WebSAM SystemManager Ver5.2.1
セキュリティターゲット

バージョン: 1.10

2008 年 9 月 25 日

日本電気株式会社

更新履歴

バージョン	変更概要	変更箇所		変更日	変更者
		章・節・項	内容		
1.0	初版	-	-	2008/05/20	日本電気株式会社
1.01	指摘事項の反映	1.4.4	アクセス制御機能が監視端末経由のアクセスのみを対象にする旨を追加	2008/06/03	日本電気株式会社
		用語集	履歴情報の表現を修正	2008/06/03	日本電気株式会社
		1.4.3 1.4.4 5.1.1 6.1	履歴情報制御テーブル、オーディットログ情報制御テーブルに関する記述を削除	2008/06/05	日本電気株式会社
		5.1.1 6.1	各種テーブルへの操作がレコードについての物である旨を追加	2008/06/05	日本電気株式会社
		5.1.3 6.12	ユーザ情報管理者の権限付与に関する記述を追加	2008/06/09	日本電気株式会社
		3.1	OE.AUTHORIZATION_SETTINGに、ユーザ情報管理者が信頼できる旨を追加	2008/06/10	日本電気株式会社
1.02	指摘事項の反映	1.4.1	表 2 の注釈に、役割がグループにより実現される旨を追加	2008/06/23	日本電気株式会社
		5.1.1	表 8 の項目の表現を修正	2008/06/23	日本電気株式会社
		5.1.1	表 8 の注釈に、参照権限が全ての利用者に付与される旨を追加	2008/06/23	日本電気株式会社
		5.1.3	表 11 の項目に管理要件の列を追加	2008/06/23	日本電気株式会社
		5.1.3	表 11 の項目の記述内容を修正	2008/06/23	日本電気株式会社
		5.1.3	表 12 を削除	2008/06/23	日本電気株式会社
1.03	指摘事項の反映	1.4.4	記載内容の詳細化	2008/06/26	日本電気株式会社
		1.3.3	検証環境について追加	2008/06/27	日本電気株式会社

バージョン	変更概要	変更箇所		変更日	変更者
		章・節・項	内容		
		1.4.3	監視端末経由のアクセスのみを対象にする旨の記述を1.4.4から移動	2008/06/27	日本電気株式会社
1.04	指摘事項の反映	全般	アクセス制御に関する参照権限の記述を削除	2008/07/17	日本電気株式会社
		6.1	文書表現の修正	2008/07/17	日本電気株式会社
		5.1.2 5.1.3 6.7	権限変更反映時期について追記	2008/07/22	日本電気株式会社
1.05	指摘事項の反映	5.1.2 5.1.3 6.7 6.11	権限変更反映時期について修正	2008/07/29	日本電気株式会社
1.06	指摘事項の反映	1.2 1.4.2.3	TOEのバージョン表記について追記	2008/08/11	日本電気株式会社
1.07	指摘事項の反映	6.1	参照権限の振る舞いについて追記	2008/08/18	日本電気株式会社
1.08	ガイダンスのバージョンを修正	1.4.2.4	ガイダンスのバージョンを修正	2008/09/11	日本電気株式会社
1.09	指摘事項の反映	1.3.2	表現を修正	2008/09/18	日本電気株式会社
		1.4.2.4	ガイダンスのバージョンを修正	2008/09/18	日本電気株式会社
1.10	指摘事項の反映	1.2 1.4.2.3	TOEのバージョン表記について補足	2008/09/25	日本電気株式会社
		1.4.2.4	ガイダンスのバージョンを修正	2008/09/25	日本電気株式会社

目次

更新履歴 i
目次 iii
参考資料 v
用語・略語 vi
1. ST概説 1
1.1. ST参照 1
1.2. TOE参照 1
1.3. TOE概要 1
1.3.1. TOE種別 1
1.3.2. 主要なセキュリティ機能 1
1.3.3. TOEの動作環境 2
1.4. TOE記述 4
1.4.1. TOE関連の役割定義 4
1.4.2. TOEの物理的範囲 5
1.4.3. TOEの論理的範囲 8
1.4.4. TOEのセキュリティ機能 11
2. 適合主張 12
2.1. CC適合主張 12
2.2. PP主張 12
2.3. パッケージ主張 12
2.4. 適合根拠 12
3. セキュリティ対策方針 13
3.1. 運用環境のセキュリティ対策方針 13
4. 拡張コンポーネント定義 14
5. セキュリティ要件 15
5.1. セキュリティ機能要件 15
5.1.1. FDPクラス:利用者データ保護 15
5.1.2. FIAクラス:識別と認証 18
5.1.3. FMTクラス:セキュリティ管理 20
5.2. セキュリティ保証要件 24
5.2.1. ASEクラス :セキュリティターゲット評価 24
5.2.2. ADVクラス: 開発 24
5.2.3. AGDクラス :ガイダンス文書 25
5.2.4. ALCクラス :ライフサイクルサポート 25
5.2.5. ATEクラス :テスト 25
5.2.6. AVAクラス :脆弱性評定 25
5.3. セキュリティ要件根拠 25
6. TOE要約仕様 26
6.1. FDP_ACC.1、FDP_ACF.1 26
6.2. FIA_ATD.1 28
6.3. FIA_SOS.1 28
6.4. FIA_UAU.1 28
6.5. FIA_UAU.7 28

6.6. FIA_UID.1 28
6.7. FIA_USB.1 28
6.8. FMT_MSA.1 28
6.9. FMT_MSA.3 29
6.10. FMT_MTD.1 29
6.11. FMT_SMF.1 29
6.12. FMT_SMR1 30

参考資料

本 ST における参考資料は以下の通りである。

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

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

・Common Criteria for Information Technology Security Evaluation Part 3:
Security assurance components September 2006 Version 3.1 Revision 1
CCMB-2006-09-003

・Common Methodology for Information Technology Security Evaluation
Evaluation Methodology September 2006 Version 3.1 Revision 1
CCMB-2006-09-004

・情報技術セキュリティ評価のためのコモンクライテリア
パート 1:概説と一般モデル
2006 年 9 月 バージョン 3.1 改定第 1 版 CCMB-2006-09-001
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

・情報技術セキュリティ評価のためのコモンクライテリア
パート 2:セキュリティ機能コンポーネント
2006 年 9 月 バージョン 3.1 改定第1版 CCMB-2006-09-002
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

・情報技術セキュリティ評価のためのコモンクライテリア
パート 3:セキュリティ保証コンポーネント
2006 年 9 月 バージョン 3.1 改定第 1 版 CCMB-2006-09-003
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

・情報技術セキュリティ評価のための共通方法
評価方法 2006 年 9 月 バージョン 3.1 改定第 1 版 CCMB-2006-09-004
平成 19 年 3 月翻訳第 1.2 版
独立行政法人情報処理推進機構セキュリティセンター情報セキュリティ認証室

用語・略語

本 ST で使用している略語を以下に示す。

CC	コモンクライテリア（Common Criteria）
EAL	評価保証レベル（Evaluation Assurance Level）
PP	プロテクションプロファイル（Protection Profile）
ST	セキュリティターゲット（Security Target）
TOE	評価対象（Target of Evaluation）
TSF	TOE セキュリティ機能（TOE Security Functionality）
TSFI	TSF インタフェース（TSF Interface）
GUI	グラフィカルユーザインタフェース（Graphical User Interface）
SAR	セキュリティ保証要件（Security Assurance Requirement）
SFR	セキュリティ機能要件（Security Functional Requirement）
SFP	セキュリティ機能方針（Security Function Policy）
PC	パーソナルコンピュータ（Personal Computer）
OS	オペレーティングシステム（Operating System）

本STで使用している用語の意味を表 1に示す。

表 1 用語集

用語	定義内容
利用者	TOE の機能を利用し、業務を行なう人物。利用者は管理者とオペレータに大別される。
管理者	利用者の内、TOEの管理を行なう人物。
オペレータ	利用者の内、TOEの機能を利用して監視業務を行う人物。
責任者	TOE に対し、直接操作は行わない。管理者、オペレータを任命する人物。
監視サーバ	TOEを構成するコンポーネントの内、WebSAM SystemManager マネージャを配置したサーバ。TOEの扱う情報を蓄積、管理する。
監視対象サーバ	TOEを構成するコンポーネントの内、WebSAM SystemManager エージェントを配置したサーバ。構成情報、障害情報、性能情報を収集し、監視サーバに通知する。
監視端末	TOEを構成するコンポーネントの内、WebSAM SystemManager 監視端末を配置したクライアントPC。利用者にGUIを提供する。
構成情報	監視対象サーバを構成するOS、CPU、デバイス、アプリケーションソフト、ネットワーク、ディスクの情報。
障害情報	監視対象サーバで発生した、ログ、プロセスの情報、Windowsサービスの情報、性能情報の内、定義情報にて障害と定義されている事象。
性能情報	監視対象サーバのCPU使用率、メモリ使用量、ディスク使用量、ネットワーク使用量等、性能に関する情報。
プロセス	OSからメモリ、CPU時間、各種デバイスなどの割り当てを受けて処理を実行しているプログラム。 監視対象サーバ上で動作する。 TOEは監視対象サーバ上のプロセスを監視、操作する機能を持つ。

用語	定義内容
Windowsサービス	Windows OSのバックグラウンドで動作するプログラム。 監視対象サーバ上で動作する。 TOEは、監視対象サーバ上のWindowsサービスを監視、操作する機能を持つ。(監視対象サーバのOSがWindowsの場合のみ)
履歴情報	監視対象サーバが収集し、監視サーバが蓄積、管理している情報。
通報	TOEが監視対象サーバの障害情報を検出した時に、電子メールの送信、回転灯の鳴動により、オペレータに通知する機能。
定義情報	監視対象サーバの構成情報、障害情報、性能情報に関する監視項目、監視間隔や、履歴情報の保持期間、通報宛先、監視端末のGUI表示項目など、TOEの動作を決定する情報。
オーディットログ	TOEに対して利用者が行なった操作履歴のログ。
オーディットログ定義情報	オーディットログに関するTOEの動作を決定する情報。
ライセンス	TOEの動作に必要な情報。TOE購入時に日本電気株式会社より発行される。 ライセンスには、マネージャライセンスとエージェントライセンスの 2 種類が存在する。 マネージャライセンスが存在しない、もしくは不正な場合、TOEは使用できない。 エージェントライセンスは、監視対象サーバの数だけ必要であり、エージェントライセンス数を超過して監視対象サーバを接続することはできない。
ヘルプ	監視端末にて参照可能なマニュアル。
ユーザ	利用者を識別し、管理する単位。 通常、利用者毎にユーザを作成し、管理する。
グループ	複数のユーザを所属させ、管理する。権限を付与する単位。
ユーザ情報	ユーザのユーザ名、氏名、備考、パスワード、所属グループの情報。
グループ情報	グループのグループ名、権限、所属ユーザの情報。
権限情報	グループ情報の参照権限、操作権限、定義変更権限、ライセンス管理権限、ユーザ管理権限、オーディットログ参照権限、オーディットログ更新権限の情報。

1. ST 概説

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

1.1. ST 参照

ST の識別情報は、以下の通りである。

ST タイトル: WebSAM SystemManager Ver5.2.1 セキュリティターゲット
ST バージョン: 1.10
ST 作成者: 日本電気株式会社
ST 作成日: 2008 年 09 月 25 日

1.2. TOE 参照

TOE の識別情報は、以下の通りである。

TOE 名称: 機能特定（WebSAM SystemManager）
TOE バージョン: 5.2.1
TOE 開発者: 日本電気株式会社

上記 TOE 参照は、「WebSAM SystemManager エージェント」、「WebSAM SystemManager マネージャ」、及び「WebSAM SystemManager 監視端末」の総称である。
TOE 内では、それぞれ「WebSAM SystemManager Agent Version 5.2.1.0」、「WebSAM SystemManager Manager Version 5.2.1.0」、「WebSAM SystemManager Svc Version 5.2.1.0」と表記する。

1.3. TOE 概要

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

1.3.1. TOE 種別

本 TOE の種別は、「その他」である。

1.3.2. 主要なセキュリティ機能

TOE の使用方法は、以下の通りである。
TOEは監視対象サーバの構成情報、障害情報、性能情報を収集し、管理するソフトウェア製品である。マルチベンダ、マルチプラットフォームで構成される情報システムに存在する、多種多様なサーバの情報をGUIで一元的に監視する事により、サーバの管理業務を効率化する。
TOEは、正しい利用者が誤り無く正しい役割で利用できるよう、利用者の識別および認証、利用者の役割に基づいた情報へのアクセス制限を行なっている。
TOE の主要なセキュリティ機能は、以下の通りである。

・TOE の利用者に対する識別と認証を行う機能
・TOE の利用者役割に従い権限の割り当てを行う機能
・割り当てられた権限に基づくアクセス制御を行う機能

1.3.3. TOE の動作環境

TOE が必要とする TOE 以外のハードウェア/ソフトウェアを、以下に記述する。

1．監視端末

1-1. Windows 版

ハードウェア

本体	Express5800 シリーズ、PC/AT 互換機
CPU	PentiumⅢ 1GHz 以上
メモリ	64MB 以上
ハードディスク	100MB 以上
LAN	100Mbps 以上

ソフトウェア

OS	Windows 2000 Server (SP4) Windows Server 2003 Windows Server 2003 R2 Windows Server 2003 x64 Windows XP Professional (SP2) Windows Vista Business (SP なし) のいずれか

2．監視サーバ

2-1. Windows 版

ハードウェア

本体	Express5800 シリーズ、PC/AT 互換機
CPU	PentiumⅢ 1GHz 以上
メモリ	64MB 以上
ハードディスク	1GB 以上
LAN	100Mbps 以上

ソフトウェア

OS	Windows 2000 Server(SP4) Windows Server 2003 Windows Server 2003 R2 Windows Server 2003 x64 のいずれか

2-2. HP-UX 版

ハードウェア

本体	NX7700i シリーズ
メモリ	64MB 以上
ハードディスク	1GB 以上
LAN	100Mbps 以上

ソフトウェア

OS	HP-UX 11iV2 HP-UX 11iV3 のいずれか

3．監視対象サーバ

3-1. Windows 版

ハードウェア

本体	Express5800 シリーズ、PC/AT 互換機
CPU	PentiumⅢ 1GHz 以上
メモリ	32MB 以上
ハードディスク	300MB 以上
LAN	100Mbps 以上

ソフトウェア

OS	Windows 2000 Server(SP4) Windows Server 2003 Windows Server 2003 R2 Windows Server 2003 x64 のいずれか

3-2. HP-UX 版

ハードウェア

本体	NX7000/NX7700/NX7700i シリーズ
メモリ	32MB 以上
ハードディスク	300MB 以上
LAN	100Mbps 以上

ソフトウェア

OS	HP-UX 11i HP-UX 11iV2 HP-UX 11iV3 のいずれか

3-3. Linux 版

ハードウェア

本体	Express5800 シリーズ、PC/AT 互換機
CPU	PentiumⅢ 1GHz 以上
メモリ	32MB 以上
ハードディスク	300MB 以上
LAN	100Mbps 以上

ソフトウェア

OS	RedHat Enterprise Linux AS/ES 4.0 MIRACLE LINUX V3.0 – Asianux Inside のいずれか

3-4. Solaris 版

ハードウェア

本体	CX5000 シリーズ
CPU	Ultra SPARC-Ⅱ 650MHz 以上
メモリ	32MB 以上
ハードディスク	300MB 以上
LAN	100Mbps 以上

ソフトウェア

OS	Solaris 9 Solaris 10 のいずれか

TOEの動作環境のうち、本評価にて検証した環境を、表 2および表 3に示す。

表 2 検証環境1

	OS
監視端末	Windows XP Professional Edition (SP2)
監視サーバ	Windows Server 2003, Standard Edition (SP2)
監視対象サーバ	Windows Server 2003, Standard Edition (SP2)

表 3 検証環境2

	OS
監視端末	Windows XP Professional Edition (SP2)
監視サーバ	HP-UX 11iV3
監視対象サーバ	HP-UX 11iV3

1.4. TOE 記述

本節では、TOE 機能の詳細説明として、TOE 関連の役割定義、TOE の物理的範囲、TOE の論理的範囲、TOE サービス機能とセキュリティ機能について記述する。

1.4.1. TOE 関連の役割定義

TOEに関連する役割定義を表 4に示す。

表 4 TOE 関連の役割定義一覧

役割		内容
管理者	ビルトイン管理者	全ての操作が可能な利用者。 TOE に必ず存在する特別なユーザ情報を利用して、インストール直後に、ユーザ情報管理者のユーザ情報を作成する。 また、他の利用者役割が遂行できなくなった場合に、代行する。

役割		内容
	ライセンス情報管理者	ライセンスの情報の参照、登録、更新、削除が可能な利用者。 定義情報管理者の役割も兼ねる。
	オーディットログ参照管理者	オーディットログの情報の参照が可能な利用者。 参照オペレータの役割も兼ねる。
	オーディットログ更新管理者	オーディットログ定義情報の参照、更新および、オーディットログの削除が可能な利用者。 オーディットログ参照管理者および定義情報管理者の役割も兼ねる。
	ユーザ情報管理者	ユーザ情報、およびグループ情報の参照、登録、更新、削除が可能な利用者。 定義情報管理者の役割も兼ねる。
	定義情報管理者	定義情報の参照、登録、更新、削除および、履歴情報の削除が可能な利用者。 操作オペレータの役割も兼ねる。
オペレータ	操作オペレータ	履歴情報の更新、プロセスの起動/停止指示、および、Windows サービスの開始/再開/停止/一時停止/再起動指示が可能な利用者。 参照オペレータの役割も兼ねる。
	参照オペレータ	履歴情報、プロセスの情報、Windows サービスの情報等の参照のみが可能な利用者。

※ 利用者は、複数の役割を兼ねることが可能である。
※ 役割はグループによって実現される。

1.4.2. TOE の物理的範囲

TOE の物理的範囲(ネットワーク、コンポーネント)、ハードウェア構成、ソフトウェア構成を、以下に記述する。

1.4.2.1. TOE の物理的範囲(ネットワーク)

TOE は、監視サーバ、監視対象サーバ、監視端末上で稼働する。
監視サーバと監視対象サーバの間、および監視サーバと監視端末の間は、TCP/IP ネットワークで接続される。
1 台の監視サーバに複数台の監視対象サーバ、監視端末を接続することが可能である。
監視サーバは、監視対象サーバから送付された構成情報、障害情報、性能情報を蓄積する。TOE の利用者は監視端末から、監視サーバに蓄積された構成情報、障害情報、性能情報にアクセスする。
TOEのネットワーク構成を図 1に示す。

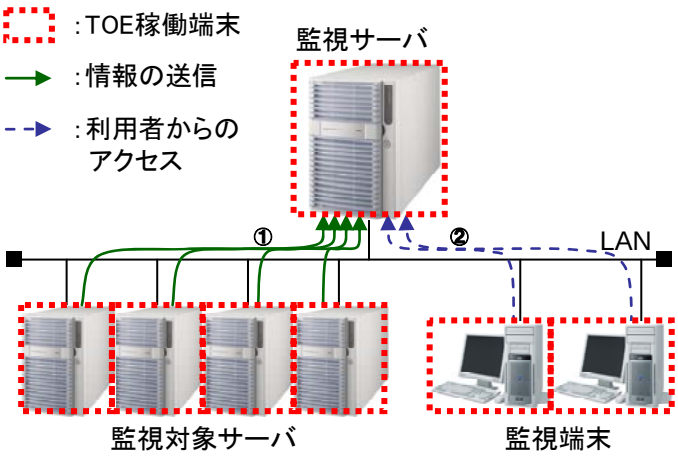

図 1 TOE のネットワーク構成

図中に TOE 稼動端末として示した部分が、TOE の稼動範囲である。

①:監視対象サーバは、構成情報、障害情報、性能情報を監視サーバに送信し、監視サーバに蓄積する。
②:利用者は監視端末から監視サーバに蓄積された、構成情報、障害情報、性能情報にアクセスする。

1.4.2.2. TOE の物理的範囲(コンポーネント)

TOE のコンポーネント構成は、以下の通りである。
TOE は、監視サーバ上で動作する WebSAM SystemManager マネージャと、監視対象サーバ上で動作する WebSAM SystemManager エージェント、および監視端末上で動作する WebSAM SystemManager 監視端末 から構成される。
TOE を稼働させる為に、監視サーバ機器、監視対象サーバ機器、監視端末機器の各ハードウェアと、それらの上で動作する OS が必要となる。
TOEのコンポーネント構成を図 2に示す。

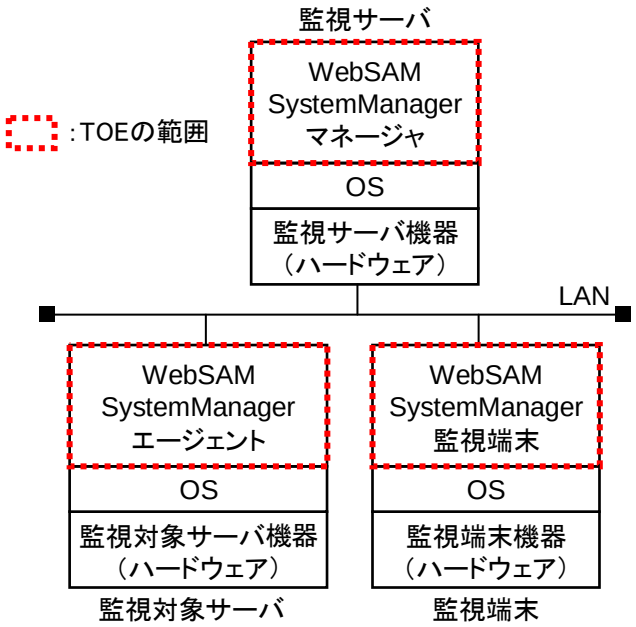

図 2 TOE の物理的範囲(コンポーネント)

図中に TOE の範囲として示した箇所が、TOE の物理的範囲である。

1.4.2.3. ソフトウェア構成

TOE に関連するソフトウェアの構成は、以下の通りである。

1． 監視端末

1-1. Windows 版

WebSAM SystemManager 監視端末 Ver5.2.1

(TOE 内では「WebSAM SystemManager Svc Version 5.2.1.0」と表記)

2． 監視サーバ

2-1. Windows 版

WebSAM SystemManager Manager for Win/Linux Ver5.2.1

(TOE 内では「WebSAM SystemManager Manager Version 5.2.1.0」と表記)

2-2. HP-UX 版

WebSAM SystemManager Manager for HP-UX/Solaris Ver5.2.1

(TOE 内では「WebSAM SystemManager Manager Version 5.2.1.0」と表記)

3． 監視対象サーバ

3-1. Windows 版

WebSAM SystemManager Agent for Win/Linux Ver5.2.1

(TOE 内では「WebSAM SystemManager Agent Version 5.2.1.0」と表記)

3-2. HP-UX 版

WebSAM SystemManager Agent for HP-UX/Solaris Ver5.2.1

(TOE 内では「WebSAM SystemManager Agent Version 5.2.1.0」と表記)

3-3. Linux 版

WebSAM SystemManager Agent for Win/Linux　Ver5.2.1
(TOE 内では「WebSAM SystemManager Agent Version 5.2.1.0」と表記)

3-4. Solaris 版

WebSAM SystemManager Agent for HP-UX/Solaris　Ver5.2.1
(TOE 内では「WebSAM SystemManager Agent Version 5.2.1.0」と表記)

1.4.2.4. ガイダンス

TOE のガイダンスは、以下の通りである。
・利用者準備ガイダンス
WebSAM SystemManager Ver5.2.1 利用者準備ガイダンス Ver1.07
・利用者操作ガイダンス
WebSAM SystemManager Ver5.2.1 利用者操作ガイダンス Ver1.08

1.4.3. TOE の論理的範囲

TOE の論理的構成を、以下に記述する。
利用者は、WebSAM SystemManager 監視端末の起動時にログイン操作を行い、成功した場合に TOE が利用可能となる。
利用者は、ログインしたユーザが所属するグループに割り当てられた権限に応じた操作が可能である。

TOEの論理範囲を図 3に示す。

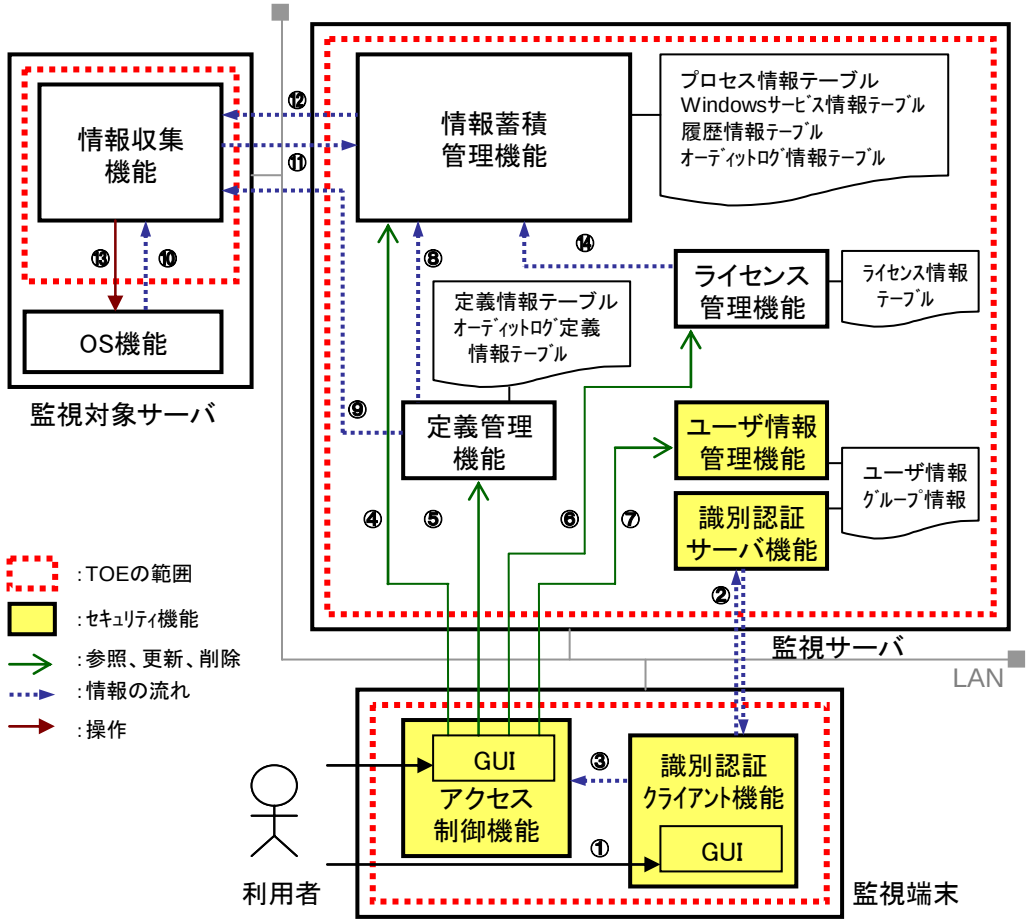

図 3 TOE の論理範囲

図中に TOE の範囲として示した箇所が、TOE の論理範囲である。

図 3におけるTOEの各機能の説明を表 5に示す。

表 5 TOE の各機能

端末	名称	説明
監視端末	識別認証クライアント機能	識別認証に関する監視端末側の処理を行う。 ログイン操作に利用する GUI を持つ。
	アクセス制御機能	GUIを持ち、利用者の権限に応じて、GUIの表示内容を切り替える。
監視サーバ	識別認証サーバ機能	識別認証に関する監視サーバ側の処理を行う。
	ユーザ情報管理機能	ユーザ情報およびグループ情報を管理する。
	情報蓄積管理機能	監視対象サーバから収集した構成情報、障害情報、性能情報や、オーディットログ等を蓄積・管理する。
	定義管理機能	定義情報、オーディットログ定義情報を管理する。
	ライセンス管理機能	ライセンスの情報を管理する。
監視対象サーバ	情報収集機能	監視対象サーバの構成情報、障害情報、性能情報を収集する。

図 3における各情報の説明を表 6に示す。

表 6 TOE の情報

名称	説明
ユーザ情報	利用者を識別する情報。
グループ情報	グループに関する情報。
定義情報テーブル	監視サーバのメモリ上に存在し、定義情報を管理するテーブル。TOE の起動時に作成される。
オーディットログ定義情報テーブル	監視サーバのメモリ上に存在し、オーディットログ定義情報を管理するテーブル。TOE の起動時に作成される。
ライセンス情報テーブル	監視サーバのメモリ上に存在し、ライセンスの情報を管理するテーブル。TOE の起動時に作成される。
プロセス情報テーブル	監視サーバのメモリ上に存在し、プロセスの情報を管理するテーブル。TOE の起動時に作成される。
Windows サービス情報テーブル	監視サーバのメモリ上に存在し、Windows サービスの情報を管理するテーブル。TOE の起動時に作成される。
履歴情報テーブル	監視サーバのメモリ上に存在し、履歴情報を管理するテーブル。TOE の起動時に作成される。
オーディットログ情報テーブル	監視サーバのメモリ上に存在し、オーディットログの情報を管理するテーブル。TOE の起動時に作成される。

TOE の動作の流れを図3の矢印の番号の順に示す。

①:利用者は監視端末の起動時に、識別認証クライアント機能の GUI(ログイン画面)に、ユーザ名とパスワードを入力する。
②:識別認証クライアント機能は、監視サーバ上に存在する識別認証サーバ機能にユーザ名とパスワードを送付し、識別認証サーバ機能にてログインの成否を判定する。ログインに成功した場合、識別認証サーバ機能は、識別認証クライアント機能にログインした利用者に割り当てられた権限情報を送付する。
③:識別認証クライアント機能は、アクセス制御機能に、権限情報を送付する。アクセス制御機能は取得した権限情報により、GUI の表示内容(メニューやボタン等の表示)を制御する。
④:利用者は、アクセス制御機能に許容された範囲で、情報蓄積管理機能が持つ各種情報の参照、更新、削除を行なう。
⑤:利用者は、アクセス制御機能に許容された範囲で、定義管理機能が持つ定義情報、オーディットログ定義情報の参照、登録、更新、削除を行なう。
⑥:利用者の操作により、アクセス制御機能に許容された範囲で、ライセンス管理機能が持つライセンスの情報の参照、登録、更新、削除を行なう。
⑦:利用者は、アクセス制御機能に許容された範囲で、ユーザ情報管理機能が持つ情報の参照、登録、更新、削除を行なう。
⑧:情報蓄積管理機能は、定義管理機能が持つ定義情報に従い動作する。
⑨:定義管理機能は、定義情報テーブルの情報を監視対象サーバの情報収集機能に通知する。
⑩:情報収集機能は、定義管理機能から通知された定義情報に従い、OS 機能から構成情報、障害情報、性能情報を取得する。
⑪:情報収集機能は、取得した構成情報、障害情報、性能情報を情報蓄積管理機能に送付する。

⑫:情報蓄積管理機能は、プロセス情報テーブルの起動/停止情報、Windows サービス情報テーブルの開始/停止/一時停止/再起動/再開情報が更新されれば、情報収集機能に指示を通知する。
⑬:情報収集機能は、通知された指示に従ってプロセスの起動/停止、Windows サービスの開始/停止/一時停止/再起動/再開を、OS 機能に命令する。
⑭:情報蓄積管理機能は、ライセンス管理機能が持つライセンスの情報を確認して、動作を行う。

本 ST では、監視端末からのアクセスについてのセキュリティ機能のみを対象にする。TOE が監視サーバおよび監視対象サーバに持つ、コマンド経由のアクセスや API 経由のアクセスについては、本 ST の対象にしない。

1.4.4. TOE のセキュリティ機能

TOE のセキュリティ機能を以下に記述する。
【識別認証機能】
TOE にアクセスする利用者を「ユーザ名」と、「パスワード」を用いて識別し、認証する。
利用者の識別認証前に、ヘルプの参照を行うことができる。
利用者の識別認証に成功した場合は、該当する利用者の権限情報をアクセス制御機能に通知する。

【ユーザ情報管理機能】
TOE にアクセスする利用者のセキュリティ属性であるユーザ情報、グループ情報、権限情報の管理をすることができる。
権限情報は、グループごとに設定することができる。グループには、複数のユーザが所属することができる。
また、ユーザは複数のグループに所属する事ができる。
利用者は、ログインしたユーザが所属する複数のグループから権限情報を取得することができる。この場合、取得した全ての権限が有効になる。
ユーザ情報、およびグループ情報の参照、登録、削除、更新は、ユーザ情報管理者、またはビルトイン管理者が行うことができる。
認証された利用者は自身の「パスワード」を変更することができる。

【アクセス制御機能】
TOE が管理する、監視サーバ上の以下の情報への、利用者のアクセスを制御する。
- 履歴情報テーブル
- プロセス情報テーブル
- Windows サービス情報テーブル
- 定義情報テーブル
- ライセンス情報テーブル
- オーディットログ情報テーブル
- オーディットログ定義情報テーブル

識別認証機能より取得した利用者の権限情報を利用して、制御を行なう。
GUI の項目(メニュー、ボタン等)の有効/無効を切り替えることで、アクセス制御を実現する。

2. 適合主張

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

2.1. CC 適合主張

本 ST は以下の通り CC 適合を主張する。

情報技術セキュリティ評価のためのコモンクライテリア
パート 1:概説と一般モデル 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 2:セキュリティ機能コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
パート 3:セキュリティ保証コンポーネント 2006 年 9 月 バージョン 3.1 翻訳第 1.2 版
CC パート 2 適合
CC パート 3 適合

2.2. PP 主張

本 ST は PP 適合を主張しない。

2.3. パッケージ主張

本 ST のパッケージ主張は以下のとおりである。
パッケージ ： EAL1 適合

2.4. 適合根拠

本 ST は、PP 適合を主張していないため、PP 適合根拠はない。

3. セキュリティ対策方針

本章では、TOE の運用環境のセキュリティ対策方針について記述する。

3.1. 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を以下に記述する。

OE.TRUSTED_ROLE（信頼される役割）
責任者は、管理者、オペレータの役割に適した者を厳重に人選し、その上で、それぞれの役割を理解させなければならない。

OE.AUTHORIZATION_SETTING（権限の設定）
ユーザ情報管理者は、管理者、オペレータに権限を付与しなければならない。
ユーザ情報管理者は権限の付与について信頼できること。

OE.PASSWORD_MANAGEMENT（パスワードの管理）
すべての利用者は、TOE にアクセスするための識別・認証情報（ユーザ名とパスワード）を管理し、他人に漏らしてはならない。また推測・解析されやすいパスワードを設定してはならず、適正な間隔で変更しなければならない。

OE.SAFE_PLACE（安全な場所）
監視端末、監視サーバ、監視対象サーバは、物理的に不正侵入されない場所に設置されなければならない。

OE.SAFE_NETWORK（安全なネットワーク）
監視端末、監視サーバ、監視対象サーバ間のネットワークは、不正な盗聴や改ざんから保護できなければならない。

OE.TRUSTED_OS（信頼できる OS）
監視端末、監視サーバ、監視対象サーバ上で稼働する OS には、OS の供給元から配布されるパッチを適切に適用しなければならない。

4. 拡張コンポーネント定義

本章では拡張コンポーネント定義について記述を行う。

本 ST には、拡張コンポーネントはない。

5. セキュリティ要件

本章ではセキュリティ要件について記述を行う。

5.1. セキュリティ機能要件

セキュリティ機能のクラス毎に以下で、機能要件の記述を行う。

5.1.1. FDP クラス:利用者データ保護

FDP_ACC.1　サブセットアクセス制御
　　下位階層:　　なし
　　依存性:　　FDP_ACF.1 セキュリティ属性によるアクセス制御

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

[割付: サブジェクト、オブジェクト、及び SFP で扱われるサブジェクトとオブジェクト間の操作のリスト] :
割付を表 7に示す。

表 7 サブジェクトとオブジェクト間の操作のリスト

サブジェクト	オブジェクト	操作
利用者代行プロセス	各種テーブル	レコードの参照 レコードの更新 レコードの削除

[割付: アクセス制御 SFP]:
データアクセス制御 SFP

FDP_ACF.1　セキュリティ属性によるアクセス制御
　　下位階層:　　なし
　　依存性:　　FDP_ACC.1 サブセットアクセス制御
　　FMT_MSA.3 静的属性初期化

FDP_ACF.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]:
割付を表 8、および表 9に示す。

表 8 サブジェクトとセキュリティ属性

サブジェクト	セキュリティ属性
利用者代行プロセス	サブジェクトに結合される利用者権限 下記 6 種類 ・参照権限 ・操作権限 ・定義変更権限 ・ライセンス管理権限 ・オーディットログ参照権限 ・オーディットログ更新権限

表 9 オブジェクトとセキュリティ属性

オブジェクト	セキュリティ属性
各種テーブル	テーブル種別 下記7種類 ・プロセス情報テーブル ・Windows サービス情報テーブル ・定義情報テーブル ・履歴情報テーブル ・ライセンス情報テーブル ・オーディットログ情報テーブル ・オーディットログ定義情報テーブル

[割付: アクセス制御 SFP]:
データアクセス制御 SFP

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

[割付: 制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]:
データアクセス制御SFPが、サブジェクトのセキュリティ属性とオブジェクトのセキュリティ属性の組合せに対して許可するアクセスを、表 10に示す。
表中に示していないアクセスは許可しない。

表 10 アクセス制御規則

サブジェクトに結合される利用者権限 / テーブル種別	参照権限がある場合	操作権限がある場合	定義変更権限がある場合	ライセンス管理権限がある場合	オーディットログ参照権限がある場合	オーディットログ更新権限と定義変更権限の両方がある場合
プロセス情報テーブル	参照	更新	－	－	－	－
Windows サービス情報テーブル	参照	更新	－	－	－	－
定義情報テーブル	－	－	参照 更新	－	－	－
履歴情報テーブル	参照	更新	削除	－	－	－
ライセンス情報テーブル	－	－	－	参照 更新	－	－
オーディットログ情報テーブル	－	－	－	－	参照	削除
オーディットログ定義情報テーブル	－	－	－	－	－	参照 更新

※ 表中の「参照」はレコードの参照を、「更新」はレコードの更新を、「削除」はレコードの削除を、それぞれ表す。

※ 参照権限は全ての利用者に付与される。

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

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

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

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

5.1.2. FIA クラス:識別と認証

FIA_ATD.1 利用者属性定義
下位階層: なし
依存性: なし

FIA_ATD.1.1 TSF は、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。:[割付: セキュリティ属性のリスト]

[割付: セキュリティ属性のリスト]:
ユーザ名
所属グループ
参照権限
操作権限
定義変更権限
ライセンス管理権限
オーディットログ参照権限
オーディットログ更新権限

FIA_SOS.1 秘密の検証
下位階層: なし
依存性: なし

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

[割付: 定義された品質尺度]:
パスワードは、6 文字以上 64 文字以下の文字列。
パスワードの先頭または、末尾に全角・半角スペースを含む文字列は使用することができない。

FIA_UAU.1 認証のタイミング
下位階層: なし
依存性: FIA_UID.1 識別のタイミング

FIA_UAU.1.1 TSF は、利用者が認証される前に利用者を代行して行われる[割付: TSF 仲介アクションのリスト]を許可しなければならない。

[割付: TSF 仲介アクションのリスト]:
ヘルプの表示

FIA_UAU.1.2 TSF は、その利用者を代行する他のすべての TSF 仲介アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

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

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

[割付:フィードバックのリスト]:
入力したパスワードの文字数と同数のアスタリスクを返す。

FIA_UID.1　識別のタイミング
下位階層:　なし
依存性:　なし

FIA_UID.1.1　TSF は、利用者が識別される前に利用者を代行して実行される[割付: TSF 仲介アクションのリスト]を許可しなければならない。

[割付 TSF 仲介アクションのリスト]:
ヘルプの表示

FIA_UID.1.2　TSF は、その利用者を代行する他の TSF 仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

FIA_USB.1　利用者-サブジェクト結合
下位階層:　なし
依存性:　FIA_ATD.1 利用者属性定義

FIA_ USB.1.1　TSF は、以下の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない。:[割付: 利用者セキュリティ属性のリスト]

[割付: 利用者セキュリティ属性のリスト]:
参照権限
操作権限
定義変更権限
ライセンス管理権限
オーディットログ参照権限
オーディットログ更新権限

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

[割付: 属性の最初の関連付けの規則]:
なし

FIA_ USB.1.3　　TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。:[割付: 属性の変更の規則]

[割付: 属性の変更の規則]:
ユーザ管理権限を持つ利用者は、参照権限を除く権限情報の変更を行うことが出来る。
権限情報はオーディットログ参照権限を除いて、即時に変更が反映される。オーディットログ参照権限は、再度ログインを行った場合に変更が反映される。

5.1.3. FMT クラス:セキュリティ管理

FMT_MSA.1 セキュリティ属性の管理
下位階層: なし
依存性: [FDP_ACC.1 サブセットアクセス制御、または FDP_IFC.1 サブセット情報フロー制御]
FMT_SMR.1 セキュリティの役割
FMT_SMF.1 管理機能の特定

FMT_MSA.1.1　　TSF は、セキュリティ属性[割付: セキュリティ属性のリスト]に対し[選択: デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]をする能力を[割付: 許可された識別された役割]に制限する[割付: アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

[割付: セキュリティ属性のリスト]:
表 11に示す。

[選択:デフォルト値変更、問い合わせ、改変、削除、[割付: その他の操作]]:
表 11示す。

[割付: 許可された識別された役割]:
表 11示す。

[割付: アクセス制御 SFP、情報フロー制御 SFP]:
データアクセス制御 SFP

表 11 セキュリティ属性の管理

セキュリティ属性のリスト	選択: デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
参照権限	問い合わせ	ユーザ情報管理者 ビルトイン管理者
操作権限	問い合わせ、改変	ユーザ情報管理者 ビルトイン管理者
定義変更権限	問い合わせ、改変	ユーザ情報管理者 ビルトイン管理者

セキュリティ属性のリスト	選択: デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
ライセンス管理権限	問い合わせ、改変	ユーザ情報管理者 ビルトイン管理者
オーディットログ参照権限	問い合わせ、改変	ユーザ情報管理者 ビルトイン管理者
オーディットログ更新権限	問い合わせ、改変	ユーザ情報管理者 ビルトイン管理者

FMT_MSA.3 静的属性初期化

下位階層: なし

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

FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性に対して[選択: 制限的、許可的、[割付: その他の特性]: から 1 つのみ選択]デフォルト値を与える[割付: アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

[選択: 制限的、許可的、[割付: その他の特性]:
制限的

[割付: アクセス制御 SFP、情報フロー制御 SFP]:
データアクセス制御 SFP

FMT_MSA.3.2 TSF は、オブジェクトや情報が生成されるとき、[割付: 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[割付: 許可された識別された役割]:
なし

FMT_MTD.1 TSF データの管理

下位階層: なし

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

FMT_MTD.1.1 TSF は、[割付: TSF データのリスト]を[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]する能力を[割付: 許可された識別された役割]に制限しなければならない。

[割付: TSF データのリスト]:
表 12に示す。

[選択: デフォルト値変更、問い合わせ、改変、削除、消去、[割付: その他の操作]]:
表 12に示す。

[割付: その他の操作]:
表 12に示す。

[割付: 許可された識別された役割]:
表 12に示す。

表 12 TSF データの管理

	TSF データのリスト	選択: デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
ユーザ情報	ユーザ名	問い合わせ、消去、登録	ユーザ情報管理者 ビルトイン管理者
	パスワード	改変、消去、登録	ユーザ情報管理者 ビルトイン管理者
		改変	識別認証された利用者
	フルネーム	問い合わせ、改変、消去、登録	ユーザ情報管理者 ビルトイン管理者
	説明	問い合わせ、改変、消去、登録	ユーザ情報管理者 ビルトイン管理者
	所属グループ	問い合わせ、改変、消去、登録	ユーザ情報管理者 ビルトイン管理者
グループ情報	グループ名	問い合わせ、改変、消去、登録	ユーザ情報管理者 ビルトイン管理者
	所属ユーザ	問い合わせ、改変、消去、登録	ユーザ情報管理者 ビルトイン管理者

FMT_SMF.1 管理機能の特定
下位階層: なし
依存性: なし

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない。:[割付: TSF によって提供される管理機能のリスト]

[割付: TSF によって提供される管理機能のリスト]:
割付を表 13に示す。

表 13 TSF によって提供される管理機能のリスト

機能要件	管理要件	管理項目
FDP_ACC.1	予見される管理アクティビティはない。	なし
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	なし
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	なし
FIA_SOS.1	秘密の検証に使用される尺度の管理。	なし
FIA_UAU.1	管理者による認証データの管理。	ユーザ情報管理者とビルトイン管理者による、パスワードの登録、変更
	関係する利用者による認証データの管理。	識別認証された利用者（パスワード所有者本人）によるパスワードの変更
	利用者が認証される前にとられるアクションのリストを管理すること。	なし
FIA_UAU.7	予見される管理アクティビティはない。	なし
FIA_UID.1	利用者識別情報の管理。	ユーザ情報管理者とビルトイン管理者による、ユーザの登録、削除、参照
	許可管理者が、識別前に許可されるアクションを変更できる場合、そのアクションリストを管理すること。	なし
FIA_USB.1	許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。	なし
	許可管理者は、サブジェクトのセキュリティ属性を変更できる。	ユーザ情報管理者とビルトイン管理者による、以下の権限の変更 ・ライセンス管理権限の変更 ・オーディットログ参照権限の変更 ・オーディットログ更新権限の変更 ・ユーザ管理権限の変更 ・定義変更権限の変更 ・操作権限の変更 なお権限情報の変更の反映は、オーディットログ参照権限を除いて、即時に行われる。オーディットログ参照権限は、再度ログインを行った際に行われる。
FMT_MSA.1	セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	ユーザ情報管理者とビルトイン管理者による、グループが関係付けられる役割の変更
FMT_MSA.3	初期値を特定できる役割のグループを管理すること。	なし
	所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	なし
FMT_MTD.1	TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	ユーザ情報管理者とビルトイン管理者による、グループが関係付けられる役割の変更
FMT_SMF.1	予見される管理アクティビティはない。	なし

機能要件	管理要件	管理項目
FMT_SMR.1	役割の一部をなす利用者のグループの管理。	ユーザ情報管理者とビルトイン管理者による、グループが関係付けられる役割の変更

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

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

[割付: 許可された識別された役割]:
ビルトイン管理者
ライセンス情報管理者
オーディットログ参照管理者
オーディットログ更新管理者
ユーザ情報管理者
定義情報管理者
操作オペレータ
参照オペレータ

ただし、ユーザ情報管理者は自身に対し全ての権限を付与することができ、ビルトイン管理者と同等の権限を保持することができる。

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。

5.2. セキュリティ保証要件

保証要件のクラス毎に以下に保証要件を記述する。
本 TOE の評価保証レベルは EAL1 である。すべての保証要件コンポーネントは、CC パート 3 で規定されている EAL1 の保証要件コンポーネントを使用する。

5.2.1. ASE クラス :セキュリティターゲット評価

ASE_CCL.1: 適合主張
ASE_ECD.1: 拡張コンポーネント定義
ASE_INT.1: ST 概説
ASE_OBJ.1: 運用環境のセキュリティ対策方針
ASE_REQ.1: 主張されたセキュリティ要件
ASE_TSS.1: TOE 要約仕様

5.2.2. ADV クラス: 開発

ADV_FSP.1: 基本機能仕様

5.2.3. AGD クラス :ガイダンス文書

AGD_OPE.1: 利用者操作ガイダンス
AGD_PRE.1: 準備手続き

5.2.4. ALC クラス :ライフサイクルサポート

ALC_CMC.1: TOE のラベル付け
ALC_CMS.1: TOE の CM 範囲

5.2.5. ATE クラス :テスト

ATE_IND.1 独立テスト - 適合

5.2.6. AVA クラス :脆弱性評定

AVA_VAN.1 脆弱性調査

5.3. セキュリティ要件根拠

セキュリティ要件のコンポーネントの依存性を表 14に示す。

表 14 セキュリティ要件依存性根拠

コンポーネント	CC Part2 における依存コンポーネント	TOE における依存コンポーネント	依存性が満たされないコンポーネント	根拠
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	なし	
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3	なし	
FIA_ATD.1	なし	なし	なし	
FIA_SOS.1	なし	なし	なし	
FIA_UAU.1	FIA_UID.1	FIA_UID.1	なし	
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1	なし	
FIA_UID.1	なし	なし	なし	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1	なし	
FMT_MSA.1	[FDP_ACC.1 または FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1	なし	
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1	なし	
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 FMT_SMF.1	なし	
FMT_SMF.1	なし	なし	なし	
FMT_SMR.1	FIA_UID.1	FIA_UID.1	なし	

表 14により、すべての依存関係を満たしている。

6. TOE 要約仕様

本章では、本 TOE がどのように SFR を満たすかを記述する。

6.1. FDP_ACC.1、FDP_ACF.1

利用者に割り当てられた権限情報より、以下のとおり、利用できる操作の制限を行なう。

1) 履歴情報テーブルのレコードの参照、更新、削除

TOE は、参照権限を持つ利用者に対してのみ、履歴情報テーブルのレコードを参照するための GUI 機能（メニューやボタンなど）を有効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、履歴情報テーブルのレコードを参照し情報を得て、監視端末上に履歴情報を表示する。参照権限は全ての利用者に付与される為、全ての利用者が履歴情報を参照する事が可能である。

TOE は、操作権限を持つ利用者に対してのみ、履歴情報テーブルのレコードを更新するための GUI 機能（メニューやボタンなど）を有効化し、操作権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、履歴情報テーブルのレコードを更新し、履歴情報を更新する。

TOE は、定義変更権限を持つ利用者に対してのみ、履歴情報テーブルのレコードを削除するための GUI 機能（メニューやボタンなど）を有効化し、定義変更権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、履歴情報テーブルのレコードを削除し、蓄積している履歴情報を削除する。

2) プロセス情報テーブルのレコードの参照、更新

TOE は、参照権限を持つ利用者に対してのみ、プロセス情報テーブルのレコードを参照するための GUI 機能（メニューやボタンなど）を有効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、プロセス情報テーブルのレコードを参照し情報を得て、監視端末上にプロセス情報を表示する。参照権限は全ての利用者に付与される為、全ての利用者がプロセス情報を参照する事が可能である。

TOE は、操作権限を持つ利用者に対してのみ、プロセス情報テーブルのレコードを更新するための GUI 機能（メニューやボタンなど）を有効化し、操作権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、プロセス情報テーブルのレコードを更新し、監視対象サーバのプロセスの起動/停止を指示する。

3) Windows サービス情報テーブルのレコードの参照、更新

TOE は、参照権限を持つ利用者に対してのみ、Windows サービス情報テーブルのレコードを参照するための GUI 機能（メニューやボタンなど）を有効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、Windows サービス情報テーブルのレコードを参照し情報を得て、監視端末上に Windows サービス情報を表示する。参照権限は全ての利用者に付与される為、全ての利用者が Windows サービス情報を参照する事が可能である。

TOE は、操作権限を持つ利用者に対してのみ、Windows サービス情報テーブルのレコードを更新するための GUI 機能（メニューやボタンなど）を有効化し、操作権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、Windows サービス情報テーブルのレコードを更新し、監視対象サーバの Windows サービスの開始/停止/一時停止/再起動/再開を指示する。

4) 定義情報テーブルのレコードの参照、更新

TOE は、定義変更権限を持つ利用者に対してのみ、定義情報テーブルのレコードを参照するための GUI 機能（メニューやボタンなど）を有効化し、定義変更権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、定義情報テーブルのレコードを参照し情報を得て、監視端末上に定義情報を表示する。

TOE は、定義変更権限を持つ利用者に対してのみ、定義テーブルのレコードを更新するための GUI 機能（メニューやボタンなど）を有効化し、定義変更権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、定義情報テーブルのレコードを更新し、定義情報を更新する。

5) ライセンス情報テーブルのレコードの参照、更新

TOE は、ライセンス管理権限を持つ利用者に対してのみ、ライセンス情報テーブルのレコードを参照するための GUI 機能（メニューやボタンなど）を有効化し、ライセンス管理権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、ライセンス情報テーブルのレコードを参照し情報を得て、監視端末上に、ライセンスの情報を表示する。

TOE は、ライセンス管理権限を持つ利用者に対してのみ、ライセンス情報テーブルのレコードを更新するための GUI 機能（メニューやボタンなど）を有効化し、ライセンス管理権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、ライセンス情報テーブルのレコードを更新し、ライセンスの登録、更新、削除を行なう。

6) オーディットログ情報テーブルのレコードの参照、削除

TOE は、オーディットログ参照権限を持つ利用者に対してのみ、オーディットログ情報テーブルのレコードを参照するための GUI 機能（メニューやボタンなど）を有効化し、オーディットログ参照権限を持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、オーディットログ情報テーブルのレコードを参照し情報を得て、監視端末上に、オーディットログの情報を表示する。

TOE は、オーディットログ更新権限と定義変更権限の両方を持つ利用者に対してのみ、オーディットログ情報テーブルのレコードを削除するための GUI 機能（メニューやボタンなど）を有効化し、オーディットログ更新権限と定義変更権限の両方を併せ持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、オーディットログ情報テーブルのレコードを削除し、オーディットログの情報を削除する。

7) オーディットログ定義情報テーブルのレコードの参照、更新

TOE は、オーディットログ更新権限と定義変更権限の両方を持つ利用者に対してのみ、オーディットログ定義情報テーブルのレコードを参照するための GUI 機能（メニューやボタンなど）を有効化し、オーディットログ更新権限と定義変更権限の両方を併せ持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、オーディットログ定義情報テーブルのレコードを参照し情報を得て、監視端末上に、オーディットログ定義情報を表示する。

TOE は、オーディットログ更新権限と定義変更権限の両方を持つ利用者に対してのみ、オーディットログ定義情報テーブルのレコードを更新するための GUI 機能（メニューやボタンなど）を有効化し、オーディットログ更新権限と定義変更権限の両方を併せ持たない利用者では無効化する。利用者が有効化された GUI 機能を操作する事により、利用者代行プロセスは、オーディットログ定義情報テーブルのレコードを更新し、オーディットログ定義情報を更新する。

6.2. FIA_ATD.1

利用者は、識別認証に使用したユーザが所属するグループに設定されている権限情報を取得することができる。

6.3. FIA_SOS.1

ユーザのパスワードが 6 文字以上 64 文字以下の文字列で、先頭または、末尾に全角・半角スペースがないことを検証する。

6.4. FIA_UAU.1

パスワードを用いて利用者を認証する。
また、利用者の認証前にヘルプ機能を許可する。

6.5. FIA_UAU.7

入力したパスワードの文字数と同数のアスタリスクをパスワードの入力フィールドに表示する。

6.6. FIA_UID.1

ユーザ名を用いて利用者を識別する。
また、利用者の識別前にヘルプ機能を許可する。

6.7. FIA_USB.1

利用者の識別認証が成功した場合に、利用者代行プロセスに対し識別認証で使用したユーザが所属するグループに設定されている権限情報を関連付ける。
ユーザ管理権限を持つ利用者は、参照権限を除く権限情報の変更を行うことができる。
権限情報はオーディットログ参照権限を除いて、即時に変更が反映される。オーディットログ参照権限は、再度ログインを行った場合に変更が反映される。

6.8. FMT_MSA.1

ユーザ管理権限を持つ利用者は、参照権限を除く権限情報の変更を行うことができる。
権限の関係を図 4に示す。
上位の権限が有効でない場合は、下位の権限を設定することはできない。
図中では、参照権限が最も上位の権限である。

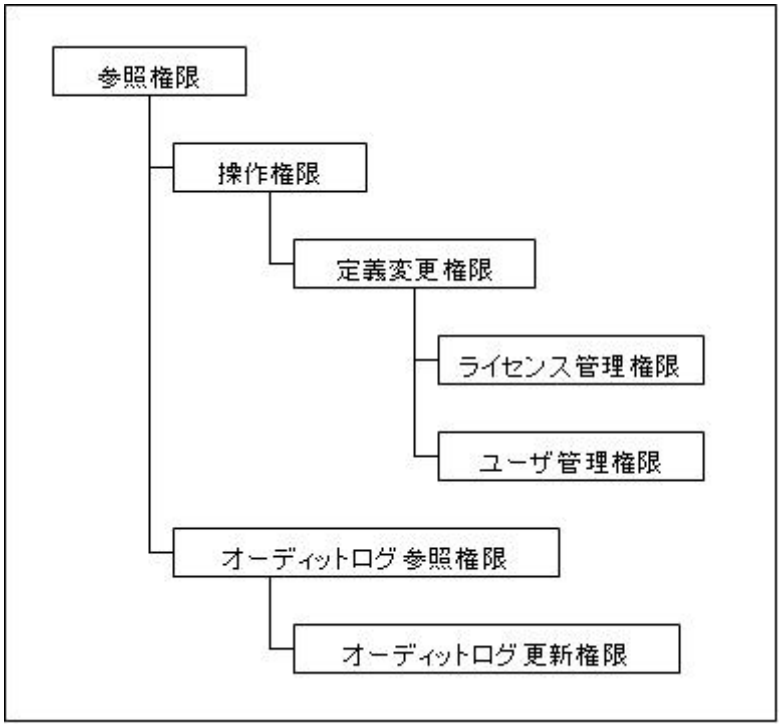

図 4 権限情報関連図

6.9. FMT_MSA.3

データアクセス制御 SFP に基づき、各種テーブルは、起動時に作成され以後変更されない。

6.10. FMT_MTD.1

識別認証された利用者は、自身のユーザのパスワードを変更することができる。
ユーザ管理権限を持つ利用者は、自身を含む全てのユーザのパスワードを変更することができる。
また、ユーザの登録、削除、参照、ユーザ名及びパスワードを除くユーザ情報の変更を行うことが可能である。
さらに、グループの登録、削除、グループ情報の変更、参照も行うことができる。

6.11. FMT_SMF.1

利用者に適用するセキュリティ管理機能と権限情報との対応関係を表 15に示す。

表 15 セキュリティ管理機能と権限の対応関係

権限情報 / セキュリティ管理機能	ユーザ管理権限	ユーザ管理権限以外
ユーザの追加機能	○	
ユーザの削除機能	○	
ユーザ情報参照機能	○	
ユーザ名、パスワードを除くユーザ情報変更機能 (*)	○	
パスワードの変更機能	○	
パスワード所有者本人のパスワード変更機能	○	○

権限情報 セキュリティ管理機能	ユーザ管理権限	ユーザ管理権限以外
グループの追加機能	○	
グループの削除機能 (*)	○	
グループ情報変更機能 (*)	○	
グループ情報参照機能	○	
参照権限を除く権限情報変更機能 (*)	○	

(*) 権限情報の変更のタイミングは、オーディットログ参照権限を除いて、即時に反映される。オーディットログ参照権限は、再度ログインを行った場合に反映される。

6.12. FMT_SMR1

利用者の識別認証が成功した場合に、識別認証で使用したユーザが所属するグループに設定されている権限情報を用いて、利用者に役割を割り当てる。

また、一人の利用者に複数の役割を割り当てる事ができる。

ユーザ情報管理者は自身に対し全ての権限を付与することができ、ビルトイン管理者と同等の権限を保持することができる。

権限情報と役割の対応関係を表 16に示す。

表 16 権限と役割の対応関係

利用者 役割 権限情報	管理者						オペレータ	
	ビルトイン管理者	ライセンス管理者	オーディットログ参照管理者	オーディットログ更新管理者	ユーザ情報管理者	定義情報管理者	操作オペレータ	参照オペレータ
参照権限	○	○	○	○	○	○	○	○
操作権限	○	○		○	○	○	○	
定義変更権限	○	○		○	○	○		
ユーザ管理権限	○				○			
ライセンス管理権限	○	○						
オーディットログ参照権限	○		○	○				
オーディットログ更新権限	○			○				