

文書管理番号	Symfo-07-DS4001
--------	-----------------

Symfoware セキュリティターゲット

第 3. 2 版

発行日:2007 年 12 月 26 日

富士通株式会社

保管期間	次期改版時
------	-------

全ページ数	109 ページ
-------	---------

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-07-DS4001		
版数	更新日	更新箇所	更新内容(概要)	更新者	承認者
1.0	2006.05.19	全体	新規作成 V4 の ST に対して下記の点を修正 - 製品の識別情報の変更 - 動作 OS の変更 - パッケージ名の変更 - 権限の操作に関する記述の追加 - CC2.3 の適用による変更 評価保証レベルの変更	鎌倉	安永課長
1.1	2006.06.20	2.4.2 2.5	シーケンス、ファンクションの説明不足対処 - 機能概要にシーケンス、ファンクションの説明を追加 TOE 保護資産に識別されたファイルとシーケンス、ファンクションの関係を明確化	鎌倉	安永課長
1.2	2006.07.11	6.1.2	シーケンス、ファンクション権限制御の対象資源の説明不足対処 - 対象者、権限、操作、資源の説明表中、シーケンス、プロシジャ、ファンクションの操作対象資源としてディクショナリを追加	鎌倉	安永課長
1.3	2006.07.31	5.1.1.1 5.1.1.6 5.2.1 表 5.3 表 5.4 8.2.3	CC2.3 適用修正漏れ対処 - CC2.3 の適用による変更(FIA_USB.1, FAU_STG.1.2, FIA_UAU.2) 評価保証レベル変更の考慮漏れ対処 - 8.2.3 TOE 保証要件根拠の内容修正	鎌倉	安永課長
1.4	2006.09.11	6.2	適切な保証手段に修正 - AGD 保証手段にメッセージ集を追加 - AGD 保証手段から RDB 運用ガイドを削除	鎌倉	安永課長
1.5	2006.09.19	更新履歴表	更新内容(概要)に修正理由を明記	鎌倉	安永課長
2.0	2006.10.31	全体	新規作成 V7 の ST に対して下記の点を修正 - 製品の識別情報の変更 - パッケージバージョンの変更 - 評価保証レベルの変更	鎌倉	安永課長
2.1	2007.02.05	6.2	保証手段のドキュメント名称誤りを修正 - ACM 保証手段 提供管理システム利用手引書(開発者編)	鎌倉	安念課長

2.2	2007.04.17	6.2	表 6.2 脆弱性評価の保証手段に以下を追加 「アプリケーション開発ガイド(埋込み SQL 編)」、「OWASP(Open Web Application Security Project)が発表している、Web サイトのセキュリティ脆弱性の情報」	笹崎	安永課長
2.3	2007.05.09	6.2	表 6.2 配布と運用の保証手段から以下を削除 「Symfoware Server RDB 運用ガイド」	笹崎	安永課長
3.0	2007.08.20	全体	新規作成 V8 の ST に対して下記の点を修正 - 製品の識別情報の変更 - パッケージバージョンの変更	笹崎	佐藤課長
3.1	2007.10.19	5.1.1.6 6.1.4 6.1.4	「3. セキュリティ監査事象選択」「FAU_SEL.1 選択的監査」に以下を追加 - 利用者識別情報 「監査ログ機能」 a) 監査ログの取得機能 「利用者からの要求によるデータベースへのアクセス」に、以下を追加。 ・ SQL 文に関する情報 ・ SQL 文の入力データに関する情報 「監査ログ機能」 a) 監査ログの取得機能 「取得対象事象および利用者の選択」に利用者の選択の記述を追加	笹崎	佐藤課長
3.2	2007.12.26	1.2 2.4.1	「ST概要」 「機能構成」 上記どちらも、パッケージ名の誤記を修正。	笹崎	佐藤課長

まえがき

本書の目的

本書は、ISO/IEC 15408に基づいたSymfoware Server Enterprise Extended Edition 9.0.1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

Sun、Sun Microsystems、Sun ロゴ、Solaris およびすべての Solaris に関連する商標及びロゴは、米国およびその他の国における米国 Sun Microsystems, Inc.の商標または登録商標であり、同社のライセンスを受けて使用している。

Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標あるいは商標です。

OpenLinux は、Caldera International, Inc.の米国ならびその他の国における登録商標あるいは商標です。

Red Hat、RPM および Red Hat をベースとしたすべての商標とロゴは、Red Hat,Inc.の米国およびその他の国における登録商標あるいは商標です。

目 次 (1 / 2)

- 1 ST概説
 - 1.1 ST識別
 - 1.2 ST概要
 - 1.3 CC適合
 - 1.4 参照資料
- 2 TOE記述
 - 2.1 TOEの概要
 - 2.2 TOEの利用
 - 2.2.1 TOEの関係者
 - 2.2.1.1 利用者
 - 2.2.1.2 管理者
 - 2.2.1.3 責任者
 - 2.2.2 利用方法
 - 2.3 TOEの構成
 - 2.3.1 TOEのハードウェア
 - 2.3.1.1 ハードウェア環境
 - 2.3.1.2 ハードウェア構成
 - 2.3.2 TOEのソフトウェア
 - 2.3.2.1 ソフトウェア環境
 - 2.3.2.2 ソフトウェア構成
 - 2.4 TOEの機能
 - 2.4.1 機能構成
 - 2.4.2 機能概要
 - 2.5 TOE保護資産
- 3 TOEセキュリティ環境
 - 3.1 前提条件
 - 3.2 脅威
 - 3.3 組織のセキュリティ方針
- 4 セキュリティ対策方針
 - 4.1 TOEのセキュリティ対策方針
 - 4.2 環境のセキュリティ対策方針

目 次 (2 / 2)

- 5 ITセキュリティ要件
 - 5.1 TOEセキュリティ要件
 - 5.1.1 TOEセキュリティ機能要件
 - 5.1.1.1 認証と識別
 - 5.1.1.2 アクセス制御
 - 5.1.1.3 資源量の制限
 - 5.1.1.4 資源保護
 - 5.1.1.5 残存情報保護
 - 5.1.1.6 監査
 - 5.1.1.7 セキュリティ管理
 - 5.1.2 TOEセキュリティ保証要件
 - 5.1.3 TOEセキュリティ機能強度
 - 5.2 IT環境に対するセキュリティ要件
 - 5.2.1 OSに依存する要件
- 6 TOE要約仕様
 - 6.1 TOEセキュリティ機能
 - 6.1.1 運用選択機能 (F. SEL)
 - 6.1.2 利用者制御機能 (F. USER)
 - 6.1.3 資源制御機能 (F. RES)
 - 6.1.4 監査ログ機能 (F. AUDIT)
 - 6.1.5 セキュリティ機能要件対応
 - 6.2 保証手段
- 7 PP主張
- 8 根拠
 - 8.1 セキュリティ対策方針根拠
 - 8.2 セキュリティ要件根拠
 - 8.2.1 依存関係
 - 8.2.2 相互支援
 - 8.2.3 TOE保証要件根拠
 - 8.2.4 機能強度根拠
 - 8.3 TOE要約仕様根拠
 - 8.3.1 機能強度仕様根拠
 - 8.4 PP主張根拠

[用語]

[略語]

表目次

表 2. 1	TOEのソフトウェア構成
表 5. 1	保証要件コンポーネント一覧
表 5. 2	セキュリティ機能要件一覧
表 5. 3	管理要件パラメータ一覧
表 5. 4	監査要件
表 6. 1	セキュリティ機能とセキュリティ機能要件
表 6. 2	保証コンポーネント名と保証手段
表 8. 1	脅威に対する対策方針
表 8. 2	要件一覧
表 8. 3	依存関係一覧
表 8. 4	相互支援一覧
表 8. 5	対応関係一覧

図目次

図 2. 1	TOEのプロセス実行イメージ
図 2. 2	機能構成
図 2. 3	TOE保護資産

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 3.2 版 富士通株式会社」は、以下の T O E 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 9.0.1
製作者:	富士通株式会社
版番号:	EEE9.0.1
適用する CC のバージョン:	CC v2.3 補足-0512 適用

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 9.0.1 (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6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*)
- ・ RDB機能(基本)
(*FJSVrdb2b*)
- ・ RDB機能(サーバ)
(*FJSVrdbdb*)
- ・ RDB機能(クライアント)
(*FJSVrdbap*)
- ・ 並列クエリ機能
(*FJSVrdbps*)

1.3 CC適合

本 T O E の C C 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 E A L 4 適合
- － 適合する P P は存在しない

1. 4 参照資料

Common Criteria for Information Technology Security Evaluation
Part 1: Introduction and general model August 2005 Version 2.3
CCMB-2005-08-001

Common Criteria for Information Technology Security Evaluation
Part 2: Security functional requirements August 2005 Version 2.3
CCMB-2005-08-002

Common Criteria for Information Technology Security Evaluation
Part 3: Security assurance requirements August 2005 Version 2.3
CCMB-2005-08-003

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

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

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

いずれも平成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

補足文書

補足- 0512

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、Red Hat Enterprise Linux 5 (for Intel Itanium)上で動作する。

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 連携機能に関する「jypvbrp.c」「jypvbsp.c」のモジュール、及びXA 連携機能に関する「jypvpxop.c」「jypvpxel.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	3910.50	RDB セキュリティ機能
2	FJSVsymex	9011.50	Symfoware 基本パッケージ
3	FJSVsymhs	9010.50	スタンバイ機能
4	FJSVsymwa	1310.50	Web ベースデータベースツール
5	FJSVsymwd	1610.50	Web ベースデータベースツール
6	FJSVhscnv	2020.50	高速コード変換機能
7	FJSVlnkexp	4012.50	Linkexpress 機能
8	FJSVlnkre	4012.50	レプリケーション機能
9	FJSVrdb2b	3910.50	RDB 機能(基本)
10	FJSVrdbdb	3910.50	RDB 機能(サーバ)
11	FJSVrdbap	3910.50	RDB 機能(クライアント)
12	FJSVrdbps	3910.50	並列クエリ機能
13	FJSVsymjd	9010.50	JDBC ドライバ
14	FJSVsymmx	9010.50	Symfoware オンラインマニュアル
15	FJSVrdbhs	3910.50	ホットスタンバイ機能
16	FJSVrdbpc	3910.50	ロードシェア機能
17	FJSVapccm	3910.50	Connection Manager 機能
18	FJSVapcdb	3910.50	Connection Manager 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、ア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。

Red Hat Enterprise Linux 5 (for Intel Itanium)

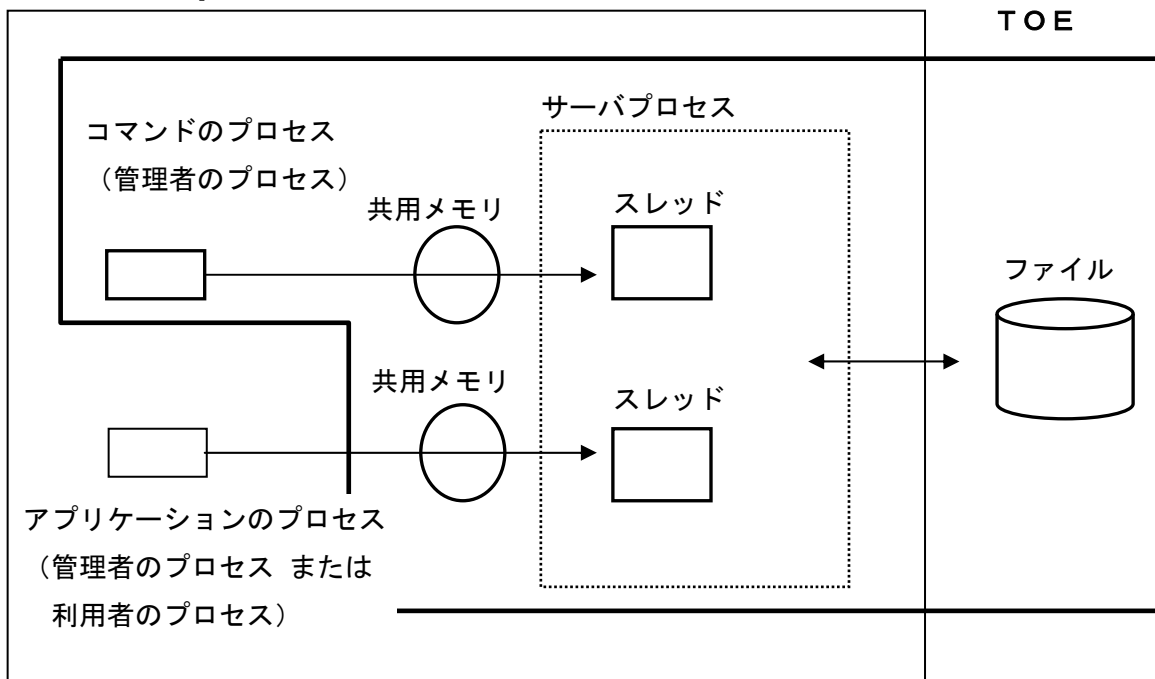


図2. 1 TOEのプロセス実行イメージ

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6つの機能(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)
- ・ RDB機能(基本) (FJSVrdb2b)
- ・ RDB機能 (サーバ) (FJSVrdbdb)
- ・ RDB機能 (クライアント) (FJSVrdbap)
- ・ 並列クエリ機能 (FJSVrdbps)

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と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と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。

セッ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。

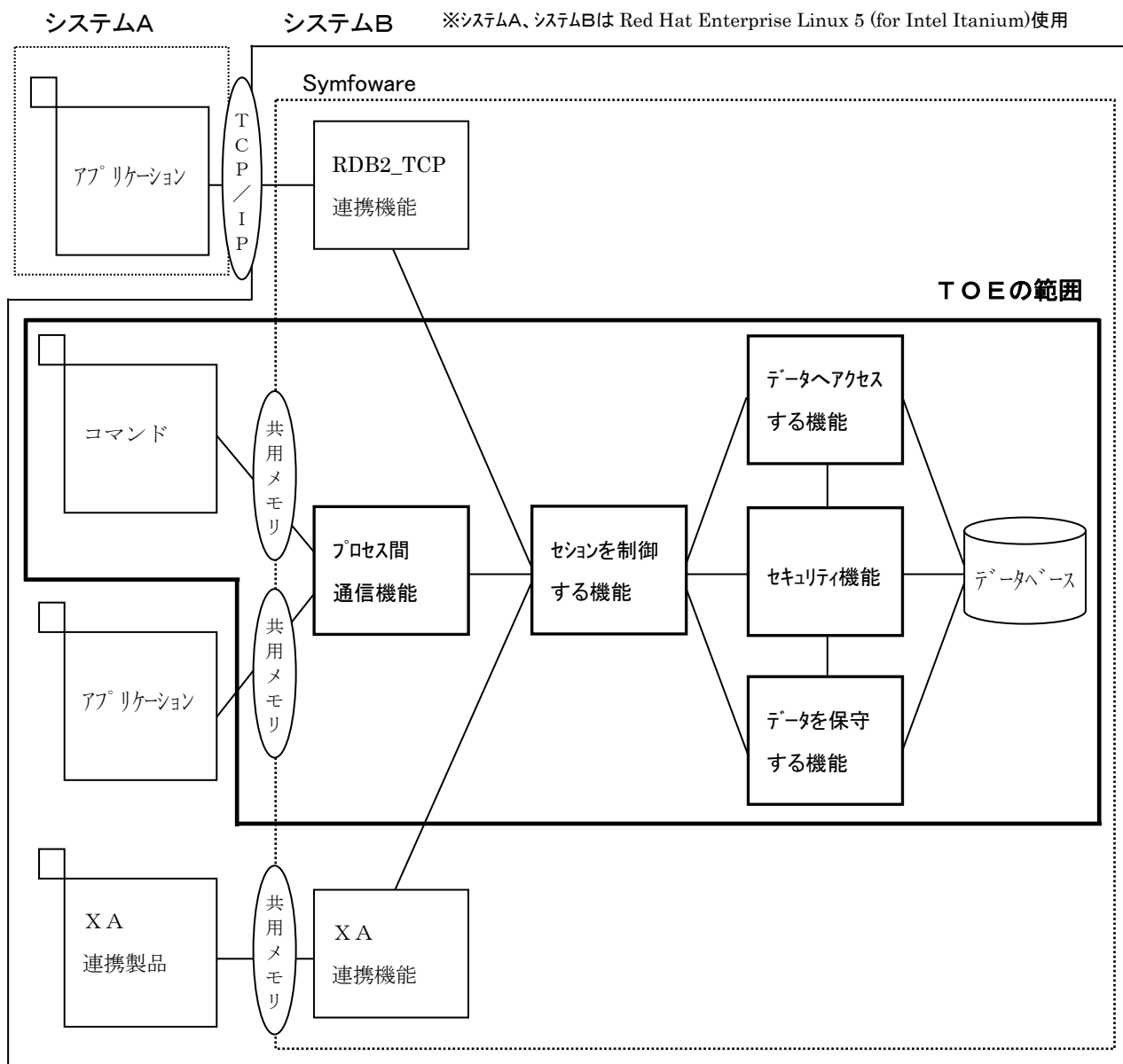


図 2. 2 機能構成

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
- － セッ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、共有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。

セッ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
- － シーケンスの参照
- － プロシジャの実行
- － ファンクションの実行

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、セッ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 T O E 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。

ー 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。

ー 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、シーケンス、プロシジャやファンクション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。ファンクションとは SQL 記述性を高めるために、利用者が複雑な演算処理をあらかじめサーバに定義・登録する機能である。

プロシジャやファンクション実行の 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やファンクションを 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。

ー 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。

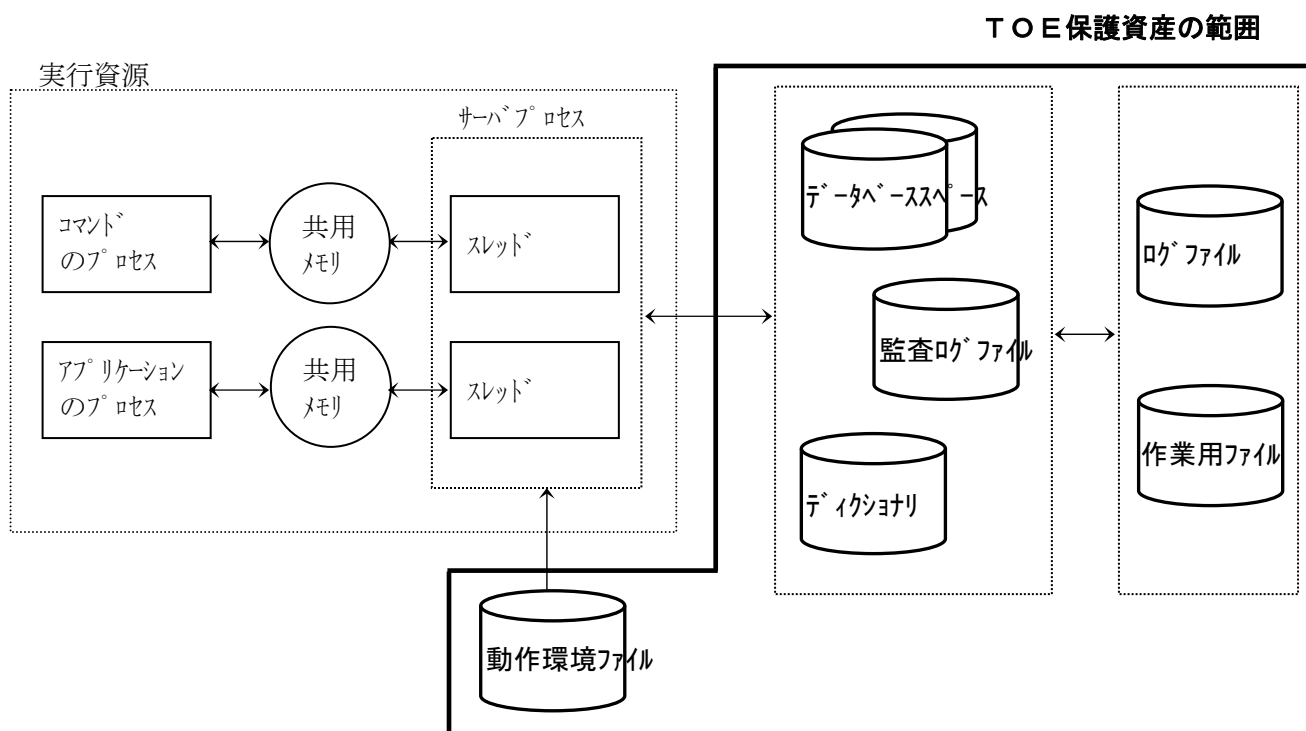


図 2. 3 TOE保護資産

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、使用可能なセッ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、[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正数値」]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。

[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

— 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、各利用者に認証が成功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。

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。

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または失敗)。

FIA_USB.1 利用者・サブジェクト結合

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]

- 権限
- 使用可能資源量
- 同時使用セッション数

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]

なし

FIA_USB.1.3

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

[割付: 属性の変更に関する規則]

なし

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**

セッ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ッション確立の[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
- － シーケンス
- － ファンクション

[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
- － シーケンスの参照
- － ファンクションの実行

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
- － シーケンス
- － ファンクション

[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
- － シーケンスの参照
- － ファンクションの実行

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、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] アクセス制御SFP

- － アクセス制御 SFP_DBM

[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

サブジェクトのリスト

- － サーバプロセス

オブジェクトのリスト

- － 表
- － シーケンス
- － プロシジャ
- － ファンクション

[割付] 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

サブジェクトに対応する SFP 関連セキュリティ属性

- － 利用者属性
- － 資源属性
- － 操作属性

オブジェクトに対応する SFP 関連セキュリティ属性

なし

SFP 関連セキュリティ属性の名前付けされたグループ

- － 管理者権限リスト

FDP_ACF.1.2(1)

TSP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)

TSP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)

TSP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)

TSP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] アクセス制御SFP

- アクセス制御 SFP_DBU

[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

サブジェクトのリスト

- サーバプロセス

オブジェクトのリスト

- 表
- シーケンス
- プロシジャ
- ファンクション

[割付] 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

サブジェクトに対応する SFP 関連セキュリティ属性

- 利用者属性
- 資源属性
- 操作属性

オブジェクトに対応する SFP 関連セキュリティ属性

なし

SFP 関連セキュリティ属性の名前付けされたグループ

- － 権限リスト

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) 複数同時セッションの制限 (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ッション数運営規則の管理。

監査: FTA_MCS.2

a) 最小: 複数同時セッションの制限に基づく新しいセッションの拒否。

FTA_MCS.2 複数同時セッションの利用者属性ごと制限

FTA_MCS.2.1

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

[割付] 最大同時セッション数の規則

- 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]セッ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を選択(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を選択(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: から一つのみ選択]レベルのすべての監査対象事象; 及び
- c) [割付: 上記以外の個別に定義した監査対象事象]。

[選択] 最小、基本、詳細、指定なし

- 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
- － 利用者識別情報

[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、監査証跡内の格納された監査記録への不正な改変を[選択: *防止*、*検出*: から一つのみ選択]できねばならない。

[選択: *防止*、*検出*]

- 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(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: から一つのみ選択]及び[割付: 監査格納失敗時にとられるその他のアクション]を行わねばならない。

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

- － 監査対象事象の無視

[割付] 監査格納失敗時にとられるその他のアクション

- － 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

FAU_STG.4.1(2)

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: から一つのみ選択]及び[割付: 監査格納失敗時にとられるその他のアクション]を行わねばならない。

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

- － 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

- － 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: 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。

[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: から一つのみ選択、[割付: 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時、[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 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。

[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 から一つのみ選択、[割付: 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時、[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のできる閾値
 - 使用可能資源量
 - 同時使用セッション数
 - 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のできる閾値
 - 権限
 - 使用可能資源量
 - 同時使用セッション数
 - 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。

なお、ASEクラスは、保証レベルに関わらず必須となる保証要件として採用する。

表 5. 1 保証要件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: 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。

※ 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: から一つのみ選択、[割付: 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時、[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、各利用者に認証が成功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 TSFD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、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。

※ 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] 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

サブジェクトのリスト

- OS上で動作する全てのプロセス

オブジェクトのリスト

- データベーススペース

[割付] 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

サブジェクトに対応する SFP 関連セキュリティ属性

- プロセスの所有者属性

オブジェクトに対応する SFP 関連セキュリティ属性

なし

SFP 関連セキュリティ属性の名前付けされたグループ

- アクセスパーミッション (OSにより、プロセス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_ACF1.3(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_ACF1.4(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 管理要件パラメータ一覧 (続)

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のできる閾値
		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 －同時使用セッション数
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		利用者毎の属性 －権限 －使用可能資源量 －同時使用セッション数	
FIA_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ッション数運営規則の管理	利用者毎の属性 －同時使用セッション数
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を選択(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を選択(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 ※

表 5. 3 管理要件パラメータ一覧 (続き)

セキュリティ機能要件	管理要件	管理項目	
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	
	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)	監査情報の取得失敗時の処理の選択
監査格納失敗時にとられるアクションの維持(改変、追加)		(固定)	
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、管理要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) 不適當な認証情報の拒否	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または失敗)	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: 複数同時セッションの制限に基づく新しいセッションの拒否	1) 同時使用セッ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ータ	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を用いるDDL文 セキュリティ情報の変更を用いる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。セッ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、セッ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)

ー 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。

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

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。

ー 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。

ー 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、スーパーユーザであり、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、反転したものではないか
- ・ 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、シーケンスの参照、プロシジャの実行およびファンクションの実行を行う。

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 ディクショナリ
	UPDATE権	表の更新	
	DELETE権	表の削除	
	INSERT権	表の挿入	
	SELECT権	シーケンスの参照	
	EXECUTE権	プロシジャの実行	
	EXECUTE権	ファンクションの実行	

－ 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、セッ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ッ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ッション数	MAX_CONNECTION	
データベーススペース	MAX_TRAN_MEM	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、セッション内で各利用者が使用する資源量を制限できる。
ディクショナリ	MAX_TRAN_TIME	
監査ログファイル		
ログファイル		
作業用ファイル	MAX_WORKFILE_USE	作業用ファイル量、ファイル数を制限す

	MAX_WORKFILE_NUM	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	セッ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ッ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、セッ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	セッ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ッ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、セッ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

ー 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類が記録される。

●) 権限情報の参照機能 (F. USER. REF)

ー 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。

ー 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)

T S Fデータの参照は、管理者のみに許可する。

T S F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 T O E 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

ー 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
- ・ SQL文に関する情報
- ・ SQL文の入力データに関する情報

ー 管理者による T O E に対する操作

管理者による T O E 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）

ー 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
- ・ 同時使用セッション数を越えた
- ・ 利用者が使用可能な最大資源量を越えた
- ・ 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。

ー 取得対象事象および取得対象利用者の選択

監査ログの取得範囲は、変更することができる。どの事象および利用者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)

ー 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。

ー 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）

セキュリティ仕様概要		F	F	F	F	F	F	F	F	F	F	F
セキュリティ機能要件		S	U	U	U	U	U	R	R	A	A	A
		E	S	S	S	S	S	E	E	U	U	U
		·	·	·	·	·	·	·	·	D	D	D
		P	A	A	P	R	R	A	I	I	I	I
		A	R	U	R	E	T	T	N	V	S	S
		R	E	T	H	E	R	I	C	O	L	P
		A	F	H	E	N	E	T	O	L	A	A
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		F	F	F	F	F	F	F	F	F	F	F
		S	U	U	U	U	U	U	U	U	U	U
セキュリティ機能要件		E	S	S	S	S	S	S	S	S	S	S
		L	E	E	E	E	E	E	E	E	E	E
	P	R	R	R	R	R	R	R	R	R	R	R
	A	·	·	·	·	·	·	·	·	·	·	·
	R	A	D	A	P	R	E	S	A	I	N	I
	A	F	U	T	H	E	N	T	R	C	O	L
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	－提供管理システム利用手引書(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 インストールガイド(サーバ編) －Symfoware Server インストールガイド(クライアント編) －Symfoware Server セキュリティ運用ガイド －製品ご案内
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 セキュリティ運用ガイド
	AGD__USR. 1	－Symfoware Server SQLリファレンス －Symfoware Server メッセージ集
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	<ul style="list-style-type: none"> －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	－アプリケーション開発ガイド(埋込み SQL 編)
	AVA_VLA. 2	－OWASP(Open Web Application Security Project)が発表している、Webサイトのセキュリティ脆弱性の情報

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・C O・N E・N E・C T	O・A C C E S S	O・R E S O U R C E	O・A T T O R	O・I N T I T	O・A U D I T	O・E C O N S I G N E C T	O・E A S S I G N	O・E U S E R	O・E P H Y S I C A L	O・E E N V	O・E O S
A. MANAGER								✓			✓	
A. USER									✓			
A. PHYSICAL										✓		
T. TCP											✓	✓
T. XA											✓	
T. ACCESS	✓	✓		✓		✓	✓				✓	✓
T. RESOURCE		✓	✓			✓					✓	
T. OS				✓							✓	✓
T. DATA					✓						✓	

ー 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。

ー 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ため、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。

ー 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。

ー 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ため、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。

ー 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）

セキュリティ対策方針 セキュリティ機能要件		O	O	O	O	O	O	O	O
		・	・	・	・	・	・	・	・
		C	A	R	A	I	A	E	E
		N	C	E	T	N	U	C	O
		O	E	S	O	I	D	N	S
		N	S	U	R	I	N	E	
		E		R		T	E	C	
		C		C				T	
		T		E					
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)

セキュリティ対策方針		O ・ C O N N E C T	O ・ A C C E S S	O ・ R E S O U R C E	O ・ A T T R	O ・ I N I T	O ・ A U D I T	O E ・ C O N N E C T	O E ・ O S
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						✓		
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	✓	✓	✓		✓	✓		
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)								✓	

ー 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。

ー 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と変わらない。)

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ッ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、セッ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ー情報や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 と変わらない。）

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り、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/変更することである。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。

- ー 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 T O E 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。

※ 2 FMT_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、迂回を抑制している。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制している。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制している。

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）

セキュリティ仕様概要		F・S E L P A R A	F・U S E R P A R A M E T E R S	F・U S E R P R I V I L E G I T Y	F・U S E R P R E S E N S I V E	F・U S E R R E F E R E N C E	F・R E S A T T R I B U T E	F・R E S I N I T I A L I Z E D	F・A U D I T C O L L E C T I O N	F・A U D I T V I E W	F・A U D I T S P A C E
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)						✓				
	FDP_RIP.1							✓			
残存情報保護	FPT_RTP.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)

セキュリティ仕様概要		F	F	F	F	F	F	F	F	F	F
		S	U	U	U	U	U	R	R	A	A
セキュリティ機能要件		E	S	S	S	S	S	E	E	U	U
		L	E	E	E	E	E	S	S	D	D
セキュリティ管理		·	·	·	·	·	·	·	·	·	·
		P	A	A	P	R	·	A	I	I	T
セキュリティ管理		A	D	A	R	R	R	T	N	T	T
		R	E	U	E	E	E	R	I	·	·
セキュリティ管理		A	F	T	V	S	F	R	C	V	S
				H	I				O	I	E
セキュリティ管理				E	N				L	E	A
				N						W	A
セキュリティ管理											E
セキュリティ管理		FMT_MOF.1	✓			✓					
		FMT_MSA.1			✓	✓	✓				
セキュリティ管理		FMT_MSA.3(1)				✓					
		FMT_MSA.3(2)				✓					
セキュリティ管理		FMT_MTD.1(2)	✓			✓					✓
		FMT_MTD.1(3)		✓	✓	✓		✓			
セキュリティ管理		FMT_MTD.1(4)	✓			✓				✓	✓
		FMT_MTD.3	✓	✓	✓	✓					
セキュリティ管理		FMT_SAE.1			✓						
		FMT_SMF.1	✓			✓	✓				✓
セキュリティ管理		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、認証時にその数を超えた場合、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、利用者による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つのセッ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つのセッ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ッ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ッ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 FAUDIT.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 FAUDIT.COL によって、取得する監査記録には、管理者または利用者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 FAUDIT.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 FAUDIT.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 FAUDIT.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 FAUDIT.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 FAUDIT.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要素は複数持つことができ、1つの要素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 ज्या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 ज्या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、T S F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、同時使用セッション数、認証が不成功回数となることのできる閾値、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T S F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、変更が可能であるため、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、変更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、変更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ー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ー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

TOE は、F.USER.AUTHEN として利用者に対する識別認証を行っている。

認証情報が従う品質基準として、以下の確率的または順列的メカニズムを採用している。

— 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ータで指定されるパスワードの最低長(6以上8以下を設定可能、既定値6)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。

また、F.USER.AUTHEN では、不成功認証試行が管理者の設定した値(最大値:11 回)に達した際に、該当する利用者を TOE に対して結合できない状態に変更するため、認証情報の推測攻撃に対して十分な対抗を保証している。

従って、F.USER.AUTHEN の強度は中レベルの攻撃能力を持つ攻撃者に対して十分に対抗することができるため、SOF-medium が妥当であると判断する。これは、IT セキュリティ要件で主張した最小機能強度 SOF-basic を満足し、特定の TOE セキュリティ機能要件(対象は、FIA_AFL.1、FIA_SOS.1、FIA_UAU.2(1)、FIA_UID.2(1))に対する機能強度 SOF-medium と一貫するものである。

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。

一時表

複数の利用者から、それぞれ同一の表名で利用しても、それぞれの利用者が格納したデータのみが参照できる表。利用者の作業域として利用。

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。

シーケンス

一意性のある番号を順番に取得する機能

例) 1 から順に値を取得するシーケンスを事前に定義する

順序 : 1 から順番に昇順に値を採番

以下のSQL文を繰り返し実行すると、表の列に1から順番に値が入る。

```
INSERT INTO 表 VALUES 列 = 順序.NEXTVAL;
```

スーパーユーザ

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。

セッション

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有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。

ファンクション

SQL 記述性を高めるために、複雑な演算処理をあらかじめデータベースに登録する機能である。

例) 二つの値の平均をとるファンクションを事前に定義

HEIKIN : 復帰値 = (入力1 + 入力2) / 2

以下のSQL文で結果表を参照すると、二つのカラム結果1と結果2の平均が取得できる。

SELECT HEIKIN(結果1,結果2) FROM 結果表;

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。

RDBディレクトリファイル

データベースをアクセスするための基本情報や、各種の運用情報を記録するファイル。

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)