OSⅣ/MSP セキュア AF2
セキュリティターゲット

Version 1.14

2007/2/15

富士通株式会社

- 更新履歴 -

バージョン	日付	更新箇所	更新内容	作成者
1.00	2006/09/06	新規作成	―	富士通株式会社
1.01	2006/09/25	2章	・記載の一貫性の観点での修正	富士通株式会社
		4章	・記載の追加	
		5章	・記載の追加	
		6章	・記載の追加	
		8章	・記載の追加	
1.02	2006/10/3	2章	・全体的な記載の修正	富士通株式会社
		4章	・全体的な記載の修正	
		5章	・全体的な記載の修正	
		6章	・全体的な記載の修正	
		8章	・全体的な記載の修正	
1.03	2006/10/31	2章	・全体的な記載の修正	富士通株式会社
		3章	・前提条件の記載を修正 ・脅威の記載を修正	
		5章	・全体的な記載の修正	
		8章	・全体的な記載の修正	
1.04	2006/11/09	2章	・記載の修正	富士通株式会社
		5章	・記載の修正	
		6章	・記載の修正	
		8章	・記載の修正	
1.05	2006/11/15	2章	・所見対応	富士通株式会社
		3章	・所見対応	
		5章	・誤記修正	
		8章	・誤記修正	
1.06	2006/12/04	4章	・所見対応	富士通株式会社
		5章	・所見対応	
		6章	・所見対応	
		8章	・所見対応	
1.07	2006/12/14	5章	・所見対応	富士通株式会社
		6章	・所見対応	
		8章	・所見対応	

1.08	2007/1/10	2章	・所見対応	富士通株式会社
		3章	・所見対応	
		5章	・所見対応	
		6章	・所見対応	
		8章	・所見対応	
1.09	2007/02/05	2章	・所見対応	富士通株式会社
		5章	・所見対応	
		6章	・所見対応	
		8章	・所見対応	
1.10	2007/02/07	6章	・記載修正	富士通株式会社
		8章	・記載修正	
1.11	2007/02/08	6章	・記載修正	富士通株式会社
		8章	・記載修正	
1.12	2007/02/13	6章	・記載修正	富士通株式会社
		8章	・記載修正	
1.13	2007/02/14	6章	・記載修正	富士通株式会社
		8章	・記載修正	
1.14	2007/02/15	6章	・記載修正	富士通株式会社
		8章	・記載修正	

～ 目次 ～

～ 図目次 ～

～ 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 の識別と管理

名称：OSⅣ/MSP セキュア AF2　セキュリティターゲット

バージョン：1.14 版

作成日：2007 年 2 月 15 日

作成者：富士通株式会社

1.1.2. TOE の識別と管理

TOE 名称　：OSⅣ/MSP セキュア AF2

TOE バージョン：V10L10　C06121

なお、TOE は以下 4 つのソフトウェアコンポーネントで構成され、

それぞれにバージョンが存在する。

・AF2 :V10L10 C06121.PTF

・RACF :V12L10 C05091.PTF

・TSS/E :V11L20 C06061.PTF

・VTAM-G:V30L20 C06121.PTF

作成者：富士通株式会社

1.1.3. 適用する CC のバージョン

・Common Criteria for Information Technology Security Evaluation Ver2.3

・補足-0512適用

1.2. ST 概要

本 ST は、エンタープライズ向けの OS である、「OSⅣ/MSP セキュア AF2」のセキュリティ仕様を規定している。

本 IT 製品を使用することにより､利用者は情報センタ内において許可された権限の範囲内で、資源を利用した作業をセキュアに行うことが可能となる。本 IT 製品では、主に以下の機能を提供する。

- アプリケーションのマルチタスクな実行環境を提供する、OS 基本機能
- 利用者が正当な人物であることを確認する、識別認証機能
- 利用者の情報センタ内に存在するデータへのアクセス許可／拒否の判定、及び、アクセス権限内でのみデータ操作を可能とする様に制限する、アクセス制御機能
- 情報センタへの不正なアクセスの兆候がないかを確認する、監査機能
- TOE の機能への設定管理を行う、TOE 管理機能

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。

1.4. 参考資料

・Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model August 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 August 2005 Version 2.3

・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

1.5. 表記規則、用語・略語

1.5.1. 表記規則

第 3 章の前提条件、脅威、組織のセキュリティ方針、及び第 4 章のセキュリティ対策方針では、それぞれのラベルを**ボールド体**フォントで記述し、続けてその定義を通常フォントで記述する。第 5 章のセキュリティ機能要件では、操作内容を*イタリック体*フォントで記述する。また、環境のセキュリティ機能要件に、識別子に[E]を付与する。

1.5.2 用語・略語

本STで使用する用語・略語を 表 1-1 に定義する。

表 1-1 用語・略語定義

用語・略語	定義内容
情報センタ	TOE を利用して構築された組織
GS シリーズ PRIMEFORCE シリーズ	富士通が提供するメインフレーム。 参考 URL：http://globalserver.fujitsu.com/jp/
資源	情報センタ内で扱う資源のこと。資源には、以下が含まれる。 ・データセット - DASD データセット - 磁気テープデータセット ・一般資源 - DASD ボリューム - 磁気テープボリューム
エンタープライズ向け	企業向け
DASD	Direct Access Storage Device の略称。 アドレスを直接指定することにより、書き込み、読み込みが

用語・略語	定義内容
	可能となる記憶装置。
ボリューム	記憶装置の単位。 ボリュームには、DASD ボリューム、磁気テープボリュームがある。
ボリューム通し番号	ボリュームに付与される名称。
データセット	DASD ボリューム、及び磁気テープボリューム内に存在するデータ群。DASD ボリューム内に存在するデータセットを、DASD データセットと呼ぶ。また、磁気テープボリューム内に存在するデータセットを、磁気テープデータセットと呼ぶ。 なお、データセットには、アプリケーションも含まれる。
RACF	Resource Access Control Facility の略。
RACF 機能	TOE が提供する機能の内、「識別認証機能」、「アクセス制御機能」、「監査機能」、「TOE 管理機能」の 4 つの機能を含めた総称。
RACF 管理簿	TOE の動作や、利用者・グループの権限等が記載される、TOE の設定に関わるデータ。
RACF 空間	RACF 機能が動作しているメモリ空間
VSAM	Virtual Storage Access Method DASD の装置タイプに依存しないアクセス法。VSAM データセットに対して順次、直接あるいはスキップ順にデータの読み込み、書き出し、追加、更新、あるいは削除を行うことができる統合されたアクセス法である。
コントロールインタバル	固定長のブロック
本名グループ	グループ間の定義を行い「グループのグループ化」をした際、基となるグループである。 一方、定義に従い関連付けられたグループを「別名グループ」と呼ぶ。
現用グループ	利用者が操作を行なう際、所属しているグループ
利用者に関する情報	利用者の識別子や、デフォルトで所属するグループ、「失権」「復権」等の状態を示した情報。
グループに関する情報	当該グループが、構造化／非構造化グループか、グループの管理者名等を示した情報
資源に関する情報	資源名や、設定されているアクセス権を示した情報
制御ブロック	TOE の動作を規定している RACF 管理簿内のデータブロック
RACF 標準命名規約	データセットの管理を容易に行なうために付与される、データセットの命名規則。この規則とは、以下の通り。

用語・略語	定義内容
	英字で始まる最大 8 文字の英数字列のことを単純名と言う。2 つ以上の単純名を、ピリオド“.”で連結した文字列のことを修飾名と言う。データセット名が単純名の場合には、単純名そのものを、また、修飾名の場合には、データセット名の最初の単純名を、第一修飾子と言う。 データセットを RACF 管理簿に登録するためには、第一修飾子は、RACF 管理簿に登録されている利用者の利用者識別名か、グループのグループ名（グループ識別名）の何れかでなければならない。
プログラム	本書においては、アプリケーションと同義
JCL	Job Control Language： TOE を利用する際に使用する言語
センタ出口ルーチン	RACF(特にアクセス制御)の処理を情報センタ固有に定義する際に利用する。

2. TOE 記述

本章では「TOE 種別」、「TOE 概要」、「TOE の物理的構成」、「TOE に関わるグループ及び人物」、「保護資産」、「TOE の論理的構成」、及び「TOE の利用方法」について記述する。

2.1. TOE 種別

TOE である「OSⅣ/MSP セキュア AF2」は、利用者のアクセス制御、識別認証等のセキュリティ面での強化を行ったエンタープライズ・コンピューティング向けの OS であり、TOE の種別としては、IT 製品である。

2.2. TOE 概要

2.2.1. TOE の利用目的

本 TOE は、利用者のアクセス制御、識別認証等のセキュリティ面での強化を行ったエンタープライズ・コンピューティング向けの OS である。本 TOE により、利用者が使用する TOE 上のアプリケーションは、マルチユーザかつマルチタスクに動作することができる。

また、本 TOE により、利用者と資源間のアクセス関係を詳細に定義することができ、定義に従ったアクセス制御が行われることで、利用者は情報センタ内で許可された権限の範囲内で資源を利用した作業をセキュアに行うことができる。

2.3　　TOE の物理的構成

2.3.1　TOE のネットワーク構成

TOE は、下図に示す情報センタにおいて、「TOE」と示した機器（GS/PRIMEFORCE シリーズサーバ）に導入されて動作する。また、図において破線は、物理的な保護環境が必要であることを示している。

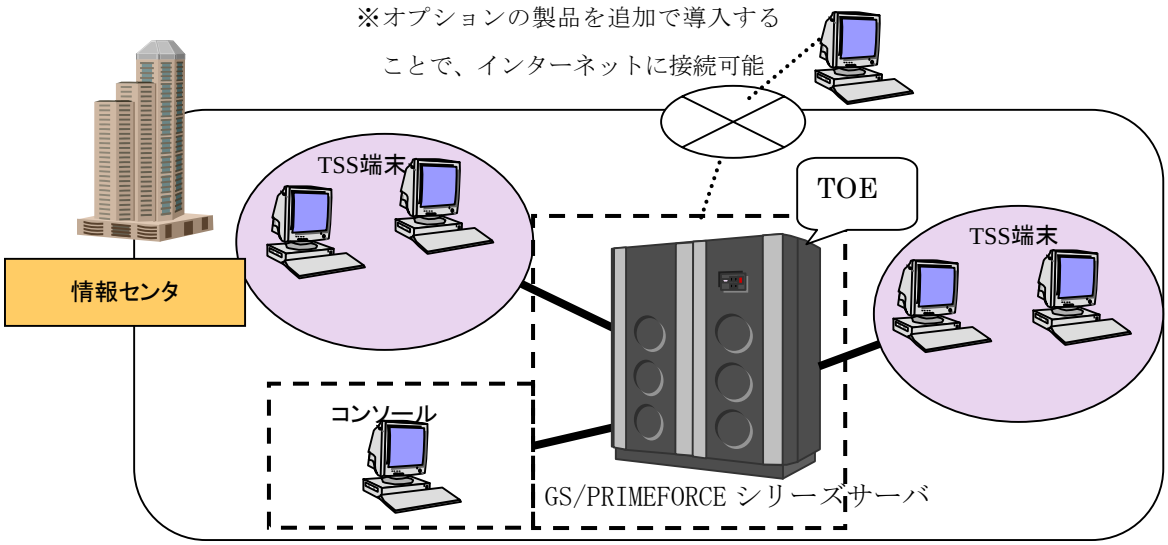

図 2-1 TOE の物理的範囲（ネットワーク構成）

本 TOE のソフトウェア構成（2.3.3 を参照）には、インターネットに接続するプログラムが含まれていない。そのため、本 TOE は、単体ではインターネットに接続することはできないが、オプションの製品を追加で導入することでインターネットに接続することが可能となる。

本 ST では、インターネットには接続できない、TOE 単体での運用を想定している。

以下では、図 2-1 に示した各機器を説明する。

・GS/PRIMEFORCE シリーズサーバ

TOE が搭載されて動作する、富士通製のメインフレームサーバ。本サーバに、資源を格納する DASD ボリュームや磁気テープボリュームが設置される。なお、GS/PRIMEFORCE シリーズサーバは、TOE において特権を有するユーザである、RACF センタ要員以外、入退室できないような物理的に保護された場所に設置される必要がある。

・TSS 端末

TOEの関連者（後述する、「2.4 TOEに関わるグループ及び人物」を参照）が、TOEを利

用する際に使用する端末である

・コンソール

RACF センタ要員が、TOE の保守、運用を行う際に使用する端末である。但し、コンソールは、RACF センタ要員以外、入退室できないような物理的に保護された場所に設置される必要がある。

2.3.2 TOE の動作環境

「2.3.1 TOE のネットワーク構成」で示した通り、TOE は以下のサーバに導入されて動作する。

・GS シリーズサーバ

・PRIMEFORCE シリーズサーバ

2.3.3 TOE のソフトウェア構成

TOEのソフトウェア構成要素の諸元について、表 2-1 に示す。

表 2-1 TOE のソフトウェアの諸元

NO	構成プログラム名	バージョン	提供機能
1	AF2	V10L10 C06121.PTF	・監査機能 ・TOE 管理機能 ・資源利用機能 ・OS 基本機能 ・各種ユーティリティ ・自動運転機能 ・システム監視 ・トラブルシューティング用ツール ・システム編集・ソフトウェア修正適用ツール
2	RACF	V12L10 C05091.PTF	・識別認証機能 ・アクセス制御機能 ・TOE 管理機能 ・監査機能
3	TSS/E	V11L20 C06061.PTF	・端末接続機能
4	VTAM-G	V30L20 C06121.PTF	・端末接続機能

なお、表の「提供機能」欄で記載している機能の詳細は、「2.6 TOE の論理的構成」を

参照して頂きたい。

2.4　　TOE に関わるグループ及び人物

2.4.1 利用者とグループ

本節では、グループの定義、グループの種類、利用者とグループの関係について説明する。

●グループとは

グループとは、情報センタを利用する利用者を、目的に沿って集合させた集団のことである。以降では、グループについての詳細を説明する。

●グループの種類

グループは、管理方法の違いにより「構造化グループ」または、「非構造化グループ」に分類される。「構造化グループ」、「非構造化グループ」とは、以下の通りである。

・非構造化グループ

グループ間に、階層構造に関係したフロー制御の規則を持たせないグループ構造である。非構造化グループのイメージ図を、図 2-2 に示す。

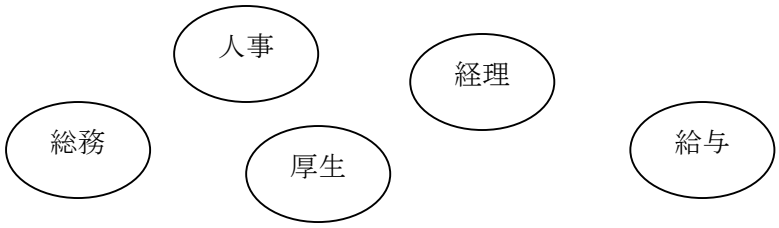

図 2-2 非構造化グループのイメージ図

[図の補足]

各グループ間に、階層構造などの関係はない。

・構造化グループ

グループ間に階層構造を持たせ、資源の利用範囲と情報の流通範囲に、上下関係によるフロー制御を行うことを可能とするグループ構造である。

構造化グループのイメージ図を、図 2-3 に示す。

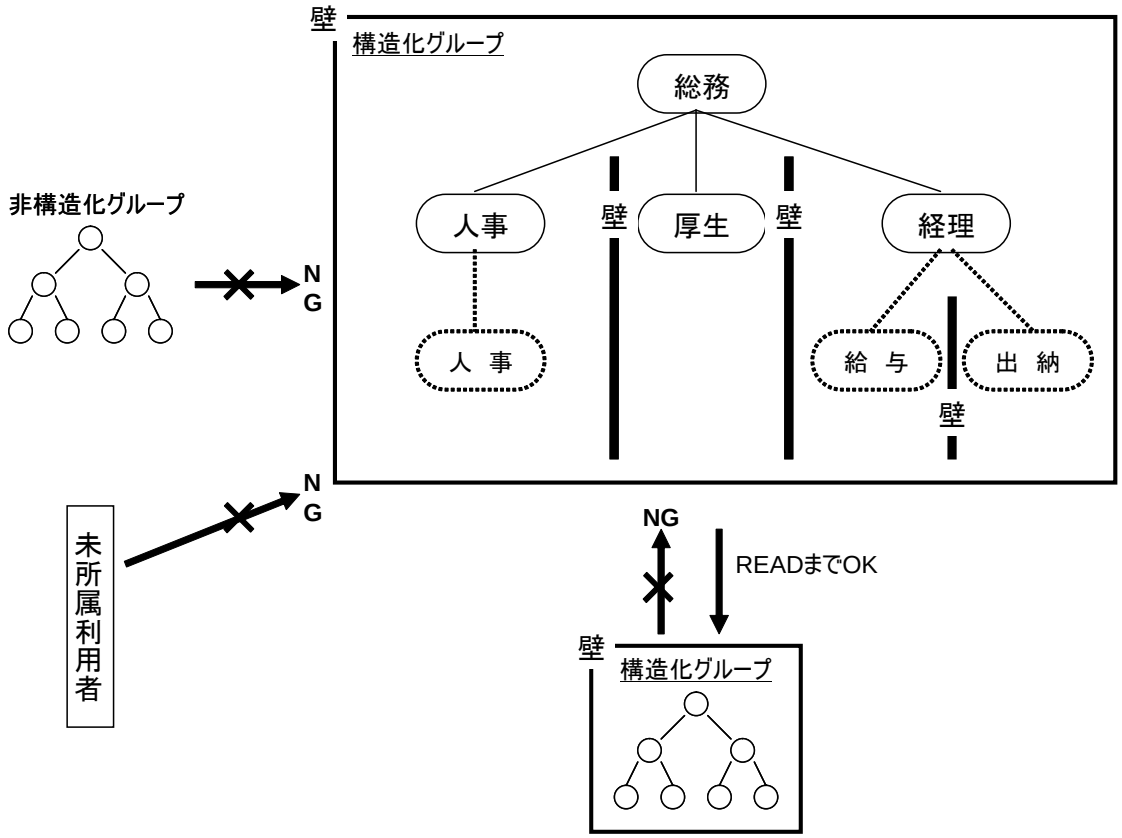

図 2-3 構造化グループのイメージ図

[図の補足]

図に示している通り、グループ間には、「上位階層のグループは、下位階層のグループ（の所有するデータセット）を、読み出しまで許可」のような制限が施される。

なお、この「非構造化グループ」及び「構造化グループ」は、グループの統合によって構築される。

●利用者とグループの関係

利用者は、グループに所属する利用者、または、グループに所属しない利用者に分類される。以下、それぞれについて説明する。

・グループに所属しない利用者

グループに所属しない利用者は、利用者に与えられている権限の範囲内で TOE を利用することができる。

・グループに所属する利用者

グループに所属している利用者は、利用者に与えられている権限と、所属しているグループに依存した権限の範囲内で TOE を利用することができる。

グループの利用者はTOEを利用する場合に、グループを明示的に指定してグループに所属する場合と、グループ名を指定せずデフォルトで設定されたグループ（このグループを「デフォルトグループ」と呼ぶ）に所属する場合の2種類の利用方法がある。但し、グループを明示的に指定して所属する場合、当該利用者は、指定対象のグループに予め登録されている必要がある。(利用者を複数のグループに登録することが可能。)

2.4.2 TOEの関係者

本節では、TOE へアクセスする人物（アクセス権限を有する者、有さない者）の体系について説明する。また、アクセス権限を有する者に関して、与えられる役割について説明する。

■TOEへアクセスする人物の体系

TOEへアクセスする人物には、TOE内の資源へアクセスする権限を有する人物と、権限を有さない人物が存在する。アクセスする権限を有する人物は、「登録済み利用者」及び「記名利用者」であり、アクセスする権限を有さない人物は、「未登録利用者」、「無記名利用者」である。詳細を以下に示す。

・登録済み利用者

RACF管理簿に登録されている利用者である。

・未登録利用者

RACF 管理簿に登録されていない利用者である。

・記名利用者

登録済み利用者が、利用者識別名と利用者パスワードを示して情報センタを利用するとき、その利用者を「記名利用者」と呼ぶ。

・無記名利用者

匿名利用者。利用者が、利用者識別名と利用者パスワードを示さずにデータセンタを利用する場合、当該利用者を「無記名利用者」と呼ぶ。未登録利用者は、TSS 端末を利用する際に、TOEにて登録されていない利用者識別名を示しても、「無記名利用者」としてTOEに判断される。

上記の利用者の体系を示したイメージを、図 2-4 に示す。

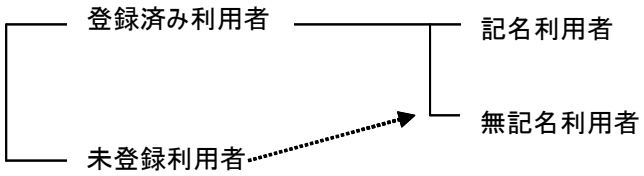

図 2-4 利用者体系のイメージ図

以降は、「記名利用者」についての役割を説明する。なお、以降、特に断りの無い場合、記名利用者のことを、「利用者」または「TOE の関係者」と呼ぶ。

TOE の関係者は、以下に示す「RACF センタ要員」、「管理者」、「一般利用者」である。

2.4.2.1 最高管理者

最高管理者は、情報センタ内の運用において責任を持つ人物を指す。最高責任者は、RACF センタ要員、管理者の任命を行なう。

2.4.2.2 RACF センタ要員

RACF センタ要員は、情報センタでの運用を考え、資源の保護体系を構築し、情報センタの保全を図る人物を指す。

なお、RACF センタ要員は、TOE の運用等の重要な行為を行うため、信頼できる人物でなければならない。

2.4.2.3 管理者

管理者は、一般利用者や、一般利用者が所属するグループ、資源を管理する人物である。

なお、管理者は、利用者・グループ、及び資源の管理行為を行うため、信頼できる人物でなければならない。

2.4.2.4 一般利用者

一般利用者は、TOE(延いては、情報センタ)を利用する人物である。TOE に対して特別な権限を有さない。

2.5　保護資産

2.5.1　TOE が取り扱う資源

本節では、TOE が取り扱う資源について説明する。

TOE が取り扱う資源は、「データセット類」と「一般資源類」に大別される。なお、以下では「類」という単語を付与して説明しているが、これは資源「群」のことを表している。

■データセット類

データセット類は、物理媒体毎に、DASD データセット、磁気テープデータセットに分類される。データセット類は、後述する「一般資源類」のボリューム類の中に存在する。また、データセット類には、利用者によって実行され TOE 上で動作する、「アプリケーション」がある。

なお、データセットには、管理を容易に行えるように「RACF 標準命名規約」が付与される。

■一般資源類

データセット類以外の、TOE で取り扱う資源である。一般資源類には以下がある。

・DASD ボリューム類

DASD ボリューム自体である。DASD ボリュームは、「ボリューム通し番号」により識別される。

・磁気テープボリューム類

磁気テープボリューム自体である。磁気テープボリュームは、「ボリューム通し番号」により識別される。

2.5.2 TOE の保護対象資産

「2.5.1 TOE が取り扱う資源」により、TOE の保護資産の候補は以下である。

・データセット類

・一般資源類

なお、上記資源に対し、機密性／完全性を保証するかどうかの判断は、資源の所有者の方針により決定される。

RACF 管理簿へ登録されていない資源(「未登録資源」)については、保護対象外であるが、当該資源へのアクセスは TOE の制御によりデフォルトでは拒否される。

なお、「TOE 管理機能」にて、作成した資源をデフォルトで RACF 管理簿に登録する「TOE の動作設定」にしておけば、一般利用者は意識することなく、作成した資源は RACF 管理簿に登録される。

一般資源類における磁気テープボリュームは、TOE が動作するサーバから取り外され、持ち出されることが想定される資源であるが、サーバから取り外された資源は TSC 外の資源となるため、保護対象外の資源とする。

TOE と TSS 端末間のネットワークを流れる資源も保護対象となる。ただし、このネットワークは、一般的な TCP/IP とは異なる、TOE 独自のプロトコルを利用している。

これら保護資産の関係について示したイメージ図を、「図 2-5 保護資産のイメージ図」に示す。

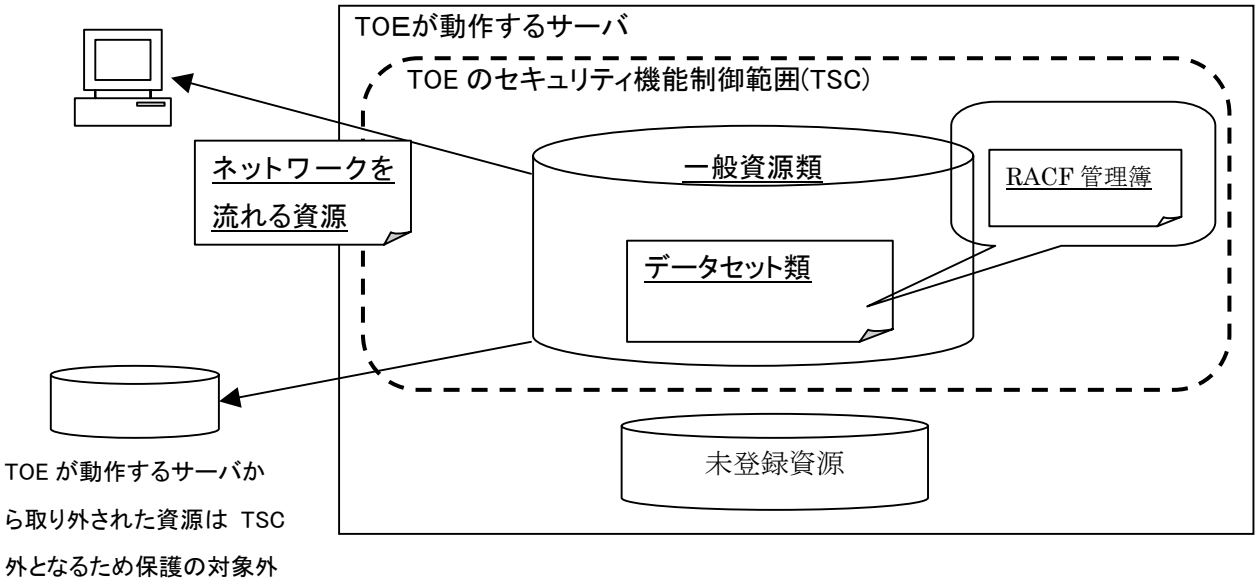

図 2-5 保護資産のイメージ図

[図の説明]

図において、下線で示した資源が保護対象資産である。

整理すると、保護資産は以下である。

- RACF 管理簿に登録された、データセット類
- RACF 管理簿に登録された、一般資源類
- ネットワークを流れる資源

2.6　TOE の論理的構成

本節では、本 TOE の論理的構成（TOE が提供する機能）を示す。利用者は、TSS 端末またはコンソールからコマンドを使用して、各機能を利用する。TOE の機能は以下である。

[セキュリティ機能]

・OS 基本機能
・識別認証機能
・アクセス制御機能
・監査機能
・TOE 管理機能

[非セキュリティ機能]

・資源利用機能
・システム監視機能
・各種ユーティリティ機能
・自動運転機能
・トラブルシューティング用ツール
・システム編集・ソフトウェア修正適用ツール
・端末接続機能

なお、当該機能を利用する端末毎に、TSS 端末（TSS 端末から利用する場合）と、コンソール（コンソールから利用する場合）と表記する。
但し、利用者に公開しているインタフェースを有する機能のみに限定する。

2.6.1　OS 基本機能

本機能は、OS としての基本機能として、複数の利用者が複数のアプリケーションを実行するマルチユーザ、かつマルチタスク環境を提供する。

本機能は、以下に示す機能を提供することで、マルチユーザかつマルチタスク環境を実現する。

- ハードウェアとの連携
- 仮想空間管理
- 複数利用者の管理
- TOE およびアプリケーション実行環境の提供
- 外部記憶装置（DASD ボリューム、磁気テープボリューム）に対するインタフェースの提供と管理

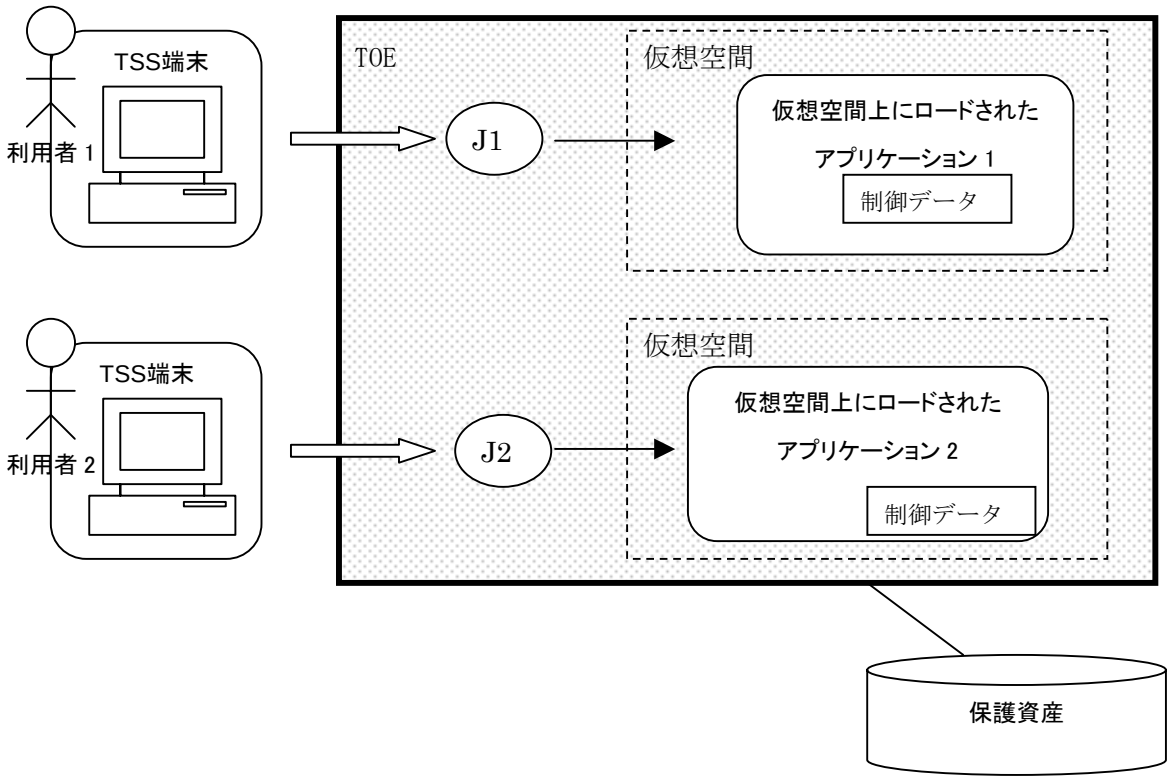

図 2-6 OS 基本機能の概念図

[図の説明]

図 2-6 の J1、J2 は、利用者を代行して TOE 内に存在するジョブである。
ジョブがアプリケーションを起動すると、「OS 基本機能」が提供する「TOE およびアプリケーション実行環境」により、OS に対する制御データが付与され仮想空間上にロードされる（図の、アプリケーション 1,2)。ジョブは、アプリケーションを通して保護資産へのアクセスを行なう。
「OS 基本機能」が提供する「仮想空間管理機能」により、仮想空間にはそれぞれ独立した仮想アドレスが割り付けられ、仮想空間を越えた互いの干渉は不可能となっている。それにより不正な利用者が、自身の起動したアプリケーションの仮想空間を越えて他のアプリケーションの制御データを改変することによって TOE を改変したり損害を与えたりすることや、他の利用者が仮想空間上にロードした保護資産を改変したり覗き見たりすることは防がれている。

2.6.2　　識別認証機能

本機能により、TOE の関係者は利用者識別名（グループに所属している場合、グループ識別名も併せて）及びパスワードを入力し、情報センタの資源を使用しても良い、正当な人物であるかを識別認証される。

本機能の管理（例えば、パスワード自体やパスワード有効期限の変更、「識別認証機能」の動作形式）は、「TOE 管理機能」にて行われる。

2.6.3　　アクセス制御機能

本機能は、TOE の関係者・グループ・アプリケーションに対して、定められた設定に従って、情報センタ内の資源へのアクセスを制御する機能である。資源へのアクセスが許可された場合、許可されたアクセス権レベル（書込み、読込み、実行）で資源への操作が可能となる。資源へのアクセスが拒否された場合、アクセス禁止となる。

2.6.3.1 アクセス制御の判定方法

本機能が資源アクセスを判定する方法は、大別すると以下の 2 種類がある。

・利用者・グループ・アプリケーションと資源間の定義関係を利用した判定

　利用者、グループ、アプリケーションと資源間のアクセス許可/拒否、及びアクセス権レベルを定義し、その定義に従ってアクセス制御を行なう方法。

・グループの構造を利用した判定

　各グループに上下関係を付与し、グループ間の階層構造により、グループが所有する資源へのアクセスの可/不可を判定する方法。但し、資源を所有するグループが、構造化グループである場合に限る。

なお、本機能の設定は、後述の「2.6.6 TOE 管理機能」にて行われる。

2.6.4　　監査機能

TSS 端末

本機能により、情報センタの利用状態や資源へのアクセスに対する監査ログが採取される。監査ログを監査することにより、不正な利用者が情報センタ及び資産を使用していないかを確認できる。監査ログの採取イベントとしては、「すべてのアクセスログを収集する」、「正当なアクセスログを収集する」、「不当なアクセスログを収集する」、「アクセスの記録を収集しない」から、監査レベルを設定することができる。なお、この設定は、「TOE 管理機能」にて行われる。

本機能は、監査ログを RACF センタ要員が監査し易いように編集し、監査レポートとして出力する機能を提供する。また、本機能は、自身が所有する資源に対して、監査レポートを出力する機能を併せて提供している。また、管理者に対しては、当該役割が管理するグループのデータセットに対して、監査レポートの出力を行う機能を提供している。

なお、監査ログが一杯になった場合、格納場所を交代用データセットに自動的に切り替え、かつ、監査ログが一杯になったことを RACF センタ要員へ通知する。

2.6.5 TOE 管理機能

本機能は、RACF センタ要員、管理者が管理行為を行なう際に利用する機能である。また、本機能は、一般利用者が、自身の TOE における設定を、限られた範囲で行う際に利用する機能である。以下では、TOE の関係者毎に本機能の内容を説明する。

2.6.5.1 RACF センタ要員向け機能

RACFセンタ要員向け機能を、表 2-2 に示す。

表 2-2 RACF センタ要員向け TOE 管理機能

NO	管理機能
1	・RACF 管理簿の問い合わせ、改変 コンソール、TSS 端末、 ・資源のデフォルトアクセス権の設定 TSS 端末
	・RACF 管理簿のバックアップ、稼動・非稼動制御コンソール、TSS 端末 ・監査ログの保全 コンソール
	時間情報の改変 コンソール
2	・セキュリティ機能のふるまいの決定、改変 コンソール ・セキュリティ機能の起動、停止 TSS 端末
3	利用者に関する情報の問い合わせ・改変・削除 TSS 端末
4	アプリケーションの、問い合わせ・改変・削除 TSS 端末
5	資源に関する情報の問い合わせ・改変・削除 TSS 端末
6	グループに関する情報の問い合わせ・改変・削除 TSS 端末
7	JCL による資源アクセス要求の定義 TSS 端末

2.6.5.2　　管理者向け機能

管理者向け機能を、表 2-3 に示す。

表 2-3 管理者向け TOE 管理機能

NO	管理機能
1	管理下の利用者に関する、利用者の情報の問い合わせ・改変・削除 TSS 端末
2	管理下のアプリケーションの、問い合わせ・改変・削除　TSS 端末
3	管理下の利用者における、資源に関する情報の問い合わせ・改変・削除 TSS 端末
4	管理下のグループに関する、情報の問い合わせ・改変・削除　TSS 端末
5	JCL による資源アクセス要求の定義　TSS 端末

2.6.5.3　　一般利用者向け機能

一般利用者向け機能を、表 2-4 に示す。

表 2-4 一般利用者向け TOE 管理機能

NO	管理機能
1	自身の利用者に関する情報の問い合わせ・改変・削除　TSS 端末
2	自身が所有するアプリケーションの、問い合わせ・改変・削除　TSS 端末
3	自身が所属するグループに関する情報の設定機能　TSS 端末
4	自身が所有する資源に関する情報の設定機能　TSS 端末
5	JCL による資源アクセス要求の定義　TSS 端末

2.6.6　　資源利用機能

TSS 端末

本機能は、TOE にて扱う資源（データセット類、一般資源類）の利用を行うための機能である。資源の利用とは、以下を指す。

- 資源へのデータの書き込み
- 資源からのデータの読み出し
- 資源（アプリケーション）の実行

2.6.7　　各種ユーティリティ機能

TSS 端末

本機能は、以下に示す機能を提供することで、システムの管理および保守を行うための各種ユーティリティを提供している。

- 情報センタに存在するデータの管理と保守
- TOE の動作アプリケーションの障害を調査する情報の収集
- 外部記憶装置の保守（初期化、不良トラック交換、定期検査）
- 資源に対するバックアップ、リカバリ

2.6.8　　自動運転機能

TSS 端末

本機能は、利用者のオペレーションを自動化し、システムの効率的運用とオペレーションの省力化を実現する機能を提供する。

2.6.9　　システム監視機能

TSS 端末

本機能は、以下の機能を提供することで、TOE を含む情報センタ全体を安全に運用するため、ハードウェアの利用状態、CPU 故障およびプログラムの性能異常による障害の発生を検知する。

- 定期的なハードウェアのチェック
- ハードウェア資源利用状況の収集およびレポート出力

2.6.10　　トラブルシューティング用ツール

TSS 端末

本機能は、以下の機能を提供することで、情報センタで発生した事象の調査／解析を行うためにトラブルシューティング用ツールを提供する。

- 出力されたメッセージやシステム完了コードの調査
- プログラムの異常終了で採取した資料の調査

2.6.11　　システム編集・ソフトウェア修正適用ツール

TSS 端末

本機能は、以下の機能を提供することで、TOE の動作プログラムの修正を行うためのシステム編集・ソフトウェア修正適用ツールを提供する。

- 修正プログラムの生成
- 修正プログラムのインストールに必要な資源の生成
- 修正プログラムの適用

2.6.12　　端末接続機能

本機能は、以下の機能を提供することで、TSS 端末を接続するための環境を提供する。

- ネットワーク定義の作成
- TSS 端末と TOE 間のデータ転送の制御

(補足) TOE の機能間の関係

2.6 において説明した機能間の関係を示したイメージを、図 2-7 に示す。

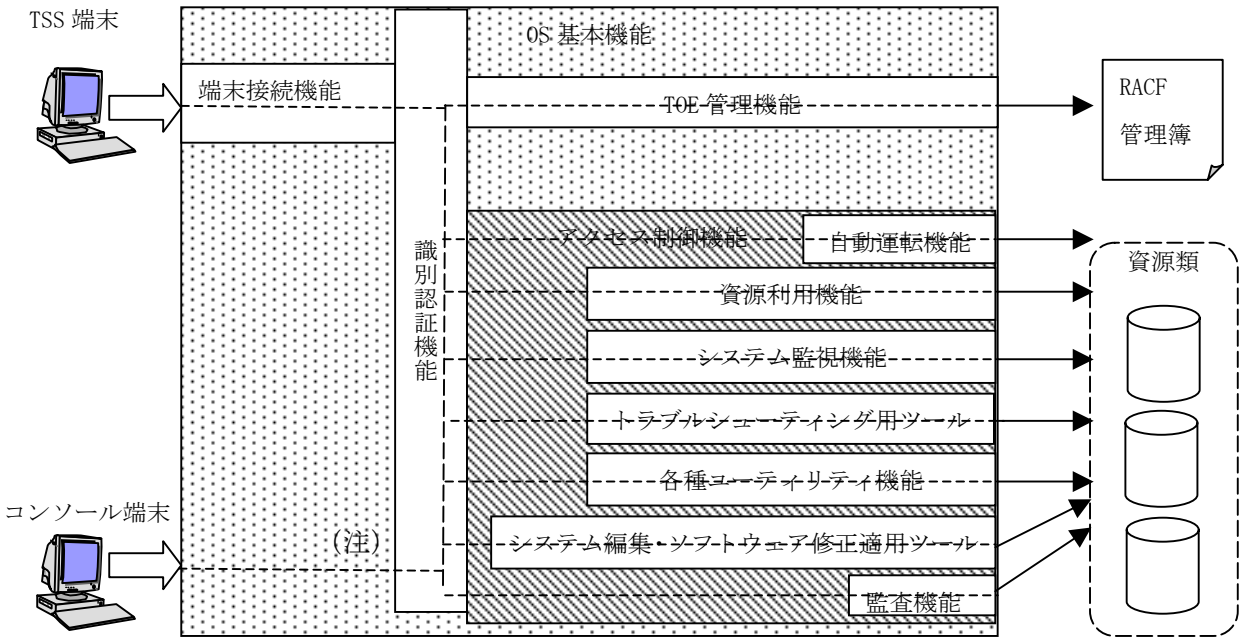

図 2-7 TOE の機能間の関係イメージ

注) コンソール端末から TOE 管理機能 (RACF 管理簿の保守) を利用する際には、識別認証機能は動作しない。

[図の説明]

「OS 基本機能」は、それ以外のすべての機能が動作する際に必要とされる機能である。

「端末接続機能」は、TSS 端末を利用する際に最初にコールされる。但し、「識別認証機能」は、コンソール端末からの「TOE 管理機能」の利用の際には動作しない。

「自動運転機能」、「資源利用機能」、「システム監視機能」、「トラブルシューティング用ツール」、「各種ユーティリティ機能」、「システム編集・ソフトウェア修正適用ツール」、「監査機能」は、資源類にアクセスするインタフェースを有する機能である。

「TOE 管理機能」は、RACF 管理簿へアクセスするインタフェースを有する機能である。「TOE 管理機能」は「アクセス制御機能」の対象外だが、RACF センタ要員、管理者、一般利用者の役割毎に利用可能な機能が制限されている。

2.7 TOE の利用方法

本節では、TOE の関係者が行う操作について説明する。なお、以下の【管理（IT）の操作】については、「2.6 TOE の論理的構成」において、TSS 端末、コンソールと記載した機能に限定して記載する。なお、最高責任者は、TOE の操作を行なわないため、下表において、説明は省略する。

[表の読み方]

【運用（非 IT）の操作】:**(導入フェーズ)**：導入フェーズで行なう、当該役割の運用操作。

【アクセス方法】：当該役割が、TOE の機能を利用するためのアクセス方法。

【管理(IT)の操作】:**(運用フェーズ)**：当該役割が運用フェーズで行う IT 操作。

2.7.1 TOE の利用方法（RACF センタ要員編）

RACFセンタ要員が行なう行為について、表 2-5 に記載する。

表 2-5 RACF センタ要員における TOE の利用方法

【運用（非 IT）の操作】:**(導入フェーズ)**	
・TOE のネットワーク環境、運用環境を構築する。この際、以下を遵守する必要がある。 － TOE を導入するサーバは、物理的にアクセス保護（入退出管理）された環境に設置する。 － TOE により構築される情報センタのネットワークは、外部ネットワークと分離された構成にする。 ・TOE のインストールを行う	
【アクセス方法】	
RACF センタ要員は、以下の方法により TOE にアクセスする。 ・物理的に保護された環境に入室した後、コンソール端末から TOE の機能を利用する。 ・TSS 端末にアクセスし、利用者識別名及びパスワードを入力し、「識別認証機能」よって正当な RACF センタ要員として識別認証された後、TOE の機能を利用する。	
【管理(IT)の操作】:**(運用フェーズ)**	
1	■TOE 管理機能の利用 RACF センタ要員は、「TOE 管理機能」を利用して、TOE の動作設定、RACF 管理簿の保守、RACF 空間の設定、センタ出口ルーチンの設定、全ての利用者に関する設定、全てのグループに関する設定、監査機能に関する設定を行なう。
2	■資源利用機能の利用 RACF センタ要員は、TOE にて扱う資源の保守を行う際に、必要に応じて、「資源利用機能」を利用して資源操作を行う。資源操作とは、以下の通り。 ・資源へデータを書き込みする

	・資源からデータを読み出しする ・資源（アプリケーション）を実行する
3	■各種ユーティリティ機能の利用 RACF センタ要員は、「各種ユーティリティ機能」を利用して、以下を行なう。 ・TOE の障害を調査する情報を収集する ・外部記憶装置の保守（初期化、不良トラック交換、定期検査）を行う ・資源に対するバックアップ、リカバリを行う
4	■システム監視機能の利用 RACF センタ要員は、「システム監視機能」を利用して、定期的なハードウェアのチェックや、ハードウェア資源利用状況の収集およびレポート出力を行う。
5	■自動運転機能の利用 RACF センタ要員は、「自動運転機能」を利用して、TOE の機能の自動運転をスケジューリングする。
6	■システム編集・ソフトウェア修正適用ツールの利用 RACF センタ要員は、「システム編集・ソフトウェア修正適用ツール」を利用して、以下を行う。 ・修正プログラムの適用に必要な資源を生成する ・TOE に修正プログラムを適用する
7	■監査機能の利用 RACF センタ要員は、「監査機能」を利用して、監査ログから監査レポートを出力する。

2.7.2　　TOE の利用方法（管理者編）

管理者が行なう行為について、表 2-6 に記載する。

表 2-6 管理者における TOE の利用方法

【運用（非 IT）の操作】: **(導入フェーズ)**	
・一般利用者に対し、パスワード管理の教育を行う。	
【アクセス方法】	
TSS 端末にアクセスし、「利用者識別名及びパスワードの入力」を利用し、「識別認証機能」よって、正当な管理者として識別認証された後、TOE の機能を利用する。	
【管理(IT)の操作】: **(運用フェーズ)**	
1	■TOE 管理機能の利用 管理者は、「TOE 管理機能」を利用して、管理下の利用者、資源、グループに関する設定を行なう。
2	■資源利用機能の利用 管理者は、管理下のグループが所有する資源を保守する際に、必要に応じて「資源利用機能」を利用して資源操作を行う。資源操作とは、以下の通り。 ・資源へデータを書き込みする ・資源からデータを読み出しする ・資源（アプリケーション）を実行する
3	■各種ユーティリティ機能の利用 管理者は、「各種ユーティリティ機能」を利用できない。
4	■システム監視機能の利用 管理者は、「システム監視機能」を利用できない。
5	■自動運転機能の利用 管理者は、「自動運転機能」を利用できない。
6	■システム編集・ソフトウェア修正適用ツールの利用 管理者は、「システム編集・ソフトウェア修正適用ツール」を利用できない。
7	■監査機能の利用 管理者は、「監査機能」を利用して、管理下のグループが所有するデータセットに対する監査レポートを出力する。

2.7.3 TOE の利用方法（一般利用者編）

一般利用者が行なう行為について、表 2-7 に記載する。

表 2-7 一般利用者における TOE の利用方法

【運用（非 IT）の操作】: **(導入フェーズ)**	
なし	
【アクセス方法】	
TSS 端末にアクセスし、「利用者識別名及びパスワードの入力」を利用し、「識別認証機能」よって、正当な一般利用者として識別認証された後、TOE の機能を利用する。	
【管理(IT)の操作】: **(運用フェーズ)**	
1	■TOE 管理機能の利用 一般利用者は、「TOE 管理機能」を利用して、自身の設定、自身が所属するグループに関する設定、自身が所有する資源に関する情報の設定を行なう。
2	■資源利用機能の利用 利用者は、自身が資源を所有し、その資源を利用するために「資源利用機能」を利用する。資源の利用とは以下の通りである。 ・ 資源へデータを書き込みする ・ 資源からデータを読み出しする ・ 資源（アプリケーション）を実行する
3	■各種ユーティリティ機能の利用 一般利用者は、「各種ユーティリティ機能」を利用できない。
4	■システム監視機能の利用 一般利用者は、「システム監視機能」を利用できない。
5	■自動運転機能 一般利用者は、「自動運転機能」を利用できない。
6	■システム編集・ソフトウェア修正適用ツールの利用 一般利用者は、「システム編集・ソフトウェア修正適用ツール」を利用できない。
7	■監査機能の利用 一般利用者は、「監査機能」を利用して、自身が所有する資源の監査レポートを出力する。

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。

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(信頼できる RACF センタ要員、管理者)

RACF センタ要員及び管理者は、不正を行わない、信頼できる人物であること。

・A.PASSWORD(パスワードの管理)

RACF センタ要員、管理者、及び一般利用者が使用するパスワードは、本人以外に知られないこと。

・A.PHY_PROTECT(物理的な保護))

コンソール及び TOE が動作するサーバには、RACF センタ要員以外が物理的にアクセスできないこと。

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、ネットワークを流れる資源への脅威に関しては、ネットワークのプロトコルが TOE 独自である事、悪用には特殊な機器が必要となる事から、低レベルの攻撃者では悪用する事が不可能である。そのため、以下では除外する。

・T.ILLIGAL_ACCESS（不正アクセス）

悪意のある人物は、コマンド／アプリケーションを利用して、資源に対し不正なアクセスを行う。

※不正なアクセスとは、資源の所有者が許可しないアクセスを指す。

・T.PROGRAM（不正なジョブの干渉）

不正なジョブがTOEの領域にアクセスし、他のジョブの実行処理に干渉することによって、資源に対し不正なアクセスを行なう。

3.3 組織のセキュリティ方針

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。

4.1 TOE の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.AUTHORIZATION(識別認証)

TOE は、TOE にアクセスする人物が、正当な TOE の関係者であるかを識別認証しなければならない。

・O.ACCESS(アクセス制御)

TOE は、TOE の関係者に対し、資源の所有者が許可するアクセスのみを許可しなければならない。

・O.PROGRAM_SEP

TOE は、ジョブが TOE の領域にアクセスし、他のジョブの実行処理に干渉しないよう、分離した空間制御を行なわなければならない。

4.2 環境のセキュリティ対策方針

本節では、前提条件を満足し、脅威及び組織のセキュリティ方針に対する TOE セキュリティ対策方針を支援するための環境のセキュリティ対策方針を示す。

・OE.ADMIN(信頼できる RACF センタ要員、管理者)

最高管理者は、RACF センタ要員、及び管理者として信頼できる人物を選任し、不正を行なわないように教育しなければならない。

・OE.PASSWORD(パスワードの管理)

RACF センタ要員、管理者は、使用するパスワードを本人以外に知られないよう定期的に変更する等、適切に管理しなければならない。また管理者は、一般利用者に対し、パスワードを本人以外に知られないよう定期的に変更する等、適切に管理するよう教育を行なわなければならない。

・OE.PHY_PROTECT(物理的な保護)

RACF センタ要員は、TOE が動作するサーバ及びコンソールを、RACF センタ要員以外が入退出できない、物理的に保護された場所に設置しなければならない。

5 IT セキュリティ要件

5.1 TOE セキュリティ要件

本節では、TOE が満たさなければならないセキュリティ要件を示す。

5.1.1 TOE セキュリティ機能要件

FAU_GEN.1　　監査データの生成

下位階層：なし

FAU_GEN.1.1

TSFは、以下の監査対象事象の監査記録を生成できなければならない：

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]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]

- 選択したレベル

指定なし

CC で定義された監査対象以外の監査事象を採取している場合、「監査事象」に、[定義された監査対象以外の操作]と記載する。

表 5-1 監査の対象

機能要件	CC で定義された監査対象	監査事象
FAU_GEN.1	予見される監査対象事象はない。	
FAU_SAR.1	a) 基本: 監査記録からの情報の読み出し。	[定義された監査対象以外の操作] 許可利用者以外の監査レポート読み込みに伴う失敗事象
FAU_SEL.1	a) 最小:監査データ収集機能が作動している間に生じる、監査設定へのすべての改変。	監査対象事象の変更事象
FAU_STG.1	予見される監査対象事象はない。	
FAU_STG.3	基本:閾値を超えたためにとられるアクション	監査ログが一杯になった際に取られる、RACF センタ要員に対するアラート通知

機能要件	CC で定義された監査対象	監査事象
FDP_ACC.1	予見される監査対象事象はない。	
FDP_ACF.1	a) 最小: SFP で扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFP で扱われるオブジェクトに対する操作の実行におけるすべての要求。 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。	[定義された監査対象以外の操作] 操作の実行における失敗事象
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)	・パスワードの失権アクション ・該当アカウントの復権アクション
FIA_ATD.1	予見される監査対象事象はない。	
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。	定義された品質尺度に対する変更事象
FIA_UAU.2	最小:認証メカニズムの不成功になった使用 基本:認証メカニズムのすべての使用	識別認証の成功・不成功のアクション
FIA_UAU.7	監査対象にすべき識別されたアクションはない。	
FIA_UID.2	a) 最小: 提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用; b) 基本: 提供される利用者識別情報を含む、利用者識別メカニズムのすべての使用。	識別認証の成功・不成功のアクション
FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)	識別認証の成功・不成功のアクション
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。	セキュリティ管理機能による、アクセス制御機能のふるまいの変更成功・失敗事象
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	利用者識別名やアクセス権レベル

機能要件	CC で定義された監査対象	監査事象
		の変更成功・失敗アクション
FMT_MSA.3	a)基本:許可的あるいは制限的規則のデフォルト設定の改変 b)基本：セキュリティ属性の初期値の改変すべて。	[定義された監査対象以外の操作] デフォルト値変更の成功・失敗事象
FMT_MTD.1	a) 基本: TSFデータの値のすべての改変	セキュリティ管理機能による TOE 定義変更の成功・失敗事象
FMT_SAE.1	a) 基本：属性に対する有効期限の時間の特定; b)基本:属性の有効期限切れによってとられるアクション	[定義された監査対象以外の操作] パスワードの有効期の変更成功・失敗事象
FMT_SMF.1	a) 最小：管理機能の使用	セキュリティ管理機能の利用成功・失敗事象
FMT_SMR.1	a) 最小: 役割の一部をなす利用者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	役割の一部をなす利用者のグループに対する改変アクションの成功・失敗アクション
FPT_AMT.1	a) 基本: 下層のマシンのテストの実行とテストの結果。	監査事象は採取しない。
FPT_RVM.1	予見される監査対象事象はない。	
FPT_SEP.1	予見される監査対象事象はない。	
FPT_STM.1	a)最小：時間の変更 b)詳細：タイムスタンプの提供	a),b)時間の設定は､監査ログの起動以前に行なわれるため、監査ログ採取は行なわない。

[割付：上記以外の個別に定義した監査対象事象]

なし

FAU_GEN.1.2

TSFは、各監査記録において少なくとも以下の情報を記録しなければならない：

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(成功または失敗)；及び

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

[割付：その他の監査関連情報]

なし

依存性：FPT_STM.1 高信頼タイムスタンプ

FAU_SAR.1　　監査レビュー

下位階層：なし

FAU_SAR.1.1(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]
・RACF センタ要員

[割付：監査情報のリスト]
すべての利用者に関する以下の情報を、監査レポートとして出力する。
・オブジェクト識別情報
・利用者識別情報
・サブジェクト識別情報
・ホスト識別情報
・事象種別

FAU_SAR.1.1(2)

TSFは、[割付：許可利用者]が、[割付：監査情報のリスト]を監査記録から読み出せるようにしなければならない。

[割付：許可利用者]
・管理者

[割付：監査情報のリスト]
管理下にあるグループに関する以下の情報を、監査レポートとして出力する。
・オブジェクト識別情報
・利用者識別情報
・サブジェクト識別情報
・ホスト識別情報
・事象種別

FAU_SAR.1.1(3)

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]

・一般利用者

[割付：監査情報のリスト]

自身に関する以下の情報を、監査レポートとして出力する。

・オブジェクト識別情報

・利用者識別情報

・サブジェクト識別情報

・ホスト識別情報

・事象種別

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_SEL.1　選択的監査

下位階層: なし

FAU_SEL.1.1

TSF は以下のような属性に基づいて、監査事象のセットから監査対象事象を含めたり、除外したりすることができなければならない:

a) [選択: *オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト識別情報、事象種別*]

[選択: *オブジェクト識別情報、利用者識別情報、サブジェクト識別情報、ホスト・識別情報、事象種別*]

・事象種別

b) [割付: *監査の選択性の基礎となる追加属性リスト*]。

[割付: *監査の選択性の基礎となる追加属性リスト*]

なし

依存性: FAU_GEN.1 監査データ生成

FMT_MTD.1 TSFデータの管理

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_STG.3　　監査データ損失恐れ発生時のアクション

下位階層：なし

FAU_STG.3.1

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

[割付：事前に定義された限界]
監査ログ領域の満杯状態

[割付：監査格納失敗の恐れ発生時のアクション]
・枯渇した監査ログ領域を保護
・監査ログの記録領域を新規に作成
・RACF センタ要員への通知

依存性：FAU_STG.1 保護された監査証跡格納

FDP_ACC.1　　サブセットアクセス制御方針

下位階層：なし

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]

表 5-2 資源アクセス制御 SFP のサブジェクト/オブジェクト/操作

サブジェクト名	オブジェクト名	操作
・ ジョブ	・ データセット ・ 一般資源	・ 資源の登録 ・ 登録取消し ・ 改名 ・ 資源の削除 ・ 書込み ・ 読出し ・ 実行

[割付：アクセス制御SFP]

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　　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

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*]

表 5-3 アクセス制御 SFP の属性

サブジェクト属性	オブジェクト属性
・利用者識別名 ・RACF センタ要員属性 ・管理者属性 ・グループ名 ・構造化グループ属性 ・アプリケーション名 ・JCL 属性（※） （※）JCL 属性には、操作対象の資源名(データセット名及び一般資源名）及び、要求操作が一覧として記載されている。	●データセットに関するオブジェクト属性 ・ 所有者名 ・ 所有グループ名 ・ 所有グループの上位グループ名 ・ 構造化グループデータセット属性 ・ 利用者に対するアクセス権（利用者識別名・アプリケーション名・アクセス権レベル） ・ グループに対するアクセス権（グループ名・アプリケーション名・アクセス権レベル） ・ 明示的なアクセス許可属性 ・ 明示的にアクセス許可するアクセス権レベル ●一般資源に関するオブジェクト属性 ・利用者に対するアクセス権（利用者識別名・アクセス権レベル） ・ グループに対するアクセス権（グループ名・アクセス権レベル）

[割付：アクセス制御SFP]

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

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

表 5-4 アクセス制御 SFP の規則

資源がデータセットの場合	
1.データセットと利用者間のアクセス制御規則	
1-1	[前提] ・ オブジェクト属性の「利用者に対するアクセス権」に「アプリケーション名」が記載されている [比較対象] サブジェクト属性である「アプリケーション名」及び「利用者識別名」と、オブジェクト属性である「利用者に対するアクセス権」に記載されている「アプリケーション名」及び「利用者識別名」の比較により、アクセス制御規則が実施される。 [処理] 複数の条件が記載されている場合、番号の若い条件が優先される。 1. 「アプリケーション名」及び「利用者識別名」が一致している場合は、「利用者に対するアクセス権」で操作が許可される。 2. 「アプリケーション名」が一致、オブジェクト属性の「利用者識別名」に「すべての利用者」が指定されている場合は、「利用者に対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 [備考] ※ 「利用者に対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該アプリケーションを介した利用者からのアクセスは、明示的に拒否される。

資源がデータセットの場合	
1.データセットと利用者間のアクセス制御規則	
1-2	[前提] ・ オブジェクト属性の「利用者に対するアクセス権」に「アプリケーション名」が記載されていない [比較対象] サブジェクト属性である「利用者識別名」と、オブジェクト属性である「利用者に対するアクセス権」に記載されている「利用者識別名」(または、オブジェクト属性の「所有者名」)の比較により、アクセス制御規則が実施される。 [処理] 複数の条件が記載されている場合、番号の若い条件が優先される。 1. 「利用者識別名」と「所有者名」が一致している場合、すべての操作が許可される。 2. 「利用者識別名」が一致している場合は、「利用者に対するアクセス権」で操作が許可される。 3. オブジェクト属性の「利用者に対するアクセス権」に「すべての利用者」が指定されている場合は、「利用者に対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 [備考] ※ 「利用者に対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該利用者からのアクセスは、明示的に拒否される。

資源がデータセットの場合	
2.構造化グループデータセットとグループ間のアクセス制御規則	
2-1	[比較対象] サブジェクト属性である「構造化グループ属性」付与の状態により、アクセス制御規則が実施される。 [処理] 1. サブジェクト属性「構造化グループ属性」が付与されている場合、サブジェクト属性である「アプリケーション名」、「グループ名」についての判定が行われる。(詳細条件は、2-2 以降を参照) 上記条件に該当しない場合は、データセットに対する操作が拒否される。

資源がデータセットの場合	
2.構造化グループデータセットとグループ間のアクセス制御規則	
2-2	[前提] ・ サブジェクト属性「構造化グループ属性」が付与されている ・ サブジェクト属性「グループ名」とオブジェクト属性の「所有グループ名」が一致している ・ オブジェクト属性の「グループに対するアクセス権」に「アプリケーション名」が記載されている [比較対象] サブジェクト属性である「アプリケーション名」及び「グループ名」と、オブジェクト属性である「グループに対するアクセス権」に記載されている「アプリケーション名」及び「グループ名」の比較により、アクセス制御規則が実施される。 [処理] 複数の条件が記載されている場合、番号の若い条件が優先される。 1. 「アプリケーション名」及び「グループ名」が一致している場合に、「グループに対するアクセス権」で操作が許可される。 2. 「アプリケーション名」が一致、オブジェクト属性の「グループに対するアクセス権」に「すべてのグループ」が指定されている場合に、「グループに対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 [備考] ※ 「グループに対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該アプリケーションを介したグループからのアクセスは、明示的に拒否される。

資源がデータセットの場合	
2.構造化グループデータセットとグループ間のアクセス制御規則	
2-3	[前提] ・ サブジェクト属性「構造化グループ属性」が付与されている ・ サブジェクト属性「グループ名」とオブジェクト属性の「所有グループ名」が一致している ・ オブジェクト属性の「グループに対するアクセス権」に「アプリケーション名」が記載されていない [比較対象] サブジェクト属性である「グループ名」と、オブジェクト属性である「グループに対するアクセス権」に記載されている「グループ名」(または、オブジェクト属性の「所有グループ名」)の比較により、アクセス制御規則が実施される。 [処理] 複数の条件が記載されている場合、番号の若い条件が優先される。 1. 「グループ名」と「所有グループ名」が一致している、かつ、「管理者属性」が付与されている場合、すべての操作が許可される。 2. 「グループ名」が一致している場合に、「グループに対するアクセス権」で操作が許可される。 3. オブジェクト属性の「グループに対するアクセス権」に「すべてのグループ」が指定されている場合に、「グループに対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 [備考] ※ 「グループに対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該アプリケーションを介したグループからのアクセスは、明示的に拒否される。

資源がデータセットの場合	
2.構造化グループデータセットとグループ間のアクセス制御規則	
2-4	[前提] ・ サブジェクト属性「構造化グループ属性」が付与されている ・ サブジェクト属性「グループ名」とオブジェクト属性の「所有グループ名」が一致していない [比較対象] サブジェクト属性である「グループ名」とオブジェクト属性の「所有グループの上位グループ名」の比較により、アクセス制御規則が実施される。 [処理] 複数の条件が記載されている場合、番号の若い条件が優先される。 1. 「グループ名」と「所有グループの上位グループ名」は一致している場合に、「グループに対するアクセス権」で読み込み以下の操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 [備考] ※ 「グループに対するアクセス権」で操作が許可されるが、読み込み以上の操作がアクセス権レベルで許可されていても読み込みの許可となる

資源がデータセットの場合	
３．非構造化グループデータセットとグループ間のアクセス制御規則	
3-1	［前提］ ・ オブジェクト属性の「グループに対するアクセス権」に「アプリケーション名」が記載されている ［比較対象］ サブジェクト属性である「アプリケーション名」及び「グループ名」と、オブジェクト属性である「グループに対するアクセス権」に記載されている「アプリケーション名」及び「グループ名」の比較により、アクセス制御規則が実施される。 ［処理］ 複数の条件が記載されている場合、番号の若い条件が優先される。 1. 「アプリケーション名」及び「グループ名」が一致している場合に、「グループに対するアクセス権」で操作が許可される。 2. 「アプリケーション名」が一致、オブジェクト属性の「グループ名」に「すべてのグループ」が指定されている場合に、「グループに対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 ［備考］ ※ 「グループに対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該アプリケーションを介したグループからのアクセスは、明示的に拒否される。

資源がデータセットの場合	
３．非構造化グループデータセットとグループ間のアクセス制御規則	
3-2	［前提］ ・ オブジェクト属性の「グループに対するアクセス権」に「アプリケーション名」が記載されていない ［比較対象］ サブジェクト属性である「グループ名」と、オブジェクト属性である「グループに対するアクセス権」に記載されている「グループ名」（または、オブジェクト属性の「所有グループ名」）の比較により、アクセス制御規則が実施される。 ［処理］ 複数の条件が記載されている場合、番号の若い条件が優先される。 1. サブジェクト属性の「グループ名」とオブジェクト属性の「所有グループ名」が一致している、かつ、サブジェクト属性に「管理者属性」が付与されている場合に、すべての操作が許可される。 2. 「グループ名」が一致している場合に、「グループに対するアクセス権」で操作が許可される。 3. オブジェクト属性の「グループ名」に「すべてのグループ」が指定されている場合に、「グループに対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 ［備考］ ※ 「グループに対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該グループからのアクセスは、明示的に拒否される。

資源が一般資源の場合	
４．一般資源と利用者間のアクセス制御規則	
4-1	[比較対象] サブジェクト属性である「利用者識別名」と、オブジェクト属性である「利用者に対するアクセス権」に記載されている「利用者識別名」（または、オブジェクト属性の「所有者名」）の比較により、アクセス制御規則が実施される。 [処理] 複数の条件が記載されている場合、番号の若い条件が優先される。 1. 「利用者識別名」と「所有者名」が一致している場合、すべての操作が許可される。 2. 「利用者識別名」が一致している場合に、「利用者に対するアクセス権」で操作が許可される。 3. オブジェクト属性の「利用者識別名」に「すべての利用者」が指定されている場合に、「利用者に対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 [備考] ※ 「利用者に対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該利用者からのアクセスは、明示的に拒否される。

資源が一般資源の場合	
５．一般資源とグループ間のアクセス制御規則	
5-1	［比較対象］ サブジェクト属性である「グループ名」と、オブジェクト属性である、「グループに対するアクセス権」に記載されている「グループ名」（または、オブジェクト属性の「所有グループ名」）の比較により、アクセス制御規則が実施される。 ［処理］ 複数の条件が記載されている場合、番号の若い条件が優先される。 1. サブジェクト属性の「グループ名」とオブジェクト属性の「所有グループ名」が一致している、かつ、サブジェクト属性に「管理者属性」が付与されている場合に、すべての操作が許可される。 2. 「グループ名」が一致している場合に、「グループに対するアクセス権」で操作が許可される。 3. オブジェクト属性の「グループ名」に「すべてのグループ」が指定されている場合に、「グループに対するアクセス権」で操作が許可される。 上記条件に該当しない場合は、操作が拒否される。 ［備考］ ※ 「グループに対するアクセス権」で操作が許可されるため、アクセス権レベルに「アクセス禁止」が記載されている場合は、当該グループからのアクセスは、明示的に拒否される。

（※）構造化グループデータセット：構造化グループデータセット属性が付与されたデータセット
非構造化グループデータセット：構造化グループデータセット属性が付与されていないデータセット

FDP_ACF.1.3

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]

表 5-5 アクセス制御 SFP を明示的に承認する規則

	明示的に承認する規則
1	サブジェクト属性である「RACF センタ要員属性」が付与されている場合、サブジェクトはオブジェクトに対する全ての操作が承認される。 ※本規則は、最優先の規則である（その他の「明示的に承認する規則」及び「明示的に拒否する規則」より優先される）
2	・「明示的に拒否する規則」によりアクセス拒否されていない　場合 オブジェクト属性である「明示的なアクセス許可属性」が付与されている場合、全てのサブジェクトはオブジェクトに対し、「明示的にアクセス許可するアクセス権」に従って操作が許可される。

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]

表 5-6 アクセス制御 SFP を明示的に拒否する規則

明示的に拒否する規則
・「RACF センタ要員属性」が付与されていない ・サブジェクト属性に「JCL 属性」が付与されている　場合 JCL 属性に記載されている操作要求が、対象とするデータセットまたは一般資源に対するオブジェクト属性の「利用者に対するアクセス権」のアクセス権レベルを超えている場合、当該アクセスを明示的に拒否する。

依存性：FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性の初期化

FIA_AFL.1　　認証の失敗の取り扱い

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：認証事象のリスト]
・TOEへのログイン時のログイン失敗

[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：*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：*許容可能な値の範囲*]
・1～999

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]
・利用者の失権

失権状態からの復権は、「権限を持つ人物による復権処理」か「一定期間経過後の自動復権」により行われる。

依存性：FIA_UAU.1 認証のタイミング

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]

表 5-7 利用者属性の定義

利用者に共通で付与される属性	グループに付与される属性	役割毎に付与される属性
・復権属性 ・失権属性	・グループ名 ・構造化グループ属性	●RACF センタ要員に付与される属性 ・RACF センタ要員属性 ●管理者に付与される属性 ・管理者属性

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]

- 利用者パスワードの構文規約チェック　:8文字以内の各国記号（¥,#,@）を含む英数字

依存性：なし

FIA_UAU.2　　アクション前の利用者認証

下位階層: FIA_UAU.1

FIA_UAU.2.1

TSF 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_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]

・ 入力文字のフィードバックは行わない（非表示）

依存性：FIA_UAU.1 認証のタイミング

FIA_UID.2	アクション前の利用者識別

下位階層：FIA_UID.1

FIA_UID.2.1

TSF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

FIA_USB.1　　利用者・サブジェクトの結合

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]

表 5-8 利用者とサブジェクト間で関連付けられるセキュリティ属性

利用者に共通で付与される属性	グループに付与される属性	役割毎に付与される属性
・復権属性 ・失権属性	・グループ名 ・構造化グループ属性	●RACF センタ要員を代行するジョブに付与される属性 ・RACF センタ要員属性 ●管理者を代行するジョブに付与される属性 ・管理者属性

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]

・識別認証が成功したタイミングで関連付けする

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]

・RACF センタ要員による、すべての利用者の属性変更

・管理者による、管理下の一般利用者に対する属性変更

依存性：FIA_ATD.1 利用者属性定義

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*]

- アクセス制御機能

[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*]

・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

[割付: *許可された識別された役割*]

- RACF センタ要員役割

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

FMT_MSA.1　　セキュリティ属性の管理

下位階層：なし

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]

表 5-9 アクセス制御 SFP において管理される属性

サブジェクト属性	オブジェクト属性
・利用者識別名 ・RACF センタ要員属性 ・管理者属性 ・グループ名 ・構造化グループ属性 ・アプリケーション名 ・JCL 属性	●データセットに関するオブジェクト属性 ・ 所有者名 ・ 所有グループ名 ・ 所有グループの上位グループ名 ・ 構造化グループデータセット属性 ・ 利用者に対するアクセス権（利用者識別名・アプリケーション名・アクセス権レベル） ・ グループに対するアクセス権（グループ名・アプリケーション名・アクセス権レベル） ・ 明示的なアクセス許可属性 ・ 明示的にアクセス許可するアクセス権レベル ●一般資源に関するオブジェクト属性 ・ 利用者に対するアクセス権（利用者識別名・アクセス権レベル） ・ グループに対するアクセス権（グループ名・アクセス権レベル）

[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]]
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]
・登録

[割付：許可された識別された役割]
・RACFセンタ要員役割
・管理者役割
・一般利用者役割

[割付：アクセス制御SFP 、情報フロー制御SFP]
・アクセス制御SFP

表 5-10 サブジェクト属性と許可利用者の操作内容の対応

管理情報	許可利用者	許可操作
利用者識別名	RACFセンタ要員	すべての利用者識別名の、問い合わせ/登録/改変/削除
	管理者	管理下の利用者識別名の、問い合わせ/登録/改変/削除
	一般利用者	自身の利用者識別名の、問い合わせ
RACF センタ要員属性 管理者属性	RACF センタ要員	問い合わせ/登録/改変/削除
グループ名	RACF センタ要員	すべてのグループ名の問い合わせ/登録/改変/削除
	管理者	管理下のグループ名の問い合わせ/登録/改変/削除
	一般利用者	自身が所属するグループ名の問い合わせ
構造化グループ属性	RACF センタ要員	すべての構造化グループ属性の、問い合わせ/登録/改変/削除
	管理者	管理下の構造化グループ属性の、問い合わせ/登録/改変/削除
	一般利用者	自身が所属するグループに対する、構造化グループ属性の問い合わせ
アプリケーション名	RACF センタ要員	すべてのアプリケーション名の、問い合わせ/登録/改変/削除
	管理者	管理下のアプリケーション名の、問い合わせ/登録/改変/削除
	一般利用者	自身が所有するアプリケーション名の、問い合わせ/登録/改変/削除
JCL 属性	RACF センタ要員	JCL 属性(要求資源)の改変
	管理者	JCL 属性(要求資源)の改変
	一般利用者	JCL 属性(要求資源)の改変

表 5-11 オブジェクト属性と許可利用者の操作内容の対応

管理情報	操作できる人物	許可操作
所有者名	RACFセンタ要員	すべての利用者が所有する資源の所有者名の、問い合わせ/登録/変更/削除
	管理者	管理下の利用者が所有する資源の所有者名の問い合わせ/登録/更新/削除
	一般利用者	自身が所有する資源の所有者名の問い合わせ/登録/削除
所有グループ名	RACFセンタ要員	すべてのグループが所有するグループデータセットの、所有グループ名の、問い合わせ/登録/削除
	管理者	管理下のグループが所有するグループデータセットの所有グループ名の、問い合わせ/登録/削除
	一般利用者	自身が所属するグループが所有するグループデータセットの所有グループ名の、問い合わせ
所有グループの上位グループ名	RACFセンタ要員	すべてのグループが所有する構造化グループデータセットの上位グループ名の、問い合わせ/登録/削除
	管理者	管理下のグループが所有する構造化グループデータセットの上位グループ名の問い合わせ/登録/削除
	一般利用者	自身が所属するグループの構造化グループデータセットの上位グループ名の参照
構造化グループデータセット属性	RACFセンタ要員	すべてのグループが所有する構造化グループデータセットの構造化グループデータセット属性の、問い合わせ/登録/改変/削除
	管理者	管理下のグループが所有する構造化グループデータセットの構造化グループデータセット属性の、問い合わせ/登録/改変/削除
	一般利用者	自身が所属するグループが所有する構造化グループデータセットのデータセットの、構造化グループデータセット属性の参照
利用者に対するアクセス権	RACFセンタ要員	すべての資源に対する、アクセス権の問い合わせ/変更/デフォルト値の変更/登録/削除
	管理者	管理下の資源に対する、アクセス権の問い合わせ/変更/登録/削除

管理情報	操作できる人物	許可操作
	一般利用者	自身の資源に対する、アクセス権の問い合わせ/変更/登録/削除
グループに対するアクセス権	RACFセンタ要員	すべてのグループに対するアクセス権の問い合わせ/登録/変更/削除
	管理者	管理下のグループに対するアクセス権の参照/登録/変更/削除
明示的なアクセス許可属性	RACFセンタ要員	明示的なアクセス許可属性の、問い合わせ/改変
明示的にアクセス許可するアクセス権レベル	RACFセンタ要員	明示的にアクセス許可するアクセス権レベルの問い合わせ/登録/変更/削除

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.3　　静的属性の初期化

下位階層：なし

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、その他の特性]
[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]
・　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]
・RACF センタ要員
・管理者

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_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]

- RACF 管理簿
- 時間情報
- パスワード

[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]]

・問い合わせ、改変

・[割付：その他の操作]

- バックアップ
- 稼動・非稼動設定

[割付：許可された識別された役割]

・RACFセンタ要員役割

表 5-12 TSF データと役割に許可された操作の対応

役割	TSFデータ	操作
RACFセンタ要員	RACF管理簿	問い合わせ、改変(※)、バックアップ 稼動・非稼動設定
	時間情報	改変
	パスワード	すべての利用者のパスワードの改変
管理者	パスワード	管理下の利用者のパスワードの改変
一般利用者	パスワード	自身のパスワードの改変

(※)RACF管理簿の改変には、FMT_MSA.1にて示したセキュリティ属性の改変に伴う改変事象は含まない。

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_SAE.1 時限付き許可

下位階層: なし

FMT_SAE.1.1

TSF は、[割付: *有効期限がサポートされるはずのセキュリティ属性のリスト*]に対する有効期限の時間を特定する能力を、[割付: *許可された識別された役割*]に制限しなければならない。

[割付: *有効期限がサポートされるはずのセキュリティ属性のリスト*]
・パスワード

[割付: *許可された識別された役割*]
・RACFセンタ要員役割
・一般利用者役割

表 5-13 役割とパスワード有効期限に関する特定範囲の対応

役割	パスワード有効期限の特定範囲
RACFセンタ要員	すべての利用者に対するパスワードの有効期限
一般利用者	自身のパスワードの有効期限

FMT_SAE.1.2

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

[割付: *各々のセキュリティ属性に対してとられるアクションのリスト*]
・パスワード変更の要求

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

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]

表 5-14 セキュリティ管理機能のリスト

機能要件	CC で定義された管理対象	管理機能
FAU_GEN.1	予見される管理アクティビティはない。	
FAU_SAR.1	以下のアクションは FMT における管理機能と考えられる: a) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	【セキュリティ管理機能】 RACF センタ要員役割の維持
FAU_SEL.1	以下のアクションは FMT における管理機能と考えられる: a) 監査事象を閲覧/改変する権限の維持。	【セキュリティ管理機能】 RACF センタ要員役割の維持
FAU_STG.1	予見される管理アクティビティはない。	
FAU_STG.3	以下のアクションは FMT における管理機能と考えられる: 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)。	管理機能はない。理由は以下の通り。 a) 閾値は固定であり、管理できない。 b) アクションは固定であり、管理できない。
FDP_ACC.1	予見される管理アクティビティはない。	
FDP_ACF.1	以下のアクションは FMT における管理機能と考えられる: 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。	【セキュリティ管理機能】 ・サブジェクト及びオブジェクト属性の管理機能
FIA_AFL.1	以下のアクションは FMT における管理機能と考えられる: a) 不成功の認証試行に対する閾値の管理	【セキュリティ管理機能】 ・認証失敗の回数の管理機能 ・失権および復権の管理機能

	b) 認証失敗の事象においてとられるアクションの管理	
FIA_ATD.1	以下のアクションは FMT における管理機能と考えられる: 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。	なし
FIA_SOS.1	以下のアクションは FMT における管理機能と考えられる: a) 秘密の検証に使用される尺度の管理。	【セキュリティ管理機能】 パスワードルール(使用文字、桁数、世代、有効期限) の管理機能
FIA_UAU.2	以下のアクションは FMT における管理機能と考えられる。 管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	【セキュリティ管理機能】 ・パスワード変更の管理機能
FIA_UAU.7	予見される管理アクティビティはない。	
FIA_UID.2	以下のアクションは FMT における管理機能と考えられる: a) 利用者識別情報の管理。	【セキュリティ管理機能】 ・利用者識別名の管理機能
FIA_USB.1	以下のアクションは FMT における管理機能と考えられる: a) 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。 b) 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変更できる。	【セキュリティ管理機能】 ・利用者に対する権限の追加機能
FMT_MOF.1	以下のアクションはFMTにおける管理機能と考えられる: a) TSFの機能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;	【セキュリティ管理機能】 以下の役割を管理する機能 ・RACF センタ要員
FMT_MSA.1	以下のアクションは FMT における管理機能と考えられる: a) 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。	【セキュリティ管理機能】 以下の役割を管理する機能 ・RACF センタ要員 ・管理者 ・一般利用者
FMT_MSA.3	以下のアクションは FMT における管理機能と考えられる:	【セキュリティ管理機能】 a)以下の役割を管理する機能

	a)初期値を特定できる役割のグループを管理すること b)所定のアクセス制御 SFP に対するデフォルトの許可的あるいは制限的設定を管理すること	・RACF センタ要員 b)デフォルト値の設定機能
FMT_MTD.1	以下のアクションは FMT における管理機能と考えられる: a) 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。	【セキュリティ機能】 以下の役割を管理する機能 ・RACF センタ要員 ・管理者 ・一般利用者
FMT_SAE.1	以下のアクションは FMT における管理機能と考えられる: a) 有効期限がサポートされるはずのセキュリティ属性のリストを管理すること; b) 有効期限の時間が過ぎたときにとられるアクション。	【セキュリティ管理機能】 a) パスワード有効期限の管理 b) アクションは固定であるため、管理機能はない。
FMT_SMF.1	予見される管理アクティビティはない。	
FMT_SMR.1	以下のアクションは FMT における管理機能と考えられる: a) 役割の一部をなす利用者のグループの管理。	【セキュリティ管理機能】 以下の役割に所属する利用者の管理 ・RACF センタ要員 ・管理者 ・一般利用者
FPT_AMT.1	以下のアクションは FMT における管理機能と考えられる: a) 初期立ち上げ中、定期的間隔、特定の状態下など､抽象マシンテストが行われる条件の管理; b) 必要ならば、時間間隔の管理。	管理機能はない。理由は以下の通り。 a) 条件は固定であり、管理できない。 b) 必要なし。
FPT_RVM.1	予見される管理アクティビティはない。	
FPT_SEP.1	予見される管理アクティビティはない。	
FPT_STM.1	以下のアクションはFMTにおける管理機能と考えられる: a) 時間の管理。	【セキュリティ管理機能】 a)時間の設定機能

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]

・RACFセンタ要員役割

・管理者役割

・一般利用者役割

FMT_SMR.1.2

TSF は、利用者を役割に関連づけなければならない。

依存性：FIA_UID.1 識別のタイミング

FPT_AMT.1　　抽象マシンテスト

下位階層：なし

FPT_AMT.1.1

TSFは、TSFの下層にある抽象マシンによって提供されるセキュリティ前提条件の正しい操作を実証するために、[選択：初期立ち上げ中、通常操作中に定期的に、許可利用者の要求で、[割付：その他の条件]]に、テストのスイートを走らせなければならない。

［選択：初期立ち上げ中、通常操作中に定期的に、許可利用者の要求で、[割付：その他の条件]］

- 初期立ち上げ中

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、それ自身の実行のため、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間の分離を実施しなければならない。

依存性：なし

FPT_STM.1　　高信頼タイムスタンプ

下位階層：なし

FPT_STM.1.1

TSF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

5.1.2　TOE セキュリティ保証要件

本ST にて要求する、TOEに対する保証レベルはEAL1 である。保証コンポーネント構成を表 5-15 に示す。

要求する各保証コンポーネントの保証エレメントは、CC Part3 の要求通りである。

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 5-15 TOE の保証要件コンポーネント一覧

TOE セキュリティ保証要件		コンポーネント
構成管理	CM 能力	ACM_CAP.1
配付と運用	設置、生成、及び立上げ	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

5.2 セキュリティ機能強度

TOE セキュリティ機能要件に対する最小機能強度は、SOF-基本である。また、明示された機能強度が適用される TOE セキュリティ機能要件は、FIA_UAU.2、FIA_UID.2、FIA_SOS.1、FIA_AFL.1 であり、機能強度は SOF-基本である。

6 TOE 要約仕様

本節では、TOEのセキュリティ機能を説明する。各機能に対応するTOEセキュリティ機能要件が示されているように、本節で説明するセキュリティ機能は、5.1.1.TOEセキュリティ機能要件で記述したTOEセキュリティ機能要件を満たす。

6.1 セキュリティ機能

表 6-1 に、TOEセキュリティ機能要件とセキュリティ機能の対応関係を示す。

表 6-1 TOE セキュリティ機能要件とセキュリティ機能の対応

NO	セキュリティ機能	機能要件
1	識別認証機能	FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FIA_AFL.1、FIA_SOS.1、FIA_ATD.1、FIA_USB.1、FPT_RVM.1
2	グローバルチェック機能	FDP_ACC.1、FDP_ACF.1、FPT_RVM.1
3	構造化グループ機能	FDP_ACC.1、FDP_ACF.1、FPT_RVM.1
4	資源アクセス制御機能	FDP_ACC.1、FDP_ACF.1、FPT_RVM.1
5	JESCI アクセス権確認機能	FDP_ACC.1、FDP_ACF.1、FPT_RVM.1
6	セキュリティ管理機能	FAU_SEL.1、FMT_MSA.1、FMT_MSA.3、FMT_MOF.1、FMT_MTD.1、FMT_SAE.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1
7	監査機能	FAU_GEN.1、FAU_SAR.1、FAU_STG.1、FAU_STG.3、FPT_RVM.1、FPT_STM.1
8	TSF 保護機能	FPT_AMT.1、FPT_RVM.1、FPT_SEP.1

6.1.1　　識別認証機能

本機能により、他のセキュリティ機能を利用する前に、TOE にアクセスする人物に対し、利用者識別（グループ）名及びパスワードを利用した識別認証が行われる。

本機能に使用するパスワードは、以下の規則に従う。

・フィードバックは行わない（非表示）
・利用者パスワードの有効期間 ： 取り得る値の範囲は、1～999（日）
パスワードの有効期間が切れた場合、パスワード変更の要求を行なう。
・利用者パスワードの構文規約チェック ：8 文字以内の各国記号（¥,#,@）を含む英数字
・利用者パスワードの変更禁止期間 ：取り得る値の範囲は、1～999（日）
・新しい利用者パスワードの入力確認：選択
・利用者パスワードの入力違反許容回数：取り得る値の範囲は、1～999
・利用者パスワード入力違反による自動失権後の自動復権 ：値の取り得る範囲は 1～999（日）
・日付指定の自動失権と自動復権 ：
- 絶対日数を指定するときの値の取り得る範囲は 1～999（日）
- 相対日数は YYMMDD 形式で指定するため、値の取り得る範囲は 800101(1980 年 1 月 1 日)～791231(2079 年 12 月 31 日)。
・システム未利用者の自動失権：値の取り得る範囲は 1～999（日）

■識別認証後の利用者のふるまい

本機能にて、正当な人物であると識別認証された後、利用者は、その利用者を代行するジョブとして TOE 内で存在する。ジョブは、利用者に関する情報をリストとして有し、利用者のふるまいを継承して、TOE の機能を実行する。

6.1.2　　アクセス制御機能

本機能は、TOE の関係者・グループ・アプリケーション（「エンティティ」と省略する）に対して、RACF 管理簿に登録された設定(資源の所有者が許可するアクセスの設定)に従って、資源へのアクセスを制御する。RACF 管理簿内に該当するエンティティと資源との規則が記載されている場合、許可されたアクセス権レベルで資源への操作を許可する。資源アクセスを不許可と判断した場合、アクセス禁止となる。

以下に、下線部の詳細を示す。

➢　アクセス権レベル

アクセス権レベルは、資源の特徴を加味し、以下の 5 種類とする。

・改名削除権

改名削除権は、資源の登録、登録取消し、改名、資源の削除を可能とする権限である。なお、本権限は、後述の「VSAM 制御権」を包含する。

・VSAM 制御権

VSAM 制御権は、対象資源が DASD データセットの場合のみに適用するアクセス権レベルである。本アクセス権レベルは、対象の DASD データセットが「VSAM データセット」である場合、コントロールインタバルでのアクセスを認め、かつ、書き込みを可能とする。また、「非 VSAM データセット」の場合、書き込み権と同じである。

・書き込み権

書き込み権は、資源へのデータの書き込みを可能とする権限である。なお、本権限は、後述の「読み出し権」を包含している。

・読み出し権

読み出し権は、資産の読み出しを可能とする権限である。本権限は、後述の「実行権」を包含している。

・実行権

実行権は、資源内のアプリケーションを実行することを可能とする権限である。

また、明示的にアクセスを不許可とする権限として、「アクセス権なし」がある。

➢　アクセス制御機能の種類

アクセス制御は、以下の 4 機能からなる。

- 特定の資源に対する、全ての利用者のアクセスを明示的に許可する「グローバルチェック機能」
- グループの階層構造を利用して、グループが所有する資源に対する、当該グループ以外の資源アクセスを制御する「構造化グループ機能」

・ 資源と利用者との関係を RACF 管理簿に登録し、その規則に従ってアクセスの制御を行なう「資源アクセス制御機能」
・JCL 投入段階で、JCL の要求が許可された範囲内であるかを判断する「JESCI アクセス権確認機能」

これら 4 機能には、適用される順序がある。この順序に関する規則を以下に示す。

表 6-2 アクセス制御の適用順序の規則

アクセス制御の適用順序の規則	
1	【分岐条件】 1. JCL 投入による資源アクセスかつ、JCL に記載された操作要求が、JCL 投入者に許可された範囲内ではない。(※) 【適用されるアクセス制御規則】 JESCI アクセス権確認機能が適用される。 ※ 許可された範囲内の規定は、「JESCI アクセス権確認機能」を参照して頂きたい。
2	【分岐条件】 1. JCL 投入による資源アクセスかつ、JCL に記載された操作要求が、JCL 投入者に許可された範囲内である。または、JCL 以外の方法による資源アクセス 2. 資源名が「グローバル資源名」である。(資源が「グローバル資源」として登録されている) 【適用されるアクセス制御規則】 グローバルチェック機能が適用される。
3	【分岐条件】 1. JCL 投入による資源アクセスかつ、JCL に記載された操作要求が、JCL 投入者に許可された範囲内である。または、JCL 以外の方法による資源アクセス 2. 資源名が「グローバル資源名」ではない 3. 資源の所有グループが、構造化グループである (資源が構造化グループデータセットである) 【適用されるアクセス制御規則】

アクセス制御の適用順序の規則	
	構造化グループ機能が適用される。
4	【分岐条件】 1. JCL 投入による資源アクセスかつ、JCL に記載された操作要求が、JCL 投入者に許可された範囲内である。または、JCL 以外の方法による資源アクセス 2. 資源名が「グローバル資源名」ではない 3. 資源の所有グループが、構造化グループではない (資源が構造化グループデータセットでない) 【適用されるアクセス制御規則】 資源アクセス制御機能が適用される。

注)ジョブに「RACF センタ要員権限」が付与されている場合、上記の規則より優先され、「改名削除」が許可される。

以降のアクセス制御機能の仕様では、この適用順序の規則は省略して記載している。

6.1.2.1 グローバルチェック機能

本機能は、JCL 以外の方法による資源アクセスの場合、他のアクセス制御機能に先んじてアクセスの判定を行い、本機能の適用範囲内であれば、資源のアクセスが可能となる機能である。なお、グローバル資源として登録されているが、アクセス要求が本機能で許可されているアクセス権レベルを超えている場合には、構造化グループ機能、延いては資源アクセス制御機能による判定が適用される。

補足：本機能の利用ポリシー

すべての資源に対し､｢資源アクセス制御機能｣に従ったアクセスチェックが行われると、負荷が大きくなり処理性能が低下する。この問題を解決するために、利用回数の多い資源は本機能による対象とする。そうすることで､､｢資源アクセス制御機能」とは別のアクセス制御が行われ、処理性能を低下させることなく資源の利用が可能となる。

[表の読み方]

アクセス制御規則：アクセス制御の規則を示す。

本機能の規則を、表 6-3 に示す。

表 6-3 グローバルチェック機能の規則

アクセス制御規則
すべてのジョブに対し、「グローバルアクセス権」に従ったアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。

6.1.2.2 構造化グループ機能

資源が構造化グループデータセットである場合に適用されるアクセス制御機能である。

グループと、グループが所有する資源間に適用されるアクセス制御規則を、条件毎に規定する。

表 6-4 構造化グループ機能のアクセス制御規則

	アクセス制御規則
1	・ジョブが構造化グループである ・ジョブが資源の所有グループでない（ジョブのグループ名とデータセット名の第一修飾子が一致していない） ・データセットを所有するグループの「上位グループ名」と、ジョブの「グループ名」が一致している場合 資源アクセスは、「資源アクセス制御機能」に従うが、アクセス権レベルは読み込み権以下に制限される。
2	・ジョブが構造化グループである ・ジョブが資源の所有グループでない ・データセットを所有するグループの「上位グループ名」と、ジョブの「グループ名」が一致していない場合 または、 ・ジョブが構造化グループでない アクセスを拒否する。
-	【資源アクセス制御機能へ】 ・ジョブが構造化グループである ・ジョブが資源の所有グループである 「資源アクセス制御機能」に従う。

6.1.2.3 資源アクセス制御機能

本機能は、以下の資源とエンティティとの間で以下のアクセスの制御を行なう。なお、本機能を設定する方法（「アクセス権を設定する方法」と称す）には、エンティティと資源の組み合わせにより、表 6-5 に示す 5 種類の方法がある。なお、設定機能を提供する機能は、セキュリティ管理機能である。

表 6-5 アクセス権を設定する方法

アクセス権を設定する方法	エンティティ		資源
	利用者／グループ	アプリケーション	
公衆アクセス権 【内容】 資源のみを特定し、アクセス権レベルを設定する方法。つまり、資源を利用する利用者及びグループに関係なくが適用される。	N/A	N/A	データセット 一般資源
グループ公衆アクセス権 【内容】 グループが所有するデータセット、及びグループに所属する利用者を特定し、アクセス権レベルを設定する方法。 （グループに所属する利用者が、発行可能なコマンドで設定を行なう。）	グループ	N/A	データセット
特定アクセス権 【内容】 資源、及び利用者(またはグループ)を特定し、アクセス権レベルを設定する方法。 （RACF センタ要員が発行可能なコマンドで設定を行なう。）	利用者 グループ	N/A	データセット 一般資源
特定パスアクセス権 【内容】 利用者（またはグループ)、データセット、アプリケーションの 3 つを特定し、アクセス権レベルを設定する方法。	利用者 グループ	アプリケーション	データセット
公衆パスアクセス権 【内容】 データセットと、アプリケーションを特定し、アクセス権レベルを設定する方法。	N/A	アプリケーション	データセット

これら「公衆アクセス権」～「公衆パスアクセス権」は、資源毎に、RACF 管理簿にアクセス権として設定される。以降、これらアクセス権を用いてアクセス制御を規定する。

利用者及び資源間に適用されるアクセス制御規則を 表 6-6 に示す。

[表の読み方]

共通条件：本機能にて共通に適用される条件を示す。

なお、**アクセス制御規則**には、優先順位の高いもの、及び低いものは省略する。(優先順位の高いものは、すべて「設定なし」。低いものの設定は「任意」)

表 6-6 資源アクセス制御規則

共通条件	
・利用者に対する特定パスアクセス権、利用者に対する特定アクセス権、グループに対する特定パスアクセス権、グループに対する特定アクセス権、公衆パスアクセス権、グループ公衆アクセス権、公衆アクセス権の順に優先順位がつけられ、優先順位の高いものが適用され、優先順位の低いものは無視される。	
資源がデータセットの場合	
アクセス制御規則	
1	・利用者に対する特定パスアクセス権：設定あり ジョブに付されている「アプリケーション名」及び「利用者識別名」と、「利用者に対する特定パスアクセス権」に記載されている「アプリケーション名」及び「利用者識別名」が一致している場合、当該ジョブは資源に対し「利用者に対する特定パスアクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
2	・利用者に対する特定アクセス権：設定あり ジョブに付されている「利用者識別名」と、「利用者に対する特定アクセス権」に記載されている「利用者識別名」が一致している場合、当該ジョブは資源に対し利用者に対する特定アクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 また、資源の所有者を代行したジョブである場合、改名削除が許可される。 また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
3	・グループに対する特定パスアクセス権：設定あり ジョブに付されている「アプリケーション名」及び「グループ名」と、「グループに対する特定パスアクセス権」に記載されている「アプリケーション名」及び「グループ名」が一致している場合、当該ジョブは資源に対し「グループに対する特定パスアクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可

	される。 　また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
4	・グループに対する特定アクセス権：設定あり 　ジョブに付されている「グループ名」と、「グループに対する特定アクセス権」に記載されている「グループ名」が一致している場合、当該ジョブは資源に対し「グループに対する特定アクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 　また、ジョブがデータセットの所有グループ、かつ、管理者権限が付与されている場合、改名削除が許可される。 　また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
5	・公衆パスアクセス権：設定あり 　ジョブに付されている「アプリケーション名」と、「公衆パスアクセス権」に記載されている「アプリケーション名」が一致している場合、当該ジョブは資源に対し「公衆パスアクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 　また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
6	・グループ公衆アクセス権：設定あり 　ジョブに付されている「グループ名」と、「グループ公衆アクセス権」に記載されている「グループ名」が一致している場合、当該ジョブは資源に対し「グループ公衆アクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 　また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
7	・公衆アクセス権：設定あり 　全てのジョブに対し「公衆アクセス権」に設定されたアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 　また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
資源が一般資源の場合	
アクセス制御規則	
1	・利用者に対する特定アクセス権：設定あり 　ジョブに付されている「利用者識別名」と、「利用者に対する特定アクセス権」」に記載されている「利用者識別名」が一致している場合、当該ジョブは「利用者に対する特定アクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 　また、資源の所有者を代行したジョブである場合、改名削除が許可される。 　また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。

2	・グループに対する特定アクセス権：設定あり ジョブに付されている「グループ名」と、「グループに対する特定アクセス権」に記載されている「グループ名」が一致している場合、当該ジョブは「グループに対する特定アクセス権」に記載されているアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 また、ジョブが一般資源の所有グループ、かつ、管理者権限が付与されている場合、改名削除が許可される。 また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。
3	・公衆アクセス権：設定あり 全てのジョブに対し「公衆アクセス権」に設定されたアクセス権レベル（改名削除、VSAM 制御、書込み、読出し、実行の何れか）が許可される。 また、アクセス権レベルが「アクセス権なし」の場合は、アクセスが拒否される。

6.1.2.4 JESCI アクセス権確認機能

本機能は、JCL の実行時に、JCL 投入者が JCL 内で指定されたデータセットの資源へのアクセス権を持っているか、JCL の構文解析を行い判断する機能である。本機能の規則を以下に示す。

表 6-7 JESCI アクセス権確認機能のアクセス制御規則

アクセス制御規則
JCL に記載された操作要求と、対象とするデータセットまたは一般資源に対する JCL 投入者に与えられた操作権限との比較が行なわれ、操作要求が操作権限を超えていた場合、当該アクセスを明示的に拒否する。

6.1.3　　監査機能

本機能は、以下のセキュリティ機能群から構成される。なお、以下で規定する「監査ログ」には、改変を防止する制御を行なう。

■監査ログの収集

本機能では、監査ログへの採取事象として、「すべてのアクセスログを収集する」、「正当なアクセスログを収集する」、「不当なアクセスログを収集する」、「アクセスの記録を収集しない」から選択される。但し、デフォルトでは「不当なアクセスログを収集する」であるため、以降、デフォルトの採取事象についてのみ規定する。なお、監査ログへの採取事象の設定機能は、セキュリティ管理機能にて提供される。(セキュリティ管理機能の、「監査機能における採取イベントの定義」)

表 6-8 の「監査イベント」に示す情報を、デフォルトで監査ログに採取する。なお、それぞれには、「日付及び時刻」、「利用者またはグループ識別情報」を採取する。(「監査イベントの種別」、「監査イベントの結果」は、下表監査イベントにて示す)

表 6-8 監査イベント

監査の対象となるセキュリティ機能	監査イベント
識別認証機能	・識別認証の成功・不成功のアクション ・識別認証への不成功の試行に対する閾値への到達、及びそれに伴いとられるアクション ・正常状態へ復帰アクション ・定義された品質尺度に対する変更事象
アクセス制御機能	・資源への操作実行における失敗事象 ・構造化グループ機能のフロー制御の拒否事象
監査機能	・監査機能の起動（※１）と終了（※２） ・監査事象の変更事象 ・許可利用者以外の監査レポート読み込みに伴う失敗事象（但し、監査データセットをアクセス制御の対象にしている場合） ・監査ログが一杯になった際に取られる、RACF センタ要員に対するアラート通知（※３）
セキュリティ管理機能	・利用者識別名やアクセス権レベルの変更成功・失敗アクション ・パスワードの有効期間の特定 ・セキュリティ管理機能の成功・失敗イベント ・セキュリティ管理機能のふるまい変更成功・失敗事象

	・デフォルト値の変更成功・失敗事象 ・セキュリティ管理機能による TOE 定義の成功・失敗事象 ・パスワードの有効期限の変更成功・失敗事象 ・役割の一部をなす利用者のグループに対する改変成功・失敗イベント

（※１）監査機能の起動に関しては、TOE の起動のタイミングで監査ログに採取されるものであるため、サブジェクト等を特定する必要がなく、サブジェクト識別情報等はログに採取しない。そのため、監査ログとしては、事象の日付・時刻及び事象の種別のみを採取する。

（※２）監査機能の終了に関しては,システムの終了時と同期しており,システム終了時に監査ログに採取されるものであるため、サブジェクト等を特定する必要がなく、サブジェクト識別情報等はログに採取しない。そのため、監査ログとしては、事象の日付・時刻及び事象の種別のみを採取する。

（※３）アラート通知に関しては、TOE が事象を検知して自動的にアラートを通知する性質のものであるため、サブジェクト識別情報はログに採取しない。そのため、監査ログとしては、事象の日付・時刻及び事象の種別のみを採取する。

■監査レポートの出力

また、本機能は、採取した監査ログを、監査レポートとして監査する人物が可読な形式で出力する。なお、監査ログから監査レポートを出力する際には、監査データセットというデータセットを作成し、この監査データセットから監査レポートの出力を行なう。

監査データセットから、監査レポートを出力する能力は、RACF センタ要員、管理者、一般利用者（資源の所有者）のみに制限している。

また、監査ログは、「情報センタの利用状況」、「資源へのアクセス状況」、「利用者単位の資源へのアクセス状況」、「資源の定義の変更状況」、「利用者単位の資源の定義の変更状況」、「データセンタの変更状況」の単位で出力することができる。なお、各監査レポートには、「日付及び時刻」が共通で含まれる。表 6-9 に監査レポートの詳細を示す。

[表の読み方]

表名称：当該監査レポートの名称

監査レポート概要：当該監査レポートの概要

出力情報：当該監査レポートに記載される情報

表 6-9 監査レポートの詳細

表名称	監査レポート概要	出力情報
認証履歴表	情報センタを「だれがどのように利用しているか（情報センタの利用状況)」を情報として抽出し出力する。具体的には、利用者がシステムを使用する頻度や利用する時間帯を表示する。さらに、利用者がシステムを不正に利用しようとしたときの利用者識別名、および利用できない理由を出力する。	・利用者識別名 ・現用グループ名 ・利用している端末名 ・当該利用者が TOE を利用不可能な理由 ・ジョブを実行した利用者識別名 ・ジョブを実行した利用者の現用グループ名
資源アクセス履歴表	資源を利用する権限のない利用者が「資源を不正に利用していないか」、および「利用できなかった理由」を情報として抽出し出力する。	・資源の所有者属性（利用者・グループ） ・資源所有者の本名グループ ・利用者識別名 ・現用グループ名 ・現用グループの本名グループ名 ・利用している端末名 ・構造化グループ機能のチェック結果 ・当該利用者・グループのアクセス権の種別 ・グローバルチェック機能、資源アクセス制御機能のチェック結果
利用者アクセス履歴表	「資源のアクセス履歴表」を利用者単位に編集して出力する。	・資源の所有者属性（利用者・グループ） ・資源所有者の本名グループ ・利用者識別名 ・現用グループ名 ・現用グループの本名グループ名 ・利用している端末名 ・構造化グループ機能のチェック結果 ・当該利用者・グループのアクセス権の種別 ・グローバルチェック機能、資源アクセス制御機能のチェック結果
資源定義履歴表	資源の定義が「どのように変更されたか」、「どの資源が不正に定義されようとしたか」を情報として抽出し出力する。	・資源の所有者属性（利用者・グループ） ・資源所有者の本名グループ ・利用者識別名

表名称	監査レポート概要	出力情報
		・現用グループ名 ・現用グループの本名グループ名 ・利用している端末名 ・定義結果（資源に対する操作の実行結果） ・利用者の権限
利用者定義履歴表	「資源定義履歴表」を利用者単位に編集し出力する。	・資源の所有者属性（利用者・グループ） ・資源所有者の本名グループ ・利用者識別名 ・現用グループ名 ・現用グループの本名グループ名 ・利用している端末名 ・定義結果（資源に対する操作の実行結果） ・利用者の権限
データセンタ属性管理履歴表	制御ブロックの設定が、「誰によって」、「どのように変更されたか」を情報として抽出し出力する。	・利用者識別名 ・現用グループ ・現用グループの本名グループ名 ・利用している端末名 ・利用結果（操作の成功／不成功） ・利用者の権限

■監査レポートの出力範囲

監査レポートは、役割ごとに出力できる範囲が異なる。各役割に与えられた監査レポートの出力範囲を以下に示す。

・ RACF センタ要員は、すべての利用者に対する監査レポートを出力できる

・ 管理者は、以下の監査レポートを出力することができる。
（但し、管理者がグループ監査役属性を行使できるグループが所有する資源のみを対象とする事ができる。）

資源アクセス履歴表
利用者アクセス履歴表
資源定義履歴表
利用者定義履歴表

・ 一般利用者は、以下の監査レポートを出力することができる。

（但し、利用者自身が所有する資源のみを対象とする事ができる。）

資源アクセス履歴表

利用者アクセス履歴表

■監査ログの保全

監査ログが監査イベントで一杯になった場合、格納場所を交代用データセットに自動的に切り替え、かつ、監査ログが一杯になったことを RACF センタ要員に通知する。

6.1.4 セキュリティ管理機能

本機能は、RACF センタ要員、管理者、一般利用者に対してセキュリティ機能の管理行為を行う能力を提供する。

本機能は、役割毎に提供する機能が異なる。そのため、以下では、役割毎に提供機能の仕様を示す。

6.1.4.1 RACF センタ要員向け機能

RACFセンタ要員向けセキュリティ管理機能を、表 6-10 に示す。

表 6-10 RACF センタ要員向けセキュリティ管理機能

NO	管理機能概要	機能詳細
1	・RACF 管理簿の問い合わせ、改変 ・資源に関する属性のデフォルト値変更 ※上記、RACF 管理簿の改変には、後述の「資源に関する属性の改変」に伴う改変事象は含まない	・「識別認証機能」の設定状況の確認、動作の設定 ・「アクセス制御機能」（グローバルチェック機能、構造化グループ機能、資源アクセス制御機能、JESCI アクセス権確認機能）の設定状況の確認、動作の設定 ・監査機能における採取イベントの定義
	RACF 管理簿のバックアップ、稼動・非稼動制御、監査ログの保全	・RACF 管理簿のバックアップ ・RACF 管理簿の稼動・非稼動の設定。本設定に伴い、「識別認証機能」、「アクセス制御機能」、「監査機能」が稼動/非稼動となる。 ・監査ログ領域の保全
	時間情報の改変	・時間の設定機能
2	セキュリティ機能のふるまいの決定、改変 セキュリティ機能の起動、停止	・RACF 空間上の、利用者及びグループに関する情報のリフレッシュ ・RACF センタ出口ルーチンの設定による、アクセス制御機能の有効・無効化、ふるまい変更設定
3	利用者属性の問い合わせ・改変・削除	・全ての利用者（RACF センタ要員、管理者、一般利用者）の登録・削除 ・全ての「利用者に関する情報」の表示/設定（但し、パスワードに関しては設定のみ）
4	アプリケーション名の、問い合わせ・登録・改変・削除	アプリケーションに対するアクセス権設定による以下の設定 ・すべてのアプリケーションの登録 ・すべてのアプリケーションの削除、参照、名称変更
5	資源に関する属性の問い合わ	・全ての資源に対する、資源の所有者及び所有グループ名、ア

	せ・改変・削除	クセス権（利用者・アプリケーション・グループと資源との間のアクセス権レベル）の表示/設定 ・全ての資源に対するアクセス制御対象のアプリケーションの表示/設定 ・すべての利用者が作成する資源に対する、作成時登録機能（作成する資源をデフォルトで RACF 管理簿に登録する/しない、を設定する機能）の設定 ・グローバルアクセス権の表示/設定 ・所有グループ名をキーとした、上位グループ名及び構造化グループデータセット属性の表示/設定
6	グループに関する属性の問い合わせ・改変・削除	・全てのグループの登録・削除 ・全ての利用者のグループへの登録・削除 ・全ての「グループに関する情報」（グループ名、構造化グループ属性、グループの管理者）の表示/設定
7	JCL 属性の改変	・JCL における操作要求の定義

（注 1）当該利用者が、RACF センタ要員及び管理者かどうかを示す。

(注 2)利用者がデータセットを作成した場合、データセット名の第一修飾子が資源の所有者名になる。また、グループがデータセットを作成した場合、データセット名の第一修飾子が所有グループ名になる。

なお、(注 2)に関しては、後述の表 6-11、6-12 においても同様である。

6.1.4.2　　管理者向け機能

管理者向け機能を、表に示す。

表 6-11 管理者向け TOE 管理機能

NO	管理機能概要	概要
1	利用者属性の問い合わせ・改変・削除	・管理下の一般利用者の登録・削除 ・管理下の「利用者に関する情報」(利用者識別名、失権状態、復権状態、認証失敗回数、パスワード）の表示/設定（但し、パスワードに関しては設定のみ)
2	アプリケーション名の、問い合わせ・登録・改変・削除	アプリケーションに対するアクセス権設定による以下の設定 ・管理範囲内でのアプリケーションの登録 ・管理下のアプリケーションの削除、参照、名称変更
3	資源に関する設定機能	・管理下の資源に対する、所有者名及び所有グループ名、アクセス権（利用者・アプリケーション・グループと資源との間のアクセス権レベル）の表示/設定 ・管理下の資源に対するアクセス制御対象のアプリケーションの表示/設定 ・管理下の利用者が作成する資源に対する、作成時登録機能の設定 ・所有グループ名をキーとした、上位グループ名及び構造化グループデータセット属性の表示/設定
4	グループに関する設定機能	・管理下のグループの登録・削除 ・管理下の一般利用者の、グループへの登録・削除 ・管理下の「グループに関する情報」(グループ名、グループの管理者、構造化グループ属性）の表示/設定
5	JCL 属性の改変	・JCL における操作要求の定義

6.1.4.3　　一般利用者向け機能

一般利用者向け機能を、表 6-12 に示す。

表 6-12 一般利用者向け TOE 管理機能

NO	管理機能概要	概要
1	自身の利用者に関する属性の問い合わせ・改変・削除	・自身の利用者識別名の表示 ・自身のパスワードの変更 ・自身のパスワードの有効期限の設定
2	アプリケーション名の、問い合わせ・登録・改変・削除	アプリケーションに対するアクセス権設定による以下の設定 ・許可範囲内でのアプリケーションの登録 ・自身が所有するアプリケーションの削除、参照、名称変更
3	自身が所属するグループに関する属性の設定機能	・自身が所属するグループ名の表示 ・自身が所属するグループの構造化グループ属性の表示
4	自身が所有する資源に関する属性の設定機能	・自身が所有する資源に対する、所有者名、アクセス権（利用者・アプリケーションと資源との間のアクセス権レベル）の表示/設定 ・自身が所有する資源に対するアクセス制御対象のアプリケーションの表示/設定 ・自身が所属するグループが所有するグループデータセットの所有グループ名の表示 ・所有グループ名をキーとした、上位グループ名及び構造化グループデータセット属性の表示
5	JCL 属性の改変	・JCL における操作要求の定義

6.1.5 TSF 保護機能

本機能は、TOE の起動時に、メモリが正常に動作するか検証を行なう。

TOE は、ジョブがアプリケーションを起動すると、仮想記憶（アプリケーションの実行環境)に OS に対する制御データが付与されたアプリケーションをローディングし実行する。本機能では、仮想記憶として、アプリケーションごとに独立した空間を作成する。この独立した仮想空間にアプリケーションが存在するため、アプリケーション間の干渉発生を防止するセキュリティドメインを構築する。それにより、不正な利用者が自身の起動したアプリケーションの仮想空間を越え他のアプリケーションの制御データを改変することによって TOE を改変したり損害を与えたりすることや、他の利用者が仮想空間上にロードした保護資産を改変したり覗き見たりすることが防がれている。

6.2　セキュリティ強度

本 TOE において、機能強度の対象となる順列的・確率的メカニズムを有する IT セキュリティ機能は識別認証機能であり、機能強度は SOF-基本である。

6.3　保証手段

保証クラスに対する保証手段を 表 6-13 に示す。

表 6-13 保証要件と保証手段の対応

クラス	コンポーネント名	保証手段
構成管理	ACM_CAP.1	・OSIV/MSP セキュア AF2 V10L10 ソフトウェア説明書 ・コマンド投入による、TOE の構成プログラム名称及びバージョンの表示
配付と運用	ADO_IGS.1	・OSIV/MSP セキュア AF2 V10L10 ソフトウェア説明書 ・OSIV/MSP RACF 導入手引書 V12L10 用 ・OSIV/MSP RACF 使用手引書 管理者編 V12L10 用 ・OSIV/MSP システム導入手引書 AFII V10 用 ・OSIV/MSP TSS/E 運用手引書 V11L20 用 ・OSIV VTAM-G 導入手引書 V30 用
開発	ADV_FSP.1	・OSIV/MSP セキュア AF2 識別認証機能 機能仕様書 ・OSIV/MSP セキュア AF2 アクセス制御機能 機能仕様書 ・OSIV/MSP セキュア AF2 RACF 機能 API　機能仕様書 ・OSIV/MSP セキュア AF2 監査機能 機能仕様書 ・OSIV/MSP セキュア AF2 セキュリティ管理機能 機能仕様書 ・OSIV/MSP セキュア AF2 セキュリティ管理機能 機能仕様書（ユーティリティ編） ・OSIV/MSP セキュア AF2 セキュリティ管理機能 機能仕様書（コンソールコマンド編） ・OSIV/MSP セキュア AF2 RACF 機能 センタ出口ルーチン 機能仕様書 ・OSIV/MSP セキュア AF2 TSF 保護機能 機能仕様書 ・OSIV/MSP セキュア AF2 非セキュリティ機能 機能仕様書
	ADV_RCR.1	・OSIV/MSP セキュア AF2 表現対応表

クラス	コンポーネント名	保証手段
ガイダンス	AGD_ADM.1	・OSⅣ/MSP RACF 運用手引書 V12L10 用 ・OSⅣ/MSP RACF 使用手引書 管理者編 V12L10 用 ・OSⅣ/MSP RACF コマンド文法書 V12L10 用 ・OSⅣ/MSP RACF システムプログラマの手引 V12L10 用 ・OSⅣ/MSP RACF ユーティリティ使用手引書 V12L10 用 ・OSⅣ/MSP RACF メッセージ説明書 V12L10 用 ・OSⅣ/MSP RACF 導入手引書 V12L10 用 ・OSⅣ/MSP AMS コマンド文法書 AFⅡ V10 用 ・OSⅣ/MSP IORGP 使用手引書 AFⅡ V10 用 ・OSⅣ PLOP/X 使用手引書 ・OSⅣ/MSP SMF 説明書 AFⅡ V10 用 ・OSⅣ/MSP SMP 使用手引書 AFⅡ V10 用 ・OSⅣ/MSP コンソールコマンド文法書 AFII V10 用 ・OSⅣ/MSP システムパラメタ文法書 AFⅡ V10 用 ・OSⅣ/MSP システムプログラミング手引書　タスク管理編 AFⅡ V10 用 ・OSⅣ/MSP システムユーティリティ 使用手引書 AFⅡ V10 用 ・OSⅣ/MSP ジョブ制御言語文法書 AFⅡ V10 用 ・OSⅣ/MSP タスク管理マクロ命令文法書 AFⅡ V10 用 ・OSⅣ/MSP タスク管理解説書 AFⅡ V10 用 ・OSⅣ/MSP メッセージ説明書 AFⅡ V10 用 ・OSⅣ/MSP 運用手引書 JES 編 AFII V10 用 ・OSⅣ/MSP 操作手引書 AFII V10 用 ・OSⅣ/MSP TSS/E コマンド文法書 V11L20 用 ・OSⅣ VTAM-G 導入手引書 V30 用 ・FACOM M シリーズ ハードウェア機能説明書 I(命令編) ・FACOM M シリーズ ハードウェア機能説明書Ⅱ(機能編) ・ソフトウェア説明書 OSIV/MSP セキュア AF2 V10 ・ソフトウェア説明書 OSIV/MSP RACF V12

クラス	コンポーネント名	保証手段
	AGD_USR.1	・OSⅣ/MSP RACF コマンド文法書 V12L10 用 ・OSⅣ/MSP RACF メッセージ説明書 V12L10 用 ・OSⅣ/MSP RACF ユーティリティ使用手引書 V12L10 用 ・OSⅣ/MSP RACF 使用手引書 利用者編 V12L10 用 ・OSⅣ/MSP ARCS 使用手引書 AFⅡ V10 用 ・OSⅣ/MSP GDS 使用手引書 AFⅡ V10 用 ・OSⅣ/MSP IORGP 使用手引書 AFⅡ V10 用 ・OSⅣ/MSP PIC 使用手引書 AFⅡ V10 用 ・OSⅣ PLOP/X 使用手引書 ・OSⅣ/MSP VSAM マクロ命令文法書 AFⅡ V10 用 ・OSⅣ/MSP アセンブラ使用手引書 AFⅡ V10 用 ・OSⅣ/MSP サービスエイド使用手引書 AFⅡ V10 用 ・OSⅣ/MSP システムプログラミング手引書 データ管理編 AFⅡ V10 用 ・OSⅣ/MSP システムユーティリティ使用手引書 AFⅡ V10 用 ・OSⅣ/MSP ジョブ制御言語文法書 AFⅡ V10 用 ・OSⅣ/MSP タスク管理マクロ命令文法書 AFⅡ V10 用 ・OSⅣ/MSP タスク管理解説書 AFⅡ V10 用 ・OSⅣ/MSP データセットユーティリティ使用手引書 AFⅡV10 用 ・OSⅣ/MSP データ管理マクロ命令文法書 AFⅡ V10 用 ・OSⅣ データ変換ユーティリティ説明書 V10 用 ・OSⅣ/MSP メッセージ説明書 AFⅡ V10 用 ・OSⅣ/MSP リンケージエディタ/ローダ使用手引書 AFⅡ V10 用 ・OSⅣ/MSP TSS/E コマンド開発手引書 V11L20 用 ・OSⅣ/MSP TSS/E コマンド文法書 V11L20 用 ・OSⅣ/MSP TSS/E メッセージ説明書 V11L20 用 ・OSⅣ/MSP TSS/E 運用手引書 V11L20 用
テスト	ATE_IND.1	

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セキュリティ環境に対応するセキュリティ対策方針の関係を『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』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

TOE セキュリティ環境 / セキュリティ対策方針	A.ADMIN	A.PASSWORD	A.PHY_PROTECT	T.ILLIGAL_ACCESS	T.PROGRAM
O.AUTHORIZATION				○	
O.ACCESS				○	
O.PROGRAM_SEP					○
OE.ADMIN	○				
OE.PASSWORD		○			
OE.PHY_RROTECT			○		

以下に、『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』の根拠を示す。

8.1.1　　前提条件に対する対策方針の対応

A.ADMIN

A.ADMIN は、利用者である RACF センタ要員および管理者が、不正を行わない信頼できる人物であることを規定した前提条件である。

この前提条件を実現するためには、RACF センタ要員および管理者に対して不正を行なわないよう教育が実施されることが必要である。

OE.ADMIN において、最高管理者が、RACF センタ要員及び管理者として信頼できる人物を選任し、不正を行わないように教育を施すことが規定されている。

従って、セキュリティ対策方針 OE.ADMIN が満たされることにより、本前提条件を実現することができる。

A.PASSWORD

A.PASSWORD は、利用者である RACF センタ要員、管理者及び一般利用者が使用するパスワードが、本人以外に知られないことを規定した前提条件である。

この前提条件を実現するためには、RACF センタ要員、管理者および一般利用者が、パスワードを他人に開示しないこと、定期的に変更することを実施することが必要となる。

OE.PASSWORD において、RACF センタ要員、管理者は使用するパスワードを本人以外に開示しないこと、定期的に変更すことが規定されている。また、同対策方針により、管理者が、一般利用者に対して、使用するパスワードを本人以外に開示しない、定期的に変更する等、適切に管理するように教育することが規定されている。

従って、セキュリティ対策方針 OE.PASSWORD が満たされることにより、本前提条件を実現することができる。

A.PHY_PROTECT

A.PHY_PROTECT は、TOE が動作するサーバおよびコンソールが、RACF センタ要員以外の人物が入退出できないことを規定した前提条件である。

この前提条件を実現するためには、TOE が動作するサーバおよびコンソールが、RACF センタ要員以外が入退室できないように管理された場所に設置されることが必要となる。

OE.PHY_PROTECT において、TOE が動作するサーバおよびコンソールは、RACF センタ要員によって、RACF センタ要員以外の人物が入退出できない、物理的に管理された場所に設置されることが規定されている。

従って、セキュリティ対策方針 OE. PHY_PROTECT が満たされることにより、本前提条件を実現することができる。

8.1.2　　脅威に対する対策方針の対応

T.ILLIGAL_ACCESS

T.ILLIGAL_ACCESSは、悪意のある人物が、コマンド／アプリケーションを利用して、資源に対し、資源の所有者が許可しない不正なアクセスを行う脅威である。

この脅威に対抗するためには、TOE にアクセスする人物が正当な TOE の関係者か識別認証した上で、TOE の関係者に、資源の所有者が許可する範囲内でのアクセスを許可することが必要である。

TOE では、O.AUTHORIZATION により、TOE にアクセスする人物が正当な TOE の関係者か識別認証する。

O.ACCESS により、TOE の関係者に対し、資源の所有者が許可するアクセスのみを許可する。

従って、O.AUTHORIZATION、O.ACCESS が満たされることにより、本脅威に対抗することができる。

T.PROGRAM

T.PROGRAM は､不正なジョブが TOE の領域にアクセスして他のジョブの実行処理に干渉することによって、資源に対して不正なアクセスを行なう脅威である。

この脅威に対抗するためには、ジョブが他のジョブの実行処理に干渉をしないよう分離した空間に配置する必要がある。

TOE では、O.PROGRAM_SEP により、ジョブが他のジョブの実行処理に干渉しないように分離した空間制御を行なう。

従って、O.PROGRAM_SEP が満たされることにより、本脅威に対抗することができる。

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

セキュリティ対策方針に対するセキュリティ機能要件の対応を『表 8-2 セキュリティ対策方針とセキュリティ機能要件の対応』に示す。

表 8-2 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.AUTHORIZATION	O.ACCESS	O.PROGRAM_SEP
FAU_GEN.1	○	○	
FAU_SAR.1	○	○	
FAU_SEL.1	○	○	
FAU_STG.1	○	○	
FAU_STG.3	○	○	
FDP_ACC.1		○	
FDP_ACF.1		○	
FIA_AFL.1	○		
FIA_ATD.1	○		
FIA_SOS.1	○		
FIA_UAU.2	○		
FIA_UAU.7	○		
FIA_UID.2	○		
FIA_USB.1	○		
FMT_MOF.1		○	
FMT_MSA.1		○	
FMT_MSA.3		○	
FMT_MTD.1	○	○	
FMT_SAE.1	○		
FMT_SMF.1	○	○	
FMT_SMR.1	○	○	
FPT_AMT.1	○	○	○

セキュリティ機能要件 ＼ セキュリティ対策方針	O.AUTHORIZATION	O.ACCESS	O.PROGRAM_SEP
FPT_RVM.1	○	○	○
FPT_SEP.1	○	○	○
FPT_STM.1	○	○	

以下に、『表 8-2 セキュリティ対策方針とセキュリティ機能要件の対応』の根拠を示す。

O.AUTHORIZATION

O.AUTHORIZATION は、TOE にアクセスする RACF センタ要員、管理者及び一般利用者が正当な人物であるかを識別し、認証する対策方針である。

本対策方針を実現するためには、正当な人物であることを確認するのに十分なセキュリティ強度を持った識別認証の機能要件を導出する必要がある。

そのため、本 TOE では以下の機能要件を導出する。

- FIA_UAU.2 及び FIA_UID.2 により、TOE の利用の前に識別認証を行なう。
  識別認証のタイミングで、FIA_ATD.1 により、利用者に属するセキュリティ属性の定義が行なわれ、FIA_USB.1 により、定義されてセキュリティ属性と利用者を代替するサブジェクト（ジョブ）との結合を行なう。
- FIA_UAU.7 により、識別認証の際に入力されるパスワードは、非表示となる。
- FIA_AFL.1 により、認証失敗時に、規定回数以上の認証失敗を繰り返した場合、失権状態とする。
  なお、復権は、同FIA_AFL.1により、「権限を持つ人物による復権操作」か、「一定期間経過後の自動復権」により行う。
- FIA_SOS.1により、識別認証に利用される秘密に対し「構文規約チェック」を行なう検証メカニズムを提供する。

また、本対策方針に関わる機能要件を管理するために、以下の機能要件を導出する。

- FMT_MTD.1 により、TSF データ（パスワード及び、識別認証の設定が記載されている RACF 管理簿）を管理する能力を、許可された識別された役割に制限する。
- FMT_SAE.1 により、パスワードの有効期限を設定する能力を、許可された識別された役割に制限する。
- FMT_SMF.1 により、FMT_MTD.1、FMT_SAE.1 の実体となる、セキュリティ管理機能を提供する。

・ FMT_SMR.1 により、許可された識別された役割の維持や、利用者との関連付けが行なわれる。

また本対策方針に関わる機能要件が確実に動作していることを監査できるようにするために、以下の機能要件を導出する。

・ FAU_GEN.1 により、識別認証に関わる機能要件に対する操作の監査ログが採取される。また、FPT_STM.1 により、FAU_GEN.1 にて使用される時間は信頼できる時間となる。
・ FAU_SAR.1 により、監査ログを解釈するのに適した形式（監査レポート）で出力する能力を、許可された役割のみに提供する。
・ FAU_STG.1 により、監査ログに対する不正な改変を防止する。
・ FAU_STG.3 により、監査ログにおいて、定義された格納領域の限界に達した際、取られるアクションが規定される。
・ FAU_SEL.1 により、、監査ログにて採取するイベントの規定能力を、許可された役割のみに制限する。

また、以下により、本対策方針に関わる機能要件の確実な実施が保証される。

・ FPT_AMT.1 により、セキュリティ機能が展開されているメモリに対する動作テストが実施される。
・ FPT_RVM.1 により、本対策方針に関わる機能要件は確実に実施され、成功することを保証する。
・ FPT_SEP.1 により、セキュリティドメインが TSF の実行のために構築される。

以上のセキュリティ機能要件によって、O.AUTHORIZATION を満たすことができる。

O.ACCESS

O.ACCESS は、TOE の関係者に対し、資源の所有者が許可するアクセスのみを許可する対策方針である。

本対策方針を実現するためには、利用者を代行するジョブに対して、資源の所有者が許可するアクセスのみを許可するアクセス制御を行なう機能要件を導出する必要がある。

・ FDP_ACC.1 により、ジョブと資源間において、資源の所有者が許可するアクセスのみを許可するアクセス制御 SFP を定義し、FDP_ACF.1 により当該アクセス制御 SFP の具体的なアクセス制御規則を規定する。

また、本対策方針に関わる機能要件を管理するために、以下の機能要件を導出する。

・ FMT_MOF.1 により、アクセス制御機能のふるまい決定、及び動作／停止させる能力を許可された識別された役割のみに制限する。
・ FMT_MSA.1 により、アクセス制御 SFP に関係する属性を管理する能力を、許可された識別された役割のみに制限する。
・ FMT_MSA.3 により、アクセス制御 SFP における、オブジェクトが生成される際にデ

フォルトで与えられる属性が定義される。

- FMT_MTD.1 により、TSF データ（アクセス制御のルールが記載されている RACF 管理簿）を管理する能力を、許可された識別された役割に制限する。
- FMT_SMF.1 により、FMT_MOF.1、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1 の実体となる、セキュリティ管理機能を提供する。
- FMT_SMR.1 により、許可された識別された役割の維持や、利用者との関連付けが行なわれる。

また、本対策方針に関わる機能要件が確実に動作していることを監査できるようにするために、以下の機能要件を導出する。

- FAU_GEN.1 により、アクセス制御の機能要件に関する操作の監査ログが採取される。また、FPT_STM.1 により、FAU_GEN.1 にて使用される時間は信頼できる時間となる。
- FAU_SAR.1 により、監査ログを解釈するのに適した形式（監査レポート）で出力する能力を、許可された役割のみに提供する。
- FAU_STG.1 により、監査ログに対する不正な改変を防止する。
- FAU_STG.3 により、監査ログにおいて、定義された格納領域の限界に達した際、取られるアクションが規定される。
- FAU_SEL.1 により、監査ログにて採取するイベントの規定能力を、許可された役割のみに制限する。

また、以下により、本対策方針に関わる機能要件の確実な実施が保証される。

- FPT_AMT.1 により、セキュリティ機能が展開されているメモリに対する動作テストが実施される。
- FPT_RVM.1 により、本対策方針に関わる機能要件は確実に実施され、成功することを保証する。
- FPT_SEP.1 により、セキュリティドメインが TSF の実行のために構築される。

以上のセキュリティ機能要件によって、O.ACCESS を満たすことができる。

O.PROGRAM_SEP

O.PROGRAM_SEP は、ジョブが他のジョブの実行処理に干渉しないように分離した空間制御を行なう対策方針である。

本対策方針を実現するためには、ジョブにより実行されたアプリケーションのロードされている空間が、それぞれ分離されていることを保証する機能要件を導出する必要がある。

TOE では、FPT_SEP.1 により、ジョブにより実行されたアプリケーションが、TOE が提供する独立したドメインに展開され、互いに干渉しないことを保証している。

また以下により、本対策方針に関わる機能要件の確実な実施が保証される。

- FPT_AMT.1 により、セキュリティ機能が展開されているメモリに対する動作テスト

が実施される。

・ FPT_RVM.1により、本対策方針に関わる機能要件は確実に実施され、成功することを保証する。

以上のセキュリティ機能要件によって、O.PROGRAM_SEPを満たすことができる。

8.2.2 TOEセキュリティ機能要件間の依存関係

TOEセキュリティ機能要件間の依存関係を『表 8-3 TOEセキュリティ機能要件間の依存関係』に示す。

表 8-3 TOEセキュリティ機能要件間の依存関係

NO	機能要件	下位階層	依存関係	参照NO	備考
1	FAU_GEN.1	なし	FPT_STM.1	25	
2	FAU_SAR.1	なし	FAU_GEN.1	1	
3	FAU_SEL.1	なし	FAU_GEN.1	1	
			FMT_MTD.1	18	
4	FAU_STG.1	なし	－	－	－
5	FAU_STG.3	なし	FAU_STG.1	4	
6	FDP_ACC.1	なし	FDP_ACF.1	8	
7	FDP_ACF.1	なし	FDP_ACC.1	6	
			FMT_MSA.3	17	
8	FIA_AFL.1	なし	FIA_UAU.1	11	FIA.UAU.2は、FIA_UAU.1の上位階層のコンポーネントである。
9	FIA_ATD.1	なし	なし	－	
10	FIA_SOS.1	なし	なし	－	
11	FIA_UAU.2	FIA_UAU.1	FIA_UID.1	13	FIA.UID.2は、FIA_UID.1の上位階層のコンポーネントである。
12	FIA_UAU.7	なし	FIA_UAU.1	11	FIA.UAU.2は、FIA_UAU.1の上位階層のコンポーネントである。
13	FIA_UID.2	FIA_UID.1	なし	－	

NO	機能要件	下位階層	依存関係	参照 NO	備考
14	FIA_USB.1	なし	FIA_ATD.1	9	
15	FMT_MOF.1	なし	FMT_SMF.1	20	
			FMT_SMR.1	21	
16	FMT_MSA.1	なし	[FDP_ACC.1 または FDP_IFC.1]	6	
			FMT_SMF.1	20	
			FMT_SMR.1	21	
17	FMT_MSA.3	なし	FMT_MSA.1	16	
			FMT_SMR.1	21	
18	FMT_MTD.1	なし	FMT_SMF.1	20	
			FMT_SMR.1	21	
19	FMT_SAE.1	なし	FMT_SMR.1	21	
			FPT_STM.1	25	
20	FMT_SMF.1	なし	なし	－	
21	FMT_SMR.1	なし	FIA_UID.1	13	FIA.UID.2 は、FIA_UID.1 の上位階層のコンポーネントである。
22	FPT_AMT.1	なし	なし	－	
23	FPT_RVM.1	なし	なし	－	
24	FPT_SEP.1	なし	なし	－	
25	FPT_STM.1	なし	なし	－	

8.2.3　　TOE セキュリティ機能要件の相互作用

明示的な依存関係は要求されないが、相互支援を目的として選択されたセキュリティ機能要件を『表 8-4 TOEセキュリティ機能要件の相互作用について』に示す。

表 8-4 TOE セキュリティ機能要件の相互作用について

NO	機能要件	相互サポート			
		迂回防止	ドメイン分離	非活性化防止	無効化検出
1	FAU_GEN.1	FPT_RVM.1	FPT_SEP.1	N/A	N/A
2	FAU_SAR.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
3	FAU_SEL.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
4	FAU_STG.1	FPT_RVM.1	FPT_SEP.1	N/A	N/A
5	FAU_STG.3	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
6	FDP_ACC.1	FPT_RVM.1	FPT_SEP.1	N/A	N/A
7	FDP_ACF.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1 FMT_MOF.1	FAU_GEN.1 FAU_SAR.1
8	FIA_AFL.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
9	FIA_ATD.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	N/A
10	FIA_SOS.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
11	FIA_UAU.2	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
12	FIA_UAU.7	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	N/A
13	FIA_UID.2	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
14	FIA_USB.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
15	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
16	FMT_MSA.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1

17	FMT_MSA.3	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
18	FMT_MTD.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
19	FMT_SAE.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
20	FMT_SMF.1	FPT_RVM.1	FPT_SEP.1	N/A	FAU_GEN.1 FAU_SAR.1
21	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1
22	FPT_AMT.1	FPT_RVM.1	N/A	N/A	不要
23	FPT_RVM.1	N/A	N/A	N/A	N/A
24	FPT_SEP.1	FPT_RVM.1	N/A	N/A	N/A
25	FPT_STM.1	FPT_RVM.1	FPT_SEP.1	FMT_MTD.1	FAU_GEN.1 FAU_SAR.1

FPT_RVM.1<迂回防止>

FPT_RVM.1 により、TSC 内の各機能の動作進行が許可される前に、識別認証機能、アクセス制御機能、監査機能、セキュリティ管理機能、及び TSF 保護機能に関するセキュリティ機能要件が呼び出され成功することが保証される。

従って、FPT_RVM.1 によって関係する機能要件への迂回防止を支援しているため、セキュリティ対策方針 O.AUTHORIZATION、O.ACCESS、O.PROGRAM_SEP が達成される。

FPT_SEP.1<ドメイン分離>

FPT_SEP.1 により、識別認証機能、アクセス制御機能、監査機能、セキュリティ管理機能に関するセキュリティ機能要件は、信頼できないサブジェクトによる干渉と改ざんから保護するセキュリティドメインが構築されることが保証される。

従って、FPT_SEP.1 によって関係する機能要件への干渉及び改ざん防止を支援しているため、セキュリティ対策方針 O.AUTHORIZATION、O.ACCESS 及び O.PROGRAM_SEP が達成される。

FMT_MTD.1、FMT_MOF.1<非活性化防止>

・1. FMT_MTD.1 による非活性化防止

FMT_MTD.1 により、識別認証機能、アクセス制御機能、監査機能、セキュリティ管理機能に関するセキュリティ機能要件が使用する TSF データ（RACF 管理簿）への操作を、特権を有した人物のみに制限しているため、TOE を非活性化させる攻撃へ対抗している。

・2. FMT_MOF.1 による非活性化防止

FMT_MOF.1 により、アクセス制御機能に関するセキュリティ機能要件への操作を、管理者権限を有した人物のみに制限しているため、TOE を非活性化させる攻撃へ対抗している。

以上、FMT_MTD.1 及び FMT_MOF.1 により、関係する機能要件への非活性化防止を支援しているため、セキュリティ対策方針 O.AUTHORIZATION、O.ACCESS が達成される。

FAU_GEN.1、FAU_SAR.1<無効化検出>

FAU_GEN.1 により、TOE のセキュリティ機能要件の実行に伴い、セキュリティ関連事象を記録する。また、FAU_SAR.1 にて、FAU_GEN.1 にて採取した監査ログを許可利用者が分かり易い形式で出力する。そのため、セキュリティ機能要件の無効化への操作を検出することが保証される（※)。

従って、FAU_GEN.1、FAU_SAR.1 によって関係する機能要件の無効化防止を支援しているため、セキュリティ対策方針 O.AUTHORIZATION 、O.ACCESS が達成される。

※FPT_AMT.1 に関しては、FPT_AMT.1 が無効化された場合、TOE 自体が動作しなくなるため、TSF が無効化された状態で運用されるという事象は発生しない。そのため、監査ログに事象を採取・解析する必要がなく、FAU_GEN.1 及び FAU_SAR.1 による、無効化検知の保証対象外とする。

8.2.4　　最小機能強度根拠

TOE が利用される環境での攻撃者の攻撃能力を低レベルと定義しているため、攻撃方法は、公開インタフェース、公開情報を利用したものとなる。低レベルの攻撃であれば、TOE が実施している対策である O.AUTHORIZATION、O.ACCESS、O.PROGRAM_SEP で対抗できるため、TOE のセキュリティ対策方針は低レベルの攻撃に対抗しているといえる。

従って、TOEのセキュリティ対策方針が低レベルの攻撃者に対抗しているため、TOEのセキュリティ対策方針は最小機能強度SOF-基本と一貫している。

また、特定の機能要件(FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.7、FIA_UID.2)の機能強度は SOF-基本であり、最小機能強度の SOF-基本と一貫している。

8.2.5　　セキュリティ保証要件根拠

TOE には、市場からの要求として、利用者のデータの保護に関して配慮されていることに関する、独立した第三者による保証が提供されていることが望まれている。そのため、TOE は仕様に対する独立テストや提供されるガイダンスの調査など、市場の要求を満たす第三者保証を得ることが求められる。

このような市場の要求に答えるための保証を得る評価保証レベルとして EAL1 は適している。

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

TOE要約仕様に適合するセキュリティ機能要件の関係を『表 8-5 TOE要約仕様とセキュリティ機能要件の対応』に示す。

表 8-5 TOE 要約仕様とセキュリティ機能要件の対応

TOE 要約仕様 / TOE セキュリティ機能要件	識別認証機能	グローバルチェック機能	構造化グループ機能	資源アクセス制御機能	JESCI アクセス権確認機能	監査機能	セキュリティ管理機能	TSF 保護機能
FAU_GEN.1						○		
FAU_SAR.1						○		
FAU_SEL.1							○	
FAU_STG.1						○		
FAU_STG.3						○		
FDP_ACC.1		○	○	○	○			
FDP_ACF.1		○	○	○	○			
FIA_AFL.1	○							
FIA_ATD.1	○							
FIA_SOS.1	○							
FIA_UAU.2	○							
FIA_UAU.7	○							
FIA_UID.2	○							
FIA_USB.1	○							
FMT_MOF.1							○	
FMT_MSA.1							○	
FMT_MSA.3							○	
FMT_MTD.1							○	

TOE 要約仕様 / TOE セキュリティ機能要件	識別認証機能	グローバルチェック機能	構造化グループ機能	資源アクセス制御機能	JESCI アクセス権確認機能	監査機能	セキュリティ管理機能	TSF 保護機能
FMT_SAE.1							○	
FMT_SMF.1							○	
FMT_SMR.1							○	
FPT_AMT.1								○
FPT_RVM.1	○	○	○	○	○	○	○	○
FPT_SEP.1								○
FPT_STM.1						○		

以下に、『表 8-5 TOE要約仕様とセキュリティ機能要件の対応』の根拠を示す。

※TOE 要約仕様が、複数の機能要件の特徴を持っている場合、当該機能要件に該当する部分に下線を引いて示す。

FAU_GEN.1

「監査機能」は、「識別認証機能」「アクセス制御機能」「監査機能」「セキュリティ管理機能」に関する監査事象を採取し、監査ログを生成している。そのため、本要件を満足することができる。

FAU_SAR.1

「監査機能」は、監査する人物が読みやすい形式（監査レポート：「認証履歴表」、「資源アクセス履歴表」、「利用者アクセス履歴表」、「資源定義履歴表」、「利用者定義履歴表」、「データセンタ属性管理履歴表」）で出力する機能を提供する。

そのため、本要件を満足することができる。

FAU_SEL.1

「セキュリティ管理機能」は、事象種別として「すべてのアクセスログを収集する」、「正当なアクセスログを収集する」、「不当なアクセスログを収集する」、「アクセスの記

録を収集しない」から監査ログに採取するイベントを選択する機能を提供している。
そのため、本要件を満足することができる。

FAU_STG.1

「監査機能」は、監査ログに対する改変を防止する制御を行なう。
そのため、本要件を満足することができる。

FAU_STG.3

「監査機能」は、監査ログが限界に達した際に、以下を行なう機能を提供する。

- 枯渇した監査ログ領域を保護
- 監査ログの記録領域を新規に作成
- RACF センタ要員への通知

そのため、本要件を満足することができる。

FDP_ACC.1

「構造化グループ機能」、「グローバルチェック機能」「資源アクセス制御機能」、「JESCI アクセス権確認機能」は、TOE の関係者に対し、資源の所有者が許可するアクセスのみを許可する機能である。
そのため、本要件を満足することができる。

FDP_ACF.1

「構造化グループ機能」、「グローバルチェック機能」、「資源アクセス制御機能」、「JESCI アクセス権確認機能」は、TOE の関係者に対し、資源の所有者が許可するアクセスのみを許可する機能である。
そのため、本要件を満足することができる。

FIA_AFL.1

「識別認証機能」は、以下を提供する機能である。
不成功のパスワード失敗が規定された回数（1～999）を超えた際に、利用者を失権する。失権状態からの復権は、「権限を持つ人物による復権処理」か「一定期間経過後の自動復権」により行われる。
そのため、本要件を満足することができる。

FIA_ATD.1

「識別認証機能」は、利用者に対し識別認証を行なう機能であり、識別認証が成功した場合、その利用者を代行するジョブとして TOE 内で存在する。ジョブは、利用者に関

する情報をリストとして有し、利用者としてのふるまいを継承している。

そのため、本要件を満足することができる。

FIA_UAU.2

「識別認証機能」は、識別認証機能以外のセキュリティ機能を使用する前に、TOE にアクセスする人物に対し、利用者識別名及びパスワードを利用した識別認証を行なう機能である。

そのため、本要件を満足することができる。

FIA_UAU.7

「識別認証機能」においては、使用するパスワードのフィードバックは行なわない（非表示）である。

そのため、本要件を満足することができる。

FIA_UID.2

「識別認証機能」は、識別認証機能以外のセキュリティ機能を使用する前に、TOE にアクセスする人物に対し、利用者識別名及びパスワードを利用した識別認証を行なう機能である。

そのため、本要件を満足することができる。

FIA_SOS.1

「識別認証機能」は、パスワードが以下の規則に従っているかを検証する機能である。

- 利用者パスワードの構文規約チェック　：8文字以内の各国記号（¥,#,@）を含む英数字

そのため、本要件を満足することができる。

FIA_USB.1

「識別認証機能」は、利用者に対し識別認証を行なう機能であり、識別認証が成功した場合、その利用者を代行するジョブとして TOE 内で存在する。

ジョブは、利用者に関する情報をリストとして有し、利用者としてのふるまいを継承している。なお、利用者を代行するジョブの属性は RACF センタ要員により変更し、管理下の一般利用者を代行するジョブの属性は管理者により変更する。

そのため、本要件を満足することができる。

FMT_MOF.1

「セキュリティ管理機能」は、RACF 空間のリフレッシュに伴う「アクセス制御機能」のふるまいの決定、及び RACF センタ出口ルーチンの設定に伴う、「アクセス制御機能」の起動、停止、ふるまいの改変、を行なう能力を RACF センタ要員のみに制限し提供する機能である。

そのため、本要件を満足することができる。

FMT_MSA.1

「セキュリティ管理機能」は、「構造化グループ機能」、「グローバルチェック機能」、「資源アクセス制御機能」「JESCIアクセス権確認機能」に関する属性の管理を、「RACFセンタ要員」「管理者」「一般利用者」に制限し提供する機能である。

そのため、本要件を満足することができる。

FMT_MSA.3

「セキュリティ管理機能」は、作成時登録機能（資源を作成すると自動的に個別名で RACF 管理簿に登録され保護される機能）を設定する機能を、RACF センタ要員、管理者に提供している。作成時登録機能が設定されていないと、利用者が作成した資源は RACF 管理簿に登録されず、所有者以外からのアクセスは拒否される。

そのため、本要件を満足することができる。

FMT_MTD.1

「セキュリティ管理機能」は、RACF 管理簿を問い合わせ、改変、バックアップ、稼動／非稼動設定、する能力を「RACF センタ要員」のみに制限し提供している。時間情報を改変する能力を「RACF センタ要員」のみに制限し提供している。また、パスワードを改変する能力をそれぞれの役割に応じて「RACF センタ要員」「管理者」「一般利用者」に制限し提供している。

そのため、本要件を満足することができる。

FMT_SAE.1

「セキュリティ管理機能」は、パスワードの有効期限の設定する能力を「RACFセンタ要員」「一般利用者」のみに制限し提供する。また、本機能では有効期限が切れた際の挙動（パスワード変更の要求）を規定し提供している。

そのため、本要件を満足することができる。

FMT_SMF.1

「セキュリティ管理機能」は、セキュリティ機能の起動・停止機能や、アクセス制御に関する属性の管理機能、TSFデータ(RACF管理簿)の管理機能(採取イベントの定義を含む)、時間の設定機能、及びパスワードの有効期限の管理機能を提供する。

そのため、本要件を満足することができる。

FMT_SMR.1

「セキュリティ管理機能」は、TSF を利用できる役割を維持している。

そのため、本要件を満足することができる。

FPT_AMT.1

「TSF 保護機能」は、TOE の起動時に、メモリが正常に動作するか検証を行う機能を提供する。

そのため、本要件を満足することができる。

FPT_RVM.1

「識別認証機能」、「アクセス制御機能」、「監査機能」、「セキュリティ管理機能」、「TSF 保護機能」は、確実に呼び出されることが保証される。

そのため、本要件を満足することができる。

FPT_SEP.1

「TSF 保護機能」は、アプリケーションごとに独立した空間（仮想記憶）を作成することで、TOE を含むアプリケーション間の干渉発生を防止し、改ざん、漏洩、暴露が発生しないセキュリティドメインを構築する。

そのため、本要件を満足することができる。

FPT_STM.1

「監査機能」は、高信頼な時間を生成し、監査ログに設定する。

そのため、本要件を満足することができる。

8.3.2　セキュリティ機能強度根拠

特定の TOE セキュリティ機能要件に対する機能強度は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2、FIA_UAU.7、FIA_UID.2 に対する機能強度である SOF-基本である。また、IT セキュリティ機能に対する機能強度は、「識別認証機能」に対する機能強度である SOF-基本である。

そのため、特定の TOE セキュリティ機能要件に対する機能強度と、IT セキュリティ機能に対する機能強度は一貫している。

8.3.3 保証手段根拠

表 6-13 に示した通り、全てのTOEセキュリティ保証要件は保証手段により示されたドキュメントのセットによって対応付けられる。

以下に、EAL1 の保証要件セットが各保証手段により満たされる根拠を示す。

ACM_CAP.1　　バージョン番号

【保証手段】

・OSIV/MSP セキュア AF2 V10L10 ソフトウェア説明書

・コマンド投入による、TOE の構成プログラム名称及びバージョンの表示

【保証要件根拠】

保証手段である、「OSIV/MSP セキュア AF2 V10L10 ソフトウェア説明書」には、TOE の名称及びバージョンを記載する。また、TOE の導入後には「コマンド投入による、TOE の構成プログラム名称及びバージョンの表示」により、TOE を構成するプログラムの名称及びバージョンを表示する。これらの手段により、TOE のリファレンスを可能とするため、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】

- OSIV/MSP セキュア AF2 V10L10 ソフトウェア説明書
- OSIV/MSP RACF 導入手引書 V12L10 用
- OSIV/MSP RACF 使用手引書 管理者編 V12L10 用
- OSIV/MSP システム導入手引書 AFII V10 用
- OSIV/MSP TSS/E 運用手引書 V11L20 用
- OSIV VTAM-G 導入手引書 V30 用

【保証要件根拠】

保証手段に示した資料には、TOE をセキュアな構成にするために採用される、設置手順及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】

- OSIV/MSP セキュア AF2 識別認証機能 機能仕様書
- OSIV/MSP セキュア AF2 アクセス制御機能 機能仕様書
- OSIV/MSP セキュア AF2 RACF 機能 API　機能仕様書
- OSIV/MSP セキュア AF2 監査機能 機能仕様書
- OSIV/MSP セキュア AF2 セキュリティ管理機能 機能仕様書
- OSIV/MSP セキュア AF2 セキュリティ管理機能 機能仕様書（ユーティリティ編）
- OSIV/MSP セキュア AF2 セキュリティ管理機能 機能仕様書（コンソールコマンド編）
- OSIV/MSP セキュア AF2 RACF 機能 センタ出口ルーチン 機能仕様書
- OSIV/MSP セキュア AF2 TSF 保護機能 機能仕様書
- OSIV/MSP セキュア AF2 非セキュリティ機能 機能仕様書

【保証要件根拠】

保証手段に示した資料には、TSF に対する全て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】

- OSIV/MSP セキュア AF2 表現対応表

【保証要件根拠】

保証手段である「OSIV/MSP セキュア AF2 表現対応表」には、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】

- OSIV/MSP RACF 運用手引書 V12L10 用
- OSIV/MSP RACF 使用手引書 管理者編 V12L10 用
- OSIV/MSP RACF コマンド文法書 V12L10 用
- OSIV/MSP RACF システムプログラマの手引 V12L10 用
- OSIV/MSP RACF ユーティリティ使用手引書 V12L10 用
- OSIV/MSP RACF メッセージ説明書 V12L10 用
- OSIV/MSP RACF 導入手引書 V12L10 用
- OSIV/MSP AMS コマンド文法書 AFⅡ V10 用

- OSⅣ/MSP IORGP 使用手引書 AFⅡ V10 用
- OSⅣ PLOP/X 使用手引書
- OSⅣ/MSP SMF 説明書 AFⅡ V10 用
- OSⅣ/MSP SMP 使用手引書 AFⅡ V10 用
- OSⅣ/MSP コンソールコマンド文法書 AFII V10 用
- OSⅣ/MSP システムパラメタ文法書 AFⅡ V10 用
- OSⅣ/MSP システムプログラミング手引書　タスク管理編 AFⅡ V10 用
- OSⅣ/MSP システムユーティリティ 使用手引書 AFⅡ V10 用
- OSⅣ/MSP ジョブ制御言語文法書 AFⅡ V10 用
- OSⅣ/MSP タスク管理マクロ命令文法書 AFⅡ V10 用
- OSⅣ/MSP タスク管理解説書 AFⅡ V10 用
- OSⅣ/MSP メッセージ説明書 AFⅡ V10 用
- OSⅣ/MSP 運用手引書 JES 編 AFII V10 用
- OSⅣ/MSP 操作手引書 AFII V10 用
- OSⅣ/MSP TSS/E コマンド文法書 V11L20 用
- OSⅣ VTAM-G 導入手引書 V30 用
- FACOM M シリーズ ハードウェア機能説明書 I(命令編)
- FACOM M シリーズ ハードウェア機能説明書Ⅱ(機能編)
- ソフトウェア説明書 OSⅣ/MSP セキュア AF2 V10
- ソフトウェア説明書 OSⅣ/MSP RACF V12

【保証要件根拠】

保証手段に示した資料には、TOE の管理者が使用するインタフェース、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 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】

- OSⅣ/MSP RACF コマンド文法書 V12L10 用
- OSⅣ/MSP RACF メッセージ説明書 V12L10 用
- OSⅣ/MSP RACF ユーティリティ使用手引書 V12L10 用
- OSⅣ/MSP RACF 使用手引書 利用者編 V12L10 用
- OSⅣ/MSP ARCS 使用手引書 AFⅡ V10 用
- OSⅣ/MSP GDS 使用手引書 AFⅡ V10 用
- OSⅣ/MSP IORGP 使用手引書 AFⅡ V10 用
- OSⅣ/MSP PIC 使用手引書 AFⅡ V10 用

- OSⅣ PLOP/X 使用手引書
- OSⅣ/MSP VSAM マクロ命令文法書 AFⅡ V10 用
- OSⅣ/MSP アセンブラ使用手引書 AFⅡ V10 用
- OSⅣ/MSP サービスエイド使用手引書 AFⅡ V10 用
- OSⅣ/MSP システムプログラミング手引書 データ管理編 AFⅡ V10 用
- OSⅣ/MSP システムユーティリティ使用手引書 AFⅡ V10 用
- OSⅣ/MSP ジョブ制御言語文法書 AFⅡ V10 用
- OSⅣ/MSP タスク管理マクロ命令文法書 AFⅡ V10 用
- OSⅣ/MSP タスク管理解説書 AFⅡ V10 用
- OSⅣ/MSP データセットユーティリティ使用手引書 AFⅡV10 用
- OSⅣ/MSP データ管理マクロ命令文法書 AFⅡ V10 用
- OSⅣ データ変換ユーティリティ説明書 V10 用
- OSⅣ/MSP メッセージ説明書 AFⅡ V10 用
- OSⅣ/MSP リンケージエディタ/ローダ使用手引書 AFⅡ V10 用
- OSⅣ/MSP TSS/E コマンド開発手引書 V11L20 用
- OSⅣ/MSP TSS/E コマンド文法書 V11L20 用
- OSⅣ/MSP TSS/E メッセージ説明書 V11L20 用
- OSⅣ/MSP TSS/E 運用手引書 V11L20 用

【保証要件根拠】

保証手段に示した資料には、TOE の利用者が使用するインタフェース、及び 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】

なし

【保証要件根拠】

保証要件 ATE_IND.1 に対する保証手段は要求されていない。

8.4　PP 主張根拠

本 ST が参照する PP はない。

（　最終ページ　）