文書管理番号	Symfo-02-DS0001

SymfoWARE セキュリティターゲット

第 2. 1 版

発行日:2003 年 08 月 20 日

富士通株式会社

保管期間	次期改版時

全ページ数	103 ﾍﾟｰｼﾞ

更新履歴表（１／１）

文書名 ： SymfoWARE セキュリティターゲット				文書管理番号: Symfo-02-DS0001	
版数	更新日	更新個所	更新内容(概要)	更新者	承認者
1.0	2002.3.20	全体	新規作成	安永	仲沢 K
1.1	2002.6.21	全体	ハードウェアや資源を明確にするなど	佐藤	仲沢 K
1.2	2002.7.4	全体	前提条件の記載内容など	佐藤	仲沢 K
1.3	2002.7.18	全体	管理者と利用者の位置付けの明確化など	佐藤	仲沢 K
1.4	2002.7.29	全体	T.SERVICE を識別するなど	佐藤	仲沢 K
1.5	2002.8.6	全体	ＯＳの認証識別機能を利用する場合の条件を追加など	佐藤	仲沢 K
1.6	2002.8.28	8 章	環境の対策方針の技術的なサポートに関する論証を追加など	佐藤	仲沢 K
1.7	2002.9.4	8 章	機能要件と仕様概要の対応関係を明確化など	佐藤	仲沢 K
1.8	2002.9.11	全体	分かりにくい説明を明確化 機能要件を整理	佐藤	仲沢 K
1.9	2002.10.9	6 章 1 章 5 章 8 章	保証手段の最新化 FMT_SMF の対応(参照資料) FMT_SMF の対応(日本語化) SOF-medium の一貫性について追加	佐藤	仲沢 K
1.10	2002.10.16	6 章	保証手段の最新化	佐藤	仲沢 K
1.11	2002.10.24	まえがき 全体	Solaris 商標について 分かりにくい説明を明確化	佐藤	仲沢 K
1.12	2002.11.14	全体	対策方針の範囲を明確化など	佐藤	仲沢 K
1.13	2002.12.9	全体	各種論証を正確に修正など	佐藤	仲沢 K
1.14	2002.12.13	全体	機能要件の使用方法の誤解を修正	佐藤	仲沢 K
1.15	2002.12.16	全体	資源保護の対策方針 OE.ENV(環境の対策方針)を TOE の対策方針に変更	佐藤	仲沢 K
1.16	2003.05.08	全体	NITE からの指摘に対応(複数箇所)	佐藤	仲沢 K
1.17	2003.06.10	全体	NITE からの指摘に対応(複数箇所)	佐藤	仲沢 K
2.0	2003.07.22	全体	NITE からの指摘に対応(複数箇所)	佐藤	仲沢 K
2.1	2003.08.20	2 章	TOE のソフトウェア構成と TOE 範囲を明確化	佐藤	仲沢 K

まえがき

本書の目的

本書は，ＩＳＯ／ＩＥＣ１５４０８に基づいたSymfoWARE Server Enterprise Extended Edition 4.0のセキュリティターゲットである。

本書の構成

本書は，以下のように構成している.

１章　ＳＴ概説：本セキュリティターゲットについて概説している。

２章　ＴＯＥ記述：製品についての概説を記述している。

３章　ＴＯＥセキュリティ環境：製品が使われると想定する環境のセキュリティの側面について記述している。

４章　セキュリティ対策方針：ＴＯＥおよびその環境に対するセキュリティ対策方針について記述している。

５章　ＩＴセキュリティ要件：ＴＯＥまたはその環境が満たすＩＴセキュリティ要件を詳細に定義している。

６章　ＴＯＥ要約仕様：ＴＯＥに対するセキュリティ要件を具体的に定義している。

７章　ＰＰ主張：ＰＰの準拠性について記述している。

８章　根拠：ＴＯＥセキュリティ環境において識別されたすべての側面を追跡することができ、かつそれらをカバーするのに適していることを実証している。

商標

目　次（１／２）

目　次（２／２）

表目次

図目次

１　ＳＴ概説

セキュリティターゲットの概観を述べている。

１．１　ＳＴ識別

本資料「SymfoWARE セキュリティターゲット 第 2.1 版　富士通株式会社」は、以下のＴＯＥを対象とするセキュリティターゲットである。

TOE名:　SymfoWARE Server Enterprise Extended Edition 4.0
製作者:　富士通株式会社
版番号:　EEE4.0

１．２　ＳＴ概要

本セキュリティターゲットは、富士通株式会社のSymfoWARE Server Enterprise Extended Edition 4.0（以後、ＳｙｍｆｏＷＡＲＥ）が提供する、リレーショナルデータベース機能について記述している。

評価の対象は、以下の７つの機能を持つパッケージから構成される範囲である。

（カッコ内はパッケージ名を表す）

- RDBセキュリティ機能
  （FJSVrdbse）
- SymfoWARE基本パッケージ
  （FJSVsymex）
- 標準コード変換機能
  （FSUNiconv）
- RDB機能
  （FSUNrdb2b）
- RDB機能のC言語プレコンパイル機能
  （FSUNrdbcc）
- RDB機能のCOBOLプレコンパイル機能
  （FSUNrdbco）
- 並列クエリ機能
  （FSUNrdbps）

１．３　ＣＣ適合

本ＴＯＥのＣＣ適合は以下のとおりである。

－　機能要件:ISO/IEC 15408 Part 2 拡張
－　保証要件:ISO/IEC 15408 Part 3 適合
－　評価保証レベル　ＥＡＬ４　適合

１．４　参照資料

Part1: Introduction and general model First edition 1999-12-01 ISO/IEC 15408-1

Part2: Security functional requirements First edition 1999-12-01 ISO/IEC 15408-2

Part3: Security assurance requirements First edition 1999-12-01 ISO/IEC 15408-3

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、1999 年8 月、バージョン2.1、CCIMB-99-031

パート2 ： セキュリティ機能要件、1999 年8 月、バージョン2.1、CCIMB-99-032

パート3 ： セキュリティ保証要件、1999 年8 月、バージョン2.1、CCIMB-99-033

いずれも平成12 年8 月翻訳第1.1 版　　情報処理振興事業協会セキュリティセンター

補足文書

CCIMB Interpretations-0210

補足- 0210

２　ＴＯＥ記述

本ＴＯＥの概要、運用環境、機能概要について説明する。

２．１　ＴＯＥの概要

本ＴＯＥは商用向けのリレーショナルなデータベースである。ユーザ業務で発生する大量のデータを迅速に処理し、目的に応じて多面的に利用できるデータベースを提供する。ＳＱＬ言語を用いて、データの構造を定義し、構造化されたデータへアクセスすることができる。

２．２　ＴＯＥの利用

本ＴＯＥの関係者と利用方法について説明する。

２．２．１　ＴＯＥの関係者

データベースを利用する人には業務用のデータ処理を目的に本ＴＯＥを使用する一般利用者（以後、利用者）と、ＴＯＥの運用や管理業務を行う運用管理者（以後、管理者）が存在する。

２．２．１．１　利用者

利用者は、業務アプリを使ってデータベースにアクセスする。

利用者がＴＯＥを利用するためには、ＴＯＥの利用を許可されている必要がある。ＴＯＥへの利用許可は、管理者がＴＯＥに利用者識別情報を登録することにより行われる。

ＴＯＥに利用者識別情報を登録する際には、ＴＯＥの動作の基になるオペレーティングシステム（以下ＯＳと記載する）の利用者識別情報を登録する場合と、ＴＯＥ専用の利用者識別情報を登録する場合の２種類がある（以下、特に断らない限り、上記２種類のいずれかの方法で登録された者を利用者と呼ぶ)。

ＴＯＥ専用に利用者識別情報が登録された者をデータベース専用利用者と呼び、ＴＯＥに利用者識別情報が登録されておらず、ＯＳのみに登録された者をＯＳ専用利用者と呼ぶ。

２．２．１．２　管理者

管理者は、利用者の登録やＴＯＥの動作に必要な条件設定などの管理業務を実施し、本ＴＯＥを使ったシステムの運用環境を管理する（ＯＳ，データベース，アクセス状況などを監視し、バックアップ／リカバリなどを行う)。

なお、管理者は、利用者が行える作業は全て行える。

管理者は、ＯＳの管理者でもある（以下、特に断らない限り、管理者とはＴＯＥとＯＳの両方の管理者である)。

２．２．１．３　責任者

責任者は、セキュリティシステムの全責任を担う責任者を指す。責任者は、ふさわしい管理者の選任、管理者の教育等を行う必要がある。

２．２．２　利用方法

ＴＯＥの機能を利用するには、「ＯＳにログインし、自システムでコマンドまたはアプリケーションを通じて利用する方法」「ＲＤＢ２＿ＴＣＰ連携機能を利用する方法」「ＸＡ連携機能を利用する方法」の３つの方法がある。ＯＳにログインして利用する方法を採る場合、管理者はローカルログインおよびネットワークを経由してログインすることが可能であり、利用者はネットワークを経由してログインすることが可能である。

上記のとおり管理者および利用者はＴＯＥの機能を、以下の方法で利用できる。

－自システムでのコマンドの実行またはアプリケーションからのＳＱＬ言語アクセス

- 管理者がＯＳにログインし、コマンドを実行する
- 管理者または利用者がＯＳにログインし、アプリケーションを実行する

　ＯＳおよびＴＯＥに登録された利用者は、ＯＳにログインした利用者識別情報をそのまま使用してアプリケーションを実行することができる。

　ＯＳに登録された利用者は、ＯＳにログインした利用者識別情報とは別のＴＯＥに登録された利用者識別情報を使用してアプリケーションを実行することもできる。これにより、ＯＳ専用利用者としてＯＳにログインし、アプリケーションの実行時にＴＯＥに登録された利用者識別情報を指定することでデータベース専用利用者に代わってＴＯＥを利用するなどの使い方ができる。

－ＲＤＢ２＿ＴＣＰ連携機能を利用したアプリケーションからのＳＱＬ言語アクセス

- 管理者または利用者がＲＤＢ２＿ＴＣＰ連携機能を利用してアプリケーションを実行する

－ＸＡ連携製品からのＳＱＬ言語アクセス

- 管理者または利用者がＸＡ連携機能を利用してＸＡ連携製品と連携する

２．３　ＴＯＥの構成

ＴＯＥのハードウェア／ソフトウェア構成について説明する。

２．３．１　ＴＯＥのハードウェア

２．３．１．１　ハードウェア環境

ＴＯＥが正常に動作するハードウェアの環境は以下のとおりである。

－プロセッサ

400MHz 以上（2CPU 以上）

－メモリ

1GB 以上

－ハードディスク

1GB 以上

※ハードウェアはＴＯＥの範囲外である。

２．３．１．２　ハードウェア構成

ＴＯＥはソフトウェア製品であるため、ハードウェア構成は存在しない。

２．３．２　ＴＯＥのソフトウェア

２．３．２．１　ソフトウェア環境

本ＴＯＥは、以下のパッチを適用したSolaris™ 7 Operating Environment（日本版）上で動作する。

・106541-08

・107544-03

ＴＯＥは、本ＯＳと連携して、セキュリティ機能を提供する。

※ＯＳはＴＯＥの範囲外である。

２．３．２．２　ソフトウェア構成

SymfoWAREを構成するプログラムの単位をパッケージと呼ぶ。SymfoWAREは下表に示すパッケージから構成されており、この中の太枠線で囲まれた部分がＴＯＥの範囲である。ただし、SymfoWARE基本パッケージの中に含まれているRDB2_TCP連携機能に関係する「jypvbrp.c」「jypvbsp.c」のモジュール、及びXA連携機能に関係する「jypvpxop.c」「jypvpxcl.c」「jypvpxst.c」「jypvpxed.c」「jypvpxtr.c」のモジュールは、TOEの物理的範囲から除外するものとする。

表２．１　SymfoWAREのソフトウェア構成

項番	パッケージ名	バージョン	機能
1	FJSVrdbse	V34L11	RDBセキュリティ機能
2	FJSVsymex	4.0	SymfoWARE基本パッケージ
3	FJSVsymhs	4.0	スタンバイ／ホットスタンバイ共通機能
4	FJSVsymwd	V11L10	Webベースデータベースツール
5	FSUNbgath	V24L23	認証機能
6	FSUNbgenv	V24L20	認証機能
7	FSUNdbag	V30L12	RDBオブジェクトマネージャ機能
8	FSUNhscnv	2.0.1	高速コード変換機能
9	FSUNiconv	1.1	標準コード変換機能
10	FSUNlnkex	0.9.3	Linkexpress機能
11	FSUNlnkre	2.0	レプリケーション機能
12	FSUNrdasv	V20L17	RDA機能
13	FSUNrdb2b	V34L11	RDB機能
14	FSUNrdbcc	V34L11	RDB機能のC言語プレコンパイル機能
15	FSUNrdbco	V34L11	RDB機能のCOBOLプレコンパイル機能
16	FSUNrdbps	V34L11	並列クエリ機能
17	FSUNsymdm	3.1.1	データベースマネージャ機能

図２．１にＴＯＥの実行イメージを示す。

利用者および管理者は、アプリケーションまたはコマンドの実行を通してＴＯＥに接続する。

アプリケーションからＴＯＥに接続する場合は、アプリケーション中のＳＱＬ文に、接続しようとする利用者の識別情報を指定して実行する。なお、コマンドの場合は識別情報の指定などは必要ない。

利用者の識別情報を指定して実行したアプリケーションのプロセスを利用者のプロセスと呼ぶ。また、管理者の識別情報を指定して実行したアプリケーションのプロセス、管理者が実行したコマンドのプロセスを管理者のプロセスと呼ぶ。

ファイルに格納されているデータに対するアクセスは、アプリケーションのプロセス（利用者のプロセスまたは管理者のプロセス）およびコマンドのプロセス（管理者のプロセス）とは別の、専用のプロセスで行う。この専用のプロセスをサーバプロセスと呼ぶ。サーバプロセスはＴＯＥ全体で一つであり、マルチスレッド動作することで、コマンドやアプリケーションの処理を複数同時に実行している。

アプリケーションのプロセス（利用者のプロセスまたは管理者のプロセス）やコマンドのプロセス（管理者のプロセス）とサーバプロセスとの間の情報の受け渡しはプロセス間共用メモリを使用して行われる。サーバプロセスは、ファイルへの物理的なアクセスは管理者権限で行うが、利用者データへの論理的なアクセスを行う場合には、アプリケーション中のＳＱＬ文に指定された、接続しようとしている利用者の識別情報（利用者または管理者）に関連付けられるアクセス権限や、コマンドの実行者の識別情報（管理者）に関連付けられるアクセス権限に従って利用者データへのアクセスを行う。

プロセスを分離している理由は、プリケーションにおける論理ミスから、資源ファイルに格納されているデータを保護するためである。

ＴＯＥがＯＳから獲得する資源(プロセス、共用メモリおよびファイル)の保護はＯＳが行う。

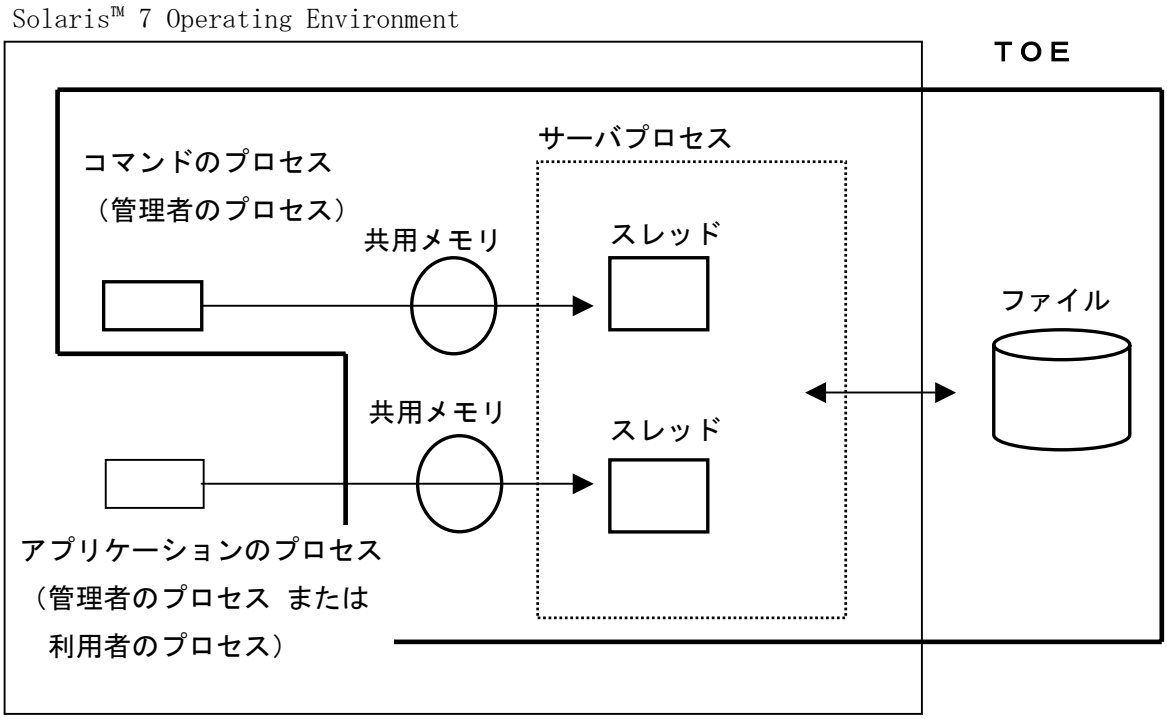

図２．１　ＴＯＥのプロセス実行イメージ

２．４　ＴＯＥの機能

ＴＯＥの機能について説明する。

２．４．１　機能構成

管理者がＴＯＥをインストールするときには、標準運用と標準セキュリティ運用を選択することができる。ＴＯＥの機能を利用するためには、インストール時に必ず標準セキュリティ運用を選択した上で、以下の７つのパッケージをインストールする必要がある。

- RDBセキュリティ機能（FJSVrdbse）
- SymfoWARE基本パッケージ（FJSVsymex）
- 標準コード変換機能（FSUNiconv）
- RDB機能（FSUNrdb2b）
- RDB機能のC言語プレコンパイル機能（FSUNrdbcc）
- RDB機能のCOBOLプレコンパイル機能（FSUNrdbco）
- 並列クエリ機能（FSUNrdbps）

ＴＯＥは上記のパッケージ群から構成され、これらのパッケージのうち「ＲＤＢセキュリティ機能(FJSVrdbse)」がＴＯＥの様々なセキュリティ機能を実現している。

図２．２に示すように、ＳｙｍｆｏＷＡＲＥと連携する機能には、ＴＣＰ／ＩＰを使用して他システムのアプリケーションと連携するＲＤＢ２__ＴＣＰ連携機能、共用メモリを使用してＸＡ連携製品と連携するＸＡ連携機能、共用メモリを使用して自システムのアプリケーションやコマンドと連携するプロセス間通信機能がある。

このうち、ＲＤＢ２__ＴＣＰ連携機能とＸＡ連携機能は特殊なインタフェースであり、ＴＯＥの対象外とする。

プロセス間通信機能では、共用メモリを使用して、アプリケーションのプロセス（利用者のプロセスまたは管理者のプロセス）およびコマンドのプロセス（管理者のプロセス）とサーバプロセスとの間での通信制御が行われる。

セションを制御する機能では、アプリケーションのプロセス（利用者のプロセスまたは管理者のプロセス）およびコマンドのプロセス（管理者のプロセス）とサーバプロセスとの結合／結合解除が行われる。

データへアクセスする機能では、サーバプロセスによるデータベースの参照、更新等が行われる。

データを保守する機能では、サーバプロセスによるデータベースの構造定義、バックアップ等が行われる。

セキュリティ機能では、各機能を安全に使用するための利用者制御、資源制御等が行われる。

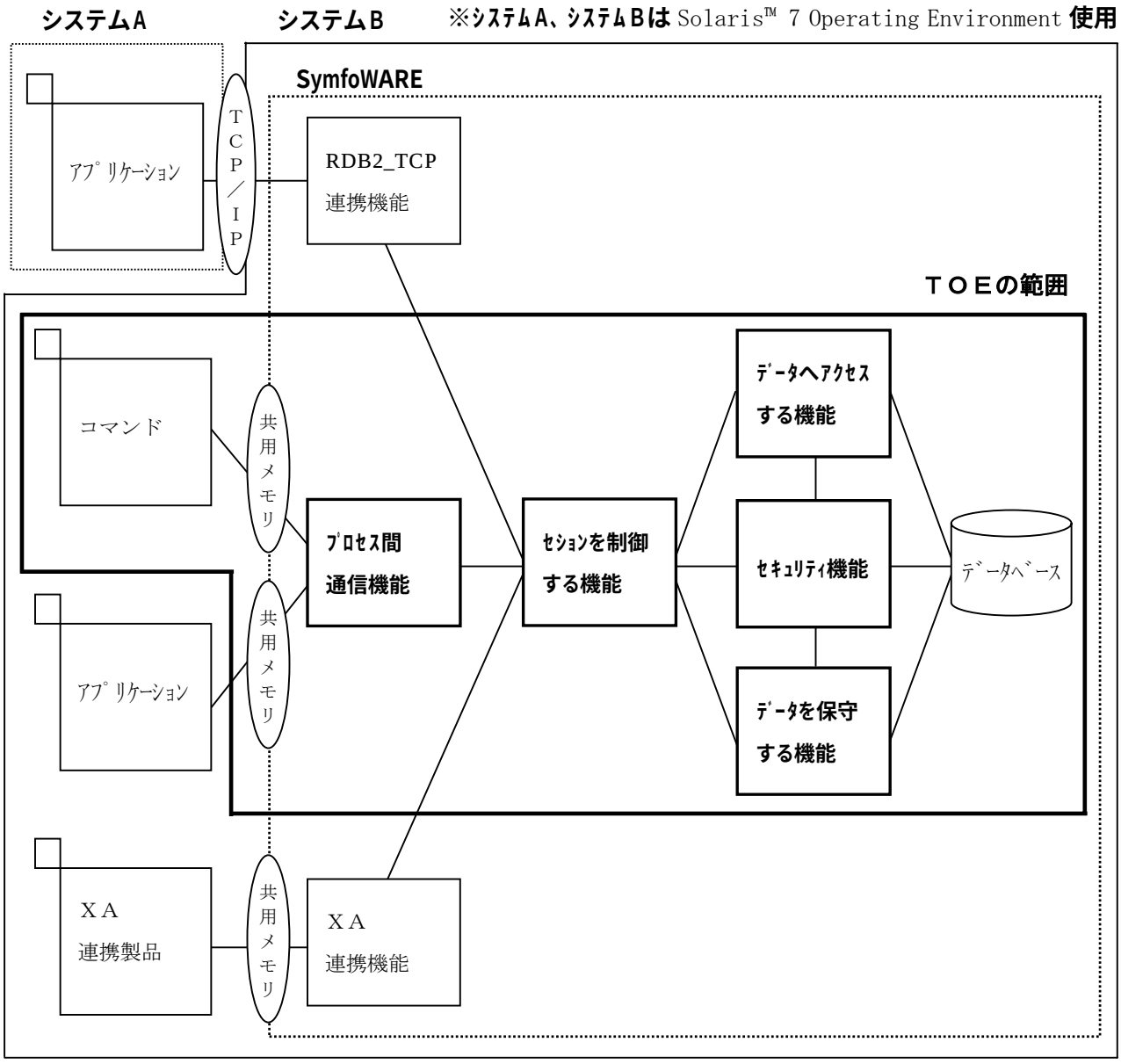

図２．２　機能構成

２．４．２　機能概要

本ＴＯＥの機能は以下の五つの機能で実現している。

- プロセス間通信機能
- セションを制御する機能
- データへアクセスする機能
- データを保守する機能
- セキュリティ機能

プロセス間通信機能は、共用メモリを使用してプロセス間の通信制御を行う機能である。

セションを制御する機能は、アプリケーションのプロセスとサーバプロセスを結合、および、結合解除する機能である。

- 結合
- 結合解除

データへアクセスする機能は、以下のものである。これらの機能は、利用者がＳＱＬ文をアプリケーションに埋め込んで実行することにより実現する。

- データの挿入
- データの更新
- データの削除
- データの参照
- プロシジャの実行

データを保守する機能は、以下のものである。これらの機能は、利用者がＳＱＬ文をアプリケーションに埋め込んで実行する、またはコマンドを実行することで実現する。

- データベースの構造定義
- データのロード
- データのアンロード
- データのバックアップ
- データのリカバリ

セキュリティ機能は、セションを制御する機能、データへアクセスする機能、データを保守する機能の各機能を安全に使用するため以下の機能を提供している。

- 運用選択機能

  セキュリティ機能の全体のふるまいを変更する機能

- 利用者制御機能

  各利用者の権限を制御し、指定された権限の範囲での処理を保証し、またその範囲を超えた処理を制限する機能である。

- 資源制御機能

  資源制御機能はＴＯＥが使用する資源を制御する機能である。

- 監査ログ機能

  監査ログ機能は、利用者や管理者の処理の情報を記録する。

２．５　ＴＯＥ保護資産

保護の対象は、利用者のデータおよびデータの構造定義情報である。

利用者のデータおよびデータの構造定義情報を合わせてデータベースデータと呼ぶ。

なお、データベースデータへのアクセスの際には、利用者および管理者の処理記録を取得し、監査ログデータとして格納する。監査ログデータもセキュリティ上重要なデータであるため、データベースデータと同様に保護対象とする。図２．３に具体的なＴＯＥ保護資産を示す。

上記データを保護するため、以下の三つのファイルを保護対象とする。これらのファイルは、アプリケーション（ＳＱＬ文）およびコマンドによるアクセスが可能である。

－ データベーススペース

利用者のデータが表の形式で格納されているファイル。

データベーススペースには、論理的なアクセスの単位である表が格納されており、利用者のデータは、この表に格納される。表は管理者が定義する。

利用者データへのアクセスを目的とするアプリケーションが実行された場合、サーバプロセスは表単位に論理的なアクセスを行う。また、コマンドが実行された場合、利用者データへのアクセスが目的のコマンドであれば、サーバプロセスが表単位に論理的なアクセスを行い、データベーススペースをファイルとしてアクセスするのが目的のコマンドであれば、表を意識せず物理的なアクセスを行う。

－ ディクショナリ

データの構造定義情報、識別認証情報、権限情報、セキュリティパラメタやプロシジャが表の形式で格納されているファイル。表はデフォルトで定義済みである。

データの構造定義情報は、データベースの定義を行う際に格納され、データベースへのアクセスの際に参照される。プロシジャとは利用者がサーバプロセスで実行するよう定義・登録した処理のリストである。プロシジャには、表に対する挿入、更新、削除、参照等の処理が含まれる。

プロシジャ実行の SQL 文が埋め込まれたアプリケーションが実行された場合、サーバプロセスは、ディクショナリからプロシジャを１つの論理的な単位として読み出し、実行する。

ディクショナリ中のデータへのアクセスを目的とするアプリケーションが実行された場合、サーバプロセスは表単位に論理的なアクセスを行う。また、コマンドが実行された場合、ディクショナリ中のデータが目的のコマンドであれば、サーバプロセスが表単位に論理的なアクセスを行い、ディクショナリをファイルとしてアクセスするのが目的のコマンドであれば、表を意識せず物理的なアクセスを行う。

－ 監査ログファイル

監査ログデータが格納されているファイル。データベースデータへのアクセスの際に利用者および管理者の処理記録として格納される。なお、監査ログファイルはデータベースの形式で管理されている。

また、上記ファイルに格納されたデータは、一時的に以下のファイルにも格納されるため、保護対象とする。これらのファイルは、アプリケーション（ＳＱＬ文）によるアクセスは不可能であるが、コマンドによるアクセスは可能である。

－ ログファイル

データベーススペース、ディクショナリ、監査ログファイルの整合性を保証するための更新ログが格納されているファイル。利用者のバックアップデータが格納されているため、保護対象とする。

－ 作業用ファイル

データベーススペース、ディクショナリ、監査ログファイルにアクセスした時点で、処理途中の

整列結果等が一時的に格納されているファイル。利用者のデータ処理途中に生成される中間データが格納されているため、保護対象とする。

なお、以下のファイルも、アプリケーションの実行時の動作を定義し、このファイルを元にアプリケーションはデータベースデータにアクセスするため、保護対象とする。このファイルは、アプリケーション（ＳＱＬ文）によるアクセスは不可能であるが、コマンドによるアクセスは可能である。

－ 動作環境ファイル

アプリケーションが動作するために必要な環境の定義が格納されている。

以後、データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル、動作環境ファイルに含まれるデータをまとめて「保護資産」と呼ぶ。また、コマンドのプロセス、コマンドのプロセスに対応する共用メモリ、コマンドのプロセスに対応するサーバプロセスのスレッド、アプリケーションのプロセス、アプリケーションのプロセスに対応する共用メモリ、アプリケーションのプロセスに対応するサーバプロセスのスレッドをまとめて「実行資源」と呼ぶ。

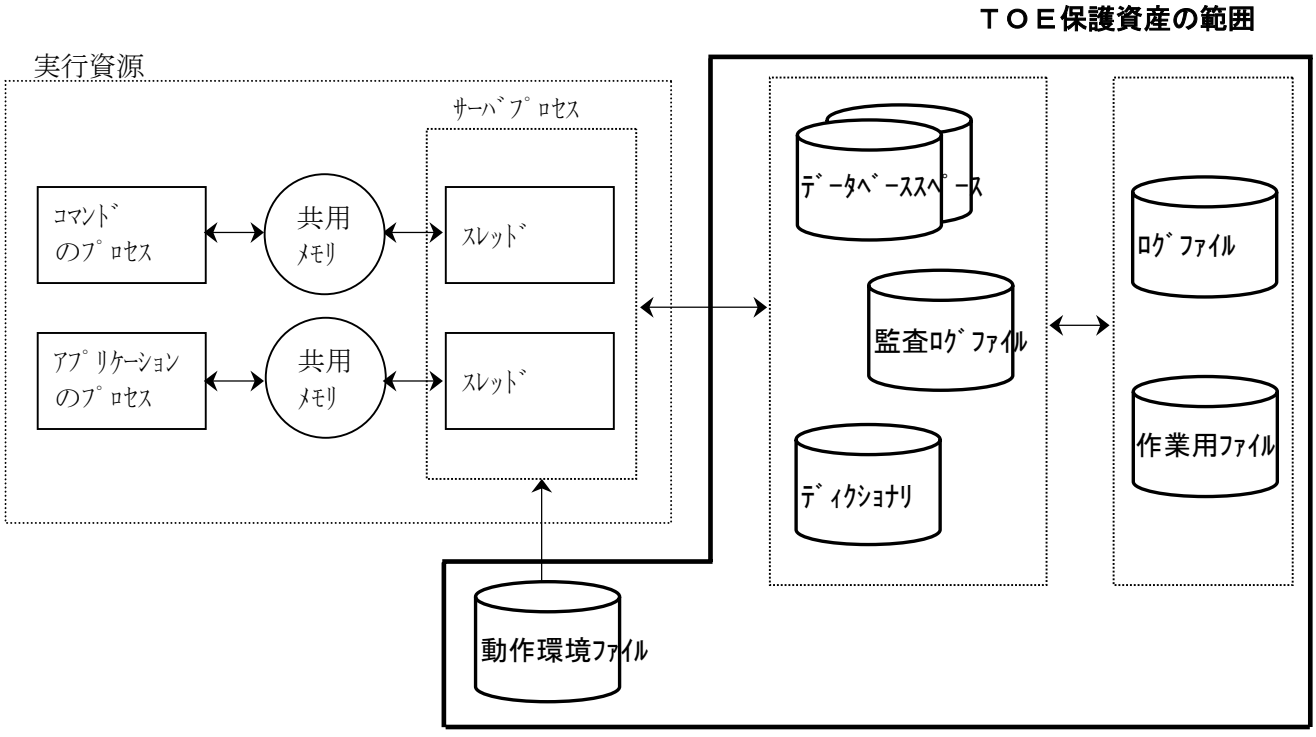

図２．３　ＴＯＥ保護資産

３　ＴＯＥセキュリティ環境

本ＴＯＥに対するセキュリティ環境について述べる。

３．１　前提条件

ＴＯＥは、以下のような使用環境を想定している。

Ａ．ＭＡＮＡＧＥＲ　管理者の正当性

管理者は、不正を行わない。

Ａ．ＵＳＥＲ　利用者による管理

利用者は、利用者自身が使用するパスワードやアプリケーションを安全に管理する。

Ａ．ＰＨＹＳＩＣＡＬ　物理的な保護

ＴＯＥの動作に関連する機器、機器を設置する部屋および建物が物理的に保護されており、管理者以外は、機器に対し物理的なアクセスを行うことはできない。

３．２　脅威

ＴＯＥに対して以下のような脅威を想定している。

Ｔ．ＴＣＰ　ＲＤＢ２＿ＴＣＰ連携機能を使用したデータベースへの結合

利用者またはＴＯＥへの結合を許可されていない者が、ＲＤＢ２＿ＴＣＰ連携機能を利用して、データベーススペース、ディクショナリ、監査ログファイルを参照、改ざんする。

Ｔ．ＸＡ　ＸＡ連携機能を使用したデータベースへの結合

利用者またはＴＯＥへの結合を許可されていない者が、ＸＡ連携機能を利用して、データベーススペース、ディクショナリ、監査ログファイルを参照、改ざんする。

Ｔ．ＡＣＣＥＳＳ　アプリケーション、コマンドを使用したデータベースへの結合

利用者またはＴＯＥへの結合を許可されていない者が、ＴＯＥの機能を使用して、保護資産への許可されていない操作を行う。この許可されていない操作には、管理者のみが実行可能な操作も含まれる。

Ｔ．ＲＥＳＯＵＲＣＥ　資源の枯渇

利用者がＴＯＥを利用する不当なアプリケーションを実行することで、ＴＯＥが動作するために必要な資源（データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル、動作環境ファイルおよび実行資源）が枯渇し、管理者や利用者のＴＯＥに対する正当な処理ができなくなる（たとえば、使用可能なセションがすべて占有されて、管理者が監査ログ情報を参照できなくなる）。

Ｔ．ＯＳ　オペレーティングシステムの機能を用いた攻撃

ＴＯＥがＯＳから獲得して使用しているデータベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル、動作環境ファイルに対し、ネットワーク経由でＯＳの機能を使用して直接アクセスすることによって、利用者またはＴＯＥへの結合を許可されていない者が、保護資産への許可されていない操作を試みる。

Ｔ．ＤＡＴＡ　使用済みの資源からの情報の取得

ＴＯＥがＯＳから獲得した後、使用済みとなり、ＯＳへ返却したデータベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル、動作環境ファイルに残存する情報を、利用者またはＴＯＥへの結合を許可されていない者が参照する。

３．３　組織のセキュリティ方針

組織のセキュリティポリシーはない。

４　セキュリティ対策方針

ＴＯＥのセキュリティ対策方針と、環境のセキュリティ対策方針について述べる。

４．１　ＴＯＥのセキュリティ対策方針

ＴＯＥのセキュリティ対策方針について述べる。

Ｏ．ＣＯＮＮＥＣＴ　識別と認証

ＴＯＥは、ＴＯＥへの結合を許可された利用者を管理し、ＯＳによって識別認証された利用者がＴＯＥへの結合を要求した場合は識別のみを行い、ＯＳによって識別認証されていない利用者がＴＯＥへの結合を要求した場合は、識別および認証を行うことによって、結合を許可されていない者の結合を制限する。

Ｏ．ＡＣＣＥＳＳ　アクセス制御

ＴＯＥは、ＴＯＥへの結合を許可された各利用者の操作および許可された保護資産への操作を管理し、利用者の許可されていない操作、あるいは、許可されていない保護資産への操作を制限する。この許可されていない操作には、管理者のみが実行可能な操作も含まれる。

Ｏ．ＲＥＳＯＵＲＣＥ　資源の制限

ＴＯＥは、ＴＯＥへの結合を許可された各利用者が使用可能な資源（データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルおよび実行資源）の量を管理し、これを超える資源の獲得を制限する。

Ｏ．ＡＴＴＲ　資源のアクセス権限設定

ＴＯＥは、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルのアクセスを正当なアクセス権限をもったものだけに限定する。

Ｏ．ＩＮＩＴ　使用済みの資源の初期化

ＴＯＥは、ＯＳから獲得し使用済みになった、データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルに残存する情報を、初期化した後に、ＯＳへ返却する。

Ｏ．ＡＵＤＩＴ　監査

ＴＯＥは、ＴＯＥへの結合の要求、保護資産への操作に関する記録をとる。この操作には、管理者のみが実行可能な操作も含まれる。また、監査ログの初期化、削除、取得情報の改変、閲覧は管理者しか行えないように制御する。

４．２　環境の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述べる。

ＯＥ．ＣＯＮＮＥＣＴ　識別と認証

ＯＳは、ＯＳへの結合を許可された利用者を管理し、ＴＯＥへ結合するためにＯＳへの結合を要求している利用者に対して、識別および認証を実施し、結合を許可されていない者の結合を制限する。

ＯＥ．ＡＳＳＩＧＮ　管理者の選任と管理

責任者は、セキュリティシステムの全責任を担う者であり、ＴＯＥの管理、および、ＴＯＥが想定するセキュアな環境の管理にふさわしい人間を、管理者として複数人選任し、教育や管理を実施しなければならない。

ＯＥ．ＵＳＥＲ　管理者による利用者の教育

管理者は、利用者に対し、パスワードやアプリケーションを適切に管理するように教育しなければならない。

ＯＥ．ＰＨＹＳＩＣＡＬ　管理者による物理的環境の管理

管理者は、ＴＯＥの動作に関連する機器が管理者以外に利用されないように管理しなければならない。

ＯＥ．ＥＮＶ　管理者による環境の管理

管理者は、監査ログを参照することで、他の管理者が操作を不当に行っていないかチェックしなければならない。また、バックアップリカバリ運用や、動作環境ファイルの管理（アクセス管理、初期化）、ＴＯＥのパラメタ管理、ＯＳにログインする利用者の管理、利用者が使用可能なプロセス数の管理など、ＴＯＥの正当な動作を維持するための適切な環境の管理を実施しなければならない。

さらに管理者は、ＸＡ連携を不可能にする設定を行い、ＴＯＥの運用中にＸＡ連携機能の利用が可能にならないよう維持、監視しなければならない。

ＯＥ．ＯＳ　ＯＳを利用した環境の管理

ＯＳは管理者による適切な管理の元で、ＲＤＢ２＿ＴＣＰ連携機能による結合拒否、利用者が使用可能なＯＳ資源の管理、データベーススペースに対する管理者のみアクセス可能なアクセス制御などを行う。

５　ＩＴセキュリティ要件

ＴＯＥのセキュリティ要件およびＩＴ環境に対するセキュリティ要件について述べる。

５．１　ＴＯＥセキュリティ要件

ＴＯＥのセキュリティ要件について述べる。

５．１．１　ＴＯＥセキュリティ機能要件

セキュリティ機能要件について述べる。

セキュリティ機能要件の一覧を表５．２に示す。

５．１．１．１　認証と識別

１）認証失敗(FIA_AFL)

管理: 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

b) 認証失敗の事象においてとられるアクションの管理

監査: FIA_AFL.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下のアクションを監査対象にすべきである:

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)。

FIA_AFL.1 認証失敗時の取り扱い

FIA_AFL.1.1

TSFは、[割付: *認証事象のリスト*]に関して、[割付: *回数*]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] *回数*

管理者が運用に応じて設定する値。省略値=6。範囲=1～11。

[割付] *認証事象のリスト*

アプリケーションからの結合依頼

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*

－ 対象の利用者をＴＯＥに対して結合できない状態に変更
（管理者のみに、対象の利用者をＴＯＥに対して結合できる状態へ復旧することを許可）

２）利用者属性定義(FIA_ATD)

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。

監査: FIA_ATD.1

FAU_GENセキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FIA_ATD.1 利用者属性定義

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*

－ 資源属性
－ 操作属性
－ 資源量属性

３）秘密についての仕様(FIA_SOS)

管理: 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。

監査: FIA_SOS.1

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;

FIA_SOS.1 秘密の検証

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*

－ パスワードが従う品質基準は以下のとおり

- 以下の文字で構成される文字列定数で指定
  ・英字
  ・数字
  ・以下の特殊文字
  , ( ) . : ; = * + - / ? < > % _ ’ ”
  ・以下の拡張文字
  @ ¥ #
- セキュリティパラメタで指定されるパスワードの最低長以上で、８文字以内の文字列でなければならない。
- 最低でも２文字以上の英字を含んでいなければならない。
- １文字以上の数字または特殊文字、拡張文字を含んでいなければならない。
- 大文字と小文字は同一文字として利用者名と比較した場合、同じものや、ずらしたもの、反転したものであってはならない。
- 大文字と小文字は同一文字として現在使用しているパスワードと比較した場合、３文字以上違うものでなければならない。

４）利用者認証(FIA_UAU)

管理: FIA_UAU.2(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。
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。

監査: FIA_UAU.2(1)

基本: 認証メカニズムのすべての使用。

FIA_UAU.2(1) アクション前の利用者認証

FIA_UAU.2.1(1)

TSFは、OSによって識別認証されていない利用者がTOEへの結合を要求した場合は、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**自分自身を認証**することを要求しなければならない。
※ 下線部は詳細化。

５）利用者識別(FIA_UID)

管理: FIA_UID.2(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) 利用者識別情報の管理。

監査: FIA_UID.2(1)

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。

FIA_UID.2(1) アクション前の利用者識別

FIA_UID.2.1(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。

６）利用者・サブジェクト結合(FIA_USB)

管理: 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。

監査: FIA_USB.1

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及び失敗)。

FIA_USB.1 利用者･サブジェクト結合

FIA_USB.1.1

TSFは、適切な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。

７）ＴＯＥ結合履歴(FTA_TCH)

管理: FTA_TCH.1

予見させる管理アクティビティはない。

監査: FTA_TCH.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FTA_TCH.1 TOE結合履歴

FTA_TCH.1.1

セション確立の成功時、TSFは、その利用者に対する最後の成功したセション確立の[選択: *日付*、*時刻*]を表示しなければならない。

[選択] *日付*、*時刻*

日付、時刻

FTA_TCH.1.2

TSFは、利用者に情報をレビューする機会を与えることなく利用者インタフェースからアクセス履歴情報を消去してはならない。

５．１．１．２　アクセス制御

１）アクセス制御方針(FDP_ACC)

管理: FDP_ACC.1(1)

このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_ACC.1(1)

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない。

FDP_ACC.1(1) サブセットアクセス制御

FDP_ACC.1.1(1)

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

[割付] *アクセス制御 **SFP***

- アクセス制御 SFP_DBM

[割付] *サブジェクト*

- サーバプロセス

[割付] *オブジェクト*

- 表
- プロシジャ

[割付] ***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*

- 表に対するデータの参照
- 表に対するデータの挿入
- 表に対するデータの更新
- 表に対するデータの削除
- プロシジャの実行

管理: FDP_ACC.1(2)

このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_ACC.1(2)

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない。

FDP_ACC.1(2) サブセットアクセス制御

FDP_ACC.1.1(2)

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

[割付] *アクセス制御 **SFP***

- アクセス制御 SFP_DBU

[割付] *サブジェクト*

- サーバプロセス

[割付] *オブジェクト*

- 表
- プロシジャ

[割付] ***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*

- 表に対するデータの参照
- 表に対するデータの挿入
- 表に対するデータの更新
- 表に対するデータの削除
- プロシジャの実行

２）アクセス制御機能(FDP_ACF)

管理: FDP_ACF.1(1)

以下のアクションはFMTの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。

監査: FDP_ACF.1(1)

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。

FDP_ACF.1(1) セキュリティ属性によるアクセス制御

FDP_ACF.1.1(1)

TSFは、[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]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] *アクセス制御**SFP***

－ アクセス制御 SFP_DBM

[割付] *セキュリティ属性*

－ 利用者属性

－ 資源属性

－ 操作属性

[割付] *名前付けされたセキュリティ属性のグループ*

－ 管理者権限リスト（TSF により、管理者がアクセス可能な資源に対して行える操作が定義されたもの）

FDP_ACF.1.2(1)

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

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

－ サーバプロセスが表やプロシジャを操作する際、管理者権限リストに登録されていれば許可する

FDP_ACF.1.3(1)

TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。

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

なし

FDP_ACF.1.4(1)

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

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

なし

管理: FDP_ACF.1(2)

以下のアクションはFMTの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。

監査: FDP_ACF.1(2)

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。

FDP_ACF.1(2) セキュリティ属性によるアクセス制御

FDP_ACF.1.1(2)

TSFは、[割付: *セキュリティ属性、名前付けされたセキュリティ属性のグループ*]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] *アクセス制御**SFP***

- アクセス制御 SFP_DBU

[割付] *セキュリティ属性*

- 利用者属性
- 資源属性
- 操作属性

[割付] *名前付けされたセキュリティ属性のグループ*

- 権限リスト（管理者により、利用者がアクセス可能な資源に対して行える操作が定義されたもの）

FDP_ACF.1.2(2)

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

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

- サーバプロセスが表やプロシジャを操作する際、権限リストに登録されていれば許可する

FDP_ACF.1.3(2)

TSFは、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない: [割付: *セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に承認する規則*]。

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

なし

FDP_ACF.1.4(2)

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

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

なし

５．１．１．３　資源量の制限

１）資源割当て(FRU_RSA)

管理: FRU_RSA.1

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) グループ及び/または個々の利用者及び/またはサブジェクトに対して、管理者が資源の最大限度を特定すること。

監査: FRU_RSA.1

a) 最小: 資源制限による割当て操作の拒否。

FRU_RSA.1 最大割当て

FRU_RSA.1.1

TSFは、[選択: *個々の利用者、定義された利用者のグループ、サブジェクト*]が[選択: *同時に、特定した時間の間*]使用できる、以下の資源*[割付: 制御下にある資源*]の最大割当てを実施しなければならない。

[割付] *制御下にある資源*

- データベーススペース
- ディクショナリ
- 監査ログファイル
- ログファイル
- 作業用ファイル
- アプリケーションのプロセスに対応する共用メモリ
- アプリケーションのプロセスに対応するサーバプロセスのスレッド

[選択] *個々の利用者、定義された利用者のグループ、サブジェクト*

- サブジェクト

[選択] *同時に、特定した時間の間*

- 同時に

２）複数同時セションの制限(FTA_MCS)

管理: FTA_MCS.2

以下のアクションはFMTにおける管理アクティビティと考えられる:

a) 管理者による最大許可同時利用者セション数運営規則の管理。

監査: FTA_MCS.2

a) 最小: 複数同時セションの制限に基づく新しいセションの拒否。

FTA_MCS.2 複数同時セションの利用者属性ごと制限

FTA_MCS.2.1

TSFは、規則[割付: *最大同時セション数の規則*]に従って、同一利用者に属する同時セションの最大数を制限しなければならない。

[割付] *最大同時セション数の規則*

－ 管理者が各利用者に対して制限した値

FTA_MCS.2.2

TSFは、デフォルトで、利用者あたり[割付: *デフォルト数*]セションの制限を実施しなければならない。

[割付] *デフォルト数*

－ 管理者が、運用に応じて指定する値。省略値＝1。範囲＝1～32767、または無制限。

５．１．１．４ 資源保護

１）ＴＳＦデータの管理(FMT_MTD)

管理: FMT_MTD.1(1)

以下のアクションはFMT管理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。

監査: FMT_MTD.1(1)

a) 基本: TSFデータの値のすべての改変。

FMT_MTD.1(1) TSFデータの管理

FMT_MTD.1.1(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。

[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

[割付] *TSF データのリスト*

- ディクショナリ
- 監査ログファイル
- ログファイル
- 作業用ファイル

[割付] *許可された識別された役割*

- 管理者

５．１．１．５　残存情報保護

１）残存情報保護(FDP_RIP)

管理: FDP_RIP.1

以下のアクションはFMT管理における管理機能と考えられる:

a) いつ残存情報保護を実施するかの選択(すなわち、割当てあるいは割当て解除において)が、TOEにおいて設定可能にされる。

監査: FDP_RIP.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない。

FDP_RIP.1 サブセット残存情報保護

FDP_RIP.1.1

TSFは、以下のオブジェクト[選択: *への資源の割当て、からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *オブジェクトのリスト*]。

[選択] *への資源の割当て、からの資源の割当て解除*

- からの資源の割当て解除

[割付] *オブジェクトのリスト*

- データベーススペース

２）残存ＴＳＦデータ保護(FPT_RTP)

管理: FPT_RTP.1

以下のアクションはFMT管理における管理機能と考えられる:

a) いつ残存TSFデータ保護を実施するかの選択(すなわち、割当てあるいは割当て解除において)が、TOEにおいて設定可能にされる。

監査: FPT_RTP.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない。

FPT_RTP.1 サブセット残存ＴＳＦデータ保護

FPT_RTP.1.1

TSFは、以下のオブジェクト[選択: *への資源の割当て、からの資源の割当て解除*]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない: [割付: *オブジェクトのリスト*]。

[選択] *への資源の割当て、からの資源の割当て解除*

- からの資源の割当て解除

[割付] *オブジェクトのリスト*

- ディクショナリ
- 監査ログファイル
- ログファイル
- 作業用ファイル

５．１．１．６ 監査

１）セキュリティ監査データ生成(FAU_GEN)

管理: FAU_GEN.1、FAU_GEN.2

予見される管理アクティビティはない。

監査: FAU_GEN.1、FAU_GEN.2

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象とすべき識別されたアクションはない。

FAU_GEN.1 監査データ生成

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*

- 指定なし

[割付] *上記以外の個別に定義した監査対象事象*

- 表５．４で定義される監査項目

－ SQL 文の処理で環境矛盾のエラー（通信異常など）が発生した場合

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*

－ 表５．４で定義される監査事象毎の付加情報

FAU_GEN.2 利用者識別情報の関連付け

FAU_GEN.2.1

TSFは、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

２）セキュリティ監査レビュー(FAU_SAR)

管理: FAU_ SAR.1

以下のアクションはFMTの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)。

監査: FAU_ SAR.1

a) 基本: 監査記録からの情報の読み出し。

FAU_SAR.1 監査レビュー

FAU_SAR.1.1

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

[割付] *許可利用者*

－ 管理者

[割付] *監査情報のリスト*

－ 表５．４で定義される監査事象毎の監査項目および付加情報

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。

管理: FAU_SAR.2、FAU_SAR.3

予見される管理アクティビティはない。

監査: FAU_SAR.2

a) 基本: 監査記録からの成功しなかった情報読み出し。

FAU_SAR.2 限定監査レビュー

FAU_SAR.2.1

TSFは、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

管理: FAU_SAR.3

予見される管理アクティビティはない。

監査: FAU_SAR.3

a) 詳細: 閲覧に使用されるパラメタ。

FAU_SAR.3 選択可能監査レビュー

FAU_SAR.3.1

TSFは、[割付: *論理的な関連の基準*]に基づいて、監査データを[選択: *検索*、*分類*、*並べ替え*]する能力を提供しなければならない。

[選択] *検索*、*分類*、*並べ替え*

- 検索
- 並べ替え
- 分類

[割付] *論理的な関連の基準*

- 監査データの任意の情報（文字列や数値）の大小関係や同値関係

３）セキュリティ監査事象選択(FAU_SEL)

管理: FAU_SEL.1

以下のアクションはFMTの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。

監査: 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。

FAU_SEL.1 選択的監査

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*]

b) [割付: *監査の選択性の基礎となる追加属性リスト*]。

[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

[割付] *監査の選択性の基礎となる追加属性リスト*

－ なし

４）セキュリティ監査事象格納(FAU_STG)

管理: FAU_ STG.1

予見される管理アクティビティはない。

監査: FAU_ STG.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査すべき識別されたアクションはない。

FAU_STG.1 保護された監査証跡格納

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、監査記録の改変を[選択: *防止*、*検出*]できねばならない。

[選択: *防止*、*検出*]

－ 防止

管理: FAU_ STG.3

以下のアクションはFMTの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)。

監査: FAU_ STG.3

a) 基本: 閾値を超えたためにとられるアクション。

FAU_STG.3 監査データ損失の恐れ発生時のアクション

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] *監査格納失敗の恐れ発生時のアクション*

－ コンソールにメッセージ出力

[割付] *事前に定義された限界*

－ 管理者が、運用に応じて指定する値

管理: FAU_ STG.4

以下のアクションはFMTの管理機能と考えられる:

a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。

監査: FAU_ STG.4

a) 基本: 監査格納失敗によってとられるアクション。

FAU_STG.4 監査データ損失の防止

FAU_STG.4.1

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

[選択] *監査対象事象の無視*、*特権を持つ許可利用者に関わるもの以外の監査対象事象の抑止*、*最も古くに格納された監査記録への上書き*

－ 監査対象事象の無視

－ 最も古くに格納された監査記録への上書き

[割付] *監査格納失敗時にとられるその他のアクション*

－ 監査対象事象の無視の場合、以下の 2 つのアクションのいずれか

・ コンソールにメッセージを出力し、ＴＯＥを緊急停止する

・ コンソールにメッセージを出力し、格納に失敗した監査対象事象をコンソールに出力する

－ 最も古くに格納された監査記録への上書きの場合、以下のアクション

・ コンソールにメッセージを出力し、監査対象事象を最も古くに格納された監査記録へ上書きする

５．１．１．７　セキュリティ管理

１）ＴＳＦにおける機能の管理(FMT_MOF)

管理: FMT_MOF.1

以下のアクションはFMT管理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;

監査: FMT_MOF.1

a) 基本: TSFの機能のふるまいにおけるすべての改変。

FMT_MOF.1 セキュリティ機能のふるまいの管理

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。

[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
- のふるまいを改変する
- を停止する
- を動作させる

[割付] *機能のリスト*

- 認証識別
- アクセス制御
- 資源量の制限
- 資源保護
- 残存情報保護
- 監査

[割付] *許可された識別された役割*

- 管理者

２）セキュリティ属性の管理(FMT_MSA)

管理: FMT_MSA.1

以下のアクションはFMT管理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。

監査: FMT_MSA.1

a) 基本: セキュリティ属性の値の改変すべて。

FMT_MSA.1 セキュリティ属性の管理

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]*アクセス制御 **SFP***、*情報フロー制御 **SFP***

- アクセス制御 SFP_DBU

[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] *セキュリティ属性のリスト*

- 利用者属性
- 資源属性
- 操作属性
- 資源量属性

[割付] *許可された識別された役割*

- 管理者

管理: FMT_MSA.3(1)

以下のアクションはFMT管理における管理機能と考えられる:

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値の許可的あるいは制限的設定を管理すること。

監査: FMT_MSA.3(1)

b) 基本: セキュリティ属性の初期値の改変すべて。

FMT_MSA.3(1) 静的属性初期化

FMT_MSA.3.1(1)

TSFは、そのSFPを実施するために使われるセキュリティ属性として、[選択: *制限的*、*許可的*、*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。

[割付] *アクセス制御 **SFP***、*情報フロー制御 **SFP***

- アクセス制御 SFP_DBM

[選択] *制限的*、*許可的*、*その他の特性*

- 許可的

FMT_MSA.3.2(1)

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

[割付] *許可された識別された役割*

－ なし

管理: FMT_MSA.3(2)

以下のアクションはFMT管理における管理機能と考えられる:

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値の許可的あるいは制限的設定を管理すること。

監査: FMT_MSA.3(2)

b) 基本: セキュリティ属性の初期値の改変すべて。

FMT_MSA.3(2) 静的属性初期化

FMT_MSA.3.1(2)

TSFは、そのSFPを実施するために使われるセキュリティ属性として、[選択: *制限的*、*許可的*、*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。

[割付] *アクセス制御 SFP*、*情報フロー制御 SFP*

－ アクセス制御 SFP_DBU

[選択] *制限的*、*許可的*、*その他の特性*

－ 制限的

FMT_MSA.3.2(2)

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

[割付] *許可された識別された役割*

－ なし

３）ＴＳＦデータの管理(FMT_MTD)

管理: FMT_MTD.1(2)

以下のアクションはFMT管理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。

監査: FMT_MTD.1(2)

a) 基本: TSFデータの値のすべての改変。

FMT_MTD.1(2) TSFデータの管理

FMT_MTD.1.1(2)

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。

[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*]

- デフォルト値変更
- 削除

[割付] *その他の操作*

- なし

[割付] ***TSF** データのリスト*

- ディクショナリ（表５．３で与えられる以下の管理項目）
  - 利用者毎の属性
    - 認証が不成功回数となることができる閾値
    - 使用可能資源量
    - 同時使用セション数
    - 認証情報の寿命
- 監査ログファイル（表５．４で与えられる監査項目）
- ログファイル

[割付] *許可された識別された役割*

- 管理者

管理: FMT_MTD.1(3)

以下のアクションはFMT管理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。

監査: FMT_MTD.1(3)

a) 基本: TSFデータの値のすべての改変。

FMT_MTD.1(3) TSFデータの管理

FMT_MTD.1.1(3)

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。

[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*

- なし

[割付] ***TSF** データのリスト*

- ディクショナリ（表５．３で与えられる以下の管理項目）

- 利用者毎の属性
  - 認証が不成功回数となることができる閾値
  - 権限
  - 使用可能資源量
  - 同時使用セション数
  - 認証情報の寿命
- 識別認証情報
  - 認証情報
  - 利用者一覧

[割付] *許可された識別された役割*

- 管理者
- 利用者毎の属性および識別認証情報に関連付けられる利用者

管理: FMT_MTD.1(4)

以下のアクションはFMT管理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。

監査: FMT_MTD.1(4)

a) 基本: TSFデータの値のすべての改変。

FMT_MTD.1(4) TSFデータの管理

FMT_MTD.1.1(4)

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。

[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*

- なし

[割付] *TSF データのリスト*

- ディクショナリ（表５．３で与えられる以下の管理項目）
  - 初期化資源の選択
  - 監査ログの取得範囲
  - 危険値（エレメントサイズ）
  - 監査情報の取得失敗時の処理の選択
  - セキュリティの初期値の強弱
- 監査ログファイル（表５．４で与えられる監査項目）

[割付] *許可された識別された役割*

－ 管理者

管理: FMT_MTD.3

このコンポーネントについて、予見される追加の管理アクティビティはない。

監査: FMT_MTD.3

a) 最小: TSFデータのすべての拒否された値。

FMT_MTD.3 セキュアなTSFデータ

FMT_MTD.3.1

TSFは、TSFデータとしてセキュアな値だけが受け入れられることを保証しなければならない。

４）セキュリティ属性有効期限(FMT_SAE)

管理: FMT_SAE.1

以下のアクションはFMT管理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。

監査: 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。

FMT_SAE.1 時限付き許可

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*

－ 認証情報

[割付] *許可された識別された役割*

－ 管理者

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*

－ 認証情報の無効化により、ＴＯＥの利用を不可能にする

５）管理機能の特定(FMT_SMF)

管理: FMT_SMF.1
このコンポーネントに関して予見される管理アクティビティはない。

監査: FMT_SMF.1
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていれば、以下の事象を監査対象にすべきである:
a) 最小: 管理機能の使用。

FMT_SMF.1 管理機能の特定
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５．３で与えられる管理項目を管理する機能

６）セキュリティ管理役割(FMT_SMR)

管理: FMT_SMR.1(1)
以下のアクションはFMT管理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。

監査: FMT_SMR.1(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;

FMT_SMR.1(1) セキュリティ役割
FMT_SMR.1.1(1)
TSFは、役割[割付: *許可された識別された役割*]を維持しなければならない。
[割付]*許可された識別された役割*
－ 管理者
－ 利用者毎の属性および識別認証情報に関連付けられる利用者

FMT_SMR.1.2(1)
TSFは、利用者を役割に関連づけなければならない。

５．１．２　ＴＯＥセキュリティ保証要件

ＳｙｍｆｏＷＡＲＥは一般のコマーシャルシステムの中で利用される。ＳｙｍｆｏＷＡＲＥは企業の秘密情報や顧客データなどのプライバシー情報の管理を行う。このため信頼性確保が必要になるため、ＥＡＬ４を品質保証レベルとする。なお、ＥＡＬ４を超える特定の保証対策はない。

ＥＡＬ４保証要件コンポーネントは以下の表５．１のとおり。

表５．１　保証要件コンポーネント一覧

クラス	コンポーネント名
構成管理	ACM_AUT.1
	ACM_CAP.4
	ACM_SCP.2
配付と運用	ADO_DEL.2
	ADO_IGS.1
開発	ADV_FSP.2
	ADV_HLD.2
	ADV_IMP.1
	ADV_LLD.1
	ADV_RCR.1
	ADV_SPM.1
ガイダンス文書	AGD_ADM.1
	AGD_USR.1
ライフサイクルサポート	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
テスト	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
脆弱性評定	AVA_MSU.2
	AVA_SOF.1
	AVA_VLA.2

５．１．３　ＴＯＥセキュリティ機能強度

ＳｙｍｆｏＷＡＲＥは一般のコマーシャルシステムの中で利用されることを想定しているため、最小機能強度レベルは”ＳＯＦ-basic”である。

機能強度が適用される TOE セキュリティ機能要件は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2(1)、FIA_UID.2(1)であり、その明示された機能強度は”ＳＯＦ-medium”である。

５．２　ＩＴ環境に対するセキュリティ要件

ＩＴ環境に対するセキュリティ要件について述べる。

５．２．１　ＯＳに依存する要件

１）セキュリティ管理役割(FMT_SMR)

管理: FMT_SMR.1(2)

以下のアクションはFMT管理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。

監査: FMT_SMR.1(2)

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;

FMT_SMR.1(2) セキュリティ役割

FMT_SMR.1.1(2)

OS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。

※ 下線部は詳細化

[割付]*許可された識別された役割*

－　管理者

FMT_SMR.1.2(2)

OSは、利用者を役割に関連づけなければならない。

※ 下線部は詳細化

２）セキュリティ属性の管理(FMT_MSA)

管理: FMT_MSA.3(3)

以下のアクションはFMT管理における管理機能と考えられる:

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値の許可的あるいは制限的設定を管理すること。

監査: FMT_MSA.3(3)

b) 基本: セキュリティ属性の初期値の改変すべて。

FMT_MSA.3(3) 静的属性初期化

FMT_MSA.3.1(3)

OS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*、*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。

※ 下線部は詳細化

[割付] *アクセス制御 SFP、情報フロー制御 SFP*

－ アクセス制御 SFP_AT

[選択] *制限的、許可的、その他の特性*

－ 許可的

FMT_MSA.3.2(3)

OS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。

※ 下線部は詳細化

[割付] *許可された識別された役割*

－ なし

３）タイムスタンプ(FPT_STM)

管理: FPT_STM.1

以下のアクションはFMTの管理機能と考えられる:

a) 時間の管理。

監査: FPT_STM.1

a) 最小: 時間の変更;

FPT_STM.1 高信頼タイムスタンプ

FPT_STM.1.1

OSは、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

※ 下線部は詳細化

４）リファレンス調停(FPT_RVM)

管理: FPT_RVM.1

予見される管理アクティビティはない。

監査: FPT_RVM.1

FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FPT_RVM.1 TSPの非バイパス性

FPT_RVM.1.1

OS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。

※ 下線部は詳細化

５）利用者認証(FIA_UAU)

管理: FIA_UAU.2(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。

監査: FIA_UAU.2(2)

基本: 認証メカニズムのすべての使用。

FIA_UAU.2(2) アクション前の利用者認証

FIA_UAU.2.1(2)

OSは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に**自分自身を認証**することを要求しなければならない。

※ 下線部は詳細化

６）利用者識別(FIA_UID)

管理: FIA_UID.2(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。

監査: FIA_UID.2(2)

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。

FIA_UID.2(2) アクション前の利用者識別

FIA_UID.2.1(2)

OSは、その利用者を代行する他のTSF調停アクションを許可する前に、各利用者に**自分自身を識別**することを要求しなければならない。

※ 下線部は詳細化

７）ドメイン分離(FPT_SEP)

管理: FPT_SEP.1
予見される管理アクティビティはない。

監査: FPT_SEP.1
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない。

FPT_SEP.1 TSFドメイン分離

FPT_SEP.1.1
OS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と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。
※ 下線部は詳細化

FPT_SEP.1.2
OS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。
※ 下線部は詳細化

８）アクセス制御方針(FDP_ACC)

管理: FDP_ACC.1(3)
このコンポーネントについて予見される管理アクティビティはない。

監査: FDP_ACC.1(3)
FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき
識別された事象はない。

FDP_ACC.1(3) サブセットアクセス制御

FDP_ACC.1.1(3)
OS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。
※ 下線部は詳細化
[割付] *アクセス制御 **SFP***
　－　アクセス制御 SFP_AT
[割付] *サブジェクト*
　－　OS 上で動作する全てのプロセス
[割付] *オブジェクト*

－ データベーススペース

[割付] *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*

－ データベーススペースに対する読み出し、書き込み

９）アクセス制御機能(FDP_ACF)

管理: FDP_ACF.1(3)

以下のアクションはFMTの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。

監査: FDP_ACF.1(3)

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。

FDP_ACF.1(3) セキュリティ属性によるアクセス制御

FDP_ACF.1.1(3)

OSは、[割付: *セキュリティ属性*、*名前付けされたセキュリティ属性のグループ*]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。

※ 下線部は詳細化

[割付] *アクセス制御SFP*

－ アクセス制御 SFP_AT

[割付] *セキュリティ属性*

－ プロセスの所有者属性

[割付] *名前付けされたセキュリティ属性のグループ*

－ アクセスパーミッション（OS により、プロセスの所有者属性ごとの資源に対する許可操作が定義されたもの）

FDP_ACF.1.2(3)

OS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*]。

※ 下線部は詳細化

[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*

－ OS 上で動作する全てのプロセスの所有者がデータベーススペースを操作する際、アクセスパーミッションで操作を許されているものであれば許可する

FDP_ACF.1.3(3)

OS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*]。

※ 下線部は詳細化

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

なし

FDP_ACF.1.4(3)

OS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。

※ 下線部は詳細化

[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

表５．２　セキュリティ機能要件一覧

セキュリティ機能要件	
認証、識別	FIA_AFL.1
	FIA_ATD.1
	FIA_SOS.1
	FIA_UAU.2(1)
	FIA_UID.2(1)
	FIA_USB.1
	FTA_TCH.1
アクセス制御	FDP_ACC.1(1)
	FDP_ACF.1(1)
	FDP_ACC.1(2)
	FDP_ACF.1(2)
資源量の制御	FRU_RSA.1
	FTA_MCS.2
資源保護	FMT_MTD.1(1)
残存情報保護	FDP_RIP.1
	FPT_RTP.1
監査	FAU_GEN.1
	FAU_GEN.2
	FAU_SAR.1
	FAU_SAR.2
	FAU_SAR.3
	FAU_SEL.1
	FAU_STG.1
	FAU_STG.3
	FAU_STG.4
セキュリティ管理	FMT_MOF.1
	FMT_MSA.1
	FMT_MSA.3(1)
	FMT_MSA.3(2)
	FMT_MTD.1(2)
	FMT_MTD.1(3)
	FMT_MTD.1(4)
	FMT_MTD.3
	FMT_SAE.1
	FMT_SMF.1
	FMT_SMR.1(1)
ＯＳに依存する機能	FMT_SMR.1(2)
	FMT_MSA.3(3)
	FPT_STM.1
	FPT_RVM.1
	FIA_UAU.2(2)
	FIA_UID.2(2)
	FPT_SEP.1
	FDP_ACC.1(3)
	FDP_ACF.1(3)

表５．３　管理要件パラメター覧（続く）

セキュリティ機能要件		管理要件	管理項目
認証、識別	FIA_AFL.1	不成功の認証試行に対する閾値の管理	利用者毎の属性 －認証が不成功回数となることができる閾値
		認証失敗の事象においてとられるアクションの管理	（固定）
	FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる	利用者毎の属性 －権限 －使用可能資源量
	FIA_SOS.1	秘密の検証に使用される尺度の管理	（固定）
	FIA_UAU.2(1)	管理者による認証データの管理	認証情報
		このデータに関係する利用者による認証データの管理	認証情報
	FIA_UID.2(1)	利用者識別情報の管理	利用者一覧
	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	利用者毎の属性 －権限 －使用可能資源量 －同時使用セション数
	FTA_TCH.1	予見させる管理アクティビティはない	
アクセス制御	FDP_ACC.1(1)	このコンポーネントについて予見される管理アクティビティはない	
	FDP_ACF.1(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	（固定）
	FDP_ACC.1(2)	このコンポーネントについて予見される管理アクティビティはない	
	FDP_ACF.1(2)	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	利用者毎の属性 －権限
資源量の制御	FRU_RSA.1	グループ及び/または個々の利用者及び/またはサブジェクトに対して、管理者が資源の最大限度を特定すること	利用者毎の属性 －使用可能資源量
	FTA_MCS.2	管理者による最大許可同時利用者セション数運営規則の管理	利用者毎の属性 －同時使用セション数
資源保護	FMT_MTD.1(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	（固定）
残存情報保護	FDP_RIP.1	いつ残存情報保護を実施するかの選択(すなわち、割当てあるいは割当て解除において)が、TOEにおいて設定可能にされる	（固定）
	FPT_RTP.1	いつ残存情報保護を実施するかの選択(すなわち、割当てあるいは割当て解除において)が、TOEにおいて設定可能にされる	初期化資源の選択 ※
監査	FAU_GEN.1	予見される管理アクティビティはない	
	FAU_GEN.2	予見される管理アクティビティはない	

表５．３　管理要件パラメター覧（続き）

セキュリティ機能要件		管理要件	管理項目
監査	FAU_SAR.1	監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)	（固定）
	FAU_SAR.2	予見される管理アクティビティはない	
	FAU_SAR.3	予見される管理アクティビティはない	
	FAU_SEL.1	監査事象を閲覧/改変する権限の維持	監査ログの取得範囲 ※
	FAU_STG.1	予見される管理アクティビティはない	
	FAU_STG.3	閾値の維持	危険値（エレメントサイズ)
		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)	（固定）
	FAU_STG.4	監査格納失敗時にとられるアクションの維持(削除、改変、追加)	監査情報の取得失敗時の処理の選択
セキュリティ管理	FMT_MOF.1	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	（固定）
	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	（固定）
	FMT_MSA.3(1)	初期値を特定できる役割のグループを管理すること	（固定）
		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	（固定）
	FMT_MSA.3(2)	初期値を特定できる役割のグループを管理すること	（固定）
		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	セキュリティの初期値の強弱
	FMT_MTD.1(2)	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	（固定）
	FMT_MTD.1(3)	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	（固定）
	FMT_MTD.1(4)	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	（固定）
	FMT_MTD.3	このコンポーネントについて、予見される追加の管理アクティビティはない	
	FMT_SAE.1	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	利用者毎の属性 －認証情報の寿命
		有効期限の時間が過ぎたときにとられるアクション	（固定）
	FMT_SMF.1	このコンポーネントに関して予見される管理アクティビティはない	
	FMT_SMR.1(1)	役割の一部をなす利用者のグループの管理	利用者毎の属性 －権限

補足　（固定）とは、ＴＯＥの場合は変更できない仕様であるため、管理の要件がないことを意味する。

※ この管理項目は、管理用件として要求されているものではないが、ＴＯＥとして管理が必要であるため、管理項目としている。

表５．４　監査要件（続く）

セキュリティ機能要件		監査要件	監査項目	付加される情報
認証、識別	FIA_AFL.1	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)	１）認証失敗 ２）連続的な認証失敗による認証情報の無効化	なし なし
	FIA_ATD.1	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない		
	FIA_SOS.1	基本: TSFによる、テストされた秘密の拒否または受け入れ	１）不適当な認証情報の拒否	なし
	FIA_UAU.2(1)	基本: 認証メカニズムのすべての使用	１）認証成功 ２）認証失敗	なし なし
	FIA_UID.2(1)	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	１）認証成功 ２）認証失敗	なし なし
	FIA_USB.1	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及び失敗)	１）認証成功 ２）認証失敗	なし なし
	FTA_TCH.1	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別されたアクションはない		
アクセス制御	FDP_ACC.1(1)	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない		
	FDP_ACF.1(1)	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	１）権限チェック成功 ２）権限チェック失敗	権限、アクセス対象 権限、アクセス対象
	FDP_ACC.1(2)	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない		
	FDP_ACF.1(2)	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	１）権限チェック成功 ２）権限チェック失敗	権限、アクセス対象 権限、アクセス対象
資源量の制御	FRU_RSA.1	最小: 資源制限による割当て操作の拒否	１）最大資源量を超えるかのチェックに該当	資源種別

表５．４　監査要件（続き）

セキュリティ機能要件		監査要件	監査項目	付加される情報
資源量の制御	FTA_MCS.2	最小: 複数同時セションの制限に基づく新しいセションの拒否	1）同時使用セション数を超えるかのチェックに該当	なし
資源保護	FMT_MTD.1(1)	基本: TSFデータの値のすべての改変	なし	
残存情報保護	FDP_RIP.1	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない		
	FPT_RTP.1	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象にすべき識別された事象はない		
監査	FAU_GEN.1	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象とすべき識別されたアクションはない		
	FAU_GEN.2	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査対象とすべき識別されたアクションはない		
	FAU_SAR.1	基本: 監査記録からの情報の読み出し	1）監査情報の参照	監査情報の参照に用いるＳＱＬ文
	FAU_SAR.2	基本: 監査記録からの成功しなかった情報読み出し	1）監査情報の参照の失敗（権限チェック失敗）	権限、アクセス対象
	FAU_SAR.3	詳細: 閲覧に使用されるパラメタ	1）監査情報の参照に用いるＳＱＬ文	監査情報の参照に用いるＳＱＬ文
	FAU_SEL.1	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	1）監査ログの取得範囲変更（DDL 文実行）	監査ログの取得範囲変更に用いる DDL 文
	FAU_STG.1	FAU_GEN セキュリティ監査データ生成がPP/STに含まれていても、監査すべき識別されたアクションはない		
	FAU_STG.3	基本: 閾値を超えたためにとられるアクション	1）監査情報量が危険値に達した時にとられる処理	なし
	FAU_STG.4	基本: 監査格納失敗によってとられるアクション	1）監査情報量が満杯に達した時にとられる処理	なし

表５．４　監査要件（続き）

セキュリティ機能要件		監査要件	監査項目	付加される情報
セキュリティ管理	FMT_MOF.1	基本: TSFの機能のふるまいにおけるすべての改変	1）セキュリティ機能の変更操作（DDL 文実行、保守・管理用のコマンドの実行）	セキュリティ機能の変更操作に用いる DDL 文およびコマンドの引数
	FMT_MSA.1	基本: セキュリティ属性の値の改変すべて	1）セキュリティ属性の変更（DDL 文実行）	セキュリティ属性の変更に用いる DDL 文
	FMT_MSA.3(1)	基本: セキュリティ属性の初期値の改変すべて	なし	
	FMT_MSA.3(2)	基本: セキュリティ属性の初期値の改変すべて	1）セキュリティ属性の変更（DDL 文実行）	セキュリティ属性の変更に用いる DDL 文
	FMT_MTD.1(2)	基本: TSFデータの値のすべての改変	1）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行）	セキュリティ情報の変更に用いる DDL 文およびコマンドの引数
	FMT_MTD.1(3)	基本: TSFデータの値のすべての改変	1）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行） 2）認証情報の変更（SET USER PASSWORD 文実行）	セキュリティ情報の変更に用いる DDL 文およびコマンドの引数 なし
	FMT_MTD.1(4)	基本: TSFデータの値のすべての改変	1）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行）	セキュリティ情報の変更に用いる DDL 文およびコマンドの引数
	FMT_MTD.3	最小: TSFデータのすべての拒否された値	1）セキュリティ情報の変更（DDL 文実行）	セキュリティ情報の変更に用いる DDL 文
	FMT_SAE.1	基本: 属性に対する有効期限の時間の特定;	1）認証情報の寿命の設定（DDL 文実行）	認証情報の寿命の設定に用いる DDL 文
		基本: 属性の有効期限切れによってとられるアクション	1）認証情報が寿命に達した（認証失敗）	なし

表５．４　監査要件（続き）

セキュリティ機能要件		監査要件	監査項目	付加される情報
セキュリティ管理	FMT_SMF.1	最小: 管理機能の使用	1）セキュリティ機能の変更操作（DDL 文実行、保守・管理用のコマンドの実行） 2）セキュリティ属性の変更（DDL 文実行） 3）セキュリティ情報の変更（DDL 文実行、保守・管理用のコマンドの実行）	セキュリティ機能の変更操作に用いる DDL 文およびコマンドの引数 セキュリティ属性の変更に用いる DDL 文 セキュリティ情報の変更に用いる DDL 文およびコマンドの引数
	FMT_SMR.1(1)	最小: 役割の一部をなす利用者のグループに対する改変	1）利用者属性の変更（DDL 文実行）	利用者属性の変更に用いる DDL 文

補足１

FAU_GEN1 について

FAU_GEN1 から、以下の事象も監査の対象となる。（ ）は付加される情報。

－　SQL 文の処理で発生した環境矛盾のエラー（異常メッセージ）

補足２

FMT_MTD.1(1)について

本来 TSF データが変更されたことを監査ログに取るべきであるが、TSF データの改変はできないため、FMT_MTD.1(1)では、監査項目は存在しない。

補足３

FMT_MSA.3(1)について

本来セキュリティ属性の初期値が変更されたことを監査ログに取るべきであるが、全ての表やプロシジャにアクセス可能な属性という初期値は変更できない。そのため、「セキュリティ属性の初期値の改変」は行われず、FMT_MSA.3(1)では、監査項目は存在しない。

補足４

FMT_MTD.1(3)について

SET USER PASSWORD 文は、結合済みでなければ実行できない文であり、結合中に何度実行しても有効なのは最後に実行したものだけである。セションに関する情報を取得することにより、SET USER PASSWORD 文を実行したアプリケーション名、時間が分かるため、利用者は認証情報が変更されたことを知ることができ、追跡・対処が可能である。そのため、FMT_MTD.1(3)では、セションに関する情報を SET USER PASSWORD 文の情報としている。

６　ＴＯＥ要約仕様

セキュリティ機能としては、以下のような四つの機能をもっている。

１）運用選択機能（Ｆ．ＳＥＬ）
　セキュリティ機能のふるまいを変更する機能である。
２）利用者制御機能（Ｆ．ＵＳＥＲ）
　各利用者の権限を制御し、指定された権限の範囲での処理を保証し、またその範囲を超えた処理を制限する機能である。
３）資源制御機能（Ｆ．ＲＥＳ）
　ＴＯＥが使用する資源を制御する機能である。
４）監査ログ機能（Ｆ．ＡＵＤＩＴ）
　利用者や管理者が行った処理に関する情報を保持しておく機能である。

６．１　ＴＯＥセキュリティ機能

６．１．１　運用選択機能（Ｆ．ＳＥＬ）

セキュリティパラメタを使用して、セキュリティ機能のふるまいを変更する機能である。この機能を使用して、セキュリティの強度を変更することができる。なお、インストール時に標準セキュリティ運用を選択した場合、セキュリティパラメタはセキュリティ上最も安全な値が設定されている。

ａ）パラメタを変更する機能（Ｆ．ＳＥＬ．ＰＡＲＡ）

－　パラメタの種類

セキュリティパラメタには、以下のものがある。

- 運用全体に関係するパラメタ
- 利用者制御機能に関係するパラメタ
- 監査ログ機能に関係するパラメタ

利用者のアプリケーションからのＳＱＬ文のアクセス機能も、使用可能な範囲を指定し、運用として不用な機能を抑止するパラメタがある。

－　パラメタの変更機能

セキュリティパラメタの設定には、以下のようなＤＤＬ文を用いる。ＤＤＬ文実行時には、設定値が実行可能な範囲にあるか否かのチェックを行う。

　　ＳＥＴ　ＳＹＳＴＥＭ　ＰＡＲＡＭＥＴＥＲ文

上記のＳＱＬ文は管理者のみが実行可能である。

－　監査ログ

セキュリティパラメタの設定は、管理者の行為として記録される。ＤＤＬ文全体が記録される。

６．１．２　利用者制御機能（Ｆ．ＵＳＥＲ）

各利用者を識別し、権限を制御し、指定された権限の範囲での処理を保証し、さらに範囲を超えた処理を制限する。

－　利用者を登録する機能
－　管理者および利用者を認証識別する機能
－　管理者および利用者の権限を制御する機能
－　利用者の資源量を制御する機能
－　利用者の権限を参照する機能

管理者は、スーパユーザであり、変更することはできない。管理者は、全ての権限を保持し、資源も無制限に使用できる。これらのことから、管理者の登録、管理者の権限や資源量を制御する機能はない。

ａ）利用者の登録機能（Ｆ．ＵＳＥＲ．ＤＥＦ）

－　利用者の登録

ＴＯＥは、ＯＳにログインできる利用者の一部に対してＴＯＥを使用させる機能と、ＯＳのログインユーザとは別にＴＯＥで独自に利用者を管理する機能がある。

識別に必要な情報をＴＯＥに対して登録する。ＯＳにログインできる利用者の一部に対してＴＯＥを使用させる場合は、識別情報のみを登録する。ＯＳのログインユーザとは別にＴＯＥで独自に管理された利用者に対しては、認証情報と識別情報を登録する。（識別情報は、１８バイト以内の先頭が英字で始まる英字または数字、もしくは１８バイト以内の日本語文字列でなければならない）

利用者の登録、および登録した情報の変更や破棄には、以下のようなＤＤＬ文を用いる。

登録　ＣＲＥＡＴＥ　ＵＳＥＲ文
変更　ＡＬＴＥＲ　ＵＳＥＲ文
破棄　ＤＲＯＰ　ＵＳＥＲ文

－　監査ログ

これらの文で指定するパラメタ変更は、管理者の行為としてＤＤＬ文全体が記録される。

ｂ）認証識別機能（Ｆ．ＵＳＥＲ．ＡＵＴＨＥＮ）

－　認証識別

ＯＳにログインした利用者が、そのままＴＯＥに結合しようとした場合、つまりＯＳによって識別認証された利用者がＴＯＥへの結合を要求した場合は、認証はログイン時に終了しているので、ＴＯＥは、その利用者がＴＯＥに正当に登録されているか、識別を行う。

ＯＳにログインした利用者が、別の利用者に代わってＴＯＥに結合しようとした場合、つまりＯＳによって識別認証されずにＴＯＥへの結合を要求した場合は、代わろうとしている利用者がＯＳで管理されている場合と、ＴＯＥで独自に管理されている場合の２つの利用形態がある。どちらの場合も、ＴＯＥはその利用者がＴＯＥに正当に登録されているか、識別と認証を行う。

－　アクセス履歴の表示

ＴＯＥは、結合処理の正常メッセージの中に最終の成功結合の日時を埋め込んで表示する。また、システム表に、各利用者の最終成功の結合依頼の日時と、最終成功の結合依頼以降の不成功の結合依頼の回数を保持する。この情報は、管理者と利用者が参照可能である。

－　認証失敗時の動作

認証に失敗した場合は、連続攻撃を防ぐために、結合依頼を一定時間待ち状態にする。

－　認証連続失敗時の動作

認証に連続して失敗した場合、その認証情報を無効化することで、ＴＯＥの利用を不可能にする。この最大の連続失敗回数は、管理者が利用者に対して指定することができる。また、管理者のみが、無効化された認証情報を有効にすることができる。

－　利用者による認証情報の変更

認証情報は利用者自身による変更も可能であり、以下のＳＱＬ文を用いて行う。

ＳＥＴ　ＵＳＥＲ　ＰＡＳＳＷＯＲＤ文

－　認証情報の適合性

ＴＯＥに登録される認証情報は、ＯＳに登録する認証情報と同程度の品質基準を保持していなければならない。検査の対象は以下の通りである。

- 以下の文字で構成される文字列定数で指定されているか
  - ・英字
  - ・数字
  - ・以下の特殊文字

    , ( ) . : ; = * + - / ? < > % _ ’ ”
  - ・以下の拡張文字

    @ ¥ #
- セキュリティパラメタで指定されるパスワードの最低長以上で、８文字以内の文字列であるか
- 最低でも２文字以上の英字を含んでいるか
- １文字以上の数字または特殊文字、拡張文字を含んでいるか
- 大文字と小文字は同一文字として利用者名と比較した場合、同じものや、ずらしたもの、反転したものでないか
- 大文字と小文字は同一文字として現在使用しているパスワードと比較した場合、３文字以上違うものであるか

なお、本ＴＯＥセキュリティ機能の機能強度は、ＳＯＦ-medium である。

－ 認証情報の寿命

長期間に渡って同一の認証情報を使用するのは、漏洩の危険性がある。このため、管理者は、認証情報の寿命を定義することができる。管理者が定めた期間が過ぎると、利用者に対して認証情報の変更を促したり、利用者が変更しない場合に認証情報を無効化することでＴＯＥの利用を不可能にする。

－ 監査ログ

以下の事象が監査ログの対象となる。

- 認証の成功
- 認証の失敗
- 連続失敗による認証情報の無効化

それぞれの事象において、利用者およびアクセス方法を特定する情報が記録される。

c）権限の制御機能（Ｆ．ＵＳＥＲ．ＰＲＩＶ）

－ 資源へのアクセス

各資源へのアクセスは、サーバプロセスが一括して行う。サーバプロセスは共用メモリを介して利用者のプロセスおよび管理者のプロセスの識別情報（プロセスがアプリケーションの場合 SQL 文中の識別情報、コマンドの場合実行者の識別情報）に関連付けられるアクセス権限に従ってアクセスを実行する。

－ 権限

TOE は管理者や利用者に対して権限の制御を行っている。

権限制御の初期値は、管理者に対してはすべての操作を可能、利用者に対してはすべての操作を不可能に設定されている。

管理者は全てのアプリケーションおよびコマンド実行権限を持つ。

管理者は必要に応じて利用者に権限を付与し、利用者は管理者から付与される権限の範囲で、表の操作およびプロシジャの実行を行う。

対象者		権限	操作	資源
管理者		全て	データの保守 （アプリケーション、 コマンド）	データベーススペース ディクショナリ 監査ログファイル
	利用者	ＳＥＬＥＣＴ権	表の参照	データベーススペース
		ＵＰＤＡＴＥ権	表の更新	
		ＤＥＬＥＴＥ権	表の削除	
		ＩＮＳＥＲＴ権	表の挿入	
		ＥＸＥＣＵＴＥ権	プロシジャの実行	

－ 権限の制御

利用者に対する権限の付与、あるいは、剥奪は、管理者のみが実行できる。この権限の付与、および付与した権限の剥奪には、以下のようなＤＤＬ文を用いる。

付与　ＧＲＡＮＴ文

剥奪　ＲＥＶＯＫＥ文

－　権限のチェック

アプリケーション実行中に、その利用者に対する権限が変更されることを想定して、データベースのアクセス時に毎回、権限のチェックを実施する。

コマンドは、ＴＯＥが実行者を識別し、管理者のみが実行できる。

－　監査ログ

以下の事象が監査ログの対象となる。

・　権限のチェック成功

・　権限のチェック失敗

それぞれの事象において、チェックの対象となった、権限、アクセス対象が記録される。

ｄ）資源量の制御機能（Ｆ．ＵＳＥＲ．ＲＥＳ）

－　資源量の制御

管理者は、各利用者が使用可能な資源量を制限する。利用者は管理者が制限する資源量の範囲で、アプリケーションの実行を行う。制限の対象となる資源は以下の通りであり、セション毎に管理されている。また、一人の利用者が同時に使用可能なセション数も管理している。

・データベーススペース

・ディクショナリ

・監査ログファイル

・ログファイル

・作業用ファイル

・アプリケーションのプロセスに対応する共用メモリ

・アプリケーションのプロセスに対応するサーバプロセスのスレッド

上記の資源量の制御は、セキュリティパラメタにより行う。

資源	セキュリティパラメタ	補足説明
一人の利用者が同時に使用可能なセション数	MAX_CONNECTION	
データベーススペース ディクショナリ 監査ログファイル ログファイル	MAX_TRAN_MEM MAX_TRAN_TIME	対象の資源はトランザクション単位で書き込まれる。トランザクションあたりのメモリ量、時間を制限することで、セション内で各利用者が使用する資源量を制限できる。
作業用ファイル	MAX_WORKFILE_USE MAX_WORKFILE_NUM	作業用ファイル量、ファイル数を制限することで、各利用者が使用する作業用ファイル量を制限できる。

アプリケーションのプロセスに対応する共用メモリ	MAX_WAIT_TIME	セションあたりの共用メモリの量は事前に管理者により決められている。また、無応答待ち時間を指定して時間を超過したセションを切断することで、メモリの不当な占有を制限する。 上記より、セション内で各利用者が使用する共用メモリを制限できる。
アプリケーションのプロセスに対応するサーバプロセスのスレッド	MAX_MEMORY_USE MAX_WAIT_TIME	セションあたりのスレッド数は１（固定）であり、利用者が使用可能なスレッドの資源は、スレッドが獲得するメモリだけである。最大メモリ量を指定することでスレッドが獲得するメモリ量を制限できる。また、無応答待ち時間を指定して時間を超過したセションを切断することで、スレッドやメモリの不当な占有を制限する。 上記より、セション内で各利用者が使用するスレッドの資源を制限できる。

これら利用者毎の資源量の指定は、利用者の登録、変更時に設定する。

登録　ＣＲＥＡＴＥ　ＵＳＥＲ文

変更　ＡＬＴＥＲ　ＵＳＥＲ文

－　監査ログ

使用可能な資源量を超えた獲得は、監査ログの対象となる。この時、獲得しようとした資源の種別が記録される。

ｅ）権限情報の参照機能（Ｆ．ＵＳＥＲ．ＲＥＦ）

－　権限情報の参照

各利用者の識別に必要な情報、保持している権限や、使用可能な資源量は、ディクショナリ内に格納される。これらの情報は、ＳＱＬ文を使用して参照でき、更新することはできない。

管理者は、全利用者に関する情報を参照することができる。利用者は、自分に関する情報のみ参照することができる。

－　監査ログ

以下の事象が監査ログの対象となる。

- 権限のチェック成功
- 権限のチェック失敗

それぞれの事象において、チェックの対象となった、権限、アクセス対象が記録される。

６．１．３　資源制御機能（Ｆ．ＲＥＳ）

資源制御機能とは、ＴＯＥが使用する資源を制御する機能である。

以下の二つの機能からなる。

－ 属性の制御機能

－ 使用済み資源の初期化機能

ａ）属性の制御機能（Ｆ．ＲＥＳ．ＡＴＴＲ）

ＴＳＦデータの参照は、管理者のみに許可する。

ＴＳＦデータとは以下のものである。

－ ディクショナリ

－ 監査ログファイル

－ ログファイル

－ 作業用ファイル

ｂ）使用済み資源の初期化機能（Ｆ．ＲＥＳ．ＩＮＩＴ）

ＴＯＥがＯＳから獲得し、使用済となったファイルは、ＯＳへの返却前に残存情報を初期化する。

使用済となったファイルとは、以下のものである。

－ データベーススペース

－ ディクショナリ

－ 監査ログファイル

－ ログファイル

－ 作業用ファイル

６．１．４ 監査ログ機能（Ｆ．ＡＵＤＩＴ）

監査ログ機能とは、利用者や管理者の処理の情報を保持しておく機能である。以下の機能からなる。

－ 監査ログの取得機能

－ 監査ログの参照機能

－ 監査ログの領域管理機能

ａ）監査ログの取得機能（Ｆ．ＡＵＤＩＴ．ＣＯＬ）

監査ログの取得の対象となる事象は以下の通りである。

・ 利用者によるＴＯＥに対する結合と結合解除

・ 利用者からの要求によるデータベースへのアクセス

・ 管理者によるＴＯＥに対する操作

・ システムで発生した異常に関する情報

－ 利用者によるＴＯＥに対する結合処理と結合解除処理

利用者によるＴＯＥに対する結合処理と結合解除処理の情報を取得する。ただし、管理者がアプリケーションを実行した場合も、情報が取得される。

これらの事象に対して、以下のような情報が取得される。

- 事象の発生した日時
- 認証成功／失敗
- 認証に失敗した場合、失敗した理由
- アプリケーションを識別する情報
- 利用者名
- 結合から結合解除までに行われた処理の要約

－ 利用者からの要求によるデータベースへのアクセス

利用者からの要求によるデータベースへのアクセス時、権限のチェックの情報を取得する。また、管理者がアプリケーションを実行した場合も、情報が取得される。さらに、ＳＱＬ文でアクセス可能なシステムディクショナリや監査ログの参照に関しても、情報が取得される。

これらの事象に対して、以下のような情報が取得される。

- 事象の発生した日時
- 権限チェック成功／失敗
- アプリケーションを識別する情報
- 利用者名
- アクセス対象の資源
- 権限

－ 管理者によるＴＯＥに対する操作

管理者によるＴＯＥに対する操作の情報を取得する。これは、管理者にのみ許可された機能が誤用された場合の影響が大きいためである。以下の事象がある。

- 保守・管理用のコマンドの実行
- ＤＤＬ文の実行
- 監査ログに対する参照

保守・管理用のコマンドには、システムの起動・停止も含まれている。これらの事象に対して、以下のような情報がある。

- 事象の発生した日時
- 管理者の処理を識別する情報（コマンドの引数、ＳＱＬ文など）

－ システムで発生した異常に関する情報

システムで発生した異常に関する情報には、以下のものがある。

- 監査ログが満杯になった
- 監査ログ量が危険値に達した
- 連続的な認証失敗により認証情報を無効化した
- 同時使用セション数を超えた

・ 利用者が使用可能な最大資源量を超えた
・ ＳＱＬ文の処理で環境矛盾のエラーが発生した
（ＳＥＴ ＵＳＥＲ ＰＡＳＳＷＯＲＤ文実行時のパスワード適切性チェックエラーなど）

これらの事象に対して、以下のような情報が取得される。

・ アプリケーションを識別する情報
・ 利用者名
・ 異常事象を識別する情報（エラーメッセージ）

ただし、アプリケーションや利用者と直接関わらない場所で発生した異常事象に関しては、異常事象の主体はシステムと識別され、それらに関する情報は取得されない。

－ 取得対象事象の選択

監査ログの取得範囲は、変更することができる。どの事象に対して取得するかを選択することができる。この機能は管理者のみが実行可能である。

ｂ）監査ログの参照機能（Ｆ．ＡＵＤＩＴ．ＶＩＥＷ）

監査ログは、表の形式で格納されるので、ＳＱＬ文を使用して参照可能である。ＳＱＬ文を用いることによって、条件づけによる情報の絞込みや、取り出し順番を自由に指定することができる。

監査ログのＳＱＬ文による参照は、管理者のみ実行可能である。また、管理者による参照を妨害させないために、管理者のみデータベース操作を可能にすることもできる。

ｃ）監査ログ領域管理機能（Ｆ．ＡＵＤＩＴ．ＳＰＡＣＥ）

－ 監査ログの領域管理

監査ログは、複数個の単位に分割して格納する。この分割の単位をエレメントと呼ぶ。監査ログに対する操作は、エレメント単位に行う。監査ログの作成、追加、削除、バックアップや初期化、復元は、エレメント単位に行うことができる。なお、監査ログの作成、追加、削除、バックアップや初期化、復元は管理者のみ実行可能である。

ＴＯＥは、一つのエレメントに監査ログを取得し、それが満杯になると、管理者にその事象を通知した後に、別のエレメントに情報を取得する。管理者は、全てのエレメントが満杯になるまでの間に、いずれかの（通常は最も古い）エレメントをバックアップ、初期化する。ＴＯＥは、初期化済みのエレメントに監査ログを取得する。

－ 監査ログが満杯時の事象

監査ログの満杯は、通常の運用の中では発生しない事象である。これが発生した場合、管理者はセキュリティパラメタを選択することにより、監査対象事象を無視してＴＯＥを緊急停止、監査対象事象をコンソールに出力してＴＯＥの動作継続、最も古くに格納された監査ログを上書きしてＴＯＥの動作継続を行うことができる。

６．１．５　セキュリティ機能要件対応

６．１．１から６．１．４のＴＯＥセキュリティ機能は、セキュリティ機能要件と以下の表６．１の通り対応する。

表６．１　セキュリティ機能とセキュリティ機能要件（続く）

セキュリティ機能要件 ＼ セキュリティ仕様概要		F・SEL・PARA	F・USER・DEF	F・USER・AUTHEN	F・USER・PRIV	F・USER・RES	F・USER・REF	F・RES・ATTR	F・RES・INIT	F・AUDIT・COL	F・AUDIT・VIEW	F・AUDIT・SPACE
認証・識別	FIA_AFL.1			✓								
	FIA_ATD.1		✓		✓	✓						
	FIA_SOS.1			✓								
	FIA_UAU.2(1)			✓								
	FIA_UID.2(1)			✓								
	FIA_USB.1				✓	✓						
	FTA_TCH.1			✓								
アクセス制御	FDP_ACC.1(1)				✓							
	FDP_ACF.1(1)				✓							
	FDP_ACC.1(2)				✓							
	FDP_ACF.1(2)				✓							
資源量の制御	FRU_RSA.1					✓						
	FTA_MCS.2					✓						
資源保護	FMT_MTD.1(1)							✓				
残存情報保護	FDP_RIP.1								✓			
	FPT_RTP.1								✓			
監査	FAU_GEN.1									✓		
	FAU_GEN.2									✓		
	FAU_SAR.1										✓	
	FAU_SAR.2										✓	
	FAU_SAR.3										✓	
	FAU_SEL.1									✓		
	FAU_STG.1											✓
	FAU_STG.3											✓
	FAU_STG.4											✓

表６．１　セキュリティ機能とセキュリティ機能要件（続き）

セキュリティ仕様概要 / セキュリティ機能要件		F・SEL・PARA	F・USER・DEF	F・USER・AUTHEN	F・USER・PRIV	F・USER・RES	F・USER・REF	F・RES・ATTR	F・RES・INIT	F・AUDIT・COL	F・AUDIT・VIEW	F・AUDIT・SPACE
セキュリティ管理	FMT_MOF.1	✓			✓							
	FMT_MSA.1			✓	✓	✓						
	FMT_MSA.3(1)				✓							
	FMT_MSA.3(2)				✓							
	FMT_MTD.1(2)	✓			✓							✓
	FMT_MTD.1(3)		✓	✓	✓		✓					
	FMT_MTD.1(4)	✓			✓						✓	✓
	FMT_MTD.3	✓	✓	✓	✓							
	FMT_SAE.1			✓								
	FMT_SMF.1	✓			✓	✓					✓	✓
	FMT_SMR.1(1)		✓									

６．２　保証手段

本ＳＴにおける保証コンポーネント名と保証手段を表６．２に示す。

表６．２　保証コンポーネント名と保証手段（続く）

クラス	コンポーネント名	保証手段
構成管理	ACM_AUT.1	－構成管理手順
	ACM_CAP.4	－構成管理ツール利用手引書(開発者編)
	ACM_SCP.2	－構成管理ツール利用手引書(管理者編) －障レリスト QQM －マニュアル要望一覧 －文書管理手順 －品質記録管理手順 －ファイル命名規約 －ソースプログラム一覧リスト －構成リスト －文書管理台帳 －マニュアル識別方法
配付と運用	ADO_DEL.2	－配布規定
	ADO_IGS.1	－SymfoWARE Server インストールガイド －SymfoWARE Server セキュリティガイド －SymfoWARE Server RDB 管理者ガイド
開発	ADV_FSP.2	－セキュリティ機能仕様書
	ADV_HLD.2	－セキュリティ構成仕様書
	ADV_IMP.1	－セキュリティ詳細仕様書
	ADV_LLD.1	－「ソースプログラム一覧リスト」で識別されるソースプログラム
	ADV_RCR.1	－セキュリティポリシーモデル
	ADV_SPM.1	－セキュリティ対応表 －セキュリティ用語集
ガイダンス文書	AGD_ADM.1	－SymfoWARE Server セキュリティガイド
	AGD_USR.1	－SymfoWARE Server RDB 管理者ガイド －SymfoWARE Server SQL リファレンスガイド
ライフサイクルサポート	ALC_DVS.1	－開発環境管理規定
	ALC_LCD.1	－コンパイル／リンクオプション体系
	ALC_TAT.1	

表６．２　保証コンポーネント名と保証手段（続き）

クラス	コンポーネント名	保証手段
テスト	ATE_COV.2	－セキュリティテスト仕様書
	ATE_DPT.1	－運用選択機能テスト計画／報告書
	ATE_FUN.1	－運用選択機能テスト手順書
	ATE_IND.2	－脅威テスト計画／報告書 －脅威テスト手順書 －提供ファイルの権限テスト計画／報告書 －提供ファイルの権限テスト手順書 －認証識別テスト計画／報告書 －認証識別テスト手順書 －コマンドの利用者認証テスト計画／報告書 －コマンドの利用者認証テスト手順書 －権限チェックテスト計画／報告書 －権限チェックテスト手順書 －コマンド実行権限テスト計画／報告書 －コマンド実行権限テスト手順書 －資源量検査テスト計画／報告書 －資源量検査テスト手順書 －システム表/監査ログ表権限テスト計画／報告書 －システム表/監査ログ表権限テスト手順書 －属性制御テスト計画／報告書 －属性制御テスト手順書 －資源作成時の権限テスト計画／報告書 －資源作成時の権限テスト手順書 －初期化テスト計画／報告書 －初期化テスト手順書 －資源削除時の情報初期化テスト計画／報告書 －資源削除時の情報初期化テスト手順書 －監査ログ取得テスト計画／報告書 －監査ログ取得テスト手順書 －コマンド実行時の監査ログテスト計画／報告書 －コマンド実行時の監査ログテスト手順書 －監査ログ制御テスト計画／報告書 －監査ログ制御テスト手順書 －セキュリティ用語集
脆弱性評定	AVA_MSU.2	－セキュリティ脆弱性アセスメント
	AVA_SOF.1	
	AVA_VLA.2	

７　ＰＰ主張

本ＳＴに準拠するＰＰはない。

８　根拠

セキュリティ対策方針、セキュリティ要件、セキュリティ仕様概要およびＰＰ準拠の各検証について述べている。

８．１　セキュリティ対策方針根拠

表８．１に示すように、“前提条件”（この章では、“想定される環境”と表現）と“環境のセキュリティ対策方針”（この章では、“非ＩＴ対策方針”と省略して表現）は、“ＴＯＥのセキュリティ対策方針”（この章では、“ＩＴ対策方針”と省略して表現）が動作する基本になっている。また、ＩＴ対策方針は、それぞれの想定する脅威に対抗するためにたてられたものであり、想定されない環境や、想定されない環境下での対策方針はない。

想定する脅威に対して、ＩＴ対策方針が十分であること、運用環境に対する脅威に対しては、非ＩＴ対策方針が十分であることを説明する。

表８．１　脅威に対する対策方針

脅威＼対策方針	O・CONNECT	O・ACCESS	O・RESOURCE	O・ATTR	O・INIT	O・AUDIT	OE・CONNECT	OE・ASSIGN	OE・USER	OE・PHYSICAL	OE・ENV	OE・OS
A．MANAGER								✓			✓	
A．USER									✓			
A．PHYSICAL										✓		
T．TCP											✓	✓
T．XA											✓	
T．ACCESS	✓	✓		✓		✓	✓				✓	✓
T．RESOURCE		✓	✓			✓					✓	
T．OS				✓							✓	✓
T．DATA					✓						✓	

－　A．MANAGERの実現

前提条件A．MANAGERは、OE．ASSIGNによるふさわしい管理者の選任と、その管理者に対する教育および管理、OE．ENVによる、管理者が監査ログを参照することで行う他の管理者のチェックにより実現できる。

－　A．USERの実現

前提条件A．USERは、OE．USERにより、管理者が利用者に対し、パスワードやアプリケー

ションを他人に利用されないよう教育することで実現できる。

－ Ａ．ＰＨＹＳＩＣＡＬの実現

前提条件Ａ．ＰＨＹＳＩＣＡＬは、ＯＥ．ＰＨＹＳＩＣＡＬによる物理的環境の管理により実現できる。

－ Ｔ．ＴＣＰに対する対策方針

脅威Ｔ．ＴＣＰに対抗するためには、ＲＤＢ２＿ＴＣＰ連携不可能状態にする。

ＯＥ．ＥＮＶによって、管理者がＲＤＢ２＿ＴＣＰ連携を不可能にするパラメタ（ＯＳのパラメタ）を設定すると、ＯＥ．ＯＳによって、ＲＤＢ２＿ＴＣＰ連携機能を利用した結合が拒否される。この予防の対策により、想定される脅威に適切に対抗している。

－ Ｔ．ＸＡに対する対策方針

脅威Ｔ．ＸＡに対抗するためには、ＸＡ連携不可能状態にする。

ＯＥ．ＥＮＶによって、管理者がＸＡ連携を不可能にする設定を行い、ＴＯＥの運用中にＸＡ連携機能の利用が可能にならないよう維持、監視する。この予防の対策により、想定される脅威に適切に対抗している。

－ Ｔ．ＡＣＣＥＳＳに対する対策方針

脅威Ｔ．ＡＣＣＥＳＳに対抗するためには、まずＴＯＥへの結合を許可されていない者の結合を拒否し、次に利用者の権限の有無をチェックすればよい。

結合時に識別情報を指定しない場合は、ＯＥ．ＣＯＮＮＥＣＴによってＯＳで行われた識別認証における識別情報を引き継ぎ、Ｏ．ＣＯＮＮＥＣＴによって識別のみ行う。また、識別情報を指定している場合には、Ｏ．ＣＯＮＮＥＣＴによって、新たに認証を行い識別情報の正当性を確認しており、ＴＯＥへの結合を許可されていない者の結合を拒否している。

ＴＯＥへの結合を許可された利用者がＴＯＥの機能を利用して保護資産にアクセスする方法は、アプリケーションでのＳＱＬ文によるアクセスとコマンドによるアクセスのみである。

アプリケーションでのＳＱＬ文によるアクセスの場合、データベース形式のファイルしかアクセスできないため、ログファイル、作業用ファイル、動作環境ファイルの３つのファイルはアクセス不可能である。データベーススペース、ディクショナリ、監査ログファイルについては、Ｏ．ＡＣＣＥＳＳによって、ＴＯＥは権限の有無をチェックし、権限のないものには処理を制限している。

コマンドによるアクセスの場合、保護資産全てにアクセスできる。アクセス対象の保護資産は、ＯＥ．ＯＳによってデータベーススペースに対してアクセス制御が行われ、管理者のみアクセス可能となっている。ディクショナリ、監査ログファイル、ログファイル、作業用ファイルはＯ．ＡＴＴＲによって管理者のみアクセス可能である。動作環境ファイルも、ＯＥ．ＥＮＶによって、管理者の責任で管理者のみアクセス可能なアクセス制御が行われる。したがって、コマンドによる保護資産へのアクセスは制限されている。しかし、コマンドの中には、ＴＯＥの権限（管理者権限）で動作し、保護資産

にアクセスするものもある。これらのコマンドは、O．ＡＣＣＥＳＳによって、実行者が管理者であるかチェックされるため、コマンドによる保護資産へのアクセスは管理者に限られる。

これらにより、脅威T．ＡＣＣＥＳＳを抑止する対策をとっている。

また、何らかの状況で、想定される環境が崩れる、あるいは非ＩＴ対策方針が満たされないために、O．ＣＯＮＮＥＣＴおよびOＥ．ＣＯＮＮＥＣＴが有効に動作しない場合、そのような状態異常を検知するための対策方針として、O．ＡＵＤＩＴをとっている。これによって、ＴＯＥへの結合を許可されていない者が存在してもＴＯＥへの結合時のログが残される。同様に、O．ＡＣＣＥＳＳが有効に動作しない場合を考え、そのような状態異常を検知するための対策方針として、O．ＡＵＤＩＴをとっている。これによって、利用者が権限チェックを不当に成功させたとしても、チェック時のログが残される。

さらに、OＥ．ＥＮＶによって管理者がバックアップリカバリ運用を実施しているので、リカバリ処理を行うことにより、データが破壊や改ざんされた場合も退避データから復旧することができる。

上記の予防、検出、回復の三つの対策により、想定される脅威に適切に対抗している。

－　T．ＲＥＳＯＵＲＣＥに対する対策方針

まず、OＥ．ＥＮＶにより、動作環境ファイルは管理者の責任で適切に管理され、アプリケーションのプロセスも、管理者が利用者の環境を適切に管理することで、利用者がアプリケーションを実行する環境は制限されるため、枯渇しない。枯渇する可能性のある資源（データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルおよびアプリケーションのプロセスを除く実行資源）について脅威T．ＲＥＳＯＵＲＣＥに対抗するためには、資源量をチェックすればよい。

データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルおよびアプリケーションの実行に関する資源（アプリケーションのプロセスに対応する共用メモリおよびサーバプロセスのスレッド）は、O．ＲＥＳＯＵＲＣＥによって、各利用者が使用可能な資源量をチェックすることで制限している。コマンドの実行に関する資源（コマンドのプロセス、コマンドのプロセスに対応する共用メモリおよびサーバプロセスのスレッド）は、O．ＡＣＣＥＳＳで管理者以外がコマンドを実行できないように制限している。よって、資源を過度に使用することはできない。

また、何らかの状況で、想定される環境が崩れる、あるいは非ＩＴ対策方針が満たされていない場合に、O．ＲＥＳＯＵＲＣＥが有効に動作しない場合を考え、そのような状態でも異常を検出するための対策方針として、O．ＡＵＤＩＴをとっている。これによって、ＴＯＥが資源枯渇により正常に動作しなくなった場合の異常事象のログが残される。

上記の予防、検出の対策により、想定される脅威に適切に対抗している。

－　T．ＯＳに対する対策方針

ＯＥ．ＥＮＶによって、管理者はネットワーク経由でのＯＳへのログインが可能な利用者を管理している。O．ＡＴＴＲによって、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルが管理者のみアクセス可能となり、正当なアクセス権限をもったもののみアクセス可能である。また、

ＯＥ．ＯＳによって、データベーススペースに対するアクセス制御が行われ、管理者のみアクセス可能となる。そして、動作環境ファイルも、ＯＥ．ＥＮＶによって、管理者のみアクセス可能なアクセス制御が行われる。

これらにより、脅威Ｔ．ＯＳを抑止する対策をとっている。

さらに、ＯＥ．ＥＮＶによって管理者がバックアップリカバリ運用を実施しているので、リカバリ処理を行うことにより、データが破壊や改ざんされた場合も退避データから復旧することができる。

上記の予防、回復の対策により、想定される脅威に適切に対抗している。

－　Ｔ．ＤＡＴＡに対する対策方針

Ｏ．ＩＮＩＴによって、破棄される資源（データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル）はすべて初期化される。また、動作環境ファイルも、ＯＥ．ＥＮＶによって、管理者の責任で初期化を行う。従って、残存情報を参照することはできない。

上記の予防の対策により、想定される脅威に適切に対抗している。

８．２　セキュリティ要件根拠

セキュリティ対策方針に対するセキュリティ機能要件が、適切かつ十分なものであるかどうかを表８．２に示す。

表８．２　要件一覧（続く）

セキュリティ機能要件 ＼ セキュリティ対策方針		O・CONNECT	O・ACCESS	O・RESOURCE	O・ATTR	O・INIT	O・AUDIT	OE・CONNECT	OE・OS
認証、識別	FIA_AFL.1	✓							
	FIA_ATD.1		✓	✓					
	FIA_SOS.1	✓							
	FIA_UAU.2(1)	✓							
	FIA_UID.2(1)	✓							
	FIA_USB.1		✓	✓					
	FTA_TCH.1	✓							
アクセス制御	FDP_ACC.1(1)		✓						
	FDP_ACF.1(1)		✓						
	FDP_ACC.1(2)		✓						
	FDP_ACF.1(2)		✓						
資源量の制御	FRU_RSA.1			✓					
	FTA_MCS.2			✓					
資源保護	FMT_MTD.1(1)				✓				

表８．２　要件一覧（続き）

セキュリティ機能要件 ＼ セキュリティ対策方針		O・CONNECT	O・ACCESS	O・RESOURCE	O・ATTR	O・INIT	O・AUDIT	OE・CONNECT	OE・OS
残存情報保護	FDP_RIP.1					✓			
	FPT_RTP.1					✓			
監査	FAU_GEN.1						✓		
	FAU_GEN.2						✓		
	FAU_SAR.1						✓		
	FAU_SAR.2						✓		
	FAU_SAR.3						✓		
	FAU_SEL.1						✓		
	FAU_STG.1						✓		
	FAU_STG.3						✓		
	FAU_STG.4						✓		
セキュリティ管理	FMT_MOF.1	✓	✓	✓	✓	✓	✓		
	FMT_MSA.1		✓	✓					
	FMT_MSA.3(1)		✓						
	FMT_MSA.3(2)		✓						
	FMT_MTD.1(2)		✓						
	FMT_MTD.1(3)	✓	✓						
	FMT_MTD.1(4)					✓	✓		
	FMT_MTD.3	✓	✓			✓	✓		
	FMT_SAE.1	✓							
	FMT_SMF.1	✓	✓	✓		✓	✓		
	FMT_SMR.1(1)	✓	✓	✓	✓	✓	✓		
ＯＳに依存する機能	FMT_SMR.1(2)								✓
	FMT_MSA.3(3)								✓
	FPT_STM.1								✓
	FPT_RVM.1	✓	✓	✓	✓	✓	✓	✓	✓
	FIA_UAU.2(2)							✓	
	FIA_UID.2(2)							✓	
	FPT_SEP.1	✓	✓	✓	✓	✓	✓	✓	✓
	FDP_ACC.1(3)								✓
	FDP_ACF.1(3)								✓

－　全ての対策方針の前提となる機能要件

FPT_RVM.1 セキュリティ機能要件を採用することにより、ＴＯＥの各機能が利用されようとする際には、必ずセキュリティ機能が呼び出されるため、セキュリティ機能を迂回することはできない。

また、FPT_SEP.1 セキュリティ機能要件を採用することにより、ＴＯＥの動作空間において利用者

がアクセス可能な共用メモリとセキュリティ機能が動作するサーバプロセスが分離され、セキュリティ機能への不当な干渉を防ぐことができる。

これらにより、セキュリティ機能が迂回されたり干渉されたりせず、正しく動作する。

－ ＩＴ対策方針に対して採用する機能要件

・Ｏ．ＣＯＮＮＥＣＴに対して採用する機能要件

本ＴＯＥが安全にデータベースサービスを提供するためには、利用者に対してＴＯＥを使用させる前に利用者の身元を識別し、本人であることを認証しなければならない。

識別および認証では、以下の２つの方法がある。１つは、ＴＯＥが FIA_UID.2(1)セキュリティ機能要件に基づいてその利用者を識別し、その後、FIA_UAU.2(1)セキュリティ機能要件に基づき認証を行う。もう１つは結合時に識別情報および認証情報を指定しない場合で、ＯＥ．ＣＯＮＮＥＣＴに対して採用するセキュリティ機能要件に基づき識別認証を行う。この場合、ＴＯＥはＯＳから認証完了の情報を引き継ぎ、FIA_UID.2(1)セキュリティ機能要件に基づいて識別のみを行う。

FMT_MTD.1(3)セキュリティ機能要件により、管理者は全利用者の認証情報を、利用者は自分自身の認証情報を変更可能である。また、FIA_SOS.1 セキュリティ機能要件を採用することにより、認証情報は適切な複雑さを持ち、利用者が認証に連続して失敗した際には、FIA_AFL.1 セキュリティ機能要件に基づいて、その回数によって接続を拒否する。認証に成功した際には、FTA_TCH.1 セキュリティ機能要件を採用することによって過去の認証履歴を表示し、本人以外の利用の有無を確認できる。（なお、FTA_TCH.1 は拡張要件である。本来、FTA_TAH を使用したいが、FTA_TAH.1.2 の選択が「なし」となるため、新たに拡張している。FTA_TAH.1.2 を除いた点は、FTA_TAH と変わりない。）

そして、FMT_SMF.1 セキュリティ機能要件を採用することにより、セキュリティ機能、セキュリティ属性およびＴＳＦデータを管理する機能を持つ。FMT_MOF.1 セキュリティ機能要件を採用することにより、認証情報の有効期限や、認証の連続失敗回数を変更することなどができ、認証識別機能の振る舞いを改変できる。FMT_SAE.1 セキュリティ機能要件を採用することで、管理者は認証情報の有効期限を設定できるため、本人以外の利用者が認証情報を推測して利用することは困難となる。また、FMT_MTD.3 セキュリティ機能要件を採用することで、変更するＴＳＦデータの正当性もチェックされる。

なお、管理者、利用者という役割は、FMT_SMR.1(1)により維持される。

これらにより、利用者の確実な識別および認証が可能である。

・Ｏ．ＡＣＣＥＳＳに対して採用する機能要件

本ＴＯＥが安全にデータベースサービスを提供するためには、データベースとデータベースへの操作を制御し、ＴＯＥへの結合を許可した各利用者に対して、利用者毎の職務権限に応じた割当業務のみを遂行できるように制御するといったように必要最低限のアクセス権限のみを付与しなければならない。

まず、本ＴＯＥでは、利用者のアクセス制御を行う際には、FIA_ATD.1 セキュリティ機能要件を採用することによって、あらかじめ定義された利用者の利用可能な資源、操作方法が管理され、FIA_USB.1 セキュリティ機能要件により利用者と関連付けられる。アクセス制御は、この関連付けられた資源、操作方法に従って行われる。

FMT_MSA.3(1)セキュリティ機能要件を採用することにより、表のアクセス権限およびプロシジャの実行権限は、管理者に全て与えられており、FDP_ACC.1(1)および FDP_ACF.1(1)セキュリティ機能要件を採用することにより、管理者のデータベースへのアクセスが制御される。

また、FMT_MSA.3(2)セキュリティ機能要件を採用することにより、管理者のみ表のアクセス権限、及び、プロシジャの実行権限の初期値を指定でき、FMT_MSA.1 セキュリティ機能要件により、管理者のみ表のアクセス権限、及び、プロシジャの実行権限の変更を行える。FDP_ACC.1(2)および FDP_ACF.1(2)セキュリティ機能要件を採用することにより、利用者は管理者に付与された範囲でのみデータベースへのアクセスを行う。

そして、FMT_SMF.1 セキュリティ機能要件を採用することにより、セキュリティ機能、セキュリティ属性およびＴＳＦデータを管理する機能を持つ。FMT_MOF.1 セキュリティ機能要件により、管理者のみセキュリティ機能の振る舞いの管理を含むデータの保守を行える。また、FMT_MTD.1(2)および FMT_MTD.1(3)セキュリティ機能要件を採用することによって、管理者のみ権限情報、資源量や認証情報の管理を行うことができ、FMT_MTD.3 セキュリティ機能要件を採用することで、変更するこれらの値の正当性がチェックされる。

さらに、利用者に付与された権限情報や、使用可能な資源量、および識別認証情報は、FMT_MTD.1(3)セキュリティ機能要件により管理者は全利用者の情報を、利用者は自分に関する情報を参照することができる。なお、管理者、利用者という役割は、FMT_SMR.1(1)により維持される。

・Ｏ．ＲＥＳＯＵＲＣＥに対して採用する機能要件

本ＴＯＥが安定したデータベースサービスを提供維持するためには、各利用者が使用することができるデータベースを制御し、特定の利用者による資源の占有により、他利用者へのサービスが滞ることを防止することが必要不可欠である。

本ＴＯＥでは、識別および認証が完了し、利用者の資源量制御を行う際には、FIA_ATD.1 セキュリティ機能要件を採用することによって、あらかじめ定義された利用者の利用可能な資源量を管理され、FIA_USB.1 セキュリティ機能要件により利用者と関連付けられる。資源量制御は、この関連付けられた資源量に従って行われる。

FTA_MCS.2 セキュリティ機能要件を採用することにより、データベースサービスの使用を開始しようとする全ての利用者に対して、同時に開設することが可能なセション数を制限する。さらに、FRU_RSA.1 セキュリティ機能要件を採用することで、セション毎に使用することができる最大のＯＳ資源量を制限する。

また、本ＴＯＥは、FMT_SMF.1 セキュリティ機能要件を採用することにより、セキュリティ機能、セキュリティ属性およびＴＳＦデータを管理する機能を持つ。FMT_MOF.1 セキュリティ

機能要件を採用することにより、管理者のみセキュリティ機能の振る舞いの管理を行うことができる。セキュリティ機能の振る舞いの管理とは、セキュリティ機能の振る舞いを決定／改変することである。FMT_MSA.1 セキュリティ機能要件を採用することによって、管理者のみ利用者が使用可能な資源量の管理を行うことができる。なお、管理者という役割は、FMT_SMR.1(1)により維持される。

・Ｏ．ＡＴＴＲに対して採用する機能要件

本ＴＯＥが十分な信頼性を確保するためには、アクセス制御が行われるのに必要なアクセス権限を適切に設定し、正当なアクセス権限をもたない者が資源を盗み見る／改ざんすることを防止することが必要不可欠である。

本ＴＯＥでは、FMT_MTD.1(1)セキュリティ機能要件により、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルは管理者のみ読み出し可能である。従って、正当なアクセス権限をもったものだけがアクセス可能である。また、FMT_MOF.1 セキュリティ機能要件を採用することにより、管理者のみセキュリティ機能の振る舞いの管理を行うことができる。なお、管理者という役割は、FMT_SMR.1(1)により維持される。

・Ｏ．ＩＮＩＴに対して採用する機能要件

本ＴＯＥが十分な信頼性を確保するためには、利用者のプライバシ情報やＴＯＥの動作制御情報をＯＳ資源（ファイル）上で内部的に処理し、その使用済みとなったＯＳ資源にまで管理処理を施すことで、開放した資源に残存する秘匿情報を不当に参照されることを防止することが必要不可欠である。

本ＴＯＥでは、FDP_RIP.1 セキュリティ機能要件を採用することによりデータベーススペースを、FPT_RTP.1 セキュリティ機能要件を採用することによりディクショナリ、監査ログファイル、ログファイル、作業用ファイルを初期化している。これにより、データベースサービスを提供するために内部的に獲得したＯＳ資源（データベーススペース、ディクショナリ、監査ログファイル、ログファイル、作業用ファイル）が使用済みとなり、ＯＳへ返却する場合に秘匿データや内部制御情報が残存することはない。（なお、FPT_RTP.1 は拡張要件である。本来、FDP_RIP を使用したいが、FDP_RIP は TSF データを対象にしないため、新たに拡張している。対象が TSF データであることを除いた点は、FDP_RIP と変わりない。）

また、FMT_SMF.1 セキュリティ機能要件を採用することにより、セキュリティ機能、セキュリティ属性およびＴＳＦデータを管理する機能を持つ。FMT_MOF.1 セキュリティ機能要件を採用することにより、管理者のみセキュリティ機能の振る舞いの管理を行うことができる。セキュリティ機能の振る舞いの管理とは、セキュリティ機能を動作させる／停止することである。FMT_MTD.1(4)セキュリティ機能要件を採用することによって、管理者のみセキュリティパラメタによりＯＳへ返却する資源の初期化実施可否の管理を行うことができ、FMT_MTD.3 セキュリティ機能要件を採用することで、変更するセキュリティパラメタの正当性がチェックされる。なお、管理者という役割は、FMT_SMR.1(1)により維持される。

・Ｏ．ＡＵＤＩＴに対して採用する機能要件

本ＴＯＥが健全なデータベースサービスを維持するためには、データベースへのアクセスを監査記録として取得、その内容が十分であって改ざん等が行われていないことを保証し、また、その内容を閲覧、分析することにより不正なアクセスや動作異常を迅速に検出し、適切な処置を施すことが必要不可欠である。

まず、監査記録の取得であるが、本ＴＯＥでは、FAU_GEN.1 セキュリティ機能要件を採用することにより、データベースへの操作、および管理行為に関する記録を採取する。その記録には、FAU_GEN.2 セキュリティ機能要件に基づき、どの利用者、または管理者の操作の結果として監査対象事象が発生したのかも併せて記録される。また、FAU_SEL.1 セキュリティ機能要件に基づき、監査対象の目的に応じて効率的に監査記録を調査分析するための機構を有している。

また、監査記録の保証については、FAU_STG.1 セキュリティ機能要件を採用することにより、管理者のみ監査記録の初期化および削除を行うことで、不正な監査記録の削除に対処できる。また、FAU_STG.3 セキュリティ機能要件に基づき、監査記録の格納媒体として複数の監査記録データベースのエレメントを用意し、１つのエレメントが満杯になる毎にその旨をコンソールに出力するため、監査記録の満杯の危険を知ることができる。さらに、FAU_STG.4 セキュリティ機能要件に基づき、監査記録データベースが満杯になった場合に、古い監査記録データベースの上書き、コンソール出力、システムの停止のいずれかを行うため、監査記録が採られなくなることはない。

そして、監査記録の閲覧については、FAU_SAR.1 セキュリティ機能要件を採用することによる、管理者による本ＴＯＥへのアクセス状況のモニタリング、監査記録の監査、および FAU_SAR.2 セキュリティ機能要件に基づいた管理者以外の監査記録へのアクセス禁止を行い、監査分析行為を高精度かつ効率的に遂行するための監査記録データに対する整列や検索などの加工を行うために、FAU_SAR.3 セキュリティ機能要件を採用する。

さらに、本ＴＯＥは、FMT_SMF.1 セキュリティ機能要件を採用することにより、セキュリティ機能、セキュリティ属性およびＴＳＦデータを管理する機能を持つ。FMT_MOF.1 セキュリティ機能要件を採用することにより、管理者のみセキュリティ機能の振る舞いの管理を行うことができる。セキュリティ機能の振る舞いの管理とは、セキュリティ機能の振る舞いを決定／改変することである。FMT_MTD.1(4)セキュリティ機能要件を採用することによって、管理者のみ取得する監査情報、満杯になった場合の動作の選択を行うことができ、FMT_MTD.3 セキュリティ機能要件を採用することで、変更するこれらの値の正当性がチェックされる。

なお、管理者という役割は、FMT_SMR.1(1)により維持される。

これらにより、監査記録を確実に取得、閲覧が可能になる。

－　非ＩＴ対策方針に対して採用する機能要件

・ＯＥ．ＣＯＮＮＥＣＴに対して採用する機能要件

本ＴＯＥが安全にデータベースサービスを提供するためには、利用者に対してＴＯＥを使用さ

せる前に利用者の身元を識別し、本人であることを認証しなければならない。

識別および認証では、以下の２つの方法がある。１つはO．ＣＯＮＮＥＣＴに対して採用するセキュリティ機能要件に基づき識別認証を行う方法である。もう１つはＯＳへのログイン時に、FIA_UID.2(2)セキュリティ機能要件に基づいて識別を、FIA_UAU.2(2)セキュリティ機能要件に基づき認証を行う方法である。この場合、ＴＯＥはＯＳから認証完了の情報を引き継ぎ、Ｏ．ＣＯＮＮＥＣＴに対して採用するセキュリティ機能要件に基づき識別のみを行う。

・ＯＥ．ＯＳに対して採用する機能要件

本ＴＯＥが安定したデータベースサービスを提供維持するためには、ＴＯＥが動作する環境が適切であることが必要不可欠である（たとえばＲＤＢ２__ＴＣＰ連携を拒否するパラメタを設定する)。

本ＴＯＥでは、FMT_MSA.3(3) セキュリティ機能要件により、データベーススペースに対しては管理者のみアクセス可能であり、FDP_ACC.1(3)および FDP_ACF.1(3)セキュリティ機能要件により、データベーススペースに対してＯＳによるアクセス制御が行われる。なお、管理者という役割は、FMT_SMR.1(2)により維持される。

そして、認証情報の有効期限、認証履歴、監査記録の取得のためには、正確な時間情報が必要であるが、時間情報の取得はＯＳを利用するため、FPT_STM.1 セキュリティ機能要件を採用することにより、ＯＳの適切な管理の元で正確である。

これらにより、ＴＯＥが動作する適切な環境は維持される。

８．２．１　依存関係

セキュリティ要件に対する依存関係一覧を表８．３に示す。

表８．３　依存関係一覧（続く）

項番	セキュリティ機能要件		依存する要件	参照項番
1	認証、識別	FIA_AFL.1	FIA_UAU.2(1) ※１	4
2		FIA_ATD.1	なし	
3		FIA_SOS.1	なし	
4		FIA_UAU.2(1)	FIA_UID.2(1) ※１	5
5		FIA_UID.2(1)	なし	
6		FIA_USB.1	FIA_ATD.1	2
7		FTA_TCH.1	なし	
8	アクセス制御	FDP_ACC.1(1)	FDP_ACF.1(1)	9
9		FDP_ACF.1(1)	FDP_ACC.1(1) FMT_MSA.3(1)	8 28
10		FDP_ACC.1(2)	FDP_ACF.1(2)	11
11		FDP_ACF.1(2)	FDP_ACC.1(2) FMT_MSA.3(2)	10 29
12	資源量の制御	FRU_RSA.1	なし	
13		FTA_MCS.2	FIA_UID.2(1) ※１	5
14	資源保護	FMT_MTD.1(1)	FMT_SMR.1(1) FMT_SMF.1	36 35
15	残存情報保護	FDP_RIP.1	なし	
16		FPT_RTP.1	なし	
17	監査	FAU_GEN.1	FPT_STM.1	39
18		FAU_GEN.2	FAU_GEN.1 FIA_UID.2(1) ※１	17 5
19		FAU_SAR.1	FAU_GEN.1	17
20		FAU_SAR.2	FAU_SAR.1	19
21		FAU_SAR.3	FAU_SAR.1	19
22		FAU_SEL.1	FAU_GEN.1 FMT_MTD.1(2) FMT_MTD.1(4)	17 30 32
23		FAU_STG.1	FAU_GEN.1	17
24		FAU_STG.3	FAU_STG.1	23
25		FAU_STG.4	FAU_STG.1	23

表８．３　依存関係一覧（続き）

項番	セキュリティ機能要件		依存する要件	参照項番
26	セキュリティ管理	FMT_MOF.1	FMT_SMR.1(1) FMT_SMF.1	36 35
27		FMT_MSA.1	FMT_SMR.1(1) FDP_ACC.1(2) FMT_SMF.1	36 10 35
28		FMT_MSA.3(1) ※２	FMT_SMR.1(1)	36
29		FMT_MSA.3(2)	FMT_MSA.1 FMT_SMR.1(1)	27 36
30		FMT_MTD.1(2)	FMT_SMR.1(1) FMT_SMF.1	36 35
31		FMT_MTD.1(3)	FMT_SMR.1(1) FMT_SMF.1	36 35
32		FMT_MTD.1(4)	FMT_SMR.1(1) FMT_SMF.1	36 35
33		FMT_MTD.3	FMT_MTD.1(2) FMT_MTD.1(3) FMT_MTD.1(4) ADV_SPM.1	30 31 32 －
34		FMT_SAE.1	FMT_SMR.1(1) FPT_STM.1	36 39
35		FMT_SMF.1	なし	
36		FMT_SMR.1(1)	FIA_UID.2(1) ※１	5
37	ＯＳに依存する機能	FMT_SMR.1(2)	FIA_UID.2(2) ※１	42
38		FMT_MSA.3(3) ※２	FMT_SMR.1(2)	37
39		FPT_STM.1	なし	
40		FPT_RVM.1	なし	
41		FIA_UAU.2(2)	FIA_UID.2(2) ※１	42
42		FIA_UID.2(2)	なし	
43		FPT_SEP.1	なし	
44		FDP_ACC.1(3)	FDP_ACF.1(3)	45
45		FDP_ACF.1(3)	FDP_ACC.1(3) FMT_MSA.3(3)	44 38

上記の依存関係を確認した。

※１本来依存する要件は FIA_UID.1 および FIA_UAU.1 だが、本ＴＯＥのセキュリティ機能は FIA_UID.2 および FIA_UAU.2 を必要とするため、ここでは FIA_UID.2 および FIA_UAU.2 としている。

※２FMT_MSA.3(1)および FMT_MSA.3(3)のセキュリティ属性は固定であり、変更は行われないものであるため、FMT_MSA.1 への依存関係を構築しないものとする。

８．２．２　相互支援

セキュリティ機能要件に対する相互支援一覧を表８．４に示す。

表８．４　相互支援一覧

セキュリティ機能要件		防御を提供している要件		
		迂回抑止	干渉抑止	非活性化抑止
認証、識別	FIA_AFL.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FIA_ATD.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FIA_SOS.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FIA_UAU.2(1)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FIA_UID.2(1)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FIA_USB.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FTA_TCH.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
アクセス制御	FDP_ACC.1(1)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FDP_ACF.1(1)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FDP_ACC.1(2)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FDP_ACF.1(2)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
資源量の制御	FRU_RSA.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FTA_MCS.2	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
資源保護	FMT_MTD.1(1)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
残存情報保護	FDP_RIP.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FPT_RTP.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
監査	FAU_GEN.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_GEN.2	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_SAR.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_SAR.2	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_SAR.3	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_SEL.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_STG.1	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_STG.3	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FAU_STG.4	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
セキュリティ管理	FMT_MOF.1	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_MSA.1	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_MSA.3(1)	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_MSA.3(2)	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_MTD.1(2)	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_MTD.1(3)	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_MTD.1(4)	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FMT_MTD.3	FPT_RVM.1	FPT_SEP.1	FMT_MOF.1
	FMT_SAE.1	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_SMF.1	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_SMR.1(1)	FPT_RVM.1	FPT_SEP.1	N/A
ＯＳに依存する機能	FMT_SMR.1(2)	FPT_RVM.1	FPT_SEP.1	N/A
	FMT_MSA.3(3)	FPT_RVM.1	FPT_SEP.1	N/A
	FPT_STM.1	FPT_RVM.1	FPT_SEP.1	N/A
	FPT_RVM.1	N/A	FPT_SEP.1	N/A
	FIA_UAU.2(2)	FPT_RVM.1	FPT_SEP.1	N/A
	FIA_UID.2(2)	FPT_RVM.1	FPT_SEP.1	N/A
	FPT_SEP.1	FPT_RVM.1	N/A	N/A
	FDP_ACC.1(3)	FPT_RVM.1	FPT_SEP.1	N/A
	FDP_ACF.1(3)	FPT_RVM.1	FPT_SEP.1	N/A

各機能が動作する場合、最初にセキュリティ機能が呼び出され、成功した場合にのみ、その動作進行

が許可されることによって、迂回を抑止している。また、利用者が処理を行う空間と、ＴＯＥが動作する空間を分離することによって、各種機能への干渉を抑止している。さらに、セキュリティ機能のふるまいの管理を管理者のみに許可することによって、セキュリティ機能が非活性化されることを抑止している。

８．２．３　ＴＯＥ保証要件根拠

ＳｙｍｆｏＷＡＲＥは一般のコマーシャルシステムの中で利用される。ＳｙｍｆｏＷＡＲＥは企業の秘密情報や顧客データなどのプライバシー情報の管理を行う。このため信頼性確保が必要になるため、ＥＡＬ４を品質保証レベルとする。なお、ＥＡＬ４を超える特定の保証対策はない。

８．２．４　機能強度根拠

ＳｙｍｆｏＷＡＲＥは一般のコマーシャルシステムの中で利用されることを想定しているため、想定される不正行為は、公開情報を利用した攻撃である。このため、攻撃者の攻撃力は”低レベル”である。

攻撃者は認証を迂回してＳｙｍｆｏＷＡＲＥを利用することはできず、低レベルの攻撃能力を持つ攻撃者からの公開情報を利用した不正行為に対抗できるため、ＳｙｍｆｏＷＡＲＥの最小機能強度レベルは”ＳＯＦ-basic”である。

８．３　ＴＯＥ要約仕様根拠

セキュリティ機能要件とセキュリティ仕様概要の対応関係一覧を表８．５に示す。

表８．５　対応関係一覧（続く）

セキュリティ機能要件 ＼ セキュリティ仕様概要		F・SEL・PARA	F・USER・DEF	F・USER・AUTHEN	F・USER・PRIV	F・USER・RES	F・USER・REF	F・RES・ATTR	F・RES・INIT	F・AUDIT・COL	F・AUDIT・VIEW	F・AUDIT・SPACE
認証・識別	FIA_AFL.1			✓								
	FIA_ATD.1		✓		✓	✓						
	FIA_SOS.1			✓								
	FIA_UAU.2(1)			✓								
	FIA_UID.2(1)			✓								
	FIA_USB.1				✓	✓						
	FTA_TCH.1			✓								
アクセス制御	FDP_ACC.1(1)				✓							
	FDP_ACF.1(1)				✓							
	FDP_ACC.1(2)				✓							
	FDP_ACF.1(2)				✓							
資源量の制御	FRU_RSA.1					✓						
	FTA_MCS.2					✓						
資源保護	FMT_MTD.1(1)							✓				
残存情報保護	FDP_RIP.1								✓			
	FPT_RTP.1								✓			
監査	FAU_GEN.1									✓		
	FAU_GEN.2									✓		
	FAU_SAR.1										✓	
	FAU_SAR.2										✓	
	FAU_SAR.3										✓	
	FAU_SEL.1									✓		
	FAU_STG.1											✓
	FAU_STG.3											✓
	FAU_STG.4											✓

表８．５　対応関係一覧（続き）

セキュリティ機能要件 ＼ セキュリティ仕様概要		F・SEL・PARA	F・USER・DEF	F・USER・AUTHEN	F・USER・PRIV	F・USER・RES	F・USER・REF	F・RES・ATTR	F・RES・INIT	F・AUDIT・COL	F・AUDIT・VIEW	F・AUDIT・SPACE
セキュリティ管理	FMT_MOF.1	✓			✓							
	FMT_MSA.1			✓	✓	✓						
	FMT_MSA.3(1)				✓							
	FMT_MSA.3(2)				✓							
	FMT_MTD.1(2)	✓			✓							✓
	FMT_MTD.1(3)		✓	✓	✓		✓					
	FMT_MTD.1(4)	✓			✓						✓	✓
	FMT_MTD.3	✓	✓	✓	✓							
	FMT_SAE.1			✓								
	FMT_SMF.1	✓			✓	✓					✓	✓
	FMT_SMR.1(1)		✓									

なお、セキュリティ保証要件については、表６．２に示すように、すべてのＴＯＥセキュリティ保証要件は保証手段として示されたドキュメントのセットにより対応される。

また、保証手段として示された各ドキュメントにより、本セキュリティターゲットが規定したＴＯＥセキュリティ保証要件が要求する事項を満たしている。

認証・識別に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

- FIA_AFL.1

  本セキュリティ機能要件では、利用者の認証における連続した認証の失敗時に、その回数によって接続を拒否できる必要がある。

  セキュリティ機能 F.USER.AUTHEN は、管理者が利用者に対し連続失敗回数を設定し、認証時にその数に超えた場合、認証情報を無効化できるため、セキュリティ機能要件を満足している。

- FIA_ATD.1

  本セキュリティ機能要件では、管理者は利用者に対する利用可能範囲を維持できる必要がある。

  セキュリティ機能 F.USER.DEF は利用者登録する際に、利用可能範囲を設定できる。

  セキュリティ機能 F.USER.PRIV によって、管理者はデータベースにアクセスする権限を利用者

に対して付与することができ、セキュリティ機能 F.USER.RES によって各利用者が使用可能な資源量を制限することができる。

これら３つのセキュリティ機能の組み合わせによって、管理者は利用者に対してその利用可能範囲を維持でき、セキュリティ機能要件を満足している。

- FIA_SOS.1

本セキュリティ機能要件では、利用者が指定する認証情報について、ある程度の複雑さをもたなければならない。

セキュリティ機能 F.USER.AUTHEN は、認証情報が文字列長や類似性について、ある程度の複雑さを持たない場合、認証情報の登録を拒否するため、セキュリティ機能要件を満足している。

- FIA_UAU.2(1)

本セキュリティ機能要件では、ＴＯＥの利用前に利用者が識別された利用者本人であることを確認できる必要がある。

セキュリティ機能 F.USER.AUTHEN は、ＴＯＥの利用前に識別された利用者の認証情報による確認を行うため、セキュリティ機能要件を満足している。

- FIA_UID.2(1)

本セキュリティ機能要件では、ＴＯＥの利用前に利用者を識別できる必要がある。

セキュリティ機能 F.USER.AUTHEN は、ＴＯＥの利用前に利用者の識別を行うため、セキュリティ機能要件を満足している。

- FIA_USB.1

本セキュリティ機能要件では、利用者にその利用者のセキュリティ属性を関連付ける必要がある。

セキュリティ機能 F.USER.PRIV で、利用者は管理者に与えられた権限の範囲で表の操作やプロシジャの実行を行う。

セキュリティ機能 F.USER.RES は、利用者は管理者により制限された資源量の範囲で表の操作やプロシジャの実行を行う。

以上２つのセキュリティ機能により、表の操作やプロシジャの実行時には利用者のセキュリティ属性が関連付けられているため、セキュリティ機能要件を満足している。

- FTA_TCH.1

本セキュリティ機能要件では、利用者の過去の認証履歴を表示できる必要がある。

セキュリティ機能 F.USER.AUTHEN は、利用者の最終成功結合の日時および最終成功結合の日時以降の失敗回数の表示を行うことができるため、セキュリティ機能要件を満足している。

アクセス制御に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおり

である。

- FDP_ACC.1(1)

  本セキュリティ機能要件では、管理者は全ての資源に対する全ての操作を実行できる必要がある。

  セキュリティ機能 F.USER.PRIV では、サーバプロセスは、管理者のプロセスからのデータベースへのアクセス要求に対し、全ての資源に対する全ての操作を実行するので、セキュリティ機能要件を満足している。

- FDP_ACF.1(1)

  本セキュリティ機能要件では、管理者は全ての資源に対する全ての操作を常に実行できる必要がある。

  セキュリティ機能 F.USER.PRIV では、サーバプロセスは、管理者のプロセスからのデータベースへのアクセス要求に対し、全ての資源に対する全ての操作を実行するので、セキュリティ機能要件を満足している。

- FDP_ACC.1(2)

  本セキュリティ機能要件では、利用者は、管理者に付与された権限の範囲内で資源に対する操作を行う必要がある。

  セキュリティ機能 F.USER.PRIV では、サーバプロセスは、利用者のプロセスからのデータベースへのアクセス要求に対し、その利用者が管理者から付与されたデータベースに対する操作の権限の範囲でのみデータベースに対する操作を行うため、セキュリティ機能要件を満足している。

- FDP_ACF.1(2)

  本セキュリティ機能要件では、利用者は、管理者に付与された権限の範囲内で資源に対する操作を行う必要がある。

  セキュリティ機能 F.USER.PRIV では、サーバプロセスは、利用者のプロセスからのデータベースへのアクセス要求に対し、その利用者が管理者から付与されたデータベースに対する操作の権限の範囲でのみデータベースに対する操作を行うため、セキュリティ機能要件を満足している。

資源量の制御に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

- FRU_RSA.1

  本セキュリティ機能要件では、各利用者が１つのセションで利用可能なメモリ量、ファイル量の制限が行える必要がある。

  セキュリティ機能 F.USER.RES は、管理者がセキュリティパラメタに適切な値を指定することで、一人の利用者が１つのセションで利用可能なメモリ量、ファイル量を制限することができ、セキュリティ機能要件を満足している。

- FTA_MCS.2

  本セキュリティ機能要件では、各利用者が同時に利用可能なセション数の制限が行える必要がある。

  セキュリティ機能 F.USER.RES は、管理者がセキュリティパラメタに適切な値を指定することで、一人の利用者が同時に利用可能なセション数を制限することができ、セキュリティ機能要件を満足している。

資源保護に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

- FMT_MTD.1(1)

  本セキュリティ機能要件では、管理者にのみ TSF データに対する読み出し可能な属性の設定が行われる必要がある。

  セキュリティ機能 F.RES.ATTR によって、ディクショナリ、監査ログファイル、ログファイル、作業用ファイルは管理者のみ読み出し可能であり、セキュリティ機能要件を満足している。

残存情報保護に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

- FDP_RIP.1

  本セキュリティ機能要件では、ＴＯＥが獲得し、使用を終えた利用者のデータを含む資源をＯＳに返却する際、その内容が初期化されている必要がある。

  セキュリティ機能 F.RES.INIT によって、ＴＯＥがＯＳから獲得し、使用済みとなった資源データベーススペースは、ＯＳへの返却前に初期化しているため、セキュリティ機能要件を満足している。

- FPT_RTP.1

  本セキュリティ機能要件では、ＴＯＥが獲得し、使用を終えた TSF データをＯＳに返却する際、その内容が初期化されている必要がある。

  セキュリティ機能 F.RES.INIT によって、ＴＯＥがＯＳから獲得し、使用済みとなったディクショナリ、監査ログファイル、ログファイル、作業用ファイルは、ＯＳへの返却前に初期化しているため、セキュリティ機能要件を満足している。

監査に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

- FAU_GEN.1

  本セキュリティ機能要件では、監査対象事象について、監査記録を取得可能である必要がある。

  セキュリティ機能 F.AUDIT.COL によって、監査記録は本セキュリティ機能要件で定義した情報が常に取得可能であり、セキュリティ機能要件を満足している。

- FAU_GEN.2

  本セキュリティ機能要件では、監査対象事象について、その事象を誰が発生させたか記録する必要がある。

  セキュリティ機能 F.AUDIT.COL によって、取得する監査記録には、管理者または利用者名が常に記録されるため、セキュリティ機能要件を満足している。

- FAU_SAR.1

  本セキュリティ機能要件では、管理者のみ監査記録を読み出すことが可能である必要がある。

  セキュリティ機能 F.AUDIT.VIEW は､監査記録データベースに対する属性として管理者のみアクセス可としているため、管理者のみ読み出すことができる。さらに、管理者以外のデータベース操作を全て不可能にすることにより管理者の監査記録読み出しの妨害に対抗することもできるため、セキュリティ機能要件を満足している。

- FAU_SAR.2

  本セキュリティ機能要件では、管理者以外の利用者は、読み出しが失敗する必要がある。

  セキュリティ機能 F.AUDIT.VIEW は､監査記録データベースに対する属性として管理者のみアクセス可としているため、利用者のアクセスは拒否される。

  これによりセキュリティ機能要件を満足している。

- FAU_SAR.3

  本セキュリティ機能要件では、取得した監査記録について、検索、分類、並べ替えして読み出せる必要がある。

  セキュリティ機能 F.AUDIT.VIEW は、データベース形式の監査記録に対して、監査記録の参照時には、ＳＱＬ文を用いることで、その取り出しおよび整列を行うことを可能としているため、セキュリティ機能要件を満足している。

- FAU_SEL.1

  本セキュリティ機能要件では、取得する監査記録について、取得内容を選択できる必要がある。

  セキュリティ機能 F.AUDIT.COL によって取得する監査記録の範囲を変更できるため、セキュリティ機能要件を満足している。

- FAU_STG.1

  本セキュリティ機能要件では、監査記録が削除されてはならない。

  セキュリティ機能 F.AUDIT.SPACE では、管理者のみ監査記録の初期化、削除を行えるため、監査記録の不当な削除は行えない。

  これによりセキュリティ機能要件を満足している。

- FAU_STG.3

本セキュリティ機能要件では、監査記録が満杯に近づいた場合、警告が行われなければならない。

セキュリティ機能 F.AUDIT.SPACE では、監査記録データベースのエレメントは複数持つことができ、１つのエレメントが満杯になるたびにコンソールにメッセージを出力することで、管理者は監査記録が満杯に近づいていることを知ることができる。

これによりセキュリティ機能要件を満足している。

- FAU_STG.4

本セキュリティ機能要件では、監査記録が満杯になった場合の振る舞いについて決定し、監査記録の取得を失敗してはならない。

セキュリティ機能 F.AUDIT.SPACE は、監査記録が満杯になった場合、管理者がセキュリティパラメタに設定した内容に従うことによって満杯時の動作を決定し、監査ログの損失を防ぐことができ、セキュリティ機能要件を満足している。

セキュリティ管理に関するセキュリティ機能要件と、それを満たすセキュリティ仕様概要は以下のとおりである。

- FMT_MOF.1

本セキュリティ機能要件では、管理者によってのみ、セキュリティの振る舞いが決定／変更され、また、動作／停止が行われる必要がある。

セキュリティの振る舞いの決定／変更、あるいは動作／停止はセキュリティパラメタの設定により行われる。セキュリティ機能 F.SEL.PARA によって、管理者のみセキュリティパラメタを設定することが可能であり、また、セキュリティパラメタの設定を含むデータの保守は、セキュリティ機能 F.USER.PRIV によって管理者のみ行うことが可能である。

以上２つのセキュリティ機能により、管理者によってのみ、セキュリティの振る舞いが決定／変更され、また、動作／停止が行われるため、セキュリティ機能要件を満足している。

- FMT_MSA.1

本セキュリティ機能要件では、利用者と利用者が利用可能な資源、それに対する操作や、資源量を管理できるのは管理者のみでなくてはならない。

セキュリティ機能 F.USER.PRIV によって、管理者のみ利用者に対しデータベースに対する操作の権限付与および剥奪を行うことができる。

セキュリティ機能 F.USER.RES によって、管理者のみ利用者が使用可能な資源量を制限できる。

セキュリティ機能 F.USER.AUTHEN によって、管理者のみ認証情報の有効期限を管理できる。

以上３つのセキュリティ機能により、セキュリティ機能要件を満足している。

- FMT_MSA.3(1)

本セキュリティ機能要件では、管理者が利用可能な資源、それに対する操作の初期値が設定され

変更できない必要がある。

セキュリティ機能 F.USER.PRIV によって、管理者に対する初期値として、全ての表やプロシジャに対して全ての操作を行うように設定され、その初期値を変更することはできないため、セキュリティ機能要件を満足している。

- FMT_MSA.3(2)

本セキュリティ機能要件では、利用者が利用可能な資源、それに対する操作の初期値が設定され変更できない必要がある。

利用者が利用可能な資源、それに対する操作の初期値は、セキュリティ機能 F.USER.PRIV によって、全ての表やプロシジャに対する全ての操作が不可能に設定されており、その初期値を変更することはできないため、セキュリティ機能要件を満足している。

- FMT_MTD.1(2)

本セキュリティ機能要件では、ＴＳＦデータの初期値変更、削除が可能なのは管理者のみでなくてはならない。

セキュリティ機能 F.SEL.PARA によって、管理者のみセキュリティパラメタを変更することにより、全利用者共通の使用可能資源量、同時使用セション数、認証が不成功回数となることができる閾値、認証情報の寿命の初期値の変更が可能である。

セキュリティ機能 F.USER.PRIV によって、管理者のみデータの保守を行うためのコマンドを使用することでログファイルの削除が可能である。

セキュリティ機能 F.AUDIT.SPACE によって、管理者のみ監査記録の削除を行える。

以上３つのセキュリティ機能により、ディクショナリ、監査ログファイル、ログファイルの初期値変更、削除が行えるのは管理者のみであるため、セキュリティ機能要件を満足している。

- FMT_MTD.1(3)

本セキュリティ機能要件では、利用者毎のＴＳＦデータの問い合わせ、改変が可能なのは、管理者および、そのセキュリティ属性に関連付けられた利用者のみでなくてはならない。

セキュリティ機能 F.USER.DEF によって、利用者の登録、変更、および削除を行うことにより、管理者のみ識別情報の変更が行える。

セキュリティ機能 F.USER.PRIV によって、アクセス権限を変更可能なのは管理者のみである。

セキュリティ機能 F.USER.REF によって、管理者は、全利用者の識別認証情報、権限情報、使用可能資源量を、利用者は、自分に関する識別認証情報、権限情報、使用可能資源量のみ参照できる。

セキュリティ機能 F.USER.AUTHEN によって、管理者は、全利用者の認証情報を、利用者は、自分の認証情報を変更できる。

以上４つのセキュリティ機能により、管理者は、全利用者の認証情報、権限情報、セキュリティパラメタ（使用可能資源量など利用者毎にあるもの）の問い合わせ、改変が可能であり、利用者は、自分自身の識別認証情報、権限情報、およびセキュリティパラメタ（使用可能資源量など利用者毎

にあるもの）の問い合わせ、改変が可能であるため、セキュリティ機能要件を満足している。

- FMT_MTD.1(4)

本セキュリティ機能要件では、ＴＳＦデータの問い合わせ、改変が可能なのは管理者のみでなくてはならない。

セキュリティ機能 F.SEL.PARA によって、管理者のみセキュリティパラメタを変更することが可能である。

セキュリティ機能 F.USER.PRIV によって、セキュリティパラメタにアクセス可能なのは管理者のみである。

セキュリティ機能 F.AUDIT.VIEW は、監査記録データベースに対する属性として管理者のみアクセス可としているため、管理者のみ読み出すことができる。

セキュリティ機能 F.AUDIT.SPACE では、管理者のみ監査記録の初期化を行える。

以上４つのセキュリティ機能により、ディクショナリ、監査ログファイル、ログファイルの問い合わせ、改変が可能なのは管理者のみであるため、セキュリティ機能要件を満足している。

- FMT_MTD.3

本セキュリティ機能要件では、ＴＳＦデータに対して設定される値はセキュアでなくてはならない。

セキュリティ機能 F.SEL.PARA によって、セキュリティパラメタの値がセキュアな値かどうかチェックされる。

セキュリティ機能 F.USER.DEF によって、識別情報がＴＯＥに登録可能な識別情報かチェックされる。

セキュリティ機能 F.USER.AUTHEN によって、認証情報が使用可能な認証情報かチェックされる。

セキュリティ機能 F.USER.PRIV によって、付与しようとする対象の資源および操作が適切かチェックされる。

以上４つのセキュリティ機能により、セキュリティパラメタ、権限情報、および識別認証情報に対して設定される値はセキュアである。

また、ディクショナリ（セキュリティパラメタ、権限情報、および識別認証情報を除く）、監査ログファイル、ログファイル、作業用ファイルに値を設定する場合、ＴＯＥ自身により値を設定するフォーマットが生成され、セキュアでない値が設定されないようにチェックしているため、常にセキュアである。

以上により、ＴＳＦデータに対して設定される値はセキュアであり、セキュリティ機能要件を満足している。

- FMT_SAE.1

本セキュリティ機能要件では、管理者は認証情報に有効期限を設けることが可能である必要があ

る。

セキュリティ機能 F.USER.AUTHEN によって、管理者は、利用者の認証情報に有効期限を設定することができるため、セキュリティ機能要件を満足している。

- FMT_SMF.1

本セキュリティ機能要件では、表５．３で与えられる管理項目の管理が行える。

セキュリティ機能 F.SEL.PARA および F.USER.RES によって、管理者のみセキュリティパラメタやセキュリティ属性を変更することが可能である。

同様に、セキュリティ機能 F.USER.PRIV によって、管理者のみセキュリティパラメタの閲覧およびデータの保守を行うことが可能である。監査記録についても、セキュリティ機能 F.AUDIT.VIEW によって、監査記録データベースに対する属性として管理者のみアクセス可としているため、管理者のみ読み出すことができ、セキュリティ機能 F.AUDIT.SPACE によって、管理者のみ監査記録の初期化、削除を行える。

以上５つのセキュリティ機能により、表５．３で与えられる管理項目の管理が行えるため、セキュリティ機能要件を満足している。

- FMT_SMR.1(1)

本セキュリティ機能要件では、管理者、利用者という役割が維持される必要がある。

セキュリティ機能 F.USER.DEF によって、管理者は管理者として登録され、利用者は管理者により利用者として登録されるため、セキュリティ機能要件を満足している。

８．３．１　機能強度仕様根拠

ＳｙｍｆｏＷＡＲＥは、OS である Solaris™ 7 Operating Environment 上で動作し、本 OS と分担、連携して識別認証を実施している。このため、本 OS が求められている機能強度（参考として、Solaris™ 8 Operating Environment の機能強度はＳＯＦ-medium である）と均衡をとるために、認証の機能強度を”ＳＯＦ-medium”としている。

８．４　ＰＰ主張根拠

PP 準拠なし。

【用 語】

アプリケーション

本書では、利用者が作成するアプリケーションプログラムすべてを指す。

エレメント

本書では、監査ログエレメントを指す。監査ログ表は、複数の DSI に分割されている。この監査ログ表の DSI を監査ログエレメント(または略してエレメント)と呼ぶ。

監査ログ

日常の管理者および利用者の監視や、セキュリティ上の問題が発生した場合の原因を特定するための情報として、利用者の行った処理、管理者の行った処理、発生した異常な事象をログとして残している。このログを監査ログと呼ぶ。

管理者

本書では、SymfoWARE を管理する管理者を指す。また、SymfoWARE の管理者はＯＳの管理者でもある。

コマンド

本書では、SymfoWARE を運用するためのコマンドを指す。

共用メモリ

プロセス間で相互に参照が可能なメモリ領域をいう。

サーバプロセス

本書では、アプリケーションやコマンドの処理を行う SymfoWARE のプロセスを指す。

作業用ファイル

作業用テーブルおよび作業用ソート領域を指す。

スーパユーザ

UNIX システムを管理する特別の権限を持ったシステム管理者のことを指す。

スレッド

プロセス内で実行されるサブプロセスを指す。

責任者

本書では、セキュリティシステムの全責任を担う責任者を指す。責任者は、ふさわしい管理者の選任、管理者の教育等を行う必要がある。

セキュリティパラメタ

セキュリティシステムにおいて、SymfoWARE のアクセスを制約する各種パラメタを指す。

セション

SymfoWARE に結合した時点から結合解除までの間を指す。

データベース

相互に関連するデータを整理・統合し，検索しやすくしたファイル。また，このようなファイルの共用を可能にするシステム。

データベーススペース

利用者のデータが格納されているファイル。データベーススペースには、論理的なアクセスの単位である表が格納されており、利用者のデータは、この表に格納される。

ディクショナリ

利用者が作成したデータベースに対して、データベースの論理構造／格納構造／物理構造に関する情報が格納されている。実際は、SymfoWARE の RDB ディクショナリと RDB ディレクトリファイルがあり、RDB ディクショナリは、SQL で利用者によりアクセスされるものであり、RDB ディレクトリファイルは、SymfoWARE が内部的に使用するものである。

動作環境ファイル

アプリケーションの実行時の動作環境を規定するためのファイル。

トランザクション

データベースのアクセスにおける一連のデータ操作の一貫性を保証する単位をトランザクションと呼ぶ。

並列クエリ

大量データを扱う業務の情報処理効率を上げるために、データベースを複数の DSI に分割し、それぞれを並列に処理する機能である。

標準運用

利用者に対する権限付与の制御による機密保護レベルのセキュリティ運用を指す。

標準セキュリティ運用

監査ログの取得、利用者への機能制限や資産へのアクセスの制限など、データベースシステム全体としてセキュリティ強度の高いセキュリティ運用を指す。本書では、標準セキュリティ運用を設定することを前提として説明している。

ファイル

本書では、ファイルシステム上のファイルとローデバイスの両方を指す。

プロシジャ

サーバに登録する処理手続きを指す。プロシジャルーチンを呼び出し、サーバ側で一連のトランザクション処理を実行することで、性能限界解消を図る。

プロセス

UNIX システムの仕事の単位を指す。

プロトコル

データ通信を行うため、あらかじめ定めておく規約。信号送信の手順、データの表現法、誤り検出法などを定める。通信規約。

利用者

本書では、SymfoWARE を利用する一般利用者を指す。

リレーショナルデータベース

SymfoWARE が採用しているデータベースである。リレーショナルデータベースでは、データを行と列からなる二次元の表で表現する。データベース操作は、データベース言語 SQL で行う。

ローデバイス

UNIX ファイルシステムとは関係なくデータ操作することのできるディスク領域のこと。

ログファイル

ログファイルには、テンポラリログファイルおよびアーカイブログファイルがある。テンポラリログファイルには、データベースの更新履歴が収集される。アーカイブログファイルには、トランザクションの更新履歴が収集される。

ALTER USER 文

利用者変更文。利用者の属性を変更する DDL 文。

CREATE USER 文

利用者定義文。データベースシステムにアクセスする利用者を定義する DDL 文。

DDL 文

データ定義文。データベースの作成、削除等に使用する SQL 文。

DELETE 権

表の行を削除するための権限。

DML 文

データ操作文。データベースの参照、追加、削除および更新に使用する SQL 文。

DROP USER 文

利用者削除文。利用者の定義を削除する DDL 文。

DSI

表のデータを格納する領域を、データベーススペースに割付けるために定義するもの。

EXECUTE 権

プロシジャルーチンを実行するための権限。

GRANT 文

利用者に対して権限を付与する DDL 文。

INSERT 権

表に行を挿入するための権限。

RDB

Relational DataBase の省略形。リレーショナルデータベースに同じ。

RDB2_TCP 連携

TCP/IP 接続を使用して SymfoWARE と連携することを意味する。

REVOKE 文

利用者に対して付与した権限を剥奪する DDL 文。

SELECT 権

表の行を参照するための権限。

SET SYSTEM PARAMETER 文

セキュリティパラメタを設定するための DDL 文。

SQL

国際標準のリレーショナルデータベース操作言語であり、データベースの構造を定義するＤＤＬ(Data Definition Language)とデータベースへのデータの入力、登録、更新、変更、削除、検索などの操作を行うＤＭＬ(Data Manipulation Language)より構成される。

TCP/IP

Transmission Control Protocol/Internet Protocol の省略形。通信プロトコル。インターネットの標準プロトコルであり、現在最も普及しているプロトコル。

UPDATE 権

表の行を更新するための権限。

XA インタフェース

分散トランザクション処理モデルでのトランザクションモニタと、リレーショナルデータベース管理システムとの連携インタフェースを XA インタフェースと呼ぶ。XA インタフェースは、実質的な UNIX の標準を制定する団体 X/Open が規定している。

XA 連携

XA インタフェースを使用して SymfoWARE と連携することを意味する。

【略 語】

CC コモンクライテリア(Common Criteria)

EAL 評価保証レベル（Evaluation Assurance Level ）

IT 情報技術（Information Technology ）

PP プロテクションプロファイル（Protection Profile ）

SF セキュリティ機能（Security Function ）

SFP セキュリティ機能方針（Security Function Policy ）

SOF 機能強度（Strength of Function ）

ST セキュリティターゲット（Security Target ）

TOE 評価対象（Target of Evaluation ）

TSC TSF 制御範囲（TSF Scope of Control ）

TSF TOE セキュリティ機能（TOE Security Functions ）

TSFI TSF インタフェース（TSF Interface ）

TSP TOE セキュリティ方針（TOE Security Policy ）