うデータは運用管理サーバに集まるデータの中の全体監視に係るデータであり、ネットワーク接続の方式や運用操作の仕組みは運用管理サーバと同一である。よって、部門管理サーバと同様、全体監視サーバの導入による新たな不正利用の脅威は存在しない。

表 2.7　サーバ、クライアントの接続関係

接続可能なサーバ、クライアント / サーバ、クライアント	運用管理ｻｰﾊﾞ	運用管理ｸﾗｲｱﾝﾄ	開発ｼｽﾃﾑ	業務ｻｰﾊﾞ	業務ｸﾗｲｱﾝﾄ	部門管理ｻｰﾊﾞ	全体監視ｻｰﾊﾞ
運用管理ｻｰﾊﾞ		○	○	○	－	○	○
運用管理ｸﾗｲｱﾝﾄ	○		－	○	○	○	○
開発ｼｽﾃﾑ	○	－		－	－	－	－
業務ｻｰﾊﾞ	○	○	－		○	○	－
業務ｸﾗｲｱﾝﾄ	－	○	－	○		○	－
部門管理ｻｰﾊﾞ	○	○	－	○	○		－
全体監視ｻｰﾊﾞ	○	○	－	－	－	－	

2.6　保護対象とする資産

本 TOE は業務システムの可用性向上に貢献することから、本 TOE の適用により業務システム資産が享受する可用性を保護資産とする。可用性の主たるものは業務システムの安定

稼動であり、それは本 TOE の 4 つの運用管理フェーズが一連のサイクルとして回ることで実現される。よって、各々の運用管理フェーズを支援する運用管理機能が対象とする資産が可用性を保護するための具体的な保護資産である。

1) デプロイ（配付）における保護資産

このフェーズを支援する運用管理機能は資源配付機能である。以下の保護資産がある。

【資産】	【説明】
配付資源	：業務ｻｰﾊﾞや業務ｸﾗｲｱﾝﾄで使用されるｿﾌﾄｳｪｱやﾃﾞｰﾀである。業務情報を含む可能性があり、完全性と機密性を保護する必要がある。また、配付資源が正しく配付・適用されていることを保証するため、業務ｻｰﾊﾞや業務ｸﾗｲｱﾝﾄにおける配付・適用状況についても保護を行う。
資源配付のための定義情報	：資源配付の動作環境を定義した情報であり、機密性の保護は必要ないが、完全性を保護する必要がある。 なお、業務ｸﾗｲｱﾝﾄには配付資源をﾀﾞｳﾝﾛｰﾄﾞするための定義情報が存在する。この定義情報は業務運用中にその業務ｸﾗｲｱﾝﾄを所有する一般利用者によって変更が可能である。

2) モニタリング（監視）における保護資産

このフェーズを支援する運用管理機能は、サーバ管理とネットワーク管理である。以下の保護資産がある。

【資産】	【説明】
収集情報（監視対象ｲﾍﾞﾝﾄ情報）	：本 TOE はこの情報を使って状況監視を行うため、完全性を保護する必要がある。また、監視対象ｲﾍﾞﾝﾄ情報それ自体には機密性はないが、定義情報等と組み合わされ意味のある形で運用管理ｸﾗｲｱﾝﾄに表示された場合には、不正に対してﾋﾝﾄを与える可能性が予想されることから、権限のある者のみに表示操作を許可することで、その保護を行う。
監視のための定義情報	：監視対象の業務ｼｽﾃﾑ資産や、監視対象ｲﾍﾞﾝﾄとその通知先等を定義した情報である。機密性の保護は不要であるが、誤りのない監視を行うため、完全性を保証する必要がある。

3) リカバリ（復旧）における保護資産

このフェーズを支援する運用管理機能は、サーバ管理、ネットワーク管理、そして

LiveHelp である。以下の保護資産がある。

【資産】	【説明】
業務ｻｰﾊﾞの OS やｱﾌﾟﾘｹｰｼｮﾝを復旧するための操作環境	：本 TOE は業務ｻｰﾊﾞの OS やｱﾌﾟﾘｹｰｼｮﾝと連携し、各々がもつ復旧操作のｲﾝﾀﾌｪｰｽを運用管理ｸﾗｲｱﾝﾄからﾘﾓｰﾄで操作できる環境を用意することで、迅速な原因究明や復旧を実現している。 この操作環境が不正利用された場合、対象となる業務ｻｰﾊﾞの OS やｱﾌﾟﾘｹｰｼｮﾝの可用性を損なう可能性があるため、不正利用から保護する。
ﾈｯﾄﾜｰｸ機器を復旧するための操作環境	：ﾈｯﾄﾜｰｸ機器の復旧操作に対しても、本 TOE はﾈｯﾄﾜｰｸ機器と連携することで運用管理ｸﾗｲｱﾝﾄからﾘﾓｰﾄで行える環境を用意しており、上記と同様、不正利用から保護する。
LiveHelp ｸﾗｲｱﾝﾄを復旧するための操作環境	：LiveHelp ｸﾗｲｱﾝﾄを復旧させるためのﾘﾓｰﾄ操作環境であり、上記と同様、不正利用から保護する。
ﾘﾓｰﾄ操作時のﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞ	：ﾘﾓｰﾄ操作を行う LiveHelp ｸﾗｲｱﾝﾄにﾛｸﾞｲﾝする際のﾊﾟｽﾜｰﾄﾞであり、ﾈｯﾄﾜｰｸに接続された装置から盗聴されないよう保護する。
復旧のための定義情報	：復旧のためのｺﾏﾝﾄﾞや宛先ｼｽﾃﾑ等を定義した情報であり、機密性の保護は不要であるが、復旧操作を正しく動作させるために完全性を保証する必要がある。

4) アセスメント（査定）における保護資産

このフェーズを支援する運用管理機能はレポーティング機能である。以下の保護資産がある。

【資産】	【説明】
収集情報（ﾛｸﾞﾌｧｲﾙ情報）	：本 TOE はこの情報をもとに業務ｼｽﾃﾑの稼動分析を行うため、完全性を保護する必要がある。また、ﾛｸﾞﾌｧｲﾙ情報それ自体には機密性はないが、定義情報と組み合わされ意味のある形で運用管理ｸﾗｲｱﾝﾄに表示された場合には、不正に対してﾋﾝﾄを与える可能性が予想されることから、権限のある者のみに表示操作を許すことで、その保護を行う。
ﾛｸﾞ収集のための定義情報	：ﾛｸﾞﾌｧｲﾙのﾌｧｲﾙ名や所在を定義した情報であり、機密性の保護は不要であるが、正しく収集操作が行われるよう完全性を保護する必要がある。

5) 各フェーズに共通な保護資産

前述した保護資産に加え以下の保護資産がある。

【資産】	【説明】
ｻｰﾊﾞ上の TOE にﾛｸﾞｲﾝするためのﾊﾟｽﾜｰﾄﾞ	：ｻｰﾊﾞ上で動作する TOE にﾛｸﾞｲﾝする際のﾊﾟｽﾜｰﾄﾞである。ﾈｯﾄﾜｰｸに接続された装置から盗聴されないよう保護する。

〔補足〕

なお、ここに示した資産をネットワーク上でやり取りする際の完全性の保護については、攻撃者は本 TOE の非公開プロトコルを理解した上で行う必要があり、本 TOE が想定する低レベルの攻撃者では不可能であることから、ネットワーク上での完全性保護のための機構は導入しない。

3. TOE セキュリティ環境

本章では、前提条件、脅威、組織のセキュリティ方針について記述する。

なお、その記述に際しては、前提条件、脅威および組織のセキュリティ方針を示すそれぞれのラベルを***ボールド体***を使って明示する。

3.1 前提条件

TOE には、意図する使用方法及び使用環境に関して、以下の前提条件が存在する。

■ **A.ADMIN（システム管理者、運用管理者）**

システム管理者、運用管理者は不正を行わない信頼できる者とする。

■ **A.PASSWORD（パスワードの管理）**

本 TOE にログインするためのパスワードについて、本人以外の者がパスワードを知ることはできないものとする。

■ **A.NETWORK（ネットワーク環境）**

本 TOE が動作するサーバ、クライアントおよび本 TOE が運用管理の対象とする業務システム資産は、インターネットなど信頼されない外部ネットワークから直接アクセスされないネットワーク環境で動作するものとする。

■ **A.PLACE（設置場所）**

開発用サーバを除く本 TOE が動作するサーバは、システム管理者以外の者が入退出できない、物理的に保護された場所に設置するものとする。

■ **A.OS_ACCESS（OS を経由したアクセス）**

本 TOE が運用管理で使用する資産（“2.2.2 TOE の利用環境”の 6 項参照）を格納したファイルや、その処理のための作業用ファイルについては、OS 経由でのアクセスが行われないものとする。

■ **A.DEPLOY_ENCR（機密性ある配付資源）**

本 TOE を使って配付される配付資源は、ネットワーク上で盗聴されないものとする。

■ **A.CLIENT（業務クライアントおよび開発用クライアントの運用）**

業務クライアントおよび開発用クライアントは、不正に利用されないものとする。

■ **A.LIVEHELP_PWD（LiveHelp 接続認証でのパスワード長）**

LiveHelp クライアントのリモート操作において、パスワード認証方式を利用する場合は、7 文字以上のパスワードが設定されているものとする。

3.2 脅威

TOE には、意図する使用方法及び使用環境に関して、以下の脅威が存在する。

本 TOE では、低レベルの攻撃者を想定する。

なお、以下の記述において、運用担当者は作業効率上または職務権限上、作業範囲の局所化のために運用が行える担当範囲が個別に定められており、その担当範囲外に対しては脅威を与える可能性がある。

〔すべての運用管理フェーズに共通な脅威〕

■ T.PASSWORD（パスワードの盗聴）

攻撃者によって､サーバ上の本 TOE にログインするためのパスワードがネットワークに接続された装置をとおして盗聴され、その内容が漏洩するかもしれない。

■ T.UAACTION（運用担当者からの不正な操作）

運用担当者の役割を与えられた者が、運用管理クライアントまたは TOE が提供するコマンドを使って許可されない操作を不正に行い、デプロイ、モニタリング、リカバリおよびアセスメントの各運用操作の遂行に悪影響を与えるかもしれない。

■ T.OPCL_UAUSER（運用管理クライアントでの成りすまし）

攻撃者が運用管理クライアントの操作権限のある者に成りすまし、デプロイ、モニタリングおよびアセスメントの情報を暴露・改ざん、または不正なリカバリ操作を行うかもしれない。

■ T.CMD_UAUSER（コマンド操作における成りすまし）

攻撃者が TOE の提供するコマンドを操作できる権限のある者に成りすまし、コマンドを使ってサーバ上の本 TOE や本 TOE の保護資産を不正に操作するかもしれない。

■ T.SV_DEF_FALS（定義情報の改ざん）

運用担当者の役割を与えられた者が、自身の役割を超えて、運用管理サーバ、部門管理サーバ、および業務サーバ上の本 TOE の定義情報を改ざんすることで、本 TOE を使った運用管理が行えなくなるかもしれない。

〔デプロイでの脅威〕

■ T.D_DELIVER_FAIL（配付異常の検知遅れ）

通信路や配付先の業務サーバの異常により資源が配付されなかった場合に、それに気づかずに運用が継続されるかもしれない。

■ T.D_APPLY_FAIL（適用異常の検知遅れ）

業務サーバや業務クライアントへ資源が配付されたのち、配付先の業務サーバや業務クライアントの異常により配付資源が適用されなかった場合に、それに気づかずに運用が継続されるかもしれない。

〔モニタリングおよびアセスメントでの脅威〕

■ T.MA_OPCL_VIOLATION（担当範囲外への不正な監視／査定操作）
　運用担当者の役割を与えられた者が、運用管理クライアントから担当範囲外の業務システム資産に対して許可されない監視／査定操作を行い、運用管理クライアントに表示された情報を不正に入手するかもしれない。

〔リカバリでの脅威〕

■ T.R_OPCL_VIOLATION（担当範囲外への不正な復旧操作）
　運用担当者の役割を与えられた者が、運用管理クライアントから担当範囲外の業務システム資産に対して許可されない復旧操作を行い、該当する業務サーバやネットワーク機器に悪影響を与えるかもしれない。
■ T.R_RMTCL（リモート操作における成りすまし）
　攻撃者がリモート操作を行える者に成りすまし、運用管理クライアントから不正に LiveHelp クライアントをリモート操作することで、LiveHelp クライアントに悪影響を与えるかもしれない。
■ T.R_RMTCL_PWD（リモート操作でのログイン・パスワードの盗聴）
　リモート操作の対象となる LiveHelp クライアントへログインするためのパスワードが、攻撃者によりネットワークに接続した装置をとおして盗聴され、その内容が漏洩するかもしれない。

3.3　組織のセキュリティ方針

本 TOE には、意図する使用方法及び使用環境に関する組織のセキュリティ方針はない。

4. セキュリティ対策方針

本章では、TOE セキュリティ対策方針、環境のセキュリティ対策方針について記述する。

なお、その記述に際しては、各々のセキュリティ対策方針を示すラベルを***ボールド体***で明示する。

4.1. TOE セキュリティ対策方針

本節は、脅威に対抗し、組織のセキュリティ方針を実現するための TOE のセキュリティ対策方針を示す。

■ **O.PWD_ENCR**（運用管理サーバにログインするパスワードの保護）

本 TOE は、運用管理クライアントまたは業務クライアント上の TOE を使ってサーバ上の TOE にログインする際、ログイン・パスワードの内容を異なるデータに変換することで解析できないようにする。

■ **O.ACCESS_CTL(1)**（ロールに基づくアクセス制御）

本 TOE は、運用管理クライアントまたは TOE が提供するコマンドを使った操作に対し、ロールに基づく操作制限を実施する。

■ **O.ACCESS_CTL(2)**（運用担当者毎のアクセス制御）

本 TOE は、運用管理クライアントからの操作に対し、運用担当者毎の操作制限を実施する。

■ **O.IDFY**（利用者の識別）

本 TOE は、LiveHelp を除く運用管理機能を使用する者について、システム管理者、運用管理者、運用担当者の識別を行う。

■ **O.LIVEHELP_I&A**（LiveHelp 利用者の識別認証）

本 TOE は、LiveHelp の利用でパスワード認証方式が選択された場合、リモート操作の対象となる LiveHelp クライアントにおいて、リモート操作を行う運用担当者を識別認証する。

■ **O.STATUS_NOTIFY**（配付および適用結果の自動通知）

本 TOE は、資源の配付や適用を行った場合、その結果を示す資源の配付・適用結果データを運用管理サーバに自動通知する。

4.2. 環境のセキュリティ対策方針

脅威に対抗するための技術的な環境のセキュリティ対策方針を以下に示す。

■ **OE.OPSV_OS_I&A**（運用管理サーバの OS での識別認証）

運用管理サーバの OS は、そのサーバに登録された本 TOE の関連者を識別認証する。

■ OE.JOBSV_OS_I&A（業務サーバおよび部門管理サーバの OS での識別認証）

業務サーバおよび部門管理サーバの OS は、そのサーバに登録された本 TOE の関連者を識別認証する。

■ OE.CL_OS_I&A（クライアントの OS での識別認証）

リモート操作の対象となる LiveHelp クライアントの中で、業務クライアントまたは運用管理クライアントの OS は、そのクライアントに登録された本 TOE の関連者を識別認証する。

■ OE.RMTCL_ENCR（リモート操作でのパスワードの保護）

リモート操作において､運用管理クライアントと LiveHelp クライアントの OS は、運用管理クライアントから LiveHelp クライアントにパスワードを送付する際、パスワードの内容が解析できないようにする。

■ OE.OS_AUDIT（OS による監査記録の代替）

運用管理クライアントの OS は、運用管理クライアント操作の監査ログ機能の起動と終了について、その事象をイベントログに記録する。

■ OE.OS_DATETIME（OS での日付時刻の取得）

運用管理クライアント、運用管理サーバ、部門管理サーバおよび業務サーバの OS は、高信頼なタイムスタンプ値を提供する。

非技術的な環境のセキュリティ対策方針を以下に示す。

■ OE.ASSIGN（選任）

運用管理部門は、システム管理者および運用管理者として、信頼できる者を選任しなければならない。

■ OE.PASSWORD（パスワードの管理）

運用管理部門は、本 TOE の関連者に対して、パスワードを口外しないよう周知徹底し、本 TOE の関連者はそれを遵守しなければならない。

■ OE.NETWORK（ネットワーク環境）

システム管理者は、本 TOE が動作するサーバ、クライアントおよび本 TOE が運用管理の対象とする業務システム資産をネットワークに接続する場合、ファイアウォールで区切られたイントラネット内に接続しなければならない。

■ OE.PLACE（設置場所）

システム管理者は、開発用サーバを除く本 TOE が動作するサーバを人的、機械的または電子的な手段による入退出管理が施された、システム管理者以外の者が容易に入室不可能な事務フロアやサーバルーム等に設置しなければならない。

■ OE.OS_SETUP（OS のアクセス設定）

システム管理者は、本 TOE を介さずに直接 OS から不正が行われないよう、OS のア

クセス制御設定について、インストール時の設定を維持しなければならない。

■ OE.DEPLOY_ENCR（機密性ある配付資源の事前暗号化）

機密性のある資源を配付する場合、システム管理者または運用管理者は、運用担当者に対して、TOE 外で事前に暗号化し配付するよう指示しなければならない。

■ OE.CLIENT_SETUP（システム管理者によるクライアントのセットアップ）

システム管理者は、業務クライアントおよび開発用クライアントについて、正しく本 TOE が利用されるよう、その OS および本 TOE をセットアップしなければならない。

■ OE.CLIENT_CHK（定期的なクライアントの監査）

システム管理者は、定期的に業務クライアントや開発用クライアントの利用状況を確認し、不正の兆候がないか監査しなければならない。

■ OE.OSCONS_ENCR（セキュアな通信手段によるパスワードの保護）

システム管理者は、本 TOE が動作するサーバ上の OS に対するログイン・パスワードを保護するため、セキュアな通信手段である SSH を適用しなければならない。

■ OE.LIVEHELP_PWD（リモート操作でのパスワード長）

パスワード認証方式を利用してリモート操作の識別認証を行う場合、システム管理者は 7 文字以上のパスワードを設定しなければならない。

5. IT セキュリティ要件

本章では、TOE のセキュリティ機能要件、TOE のセキュリティ保証要件、TOE の機能強度および IT 環境に対するセキュリティ要件について示す。

なお、セキュリティ機能要件コンポーネントに対する操作内容について、以下のとおり表記する。

- 割付および選択は、操作内容をイタリック体かつ**ボールド体**で表記する。
- 繰り返しは、コンポーネントのラベルの末尾に括弧付きの数字（(1)、(2)等）を付与して区別する。
  なお、IT 環境のセキュリティ機能要件については、IT 環境であることを明示するため、識別子[ENV]を付与している。そのため、IT 環境のセキュリティ機能要件が繰り返しの対象である場合には、FAU_GEN.1[ENV](3)のように表記する。
- 詳細化は、詳細化したテキストを直接ステートメント中にイタリック体かつ**ボールド体**で記述し、下線を付加して明示する。

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

本 TOE では、以下のセキュリティ機能要件を定義する。

FAU_GEN.1(1) 監査データ生成

下位階層: なし

FAU_GEN.1.1(1)

ACL マネージャ機能の監査ログ機能は、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：

a) 監査機能の起動と終了；

b) 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

c) [割付: *上記以外の個別に定義した監査対象事象*]。

[選択: *最小、基本、詳細、指定なし：から一つのみ選択*]

― ***最小***

機能要件	CC で定義された監査対象	監査事象
FAU_GEN.1(1)	なし	
FAU_GEN.1(2)	なし	
FAU_SAR.1	a) 基本：監査記録からの情報の読み出し	―（最小を選択しているため対象外、以下同様）
FAU_STG.1	なし	
FAU_STG.3	a) 基本：閾値を超えたためにとられるｱｸｼｮﾝ	―
FAU_STG.4	a) 基本：監査格納失敗によってとられるｱｸｼｮﾝ	―
FDP_ACC.1 (1)(2)	なし	
FDP_ACF.1(1)	a) 最小：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行における成功した要求。 b) 基本：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行におけるすべての要求。 c) 詳細：ｱｸｾｽﾁｪｯｸ時に用いられる特定のｾｷｭﾘﾃｨ属性。	ﾛｰﾙで許可されたｺﾏﾝﾄﾞを実行した事象（ﾒﾆｭｰを実行した場合の事象については FAU_GEN.1(2)で規定）
FDP_ACF.1(2)	a) 最小：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行における成功した要求。 b) 基本：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行におけるすべての要求。 c) 詳細：ｱｸｾｽﾁｪｯｸ時に用いられる特定のｾｷｭﾘﾃｨ属性。	対象外（当該監査事象は FAU_GEN.1(2)で規定）
FDP_IFC.1	なし	

機能要件	CC で定義された監査対象	監査事象
FDP_IFF.1	a) 最小: 要求された情報ﾌﾛｰを許可する決定。 b) 基本: 情報ﾌﾛｰに対する要求に関するすべての決定。 c) 詳細: 情報ﾌﾛｰの実施を決定する上で用いられる特定のｾｷｭﾘﾃｨ属性 d) 詳細：方針目的(policy goal)に基づいて流れた特定の情報のｻﾌﾞｾｯﾄ（例えば、対象物のﾚﾍﾞﾙ低下の監査）	対象外（当該監査事象はFAU_GEN.1(2)で規定）
FIA_AFL.1	a) 最小：不成功の認証試行に対する閾値への到達及びそれに続いてとられるｱｸｼｮﾝ（例えば端末の停止）、もし適切であれば、正常状態への復帰（例えば端末の再稼動）	対象外（当該監査事象はFAU_GEN.1(2)で規定）
FIA_ATD.1	なし	
FIA_SOS.1	a) 最小: TSFによる、ﾃｽﾄされた秘密の拒否; b) 基本: TSFによる、ﾃｽﾄされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	対象外（当該監査事象はFAU_GEN.1(2)で規定）
FIA_UAU.2(1)	a) 最小:認証ﾒｶﾆｽﾞﾑの不成功になった使用; b) 基本:認証ﾒｶﾆｽﾞﾑのすべての使用	対象外（当該監査事象はFAU_GEN.1(2)で規定）
FIA_UAU.6	a) 最小：再認証の失敗 b) 基本：すべての再認証試行	ｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間が切れた際の再認証事象（成功、失敗）
FIA_UAU.7	なし	
FIA_UID.2(1)	a) 最小: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑのすべての使用。	ACL ﾏﾈｰｼﾞｬ機能におけるｼｽﾃﾑ管理者、運用管理者および運用担当者の識別認証事象（成功、失敗）
FIA_UID.2(2)	a) 最小: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑのすべての使用。	対象外（当該監査事象はFAU_GEN.1(2)で規定）
FIA_USB.1	a) 最小: 利用者ｾｷｭﾘﾃｨ属性のｻﾌﾞｼﾞｪｸﾄに対する不成功結合(例えば、ｻﾌﾞｼﾞｪｸﾄの生成)。 b) 基本: 利用者ｾｷｭﾘﾃｨ属性のｻﾌﾞｼﾞｪｸﾄに対する結合の成功及び失敗(例えば、ｻﾌﾞｼﾞｪｸﾄの生成の成功または失敗)。	ACL ﾏﾈｰｼﾞｬ機能におけるｼｽﾃﾑ管理者、運用管理者および運用担当者の識別認証事象（成功、失敗）
FMT_MOF.1	a) 基本：TSF の機能のふるまいにおけるすべての改変	－
FMT_MSA.1(1)	a) 基本: ｾｷｭﾘﾃｨ属性の値の改変すべて。	－
FMT_MSA.1(2)	a) 基本: ｾｷｭﾘﾃｨ属性の値の改変すべて。	－
FMT_MSA.1(3)	a) 基本: ｾｷｭﾘﾃｨ属性の値の改変すべて。	－
FMT_MSA.3(1)	a) 基本：許可的あるいは制限的規則のﾃﾞﾌｫﾙﾄ設定の改変 b) 基本：ｾｷｭﾘﾃｨ属性の初期値の改変すべて。	－

機能要件	CC で定義された監査対象	監査事象
FMT_MSA.3(2)	a) 基本：許可的あるいは制限的規則のﾃﾞﾌｫﾙﾄ設定の改変 b) 基本：ｾｷｭﾘﾃｨ属性の初期値の改変すべて。	－
FMT_MSA.3(3)	a) 基本：許可的あるいは制限的規則のﾃﾞﾌｫﾙﾄ設定の改変 b) 基本：ｾｷｭﾘﾃｨ属性の初期値の改変すべて。	－
FMT_MTD.1	a) 基本：TSFﾃﾞｰﾀの値のすべての改変。	－
FMT_SMF.1	a) 最小：管理機能の使用	対象外（当該監査事象は FAU_GEN.1(2)で規定）
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のｸﾞﾙｰﾌﾟに対する改変; b) 詳細: 役割の権限の使用すべて。	なし
FPT_ITT.1(1)	なし	
FPT_RVM.1	なし	
FPT_SEP.1	なし	

[割付: *上記以外の個別に定義した監査対象事象*]

— ***ACL ﾏﾈｰｼﾞｬ機能におけるﾕｰｻﾞ名へのﾛｰﾙの登録、削除を行った事象***

FAU_GEN.1.2(1)

ACL マネージャ機能の監査ログ機能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：

a) 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（成功又は失敗）；及び

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

[割付: *その他の監査関連情報*]

— ***操作を行った運用管理クライアントのホスト名***

依存性: FPT_STM.1 高信頼タイムスタンプ（FPT_STM.1[ENV]）

FAU_GEN.1(2) 監査データ生成

下位階層: なし

FAU_GEN.1.1(2)

運用管理クライアント操作の監査ログ機能は、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：

a) 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

b) [割付: *上記以外の個別に定義した監査対象事象*]。

[選択: *最小、基本、詳細、指定なし：から一つのみ選択*]

― ***最小***

機能要件	CC で定義された監査対象	監査事象
FAU_GEN.1(1)	なし	
FAU_GEN.1(2)	なし	
FAU_SAR.1	a) 基本：監査記録からの情報の読み出し	―（最小を選択しているため対象外、以下同様）
FAU_STG.1	なし	
FAU_STG.3	a) 基本：閾値を超えたためにとられるｱｸｼｮﾝ	―
FAU_STG.4	a) 基本：監査格納失敗によってとられるｱｸｼｮﾝ	―
FDP_ACC.1 (1)(2)	なし	
FDP_ACF.1(1)	a) 最小：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行における成功した要求。 b) 基本：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行におけるすべての要求。 c) 詳細：ｱｸｾｽﾁｪｯｸ時に用いられる特定のｾｷｭﾘﾃｨ属性。	ACL ﾏﾈｰｼﾞｬ機能でのﾛｰﾙで許可されたﾒﾆｭｰを実行した事象
FDP_ACF.1(2)	a) 最小：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行における成功した要求。 b) 基本：SFP で扱われるｵﾌﾞｼﾞｪｸﾄに対する操作の実行におけるすべての要求。 c) 詳細：ｱｸｾｽﾁｪｯｸ時に用いられる特定のｾｷｭﾘﾃｨ属性。	ｺﾝｿｰﾙ操作制御機能での定義されたﾒﾆｭｰを実行した事象
FDP_IFC.1	なし	

機能要件	CC で定義された監査対象	監査事象
FDP_IFF.1	a) 最小: 要求された情報ﾌﾛｰを許可する決定。 b) 基本: 情報ﾌﾛｰに対する要求に関するすべての決定。 c) 詳細: 情報ﾌﾛｰの実施を決定する上で用いられる特定のｾｷｭﾘﾃｨ属性 d) 詳細：方針目的(policy goal)に基づいて流れた特定の情報のｻﾌﾞｾｯﾄ（例えば、対象物のﾚﾍﾞﾙ低下の監査）	配付資源の適用結果の自動通知を有効にする定義を実行した事象
FIA_AFL.1	a) 最小：不成功の認証試行に対する閾値への到達及びそれに続いてとられるｱｸｼｮﾝ（例えば端末の停止）、もし適切であれば、正常状態への復帰（例えば端末の再稼動）	ACL ﾏﾈｰｼﾞｬ機能の識別認証における閾値到達とﾛｸﾞｲﾝ画面を閉じたことを示す事象
FIA_ATD.1	なし	
FIA_SOS.1	a) 最小: TSFによる、ﾃｽﾄされた秘密の拒否; b) 基本: TSFによる、ﾃｽﾄされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	LiveHelp 接続認証機能における不当ﾊﾟｽﾜｰﾄﾞを拒否した事象
FIA_UAU.2(1)	a) 最小:認証ﾒｶﾆｽﾞﾑの不成功になった使用; b) 基本:認証ﾒｶﾆｽﾞﾑのすべての使用	LiveHelp 接続認証機能における識別認証事象（成功、失敗）
FIA_UAU.6	a) 最小：再認証の失敗 b) 基本：すべての再認証試行	対象外（当該監視事象はFAU_GEN.1(1)で規定）
FIA_UAU.7	なし	
FIA_UID.2(1)	a) 最小: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑのすべての使用。	対象外（当該監査事象はFAU_GEN.1(1)で規定）
FIA_UID.2(2)	a) 最小: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別ﾒｶﾆｽﾞﾑのすべての使用。	LiveHelp 接続認証機能における識別認証事象（成功、失敗）
FIA_USB.1	a) 最小: 利用者ｾｷｭﾘﾃｨ属性のｻﾌﾞｼﾞｪｸﾄに対する不成功結合(例えば、ｻﾌﾞｼﾞｪｸﾄの生成)。 b) 基本: 利用者ｾｷｭﾘﾃｨ属性のｻﾌﾞｼﾞｪｸﾄに対する結合の成功及び失敗(例えば、ｻﾌﾞｼﾞｪｸﾄの生成の成功または失敗)。	対象外（当該監査事象はFAU_GEN.1(1)で規定）
FMT_MOF.1	a) 基本：TSF の機能のふるまいにおけるすべての改変	－
FMT_MSA.1(1)	a) 基本: ｾｷｭﾘﾃｨ属性の値の改変すべて。	－
FMT_MSA.1(2)	a) 基本: ｾｷｭﾘﾃｨ属性の値の改変すべて。	－
FMT_MSA.1(3)	a) 基本: ｾｷｭﾘﾃｨ属性の値の改変すべて。	－
FMT_MSA.3(1)	a) 基本：許可的あるいは制限的規則のﾃﾞﾌｫﾙﾄ設定の改変 b) 基本：ｾｷｭﾘﾃｨ属性の初期値の改変すべて。	－

機能要件	CC で定義された監査対象	監査事象
FMT_MSA.3(2)	a) 基本：許可的あるいは制限的規則のﾃﾞﾌｫﾙﾄ設定の改変 b) 基本：ｾｷｭﾘﾃｨ属性の初期値の改変すべて。	－
FMT_MSA.3(3)	a) 基本：許可的あるいは制限的規則のﾃﾞﾌｫﾙﾄ設定の改変 b) 基本：ｾｷｭﾘﾃｨ属性の初期値の改変すべて。	－
FMT_MTD.1	a) 基本：TSFﾃﾞｰﾀの値のすべての改変。	－
FMT_SMF.1	a) 最小：管理機能の使用	以下の管理機能を使用した事象 ・ 運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能における監査ﾛｸﾞﾌｧｲﾙの保存日数の管理機能 ・ 操作ﾚﾍﾞﾙと許可操作ﾚﾍﾞﾙの維持管理機能 ・ ﾕｰｻﾞ名に関するｺﾝｿｰﾙ操作制御機能の利用形態および再認証の決定に使用するﾕｰｻﾞ名の有効期間の各管理機能 ・ FMT_MOF.1 が関係する各ｾｷｭﾘﾃｨ機能での起動と停止を行う機能
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のｸﾞﾙｰﾌﾟに対する改変; b) 詳細: 役割の権限の使用すべて。	なし
FPT_ITT.1(1)	なし	
FPT_RVM.1	なし	
FPT_SEP.1	なし	

[割付: *上記以外の個別に定義した監査対象事象*]

－ ***なし***

FAU_GEN.1.2(2)

運用管理クライアント操作の監査ログ機能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：

a) 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（成功又は失敗）；及び

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

[割付：*その他の監査関連情報*]

－ ***操作を行った運用管理クライアントのホスト名***

依存性： FPT_STM.1 高信頼タイムスタンプ（FPT_STM.1[ENV]）

FAU_SAR.1　監査レビュー

下位階層：　　なし

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*]
- ***下表参照***

[割付：*監査情報のリスト*]
- ***下表参照***

許可利用者	***監査情報のリスト***
ｼｽﾃﾑ管理者	***FAU_GEN.1(1)およびFAU_GEN.1(2)で示したすべての監査事象の監査記録***

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。

依存性：　　FAU_GEN.1　監査データ生成（FAU_GEN.1(1)、(2)、および FAU_GEN.1[ENV](3)）

FAU_STG.1 保護された監査証跡格納

下位階層: なし

FAU_STG.1.1

TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2

TSF は、監査証跡内の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*]できねばならない。

[選択：*防止、検出：から一つのみ選択*]

－ ***防止***

依存性: FAU_GEN.1 監査データ生成（FAU_GEN.1(1)、(2)、および FAU_GEN.1[ENV](3)）

FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層: なし

FAU_STG.3.1

運用管理クライアント操作の監査ログ機能は、監査証跡が[割付: *事前に定義された限界*]を超えた場合、[割付: *監査格納失敗の恐れ発生時のアクション*]をとらなければならない。

[割付: *事前に定義された限界*]

- ***監査ログファイルの保存日数***

[割付: *監査格納失敗の恐れ発生時のアクション*]

- ***保存日数が超過した監査ログファイルの削除***

依存性: FAU_STG.1 保護された監査証跡格納（FAU_STG.1）

FAU_STG.4 監査データ損失の防止

下位階層: FAU_STG.3

FAU_STG.4.1

ACL マネージャ機能の監査ログ機能は、監査証跡が満杯になった場合、[選択: *監査対象事象の無視、特権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、最も古く格納された監査記録への上書き：から一つのみ選択*]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*]を行わねばならない。

[選択: *監査対象事象の無視、特権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、最も古く格納された監査記録への上書き：から一つのみ選択*]

- ***最も古く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***

依存性: FAU_STG.1 保護された監査証跡格納（FAU_STG.1）

FDP_ACC.1(1) サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1(1)

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

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

- ***下記参照***

ｻﾌﾞｼﾞｪｸﾄ	*ｵﾌﾞｼﾞｪｸﾄ*		*操作*
TOE 利用者ﾌﾟﾛｾｽ	*監視機能*	*環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ* *操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ* *表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ* *上記以外の TOE が提供するｺﾏﾝﾄﾞ*	*実行*
	資源配付機能	*環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ* *操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ* *表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ* *上記以外の TOE が提供するｺﾏﾝﾄﾞ*	

[割付: *アクセス制御 SFP*]

- ***ACL マネージャアクセス制御 SFP***

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御（FDP_ACF.1(1)）

FDP_ACC.1(2) サブセットアクセス制御

下位階層: なし

FDP_ACC.1.1(2)

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*]

— ***下記参照***

ｻﾌﾞｼﾞｪｸﾄ	*ｵﾌﾞｼﾞｪｸﾄ*	*操作*
TOE 利用者ﾌﾟﾛｾｽ	*監視機能（注）の操作に係るﾒﾆｭｰ* *監視機能（注）の表示に係るﾒﾆｭｰ*	*実行*

注）LiveHelp は除く

[割付: *アクセス制御 SFP*]

— ***コンソール操作制御アクセス制御 SFP***

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御（FDP_ACF.1(2)）

FDP_ACF.1(1) セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1(1)

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

[割付:*示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ*]

- ***下表参照***

[割付: *アクセス制御 SFP*]

- ***ACL マネージャアクセス制御 SFP***

ｻﾌﾞｼﾞｪｸﾄ		***ｾｷｭﾘﾃｨ属性***
TOE 利用者ﾌﾟﾛｾｽ		***ﾛｰﾙ***
ｵﾌﾞｼﾞｪｸﾄ		***ｾｷｭﾘﾃｨ属性***
監視機能	***環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ*** ***操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ*** ***表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ*** ***上記以外の TOE が提供するｺﾏﾝﾄﾞ***	***許可ﾛｰﾙ***
資源配付機能	***環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ*** ***操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ*** ***表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ*** ***上記以外の TOE が提供するｺﾏﾝﾄﾞ***	

FDP_ACF.1.2(1)

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*]

― ***下表の規則のとおり、操作の実行の許可（○印）と拒否（×印）を行う。***

オブジェクト		***サブジェクトのロール***					
		DmAdmin	***DmOperation***	***DmReference***	***DistributionAdmin***	***DistributionOperation***	***DistributionReference***
監視機能	***環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ***	○	×	×	×	×	×
	操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	○	○	×	×	×	×
	表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	○	○	○	×	×	×
	上記以外のTOEが提供するｺﾏﾝﾄﾞ	×	×	×	×	×	×
資源配付機能	***環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ***	×	×	×	○	×	×
	操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	×	×	×	○	○	×
	表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	×	×	×	○	○	○
	上記以外の TOE が提供するｺﾏﾝﾄﾞ	×	×	×	×	×	×

FDP_ACF.1.3(1)

TSF は、以下の追加規則に基づいて、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承認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承認する規則*]。

[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承認する規則*]

― ***以下のとおり***

- ***TOE 利用者プロセスがシステム管理者プロセスの場合、上記の表に示したすべてのメニューとすべてのコマンドの両方について操作の実行を許可する。***

FDP_ACF.1.4(1)

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**

依存性: FDP_ACC.1 サブセットアクセス制御（FDP_ACC.1(1)）
FMT_MSA.3 静的属性初期化（FMT_MSA.3(1)）

FDP_ACF.1(2) セキュリティ属性によるアクセス制御

下位階層: なし

FDP_ACF.1.1(2)

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*]

— ***下表参照***

[割付: *アクセス制御 SFP*]

— ***コンソール操作制御アクセス制御 SFP***

ｻﾌﾞｼﾞｪｸﾄ	対応するｾｷｭﾘﾃｨ属性
TOE 利用者ﾌﾟﾛｾｽ	操作ﾚﾍﾞﾙ
ｵﾌﾞｼﾞｪｸﾄ	対応するｾｷｭﾘﾃｨ属性
監視機能（注）の操作に係るﾒﾆｭｰ 監視機能（注）の表示に係るﾒﾆｭｰ	許可操作ﾚﾍﾞﾙ

注）LiveHelp は除く

FDP_ACF.1.2(2)

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

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

— ***以下の規則のとおり、実行の許可（○印）と拒否（×印）を行う。***

ｵﾌﾞｼﾞｪｸﾄ	*操作ﾚﾍﾞﾙと許可操作ﾚﾍﾞﾙの関係*		
	A > B	*A = B*	*A < B*
操作に係るﾒﾆｭｰ	○	○	×
表示に係るﾒﾆｭｰ	○	○	×

A:操作ﾚﾍﾞﾙ　B:許可操作ﾚﾍﾞﾙ

FDP_ACF.1.3(2)

TSF は、以下の追加規則に基づいて、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承認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承認する規則*]。

[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承認する規則*]

― ***なし***

FDP_ACF.1.4(2)

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***

依存性: FDP_ACC.1 サブセットアクセス制御（FDP_ACC.1(2)）
FMT_MSA.3 静的属性初期化（FMT_MSA.3(2)）

FDP_IFC.1 サブセット情報フロー制御

下位階層: なし

FDP_IFC.1.1

TSF は、[割付：*サブジェクト、情報、及び、SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作*]に対して[割付: *情報フロー制御 SFP*]を実施しなければならない。

[割付: *サブジェクト、情報、及び SFP で扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作*]

- *サブジェクト* ***：通知元の資源配付プロセス***
- *情報* ***：資源の配付・適用結果データ（結果データ）***
- *SFP によって扱われる制御されたサブジェクトに、またはサブジェクトから制御された情報の流れを引き起こす操作* ***：通知先の資源配付プロセスに送る***

[割付: *情報フロー制御 SFP*]

- ***資源配付結果通知データ保護 SFP***

依存性: FDP_IFF.1 単純セキュリティ属性（FDP_IFF.1）

FDP_IFF.1 単純セキュリティ属性

下位階層: なし

FDP_IFF.1.1

TSF は、以下のサブジェクト及び情報のセキュリティ属性の種別に基づいて、[割付：*情報フロー制御 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情報のリスト、及び各々のセキュリティ属性*] 。

[割付: *情報フロー制御 SFP*]

— ***資源配付結果通知データ保護 SFP***

[割付: *示された SFP 下において制御されるサブジェクトと情報のリスト、及び各々のセキュリティ属性*]

示された SFP 下において制御されるｻﾌﾞｼﾞｪｸﾄ	***ｾｷｭﾘﾃｨ属性***
通知元の資源配付ﾌﾟﾛｾｽ	***通知先ｼｽﾃﾑ名***
情報	***ｾｷｭﾘﾃｨ属性***
資源の配付・適用結果ﾃﾞｰﾀ（結果ﾃﾞｰﾀ）	***なし***

FDP_IFF.1.2

TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない：[割付：*各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*] 。

[割付：*各々の操作に対して、サブジェクトと情報のセキュリティ属性間に保持せねばならない、セキュリティ属性に基づく関係*]

— ***以下のとおり***

- ***通知元の資源配付プロセスは、資源の配付と適用を行った際、資源の配付・適用結果データ（結果データ）を、通知先システム名が示す通知先の資源配付プロセスに送る。***

FDP_IFF.1.3

TSF は、[割付：*追加の情報フロー制御 SFP 規則*]を実施しなければならない。

[割付：*追加の情報フロー制御 SFP 規則*]

— ***以下のとおり***

- ***通知元の資源配付プロセスは、そのプロセスが動作するサーバの配下クライアントから通知された結果データについても通知先の資源配付プロセスに送る。***
- ***配下クライアントで動作する通知元の資源配付プロセスは、資源配付を受けたサーバを通知すべきシステムと定め、結果データをそのサーバ上で動作する通知先の資源配付プロセスに送る。***

FDP_IFF.1.4

TSF は、以下の[割付：*追加の SFP 能力のリスト*]を提供しなければならない。

[割付：*追加の SFP 能力のリスト*]

— ***なし***

FDP_IFF.1.5

TSF は、以下の規則に基づいて、情報フローを明示的に承認しなければならない：[割付：*セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]を実施しなければならない。

[割付：*セキュリティ属性に基づいて、明示的に情報フローを承認する規則*]

— ***なし***

FDP_IFF.1.6

TSF は、次の規則に基づいて、情報フロー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、明示的に情報フローを拒否する規則*]。

[割付：*セキュリティ属性に基づいて、明示的に情報フローを拒否する規則*]

— ***なし***

依存性: FDP_IFC.1 サブセット情報フロー制御（FDP_IFC.1）
FMT_MSA.3 静的属性初期化（FMT_MSA.3(3)）

FIA_AFL.1 認証失敗時の取り扱い

下位階層: なし

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: *セキュリティ属性のリスト*]

- ***運用管理クライアントから運用管理サーバへのログイン（Systemwalker コンソール機能利用時）***

[選択：[割付：*正の整数値*]、「[割付：*許容可能な値の範囲*]内における管理者設定可能な正の整数値]」]

- **[割付：*正の整数値*]**

  正の整数値 = 3

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*]

- ***ログイン画面を閉じてログイン処理を終了***

依存性: FIA_UAU.1 認証のタイミング（FIA_UAU.2[ENV](2)）

FIA_ATD.1 利用者属性定義

下位階層: 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[割付：*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*]

- ***ロール、操作レベル***

依存性: なし

FIA_SOS.1 秘密の検証

下位階層: 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*]

- ***パスワード長は7文字以上、半角16文字以内***
- ***大文字、小文字、数字、空白、およびダブルクォーテーション(")を除く特殊文字が使用可能***

依存性: なし

FIA_UAU.2(1) アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1(1)

TSF は、***リモート操作を行う運用担当者***を代行する他の TSF 調停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。

依存性: FIA_UID.1 識別のタイミング（FIA_UID.2(2)）

FIA_UAU.6 再認証

下位階層: 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

[割付: *再認証が要求される条件のリスト*]

- ***コンソール操作制御機能の利用形態の選択情報が、操作の都度ユーザ名を入力する形態に設定されている状態において、コンソール操作制御機能におけるユーザ名の有効期間が切れた場合***

依存性: なし

FIA_UAU.7 保護された認証フィードバック

下位階層: なし

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***リモート操作を行う運用担当者***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*]

- ***入力されたパスワード文字列を“＊”で表示***

依存性: FIA_UAU.1 認証のタイミング（FIA_UAU.2(1)）

FIA_UID.2(1) アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1(1)

TSF は、***システム管理者、運用管理者、または運用担当者***を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

FIA_UID.2(2) アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2.1(2)

TSF は、***リモート操作を行う運用担当者***を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

FIA_USB.1 利用者・サブジェクト結合

下位階層: なし

FIA_USB.1.1

TSF は、次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*]

— ***ロール、操作レベル***

FIA_USB.1.2

TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない: [割付: *属性の最初の関連付けに関する規則*]

[割付: *属性の最初の関連付けに関する規則*]

— ***利用者識別が成功した時点で関連付けを行う***

FIA_USB.1.3

TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない: [割付: *属性の変更に関する規則*]

[割付: *属性の変更に関する規則*]

— ***なし***

依存性: FIA_ATD.1 利用者属性定義（FIA_ATD.1）

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層: なし

FMT_MOF.1.1

TSF は、機能[割付: *機能のリスト*][選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]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: *機能のリスト*]

— ***下表参照***

[選択: *のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する*]

— ***下表参照***

[割付: *許可された識別された役割*]

— ***下表参照***

機能のﾘｽﾄ	*ふるまい*	*許可された識別された役割*
ｺﾝｿｰﾙ操作制御機能	*を停止する* *を動作させる*	*ｼｽﾃﾑ管理者*
適用結果の自動通知機能	*を停止する* *を動作させる*	*ｼｽﾃﾑ管理者、および* *DistributionAdmin ﾛｰﾙをもつ* *運用管理者*
ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能	*を停止させる* *を動作させる*	*ｼｽﾃﾑ管理者*
運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能	*を停止させる* *を動作させる*	*ｼｽﾃﾑ管理者*

依存性: FMT_SMF.1 管理機能の特定（FMT_SMF.1）
FMT_SMR.1 セキュリティ役割（FMT_SMR.1）

FMT_MSA.1(1) セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1(1)

TSF は、セキュリティ属性[割付：*セキュリティ属性のリスト*]に対し[選択：*デフォルト値変更、問い合わせ、改変、削除、*[割付：*その他の操作*]]をする能力を[割付：*許可された識別された役割*]に制限するために[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*]

— ***下表参照***

[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*]]

— ***下表参照***

[割付：*許可された識別された役割*]

— ***下表参照***

[割付：*アクセス制御 SFP、情報フロー制御 SFP*]

— ***ACL マネージャアクセス制御 SFP***

区分	*セキュリティ属性のリスト* *注）セキュリティ属性はロールであり、TOE はACL マネージャアクセス制御 SFP のための ロールとして以下のものを定義する。*	*能力*	*許可された識別された役割*		
			システム管理者	*DmAdmin ロールを もつ運用管理者*	*Distribution Admin ロールをもつ 運用管理者*
サブジェクト	*ロール（DmAdmin）*	*登録、削除*	○	○	×
	ロール（DmOperation、DmReference）		○	○	×
	ロール（DistributionAdmin）		○	×	○
	ロール（DistributionOperation、DistributionReference）		○	×	○

○：能力がある　×：能力がない

依存性: FDP_ACC.1　サブセットアクセス制御（FDP_ACC.1(1)）
FMT_SMF.1　管理機能の特定（FMT_SMF.1）
FMT_SMR.1　セキュリティ役割（FMT_SMR.1）

FMT_MSA.1(2) セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1(2)

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*]に制限するために[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*]

— ***下表参照***

[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*]]

— ***下表参照***

[割付：*許可された識別された役割*]

— ***下表参照***

区分	*ｾｷｭﾘﾃｨ属性*	*能力*	*許可された識別された役割*
ｻﾌﾞｼﾞｪｸﾄ	*操作ﾚﾍﾞﾙ*	*登録、削除*	*ｼｽﾃﾑ管理者*
ｵﾌﾞｼﾞｪｸﾄ	*許可操作ﾚﾍﾞﾙ*	*登録、削除*	*ｼｽﾃﾑ管理者*

[割付：*アクセス制御 SFP、情報フロー制御 SFP*]

— ***コンソール操作制御アクセス制御 SFP***

依存性: FDP_ACC.1 サブセットアクセス制御（FDP_ACC.1(2)）
FMT_SMF.1 管理機能の特定（FMT_SMF.1）
FMT_SMR.1 セキュリティ役割（FMT_SMR.1）

FMT_MSA.1(3) セキュリティ属性の管理

下位階層: なし

FMT_MSA.1.1(3)

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*]に制限するために[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*]

- ***通知先システム名***

[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*]]

- ***改変、削除、[割付：その他の操作]***
  その他の操作 = 登録

[割付：*許可された識別された役割*]

- ***システム管理者、および DistributionAdmin ロールをもつ運用管理者***

[割付：*アクセス制御 SFP、情報フロー制御 SFP*]

- ***資源配付結果通知データ保護 SFP***

依存性: FDP_IFC.1 サブセット情報フロー制御（FDP_IFC.1）
FMT_SMF.1 管理機能の特定（FMT_SMF.1）
FMT_SMR.1 セキュリティ役割（FMT_SMR.1）

FMT_MSA.3(1) 静的属性初期化

下位階層: なし

FMT_MSA.3.1(1)

TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択：*制限的、許可的：から一つのみ選択、[割付：その他の特性]*]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：から一つのみ選択、[割付：その他の特性]*]

- ***制限的***

[割付: *アクセス制御 SFP、情報フローSFP*]

- ***ACL マネージャアクセス制御 SFP***

FMT_MSA.3.2(1)

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指定することを許可しなければならない。

[割付：*許可された識別された役割*]

- ***なし***

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

FMT_MSA.3(2) 静的属性初期化

下位階層: なし

FMT_MSA.3.1(2)

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として、[選択：*制限的、許可的：から一つのみ選択、[割付：その他の特性]*]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：から一つのみ選択、[割付：その他の特性]*]

- ***制限的***

[割付: *アクセス制御 SFP、情報フローSFP*]

- ***コンソール操作制御アクセス制御 SFP***

FMT_MSA.3.2(2)

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

[割付：*許可された識別された役割*]

- ***なし***

依存性: FMT_MSA.1 セキュリティ属性の管理（FMT_MSA.1(2)）
FMT_SMR.1 セキュリティの役割

FMT_MSA.3(3) 静的属性初期化

下位階層: なし

FMT_MSA.3.1(3)

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として、[選択：*制限的、許可的：から一つのみ選択、[割付：その他の特性]*]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：から一つのみ選択、[割付：その他の特性]*]

- ***制限的***

[割付: *アクセス制御 SFP、情報フローSFP*]

- ***資源配付結果通知データ保護 SFP***

FMT_MSA.3.2(3)

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指定することを許可しなければならない。

[割付：*許可された識別された役割*]

- ***なし***

依存性: FMT_MSA.1 セキュリティ属性の管理（FMT_MSA.1(3)）
FMT_SMR.1 セキュリティの役割

FMT_MTD.1 TSF データの管理

下位階層: なし

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*]

— ***下表参照***

[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*]]

— ***下表参照***

[割付：*許可された識別された役割*]

— ***下表参照***

TSFデータ	*操作*	*許可された識別された役割*
運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能における監査ﾛｸﾞﾌｧｲﾙの保存日数	***改変***	***ｼｽﾃﾑ管理者***
ｺﾝｿｰﾙ操作制御機能の利用形態の選択情報	***改変***	***ｼｽﾃﾑ管理者***
ｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間	***改変***	***ｼｽﾃﾑ管理者***

依存性: FMT_SMF.1　管理機能の特定（FMT_SMF.1）
FMT_SMR.1　セキュリティの役割（FMT_SMR.1）

FMT_SMF.1 管理機能の特定

下位階層: なし

FMT_SMF.1.1

TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]。

[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]

― ***以下のとおり***

機能要件	CC で定義された管理対象 （FMT における管理機能と考えられるｱｸｼｮﾝ）	TSF が提供するｾｷｭﾘﾃｨ管理機能
FAU_GEN.1(1)	なし。	―
FAU_GEN.1(2)	なし。	―
FAU_SAR.1	a) 監査記録に対して読み出し権のある利用者ｸﾞﾙｰﾌﾟの維持（削除、改変、追加）。	a) なし（読み出し権のある利用者ｸﾞﾙｰﾌﾟは固定のため）
FAU_STG.1	なし。	―
FAU_STG.3	a) 閾値の維持 b) 監査格納失敗が切迫したときにとられるｱｸｼｮﾝの維持（削除、改変、追加）。	a) 運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能における監査ﾛｸﾞﾌｧｲﾙの保存日数の管理機能 b) なし（ｱｸｼｮﾝは固定のため）
FAU_STG.4	a) 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）	a) なし（ｱｸｼｮﾝは固定のため）
FDP_ACC.1(1)(2)	なし。	―
FDP_ACF.1(1)	a) 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。	a) ｻﾌﾞｼﾞｪｸﾄがもつｱｸｾｽ制御に係る属性（ﾛｰﾙ）の維持管理機能
FDP_ACF.1(2)	a) 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。	a) ｻﾌﾞｼﾞｪｸﾄ及びｵﾌﾞｼﾞｪｸﾄがもつｱｸｾｽ制御に係る属性（操作ﾚﾍﾞﾙ、許可操作ﾚﾍﾞﾙ）の維持管理機能
FDP_IFC.1	なし。	―
FDP_IFF.1	a) 明示的なｱｸｾｽに基づく決定に使われる属性の管理。	a) ｻﾌﾞｼﾞｪｸﾄ間の情報ﾌﾛｰ制御に係る属性（通知先ｼｽﾃﾑ名）の維持管理機能
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるｱｸｼｮﾝの管理	a) なし（閾値は固定のため） b) なし（ｱｸｼｮﾝは固定のため）

機能要件	CC で定義された管理対象 （FMT における管理機能と考えられるｱｸｼｮﾝ）	TSF が提供するｾｷｭﾘﾃｨ管理機能
FIA_ATD.1	a) 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。	a) なし（許可管理者が定義する追加のｾｷｭﾘﾃｨ属性はないため）
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理。	a) なし（尺度の管理は運用依存（OE.LIVEHELP_PWD）のため）
FIA_UAU.2(1)	a) 管理者による認証ﾃﾞｰﾀの管理; b) このﾃﾞｰﾀに関係する利用者による認証ﾃﾞｰﾀの管理。	a) なし（管理者による認証ﾃﾞｰﾀの管理は運用依存（OE.CLIENT_SETUP および OE.LIVEHELP_PWD）のため） b) なし（同上）
FIA_UAU.6	a) 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	a) ﾕｰｻﾞ名に関するｺﾝｿｰﾙ操作制御機能の利用形態の管理機能、および再認証の決定に使用されるﾕｰｻﾞ名の有効期間の管理機能
FIA_UAU.7	なし。	－
FIA_UID.2(1)	a) 利用者識別情報の管理。	a) なし（識別認証は OS に依存しているため）
FIA_UID.2(2)	a) 利用者識別情報の管理。	a) なし（利用者識別情報の管理は運用依存（OE.CLIENT_SETUP および OE.LIVEHELP_PWD）のため）
FIA_USB.1	a) 許可管理者は、ﾃﾞﾌｫﾙﾄのｻﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性を定義できる。 b) 許可管理者は、ﾃﾞﾌｫﾙﾄのｻﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性を変更できる。	a) なし（ﾃﾞﾌｫﾙﾄのｻﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性はないため） b) 同上
FMT_MOF.1	a) TSF の機能と相互に影響をおよぼし得る役割のｸﾞﾙｰﾌﾟを管理すること。	a) なし（該当する役割のｸﾞﾙｰﾌﾟは固定のため） b) ｺﾝｿｰﾙ操作制御機能、適用結果の自動通知機能、ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能、および運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能各々において、その起動と停止を行う機能（注）
FMT_MSA.1(1)	a) ｾｷｭﾘﾃｨ属性と相互に影響を及ぼし得る役割のｸﾞﾙｰﾌﾟを管理すること。	a) なし（該当する役割のｸﾞﾙｰﾌﾟは固定のため）
FMT_MSA.1(2)	a) ｾｷｭﾘﾃｨ属性と相互に影響を及ぼし得る役割のｸﾞﾙｰﾌﾟを管理すること。	a) なし（該当する役割のｸﾞﾙｰﾌﾟは固定のため）
FMT_MSA.1(3)	a) ｾｷｭﾘﾃｨ属性と相互に影響を及ぼし得る役割のｸﾞﾙｰﾌﾟを管理すること。	a) なし（該当する役割のｸﾞﾙｰﾌﾟは固定のため）

機能要件	CC で定義された管理対象 （FMT における管理機能と考えられるｱｸｼｮﾝ）	TSF が提供するｾｷｭﾘﾃｨ管理機能
FMT_MSA.3(1)	a) 初期値を特定できる役割のｸﾞﾙｰﾌﾟを管理すること b) 所定のｱｸｾｽ制御 SFP に対するﾃﾞ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	a) なし（初期値を特定できる役割はないため） b) なし（許可的あるいは制限的設定は TOE で固定のため）
FMT_MSA.3(2)	a) 初期値を特定できる役割のｸﾞﾙｰﾌﾟを管理すること b) 所定のｱｸｾｽ制御 SFP に対するﾃﾞ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	a) なし（初期値を特定できる役割はないため） b) なし（ｱｸｾｽ制御 SFP に係る定義にはﾃﾞﾌｫﾙﾄ値がないため）
FMT_MSA.3(3)	a) 初期値を特定できる役割のｸﾞﾙｰﾌﾟを管理すること b) 所定のｱｸｾｽ制御 SFP に対するﾃﾞ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	a) なし（初期値を特定できる役割はないため） b) なし（情報ﾌﾛｰ制御 SFP に係る定義にはﾃﾞﾌｫﾙﾄ値がないため）
FMT_MTD.1	a) TSF ﾃﾞｰﾀと相互に影響を及ぼし得る役割のｸﾞﾙｰﾌﾟを管理すること。	a) なし（該当する役割のｸﾞﾙｰﾌﾟは固定のため）
FMT_SMF.1	なし。	－
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	a) なし（役割の一部をなす利用者のｸﾞﾙｰﾌﾟは固定のため）
FPT_ITT.1(1)	a) TSF が保護すべき改変の種別の管理: b) TSF の異なるﾊﾟｰﾂ間の転送中にﾃﾞｰﾀ保護を提供するために使われるﾒｶﾆｽﾞﾑの管理	a) なし（暴露からの保護であり、改変はないため） b) なし（ﾒｶﾆｽﾞﾑは固定のため）
FPT_RVM.1	なし。	－
FPT_SEP.1	なし。	－

注) これらはFMT_MOF.1のための管理機能ではないが、その対象は複数の機能要件に跨ることから、煩雑にならないよう、ここにまとめて記述する。

依存性: なし

FMT_SMR.1 セキュリティ役割

下位階層: なし

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*]

- ***システム管理者、運用管理者***

FMT_SMR.1.2

TSF は、利用者を役割に関連付けなければならない。

依存性: FIA_UID.1 識別のタイミング（FIA_UID.2(1)）

FPT_ITT.1(1) 基本 TSF 内データ転送保護

下位階層: なし

FPT_ITT.1.1(1)

TSF は、***サーバ上の TOE にログインするためのパスワード***が TOE の別々のパーツ間で送られる場合、***サーバ上の TOE にログインするためのパスワード***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***

依存性: なし

FPT_RVM.1 TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1

TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性: なし

FPT_SEP.1 TSF ドメイン分離

下位階層: なし

FPT_SEP.1.1

TSF は、その自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2

TSF は、TSC 内でサブジェクトのセキュリティドメインの分離を実施しなければならない。

依存性: なし

5.1.2. TOE セキュリティ保証要件

本 TOE に対して、本 ST が要求する保証レベルは EAL1 である。

表 5.1 に、EAL1 に対する保証コンポーネント一覧を示す。要求する各保証コンポーネントの保証エレメントは CC パート 3 の要求どおりである。なお、ASE クラスは保証レベルに関わらず必須となる保証要件として採用する。

表 5.1　保証要件一覧

TOE セキュリティ保証要件		コンポーネント
構成管理	バージョン番号	ACM_CAP.1
配付と運用	設置、生成及び立上げ手順	ADO_IGS.1
開発	機能仕様	ADV_FSP.1
	表現対応	ADV_RCR.1
ガイダンス文書	管理者ガイダンス	AGD_ADM.1
	利用者ガイダンス	AGD_USR.1
テスト	独立テスト	ATE_IND.1

5.1.3. TOE セキュリティ機能強度

本 ST が要求する TOE の保証レベルは EAL1 であり、保証要件に AVA_SOF.1 を含まないことから、セキュリティ機能強度は主張しない。

5.2. IT 環境に対するセキュリティ機能要件

本 TOE が関係する IT 環境のセキュリティ機能要件として、以下のものを定義する。

FAU_GEN.1[ENV](3) 監査データ生成

下位階層: なし

FAU_GEN.1.1[ENV](3)

運用管理クライアントの OS 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：

a) ***運用管理クライアント操作の監査ログ機能***の起動と停止。

FAU_GEN.1.2[ENV](3)

運用管理クライアントの OS 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：

a) 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（成功又は失敗）；及び

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

[割付：*その他の監査関連情報*]

― ***なし***

依存性: FPT_STM.1 高信頼タイムスタンプ（FPT_STM.1[ENV]）

FIA_UAU.2[ENV](2) アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2[ENV](2)

運用管理サーバ、業務サーバ、部門管理サーバ、業務クライアントおよび運用管理クライアントの OS は、その利用者を代行する他の TSF 調停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。

依存性: FIA_UID.1 識別のタイミング (FIA_UID.2[ENV](3))

FIA_UID.2[ENV](3) アクション前の利用者識別

下位階層: FIA_UID.1

FIA_UID.2[ENV](3)

運用管理サーバ、業務サーバ、部門管理サーバ、業務クライアントおよび運用管理クライアントの OS は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性: なし

FPT_ITT.1[ENV](2) 基本 TSF 内データ転送保護

下位階層: なし

FPT_ITT.1.1[ENV](2)

運用管理クライアントおよび LiveHelp クライアントの OS は、***リモート操作時のログイン・パスワード***が TOE の別々のパーツ間で送られる場合、***リモート操作時のログイン・パスワード***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***

依存性: なし

FPT_STM.1[ENV] 高信頼タイムスタンプ

下位階層: なし

FPT_STM.1.1[ENV]

運用管理クライアント、運用管理サーバ、部門管理サーバおよび業務サーバの OS は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性: なし

6. TOE 要約仕様

本章では、本 TOE のセキュリティ機能の要約仕様を記述する。

6.1. TOE セキュリティ機能

本節では、TOE のセキュリティ機能を説明する。表 6.1 に示したとおり、本節で説明するセキュリティ機能は、“第 5 章 TOE セキュリティ機能要件”に示したセキュリティ機能要件を満たす。

なお、表中の略称の意味は次のとおり（括弧内はセキュリティ機能名）であり、本章以降では、当略称を必要に応じて使用する。

F.ACL_SECURITY（ACL マネージャ機能）

F.CONSOLE_SECURITY（コンソール操作制御機能）

F.LIVEHELP_SECURITY（LIVEHELP 接続認証機能）

F.AUDIT_ACL（ACL マネージャ機能の監査ログ機能）

F.AUDIT_CMGR/CL(M)（運用管理クライアント操作の監査ログ機能）

F.DEPLOY_SECURITY（適用結果の自動通知機能）

F.PWD_SECURITY（サーバ上の TOE にログインするためのパスワードの保護機能）

表 6.1　TOE のセキュリティ機能とセキュリティ機能要件の対応

セキュリティ機能 / セキュリティ機能要件	F.ACL_SECURITY	F.CONSOLE_SECURITY	F.LIVEHELP_SECURITY	F.AUDIT_ACL	F.AUDIT_CMGR/CL(M)	F.DEPLOY_SECURITY	F.PWD_SECURITY
FAU_GEN.1(1)				✓			
FAU_GEN.1(2)					✓		
FAU_SAR.1				✓	✓		
FAU_STG.1				✓	✓		
FAU_STG.3					✓		
FAU_STG.4				✓			
FDP_ACC.1(1)	✓						
FDP_ACC.1(2)		✓					
FDP_ACF.1(1)	✓						
FDP_ACF.1(2)		✓					
FDP_IFC.1						✓	
FDP_IFF.1						✓	
FIA_AFL.1	✓						
FIA_ATD.1	✓	✓					
FIA_SOS.1			✓				
FIA_UAU.2(1)			✓				
FIA_UAU.6	✓	✓					
FIA_UAU.7			✓				
FIA_UID.2(1)	✓						
FIA_UID.2(2)			✓				
FIA_USB.1	✓	✓					
FMT_MOF.1		✓		✓	✓	✓	
FMT_MSA.1(1)	✓						
FMT_MSA.1(2)		✓					
FMT_MSA.1(3)						✓	
FMT_MSA.3(1)	✓						
FMT_MSA.3(2)		✓					

セキュリティ機能 / セキュリティ機能要件	F.ACL_SECURITY	F.CONSOLE_SECURITY	F.LIVEHELP_SECURITY	F.AUDIT_ACL	F.AUDIT_CMGR/CL(M)	F.DEPLOY_SECURITY	F.PWD_SECURITY
FMT_MSA.3(3)						✓	
FMT_MTD.1		✓			✓		
FMT_SAE.1		✓					
FMT_SMF.1	✓	✓		✓	✓	✓	
FMT_SMR.1	✓	✓		✓	✓	✓	
FPT_ITT.1(1)							✓
FPT_RVM.1	✓	✓	✓	✓	✓	✓	✓
FPT_SEP.1	✓	✓	✓	✓	✓	✓	✓

6.1.1. ACL マネージャ機能（F.ACL_SECURITY）

ACL マネージャ機能は、本 TOE の利用者に対して、システム管理者、運用管理者、および運用担当者の識別と、その識別結果に応じた運用管理クライアントからの操作に対するアクセス制御機能を提供する。また、CMGR/MGR、CMGR/Agent(S)および CMGR/Agent(J)が提供するコマンドを使用した操作についても同様にアクセス制御を行う。

当機能は必ず動作する機能であり、LiveHelp を除く運用管理機能の利用に先立ち、それら機能の利用者を識別する。LiveHelp については、“6.1.3 LiveHelp 接続認証機能”で示した識別認証機能を使用する。

1) 主な定義情報とその管理

当機能は、運用管理クライアントからのメニューによる操作、およびコマンドを使った操作に対して、ロールによるアクセス制御を行う。使用するロールは TOE で固定（表 2.2 参照）であり、追加や削除を行うことはできない。

利用者のロールについては、その登録と削除の操作を行える者をシステム管理者および運用管理者とする。詳細は以下のとおり。

- DmAdmin ロールをもつ運用管理者は、DmAdmin、DmOperation および DmReference 各ロールの登録と削除が行える。
- DistributionAdmin ロールをもつ運用管理者は、DistributionAdmin、DistributionOperation および DistributionReference 各ロールの登録と削除

が行える。

・　システム管理者はすべてのロールの登録と削除が行える。

割り当てたロールとユーザ名の実際の関係付けは、次項に示す利用者の識別が完了した時点で行う。関係付けたロールの変更は行えない。

メニューとコマンドのロール（許可ロール）については、TOE で固定であり、必要とされる登録と削除の操作はない。

2) 利用者の識別と権限の付与

当機能は OS 機能を使って識別認証を行い、その結果からシステム管理者を識別する。運用管理者および運用担当者については、登録されたロールにより識別を行う。ロールが登録されていない場合、本 TOE はログイン要求を拒否する。この処理は、F.CONSOLE_SECURITY において再認証が要求された場合にも動作する。

なお、運用管理クライアントから運用管理サーバにログイン（Systemwalker ｺﾝｿｰﾙ機能利用時）する場合に限って、OS による識別認証が続けて 3 回失敗した場合、当機能はいったんログイン画面を閉じることで不正に認証試行が繰り返されることを防ぐ。

3) ロールによるアクセス制御

当機能は、運用管理クライアントからのメニューによる操作、およびコマンドを使った操作に対して、利用者のロールと一致する許可ロールをもつメニューおよびコマンドのみ操作を許可（メニューについては許可されないものをグレーアウト）する。表 6.2 は、主な操作内容と必要な利用者のロールを示したものである。許可ロールは TOE で固定であることから、例えば、利用者のロールが DmOperation の場合、監視機能の操作と表示に係るメニューすべてが使用可能となる。その一部を制限することはできない。コマンドについても同様であり、一部を制限することはできない。

システム管理者については、表 6.2 に示したすべてのメニューとすべてのコマンドの両方を操作できる。

4) 必要な役割と能力

当機能に必要な許可された識別された役割には、システム管理者、DmAdmin ロールをもつ運用管理者、および DistributionAdmin ロールをもつ運用管理者がある。当機能は、利用者の識別結果を基に、これら役割と利用者との関連付けを行う。関連付けた役割に対しては、1)項に示したとおり操作を許可する。

表 6.2　主な操作内容とロールの関係

機能	操作内容の体系		必要なﾛｰﾙ（注 3）
監視	環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ（注 1）	・ 監視ﾂﾘｰの作成、削除 ・ 監視対象ｵﾌﾞｼﾞｪｸﾄの追加、削除 ・ ｲﾍﾞﾝﾄに対するｱｸｼｮﾝの設定 ・ 運用ﾎﾟﾘｼｰの定義など	DmAdmin
	操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	・ ﾘﾓｰﾄｺﾏﾝﾄﾞの発行など	DmOperation
	表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	・ 監視ﾂﾘｰの表示 ・ 監視対象ｵﾌﾞｼﾞｪｸﾄの状態表示 ・ ｲﾍﾞﾝﾄの一覧検索、表示 ・ 設定内容、定義内容の表示など	DmReference
	上記以外の TOE が提供するｺﾏﾝﾄﾞ		（注 4）
資源配付	環境設定に係るﾒﾆｭｰとｺﾏﾝﾄﾞ（注 2）	・ 配付ﾙｰﾄの登録、変更 ・ 資源配付先の追加、削除など	DistributionAdmin
	操作に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	・ 配付資源の登録 ・ 資源配付の実行など	DistributionOperation
	表示に係るﾒﾆｭｰとｺﾏﾝﾄﾞ	・ 資源配付状態の表示 ・ 配付ﾙｰﾄの表示など	DistributionReference
	上記以外の TOE が提供するｺﾏﾝﾄﾞ		（注 4）

注1）対象となる定義情報は、事象監視、復旧操作およびﾛｸﾞ収集のための定義情報である。

注2）対象となる定義情報は、資源配付のための定義情報である。

注3）DmOperation は DmReference の権限を包含し、DmAdmin は DmOperation の権限を包含する。同様に、DistributionOperation は DistributionReference の権限を包含し、DistributionAdmin は DistributionOperation の権限を包含する。また、ｼｽﾃﾑ管理者はすべてのﾛｰﾙをもつと見なされる。

注4）これらｺﾏﾝﾄﾞはｼｽﾃﾑ管理者のみが操作できる。

6.1.2. コンソール操作制御機能（F.CONSOLE_SECURITY）

コンソール操作制御機能は、ロールによって決まる運用管理クライアントからの操作について、運用担当者毎さらに細かく制御できるようにするため、メニュー単位でのアクセス制御機能を提供する。対象となる操作は、資源配付および LiveHelp を除く運用管理機能の操作である。

当機能を使用する場合は、以下に示すコンソール操作制御条件ファイルで当機能を有効にする設定を行う。これが有効と設定された場合、当機能は本 TOE の起動時に必ず動作し、

TOE が停止するまで有効である。コンソール操作制御条件ファイルのデフォルトはない。

1) 主な定義情報とその管理

当機能は、アクセス制御のための属性として操作レベルを使用する。利用者に対する操作レベルは、その者が操作できるレベルであり、メニューに対する操作レベルは、各々のメニューが操作を許可するレベル（許可操作レベル）である。図 6.1 に、操作レベルを定義するためのコンソール操作制御条件ファイルを示す。

- 図中(1)はユーザ名をグループ化する定義である。USER-A、USER-B および USER-C はユーザ名を表し、グループ 1 およびグループ 2 はグループ名を表す。ここで定義するユーザ名には、F.ACL_SECURITY により、DmAdmin、DmOperation、DmReference のどれかのロールが登録されている必要がある。
- 図中(2)はメニュー毎に操作レベル（許可操作レベル）を定義する情報である。
- 図中(3)は操作レベルを運用形態に応じてグループ分けする情報である。NORMAL、SPECIAL はグループに割当てた名前である。ここで指定した操作レベルが利用者に対する操作レベルである。
- 図中(4)はユーザのグループと操作レベルのグループを関連付ける情報である。この中の業務サーバ S1 および業務サーバ S2 は操作対象の業務サーバを表す。

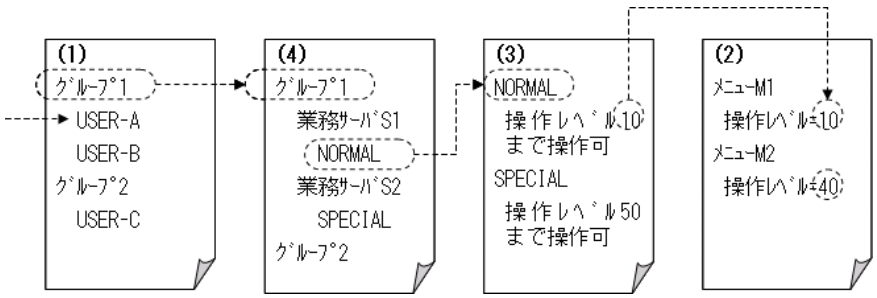

図 6.1　コンソール操作制御条件ファイル

図中の破線の矢印は、ユーザ名を起点とした定義情報の関連を示す。この図の場合、USER-A の利用者は、業務サーバ S1 に対してメニューM1 が使用でき、業務サーバ S2 に対してメニューM1 と M2 が使用できる（USER-B の利用者も同様）。

このコンソール操作制御条件ファイルによる操作レベルの登録と削除を行える者はシステム管理者である。

ここで定義した操作レベルとユーザ名の実際の関係付けは、F.ACL_SECURITY による利用者の識別が完了した時点で行う。関係付けた操作レベルの変更は行えない。

2) メニュー単位でのアクセス制御

当機能を利用する場合、次の二つの利用形態を選択できる。この選択を行える者はシステム管理者である。

・ 運用管理クライアントにログインした時のユーザ名を使って制限する形態
・ 操作の都度ユーザ名を入力させ、そのユーザ名を使って制限する形態

前者は運用管理クライアント毎に専任の者を配置する運用を行う場合であり、当機能はログイン時のユーザ名に登録された操作レベルを使って、その操作レベルに等しいか、それ以下の操作レベルをもつメニューのみ操作を許可する。後者は一台の運用管理クライアントを複数の者が操作する場合であり、運用管理クライアントで操作を行う都度、当機能はユーザ名とパスワードを要求するダイアログを表示する。そして、入力されたユーザ名とパスワードを使って識別認証（F.ACL_SECURITY 機能を利用）を行ったのち、そのユーザ名に登録された操作レベルを使って、上記と同様にアクセス制御を行う。ただし、どちらの場合も、操作可能な範囲はユーザ名に登録されたロールで制限される。

3) ユーザ名の有効期間の制御

当機能は、前項に示した操作の都度ユーザ名を入力させる運用の場合、入力されたユーザ名を保護するため、ユーザ名に有効期間を設定できるようにし、有効期間が切れた場合には利用者に再認証を要求する。有効期間の設定を行える者はシステム管理者であり、以下の中から選んで設定できる。

① 毎回ユーザ名を無効にする（操作の都度ユーザ名の入力が必要）
② ユーザ名を入力した利用者がそのユーザ名を無効にするまで有効とする
③ 指定時間が経過した時点でユーザ名を無効にする。

また、有効期間を判定するための日付時刻は OS から取得する。

4) 必要な役割と能力

当機能に必要な許可された識別された役割には、システム管理者がある。当機能は、F.ACL_SECURITY による利用者の識別結果を基に、この役割と利用者との関連付けを行う。関連付けた役割に対しては、1)から 3)項に示したとおり操作を許可する。

6.1.3. LiveHelp 接続認証機能（F.LIVEHELP_SECURITY）

LiveHelp 接続認証機能は、LiveHelp クライアントで動作し、LiveHelp クライアントをリモート操作する運用担当者を識別認証する。

当機能は識別認証に必要な定義情報の設定が行なわれた場合、必ず動作する。

1) 主な定義情報とその管理

当機能を有効にする場合は、LiveHelp クライアントに対して、認証方式と必要情報を定義する。パスワード認証方式を使用する場合は、パスワードを定義する。OS 認証方式を使用する場合は、LiveHelp クライアントの OS に対してユーザ名とパスワードを登録する。なお、これら定義操作は一般利用者が行えるため、LiveHelp クライアントの中の業務クライアントについては、 ”4.2 環境のセキュリティ対策方針 ”に示した

とおり、システム管理者のみが設定できる運用にする必要がある。

2) 接続要求に対する利用者の識別認証

リモート操作を行う運用担当者は、事前に通知されたパスワード(パスワード認証方式の場合)またはユーザ名とパスワード（OS 認証方式の場合）を使って、運用管理クライアントから対象とする LiveHelp クライアントにログインする。当機能は指定されたユーザ名やパスワードが定義されているものと一致した場合、ログインを受け入れ、それ以外の場合はログインを拒否する。

また、パスワード認証方式におけるパスワードの扱いは、以下のとおりである。

- パスワードは 7 文字以上、半角 16 文字以内であり、大文字、小文字、数字、空白、およびダブルクォーテーション(“)を除く特殊文字が使用できる。
- 入力されたパスワード文字列は”＊”で置き換えて表示することで保護する。

3) 必要な役割と能力

当機能には必要とする許可された識別された役割はない。

6.1.4. ACL マネージャ機能の監査ログ機能（F.AUDIT_ACL）

ACL マネージャ機能の監査ログ機能は、ACL マネージャ機能によるシステム管理者、運用管理者、運用担当者の識別認証処理、およびコマンドに対するロールによるアクセス制御処理に係る監査ログを採取する機能を提供する。当機能は監査ログの採取が指示された場合、必ず動作する。

1) 監査対象事象と採取情報

当機能が対象とする監査事象は以下のとおりである。

- 当機能の起動と終了事象
- 運用管理クライアントに対する利用者の識別認証および再認証事象（OS の識別認証の結果を本 TOE で監査ログとして採取）
- ロールに対してユーザの登録および削除を実行した事象
- ロールで許可されたコマンドを実行した事象（メニューを実行した場合の事象は F.AUDIT_CMGR/CL(M)で採取）

また、監査ログに記録する情報は以下のとおりである。

- 監査ログを記録した日付／時刻（秒単位の日付／時刻を OS から取得）
- 監査ログ採取の契機となった操作を行ったユーザ名
- 行った操作内容
- 実行結果（成功または失敗）
- 操作を行った運用管理クライアントのホスト名など

2) 監査ログの格納管理

当機能は監査ログを CSV 形式で監査ログファイルに記録する。監査ログファイルは、

監査事象の発生時に監査ログを記録する 1 つのログファイルと、そのファイルの内容を退避するための 10 個のバックアップファイルから成る。前者のログファイルが満杯になった場合、その内容をバックアップファイルへ自動退避し、監査ログの記録を継続する。バックアップファイルを使いきった場合には、最も古く退避されたバックアップファイルへの上書き退避を行い、以降サイクリックに使用する。

また、不正な改ざんや削除から監査ログを保護するため、当機能は上記の監査ログファイルとバックアップファイルに対するパーミッションの設定を行う。

3) 管理機能

当機能の起動と終了、監査事象の設定変更、およびログの出力先ディレクトリの変更の各機能がある。出力先変更時は、監査ログの不正な改ざんや削除を防止するため、出力先を変更するコマンドの中で変更先に対するパーミッションの設定を行う。これら管理機能を使用できる者はシステム管理者である。

4) 監査ログによる監査

採取した監査ログはシステム管理者のみが利用できる。監査ツールとしては流通する市販のソフト等を使用する。

5) 必要な役割と能力

当機能が必要とする許可された識別された役割には、システム管理者がある。当機能は、利用者に関連付けたこの役割に対して、3)および 4)項に示したとおり操作を許可する。

6.1.5. 運用管理クライアント操作の監査ログ機能（F.AUDIT_CMGR/CL(M)）

運用管理クライアント操作の監査ログ機能は、運用管理クライアントからの操作に係る監査ログを採取する機能を提供する。当機能は監査ログの採取が指示された場合、必ず動作する。

1) 監査対象事象

当機能が対象とする監査事象は以下のとおりである。監査機能の起動・終了についてのログは、運用管理クライアントのイベントログに出力されるログで代替する。

- ロールで許可されたメニューを実行した事象
- コンソール操作制御機能で定義されたメニューを実行した事象
- 不成功のログイン操作に対する閾値到達とログイン画面を閉じた事象
- LiveHelp の識別認証事象
- 資源配付に対して設定変更を行った事象など

また、監査ログに記録する情報は以下のとおりである。

- 監査ログを記録した日付／時刻（ミリ秒単位の日付／時刻を OS から取得）
- 監査ログ採取の契機となった操作を行ったユーザ名

・ 行った操作内容
・ 実行結果（成功または失敗）
・ 操作を行った運用管理クライアントのホスト名など

2) 監査ログの格納管理

当機能は日単位で監査ログファイルを作成し、監査ログを CSV 形式で記録する。そして、その監査ログファイルに保存日数を指定し、保存日数が過ぎた監査ログファイルを自動削除することで連続した監査ログ採取を行う。

また、不正な改ざんや削除から監査ログを保護するため、当機能は上記の監査ログファイルに対するパーミッションの設定を行う。

3) 管理機能

当機能の起動と終了、ログの出力先ディレクトリの変更、および監査ログファイルの保存日数の変更の各機能がある。出力先変更時は、監査ログの不正な改ざんや削除を防止するため、出力先を変更するコマンドの中で変更先に対するパーミッションの設定を行う。これら機能を使用できる者はシステム管理者である。

4) 監査ログによる監査

採取した監査ログはシステム管理者のみが利用できる。監査ツールとしては流通する市販のソフト等を使用する。

5) 必要な役割と能力

当機能が必要とする許可された識別された役割には、システム管理者がある。当機能は、利用者に関連付けたこの役割に対して、3)および 4)項に示したとおり操作を許可する。

6.1.6. 適用結果の自動通知機能（F.DEPLOY_SECURITY）

適用結果の自動通知機能は、本 TOE の資源配付機能を構成する機能要素の一つであり、CMGR/MGR、CMGR/Agent(J)、CMGR/Agent(S)および CMGR/CL(U)で動作する。配付された資源について、その配付結果および適用結果を以下のとおり上位のシステムに自動通知することで、運用管理クライアントから配付資源の適用状況を確実に把握できるようにする。

・ 業務クライアントの CMGR/CL(U)は、資源のダウンロードを行った業務サーバの CMGR/Agent(J)または部門管理サーバの CMGR/Agent(S)に自動通知する
・ CMGR/Agent(J)または CMGR/Agent(S)は、通知先システムとして定義された運用管理サーバの CMGR/MGR に自動通知する。その際、配下クライアントの適用結果についても同時に通知する。

1) 主な定義情報とその管理

当機能を使用する場合、CMGR/Agent(J)および CMGR/Agent(S)に対して、通知先システムの定義を行う。この定義を行える者は、システム管理者および DistributionAdmin

ロールをもつ運用管理者である。

当機能の有効／無効はこの定義の有無で決まる。この定義が行なわれた場合、当機能は該当する業務サーバまたは部門管理サーバで必ず動作する。

2) 必要な役割と能力

当機能に必要な役割には、システム管理者、および DistributionAdmin ロールをもつ運用管理者がある。当機能は、利用者に関連付けたこれらの役割に対して、1)項に示したとおり操作を許可する。

6.1.7. サーバ上の TOE にログインするためのパスワードの保護機能（F.PWD_SECURITY）

当機能は、CMGR/CL(M)または CMGR/CL(U)を使って CMGR/MGR、CMGR/Agent(S)および CMGR/Agent(J)にログインする際のパスワードについて、入力されたパスワードが解読されないよう、送信に際して、パスワードデータを本 TOE 独自のメカニズムにより異なるデータに変換および元のデータに復元する機能を提供する。当機能に対する設定等の管理機能はない。必要とする許可された識別された役割もない。当機能は必ず動作する。

6.2. TSF ドメイン分離の確保

本 TOE は、前述のセキュリティ機能に対する信頼されないサブジェクトからの分離を確実にするため、サブジェクトに与える役割を定義し、サブジェクトに対して提供するインタフェースに含まれるコマンド、オペランド、オペランド値などそれぞれに対して、その使用が許可されるサブジェクトの役割を明確化することで、不正な干渉や改ざんにつながるインタフェースが実装されないようにする。さらに、OS が提供する仮想空間の制御機能を利用し、プロセスを跨いだ不正な干渉や改ざんが行われないようにする。

6.3. セキュリティ機能強度

本 ST が要求する TOE の保証レベルは EAL1 であり、保証要件に AVA_SOF.1 を含まないことから、セキュリティ機能強度は主張しない。

6.4. セキュリティメカニズム

本 TOE において、順列的・確率的メカニズム以外のものは存在しない。順列的・確率的メカニズムとしては、F.LIVEHELP_SECURITY 及び F.PWD_SECURITY におけるログイン・パスワードのみが該当する。

6.5. 保証手段

以下に本 TOE の保証手段を示す。なお、ASE クラスに対する保証手段は本 ST である。

ACM_CAP.1　　バージョン番号

【保証手段】

・ TOE バージョンの表示

ADO_IGS.1　　設置、生成、及び立上げ手順

【保証手段】

・ Systemwalker Centric Manager 解説書　-UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 導入手引書　-UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 全体監視適用ガイド -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager V13.2.0 正誤表

ADV_FSP.1　　非形式的機能仕様

【保証手段】

・ Systemwalker Centric Manager V13.2.0 セキュリティ機能仕様書

ADV_RCR.1　　非形式的対応の実証

【保証手段】

・ Systemwalker Centric Manager V13.2.0 表現対応表

AGD_ADM.1　　管理者ガイダンス

【保証手段】

・ Systemwalker Centric Manager 解説書 -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager ｿﾘｭｰｼｮﾝｶﾞｲﾄﾞ ｾｷｭﾘﾃｨ編 -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 導入手引書 -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 使用手引書 監視機能編 -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 使用手引書 資源配付機能編 -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 使用手引書 ｿﾌﾄｳｪｱ修正管理機能編 -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 使用手引書 ﾘﾓｰﾄ操作機能編ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ -Microsoft(R) Windows(R) 2000 / Microsoft(R) Windows(R) XP / Microsoft(R) Windows Server 2003 STD / Microsoft(R) Windows(R) Server2003 EE / Microsoft(R) Windows(R) Vista-

・ Systemwalker Centric Manager 使用手引書 ﾘﾓｰﾄ操作機能編 Client ｶﾞｲﾄﾞ -Microsoft(R) Windows(R) 2000 / Microsoft(R) Windows(R) XP / Microsoft(R) Windows Server 2003 STD / Microsoft(R) Windows(R) Server2003 EE / Microsoft(R) Windows(R) Vista-

・ Systemwalker Centric Manager ﾘﾌｧﾚﾝｽﾏﾆｭｱﾙ -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager ﾒｯｾｰｼﾞ説明書 -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager 全体監視適用ガイド -UNIX/Windows(R)共通-

・ Systemwalker Centric Manager/Systemwalker Event Agent ﾄﾗﾌﾞﾙｼｭｰﾃｨﾝｸﾞｶﾞｲﾄﾞ監視機能編/ｿﾌﾄｳｪｱ修正管理機能編 -UNIX 共通- -Microsoft(R) Windows NT(R)/

Microsoft(R) Windows(R)2000/ Microsoft(R) Windows Server(TM) 2003-

- Systemwalker Centric Manager ﾄﾗﾌﾞﾙｼｭｰﾃｨﾝｸﾞｶﾞｲﾄﾞ 資源配付機能編/Systemwalker Software Delivery ﾄﾗﾌﾞﾙｼｭｰﾃｨﾝｸﾞｶﾞｲﾄﾞ -UNIX 共通- -Microsoft(R) Windows NT(R)/ Microsoft(R)Windows(R) 2000/ Microsoft(R) Windows Server(TM) 2003-
- Systemwalker Centric Manager ﾍﾙﾌﾟ
- 資源配付のﾍﾙﾌﾟ（ﾛｸﾞｲﾝ画面用ﾍﾙﾌﾟとそれ以外の画面用ﾍﾙﾌﾟ）
- 資源配付環境設定のﾍﾙﾌﾟ
- Systemwalker Centric Manager V13.2.0 正誤表

AGD_USR.1　　利用者ガイダンス

【保証手段】

- AGD_ADM.1 に対する保証手段と同じ

ATE_IND.1　　独立テスト － 準拠

【保証手段】

- テストに適した TOE

7. PP 主張

本 ST が適合する PP は存在しない。

8. 根拠

8.1. セキュリティ対策方針根拠

TOE セキュリティ環境とセキュリティ対策方針の対応を表 8.1～表 8.2 に示す。

表 8.1 TOE セキュリティ環境とセキュリティ対策方針の対応（その 1）

TOE セキュリティ環境 / セキュリティ対策方針	T.PASSWORD	T.UAACTION	T.OPCL_UAUSER	T.CMD_UAUSER	T.SV_DEF_FALS	T.D_DELIVER_FAIL	T.D_APPLY_FAIL	T.MA_OPCL_VIOLATION	T.R_OPCL_VIOLATION	T.R_RMTCL	T.R_RMTCL_PWD
O.PWD_ENCR	✓										
O.ACCESS_CTL(1)		✓			✓			✓	✓		
O.ACCESS_CTL(2)								✓	✓		
O.IDFY			✓	✓							
O.LIVEHELP_I&A										✓	
O.STATUS_NOTIFY						✓	✓				
OE.OPSV_OS_I&A			✓	✓						✓	
OE.JOBSV_OS_I&A			✓	✓						✓	
OE.CL_OS_I&A										✓	
OE.RMTCL_ENCR											✓
OE.OS_AUDIT		✓			✓	✓	✓	✓	✓	✓	
OE.OS_DATETIME		✓	✓	✓	✓	✓	✓	✓	✓	✓	
OE.ASSIGN											
OE.PASSWORD											
OE.NETWORK											
OE.PLACE											
OE.OS_SETUP											
OE.DEPLOY_ENCR											
OE.CLIENT_SETUP											
OE.CLIENT_CHK											
OE.OSCONS_ENCR	✓										
OE.LIVEHELP_PWD											

表 8.2　TOE セキュリティ環境とセキュリティ対策方針の対応（その 2）

TOE セキュリティ環境 / セキュリティ対策方針	A.ADMIN	A.PASSWORD	A.NETWORK	A.PLACE	A.OS_ACCESS	A.DEPLOY_ENCR	A.CLIENT	A.LIVEHELP_PWD
O.PWD_ENCR								
O.ACCESS_CTL(1)								
O.ACCESS_CTL(2)								
O.IDFY								
O.LIVEHELP_I&A								
O.STATUS_NOTIFY								
OE.OPSV_OS_I&A								
OE.JOBSV_OS_I&A								
OE.CL_OS_I&A								
OE.RMTCL_ENCR								
OE.OS_AUDIT								
OE.OS_DATETIME								
OE.ASSIGN	✓							
OE.PASSWORD		✓						
OE.NETWORK			✓					
OE.PLACE				✓				
OE.OS_SETUP					✓			
OE.DEPLOY_ENCR						✓		
OE.CLIENT_SETUP							✓	
OE.CLIENT_CHK							✓	
OE.OSCONS_ENCR								
OE.LIVEHELP_PWD								✓

以下に、対策方針が脅威に対抗できる根拠を示す。

〔T.PASSWORD〕

T.PASSWORD は、ｻｰﾊﾞ上の本 TOE にﾛｸﾞｲﾝする際、ﾈｯﾄﾜｰｸ上でﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞが盗聴され

暴露されるかもしれないという脅威である。この対策としては、ﾊﾟｽﾜｰﾄﾞの内容が解析できないようにする必要がある。これに対して、O.PWD_ENCR は、運用管理ｸﾗｲｱﾝﾄまたは業務ｸﾗｲｱﾝﾄ上の本 TOE からｻｰﾊﾞ上の本 TOE にﾛｸﾞｲﾝする際、入力されたﾊﾟｽﾜｰﾄﾞを異なるﾃﾞｰﾀに変換することで、その内容が解析できないようにする。よって、T.PASSWORD の脅威に対抗できる。加えて、OE.OSCONS_ENCR は、ｺﾏﾝﾄﾞによる操作のために本 TOE が動作するｻｰﾊﾞの OS にﾛｸﾞｲﾝする際、ｻｰﾊﾞとの通信にｾｷｭｱな通信手段である SSH を適用することで、ﾊﾟｽﾜｰﾄﾞが解析できないようにする。

〔T.UAACTION〕

T.UAACTION は、運用担当者の役割を与えられた者が、運用管理ｸﾗｲｱﾝﾄまたは TOE が提供するｺﾏﾝﾄﾞを使って、許可されない操作を不正に行うかもしれないという脅威である。この対策としては、操作を行う者に対して権限を割り当て、その権限に応じた操作制限が必要である。これに対して、O.ACCESS_CTL(1)は、運用管理ｸﾗｲｱﾝﾄまたは TOE が提供するｺﾏﾝﾄﾞを使った操作に対し、ﾛｰﾙによるｱｸｾｽ制御を実現する。よって、T.UAACTION の脅威に対抗できる。また、OE.OS_AUDIT は、O.ACCESS_CTL(1)に係る監査ﾛｸﾞの採取に関して、その監査機能の起動と終了の監査ﾛｸﾞを代替するﾛｸﾞを運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに採取し、OE.OS_DATETIME は、監査ﾛｸﾞに設定する日付時刻を提供する。

〔T.OPCL_UAUSER〕

T.OPCL_UAUSER は、攻撃者が運用管理ｸﾗｲｱﾝﾄを利用する権限のある者に成りすますことで、運用管理ｸﾗｲｱﾝﾄから運用管理ｻｰﾊﾞ、業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞの保護資産を不正に操作するかもしれないという脅威である。この対策としては、運用管理ｸﾗｲｱﾝﾄを利用する者を識別認証する必要がある。これに対して、OE.OPSV_OS_I&A は、運用管理ｻｰﾊﾞの OS に登録されたﾕｰｻﾞ名とﾊﾟｽﾜｰﾄﾞを使って運用管理ｸﾗｲｱﾝﾄからﾛｸﾞｲﾝした者を識別認証する。同様に、OE.JOBSV_OS_I&A は、業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞの OS に登録されたﾕｰｻﾞ名とﾊﾟｽﾜｰﾄﾞを使って運用管理ｸﾗｲｱﾝﾄからﾛｸﾞｲﾝした者を識別認証する。そして、その結果を使って、O.IDFY が本 TOE を利用する運用管理者、運用担当者およびｼｽﾃﾑ管理者を識別する。よって、T.OPCL_UAUSER の脅威に対抗できる。また、OE.OS_DATETIME は、O.IDFY に係る監査ﾛｸﾞ採取に関して、監査ﾛｸﾞに設定する日付時刻を提供する。

〔T.CMD_UAUSER〕

T.CMD_UAUSER は、攻撃者が TOE の提供するｺﾏﾝﾄﾞを操作できる権限のある者に成りすまし、ｺﾏﾝﾄﾞを使ってｻｰﾊﾞ上の本 TOE や本 TOE の保護資産を不正に操作するかもしれないという脅威である。この対策としては、各ｻｰﾊﾞにおいてｺﾏﾝﾄﾞ操作を行う者を識別認証する必要がある。これに対して、OE.OPSV_OS_I&A は、運用管理ｻｰﾊﾞの OS に登録されたﾕｰｻﾞ名とﾊﾟｽﾜｰﾄﾞを使って、直接 OS にﾛｸﾞｲﾝした者を識別認証する。同様に、OE.JOBSV_OS_I&A は、業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞの OS に登録されたﾕｰｻﾞ名とﾊﾟｽﾜｰﾄﾞを使って、直接 OS にﾛｸﾞｲﾝした者を識別認証する。そして、その結果を使って、ｺﾏﾝﾄﾞ操作が行われた際、O.IDFY が本 TOE を利用する運用管理者、運用担当者およびｼｽﾃﾑ管理者を識別する。よっ

て、T.CMD_UAUSER の脅威に対抗できる。また、OE.OS_DATETIME は、O.IDFY に係る監査ﾛｸﾞ採取に関して、監査ﾛｸﾞに設定する日付時刻を提供する。

〔T.SV_DEF_FALS〕

T.SV_DEF_FALS は、運用担当者の役割を与えられた者によって、運用管理ｻｰﾊﾞ、業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞに登録された定義情報が改ざんされるかもしれないという脅威である。この対策としては、定義情報の操作を信頼できる者のみに制限することが必要である。これに対して、O.ACCESS_CTL(1)は、ｼｽﾃﾑ管理者または必要な管理系ﾛｰﾙを持った運用管理者にのみ定義情報の操作を許可する。よって、T.SV_DEF_FALS の脅威に対抗できる。また、OE.OS_AUDIT は、O.ACCESS_CTL(1)に係る監査ﾛｸﾞ採取に関して、その監査機能の起動と終了の監査ﾛｸﾞを代替するﾛｸﾞを運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに採取し、OE.OS_DATETIME は、監査ﾛｸﾞに設定する日付時刻を提供する。

〔T.D_DELIVER_FAIL〕

T.D_DELIVER_FAIL は、通信路や配付先の業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞの異常による配付失敗に気づかないかもしれないという脅威である。この対策としては、配付結果を確認できる手段を用意することが必要である。これに対して、O.STATUS_NOTIFY は、配付資源の配付や適用が行われた場合、その結果を運用管理ｻｰﾊﾞに自動通知する。このため、自動通知された結果を検索することで配付の状況を把握でき、必要であれば速やかに原因究明と対処を行える。よって、T.D_DELIVER_FAIL の脅威に対抗できる。また、OE.OS_AUDIT は、O.STATUS_NOTIFY に係る監査ﾛｸﾞ採取に関して、その監査機能の起動と終了の監査ﾛｸﾞを代替するﾛｸﾞを運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに採取し、OE.OS_DATETIME は、監査ﾛｸﾞに設定する日付時刻を提供する。

〔T.D_APPLY_FAIL〕

T.D_APPLY_FAIL は、業務ｻｰﾊﾞ、部門管理ｻｰﾊﾞまたは業務ｸﾗｲｱﾝﾄの異常による配付資源の適用失敗に気づかないかもしれないという脅威である。この対策としては、配付資源の適用結果を確認できる手段を用意することが必要である。これに対して、O.STATUS_NOTIFY は、配付資源の適用が行われた場合、その結果を運用管理ｻｰﾊﾞに自動通知する。このため、自動通知された結果を検索することで適用の状況を把握でき、必要であれば速やかに原因究明と対処を行える。よって、T.D_APPLY_FAIL の脅威に対抗できる。また、OE.OS_AUDIT は、O.STATUS_NOTIFY に係る監査ﾛｸﾞ採取に関して、その監査機能の起動と終了の監査ﾛｸﾞを代替するﾛｸﾞを運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに採取し、OE.OS_DATETIME は、監査ﾛｸﾞに設定する日付時刻を提供する。

〔T.MA_OPCL_VIOLATION〕

T.MA_OPCL_VIOLATION は、運用担当者の役割を与えられた者が、担当範囲外の業務ｼｽﾃﾑ資産（他の運用担当者が管理する業務ｼｽﾃﾑ資産）の監視、査定の各操作を不正に行うことで、運用管理ｸﾗｲｱﾝﾄから表示情報を不正に入手するかもしれないという脅威である。この対策としては、ﾛｰﾙによるｱｸｾｽ制御を前提に、運用管理ｸﾗｲｱﾝﾄのﾒﾆｭｰや対象となる業

務ｼｽﾃﾑ資産を運用担当者毎さらに細かく制限する必要がある。これに対して、O.ACCESS_CTL(2)は、運用担当者毎に監視／査定のためのﾒﾆｭｰや対象とする業務ｼｽﾃﾑ資産を制限できるｱｸｾｽ制御を実現する。そして、O.ACCESS_CTL(1)が、O.ACCESS_CTL(2)の前提となるﾛｰﾙによるｱｸｾｽ制御を実現する。よって、T.MA_OPCL_VIOLATION の脅威に対抗できる。また、OE.OS_AUDIT は、O.ACCESS_CTL(2)および O.ACCESS_CTL(1)に係る監査ﾛｸﾞ採取に関して、その監査機能の起動と終了の監査ﾛｸﾞを代替するﾛｸﾞを運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに採取し、OE.OS_DATETIME は、監査ﾛｸﾞに設定する日付時刻、およびｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間を判定するための日付時刻を提供する。

〔T.R_OPCL_VIOLATION〕

T.R_OPCL_VIOLATION は、運用担当者の役割を与えられた者が、担当範囲外の業務ｼｽﾃﾑ資産（他の運用担当者が管理する業務ｼｽﾃﾑ資産）に対して不正に復旧操作を行うことで、業務ｼｽﾃﾑ資産に悪影響を与えるかもしれないという脅威である。この対策としては、T.MA_OPCL_VIOLATION と同様、ﾛｰﾙによるｱｸｾｽ制御を前提に、運用担当者毎のきめ細かな操作制限が必要である。これに対して、O.ACCESS_CTL(2)は、運用担当者毎に復旧のためのﾒﾆｭｰや対象とする業務ｼｽﾃﾑ資産を制限できるｱｸｾｽ制御を実現する。そして、O.ACCESS_CTL(1)は、O.ACCESS_CTL(2)の前提となるﾛｰﾙによるｱｸｾｽ制御を実現する。よって、T.R_OPCL_VIOLATION の脅威に対抗できる。また、OE.OS_AUDIT は、O.ACCESS_CTL(2)および O.ACCESS_CTL(1)に係る監査ﾛｸﾞ採取に関して、その監査機能の起動と終了の監査ﾛｸﾞを代替するﾛｸﾞを運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに採取し、OE.OS_DATETIME は、監査ﾛｸﾞに設定する日付時刻、およびｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間を判定するための日付時刻を提供する。

〔T.R_RMTCL〕

T.R_RMTCL は、攻撃者がﾘﾓｰﾄ操作を行える者になりすまし、運用管理ｸﾗｲｱﾝﾄから LiveHelp ｸﾗｲｱﾝﾄを不正にﾘﾓｰﾄ操作することで、LiveHelp ｸﾗｲｱﾝﾄに悪影響を与えるかもしれないという脅威である。この対策としては、LiveHelp ｸﾗｲｱﾝﾄにおいてﾘﾓｰﾄ操作を行う者を識別認証する必要がある。これに対して、O.LIVEHELP_I&A は、ﾊﾟｽﾜｰﾄﾞ認証方式が選択された場合に、本 TOE の識別認証機能を使ってﾘﾓｰﾄ操作を行う運用担当者の識別認証を行う。また、OE.OPSV_OS_I&A、OE.JOBSV_OS_I&A および OE.CL_OS_I&A は、OS 認証方式が選択された場合に、LiveHelp ｸﾗｲｱﾝﾄの OS の識別認証機能を使って、LiveHelp ｸﾗｲｱﾝﾄに登録された本 TOE の関連者の識別認証を行う。よって、T.R_RMTCL の脅威に対抗できる。なお、ﾊﾟｽﾜｰﾄﾞ認証方式と OS 認証方式を同時に選択することはできないため、O.LIVEHELP_I&A と、OE.CL_OS_I&A の対策方針が競合することはない。また、OE.OS_AUDIT は、O.LIVEHELP_I&A に係る監査ﾛｸﾞ採取に関して、その監査機能の起動と終了の監査ﾛｸﾞを代替するﾛｸﾞを運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに採取し、OE.OS_DATETIME は、監査ﾛｸﾞに設定する日付時刻を提供する。

〔T.R_RMTCL_PWD〕

T.R_RMTCL_PWD は、ﾘﾓｰﾄ操作のために目的の LiveHelp ｸﾗｲｱﾝﾄにﾛｸﾞｲﾝする際、ﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞが盗聴され、その内容が漏洩するかもしれないという脅威である。この対策としては、ﾊﾟｽﾜｰﾄﾞの内容が解析できないようにする必要がある。これに対して、**OE.RMTCL_ENCR** は、運用管理ｸﾗｲｱﾝﾄと LiveHelp ｸﾗｲｱﾝﾄの OS の機能を使ってﾊﾟｽﾜｰﾄﾞの内容が解析できないようにする。よって、T.R_RMTCL_PWD の脅威に対抗できる。

〔**A.ADMIN**〕

A.ADMIN は、ｼｽﾃﾑ管理者および運用管理者は不正を行わない信頼できる者であるということを保証した前提条件である。この前提条件に対して、**OE.ASSIGN** は、運用管理部門が信頼できる者をｼｽﾃﾑ管理者および運用管理者に選任することを要求する。よって、A.ADMIN の前提条件は実現できる。

〔**A.PASSWORD**〕

A.PASSWORD は、本 TOE にﾛｸﾞｲﾝするためのﾊﾟｽﾜｰﾄﾞについて、本人以外の者が知ることはできないことを保証した前提条件である。この前提条件に対して、**OE.PASSWORD** は、本 TOE の関連者に対して、自身のﾊﾟｽﾜｰﾄﾞ保護を適切に行うことを遵守させる。よって、A.PASSWORD の前提条件は実現できる。

〔**A.NETWORK**〕

A.NETWORK は、本 TOE の動作するｻｰﾊﾞ、ｸﾗｲｱﾝﾄおよび本 TOE が運用管理の対象とする業務ｼｽﾃﾑ資産が、ｲﾝﾄﾗﾈｯﾄのみに接続されることを保証した前提条件である。この前提条件に対して、**OE.NETWORK** は、本 TOE の動作するｻｰﾊﾞ、ｸﾗｲｱﾝﾄおよび本 TOE が運用管理の対象とする業務ｼｽﾃﾑ資産が接続できるﾈｯﾄﾜｰｸを、ﾌｧｲｱｳｫｰﾙで保護されたｲﾝﾄﾗﾈｯﾄのみに制限する。よって、A.NETWORK の前提条件は実現できる。

〔**A.PLACE**〕

A.PLACE は、開発用ｻｰﾊﾞを除く本 TOE の動作するｻｰﾊﾞが、ｼｽﾃﾑ管理者以外は入退出できない入退出管理が施された事務ﾌﾛｱやｻｰﾊﾞﾙｰﾑに設置されることを保証した前提条件である。この前提条件に対して、**OE.PLACE** は、本 TOE の動作するｻｰﾊﾞが、ｼｽﾃﾑ管理者以外は入退出できない入退出管理が施された事務ﾌﾛｱやｻｰﾊﾞﾙｰﾑに設置されることを規定する。よって、A.PLACE の前提条件は実現できる。

〔**A.OS_ACCESS**〕

A.OS_ACCESS は、本 TOE が運用管理で使用する資産を格納したファイルや、その処理のための作業用ファイルに対し、OS 経由での不正なｱｸｾｽがないことを保証した前提条件である。この前提条件に対して、**OE.OS_SETUP** は、OS に対する適切なｱｸｾｽ権設定により、OS 経由による改ざんから保護する。よって、A.OS_ACCESS の前提条件は実現できる。

〔**A.DEPLOY_ENCR**〕

A.DEPLOY_ENCR は、配付資源に対するﾈｯﾄﾜｰｸ上での盗聴がないことを保証した前提条件である。この前提条件に対して、**OE.DEPLOY_ENCR** は、ｼｽﾃﾑ管理者または運用管理者が事前に暗号化するよう運用担当者に指示することを要求する。よって、A.DEPLOY_ENCR の

前提条件は実現できる。

〔A.CLIENT〕

A.CLIENT は、業務ｸﾗｲｱﾝﾄおよび開発用ｸﾗｲｱﾝﾄについて、不正な利用がないことを保証した前提条件である。この前提条件に対して、OE.CLIENT_SETUP は、ｼｽﾃﾑ管理者に対して本 TOE が正しく利用されるようｾｯﾄｱｯﾌﾟを行うことを要求する。さらに、OE.CLIENT_CHK は、ｼｽﾃﾑ管理者に対して定期的に利用状況を確認するよう要求する。よって、A.CLIENT の前提条件は実現できる。

〔A.LIVEHELP_PWD〕

A.LIVEHELP_PWD は、ﾘﾓｰﾄ操作で使用するﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞのﾊﾟｽﾜｰﾄﾞ長を 7 文字以上とする前提条件である。この前提条件に対して、OE.LIVEHELP_PWD は、ｼｽﾃﾑ管理者に対して LiveHelp ｸﾗｲｱﾝﾄ上の本 TOE に 7 文字以上のﾊﾟｽﾜｰﾄﾞを設定するよう要求する。よって、A.LIVEHELP_PWD の前提条件は実現できる。

8.2. セキュリティ要件根拠

8.2.1. セキュリティ機能要件根拠

表8.3に、セキュリティ対策方針に対して導出したセキュリティ機能要件の対応を示す。

表 8.3 セキュリティ対策方針とセキュリティ機能要件の対応

セキュリティ対策方針 / セキュリティ機能要件	O.PWD_ENCR	O.ACCESS_CTL(1)	O.ACCESS_CTL(2)	O.IDFY	O.LIVEHELP_I&A	O.STATUS_NOTIFY	OE.OPSV_OS_I&A	OE.JOBSV_OS_I&A	OE.CL_OS_I&A	OE.RMTCL_ENCR	OE.OS_AUDIT	OE.OS_DATETIME
FAU_GEN.1(1)		✓		✓								
FAU_GEN.1(2)		✓	✓		✓	✓						
FAU_SAR.1		✓	✓	✓	✓	✓						
FAU_STG.1		✓	✓	✓	✓	✓						
FAU_STG.3		✓	✓		✓	✓						
FAU_STG.4		✓		✓								
FDP_ACC.1(1)		✓										
FDP_ACC.1(2)			✓									
FDP_ACF.1(1)		✓										
FDP_ACF.1(2)			✓									
FDP_IFC.1						✓						
FDP_IFF.1						✓						
FIA_AFL.1				✓								
FIA_ATD.1				✓								
FIA_SOS.1					✓							
FIA_UAU.2(1)					✓							
FIA_UAU.6				✓								
FIA_UAU.7					✓							
FIA_UID.2(1)				✓								
FIA_UID.2(2)					✓							
FIA_USB.1				✓								
FMT_MOF.1		✓	✓	✓	✓	✓						
FMT_MSA.1(1)		✓										
FMT_MSA.1(2)			✓									

セキュリティ対策方針 / セキュリティ機能要件	O.PWD_ENCR	O.ACCESS_CTL(1)	O.ACCESS_CTL(2)	O.IDFY	O.LIVEHELP_I&A	O.STATUS_NOTIFY	OE.OPSV_OS_I&A	OE.JOBSV_OS_I&A	OE.CL_OS_I&A	OE.RMTCL_ENCR	OE.OS_AUDIT	OE.OS_DATETIME
FMT_MSA.1(3)						✓						
FMT_MSA.3(1)		✓										
FMT_MSA.3(2)			✓									
FMT_MSA.3(3)						✓						
FMT_MTD.1		✓	✓		✓	✓						
FMT_SMF.1		✓	✓	✓	✓	✓						
FMT_SMR.1		✓	✓	✓	✓	✓						
FPT_ITT.1(1)	✓											
FPT_RVM.1	✓	✓	✓	✓	✓	✓						
FPT_SEP.1	✓	✓	✓	✓	✓	✓						
FAU_GEN.1[ENV](3)											✓	
FIA_UAU.2[ENV](2)							✓	✓	✓			
FIA_UID.2[ENV](3)							✓	✓	✓			
FPT_ITT.1[ENV](2)										✓		
FPT_STM.1[ENV]												✓

この表のとおり、各対策方針は監査機能のための機能要件を含む。また、機能要件には、繰り返しの操作により複数の対策方針に出現するものがある。よって、以下の内容を明らかにすることで、対策方針に対する機能要件の根拠とする。

- 監査機能に適用される機能要件が監査機能を満たすこと、およびそのセットが内部的に一貫していること
- 各対策方針に適用される機能要件（上記の機能要件は除く）がその対策方針を満たすこと、および監査機能に適用される機能要件も含め、そのセットが内部的に一貫していること
- 複数の対策方針に出現する機能要件について、重複した定義等がなく、対策方針毎独立していること

また、内部的に一貫していることについては、機能要件間において競合の可能性がある同タイプの事象、操作、またはデータの取り扱いの存在がないことを検証する（テストを取り扱う機能要件はないので除く）。

1)　監査機能に適用される機能要件

対策方針の中で、O.ACCESS_CTL(1)、O.ACCESS_CTL(2)、O.IDFY、O.LIVEHELP_I&A、および O.STATUS_NOTIFY は、監査機能の対象としている。

表 8.4 は監査機能に適用する機能要件の内訳(FAU_GEN.1[ENV](3)および FPT_STM.1[ENV]は、監査機能を支援する OE.OS_AUDIT および OE.OS_DATETIME に適用される機能要件）である。なお、本 TOE は、監査機能を①運用管理者、運用担当者およびシステム管理者の識別認証およびコマンド操作に対するロールによるアクセス制御に係る事象の監査機能（“ACL マネージャ機能の監査ログ機能”）、②運用管理クライアントからの操作事象の監査機能（“運用管理クライアント操作の監査ログ機能”）の二つで実現するため、それぞれを分けて示している。

この表に示したとおり、監査機能として必要な監査事象の採取、採取された監査記録の保護、および監査機能の利用に係る管理機能と役割それぞれについて、機能要件の矛盾する定義はなく、監査機能を実現することができる。

また、各機能要件は、監査に係る事象（監査事象)、操作（監査機能の起動と停止、保存日数の変更、監査記録の参照)、データ（監査ﾃﾞｰﾀ、保存日数）を取り扱うが、表中に示した内訳のとおり独立しており、機能要件間で競合の可能性のある同タイプの事象、操作、またはデータの取り扱いは存在しない。よって、各監査機能に適用される機能要件のセットは内部的に一貫している。監査機能間においても機能要件間の競合はない。

〔監査レベルについて〕

監査対象とする対策方針は識別認証とｱｸｾｽ制御に係るものであり、ｱｸｾｽ制御に係る対策方針が実施される場合には、先行して必ず識別認証が動作する。そのため、最低限、識別認証に係る監査事象を記録（補足）しておくことで不正の兆候を監査できる。このことから、対策方針が要求する監査ﾚﾍﾞﾙを満たすと判断できる（O.STATUS_NOTIFY も最初に通知先ｼｽﾃﾑの設定を行う際、必ず識別認証が動作する)。よって、FAU_GEN.1(1)と FAU_GEN.1(2)では、それに合致する監査ﾚﾍﾞﾙである「最小」を選択し、加えて個別に定義した監査対象事象として、ﾕｰｻﾞ名へのﾛｰﾙの登録と削除を行った事象を記録している。

補足）本 TOE は識別認証を OS に依存しているが、OS から返された識別認証の結果を監査ﾛｸﾞに反映しており、識別認証事象（成功、失敗）を記録できる。

表 8.4　監査機能に適用されるセキュリティ機能要件の内訳

区分	監査対象とする対策方針と監査事象	監査記録の保護	必要な管理と役割
ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能	**FAU_GEN.1(1)** 監査事象（O.IDFY のｼｽﾃﾑ管理者、運用管理者および運用担当者に係る識別認証事象、O.ACCESS_CTL(1)のｺﾏﾝﾄﾞを実行した事象）を採取。 ただし、FIA_AFL.1 の事象は操作に係る事象であり FAU_GEN.1(2)で採取。 O.LIVEHELP_I&A もﾘﾓｰﾄ操作の中で動作することから FAU_GEN.1(2)で採取。 **FPT_STM.1[ENV]** 監査事象の監査項目（日付時刻）を OS から取得するため。	**FAU_SAR.1** 当機能の監査ﾛｸﾞﾌｧｲﾙに採取された監査記録を許可された識別された役割（ｼｽﾃﾑ管理者）に対して、解釈可能な形で提供するため。 **FAU_STG.1** 上記監査ﾛｸﾞﾌｧｲﾙの監査記録の不正な削除や改ざんからの保護を行うため。 **FAU_STG.4** 上記監査ﾛｸﾞﾌｧｲﾙの監査記録の損失を防止するためのｱｸｼｮﾝを規定するため。	**FMT_MOF.1** 当機能の起動と終了を行う能力を許可された識別された役割（ｼｽﾃﾑ管理者）に制限するため。 **FMT_SMF.1** 上記 FMT_MOF.1 が示す当機能の管理機能（起動と停止を行う機能）を定義するため。 **FMT_SMR.1** 上記 FMT_MOF.1 の許可された識別された役割（ｼｽﾃﾑ管理者）に対して、その維持と利用者との関係付けを行うため。
運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能	**FAU_GEN.1(2)** 監査事象（O.ACCESS_CTL(1)のﾒﾆｭｰを実行した事象、O.ACCESS_CTL(2)、O.LIVEHELP_I&A、および O.STATUS_NOTIFY に係る操作事象）を採取。 **FAU_GEN.1[ENV](3)** 当機能の起動と終了の監査記録をｲﾍﾞﾝﾄﾛｸﾞのﾒｯｾｰｼﾞで代替するため。 **FPT_STM.1［ENV］** 監査事象の監査項目（日付時刻）を OS から取得するため。	**FAU_SAR.1** 当機能の監査ﾛｸﾞﾌｧｲﾙに採取された監査記録を許可された識別された役割（ｼｽﾃﾑ管理者）に対し、解釈可能な形で提供するため。 **FAU_STG.1** 上記監査ﾛｸﾞﾌｧｲﾙの監査記録の不正な削除や改ざんからの保護を行うため。 **FAU_STG.3** 上記監査ﾛｸﾞﾌｧｲﾙの監査記録損失の恐れ発生時のｱｸｼｮﾝを規定するため。	**FMT_MOF.1** 当機能の起動と終了を行う能力を許可された識別された役割（ｼｽﾃﾑ管理者）に制限するため。 **FMT_MTD.1** 当機能の監査ﾛｸﾞﾌｧｲﾙの監査記録の保存日数の変更を許可された識別された役割（ｼｽﾃﾑ管理者）に制限するため。 **FMT_SMF.1** 左記 FAU_STG.3 の管理機能（監査記録の保存日数の管理機能）、および上記 FMT_MOF.1 が示す当機能の管理機能（起動と停止を行う機能）を定義するため。 **FMT_SMR.1** 上記 FMT_MOF.1、FMT_MTD.1 の許可された識別された役割（ｼｽﾃﾑ管理者）に対して、その維持と利用者との関係付けを行うため。

2) 対策方針に適用される機能要件

ここでは、前項の監査機能に適用される機能要件を除く、チェックされた機能要件について、そのセットが各々の対策方針を満たすこと、加えて、1)項の該当する監査機能の機能要件を含め、内部的に一貫していることの根拠を示す。

〔O.PWD_ENCR〕

O.PWD_ENCR は、ﾈｯﾄﾜｰｸを介して本 TOE の異なるﾊﾟｰﾂ間で流れるﾃﾞｰﾀ（ﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞ）について、その内容を解析できないようにする対策方針であり、解析できないようにする目的は、漏洩や暴露からの保護である。そのため、TSF 内ﾃﾞｰﾀ転送保護のための機能要件である FPT_ITT.1(1)により、ﾃﾞｰﾀ（ｻｰﾊﾞ上の本 TOE にﾛｸﾞｲﾝするためのﾊﾟｽﾜｰﾄﾞ）がｸﾗｲｱﾝﾄ上の TOE からｻｰﾊﾞ上の TOE に送られる際に暴露から保護する。さらに、以下の機能要件を適用することで、FPT_ITT.1(1)が確実に実施されることを保証する。

- FPT_RVM.1 により、迂回されることを防止する。
- FPT_SEP.1 により、信頼できないｻﾌﾞｼﾞｪｸﾄからの干渉や改ざんを防止する。

以上のことから、O.PWD_ENCR を満たすことができる。また、機能要件間で競合する可能性のあるﾃﾞｰﾀの取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔O.ACCESS_CTL(1)〕

O.ACCESS_CTL(1)は、運用管理ｸﾗｲｱﾝﾄまたは TOE が提供するｺﾏﾝﾄﾞを使った不正な操作を防ぐ対策方針であり、それを実現する手段は、ﾛｰﾙによるｱｸｾｽ制御の適用である。そのため、以下のとおり、ｱｸｾｽ制御のための機能要件と、それらに必要な管理のための機能要件を適用する。

- FDP_ACC.1(1)により、ｻﾌﾞｼﾞｪｸﾄ（TOE の利用者）とｵﾌﾞｼﾞｪｸﾄ（ﾒﾆｭｰおよびｺﾏﾝﾄﾞ）間の操作のﾘｽﾄ（ﾒﾆｭｰおよびｺﾏﾝﾄﾞの実行）に対して、ﾛｰﾙによるｱｸｾｽ制御を行う ACL ﾏﾈｰｼﾞｬｱｸｾｽ制御 SFP を適用する。
- FDP_ACF.1(1)により、ACL ﾏﾈｰｼﾞｬｱｸｾｽ制御 SFP のためのｾｷｭﾘﾃｨ属性として、ｻﾌﾞｼﾞｪｸﾄの属性（ﾛｰﾙ）とｵﾌﾞｼﾞｪｸﾄの属性（許可ﾛｰﾙ）を定義し、それを使った具体的なｱｸｾｽ制御規則を規定する。
- FMT_MSA.1(1)により、TOE の利用者を表すﾕｰｻﾞ名に対するｻﾌﾞｼﾞｪｸﾄの属性（ﾛｰﾙ）の操作（登録と削除）を行う能力を許可された識別された役割（ｼｽﾃﾑ管理者、運用管理者）に制限する。
- FMT_MSA.3(1)により、ｵﾌﾞｼﾞｪｸﾄ属性（許可ﾛｰﾙ）に対して制限的ﾃﾞﾌｫﾙﾄ値を与えること、初期値の設定に関する許可された識別された役割はないことを規定する。
- FMT_SMF.1 により、FDP_ACF.1(1)に対する管理機能（ｱｸｾｽ制御に係る属性（ﾛｰﾙ）の維持管理機能）を定義する。
- FMT_SMR.1 により、FMT_MSA.1(1)の許可された識別された役割（ｼｽﾃﾑ管理者、運

用管理者）の維持および利用者との関係付けを行う。

さらに、以下の機能要件を適用することにより、1)項の“運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能”の機能要件を含め、これら機能要件が確実に実施されることを保証する。

- FPT_RVM.1 により、迂回されることを防止する。
- FPT_SEP.1 により、信頼できないｻﾌﾞｼﾞｪｸﾄからの干渉や改ざんを防止する。

以上のことから、O.ACCESS_CTL(1)を満たすことができる。また、上記ならびに前述の表 8.4 に括弧付きで内訳を示したように、機能要件間で競合する可能性のある操作、ﾃﾞｰﾀの取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔O.ACCESS_CTL(2)〕

O.ACCESS_CTL(2)は、運用管理ｸﾗｲｱﾝﾄからの運用担当者による担当範囲外への不正な操作を防ぐ対策方針であり、それを実現する手段は、運用担当者毎に操作を制限するｱｸｾｽ制御の適用である。そのため、以下のとおりｱｸｾｽ制御のための機能要件と、それらに必要な管理のための機能要件を適用する。

- FDP_ACC.1(2)により、ｻﾌﾞｼﾞｪｸﾄ（TOE 利用者）とｵﾌﾞｼﾞｪｸﾄ（ﾒﾆｭｰ）間の操作のﾘｽﾄ（ﾒﾆｭｰの実行）に対して、運用担当者毎のｱｸｾｽ制御を行うｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP を適用する。
- FDP_ACF.1(2)により、ｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP のためのｾｷｭﾘﾃｨ属性として、ｻﾌﾞｼﾞｪｸﾄの属性（操作ﾚﾍﾞﾙ）、およびｵﾌﾞｼﾞｪｸﾄの属性（許可操作ﾚﾍﾞﾙ）を定義し、それらを使った具体的なｱｸｾｽ制御規則を規定する。
- FMT_MOF.1 により、ｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP を実施するｾｷｭﾘﾃｨ機能（“ｺﾝｿｰﾙ操作制御機能”）に対する操作（停止と動作）を行う能力を許可された識別された役割（ｼｽﾃﾑ管理者）に制限する。
- FMT_MSA.1(2)により、運用担当者を表すﾕｰｻﾞ名に対するｻﾌﾞｼﾞｪｸﾄの属性（操作ﾚﾍﾞﾙ）の操作（登録と削除）、およびﾒﾆｭｰに対するｵﾌﾞｼﾞｪｸﾄの属性（許可操作ﾚﾍﾞﾙ）の操作（登録と削除）を行う能力を許可された識別された役割（ｼｽﾃﾑ管理者、運用管理者）に制限する。
- FMT_MSA.3(2)により、ｵﾌﾞｼﾞｪｸﾄの属性（許可操作ﾚﾍﾞﾙ）に対して、制限的ﾃﾞﾌｫﾙﾄ値を与えること、初期値の設定に関する許可された役割はないことを規定する。
- FMT_MTD.1 により、ｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP に係る TSF ﾃﾞｰﾀ（ｺﾝｿｰﾙ操作制御機能の利用形態の選択情報、およびｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間）の操作（改変）を許可された識別された役割（ｼｽﾃﾑ管理者）に制限する。
- FMT_SMF.1 により、FDP_ACF.1(2)に対する管理機能（ｱｸｾｽ制御に係る属性（操作ﾚﾍﾞﾙおよび許可操作ﾚﾍﾞﾙ）の維持管理機能）、および FMT_MOF.1 が示す“ｺﾝｿｰﾙ操作制御機能”の管理機能（起動と停止を行う機能）を定義する。
- FMT_SMR.1 により、FMT_MOF.1、FMT_MSA.1(2)、FMT_MTD.1 の許可された識別された役割（ｼｽﾃﾑ管理者）に対して、その維持および利用者との関係付けを行う。

さらに、以下の機能要件を適用することで、1)項の“運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能”の機能要件を含め、これら機能要件が確実に実施されることを保証する。

- FPT_RVM.1 により、迂回されることを防止する。
- FPT_SEP.1 により、信頼できないｻﾌﾞｼﾞｪｸﾄからの干渉や改ざんを防止する。

以上のことから、O.ACCESS_CTL(2)を満たすことができる。また、上記ならびに前述の表 8.4 に括弧付きで内訳を示したように、機能要件間で競合する可能性のある操作、ﾃﾞｰﾀの取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔O.IDFY〕

O.IDFY は、運用管理者、運用担当者およびｼｽﾃﾑ管理者に対する成りすましを防ぐための対策方針であり、それを実現する手段は、本 TOE の利用者に対する識別認証である。また、本 TOE は OS 機能を利用してﾕｰｻﾞ名とﾊﾟｽﾜｰﾄﾞによる識別認証を行い、それが成功したのち、運用管理者、運用担当者およびｼｽﾃﾑ管理者の識別を行う。そのため、識別認証に係る機能要件と、それらに必要な管理のための機能要件を以下のとおり適用する。

- FIA_AFL.1 により、指定した認証事象（運用管理ｸﾗｲｱﾝﾄから運用管理ｻｰﾊﾞにﾛｸﾞｲﾝ（Systemwalker ｺﾝｿｰﾙ機能利用時））において、OS による識別認証が連続して 3 回失敗した場合のｱｸｼｮﾝ（ﾛｸﾞｲﾝ処理を終了）を定義する。
- FIA_UID.2(1)により、OS による識別認証が成功した者に対して、操作（運用管理者、運用担当者またはｼｽﾃﾑ管理者の識別）を要求する。
- FIA_USB.1 により、FIA_UID.2(1)による操作（識別）が成功した利用者に対して、ｻﾌﾞｼﾞｪｸﾄへのｾｷｭﾘﾃｨ属性（運用管理者または運用担当者の場合はﾛｰﾙおよび操作ﾚﾍﾞﾙ）の関連付けを行い、FIA_ATD.1 により、その関連付けたｾｷｭﾘﾃｨ属性の維持を実現する。
- FIA_UAU.6 により、再認証の要求事象（ｺﾝｿｰﾙ操作制御機能の利用形態の選択情報が操作の都度ﾕｰｻﾞ名を入力する形態に設定されている状態において、ｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間が切れた場合）が発生した際、利用者（ｺﾝｿｰﾙ操作制御を利用する運用担当者）の再認証を行う。なお、再認証の要求は、“ｺﾝｿｰﾙ操作制御機能”より行われる。
- FMT_SMF.1 により、FIA_UAU.6 に対する管理機能（ﾕｰｻﾞ名に関するｺﾝｿｰﾙ操作制御機能の利用形態の管理機能、および再認証の決定に使用されるﾕｰｻﾞ名の有効期間の管理機能）を定義する。

さらに、以下の機能要件を適用することで、1)項の“ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能”の機能要件も含め、これら機能要件が確実に実施されることを保証する。

- FPT_RVM.1 により、迂回されることを防止する。
- FPT_SEP.1 により、信頼できないｻﾌﾞｼﾞｪｸﾄからの干渉や改ざんを防止する。

以上のことから、O.IDFY を満たすことができる。また、上記ならびに前述の表 8.4 に括弧付きで内訳を示したように、機能要件間で競合する可能性のある事象、操作、ﾃﾞｰﾀ

の取り扱いは存在しないことから、適用する機能要件のｾｯﾄは内部的に一貫している。なお、OS による識別認証の対策方針（OE.OPSV_OS_I&A、OE.JOBSV_OS_I&A）に適用される機能要件との関係については 3)項に示す。

〔O.LIVEHELP_I&A〕

O.LIVEHELP_I&A は、ﾘﾓｰﾄ操作の対象となる LiveHelp ｸﾗｲｱﾝﾄにおいて、ﾘﾓｰﾄ操作を行う者に対する成りすましを防止するための対策方針である。この対策方針を実現する手段は、LiveHelp ｸﾗｲｱﾝﾄ上の本 TOE によるﾘﾓｰﾄ操作を行う者に対する識別認証である。そのため、以下のとおり識別認証のための機能要件を適用する。

- FIA_UAU.2(1)および FIA_UID.2(2)により、利用者に対する認証と識別の操作（ﾘﾓｰﾄ操作を行う運用担当者の認証と識別）を要求する。
- FIA_SOS.1 により、識別認証のために入力されたﾊﾟｽﾜｰﾄﾞﾃﾞｰﾀ（ﾘﾓｰﾄ操作のためのﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞ）に対する定められた尺度による検証を実現する。
- FIA_UAU.7 により、認証中はﾃﾞｰﾀ（ｱｽﾀﾘｽｸに置き換えたﾊﾟｽﾜｰﾄﾞ文字列）のみﾘﾓｰﾄ操作を行う運用担当者にﾌｨｰﾄﾞﾊﾞｯｸする。

さらに、以下の機能要件を適用することで、1)項の“運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能”の機能要件も含め、これら機能要件が確実に実施されることを保証する。

- FPT_RVM.1 により、迂回されることを防止する。
- FPT_SEP.1 により、信頼できないｻﾌﾞｼﾞｪｸﾄからの干渉や改ざんを防止する。

以上のことから、O.LIVEHELP_I&A を満たすことができる。また、上記ならびに前述の表 8.4 に括弧付きで内訳を示したように、機能要件間で競合する可能性のある操作、ﾃﾞｰﾀの取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔O.STATUS_NOTIFY〕

O.STATUS_NOTIFY は、配付資源の配付適用結果が確実に運用管理ｻｰﾊﾞに通知されることを保証するための対策方針であり、それを実現する手段は、資源配付結果通知ﾃﾞｰﾀに対する情報ﾌﾛｰ制御の適用である。そのため、以下のとおり、情報ﾌﾛｰ制御のための機能要件と、それらに必要な管理のための機能要件を適用する。

- FDP_IFC.1 により、ｻﾌﾞｼﾞｪｸﾄ（通知元の資源配付ﾌﾟﾛｾｽ）、情報（資源の配付・適用結果ﾃﾞｰﾀ）、および情報の流れを引き起こす操作（通知先の資源配付ﾌﾟﾛｾｽに送る）に対して、情報ﾌﾛｰ制御 SFP である資源配付結果通知ﾃﾞｰﾀ保護 SFP を適用する。
- FDP_IFF.1 により、資源配付結果通知ﾃﾞｰﾀ保護 SFP のためのｻﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性（通知先ｼｽﾃﾑ名）を定義し、それを使った具体的な情報ﾌﾛｰの規則を規定する。
- FMT_MOF.1 により、資源配付結果通知ﾃﾞｰﾀ保護 SFP を実施するｾｷｭﾘﾃｨ機能（“適用結果の自動通知機能”）に対する操作（起動／停止）を行う能力を許可された識別された役割に制限する。
- FMT_MSA.1(3)により、ｾｷｭﾘﾃｨ属性（通知先ｼｽﾃﾑ名）について、その属性を操作（改変、削除、登録）する能力を許可された識別された役割に制限する。

・ FMT_MSA.3(3)により、ｾｷｭﾘﾃｨ属性（通知先ｼｽﾃﾑ名）に対して制限的ﾃﾞﾌｫﾙﾄ値を与えること、初期値の設定に関する許可された役割はないことを規定する。
・ FMT_SMF.1 により、FDP_IFF.1 に対する管理機能（情報ﾌﾛｰ制御に係る属性（通知先ｼｽﾃﾑ名）の維持管理機能）、および FMT_MOF.1 が示す“適用結果の自動通知機能”の管理機能（起動と停止を行う機能）を定義する。
・ FMT_SMR.1 により、上記の FMT_MOF.1、FMT_MSA.1(3)の許可された識別された役割（ｼｽﾃﾑ管理者、運用管理者）に対して、その維持と利用者との関係付けを行う。

さらに、以下の機能要件を適用することで、1)項の“運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能”の機能要件も含め、これら機能要件が確実に実施されることを保証する。

・ FPT_RVM.1 により、迂回されることを防止する。
・ FPT_SEP.1 により、信頼できないｻﾌﾞｼﾞｪｸﾄからの干渉や改ざんを防止する。

以上のことから、O.STATUS_NOTIFY を満たすことができる。また、上記ならびに前述の表 8.4 に括弧付きで内訳を示したように、機能要件間で競合する可能性のある操作、ﾃﾞｰﾀの取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔OE.OPSV_OS_I&A〕

OE.OPSV_OS_I&A は、運用管理ｻｰﾊﾞの OS が本 TOE の利用者を識別認証し、識別認証に失敗した場合、TOE の利用を拒否する対策方針である。そのため、運用管理ｻｰﾊﾞの OS に対して、識別認証のための機能要件である FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)を適用することにより、利用者（運用管理ｻｰﾊﾞにﾛｸﾞｲﾝできる利用者）に対する認証と識別を要求する。以上のことから、OE.OPSV_OS_I&A を満たすことができる。また、機能要件間で競合する可能性のある操作の取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔OE.JOBSV_OS_I&A〕

OE.JOBSV_OS_I&A は、業務ｻｰﾊﾞおよび部門管理ｻｰﾊﾞの OS が本 TOE の利用者を識別認証し、識別認証に失敗した場合、TOE の利用を拒否する対策方針である。そのため、部門管理ｻｰﾊﾞと業務ｻｰﾊﾞの OS に対して、識別認証のための機能要件である FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)を適用することにより、利用者（部門管理ｻｰﾊﾞまたは業務ｻｰﾊﾞにﾛｸﾞｲﾝできる利用者）に対する認証と識別を要求する。以上のことから、OE.JOBSV_OS_I&A を満たすことができる。また、機能要件間で競合する可能性のある操作の取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔OE.CL_OS_I&A〕

OE.CL_OS_I&A は、LiveHelp ｸﾗｲｱﾝﾄの一つである運用管理ｸﾗｲｱﾝﾄまたは業務ｸﾗｲｱﾝﾄの OS が、本 TOE の利用者を識別認証し、識別認証に失敗した場合、TOE の利用を拒否する対策方針である。そのため、OS に対して、識別認証のための機能要件である FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)を適用することにより、利用者（運用管理ｸﾗｲｱﾝﾄまたは業務ｸﾗｲｱﾝﾄにﾛｸﾞｲﾝできる利用者）に対する認証と識別を要求する。以上の

ことから、OE.CL_OS_I&A を満たすことができる。また、機能要件間で競合する可能性のある操作の取り扱いは存在しないことから、機能要件のｾｯﾄは内部的に一貫している。

〔OE.RMTCL_ENCR〕

OE.RMTCL_ENCR は、ﾈｯﾄﾜｰｸ上を流れるﾘﾓｰﾄ操作のためのﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞについて、その内容を解析できないようにする対策方針であり、解析できないようにする目的は漏洩や暴露からの保護である。そのため、運用管理ｸﾗｲｱﾝﾄと LiveHelp ｸﾗｲｱﾝﾄの OS に対して、TSF 内ﾃﾞｰﾀ転送保護のための機能要件である FPT_ITT.1[ENV](2)を適用することにより、ﾃﾞｰﾀ（ﾘﾓｰﾄ操作のためのﾛｸﾞｲﾝ・ﾊﾟｽﾜｰﾄﾞ）を暴露から保護する。以上のことから、OE.RMTCL_ENCR を満たすことができる。また、適用される機能要件は他にないことから、機能要件間の競合はない。

〔OE.OS_AUDIT〕

OE.OS_AUDIT は、“運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能”の起動と終了事象の監査ﾛｸﾞをｲﾍﾞﾝﾄﾛｸﾞのﾒｯｾｰｼﾞで代替する対策方針である。そのため、運用管理ｸﾗｲｱﾝﾄの OS に対して監査ﾃﾞｰﾀ生成のための機能要件である FAU_GEN.1[ENV](3)を適用することにより、OS による監査事象（監査ﾛｸﾞ機能の起動と停止事象）の記録を実現する。以上のことから、OE.OS_AUDIT を満たすことができる。また、適用される機能要件は他にないことから、機能要件間の競合はない。

〔OE.OS_DATETIME〕

OE.OS_DATETIME は、すべての監査ﾛｸﾞに設定する日付時刻、およびｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間を判定するための日付時刻を OS から取得する対策方針である。そのため、監査ﾛｸﾞに記録する日付時刻については、運用管理ｸﾗｲｱﾝﾄ、運用管理ｻｰﾊﾞ、部門管理ｻｰﾊﾞおよび業務ｻｰﾊﾞの OS に対して、ﾀｲﾑｽﾀﾝﾌﾟを提供するための機能要件である FPT_STM.1[ENV]を適用することにより、OS からの高信頼なﾀｲﾑｽﾀﾝﾌﾟの取得を実現する。ｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間を判定するための日付時刻については、運用管理ｻｰﾊﾞの OS に対し同様に適用することで、OS からの高信頼なﾀｲﾑｽﾀﾝﾌﾟの取得を実現する。以上のことから、OE.OS_DATETIME を満たすことができる。また、適用される機能要件は他にないことから、機能要件間の競合はない。

3) 複数の対策方針に出現する機能要件

機能要件が複数の対策方針に適用されている場合においても、以下のとおり、取り扱う対象が対策方針毎独立しており、対策方針間で動作が競合することはない。

- FAU_GEN.1(1)～(2)および FAU_GEN.1[ENV](3)については、1)項に示したとおり。
- FDP_ACC.1(1)～(2)、および FDP_ACF.1(1)～(2)については、実施されるｱｸｾｽ制御 SFP が対策方針ごと異なり、使用されるｾｷｭﾘﾃｨ属性も異なる。同様に、そのｾｷｭﾘﾃｨ属性の管理や扱いを規定した FMT_MSA.1(1)～(2)、および FMT_MSA.3(1)～(2)についても、各々対象とするｾｷｭﾘﾃｨ属性が異なる。FMT_MSA.1(3)と FMT_MSA.3(3)につい

ては、FDP_IFC.1 および FDP_IFF.1 に係るｾｷｭﾘﾃｨ属性が対象である。

- FIA_UAU.2(1)、FIA_UAU.2[ENV](2)、FIA_UID.2(1)、FIA_UID.2(2)、および FIA_UID.2[ENV](3)については、表 8.5 のとおり、識別認証の目的と対象が異なる。さらに、OS の識別認証に適用される機能要件の動作に続け TOE の機能要件が動作する場合においても、両者の操作内容は整合している。
- FPT_ITT.1(1)および FPT_ITT.1[ENV](2)については、適用される場所が異なる。

表 8.5　識別認証に係る機能要件の関連

ﾛｸﾞｲﾝ先	OS に依存する SFR と操作内容		TOE の SFR と操作内容	
	SFR	操作内容	SFR	操作内容
運用管理ｻｰﾊﾞの TOE	FIA_UAU.2[ENV](2) FIA_UID.2[ENV](3)	TOE にﾛｸﾞｲﾝできる利用者を識別認証	FIA_UID.2(1)	運用管理者、運用担当者およびｼｽﾃﾑ管理者を識別
部門管理/業務各ｻｰﾊﾞの TOE	FIA_UAU.2[ENV](2) FIA_UID.2[ENV](3)	同上	FIA_UID.2(1)	運用管理者、運用担当者およびｼｽﾃﾑ管理者を識別
LiveHelp ｸﾗｲｱﾝﾄの TOE	FIA_UAU.2[ENV](2) FIA_UID.2[ENV](3)	同上		
			FIA_UAU.2(1) FIA_UID.2(2)	ﾘﾓｰﾄ操作を行う運用担当者を識別認証

8.2.2.　TOE セキュリティ機能要件間の依存関係

表 8.6 に、機能要件間の依存関係と、その依存関係に問題がないことの根拠を示す。

表 8.6　セキュリティ機能要件の依存関係

ｺﾝﾎﾟｰﾈﾝﾄ	依存関係	依存関係に問題がないことの根拠
FAU_GEN.1(1)	FPT_STM.1[ENV]	すべての依存関係を満たす。
FAU_GEN.1(2)	FPT_STM.1[ENV]	すべての依存関係を満たす。
FAU_SAR.1	FAU_GEN.1(1) FAU_GEN.1(2) FAU_GEN.1[ENV](3)	すべての依存関係を満たす。
FAU_STG.1	FAU_GEN.1(1) FAU_GEN.1(2) FAU_GEN.1[ENV](3)	すべての依存関係を満たす。
FAU_STG.3	FAU_STG.1	すべての依存関係を満たす。
FAU_STG.4	FAU_STG.1	すべての依存関係を満たす。

ｺﾝﾎﾟｰﾈﾝﾄ	依存関係	依存関係に問題がないことの根拠
FDP_ACC.1(1)	FDP_ACF.1(1)	すべての依存関係を満たす。
FDP_ACC.1(2)	FDP_ACF.1(2)	すべての依存関係を満たす。
FDP_ACF.1(1)	FDP_ACC.1(1) FMT_MSA.3(1)	すべての依存関係を満たす。
FDP_ACF.1(2)	FDP_ACC.1(2) FMT_MSA.3(2)	すべての依存関係を満たす。
FDP_IFC.1	FDP_IFF.1	すべての依存関係を満たす。
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3(3)	すべての依存関係を満たす。
FIA_AFL.1	FIA_UAU.2[ENV](2)	本来の依存関係は FIA_UAU.1 であるが、FIA_UAU.2 はその上位ｺﾝﾎﾟｰﾈﾝﾄである。
FIA_ATD.1		－
FIA_SOS.1		－
FIA_UAU.2(1)	FIA_UID.2(2)	本来の依存関係は FIA_UID.1 であるが、FIA_UID.2 はその上位ｺﾝﾎﾟｰﾈﾝﾄである。
FIA_UAU.6		－
FIA_UAU.7	FIA_UAU.2(1)	本来の依存関係は FIA_UAU.1 であるが、FIA_UAU.2 はその上位ｺﾝﾎﾟｰﾈﾝﾄである。
FIA_UID.2(1)		－
FIA_UID.2(2)		－
FIA_USB.1	FIA_ATD.1	すべての依存関係を満たす。
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たす。
FMT_MSA.1(1)	FDP_ACC.1(1) FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たす。
FMT_MSA.1(2)	FDP_ACC.1(2) FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たす。
FMT_MSA.1(3)	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たす。
FMT_MSA.3(1)	FMT_MSA.1(1)	当機能要件には許可された識別された役割はない。よって、CC が規定する FMT.SMR.1 に対する依存関係は不要である。
FMT_MSA.3(2)	FMT_MSA.1(2)	当機能要件には許可された識別された役割はない。よって、CC が規定する FMT.SMR.1 に対する依存関係は不要である。

ｺﾝﾎﾟｰﾈﾝﾄ	依存関係	依存関係に問題がないことの根拠
FMT_MSA.3(3)	FMT_MSA.1(3)	当機能要件には許可された識別された役割はない。よって、CC が規定する FMT.SMR.1 に対する依存関係は不要である。
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	すべての依存関係を満たす。
FMT_SMF.1		－
FMT_SMR.1	FIA_UID.2(1)	本来の依存関係は FIA_UID.1 であるが、FIA_UID.2 はその上位ｺﾝﾎﾟｰﾈﾝﾄである。
FPT_ITT.1(1)		－
FPT_RVM.1		－
FPT_SEP.1		－
FAU_GEN.1[ENV](3)	FPT_STM.1[ENV]	すべての依存関係を満たす。
FIA_UAU.2[ENV](2)	FIA_UID.2[ENV](3)	本来の依存関係は FIA_UID.1 であるが、FIA_UID.2 はその上位ｺﾝﾎﾟｰﾈﾝﾄである。
FIA_UID.2[ENV](3)		－
FPT_ITT.1[ENV](2)		－
FPT_STM.1[ENV]		－

表 8.6 のとおり、それぞれのセキュリティ機能要件は、依存関係のあるセキュリティ機能要件と相互補完している。CC に規定された依存関係を満たさないものについても、表中の根拠のとおり正当性を主張できる。

8.2.3. TOE セキュリティ機能要件の相互作用

セキュリティ機能要件の相互支援に関して、その内訳を表 8.7 に示す。

表 8.7 セキュリティ機能要件の相互支援

コンポーネント	迂回	無効化	非活性化	干渉・破壊
FAU_GEN.1(1)	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FAU_GEN.1(2)	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FAU_SAR.1	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FAU_STG.1	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FAU_STG.3	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FAU_STG.4	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FDP_ACC.1(1)	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FDP_ACC.1(2)	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FDP_ACF.1(1)	FPT_RVM.1	FAU_GEN.1(1) FAU_GEN.1(2)	N/A	FPT_SEP.1

コンポーネント	迂回	無効化	非活性化	干渉・破壊
FDP_ACF.1(2)	FPT_RVM.1	FAU_GEN.1(2)	FMT_MOF.1	FPT_SEP.1
FDP_IFC.1	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FDP_IFF.1	FPT_RVM.1	FAU_GEN.1(2)	FMT_MOF.1	FPT_SEP.1
FIA_AFL.1	FPT_RVM.1	FAU_GEN.1(2)	N/A	FPT_SEP.1
FIA_ATD.1	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FIA_SOS.1	FPT_RVM.1	FAU_GEN.1(2)	N/A	FPT_SEP.1
FIA_UAU.2(1)	FPT_RVM.1	FAU_GEN.1(2)	N/A	FPT_SEP.1
FIA_UAU.6	FPT_RVM.1	FAU_GEN.1(1)	FMT_MOF.1	FPT_SEP.1
FIA_UAU.7	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FIA_UID.2(1)	FPT_RVM.1	FAU_GEN.1(1)	N/A	FPT_SEP.1
FIA_UID.2(2)	FPT_RVM.1	FAU_GEN.1(2)	N/A	FPT_SEP.1
FIA_USB.1	FPT_RVM.1	FAU_GEN.1(1)	N/A	FPT_SEP.1
FMT_MOF.1	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FMT_MSA.1(1)	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FMT_MSA.1(2)	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FMT_MSA.1(3)	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FMT_MSA.3(1)	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FMT_MSA.3(2)	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FMT_MSA.3(3)	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FMT_MTD.1	FPT_RVM.1	N/A	FMT_MOF.1	FPT_SEP.1
FMT_SMF.1	FPT_RVM.1	FAU_GEN.1(2)	FMT_MOF.1	FPT_SEP.1
FMT_SMR.1	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FPT_ITT.1(1)	FPT_RVM.1	N/A	N/A	FPT_SEP.1
FPT_RVM.1		N/A	N/A	FPT_SEP.1
FPT_SEP.1		N/A	N/A	

注）N/A の意味は以下のとおり

- 無効化においては監査事象のないもの
- 非活性化においては非活性化させる管理機能のないもの

〔迂回〕

本 TOE は、FPT_RVM.1 の適用により、以下のとおりセキュリティ機能要件の迂回防止を実現する。

- FAU_GEN.1(1)、FAU_GEN.1(2)については、FPT_RVM.1 により、監査事象の発生を契機に必ず動作する保証を行うことで、迂回を防止する。同様に、FAU_STG.3 および FAU_STG.4 についても、監査ログ採取の処理の延長で必ず動作する保証を行うことで、迂回を防止する。

- FAU_SAR.1 および FAU_STG.1 については、FPT_RVM.1 により、OS による識別認証のためのセキュリティ機能要件である FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)に続け必ず動作する保証を行うことで、迂回を防止する。なお、呼び出されるパスが OS からのパスのみであることから、FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)は必ず動作する。
- FDP_ACC.1(1)、FDP_ACF.1(1)については、運用管理クライアントからの操作の場合、FPT_RVM.1 により、後述の FIA_UID.2(1)、FIA_UAU.6 に続けて、操作の都度必ず動作する保証を行うことで、迂回を防止する。
  コマンドによる操作の場合は、OS による識別認証のためのセキュリティ機能要件である FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)に続けて、操作の都度必ず動作する保証を行うことで、迂回を防止する。この場合、呼び出されるパスは OS からのパスのみであることから、FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)は常に必ず動作する。
- FDP_ACC.1(2)、FDP_ACF.1(2)については、FPT_RVM.1 により、後述の FIA_UID.2(1)、FIA_UAU.6 に続けて、操作の都度必ず動作する保証を行うことで、迂回を防止する。
- FDP_IFC.1 および FDP_IFF.1 については、FPT_RVM.1 により、配付資源の配付・適用の処理の延長で必ず動作する保証を行うことで、迂回を防止する。
- FIA_UID.2(1)、FIA_UAU.6 については、FPT_RVM.1 により、運用管理クライアントからのログインを受け付けた際、または TOE が提供するｺﾏﾝﾄﾞによる操作を受け付けた際、その延長で必ず動作する保証を行うことで、迂回を防止する。ただし、FIA_UAU.6 は前者の場合のみに該当。また、FIA_AFL.1、FIA_ATD.1、および FIA_USB.1 は、これらセキュリティ機能要件の前後で必ず動作し、他に呼び出しパスがないことから、迂回防止がなされる。
- FIA_UAU.2(1)、FIA_UID.2(2)については、FPT_RVM.1 により、パスワード認証方式によるリモート操作を行う際、運用管理クライアントからのリモート操作の開始を受け付けた延長で必ず動作する保証を行うことで迂回を防止する。また、FIA_SOS.1 および FIA_UAU.7 は、これらセキュリティ機能要件と共に動作し、他の呼び出しパスがないことから、迂回防止がなされる。
- FMT クラスのセキュリティ機能要件については、前述のとおり、FPT_RVM.1 を使って、OS による識別認証（FIA_UAU.2[ENV](2)および FIA_UID.2[ENV](3)）や、本 TOE による識別（FIA_UID.2(1)、FIA_UAU.6）に続けて、必ず動作することを保証することにより、迂回を防止する。
- FPT_ITT.1(1)については、FPT_RVM.1 により、クライアント上の TOE からサーバ上の TOE へのログイン処理の延長で必ず動作する保証を行うことで、迂回を防止する。

〔無効化〕

本 TOE は、FAU_GEN.1(1)および FAU_GEN.1(2)により、セキュリティ機能要件の実行に

係る事象を監査ログとして記録する。これにより、セキュリティ機能要件の無効化を狙った攻撃（不正な認証試行など）の検出を可能にすることで、セキュリティ機能要件の無効化に対抗する。

なお、CC で規定する FMT_SMR.1 の監査対象事象について、本 TOE は利用者のグループに対する管理機能を提供しておらず、監査対象事象は存在しないことから、監査ログは取得しない。

〔非活性化〕

本 TOE は、その振る舞いを外部から管理できるセキュリティ機能(F.CONSOLE_SECURITY、F.AUDIT_ACL、F.AUDIT_CMGR/CL(M)、および F.DEPLOY_SECURITY）に適用されるセキュリティ機能要件に対して、その振る舞いの管理を **FMT_MOF.1** により、システム管理者または必要なロールをもつ運用管理者に制限する。それにより、該当するセキュリティ機能要件が非活性化されることを防止する。

〔干渉・破壊〕

本 TOE にとって、信頼されないサブジェクトからの不正な干渉や改ざんには、本 TOE がサブジェクトに対して提供するインタフェースを使った不正な干渉や改ざんと、プロセスを跨いだ不正な干渉や改ざんの二つが想定される。

このため、本 TOE は前者に対して、サブジェクトに対して提供するインタフェースを実装する際、サブジェクトの役割に応じたインタフェース項目の明確化を行い、不正な干渉や改ざんにつながるインタフェースが作り込まれないようにすることで、**FPT_SEP.1** による TSF ドメイン分離を実現する。後者のプロセスを跨いだ不正な干渉や改ざんに対しては、本 TOE は OS 上で動作する製品であり、OS が提供する仮想空間の制御機能を使って防止する。

8.2.4.　最小機能強度根拠

本 ST が要求する TOE の保証レベルは EAL1 であり、その保証要件には AVA_SOF.1 を含まないため、最小機能強度については主張しない。

8.2.5.　セキュリティ保証要件根拠

本 TOE は商用システムで使用される製品であり、資産に対する本 TOE における保護については、独立した第三者による保証が望まれる。ただし、外部の者からの攻撃や公開された手段以外による攻撃は想定されないことから、本 TOE に対する保証要件としては、ガイダンスの検証および独立テストによる動作確認を主な要件とする EAL1 が適切である。

8.3.　TOE 要約仕様根拠

8.3.1.　TOE 要約仕様に対するセキュリティ機能要件の適合性

以下に、表 6.1 に示したセキュリティ機能とセキュリティ機能要件の対応について、そ

の対応が適合する根拠、および複数のセキュリティ機能の組合せが機能要件に適合する理由について示す。

〔FAU_GEN.1(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能に対して、監査ﾚﾍﾞﾙ「最小」で規定された監査対象事象、および個別に定義した ACL ﾏﾈｰｼﾞｬ機能におけるﾕｰｻﾞ名へのﾛｰﾙの登録と削除を行った事象に対する監査記録が取得可能であることを要求する。これに対して、F.AUDIT_ACL は、その起動と終了の監査ﾛｸﾞを取得すると共に、F.ACL_SECURITY の識別認証およびｺﾏﾝﾄﾞ操作に対するﾛｰﾙによるｱｸｾｽ制御機能に関して、一部の監査対象事象を除き、監査ﾚﾍﾞﾙ「最小」に合致する監査ﾛｸﾞ、および ACL ﾏﾈｰｼﾞｬ機能におけるﾕｰｻﾞ名へのﾛｰﾙの登録と削除を行った事象の監査ﾛｸﾞを常に取得可能（識別認証事象の監査ﾛｸﾞは OS の識別認証を呼び出した結果をもとに TOE で取得）である。記録する項目は、事象の日付／時刻、事象の種別としての操作内容、ｻﾌﾞｼﾞｪｸﾄ識別情報としての事象の契機となった操作を行ったﾕｰｻﾞ名、実行結果、そして事象の契機となった操作を行った運用管理ｸﾗｲｱﾝﾄのﾎｽﾄ名である。一部の監査対象事象についても、“8.2.3 TOE ｾｷｭﾘﾃｨ機能要件の相互作用”の“〔無効化〕”で示したとおり、監査記録を取得しないことの正当性を主張できる。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FAU_GEN.1(2)〕

本ｾｷｭﾘﾃｨ機能要件は、運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能に対して、監査ﾚﾍﾞﾙ「最小」で規定された監査対象事象に対する監査記録が取得可能であることを要求する。これに対して、F.AUDIT_CMGR/CL(M)は、運用管理ｸﾗｲｱﾝﾄからの操作に関して、一部の監査対象事象を除き、監査ﾚﾍﾞﾙ「最小」に合致する監査ﾛｸﾞを常に取得可能である。記録する項目は、事象の日付／時刻、事象の種別としての操作内容、ｻﾌﾞｼﾞｪｸﾄ識別情報としての事象の契機となった操作を行ったﾕｰｻﾞ名、実行結果、そして事象の契機となった操作を行った運用管理ｸﾗｲｱﾝﾄのﾎｽﾄ名である。一部の監査対象事象についても、“8.2.3 TOE ｾｷｭﾘﾃｨ機能要件の相互作用”の“〔無効化〕”で示したとおり、監査記録を取得しないことの正当性を主張できる。なお、F.AUDIT_CMGR/CL(M)の起動と終了の監査記録については、運用管理ｸﾗｲｱﾝﾄのｲﾍﾞﾝﾄﾛｸﾞに出力されるﾛｸﾞで代替している。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FAU_SAR.1〕

本ｾｷｭﾘﾃｨ機能要件は、ｼｽﾃﾑ管理者のみに監査記録の読み出しを許すと共に、解釈が容易な形式で監査記録が読み出せるようにすることを要求する。これに対して、F.AUDIT_ACL、F.AUDIT_CMGR/CL(M)は、監査ﾛｸﾞの読み出しをｼｽﾃﾑ管理者のみに許可する。そして、市販のﾂｰﾙを使って監査記録が閲覧できるよう一般に浸透しているﾃﾞｰﾀ形式である CSV 形式でﾛｸﾞを記録している。また、これらｾｷｭﾘﾃｨ機能は独立したｴﾝﾃｨﾃｨであり、単独で本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。よって、本ｾｷ

ｭﾘﾃｨ機能要件は満たされる。

〔FAU_STG.1〕

本ｾｷｭﾘﾃｨ機能要件は、監査記録に対して、不正な削除からの保護および改ざんの防止を行うことを要求する。これに対して、F.AUDIT_ACL、およびF.AUDIT_CMGR/CL(M)は、不正な削除からの保護および改ざんの防止を行うために、監査ﾛｸﾞﾌｧｲﾙに対するﾊﾟｰﾐｯｼｮﾝの設定を行う。さらに、監査ﾛｸﾞの出力先の変更が指示された場合についても、不正な削除からの保護および改ざんの防止を行うため、出力先の変更を行うｺﾏﾝﾄﾞの中で、変更後の出力先に対するﾊﾟｰﾐｯｼｮﾝの設定を行う。これらｾｷｭﾘﾃｨ機能は独立したｴﾝﾃｨﾃｨであり、単独で本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FAU_STG.3〕

本ｾｷｭﾘﾃｨ機能要件は、運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能に対して、監査記録の格納に際しﾃﾞｰﾀ消失の恐れがある場合には、保存日数が超過した監査ﾛｸﾞﾌｧｲﾙを削除することを要求する。これに対して、F.AUDIT_CMGR/CL(M)は、日単位で作成する監査ﾛｸﾞﾌｧｲﾙに保存日数を指定し、指定された保存日数を過ぎた監査ﾛｸﾞﾌｧｲﾙを削除することで監査ﾃﾞｰﾀ消失への対処としている。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FAU_STG.4〕

本ｾｷｭﾘﾃｨ機能要件は、ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能に対して、監査記録の格納に際しﾃﾞｰﾀ損失を防止するために、最も古く格納された監査記録への上書きの実施を要求する。監査格納失敗時にとられるその他のｱｸｼｮﾝは要求しない。これに対して、F.AUDIT_ACLは、監査事象の発生の都度監査ﾛｸﾞを記録するﾌｧｲﾙが満杯になった場合、そのﾌｧｲﾙの内容を退避したﾊﾞｯｸｱｯﾌﾟﾌｧｲﾙの中で最も古く退避されたﾊﾞｯｸｱｯﾌﾟﾌｧｲﾙに対して上書き退避を行うことで、監査ﾃﾞｰﾀの損失を防止する。また、監査格納失敗時にとる処理はない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FDP_ACC.1(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ｻﾌﾞｼﾞｪｸﾄ（TOE 利用者ﾌﾟﾛｾｽ）、ｵﾌﾞｼﾞｪｸﾄ（ﾒﾆｭｰとｺﾏﾝﾄﾞ）およびｻﾌﾞｼﾞｪｸﾄとｵﾌﾞｼﾞｪｸﾄ間の操作のﾘｽﾄ（実行）に対して、ACL ﾏﾈｰｼﾞｬｱｸｾｽ制御 SFP を実施することを要求する。これに対して、F.ACL_SECURITY は、ｻﾌﾞｼﾞｪｸﾄであるｼｽﾃﾑ管理者、運用管理者および運用担当者の各ﾌﾟﾛｾｽからのｵﾌﾞｼﾞｪｸﾄであるﾒﾆｭｰとｺﾏﾝﾄﾞの操作に対して、ACL ﾏﾈｰｼﾞｬｱｸｾｽ制御 SFP としての枠組みを定義し、それに基づくｱｸｾｽ制御を実施する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FDP_ACC.1(2)〕

本ｾｷｭﾘﾃｨ機能要件は、ｻﾌﾞｼﾞｪｸﾄ（TOE 利用者ﾌﾟﾛｾｽ）、ｵﾌﾞｼﾞｪｸﾄ（ﾒﾆｭｰ）およびｻﾌﾞｼﾞｪｸﾄとｵﾌﾞｼﾞｪｸﾄ間の操作のﾘｽﾄ（実行）に対して、ｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP を実施することを要求する。これに対して、F.CONSOLE_SECURITY は、ｻﾌﾞｼﾞｪｸﾄである運用担当者のﾌﾟﾛｾｽからのｵﾌﾞｼﾞｪｸﾄであるﾒﾆｭｰの操作に対して、ｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP としての枠

組みを定義し、それに基づくｱｸｾｽ制御を実施する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FDP_ACF.1(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ｾｷｭﾘﾃｨ属性（ﾛｰﾙおよび許可ﾛｰﾙ）によるｱｸｾｽ制御の適用を要求する。また、ｻﾌﾞｼﾞｪｸﾄであるｼｽﾃﾑ管理者ﾌﾟﾛｾｽからのｱｸｾｽを明示的に承認する追加規則の適用についても要求する。これに対して、F.ACL_SECURITY は、ｻﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性としてﾛｰﾙをもち、ｵﾌﾞｼﾞｪｸﾄであるﾒﾆｭｰとｺﾏﾝﾄﾞのｾｷｭﾘﾃｨ属性として許可ﾛｰﾙをもつ。そして、そのﾛｰﾙと許可ﾛｰﾙを使って、運用管理者と運用担当者のﾌﾟﾛｾｽからの操作に対するｱｸｾｽ制御を実施する。そして、ｾｷｭﾘﾃｨ機能要件で定義するｼｽﾃﾑ管理者ﾌﾟﾛｾｽからのｱｸｾｽを明示的に承認する規則に対しては、その規則のとおり、すべてのﾒﾆｭｰとすべてのｺﾏﾝﾄﾞの操作をｼｽﾃﾑ管理者に許可している。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FDP_ACF.1(2)〕

本ｾｷｭﾘﾃｨ機能要件は、ｾｷｭﾘﾃｨ属性（操作ﾚﾍﾞﾙおよび許可操作ﾚﾍﾞﾙ）によるｱｸｾｽ制御の適用を要求する。ｻﾌﾞｼﾞｪｸﾄのｱｸｾｽを明示的に承認または拒否するための追加規則は要求しない。これに対して、F.CONSOLE_SECURITY は、ｻﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性として操作ﾚﾍﾞﾙをもち、ｵﾌﾞｼﾞｪｸﾄであるﾒﾆｭｰのｾｷｭﾘﾃｨ属性として許可操作ﾚﾍﾞﾙをもつ。そして、その操作ﾚﾍﾞﾙと許可操作ﾚﾍﾞﾙを使ってﾒﾆｭｰのｱｸｾｽ制御を実施する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FDP_IFC.1〕

本ｾｷｭﾘﾃｨ機能要件は、ｻﾌﾞｼﾞｪｸﾄ（通知元の資源配付ﾌﾟﾛｾｽ）、情報（資源の配付・適用結果ﾃﾞｰﾀ）、および情報の流れを引き起こす操作（通知先の資源配付ﾌﾟﾛｾｽに送る）に対して、その情報ﾌﾛｰを制御するための資源配付結果通知ﾃﾞｰﾀ保護 SFP の実施を要求する。これに対して、F.DEPLOY_SECURITY は、ｻﾌﾞｼﾞｪｸﾄである通知元の資源配付ﾌﾟﾛｾｽが行う配付資源の配付と適用の結果ﾃﾞｰﾀの自動通知処理に対して、資源配付結果通知ﾃﾞｰﾀ保護 SFP としての枠組みを定義し、それに基づく資源の配付と適用結果ﾃﾞｰﾀの情報ﾌﾛｰ制御を実施する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FDP_IFF.1〕

本ｾｷｭﾘﾃｨ機能要件は、ｾｷｭﾘﾃｨ属性（通知先ｼｽﾃﾑ名）による情報ﾌﾛｰ制御の適用を要求する。また、追加の資源配付結果通知ﾃﾞｰﾀ保護 SFP 規則についても要求する。これに対して、F.DEPLOY_SECURITY は、通知元の資源配付ﾌﾟﾛｾｽが動作する業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞに登録された通知先ｼｽﾃﾑ名を情報ﾌﾛｰ制御のためのｾｷｭﾘﾃｨ属性として使用し、通知先の資源配付ﾌﾟﾛｾｽが動作する運用管理ｻｰﾊﾞへの資源の配付・適用結果ﾃﾞｰﾀの自動通知処理の情報ﾌﾛｰ制御を実施する。また、ｾｷｭﾘﾃｨ機能要件が要求する追加の規則に対しては、その要求のとおり、業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞの当機能は、配下の業務ｸﾗｲｱﾝﾄの適用結果も含めて通知を行い、業務ｸﾗｲｱﾝﾄの当機能は、配付資源のﾀﾞｳﾝﾛｰﾄﾞを行った業務ｻｰﾊﾞまたは部門管理ｻｰﾊﾞを通知先として適用結果を通知する。よって、本ｾｷｭﾘﾃｨ機能要件は

満たされる。

〔FIA_AFL.1〕

本ｾｷｭﾘﾃｨ機能要件は、運用管理ｸﾗｲｱﾝﾄから運用管理ｻｰﾊﾞへのﾛｸﾞｲﾝ（Systemwalker ｺﾝｿｰﾙ機能利用時）の試行回数が 3 回を越えた場合、いったんﾛｸﾞｲﾝ画面を閉じ認証処理を終了することを要求する。これに対して、F.ACL_SECURITY は、運用管理ｸﾗｲｱﾝﾄから運用管理ｻｰﾊﾞにﾛｸﾞｲﾝ（Systemwalker ｺﾝｿｰﾙ機能利用時）する際、ﾊﾟｽﾜｰﾄﾞの不当などによりﾛｸﾞｲﾝ操作が連続して 3 回失敗した場合、ﾛｸﾞｲﾝ画面を閉じてﾛｸﾞｲﾝ処理を終了し、ﾛｸﾞｲﾝ操作が不正に繰り返されないようにする。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_ATD.1〕

本ｾｷｭﾘﾃｨ機能要件は、利用者に属するｾｷｭﾘﾃｨ属性のﾘｽﾄ（ﾛｰﾙ、操作ﾚﾍﾞﾙ）を維持することを要求する。これに対して、F.ACL_SECURITY は、運用管理者および運用担当者を表すﾕｰｻﾞ名に登録されたﾛｰﾙをｾｷｭﾘﾃｨ属性として維持管理する。同様に、F.CONSOLE_SECURITY は、そのﾕｰｻﾞ名に登録された操作ﾚﾍﾞﾙをｾｷｭﾘﾃｨ属性として維持管理する。これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、以下のとおり、単独で本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。

- F.CONSOLE_SECURITY の停止時、運用管理者および運用担当者に対して実際に維持されるｾｷｭﾘﾃｨ属性はﾛｰﾙのみであり、ACL_SECURITY がその維持を行う。
- F.CONSOLE_SECURITY の起動時、ﾛｰﾙに加えて操作ﾚﾍﾞﾙが実際にｾｷｭﾘﾃｨ属性として維持される。F.ACL_SECURITY がﾛｰﾙの維持を、F.CONSOLE_SECURITY が操作ﾚﾍﾞﾙの維持を各々行う。

よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_SOS.1〕

本ｾｷｭﾘﾃｨ機能要件は、ﾊﾟｽﾜｰﾄﾞが定義された品質尺度に合致することを検証するﾒｶﾆｽﾞﾑの提供が要求する。これに対して、F.LIVEHELP_SECURITY は、ﾊﾟｽﾜｰﾄﾞ認証方式を利用する場合、新規ﾊﾟｽﾜｰﾄﾞとして、7 文字以上、半角 16 文字以内のﾊﾟｽﾜｰﾄﾞ設定を求める。また、大文字、小文字、数字、空白、およびﾀﾞﾌﾞﾙｸｫｰﾃｰｼｮﾝ（”）を除く特殊文字の使用を許す。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_UAU.2(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ﾘﾓｰﾄ操作を行う運用担当者を代行する他の TSF 調停ｱｸｼｮﾝを許可するまえに、各利用者に認証が成功することを要求する。これに対して、F.LIVEHELP_SECURITY は、ﾊﾟｽﾜｰﾄﾞ認証方式を利用する場合、ﾘﾓｰﾄ操作の利用を許可する前に、ﾘﾓｰﾄ操作を行う運用担当者に対して利用者の認証を行う。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_UAU.6〕

本ｾｷｭﾘﾃｨ機能要件は、ｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間が切れた場合に、該当する利用者に対して再認証を要求する。これに対して、F.CONSOLE_SECURITY は、有

効期間の監視を行い、有効期間が切れた場合には、該当する利用者に対する再認証を要求する。その結果、該当する利用者が次の操作を行おうとする際、F.ACL_SECURITY によって利用者の識別認証が行われる。F.ACL_SECURITY は必ず動作する機能であり、また、F.CONSOLE_SECURITY を利用するためには運用管理ｸﾗｲｱﾝﾄでの識別認証が必須であることから、F.ACL_SECURITY による利用者の識別認証は必ず動作する。迂回されることはない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_UAU.7〕

本ｾｷｭﾘﾃｨ機能要件は、認証を行っている間、ﾘﾓｰﾄ操作を行う運用担当者に対しては、ｱｽﾀﾘｽｸに置き換えたﾊﾟｽﾜｰﾄﾞ文字列のみを提供するよう要求する。これに対して、F.LIVEHELP_SECURITY は、ﾊﾟｽﾜｰﾄﾞ認証方式を利用する場合、入力されたﾊﾟｽﾜｰﾄﾞ文字列をｱｽﾀﾘｽｸ（“＊”）に置き換え、それのみをﾘﾓｰﾄ操作を行う運用担当者に表示することで、認証時ﾌｨｰﾄﾞﾊﾞｯｸの保護を行う。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_UID.2(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ｼｽﾃﾑ管理者、運用管理者、または運用担当者を代行する他の TSF 調停ｱｸｼｮﾝを許可する前に、各利用者に自分自身を識別することを要求する。これに対して、F.ACL_SECURITY は、ｼｽﾃﾑ管理者、運用管理者および運用担当者に対する識別を行う。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_UID.2(2)〕

本ｾｷｭﾘﾃｨ機能要件は、ﾘﾓｰﾄ操作を行う運用担当者を代行する他の TSF 調停ｱｸｼｮﾝを許可するまえに、各利用者に自分自身を識別することを要求する。これに対して、F.LIVEHELP_SECURITY は、ﾊﾟｽﾜｰﾄﾞ認証方式を利用する場合、ﾘﾓｰﾄ操作の利用を許可する前に、ﾘﾓｰﾄ操作を行う運用担当者に対して利用者の識別を行う。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FIA_USB.1〕

本ｾｷｭﾘﾃｨ機能要件は、利用者とｻﾌﾞｼﾞｪｸﾄの結合に際して、適切なｾｷｭﾘﾃｨ属性（ﾛｰﾙ、操作ﾚﾍﾞﾙ）を、利用者識別が完了した時点でその利用者を代行するｻﾌﾞｼﾞｪｸﾄに関連付けること、および関連付けたｾｷｭﾘﾃｨ属性の変更管理に関する規則はないことを要求する。これに対して、F.ACL_SECURITY は、運用管理者および運用担当者の識別が完了した時点で、ｾｷｭﾘﾃｨ属性としてﾛｰﾙをｻﾌﾞｼﾞｪｸﾄに関係付ける。同様に、F.CONSOLE_SECURITY は、ｾｷｭﾘﾃｨ属性として操作ﾚﾍﾞﾙをｻﾌﾞｼﾞｪｸﾄに関係付ける。また、これらｾｷｭﾘﾃｨ機能は、関連付けたｾｷｭﾘﾃｨ属性を変更する機能は提供していない。これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、以下のとおり、単独で本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。

- F.CONSOLE_SECURITY の停止時、運用管理者および運用担当者に実際に関連付けられるｾｷｭﾘﾃｨ属性はﾛｰﾙのみであり、ACL_SECURITY がその関連付けを行う。
- F.CONSOLE_SECURITY の起動時、ﾛｰﾙに加えて操作ﾚﾍﾞﾙが実際にｾｷｭﾘﾃｨ属性として関

連付けられる。ACL_SECURITY がﾛｰﾙの関連付けを、F.CONSOLE_SECURITY が操作ﾚﾍﾞﾙの関連付けを各々行う。

よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MOF.1〕

本ｾｷｭﾘﾃｨ機能要件は、ｺﾝｿｰﾙ操作制御機能、適用結果の自動通知機能、ACL ﾏﾈｰｼﾞｬ機能の監査ﾛｸﾞ機能、および運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能について、その機能を起動・停止する能力をｼｽﾃﾑ管理者（すべての機能に対して）、および DistributionAdmin ﾛｰﾙをもつ運用管理者（適用結果の自動通知機能に対してのみ）のみに提供することを要求する。これに対して、F.CONSOLE_SECURITY、F.DEPLOY_SECURITY、F.AUDIT_ACL、および F.AUDIT_CMGR/CL(M)は、各々の機能の起動／停止を行う能力をｼｽﾃﾑ管理者のみに許可（F.DEPLOY_SECURITY については、DistributionAdmin ロールをもつ運用管理者にも許可）する。これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、単独で本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MSA.1(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ACL ﾏﾈｰｼﾞｬｱｸｾｽ制御 SFP で定義するｾｷｭﾘﾃｨ属性の中で、ﾛｰﾙの登録と削除をｼｽﾃﾑ管理者、DmAdmin ﾛｰﾙをもつ運用管理者、および DistributionAdmin ﾛｰﾙをもつ運用管理者に制限することを要求する。これに対して、F.ACL_SECURITY は、ﾛｰﾙの登録と削除をｼｽﾃﾑ管理者および必要なﾛｰﾙ（DmAdmin または DistributionAdmin）をもつ運用管理者に制限する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MSA.1(2)〕

本ｾｷｭﾘﾃｨ機能要件は、ｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP で定義するｾｷｭﾘﾃｨ属性の中で、操作ﾚﾍﾞﾙおよび許可操作ﾚﾍﾞﾙの登録と削除をｼｽﾃﾑ管理者のみに制限することを要求する。これに対して、F.CONSOLE_SECURITY は、操作ﾚﾍﾞﾙおよび許可操作ﾚﾍﾞﾙの登録と削除をｼｽﾃﾑ管理者に制限する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MSA.1(3)〕

本ｾｷｭﾘﾃｨ機能要件は、資源配付結果通知情報ﾌﾛｰ制御 SFP で定義するｾｷｭﾘﾃｨ属性（通知先ｼｽﾃﾑ名）の登録、改変、削除をｼｽﾃﾑ管理者、および DistributionAdmin ﾛｰﾙをもつ運用管理者のみに制限することを要求する。これに対して、F.DEPLOY_SECURITY は、通知先ｼｽﾃﾑ名の登録、改変、削除をｼｽﾃﾑ管理者、および DistributionAdmin ﾛｰﾙをもつ運用管理者のみに制限する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MSA.3(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ACL ﾏﾈｰｼﾞｬｱｸｾｽ制御 SFP で定義するｵﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性（許可ﾛｰﾙ）に、制限的なﾃﾞﾌｫﾙﾄ値を与えることを要求する。また、ｵﾌﾞｼﾞｪｸﾄや情報が生成される際、ﾃﾞﾌｫﾙﾄ値を上書きする代替の初期値を指定する許可された識別された役割はないことを要求する。これに対して、F.ACL_SECURITY は、ﾛｰﾙが登録されていない者からの

ﾛｸﾞｲﾝを拒否する（ｼｽﾃﾑ管理者についてはすべてのﾛｰﾙが登録されているものとみなす）。これにより、ｵﾌﾞｼﾞｪｸﾄを操作する際はｻﾌﾞｼﾞｪｸﾄに対するﾛｰﾙの登録を必須にすることで、ｵﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性に対し制限的なﾃﾞﾌｫﾙﾄ値を与える。また、許可ﾛｰﾙは TOE で固定であり、当機能は追加や削除を行う機能を用意しないことから、ｾｷｭﾘﾃｨ機能要件が要求するとおり、ﾃﾞﾌｫﾙﾄ値を上書きする代替の初期値を指定する許可された識別された役割はない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MSA.3(2)〕

本ｾｷｭﾘﾃｨ機能要件は、ｺﾝｿｰﾙ操作制御ｱｸｾｽ制御 SFP で定義するｵﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性（許可操作ﾚﾍﾞﾙ）に、制限的なﾃﾞﾌｫﾙﾄ値を与えることを要求する。また、ｵﾌﾞｼﾞｪｸﾄや情報が生成される際、ﾃﾞﾌｫﾙﾄ値を上書きする代替の初期値を指定する許可された識別された役割はないことを要求する。これに対して、F.CONSOLE_SECURITY は、その機能を利用する場合、許可操作ﾚﾍﾞﾙを登録するためのｺﾝｿｰﾙ操作制御条件ﾌｧｲﾙの定義を必須とすることで、ｵﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性に対し制限的なﾃﾞﾌｫﾙﾄ値を与える。また、許可操作ﾚﾍﾞﾙを登録するためのｺﾝｿｰﾙ操作制御条件ﾌｧｲﾙのﾃﾞﾌｫﾙﾄはないことから、ｾｷｭﾘﾃｨ機能要件が要求するとおり、ﾃﾞﾌｫﾙﾄ値を上書きする代替の初期値を指定する許可された識別された役割はない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MSA.3(3)〕

本ｾｷｭﾘﾃｨ機能要件は、資源配付結果通知情報ﾌﾛｰ制御 SFP で定義するｾｷｭﾘﾃｨ属性（通知先ｼｽﾃﾑ名）に、制限的なﾃﾞﾌｫﾙﾄ値を与えることを要求する。また、ｵﾌﾞｼﾞｪｸﾄや情報が生成される際、ﾃﾞﾌｫﾙﾄ値を上書きする代替の初期値を指定する許可された識別された役割はないことを要求する。これに対して、F.DEPLOY_SECURITY は、その機能を利用する場合、通知先ｼｽﾃﾑの定義を必須とすることで、ｵﾌﾞｼﾞｪｸﾄのｾｷｭﾘﾃｨ属性に対し制限的なﾃﾞﾌｫﾙﾄ値を与える。また、通知先ｼｽﾃﾑの定義にはﾃﾞﾌｫﾙﾄがないことから、ｾｷｭﾘﾃｨ機能要件が要求するとおり、ﾃﾞﾌｫﾙﾄ値を上書きする代替の初期値を指定する許可された識別された役割はない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_MTD.1〕

本ｾｷｭﾘﾃｨ機能要件は、運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能における監査ﾛｸﾞﾌｧｲﾙの保存日数、ｺﾝｿｰﾙ操作制御機能の利用形態の選択情報、およびｺﾝｿｰﾙ操作制御機能におけるﾕｰｻﾞ名の有効期間の各 TSF ﾃﾞｰﾀの改変をｼｽﾃﾑ管理者のみに制限することを要求する。これに対して、本 TOE のｾｷｭﾘﾃｨ機能は以下のとおり制限を行う。

- F.CONSOLE_SECURITY は、ｺﾝｿｰﾙ操作制御機能の利用形態の選択情報、およびｺﾝｿｰﾙ操作制御におけるﾕｰｻﾞ名の有効期間の改変をｼｽﾃﾑ管理者に制限する。
- F.AUDIT_CMGR/CL(M)は、運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能における監査ﾛｸﾞﾌｧｲﾙの保存日数の改変をｼｽﾃﾑ管理者に制限する。

なお、これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、単独で本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_SMF.1〕

本ｾｷｭﾘﾃｨ機能要件は、ｾｷｭﾘﾃｨ管理機能を行う能力を要求する。これに対して、以下のとおり、各ｾｷｭﾘﾃｨ機能は必要なｾｷｭﾘﾃｨ管理機能を提供する。

- F.ACL_SECURITY は、FDP_ACF.1(1)に対して、ｱｸｾｽ制御に係る属性（ﾛｰﾙ）の維持管理機能を提供する。
- F.CONSOLE_SECURITY は、FDP_ACF.1(2)に対して、ｱｸｾｽ制御に係る属性（操作ﾚﾍﾞﾙ、許可操作ﾚﾍﾞﾙ）の維持管理機能を提供し、FIA_UAU.6 に対して、再認証の決定に使用するﾕｰｻﾞ名の有効期間満了を管理する機能を提供する。そして、FMT_MOF.1 が示す当ｾｷｭﾘﾃｨ機能の起動と停止を管理する機能を提供する。
- F.DEPLOY_SECURITY は、FDP_IFF.1 に対して、情報ﾌﾛｰ制御に係る属性（通知先ｼｽﾃﾑ名）の維持管理機能を提供する。そして、FMT_MOF.1 が示す当ｾｷｭﾘﾃｨ機能の起動と停止を管理する機能を提供する。
- F.AUDIT_ACL は、FMT_MOF.1 が示す当ｾｷｭﾘﾃｨ機能の起動と停止を管理する機能を提供する。
- F.AUDIT_CMGR/CL(M)は、FAU_STG.3 に対して、運用管理ｸﾗｲｱﾝﾄ操作の監査ﾛｸﾞ機能における保存日数の管理機能を提供する。そして、FMT_MOF.1 が示す当ｾｷｭﾘﾃｨ機能の起動と停止を管理する機能を提供する。

これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、それぞれが提供する管理機能に関連する機能要件については、その根拠に示したとおり、その要求事項はｾｷｭﾘﾃｨ機能毎独立している。FIA_UAU.6 の根拠には F.ACL_SECURITY が示されているが、F.CONSOLE_SECURITY からの要求を受けて再認証を行うだけであり、管理機能に係わることはない。よって、これらｾｷｭﾘﾃｨ機能は単独で本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。また、他のｾｷｭﾘﾃｨ機能要件については管理すべきｾｷｭﾘﾃｨ管理機能がない。以上のことから、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FMT_SMR.1〕

本ｾｷｭﾘﾃｨ機能要件は、許可された識別された役割であるｼｽﾃﾑ管理者、および運用管理者の各役割について、その維持と利用者への関連付けを行うことを要求する。これに対して、F.ACL_SECURITY、F.CONSOLE_SECURITY、F.AUDIT_ACL、F.AUDIT_CMGR/CL(M)、および F.DEPLOY_SECURITY は、ｼｽﾃﾑ管理者および運用管理者の各役割について、役割と許可される操作との対応を維持すると共に、利用者の識別結果に基づく役割への関連付けを行う。これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、単独に本ｾｷｭﾘﾃｨ機能要件を実現する。組み合わされて動作することはない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FPT_ITT.1(1)〕

本ｾｷｭﾘﾃｨ機能要件は、ｻｰﾊﾞ上の TOE にﾛｸﾞｲﾝするためのﾊﾟｽﾜｰﾄﾞが TOE の別々のﾊﾟｰﾂ間で送られる場合、そのﾊﾟｽﾜｰﾄﾞを暴露から保護することを要求する。これに対して、F.PWD_SECURITY は、運用管理ｸﾗｲｱﾝﾄまたは業務ｸﾗｲｱﾝﾄの本 TOE を使って、運用管理ｻｰﾊﾞ、

部門管理ｻｰﾊﾞまたは業務ｻｰﾊﾞの本 TOE にﾛｸﾞｲﾝする際、そのﾊﾟｽﾜｰﾄﾞを本 TOE 独自のﾒｶﾆｽﾞﾑによりを異なるﾃﾞｰﾀに変換することで、解読され暴露されることがないよう保護する。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FPT_RVM.1〕

本ｾｷｭﾘﾃｨ機能要件は、ｾｷｭﾘﾃｨ機能が必ず動作することを要求する。これに対して、F.PWD_SECURITY は、利用者が本 TOE にﾛｸﾞｲﾝする際に必ず動作する。F.ACL_SECURITY、および F.CONSOLE_SECURITY は、本 TOE の利用者がﾛｸﾞｲﾝする際、ならびに操作を行う際に必ず動作する。F.LIVEHELP_SECURITY は、ﾘﾓｰﾄ操作を行う者が LiveHelp ｸﾗｲｱﾝﾄに対してﾘﾓｰﾄ操作を開始する際に必ず動作する。F.AUDIT_ACL、および F.AUDIT_CMGR/CL(M)は、監査ﾛｸﾞが採取される際に必ず動作する。そして、F.DEPLOY_SECURITY は、配付資源の配付および適用の際に必ず動作する。これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、単独で本ｾｷｭﾘﾃｨ機能要件を満足する。組み合わされて動作することはない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

〔FPT_SEP.1〕

本ｾｷｭﾘﾃｨ機能要件は、ｾｷｭﾘﾃｨ機能が信頼されないｻﾌﾞｼﾞｪｸﾄからの干渉や改ざんをうけないことを要求する。これに対して、F.ACL_SECURITY、F.CONSOLE_SECURITY、F.LIVEHELP_SECURITY、F.AUDIT_ACL、F.AUDIT_CMGR/CL(M)、F.DEPLOY_SECURITY、および F.PWD_SECURITY は、各機能が TOE の関連者に対して提供するｲﾝﾀﾌｪｰｽについて、その役割に応じたｲﾝﾀﾌｪｰｽ項目を明確化することで、不正な干渉や改ざんにつながるｲﾝﾀﾌｪｰｽが作り込まれない実装を行っている。これらｾｷｭﾘﾃｨ機能は各々独立したｴﾝﾃｨﾃｨであり、単独で本ｾｷｭﾘﾃｨ機能要件を満足する。組み合わされて動作することはない。よって、本ｾｷｭﾘﾃｨ機能要件は満たされる。

8.3.2. セキュリティ機能強度根拠

本 TOE の保証レベルは EAL1 であり、セキュリティ機能強度は主張していない。

8.3.3. 保証手段根拠

本 TOE に対する TOE セキュリティ保証要件は、“6.5 保証手段”に示したドキュメントのセットにより対応付けられる。

ACM_CAP.1　　バージョン番号

【保証手段】

・ TOE バージョンの表示

【保証要件根拠】

「TOE バージョンの表示」により、TOE の購入者に対し、TOE を一意にリファレンスする手段を提供する。そのため、保証要件 ACM_CAP.1 は満たされる。

ADO_IGS.1　　設置、生成、及び立上げ手順

【保証手段】

・ Systemwalker Centric Manager 解説書　-UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 導入手引書　-UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 全体監視適用ガイド -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager V13.2.0 正誤表

【保証要件根拠】

保証手段に示した資料には、本 TOE をセキュアな構成にするために採用される設置手順、生成手順および起動の確認方法を規定する。そのため、保証要件 ADO_IGS.1 は満たされる。

ADV_FSP.1　　非形式的機能仕様

【保証手段】

・ Systemwalker Centric Manager V13.2.0 セキュリティ機能仕様書

【保証要件根拠】

保証手段に示した資料には、本 TOE のセキュリティ機能とその外部インタフェースの仕様を規定する。そのため、保証要件 ADV_FSP.1 は満たされる。

ADV_RCR.1　　非形式的対応の実証

【保証手段】

・ Systemwalker Centric Manager V13.2.0 表現対応表

【保証要件根拠】

保証手段である「Systemwalker Centric Manager V13.2.0 表現対応表」には、本 TOE のセキュリティ機能の各レベル（要約仕様－機能仕様）での完全な対応を記述する。そのため、保証要件 ADV_RCR.1 は満たされる。

AGD_ADM.1　　管理者ガイダンス

【保証手段】

・ Systemwalker Centric Manager 解説書 -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager ｿﾘｭｰｼｮﾝｶﾞｲﾄﾞ ｾｷｭﾘﾃｨ編 -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 導入手引書　-UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 使用手引書 監視機能編 -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 使用手引書 資源配付機能編 -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 使用手引書 ｿﾌﾄｳｪｱ修正管理機能編 -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 使用手引書 ﾘﾓｰﾄ操作機能編ﾕｰｻﾞｰｽﾞｶﾞｲﾄﾞ -Microsoft(R) Windows(R) 2000 / Microsoft(R) Windows(R) XP / Microsoft(R) Windows Server 2003 STD / Microsoft(R) Windows(R) Server2003 EE / Microsoft(R) Windows(R) Vista-

・ Systemwalker Centric Manager 使用手引書 ﾘﾓｰﾄ操作機能編 Clientｶﾞｲﾄﾞ -Microsoft(R) Windows(R) 2000 / Microsoft(R) Windows(R) XP / Microsoft(R) Windows Server 2003 STD / Microsoft(R) Windows(R) Server2003 EE / Microsoft(R) Windows(R) Vista-
・ Systemwalker Centric Manager ﾘﾌｧﾚﾝｽﾏﾆｭｱﾙ -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager ﾒｯｾｰｼﾞ説明書 -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager 全体監視適用ガイド -UNIX/Windows(R)共通-
・ Systemwalker Centric Manager/Systemwalker Event Agent ﾄﾗﾌﾞﾙｼｭｰﾃｨﾝｸﾞｶﾞｲﾄﾞ監視機能編/ｿﾌﾄｳｪｱ修正管理機能編 -UNIX 共通- -Microsoft(R) Windows NT(R)/ Microsoft(R) Windows(R)2000/ Microsoft(R) Windows Server(TM) 2003-
・ Systemwalker Centric Manager ﾄﾗﾌﾞﾙｼｭｰﾃｨﾝｸﾞｶﾞｲﾄﾞ 資源配付機能編/Systemwalker Software Delivery ﾄﾗﾌﾞﾙｼｭｰﾃｨﾝｸﾞｶﾞｲﾄﾞ -UNIX 共通- -Microsoft(R) Windows NT(R)/ Microsoft(R)Windows(R) 2000/ Microsoft(R) Windows Server(TM) 2003-
・ Systemwalker Centric Manager ﾍﾙﾌﾟ
・ 資源配付のﾍﾙﾌﾟ（ﾛｸﾞｲﾝ画面用ﾍﾙﾌﾟとそれ以外の画面用ﾍﾙﾌﾟ）
・ 資源配付環境設定のﾍﾙﾌﾟ
・ Systemwalker Centric Manager V13.2.0 正誤表

【保証要件根拠】

保証手段に示した資料には、本 TOE の管理者が使用するインタフェース、本 TOE をセキュアに運用するための警告を含む使用方法、及び本 TOE の障害時に管理者が採るべきアクションについて規定する。そのため、保証要件 AGD_ADM.1 は満たされる。

AGD_USR.1　　利用者ガイダンス

【保証手段】

・ AGD_ADM.1 に対する保証手段と同じ

【保証要件根拠】

保証手段に示した資料には、本 TOE の利用者が使用するインタフェース、および本 TOE のセキュアな運用のための警告を含む使用方法を規定する。そのため、保証要件 AGD_USR.1 は満たされる。

ATE_IND.1　　独立テスト － 準拠

【保証手段】

・ テストに適した TOE

【保証要件根拠】

テストに適した TOE を提供する。そのため、ATE_IND.1 は満たされる。

8.4.　PP 主張根拠

本 ST が参照する PP はない。

以上