HiRDB

Single Server

セキュリティターゲット

2008/02/22

Version 2.20

株式会社 日立製作所

「HiRDB Single Server セキュリティターゲット」

― 変更歴 ―

項番	作成／変更年月日	ST バージョン	変更理由
1	2005/09/12	Ver 2.00	新規作成
2	2005/11/01	Ver 2.01	評価者からの指摘を検討した上での修正
3	2005/11/16	Ver 2.02	評価者からの指摘を検討した上での修正
4	2005/11/30	Ver 2.03	評価者からの指摘を検討した上での修正
5	2005/12/28	Ver 2.04	評価者からの指摘を検討した上での修正
6	2006/01/20	Ver 2.05	評価者からの指摘を検討した上での修正
7	2006/01/25	Ver 2.06	評価者からの指摘を検討した上での修正
8	2006/04/17	Ver 2.07	評価者からの指摘を検討した上での修正
9	2006/04/26	Ver 2.08	評価者からの指摘を検討した上での修正
10	2006/04/27	Ver 2.09	評価者からの指摘を検討した上での修正
11	2006/06/20	Ver 2.10	評価者からの指摘を検討した上での修正
12	2006/07/06	Ver 2.11	評価者からの指摘を検討した上での修正
13	2006/12/04	Ver 2.12	評価者からの指摘を検討した上での修正
14	2006/12/13	Ver 2.13	評価者からの指摘を検討した上での修正
15	2006/12/25	Ver 2.14	評価者からの指摘を検討した上での修正
16	2007/01/19	Ver 2.15	評価者からの指摘を検討した上での修正
17	2007/06/05	Ver 2.16	評価者からの指摘を検討した上での修正
18	2007/06/21	Ver 2.17	評価者からの指摘を検討した上での修正
19	2007/07/19	Ver 2.18	評価者からの指摘を検討した上での修正
20	2007/07/23	Ver 2.19	評価者からの指摘を検討した上での修正
21	2008/02/22	Ver 2.20	評価者からの指摘を検討した上での修正

■ 商標類

- AIX は, 米国における米国 International Business Machines Corp.の登録商標です。
- Windows は, 米国およびその他の国における米国 Microsoft Corp.の登録商標です。

■ 著作権

「HiRDB セキュリティターゲット」

― 目次 ―

1. ST 概説

本章では、ST 識別、ST 概要、CC 適合、用語の定義について記述する。

1.1. ST 識別

1.1.1. ST 識別情報

本 ST（セキュリティターゲット）の識別情報を以下に示す。

名称： HiRDB Single Server セキュリティターゲット
バージョン： 2.20
識別名： HiRDB-S-ST-2.20
作成日： 2008 年 2 月 22 日
作成者： 株式会社 日立製作所

1.1.2. TOE 識別情報

本 ST で評価する TOE（評価対象）を含む製品の名称を以下に示す。

名称： HiRDB / Single Server Version 7
バージョン： 07
リビジョン： 03
作成者： 株式会社 日立製作所
適用 OS： AIX 5L V5.3
キーワード： HiRDB、DBMS、RDBMS、データベース、リレーショナルデータベース

1.1.3. 適用 CC

本 ST は以下の CC を適用する。

CC バージョン 2.3、補足-0512 適用、ISO/IEC 15408：2005

1.2. ST 概要

1.2.1. TOE の概要

評価対象である HiRDB / Single Server Version 7 は、リレーショナルデータベース管理システム（RDBMS）のソフトウェア製品である。TOE はデータベースサーバとして機能し、データベースに格納された情報をアクセスする機能を提供する。通常、利用者は HiRDB クライアントから HiRDB サーバに対して SQL の実行を要求することによってデータベースに格納された情報にアクセスする。TOE では、利用者のニーズに沿うさまざまなデータ操作を効率良く実行するための機能を用意し、利用者データに対するアクセスを許可された利用者に制限するためのセキュリティ機能を提供する。

TOE のセキュリティ機能には次のものが含まれる。

- 監査
- アクセス制御
- 識別･認証
- 利用者･権限管理

1.3. CC 適合

本 ST は以下の通り CC 適合を主張する。

- CC バージョン 2.3 パート 2 適合
- CC バージョン 2.3 パート 3 適合

評価保証レベルは EAL4 であり、ALC_FLR.1 を追加する。

本 ST は PP（プロテクションプロファイル）を適用しない。

1.4. 用語の定義

本 ST で用いる用語の意味（要約）を表 1-1 に示す。

表 1-1 ： 用語の意味

用語	意味
DBA 権限保持者	DBA 権限を持つ DB ユーザであり、DB ユーザ、DBA 権限、スキーマ定義権限を管理する。
DB ユーザ	HiRDB サーバに接続する利用者。DB ユーザには認可識別子とパスワードが割り当てられる。
HiRDB 管理者	OS ユーザとして TOE の管理・運用業務を担う管理者。
HiRDB クライアント	SQL 文を実行するための電文を HiRDB サーバに送信し、その結果を受信するクライアント側システム。
HiRDB サーバ	TOE によって構築したデータベースが配置されるサーバ側システム。
OS	本 ST では特に断わりがない限り、HiRDB サーバの OS を指す。
OS ユーザ	HiRDB サーバの OS にログインする利用者。
SQL	リレーショナルデータベースの操作言語。SQL を用いることで、ユーザ表の定義やデータ操作など、リレーショナルデータベースに関する操作を機械可読なテキストとして記述できる。
UAP	利用者が開発するアプリケーションプログラム。TOE のガイダンスに従って開発される。
XA 連携機能	XA インタフェースを使用して、HiRDB サーバと連携する機能。
アクセス権限	ユーザ表のデータを操作するために必要な権限。アクセス権限は次に示す権限の総称であり、各権限はユーザ表毎に DB ユーザに与えられる。 ・ SELECT 権限 ・ INSERT 権限 ・ DELETE 権限 ・ UPDATE 権限
オブジェクト	TOE の機能によって定義され、情報を内蔵するデータベースの構成要素。
監査証跡表	監査データの内容を参照するために使用される表。
監査証跡ファイル	監査対象事象の発生時に監査データが格納されるオブジェクト。
監査人	監査権限を持つ DB ユーザであり、監査業務を担当する。
行	表に格納される一件一件の各データのこと。 （別名 ： ロー、レコード）
行検索	表の行をさまざまな条件で検索する機能。操作系 SQL の一種。
行更新	表の行の値を列単位で更新する機能。操作系 SQL の一種。

行削除	表の行を削除する機能。操作系 SQL の一種。
行挿入	表に行を追加する機能。操作系 SQL の一種。
クライアント機能	HiRDB サーバにおいて UAP を開発･実行するための機能であり、以下のインタフェースを含む。 ・ プリプロセサ ・ JDBC ドライバ ・ SQLJ
スキーマ	データベースの論理的構造単位（枠組）。単一の DB ユーザ（スキーマ所有者）によりただ一つのスキーマが所有される。スキーマにはユーザ表が含まれる。
スキーマ所有者	スキーマを所有する DB ユーザであり、所有するスキーマに含まれるユーザ表を所有し、管理する。スキーマを所有するには、スキーマ定義権限が必要である（スキーマ定義権限を持っていてもスキーマを所有していない場合は、スキーマ所有者には該当しない）。
スキーマ定義権限	スキーマを定義して、これを所有するのに必要な権限。
スーパユーザ	OS（UNIX）におけるシステム管理者。
制御系 SQL	HiRDB サーバとの接続や切り離しを実行する場合に使用する SQL。
操作系 SQL	表に格納されるデータを操作する場合に使用する SQL。
定義系 SQL	ユーザ表をはじめとするオブジェクトの定義や削除を実行する場合に使用する SQL。
ディクショナリ表	DB ユーザ、権限、およびユーザ表定義情報などを管理する表。
認可識別子	HiRDB サーバに接続する DB ユーザを識別するための文字列。
表	リレーショナルデータベースの基本要素であり、論理的に行と列との 2 次元構造で表現されるデータが格納されるオブジェクト。表は、以下の3つに大別される。 ・ ユーザ表 ・ ディクショナリ表 ・ 監査証跡表 （別名 ： テーブル）
表定義変更	既に定義されているユーザ実表に列を追加するなど、ユーザ実表の定義内容を変更する機能。
分散データベース機能	異なるデータベースサーバ間でユーザ表の操作要求を転送して実行する機能であり、HiRDB サーバが DB ユーザから受け付けた SQL を別のデータベースサーバに転送する分散クライアント機能と、別のデータベースサーバから転送される SQL を HiRDB サーバで処理する分散サーバ機能がある。分散データベース機能を利用するには、HiRDB サーバと同じマシンに分散データベース製品である DF/UX をインストールして連携する必要がある。

ユーザ実表	実際に、利用者データとして行の集合が格納されるユーザ表。
ユーザビュー表	ユーザ表のデータから特定の行や列を選択して、新たに定義した仮想のユーザ表。 ユーザビュー表は以下の2つに分類される。 ・ 読込み専用ビュー ・ 読込み専用ビュー以外のユーザビュー表
ユーザ表	スキーマ所有者が定義して所有する表であり、利用者データが格納される。ユーザ表は以下の2つに大別される。 ・ ユーザ実表 ・ ユーザビュー表
ユーザ表定義情報	ユーザ表の定義情報であり、以下の情報を含む。 ・ 所有者の認可識別子 ・ ユーザ表の種類 ・ 列の定義情報
読込み専用ビュー	行検索だけが実行できるユーザビュー表。
列	表に格納される各レコード(行)に共通のデータ項目。 (別名 : カラム、フィールド)

2. TOE 記述

本章では、評価対象製品概要、ソフトウェア構成、セキュリティ機能、TOE 関連の利用者役割について記述する。

2.1. 評価対象製品概要

2.1.1. TOE の種別

TOE は、リレーショナルデータベース管理システムのソフトウェア製品である。TOE は、「JIS データベース言語 SQL X3005-1995」をエントリレベルでサポートしている。

2.1.2. 製品概要

（１）製品の目的と特徴

リレーショナルデータベース管理システムはさまざまな情報システムの中核に位置するものとして利用され、その主な役割は大量なデータを複数の利用者間で矛盾なく共用するための機能を提供することである。HiRDB / Single Server Version 7 では、定義系 SQL を用いてデータの構造を定義し、操作系 SQL を用いてデータを操作する。

（２）製品の用途

HiRDB / Single Server Version 7 は汎用的なリレーショナルデータベース製品であり、幅広い業種におけるさまざまなシステムにおいて導入されることが想定される。

（３）評価構成

HiRDB / Single Server Version 7 は、クライアントーサーバ（C/S）形態で使用される。HiRDB / Single Server Version 7 がインストールされるサーバ側システムを HiRDB サーバといい、クライアント側システムを HiRDB クライアントという。

図 2-1 にクライアントーサーバ（C/S）型のシステム構成を示す。このシステム構成では、組織内の特定の従業員が HiRDB クライアントで HiRDB SQL Executer もしくは UAP を実行することにより、HiRDB サーバに構築されるデータベースにアクセスする。また、運用開始前の作業と運用業務は、特定の管理者によって HiRDB サーバにおいて実施されるものとする。

ネットワークは、HiRDB サーバと HiRDB クライアントを接続するためのものであり、他のコンピュータは接続されないものとする。

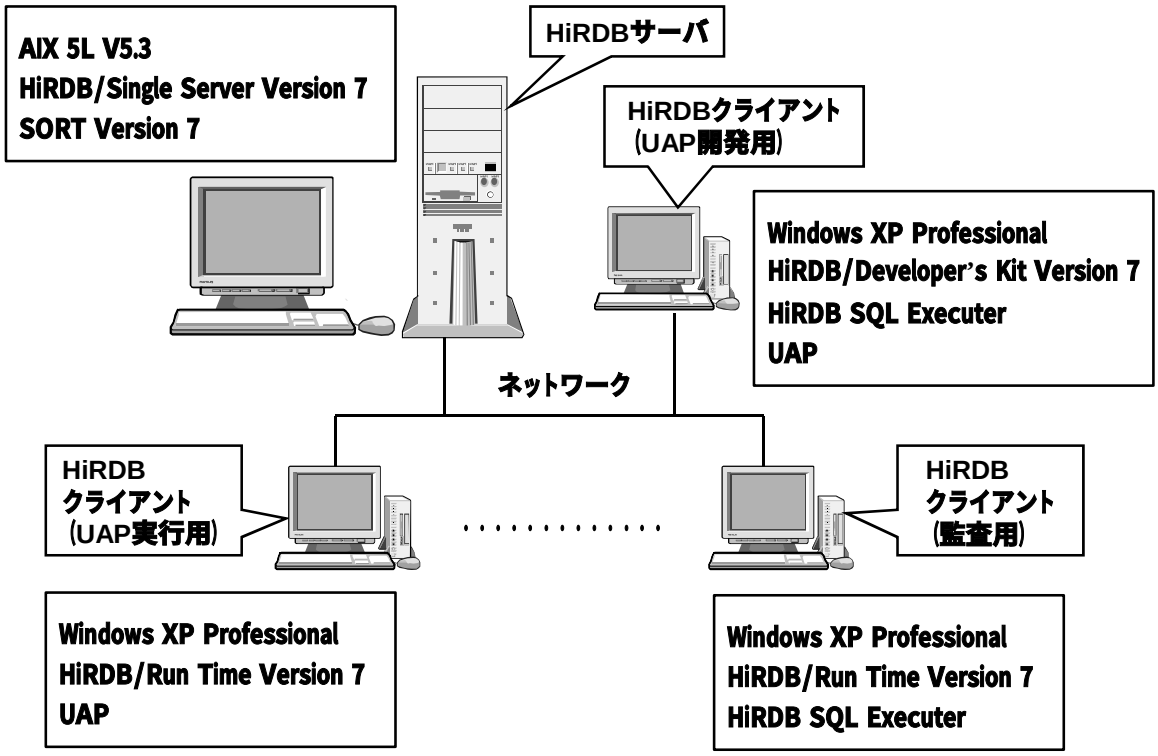

図 2-1 ： クライアントーサーバ (C/S) 型のシステム構成

以下に、図 2-1 に示すシステムを構成する各端末について説明する。

【 HiRDB サーバ 】

HiRDB サーバでは、データベースの論理的設計に基づき、データベースが構築され、データベースの運用が行われる。HiRDB サーバのコンソールからは TOE のコマンドが投入される。コマンドは信頼できる管理者によってのみ実行されるものである。

HiRDB サーバは、HiRDB クライアントから SQL 実行のための電文を受信し、その実行結果を返信する。実行結果には SQL の成否 (失敗した場合はエラーメッセージ)、および検索されたデータが含まれる。

【 HiRDB クライアント 】

HiRDB クライアントは HiRDB サーバに接続し、データベースにアクセスする端末である。HiRDB クライアントでは、データベース (表のデータ) を操作するための電文を生成して、HiRDB サーバに送信する。表のデータは、送信した電文の内容に応じて検索や変更が行われ、その実行結果を HiRDB クライアントは受信する。

HiRDB クライアントは TOE 外に位置するが、HiRDB サーバと一体となって SQL 文の実行に貢献する

ものであり、高度に信頼することのできるクライアントである。

本システム構成では、以下に説明する3種類の HiRDB クライアントが HiRDB サーバと接続されている。なお、HiRDB サーバではいずれの HiRDB クライアントからの SQL 実行要求も電文として受け取るため、共通のインタフェースが用意されている。

＜UAP 開発用＞

HiRDB クライアント（UAP 開発用）では、SQL を用いてデータベースの操作を行う UAP が作成される。UAP は利用者のニーズに基づき、業務毎に設計・開発される。開発した UAP は HiRDB クライアント（UAP 実行用）に配付される。

＜UAP 実行用＞

HiRDB クライアント（UAP 実行用）では、従業員が業務内容に応じ、配付された UAP を適時実行する。UAP が実行されると UAP で指定された SQL 文を実行するための電文が HiRDB サーバに送信され、HiRDB サーバへの接続、およびデータベースの操作が行われる。

＜監査用＞

HiRDB クライアント（監査用）では、監査人または監査証跡参照者によって、監査証跡表の監査データの検索が行われる。

次に、図 2-1 の評価構成における各端末で使用されるソフトウェアについて説明する。

【 HiRDB サーバ 】

＜ AIX 5L V5.3 ＞

AIX 5L V5.3 は HiRDB サーバに搭載される OS である。AIX 5L V5.3 は TOE 外である。

＜ HiRDB / Single Server Version 7 ＞

HiRDB / Single Server Version 7 は、リレーショナルデータベース管理システムのソフトウェア製品であり、TOE である。

＜ SORT Version 7 ＞

SORT Version 7 は HiRDB / Single Server Version 7 が AIX 5L V5.3 のプラットフォーム上で動作する場合の前提プログラムである。SORT Version 7 は TOE の内部的な処理要求に従いソート機能（複数のデータを昇順または降順に並べ替える機能）を提供するプログラムである。SORT Version 7 は日立のソフトウェア製品であり、HiRDB / Single Server Version 7 にはバンドルされない。SORT Version 7 は TOE 外である。

なお、SORT Version 7 を呼び出すのは一部のコマンドのみであり、表のデータを検索する場合には利用されない。したがって、SORT Version 7 は TOE のセキュリティ機能には関係しない。

【 HiRDB クライアント 】

＜ Windows XP Professional ＞

Windows XP Professional は、HiRDB クライアントの PC に搭載される OS である。すべての種類の HiRDB クライアントにインストールされる。Windows XP Professional は TOE 外である。

＜ HiRDB / Developer's Kit Version 7 ＞

HiRDB / Developer's Kit Version 7 は、HiRDB / Run Time Version 7 に加えて、UAP の開発に必要なプリプロセッサを含んだ製品である。プリプロセッサは、UAP のソースコードに記述された SQL 文を解析して、その部分をランタイムを呼び出すコードに変換したポストソースを生成する。ポストソースはコンパイルされ、ランタイムとリンケージをとることにより UAP が生成される。UAP の開発言語には、C、C++、COBOL85、OOCOBOL、Java を利用することができる。HiRDB / Developer's Kit Version 7 は、HiRDB クライアント（UAP 開発用）にインストールされる。HiRDB / Developer's Kit Version 7 は TOE 外である。

＜ HiRDB SQL Executer ＞

HiRDB SQL Executer は、データベースに対話形式でアクセスするための日立のソフトウェア製品である。DB ユーザは PC の画面から任意の SQL を発行し、その結果を確認することができる。このため、UAP を作成しなくてもデータベースにアクセスすることができる。HiRDB SQL Executer は UAP を開発する場合のツールとしても利用され、監査証跡表のデータを検索するツールとしても利用される。HiRDB SQL Executer は、HiRDB クライアント（UAP 開発用）と HiRDB クライアント（監査用）にインストールされる。HiRDB SQL Executer は TOE 外である。

＜ HiRDB / Run Time Version 7 ＞

HiRDB / Run Time Version 7 は、UAP もしくは HiRDB SQL Executer を動作させるための前提となる日立のソフトウェア製品である。HiRDB クライアント（UAP 実行用）と HiRDB クライアント（監査用）にインストールされる。

HiRDB / Run Time Version 7 は、HiRDB クライアントのアプリケーションから SQL を実行するために必要なランタイムを提供する。ランタイムは UAP で記述された SQL 文を実行するための電文を生成し、TOE に送信する。HiRDB / Run Time Version 7 は TOE 外である。

≪ UAP 開発上の留意事項 ≫

UAP 利用者（UAP を操作する人間）が DB ユーザである場合と、UAP 利用者自身は DB ユーザに該当しない場合がある。

① UAP 利用者（UAP を操作する人間）が DB ユーザである場合

HiRDB サーバに接続するための認可識別子とパスワードは、UAP の実行時に UAP 利用者に指定させる必要がある。UAP 利用者は DB ユーザであり、各人に認可識別子とパスワードが割り当てられる。これらの認可識別子には、UAP で発行される SQL を実行するための必要最小限の権限が与えられる。

また、UAP は DB ユーザのパスワードを変更する機能を提供しなければならない。DB ユーザは、UAP を利用してパスワードを変更することができる。

② UAP 利用者（UAP を操作する人間）が DB ユーザに該当しない場合

UAP 利用者は、HiRDB サーバに接続するための認可識別子とパスワードを指定する（知る）必要はない。UAP で使用する認可識別子とパスワードは、UAP 管理者が適切に管理しなければならない。この場合、DB ユーザは UAP 管理者となる。

（４）データベースの構成

ここではデータベースの構成要素であるユーザ表、ディクショナリ表、および監査データについて説明する。なお、本 ST では、TOE の機能によって定義され、情報を内蔵し、TOE の機能によって操作の対象となるデータベースの構成要素のことをオブジェクトと呼ぶ。

【 ユーザ表 】

以下に説明するユーザ実表とユーザビュー表を総称するものがユーザ表である。ユーザ表はスキーマ所有者によってのみ定義することができる。ユーザ表を定義、削除することにより、ユーザ表の所有者の認可識別子が定義、削除される。

｛ ユーザ実表 ｝

ユーザ実表とはリレーショナルデータベースの最も基本的なオブジェクトであり、DB ユーザが直接的に利用するデータの入れ物である。ユーザ実表の論理的構造はまさに二次元の表形式であり、横方向に並ぶ一式のデータを行といい、縦方向の各カテゴリを列という。一行は一件のデータに相当し、各列は項目に相当する。ユーザ実表には、実際に利用者データが格納される。

ユーザ実表に格納される利用者データは、行単位で操作される。ユーザ実表に対する基本的なデータ操作は、以下に示す4つである。

- 行検索
- 行挿入
- 行削除
- 行更新

｛ ユーザビュー表 ｝

ユーザ実表のデータから特定の行や列を選択して、新たに定義した仮想のユーザ表がユーザビュー表である。ユーザ実表の所有者は自らユーザビュー表を定義し、そのアクセス権限を他の利用者に与えることができる。これを利用することにより、ユーザ実表のデータにおける限られた行と列の情報だけを他の利用者に操作させることができる。ユーザビュー表を定義することにより、ユーザ実表単位よりは木目の細かいアクセス制御を実施することが可能である。ユーザビュー表とその基になるユーザ実表との基本的な関係の例を図2-2に示す。

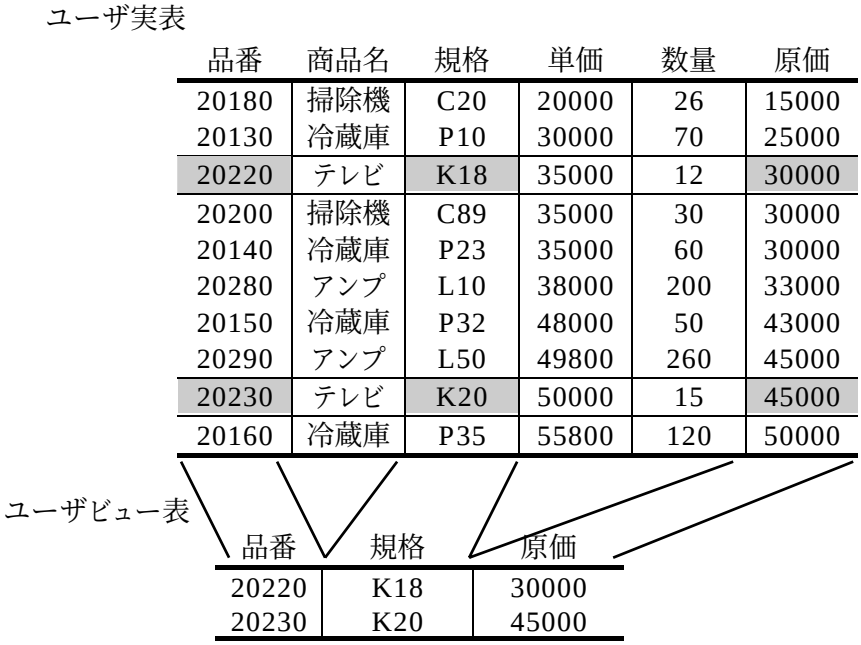

図 2-2 ： ユーザビュー表と基になるユーザ実表との関係

ユーザビュー表を基に、さらにユーザビュー表を定義することも可能である。

ユーザビュー表に対する基本的なデータ操作は、ユーザ実表と同様である。ただし、複数のユーザ表を基に定義したユーザビュー表のように行検索以外の操作が論理的に不可能となり得るユーザビュー表、および所有者の指定により行検索以外の操作が禁止されるユーザビュー表のことを読込み専用ビューと呼ぶ。

ユーザビュー表に対する行検索以外の操作の結果は、ユーザビュー表の大本になるユーザ実表に格納されるデータに反映される。

ユーザビュー表は、アクセス制御の観点から以下に示す2種類に分類することができる。

｛ 大本となるユーザ実表がすべて所有者本人のものであるユーザビュー表 ｝

このユーザビュー表のアクセス権限を与えられた利用者は、このユーザビュー表を介して大本であるユーザ実表のデータにアクセスすることができる。この際、大本であるユーザ実表のアクセス権限は必要ない。

｛ 大本となるユーザ実表に所有者本人以外のものが含まれるユーザビュー表 ｝

このユーザビュー表を介してのデータ操作は、その所有者にしか許可されない。ただし、データ操作ごとのアクセス可否は、基になる他人のユーザ表のアクセス権限の有無に依存する。

【 ディクショナリ表 】

ディクショナリ表とは TOE が内部的に利用するデータを格納し、その整合性を維持するための表のことである。用途別にさまざまなディクショナリ表があり、DB ユーザや各種権限に関する情報、ユーザ表の定義内容（メタデータ）などが格納される。

DB ユーザの認可識別子、パスワード、DB ユーザに与えられる権限情報、パスワードや認証に関する規則および選択可能な監査対象事象は、定義系 SQL の実行によってディクショナリ表に登録され、改変や削除も行われる。これらの定義系 SQL の実行は、それぞれ適切な役割にのみ許可される。

ディクショナリ表に対しては、ユーザ表と同様にデータ操作用の SQL で問合せ（行検索）を実行することができる。ただし、DB ユーザに与えられた権限に応じて参照可能な情報が制限される。DB ユーザのパスワードを格納する列は、SQL の問合せで参照することはできない。

【 監査データ 】

監査データには非参照用と参照用の2種類があり、前者を格納するオブジェクトが監査証跡ファイルであり、後者を格納するオブジェクトが監査証跡表である。以下、両オブジェクトについて説明する。

＜ 監査証跡ファイル ＞

監査対象事象の発生時に、生成される監査データを格納するオブジェクトが監査証跡ファイルである。複数世代の監査証跡ファイルが、TOE によって作成され、管理される。

＜ 監査証跡表 ＞

監査証跡表とは、監査データの内容を参照するために使用される表である。参照用の監査データ（監査証跡表のデータ）は、監査証跡ファイルのデータを監査証跡表に登録することによって生成される。監査人および監査証跡参照者は、監査証跡表に対して行検索を実行することで監査データを参照することができる。

2.2. セキュリティ機能

TOE が提供するセキュリティ機能について概要を説明する。

【 識別･認証 】

DB ユーザが HiRDB サーバに接続するには、TOE による識別と認証をパスしなければならない。DB ユーザを識別するには認可識別子が用いられ、認証にはパスワードが用いられる。DB ユーザは HiRDB サーバとの接続時に、DB ユーザ自身に割り当てられている認可識別子とパスワードを対で指定する。指定された認可識別子とパスワードの組み合わせが TOE に登録されているものと一致する場合、TOE はその DB ユーザの接続を許可する。

TOE は、パスワードの長さが予め設定された最小文字数以上であることを保証する機能を提供する。また、TOE は、同一認可識別子におけるパスワード認証が予め設定された回数連続して失敗した場合に、その認可識別子をロックする機能を提供する。

【 利用者･権限管理 】

DB ユーザの登録と削除は、DBA 権限保持者によって行われる。DB ユーザの登録時には、その DB ユーザを識別する認可識別子、初期パスワードを指定する。DB ユーザのパスワード変更は、その DB ユーザ自身、または DBA 権限保持者によって行うことができる。

また、TOE は DB ユーザに対して与奪する各種権限をサポートしている。ユーザ表単位のアクセス権限はスキーマ所有者（ユーザ表の所有者）によって与奪される。スキーマ定義権限、及び DBA 権限は DBA 権限保持者によって与奪される。監査権限は運用開始前、HiRDB 管理者によって与えられる。

認可識別子、パスワード、および上記すべての権限情報はディクショナリ表に格納され、SQL の適切な実行制御によって保護される。

【 アクセス制御 】

TOE は、ユーザ表に対して適切な利用者だけがアクセスできるようにするため、以下に示すアクセス制御機能を提供する。

- スキーマ所有者は、自分が所有するユーザ表に対して可能な操作をすべて実行することができる。
- DB ユーザが他のスキーマ所有者の所有するユーザ表を操作するには、そのスキーマ所有者によって必要なアクセス権限が与えられていなければならない。
- DBA 権限保持者は運用上の特権を有しており、あらゆるユーザ表の削除を実行することができる。ただし、ユーザ表を対象とする操作系 SQL については如何なる特権も持たない。

【 監査 】

TOE は、利用者によって実行されるデータベース操作に関する情報（監査データ）を記録し、それらの情報を参照できる監査機能を提供する。この機能により、ある操作の結果や試行が問題となる場合は、それを実行

した利用者の認可識別子を特定することができるため、その利用者にアカウンタビリティを要求することができる。

監査の対象とする操作（監査対象事象）は、監査人によって指定される。監査対象事象はディクショナリ表に格納され、SQL の適切な実行制御によって保護される。

操作実行時に生成される監査データは監査証跡ファイルに格納・蓄積されるが、監査人は監査証跡ファイルの監査データを監査証跡表へ登録することで、この監査データの内容を参照することができる。監査証跡ファイルの監査データを、参照、改変、削除する手段は提供されない。

監査証跡表の監査データは、監査人と監査証跡参照者によって SQL で検索することができるため、監査人と監査証跡参照者はさまざまな検索条件で監査データを参照（調査）することができる。なお、監査証跡表の監査データの削除は監査人にのみ許可され、監査証跡表の監査データの改変はどの役割にも許可されない。

なお、TOE は上記以外に、データの可用性や完全性に寄与する機能を有してはいるが、それらの機能は TOE のセキュリティ機能には該当しない。

2.3. TOE 関連の利用者役割

TOE に関連する利用者とその役割を説明する。

TOE の許可された管理者を以下に示す。

- スーパユーザ
- HiRDB 管理者
- DBA 権限保持者
- 監査人
- スキーマ所有者
- UAP 管理者

上記のうち、スーパユーザと HiRDB 管理者は、HiRDB サーバの OS によって維持され（OS において特定のアカウントを持つ）、DBA 権限保持者、監査人、およびスキーマ所有者は TOE によって維持される。UAP 管理者は、HiRDB サーバ（OS、TOE）で維持される必要のない役割である。

2.3.1. HiRDB サーバの OS で維持される利用者役割

HiRDB サーバの OS で維持される利用者役割について、以下に説明する。

【 スーパユーザ 】

スーパユーザは、OS およびそのユーザの管理をする OS ユーザである。スーパユーザは OS においてログイン名とパスワードにより識別･認証される。スーパユーザがデータベース構築･保守のため、OS 環境で実施すべき主な作業を以下に示す。

- HiRDB 管理者の登録
- TOE のインストール
- DBA 権限保持者、監査人、スキーマ所有者に割り当てる OS アカウントの登録

スーパユーザは、HiRDB 管理者や DB ユーザを兼任しても構わない。

【 HiRDB 管理者 】

HiRDB 管理者は、HiRDB サーバの管理をする OS ユーザである。HiRDB 管理者は OS においてログイン名とパスワードにより識別･認証される。HiRDB 管理者が実施する主な業務を以下に示す。

- DBA 権限保持者の登録
- 監査人の登録
- TOE の起動と停止
- 定期的なバックアップの取得

HiRDB 管理者は、HiRDB サーバには接続しない OS ユーザとして、TOE が提供するコマンドを利用して、保護対象資産を除いた部分のデータベース（下位オブジェクト、等）を統括的に管理する役割を担う。ただし、HiRDB 管理者が使用する上記の機能は、TOE のセキュリティ機能には該当しない。

HiRDB 管理者は、DB ユーザとしては DBA 権限保持者を兼任する。

【 一般 OS ユーザ 】

一般 OS ユーザは、ユーザ表、DB ユーザ、または監査関連のオブジェクトを管理する OS ユーザである。一般 OS ユーザは OS においてログイン名とパスワードにより識別･認証される。

次節〈2.3.2. TOE で維持される利用者役割〉で説明する TOE の役割のうち、スキーマ所有者、HiRDB 管理者以外の DBA 権限保持者、および監査人が TOE のコマンドを実行する場合、HiRDB サーバの OS にログインする必要がある。したがって、一般 OS ユーザの OS アカウントは、スキーマ所有者、HiRDB 管理者以外の DBA 権限保持者、および監査人に対して与えられるものであり、その他の者に対して与えられるものではない。

HiRDB 管理者は、TOE に関連する利用者ではあるものの、TOE の範囲外の利用者として定義される。また、一般 OS ユーザは、TOE の利用者であるスキーマ所有者、HiRDB 管理者以外の DBA 権限保持者、および監査人と同一人物であるが、HiRDB サーバに接続していない状態で OS を利用する一般 OS ユーザは、TOE の範囲外として定義される。

2.3.2. TOE で維持される利用者役割

TOE で維持される各利用者役割について、以下に説明する。

【 DB ユーザ 】

DB ユーザは、認可識別子とパスワードを持ち、自らのパスワードを変更することができる。監査人を除く DB ユーザは DBA 権限保持者によって登録される。DB ユーザは HiRDB サーバに接続することで SQL を発行することができ、与えられたアクセス権限に従ってユーザ表のデータ操作を行うことができる。

アクセス権限は、ユーザ表のデータを操作するために必要な権限である。アクセス権限はユーザ表毎に存在する権限であり、DB ユーザはそれぞれのユーザ表に対して、複数の種類のアクセス権限を持つことができる。よって、アクセス権限も他の権限同様、利用者に属するセキュリティ属性である。アクセス権限の種類を表 2-1 に示す。なお、「アクセス権限」とは、表 2-1 で示す各権限の総称として用いられる用語である。

表 2-1 ： アクセス権限の種類

アクセス権限	説明
SELECT 権限	ユーザ表の行検索を許可する。
INSERT 権限	ユーザ表の行挿入を許可する。
DELETE 権限	ユーザ表の行削除を許可する。
UPDATE 権限	ユーザ表の行更新を許可する。

以下に示す役割はすべて DB ユーザをも兼ねている。TOE の利用者はすべて DB ユーザであり、以下

に示す役割を兼ねていない DB ユーザを「一般 DB ユーザ」と呼ぶ。

【 スキーマ所有者 】

スキーマ所有者はスキーマを所有する DB ユーザであり、そのスキーマに含まれるユーザ表の所有者でもある。スキーマ所有者は、スキーマ毎に存在する管理者であり、本人が所有するただ一つのスキーマを管理する。スキーマを定義して所有するには、スキーマ定義権限が必要である。ただし、スキーマ定義権限を持っていてもスキーマを所有していない場合は、スキーマ所有者には該当しない。

スキーマ所有者が実施する主な業務を以下に示す。

- ユーザ表の定義、削除
- 他の DB ユーザに対するユーザ表のアクセス権限の付与、取消し

【 DBA 権限保持者 】

DBA 権限保持者は DBA 権限を有する DB ユーザであり、TOE 全体の管理者である。DBA 権限保持者が実施すべき主な管理･運用業務を以下に示す。

- DB ユーザの登録、削除
- DB ユーザに対するスキーマ定義権限の付与、取消し
- DB ユーザに対する DBA 権限の付与、取消し（必要であれば DBA 権限保持者を増やすことができる）
- パスワードや認証に関するセキュリティパラメタの設定

DBA 権限保持者は、HiRDB サーバに接続する DB ユーザとして、TOE の管理を担う役割である。

DBA 権限保持者は、自らがスキーマ所有者となることができる。また、DBA 権限保持者は、他のスキーマ所有者が所有するユーザ表を削除することができる。

TOE をインストール後、最初に登録される DBA 権限保持者（DB ユーザ）は、OS ユーザとしての HiRDB 管理者が兼任する。DBA 権限保持者を増やした場合、OS ユーザとしては HiRDB 管理者と一般 OS ユーザの両方が存在することになるが、DBA 権限保持者として実行可能な機能に差はない。

【 監査人 】

監査人は監査権限を持つ DB ユーザである。監査人が実施すべき主な業務を以下に示す。

- 監査対象事象の登録、除外
- 監査証跡表への監査データの登録
- 監査証跡表の行検索（監査データのチェック）

監査人は、必要であれば（大量に生成されるかもしれない監査データのチェックの作業分担、あるいは複数人による多重チェックなどを目的として）、監査証跡表の参照権限を他の DB ユーザに与えることにより、監査データのチェック（参照）を共同で実施することができる。この共同実施者の役割を「監査証跡参照者」という。

【 監査証跡参照者 】

監査証跡参照者は監査証跡表の参照権限を与えられた DB ユーザであり、監査人の指示に従い、監査証跡表の行検索（監査データのチェック）を行う。監査証跡参照者は監査人によって任命されるが、その存在は任意である。

2.3.3. UAP に関連する利用者役割

UAP に関連する各利用者役割について、以下に説明する。

【 UAP 管理者 】

HiRDB クライアントで実行する UAP の開発と保守に責任を有する人間である。UAP 管理者は、TOE のガイダンスに従ったセキュアな UAP だけが開発されることを保証しなければならない。UAP が、その利用者に拠らずに HiRDB サーバに接続する認可識別子とパスワードを指定する場合、その認可識別子とパスワードは UAP 管理者が適切に管理しなければならない。この場合、UAP 管理者が DB ユーザに該当する。

UAP 管理者が、OS、あるいは TOE で維持される他の利用者役割を兼任することは任意である。

【 UAP 利用者 】

HiRDB クライアントで実行する UAP を操作する人間である。HiRDB サーバに接続する認可識別子とパスワードを UAP 利用者が指定する場合、その認可識別子とパスワードは UAP 利用者が適切に管理しなければならない。この場合、UAP 利用者が DB ユーザに該当する。

UAP 利用者が、OS、あるいは TOE で維持される他の利用者役割を兼任することは任意である。

3. TOE セキュリティ環境

本章では、資産、前提条件、脅威、組織のセキュリティ方針について記述する。

3.1. 資産

本 TOE の保護対象資産は、利用者データおよび TSF データに分類される。

＜ 利用者データ＞

○ 利用者データ

ユーザ実表に格納される。操作系 SQL によりユーザ実表を直接、またはユーザビュー表を介してアクセスされる。

＜ TSF データ ＞

○ 管理情報

ディクショナリ表に格納される。定義系 SQL によりアクセスされる。操作系 SQL により閲覧もできる。管理情報は、以下の通り分類される。

- 識別･認証情報
  - 認可識別子
  - パスワード
- 権限情報
  - DBA 権限
  - 監査権限
  - スキーマ定義権限
  - アクセス権限
  - 監査証跡表の参照権限
- ユーザ表の所有者の認可識別子
- 監査対象事象（事象の種別のリスト）
- 連続認証失敗許容回数
- パスワード最小文字数
- ロック時間

○ 監査データ

監査証跡ファイルに格納され、監査証跡表に登録した後、操作系 SQL により閲覧される。

3.2. 前提条件

A.OS_ACCOUNT（OSのアカウント）

HiRDB サーバの OS のアカウントは、許可された管理者以外には与えられず、許可された管理者以外は HiRDB サーバの OS にログインできないものとする。

A.REMOTE_OPERATION（リモート操作の制限）

HiRDB サーバの OS には、HiRDB サーバ以外の端末からリモートログインすることはできないものとする。

A.SERVER_SOFTWARE（HiRDBサーバにおけるソフトウェア構成）

HiRDB サーバには、OS、TOE、および SORT 以外のソフトウェアはインストールされないものとする。

A.CLIENT_OF_SERVER（HiRDBサーバにおけるクライアント機能の制限）

HiRDB サーバにおけるクライアント機能は、使用されないものとする。

A.SERVER_HARDWARE（サーバにおけるハードウェア等の管理）

HiRDB サーバのためのハードウェアと周辺機器は、許可された管理者だけが入場できる場所に設置されるものとする。

A.NETWORK（ネットワーク）

HiRDB サーバには HiRDB クライアントだけが接続され、HiRDB サーバと HiRDB クライアント間の通信の秘匿性と完全性は、確保されているものとする。

A.HiRDB_CLIENT（HiRDBクライアント）

HiRDB クライアントでは、UAP と HiRDB SQL Executer 以外のネットワークを介して電文を送信できるソフトウェアは使用されないものとする。また、電文の送信先となる HiRDB サーバのポート番号を設定する環境変数には定められた値が設定され、変更がないように維持されるものとする。

A.UAP（UAPの管理）

HiRDB クライアントで使用される UAP は、TOE で定められているプロトコルに従った電文のみを HiRDB サーバに送信するよう、TOE のガイダンスに従って開発されるものとする。また、XA 連携機能は使用されないものとする。

A.ADMINISTRATORS（許可された管理者）

許可された管理者は、HiRDB サーバおよび HiRDB クライアントに対して、悪意のある操作を行わない。

A.PASSWORD（パスワードの管理）

DB ユーザのパスワードは、他人に知られないように本人によって管理される。パスワードは推測されにくいものが設定され、適切な頻度で変更される。

3.3. 脅威

3.3.1. 脅威エージェント

セキュリティ侵害を意図的、または偶然に試みる脅威エージェントを、以下のように定義する。

- 不正な利用者（TOE に接続を許可されていない者、および TOE に接続を許可されている利用者であっても他人になりすまして TOE への接続を試みる者）
- 正しく識別･認証された一般 DB ユーザ

上記の脅威エージェントは、いずれも高度な専門知識を持たず、攻撃用の特別なツールを利用することも無く、セキュリティ侵害を行う動機は強くないものとする。

3.3.2. 脅威の識別

T.ILLEGAL_CONNECT（不正な接続）

不正な利用者が、TOE に接続し、SQL を実行することによって、利用者データを暴露･改ざん･削除するかもしれない。

T.UNAUTHORIZED_ACCESS（権限外のアクセス）

正しく識別･認証された一般 DB ユーザが、SQL を実行することによって、本来は権限のない利用者データを暴露･改ざん･削除するかもしれない。

T.UNAUTHORIZED_PERMISSION_MODIFY（権限外の権限情報とパスワードの改ざん）

正しく識別･認証された一般 DB ユーザが、SQL を実行することによって、自身や他の利用者の権限情報、またはパスワードを改ざんして、本来は権限のない利用者データを暴露･改ざん･削除する結果を引き起こすかもしれない。

3.4. 組織のセキュリティ方針

P. ACCESS_PRIVILEGE（アクセス権限の管理）

スキーマ所有者は、本人が所有するユーザ表のアクセス権限を管理しなければならない。

P.DATABASE_ADMINISTRATOR（DBA権限保持者）

DBA 権限保持者は、監査人以外の識別･認証情報、DBA 権限、およびスキーマ定義権限を管理しなければならない。

P.AUDITOR（監査人）

監査人は、必要に応じ、セキュリティ機能に関する操作の中から監査対象事象を選択し、監査業務を実施しなければならない。監査証跡参照者を設ける場合は、監査人は信頼できる人物にその役割を委任しなければならない。

P.AUDIT_VIEWER（監査証跡参照者）

監査証跡参照者は、監査人の指示に従って監査データをチェックすることにより、監査人の業務を補佐しなければならない。

P.SECURITY_PARAMETER（セキュリティ変数）

DBA 権限保持者は、パスワードの最小文字数、連続認証失敗許容回数、および認可識別子のロック時間をセキュアな値に維持しなければならない。

4. セキュリティ対策方針

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

4.1. TOE セキュリティ対策方針

O.I&A（TOEにおける識別・認証）

TOE は、利用者が TOE に接続しようとするときに識別･認証を実施し、これをパスした場合にのみ DB ユーザとして接続を許可する。TOE は、DB ユーザに対して、本人のパスワードを変更する機能を提供する。TOE は、DB ユーザのパスワード長を、事前に設定された最小文字数以上に維持する機能、および同一の認可識別子による連続した認証の失敗が、事前に設定された許容回数を上回った場合、事前に設定された時間が経つまで、その認可識別子をロックする機能を提供する。TOE は、パスワード最小文字数、連続認証失敗許容回数、および認可識別子のロック時間の設定を DBA 権限保持者に制限する。

O.ACCESS_CONTROL（アクセス制御）

TOE は、DB ユーザに与えられた権限に従って、DB ユーザによる利用者データへのアクセスを制御する機能を提供する。

O.ACCESS_PRIVILEGE（アクセス権限の管理）

TOE は、スキーマ所有者に対してのみ、本人の所有するユーザ表のアクセス権限を管理する機能を提供する。

O.DATABASE_ADMINISTRATOR（DBA権限保持者）

TOE は、DBA 権限保持者に対してのみ、監査人以外の識別･認証情報、DBA 権限、およびスキーマ定義権限を管理する機能を提供する。

O.AUDIT（監査）

TOE は、セキュリティ機能に関する操作の中から、監査対象事象を表単位および事象種別の単位で選択させる機能を監査人に対して提供する。TOE は、監査対象事象が発生した場合、それを監査データとして記録する。TOE は、監査人と監査証跡参照者に対して、監査データを検索し出力する機能を提供する。

4.2. 環境セキュリティ対策方針

4.2.1. IT 環境のセキュリティ対策方針

本 ST では、IT 環境のセキュリティ対策方針は必要としない。

4.2.2. Non-IT 環境のセキュリティ対策方針

OEN.SERVER_HARDWARE（サーバにおけるハードウェア等の管理）

HiRDB サーバのためのハードウェアと周辺機器は、許可された管理者だけが入場できる場所に設置されなければならない。

OEN. HiRDB_SERVER_CONFIG（HiRDBサーバの設定）

スーパユーザは、HiRDB サーバにインストールされた OS へのリモートログインが禁止されるように設定しなければならない。

OEN. SERVER_SOFTWARE（HiRDBサーバにおけるソフトウェア構成）

スーパユーザは、OS、TOE、および SORT 以外のソフトウェアを HiRDB サーバにインストールすることを制限しなければならない。

OEN. OS_ACCOUNT（OSアカウントの管理）

スーパユーザは、許可された管理者以外の者に対して HiRDB サーバの OS のアカウントを与えてはならない。

OEN.CLIENT_OF_SEVER（HiRDBサーバにおけるクライアント機能の制限）

HiRDB サーバにおけるクライアント機能の使用は、禁止されなければならない。

OEN.NETWORK（ネットワーク管理）

ネットワークには、HiRDB サーバと HiRDB クライアント以外の機器を接続してはならない。

OEN.HiRDB_CLIENT（HiRDBクライアントの管理）

HiRDB クライアントでは、UAP と HiRDB SQL Executer 以外のネットワークを介して電文を送信できるソフトウェアの使用は禁止されなければならない。また、電文の送信先となる HiRDB サーバのポート番号を設定する環境変数には定められた値が設定され、変更がないように維持されなければならない。

OEN.UAP（UAPの管理）

UAP 管理者は、以下に示す事が守られるようにしなければならない。

- UAP は TOE で定められているプロトコルに従った電文のみを HiRDB サーバに送信するよう、TOE

のガイダンスに従って開発される。

- UAP は XA 連携機能を使用しない。

OEN. ADMINISTRATORS（許可された管理者）

許可された管理者は、HiRDB サーバおよび HiRDB クライアントに対して、悪意のある操作を行ってはならない。

OEN. SCHEMA_OWNER（スキーマ所有者）

スキーマ所有者は、TOE のガイダンス文書に従って、本人が所有するユーザ表のアクセス権限を管理しなければならない。

OEN. DATABASE_ADMINISTRATOR（DBA権限保持者）

DBA 権限保持者は、TOE のガイダンス文書に従って、監査人以外の識別･認証情報、DBA 権限、およびスキーマ定義権限を管理しなければならない。

OEN.AUDITOR（監査人）

監査人は、ユーザ表に格納されるデータの重要度に応じて監査対象事象を設定し、監査業務を実施しなければならない。また、監査証跡参照者を設ける場合には、監査人は信頼できる人物に対して、その役割を委任しなければならない。

OEN.AUDIT_VIEWER（監査証跡参照者）

監査証跡参照者は、監査人の指示に従って監査データを参照し、これをチェックしなければならない。また、不穏な事象を発見した場合には、監査人に報告しなければならない。

OEN.PASSWORD（パスワードの管理）

DB ユーザは、自分自身のパスワードを管理し、他人に漏らしてはいけない。また、TOE のガイダンス文書に従って、適切なパスワードを設定し、適切な頻度でパスワードを変更しなければならない。

OEN. SECURITY_PARAMETER（セキュリティ変数）

DBA 権限保持者は、TOE のガイダンス文書に従って、パスワードの最小文字数、連続認証失敗許容回数、および認可識別子のロック時間をセキュアな値に維持しなければならない。

5. IT セキュリティ要件

本章では、TOE セキュリティ要件について記述する。

5.1. TOE セキュリティ要件

5.1.1. TOE セキュリティ機能要件

機能要件の操作（選択、割付、詳細化）について、表記方法を以下に示す。
選択の場合は、［選択 ： 選択した内容 ］、
割付の場合は、［割付 ： 割付した内容 ］、
詳細化の場合は、［詳細化 ： 詳細化した内容 ］ のように表記する。
また、補足説明を他の節にて記載する場合は、注釈: を表記してその旨を示す。

① セキュリティ監査（FAU）

FAU_GEN.1 監査データ生成

下位階層 ： なし

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない:

a) 監査機能の起動と終了
b) 監査の ［選択 ： 指定なし］ レベルのすべての監査対象事象;及び
c) ［割付 ： 以下の監査対象事象］。

＜監査対象事象＞

各機能要件を選択した場合に監査対象とすべきアクション（CC における規定）と、それに関連する TOE の監査対象事象を表 5-1 に示す。下線は対応する監査レベルを表す。

表 5-1 ： 監査対象とすべきアクション（CC における規定）と関連する監査対象事象

機能要件	監査対象とすべきアクション	監査対象事象
FAU_GEN.1	なし	なし
FAU_GEN.2	なし	なし
FAU_SAR.1	基本:監査記録からの情報の読み出し	・ 監査証跡表の行検索
FAU_SAR.2	基本:監査記録からの成功しなかった情報の読み出し	・ 監査証跡表の行検索（失敗）
FAU_SAR.3	詳細:閲覧に使用されるパラメタ	なし
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	・ 監査対象事象の登録、除外
FAU_STG.1	なし	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	・ 監査記録の上書き開始
FDP_ACC.1	なし	なし
FDP_ACF.1	最小:SFP で扱われるオブジェクトに対する操作の実行における成功した要求 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 詳細:アクセスチェック時に用いられる特定のセキュリティ属性	・ ユーザ表の操作 ・ ユーザ表の削除
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)	・ 認可識別子のロック、ロック解除
FIA_ATD.1	なし	なし
FIA_SOS.1	最小:TSF による、テストされた秘密の拒否 基本:TSF による、テストされた秘密の拒否または受け入れ 詳細:定義された品質尺度に対する変更の識別	・ パスワードの登録、変更
FIA_UAU.2	最小:認証メカニズムの不成功になった使用 基本:認証メカニズムのすべての使用	・ 接続
FIA_UID.2	最小:提供される利用者識別情報を含む、利用者識別メカニズムの不成功使用 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	・ 接続
FIA_USB.1	最小:利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成) 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)	・ 接続(失敗及び成功)
FMT_MSA.1	基本:セキュリティ属性の値の改変すべて	・ 認可識別子の登録、削除 ・ アクセス権限の付与、取消し ・ DBA 権限の付与、取消し
FMT_MSA.3	基本:許可的あるいは制限的規則のデフォルト設定の改変 基本:セキュリティ属性の初期値の改変すべて	なし

FMT_MTD.1	基本：TSF データの値のすべての改変	・ パスワードの登録、削除、変更 ・ スキーマ定義権限の付与、取消し ・ 監査証跡表の参照権限の付与、取消し ・ 監査対象事象の登録、除外 ・ 連続認証失敗許容回数の変更 ・ パスワード最小文字数の変更 ・ ロック時間の変更
FMT_SMF.1	最小：管理機能の使用	・ 認可識別子の登録、削除 ・ パスワードの登録、変更、削除 ・ DBA 権限の付与、取消し ・ スキーマ定義権限の付与、取消し ・ アクセス権限の付与、取消し ・ 監査証跡表の参照権限の付与、取消し ・ 監査対象事象の登録、除外 ・ 監査証跡表の行削除 ・ 連続認証失敗許容回数の変更 ・ パスワード最小文字数の変更 ・ ロック時間の変更

FMT_SMR.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 詳細:役割の権限の使用すべて	・ 認可識別子の登録、削除 ・ パスワードの登録、削除、変更 ・ DBA 権限の付与、取消し ・ スキーマ定義権限の付与、取消し ・ アクセス権限の付与、取消し ・ ユーザ表の定義、削除 ・ 監査証跡表の参照権限の付与、取消し ・ 監査証跡表の行検索、行削除 ・ 監査対象事象の登録、除外 ・ 連続認証失敗許容回数の変更 ・ パスワード最小文字数の変更 ・ ロック時間の変更 ・ ユーザ表の操作
FPT_RVM.1	なし	なし
FPT_SEP.1	なし	なし
FPT_STM.1	最小:時間の変更 詳細:タイムスタンプの提供	なし

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付･時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗);及び

b) 各監査事象の種別に対して、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 : 以下の追加される監査情報］

＜追加される監査情報＞

各監査対象事象ごとに監査記録に追加される監査情報を表 5-2 に示す。

表 5-2 : 監査対象事象ごとに監査記録に追加される監査情報

監査対象事象	追加される監査情報
監査証跡表の行検索、行削除	監査証跡表の識別情報
監査対象事象の登録、除外	なし
監査記録の上書き開始	なし
ユーザ表の操作	ユーザ表の識別情報
認可識別子のロック、ロック解除	認可識別子
接続	認可識別子

認可識別子の登録、削除	登録、削除された認可識別子
パスワードの登録、削除、変更	パスワードを登録、削除、変更された DB ユーザの認可識別子
DBA 権限の付与、取消し	DBA 権限を付与、取消された DB ユーザの認可識別子
スキーマ定義権限の付与、取消し	スキーマ定義権限を付与、取消された DB ユーザの認可識別子
アクセス権限の付与、取消し	アクセス権限を付与、取消された DB ユーザの認可識別子 アクセス権限の対象であるユーザ表の識別情報
ユーザ表の定義、削除	ユーザ表の識別情報
監査証跡表の参照権限の付与、取消し	監査証跡表の参照権限を付与、取消された DB ユーザの認可識別子 監査証跡表の識別情報
連続認証失敗許容回数の変更	変更前後の値
パスワード最小文字数の変更	変更前後の値
ロック時間の変更	変更前後の値

依存性 ： **FPT_STM.1** 高信頼タイムスタンプ

FAU_GEN.2 利用者識別情報の関連付け

下位階層 ： なし

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なければならない。

依存性 ： **FAU_GEN.1** 監査データ生成
FIA_UID.1 識別のタイミング

FAU_SAR.1 監査レビュー

下位階層 ： なし

FAU_SAR.1.1 TSF は、[割付 ： 監査人、監査証跡参照者] が、[割付 ： 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)、追加される監査情報] を、監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2 TSF は、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

依存性 ： **FAU_GEN.1** 監査データ生成

FAU_SAR.2 限定監査レビュー

下位階層 ： なし

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。

依存性 ： **FAU_SAR.1** 監査レビュー

FAU_SAR.3 選択可能監査レビュー

下位階層 ： なし

FAU_SAR.3.1 TSF は、[割付 ： 監査データの任意の情報の大小関係や同値関係] に基づいて、監査データを [選択 ： 検索、並べ替え] する能力を提供しなければならない。

依存性 ： **FAU_SAR.1** 監査レビュー

FAU_SEL.1 選択的監査

下位階層 ： なし

FAU_SEL.1.1 TSF は以下のような属性に基づいて、監査事象のセットから監査対象事象を含めたり、除外したりすることができなければならない：

a) [選択 ： オブジェクト識別情報、事象種別]

b) [割付 ： 事象の結果 (成功または失敗)]。

依存性 ： **FAU_GEN.1** 監査データ生成

FMT_MTD.1 TSFデータの管理

FAU_STG.1 保護された監査証跡格納

下位階層 ： なし

FAU_STG.1.1 TSF は、格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡内の格納された監査記録への不正な改変を [選択 ： 防止] できねばならない。

依存性 ： **FAU_GEN.1** 監査データ生成

FAU_STG.4 監査データ損失の防止

下位階層 ： **FAU_STG.3**

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[選択 ： 最も古くに格納された監査記録への上書き] 及び [割付 ： 上書き開始を通知するメッセージ出力のアクション] を行わねばならない。

依存性 ： **FAU_STG.1** 保護された監査証跡格納

② 利用者データ保護 (FDP)

FDP_ACC.1 サブセットアクセス制御

下位階層 ： なし

FDP_ACC.1.1 TSF は、[割付 ： 以下のサブジェクト、オブジェクト、サブジェクトとオブジェクト間の操作] に対して [割付 ： HiRDB アクセス制御方針] を実施しなければならない。

＜サブジェクト＞

- DB ユーザのサーバプロセス

＜オブジェクト＞

- ユーザ表

＜サブジェクトとオブジェクト間の操作＞

- 行検索
- 行挿入
- 行削除
- 行更新

依存性 ： **FDP_ACF.1** セキュリティ属性によるアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層 ： なし

FDP_ACF.1.1 TSF は、以下の [割付 ： サブジェクト属性、オブジェクト属性] に基づいて、オブジェクトに対して、[割付 ： HiRDB アクセス制御方針] を実施しなければならない。

＜サブジェクト属性＞

- 認可識別子
- アクセス権限（SELECT 権限、INSERT 権限、DELETE 権限、UPDATE 権限）
- DBA 権限

＜オブジェクト属性＞

- ユーザ表の所有者の認可識別子

FDP_ACF.1.2 TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない：[割付 ： 以下の規則]。

＜規則＞

{オブジェクトがユーザ実表の場合}

(a) サーバプロセスに関連付けられた DB ユーザの認可識別子が、操作の対象となるユーザ実表の所有者の認可識別子と一致する場合、サーバプロセスがそのユーザ実表に対して要求する操作は許可される。

(b) サーバプロセスに関連付けられた DB ユーザが、操作の対象となるユーザ実表の SELECT 権限を有する場合、サーバプロセスがそのユーザ実表に対して要求する行検索は許可される。

(c) サーバプロセスに関連付けられた DB ユーザが、操作の対象となるユーザ実表の INSERT 権限を有する場合、サーバプロセスがそのユーザ実表に対して要求する行挿入は許可される。

(d) サーバプロセスに関連付けられた DB ユーザが、操作の対象となるユーザ実表の DELETE 権限を有する場合、サーバプロセスがそのユーザ実表に対して要求する行削除は許可される。

(e) サーバプロセスに関連付けられた DB ユーザが、操作の対象となるユーザ実表の UPDATE 権限を有する場合、サーバプロセスがそのユーザ実表に対して要求する行更新は許可される。

(e2) サーバプロセスに関連付けられた DB ユーザが、DBA 権限を有する場合、サーバプロセスがそのユーザ実表に対して要求する行削除は許可される。

(f) 上記(a)、(b)以外、ユーザ実表に対して要求する行検索は許可されない。

(g) 上記(a)、(c)以外、ユーザ実表に対して要求する行挿入は許可されない。

(h) 上記(a)、(d) 、(e2)以外、ユーザ実表に対して要求する行削除は許可されない。

(i) 上記(a)、(e)以外、ユーザ実表に対して要求する行更新は許可されない。

{オブジェクトが、大本となるユーザ実表がすべて所有者本人のものであるユーザビュー表の場合}

(j) サーバプロセスに関連付けられた DB ユーザの認可識別子が、操作の対象となるユーザビュー表の所有者の認可識別子と一致する場合、サーバプロセスがそのユーザビュー表に対して要求する操作は許可される。

(k) サーバプロセスに関連付けられた DB ユーザが、操作の対象となるユーザビュー表の SELECT 権限を有する場合、サーバプロセスがそのユーザビュー表に対して要求する行検索は許可される。

(l) サーバプロセスに関連付けられた DB ユーザが、操作の対象となるユーザビュー表の INSERT 権限

を有する場合、サーバプロセスがそのユーザビュー表に対して要求する行挿入は許可される。
(m) サーバプロセスに関連付けられたDBユーザが、操作の対象となるユーザビュー表のDELETE権限を有する場合、サーバプロセスがそのユーザビュー表に対して要求する行削除は許可される。
(n) サーバプロセスに関連付けられたDBユーザが、操作の対象となるユーザビュー表のUPDATE権限を有する場合、サーバプロセスがそのユーザビュー表に対して要求する行更新は許可される。
(o) 上記(j)、(k)以外、ユーザビュー表に対して要求する行検索は許可されない。
(p) 上記(j)、(l)以外、ユーザビュー表に対して要求する行挿入は許可されない。
(q) 上記(j)、(m)以外、ユーザビュー表に対して要求する行削除は許可されない。
(r) 上記(j)、(n)以外、ユーザビュー表に対して要求する行更新は許可されない。

{オブジェクトが、大本となるユーザ実表に所有者本人以外のものが含まれるユーザビュー表の場合}
(s) サーバプロセスに関連付けられたDBユーザの認可識別子が、操作の対象となるユーザビュー表の所有者の認可識別子と一致し、かつ、サーバプロセスに関連付けられたDBユーザが、そのユーザビュー表の基になるすべてのユーザ表のSELECT権限を有する場合、サーバプロセスがそのユーザビュー表に対して要求する行検索は許可される。
(t) サーバプロセスに関連付けられたDBユーザの認可識別子が、操作の対象となるユーザビュー表の所有者の認可識別子と一致し、かつ、サーバプロセスに関連付けられたDBユーザが、そのユーザビュー表の定義時以来そのユーザビュー表の基になるユーザ表のINSERT権限を持ち続けている場合、サーバプロセスがそのユーザビュー表に対して要求する行挿入は許可される。
(u) サーバプロセスに関連付けられたDBユーザの認可識別子が、操作の対象となるユーザビュー表の所有者の認可識別子と一致し、かつ、サーバプロセスに関連付けられたDBユーザが、そのユーザビュー表の定義時以来そのユーザビュー表の基になるユーザ表のDELETE権限を持ち続けている場合、サーバプロセスがそのユーザビュー表に対して要求する行削除は許可される。
(v) サーバプロセスに関連付けられたDBユーザの認可識別子が、操作の対象となるユーザビュー表の所有者の認可識別子と一致し、かつ、サーバプロセスに関連付けられたDBユーザが、そのユーザビュー表の定義時以来そのユーザビュー表の基になるユーザ表のUPDATE権限を持ち続けている場合、サーバプロセスがそのユーザビュー表に対して要求する行更新は許可される。
(w) 上記(s)以外、ユーザビュー表に対して要求する行検索は許可されない。
(x) 上記(t)以外、ユーザビュー表に対して要求する行挿入は許可されない。
(y) 上記(u)以外、ユーザビュー表に対して要求する行削除は許可されない。
(z) 上記(v)以外、ユーザビュー表に対して要求する行更新は許可されない。

FDP_ACF.1.3 TSF は、以下の追加規則に基づいて、オブジェクトに対するサブジェクトのアクセスを明示的に承認しなければならない：[割付 ： 以下の規則]

＜規則＞
なし

FDP_ACF.1.4 TSF は、[割付 ： 以下の規則] 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。

＜規則＞

なし

依存性 ： **FDP_ACC.1** サブセットアクセス制御

FMT_MSA.3 静的属性初期化

③ 識別と認証（FIA）

FIA_AFL.1 認証失敗時の取り扱い

下位階層 ： なし

FIA_AFL.1.1 TSF は、[割付 ： 同一認可識別子を指定する連続した識別･認証試行] に関して、[選択 ： 「[割付 ： 1～10] 内における管理者設定可能な正の整数値」] 回の不成功認証試行が生じた時を検出しなければならない。

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 ： 以下のアクション] をしなければならない。

＜アクション＞

- 認可識別子をロックし、ロック時間が経過した時点でロックを解除する。

依存性 ： **FIA_UAU.1** 認証のタイミング

FIA_ATD.1 利用者属性定義

下位階層 ： なし

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

＜セキュリティ属性＞

- 認可識別子
- DBA 権限
- 監査権限
- スキーマ定義権限
- アクセス権限
- 監査証跡表の参照権限

依存性 ： なし

FIA_SOS.1 秘密の検証

下位階層 ： なし

FIA_SOS.1.1 TSF は、秘密が［割付 ： 以下の品質尺度］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。

＜品質尺度＞

- 認証に用いられるパスワードは、6～15 内における管理者設定可能なパスワード最小文字数以上 30 文字以下の半角文字（英大文字、英小文字、数字）で構成される。

依存性 ： なし

FIA_UAU.2 アクション前の利用者認証

下位階層 ： **FIA_UAU.1**

FIA_UAU.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に認証が成功することを要求しなければならない。

依存性 ： **FIA_UID.1** 識別のタイミング

FIA_UID.2 アクション前の利用者識別

下位階層 ： **FIA_UID.1**

FIA_UID.2.1 TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

依存性 ： なし

FIA_USB.1 利用者・サブジェクト結合

下位階層 ： なし

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

＜利用者セキュリティ属性＞

- 認可識別子
- DBA 権限
- 監査権限
- スキーマ定義権限
- アクセス権限
- 監査証跡表の参照権限

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 ： 以下の規則]。

＜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 ： 以下の規則]。

＜規則＞

なし

依存性 ： **FIA_ATD.1** 利用者属性定義

④ セキュリティ管理（FMT）

FMT_MSA.1 セキュリティ属性の管理

下位階層 ： なし

FMT_MSA.1.1 TSF は、セキュリティ属性 [割付 ： 以下のセキュリティ属性] に対し [選択 ： [割付 ： 以下の操作]] をする能力を [割付 ： 以下の役割] に制限するために [割付 ： HiRDB アクセス制御方針] を実施しなければならない。

＜セキュリティ属性＞	＜操作＞	＜役割＞
監査人以外の認可識別子	登録、削除	DBA 権限保持者
本人が所有するユーザ表に対する他人のアクセス権限	付与、取消し	スキーマ所有者
他人の DBA 権限	付与、取消し	DBA 権限保持者

依存性 ： [**FDP_ACC.1** サブセットアクセス制御 または
FDP_IFC.1 サブセット情報フロー制御]

FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

FMT_MSA.3 静的属性初期化

下位階層 ： なし

FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択 ： 制限的] デフォルト値を与える [割付 ： HiRDB アクセス制御方針] を実施しなければならない。

FMT_MSA.3.2 TSF は、オブジェクトや情報が生成されるとき、[割付 ： 以下の役割] 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。

＜役割＞

なし

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

FMT_MTD.1 TSFデータの管理

下位階層 ： なし

FMT_MTD.1.1 TSF は、[割付 ： 以下の TSF データ] を [選択 ： [割付 ： 以下の操作]] する能力を [割付 ： 以下の役割] に制限しなければならない。

＜TSF データ＞	＜操作＞	＜役割＞
監査人以外のパスワード	登録、削除、改変	DBA 権限保持者
本人のパスワード	改変	DB ユーザ
他人のスキーマ定義権限	付与、取消し	DBA 権限保持者
監査証跡表に対する監査人以外の参照権限	付与、取消し	監査人
監査対象事象	登録、除外	監査人
監査データ（監査証跡表）	削除	監査人
連続認証失敗許容回数	設定、変更	DBA 権限保持者
パスワード最小文字数	設定、変更	DBA 権限保持者
ロック時間	設定、変更	DBA 権限保持者

依存性 ： **FMT_SMF.1** 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_SMF.1 管理機能の特定

下位階層 : なし

FMT_SMF.1.1 TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない:[割付 : 以下のセキュリティ管理機能]。

＜セキュリティ管理機能＞

各機能要件を選択した場合に管理機能と考えるアクション(CC における規定)と、それに対応するセキュリティ管理機能を表 5-3 に示す。

表 5-3 : 管理機能と考えるアクション(CC における規定)と対応するセキュリティ管理機能

機能要件	管理機能と考えるアクション	セキュリティ管理機能	相当する機能要件
FAU_GEN.1	なし	なし	なし
FAU_GEN.2	なし	なし	なし
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)。	監査証跡表の参照権限の付与、取消し	FMT_MTD.1
FAU_SAR.2	なし	なし	なし
FAU_SAR.3	なし	なし	なし
FAU_SEL.1	監査事象を閲覧／改変する権限の維持	監査権限の維持(後述)	なし
FAU_STG.1	なし	なし	なし
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)	なし(後述)	なし
FDP_ACC.1	なし	なし	なし
FDP_ACF.1	明示的なアクセスまたは拒否に基づく決定に使われる属性の管理	なし(後述)	なし
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理	連続認証失敗許容回数の変更	FMT_MTD.1
	b) 認証失敗の事象においてとられるアクションの管理	なし(後述)	
FIA_ATD.1	もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる	なし(後述)	なし

FIA_SOS.1	秘密の検証に使用される尺度の管理	パスワード最小文字数の変更	FMT_MTD.1
FIA_UAU.2	a) 管理者による認証データの管理	DBA 権限保持者によるパスワード登録、変更、削除	FMT_MTD.1
	b) このデータに関係する利用者による認証データの管理	DB ユーザ本人によるパスワード変更	
FIA_UID.2	利用者識別情報の管理	認可識別子の登録、削除	FMT_MSA.1
FIA_USB.1	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	なし（後述）	なし
	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		
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	DBA 権限の付与、取消し スキーマ定義権限の付与、取消し	FMT_MSA.1 FMT_MTD.1
FMT_MSA.3	a) 初期値を特定できる役割のグループを管理すること	なし（後述）	なし
	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		
FMT_MTD.1	TSF データと相互に影響を及ぼし得る役割のグループを管理すること	認可識別子の登録、削除 監査権限の管理（後述） DBA 権限の付与、取消し	FMT_MSA.1
FMT_SMF.1	なし	なし	なし
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理	認可識別子の登録、削除 DBA 権限の付与、取消し スキーマ定義権限の付与、取消し 監査権限の管理（後述） 監査証跡表の参照権限の付与、取消し	FMT_MSA.1 FMT_MTD.1
FPT_RVM.1	なし	なし	なし
FPT_SEP.1	なし	なし	なし
FPT_STM.1	時間の管理	なし（後述）	なし

注釈 ： （後述）となっているものに関しては、CCで規定されている管理機能を完全には満たしていない。その根拠を 8.2.6 セキュリティ管理機能根拠において説明する。

依存性 ： なし

FMT_SMR.1 セキュリティ役割

下位階層 ： なし

FMT_SMR.1.1 TSF は、役割 [割付 ： 以下の役割] を維持しなければならない。

＜役割＞

- DB ユーザ
- DBA 権限保持者
- スキーマ所有者
- 監査人
- 監査証跡参照者

FMT_SMR.1.2 TSF は、利用者を役割に関連付けなければならない。

依存性 ： **FIA_UID.1** 識別のタイミング

⑤ TSF の保護 (FPT)

FPT_RVM.1 TSPの非バイパス性

下位階層 ： なし

FPT_RVM.1.1 TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性 ： なし

FPT_SEP.1 TSFドメイン分離

下位階層 ： なし

FPT_SEP.1.1 TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2 TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性 ： なし

FPT_STM.1 高信頼タイムスタンプ

下位階層 ： なし

FPT_STM.1.1 TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性 ： なし

5.1.2. 最小機能強度レベル

TOE の最小機能強度は、SOF-基本である。

5.1.3. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL4 であり、追加する保証コンポーネント ALC_FLR.1 である。該当する保証コンポーネントを表 5-4 に示す。

表 5-4 ： 保証コンポーネント一覧 （EAL4 + ALC_FLR.1）

保証クラス	保証コンポーネント	
構成管理 （ACM クラス）	**ACM_AUT.1**	部分的な CM 自動化
	ACM_CAP.4	生成の支援と受入手続き
	ACM_SCP.2	問題追跡の CM 範囲
配付と運用 （ADO クラス）	**ADO_DEL.2**	改変の検出
	ADO_IGS.1	設置、生成、及び立上げ手順
開発 （ADV クラス）	**ADV_FSP.2**	完全に定義された外部インタフェース
	ADV_HLD.2	セキュリティ実施上位レベル設計
	ADV_IMP.1	TSF の実装のサブセット
	ADV_LLD.1	記述的下位レベル設計
	ADV_RCR.1	非形式的対応の実証
	ADV_SPM.1	非形式的な TOE セキュリティ方針モデル
ガイダンス文書 （AGD クラス）	**AGD_ADM.1**	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
ライフサイクルサポート （ALC クラス）	**ALC_DVS.1**	セキュリティ手段の識別
	ALC_FLR.1	基本的な欠陥修正
	ALC_LCD.1	開発者によるライフサイクルモデルの定義
	ALC_TAT.1	明確に定義された開発ツール
テスト （ATE クラス）	**ATE_COV.2**	カバレージの分析
	ATE_DPT.1	テスト ： 上位レベル設計
	ATE_FUN.1	機能テスト
	ATE_IND.2	独立テスト - サンプル
脆弱性評定 （AVA クラス）	**AVA_MSU.2**	分析の確認
	AVA_SOF.1	TOE セキュリティ機能強度評価
	AVA_VLA.2	独立脆弱性テスト

6. TOE 要約仕様

本章では、TOE セキュリティ機能、セキュリティ機能強度、セキュリティ保証手段について記述する。

6.1. TOE セキュリティ機能

本節では、TOE セキュリティ機能について記述する。表 6-1 に示すように、本節で説明するセキュリティ機能は、5.1.1 節で記述した TOE セキュリティ機能要件を満足している。

表 6-1 ： TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係

TOE セキュリティ機能要件 / TOE セキュリティ機能	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_SEL.1	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.2	FIA_UID.2	FIA_USB.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1
SF.AUD.GEN	○	○				○													○	○		○	○	○
SF.AUD.TBL			○	○	○		○					○							○	○			○	
SF.AUD.FIL								○															○	
SF.ACC.TBL									○	○												○	○	
SF.I&A.CON														○	○	○						○	○	
SF.I&A.HOW													○										○	
SF.I&A.LCK											○												○	
SF.PRV.CTL												○					○	○	○	○	○		○	

6.1.1. 監査

＜監査の概要＞

TOE は、次の監査機能を提供する。

- 監査対象事象における監査データの採取
- 監査データの検索、並べ替え
- 監査データの保護

監査データには、その格納先となるオブジェクトによって、2種類の状態（データ形式）が存在する。一つは、監査証跡ファイルに格納される監査データであり、もう一方は監査証跡表に格納される監査データである。監査証跡ファイルに格納される監査データは、監査対象事象発生時に出力される監査データであり、そのままで

は参照することはできない。監査証跡表に格納される監査データは、監査証跡ファイルを入力元として登録される監査データであり、参照用に用いられる。両者は内容的に同等である。

SF.AUD.GEN

TOE は、監査対象事象発生時に監査データを採取し、タイムスタンプ（日付と時刻）をつけて、監査対象事象、サブジェクト識別情報、事象の結果、およびその他の監査情報とともに、監査証跡ファイルに記録する。TOE は、タイムスタンプを生成する機能を持つ。

表 6-2 に、事象種別、監査対象事象、および監査対象事象ごとに監査記録に追加される監査情報の対応関係を示す。

TOE は、表 6-2 で示す監査対象事象の発生時に監査データを採取する。

TOE は、表 6-2 で示す事象種別の単位で、監査データを採取する監査対象事象を選択（登録、除外）する機能を提供する。ただし、監査必須事象に属する監査対象事象は予め登録されており、これらの監査対象事象を除外することはできない。また、当該機能では、監査対象となるオブジェクトを選択することができる。さらに、監査対象事象の成功または失敗時にのみ監査データを採取するように選択することができる。TOE は、監査対象事象の選択の実施を、監査人に制限する。

監査データには、以下の監査情報が含まれる。

(a) 事象の日付･時刻 （タイムスタンプを使用する）

(b) 監査対象事象 （例えば、”アクセス権限の付与”）

(c) サブジェクト識別情報 （サーバプロセスに関連付けられる DB ユーザの認可識別子、および接続通番）

(d) 事象の結果 （成功または失敗）

また、各監査対象事象毎に追加される監査情報は、表 6-2 に示す通りである。

表 6-2 ： 事象種別、監査対象事象、および監査対象事象ごとに監査記録に追加される監査情報の対応関係

事象種別	監査対象事象	追加される監査情報
監査必須事象	監査機能の起動と終了	なし
	監査証跡表の行検索、行削除	監査証跡表の識別情報
	監査対象事象の登録、除外	なし
	監査記録の上書き開始	なし
	認可識別子のロック、ロック解除	認可識別子
	連続認証失敗許容回数の変更	変更前後の値
	パスワード最小文字数の変更	変更前後の値
	ロック時間の変更	変更前後の値
接続	接続	認可識別子

権限の付与 （GRANT 文の実行）	認可識別子とパスワードの登録	登録された認可識別子
	パスワードの変更	パスワードを変更された DB ユーザの認可識別子
	DBA 権限の付与	DBA 権限を付与された DB ユーザの認可識別子
	スキーマ定義権限の付与	スキーマ定義権限を付与された DB ユーザの認可識別子
	アクセス権限の付与	アクセス権限を付与された DB ユーザの認可識別子
		アクセス権限の対象であるユーザ表の識別情報
	監査証跡表の参照権限の付与	監査証跡表の参照権限を付与された DB ユーザの認可識別子
		監査証跡表の識別情報
権限の取消し （REVOKE 文の実行）	認可識別子とパスワードの削除	削除された認可識別子
	DBA 権限の取消し	DBA 権限を取消された DB ユーザの認可識別子
	スキーマ定義権限の取消し	スキーマ定義権限を取消された DB ユーザの認可識別子
	アクセス権限の取消し	アクセス権限を取消された DB ユーザの認可識別子
		アクセス権限の対象であるユーザ表の識別情報
	監査証跡表の参照権限の取消し	監査証跡表の参照権限を取消された DB ユーザの認可識別子
		監査証跡表の識別情報
オブジェクトの定義	ユーザ表の定義	ユーザ表の識別情報
オブジェクトの削除	ユーザ表の削除	ユーザ表の識別情報
ユーザ表の行検索	ユーザ表の行検索	ユーザ表の識別情報
ユーザ表の行挿入	ユーザ表の行挿入	ユーザ表の識別情報
ユーザ表の行削除	ユーザ表の行削除	ユーザ表の識別情報
ユーザ表の行更新	ユーザ表の行更新	ユーザ表の識別情報

＜注釈＞

顧客情報のような重要なデータが格納されるユーザ表については、すべての操作が監査対象事象として設定

されるべきであり、消費者に公開される商品価格のようなデータが格納されるユーザ表については、最低でも行更新は監査対象事象として設定されるべきである。このように監査対象事象は、ユーザ表で扱うデータの重要度と特性に応じて、ユーザ表毎に監査人によって設定される。

SF.AUD.TBL

監査証跡表は、監査データを検索、並べ替えするために使用される。

監査証跡表は、監査データに記録されるすべての監査情報に対応する列を含む。

TOE は、監査証跡表に関する以下の機能を提供する。

(1) TOE は、すべての監査情報を監査証跡表から読み出す機能を提供する。監査データは行検索の機能で検索、並べ替えを行うことができ、その結果が出力される。監査データの検索、並べ替えは、任意の監査情報の大小関係や同値関係に基づいて行うことができる。監査証跡表の監査データの検索、並べ替えは、監査人および監査証跡参照者(監査証跡表の参照権限を与えられた DB ユーザ)にのみ許可される。TOE は、監査証跡表の参照権限の付与･取消しを、監査人にのみ許可する。

(2) TOE は、監査証跡表の監査データを削除する機能を提供する。監査証跡表の監査データ(行)の削除は、監査人に対してのみ許可される。なお、監査証跡表に対する操作系 SQL による行挿入、行更新はどの DB ユーザにも許可されない。

SF.AUD.FIL

TOE は、監査対象事象発生時に、監査データを監査証跡ファイルに出力する。TOE は、監査証跡ファイルを複数作成し、各監査証跡ファイルを順番に使用することで世代管理を行う。TOE は、監査データを出力中の監査証跡ファイルが満杯になった時点で、次の世代の監査証跡ファイルに出力先を変更する。出力先から切替えられた監査証跡ファイルの監査データは、適時監査人によって監査証跡表に登録されなければならない。

監査証跡ファイルの状態を以下に示す。

【現用】　：　監査データの出力先となっている監査証跡ファイル

【登録待ち】：　満杯後、中身の監査データが未だ監査証跡表へ登録されていない監査証跡ファイル

【登録済み】：　中身の監査データが監査証跡表へ登録された監査証跡ファイル

TOE は、登録済みとなった監査証跡ファイルを再度現用として使用することで、監査データの出力先をローテーションで変更する。TOE は、現用に変更することができる登録済みの監査証跡ファイルがなくなると、最も古くに現用となった登録待ちの監査証跡ファイルを監査データの出力先(現用)とし、上書き開始を通知するメッセージを出力する。

6.1.2. アクセス制御

＜アクセス制御の概要＞

アクセス制御の対象オブジェクトは、ユーザ表(ユーザ実表、ユーザビュー表)である。ユーザ表にアクセス可能なのは、TOE に接続する DB ユーザである。TOE は、スキーマ所有者(ユーザ表の所有者)の自由裁量に基づく任意アクセス制御をサポートする。

SF.ACC.TBL

アクセスを試みる DB ユーザがアクセス対象であるユーザ表の所有者であるかどうかは、DB ユーザの認可識別子とユーザ表の所有者の認可識別子が一致するかどうかで決定される。

なお、以下のアクセス制御をバイパスする手段は提供されない。

TOE は、表 6-3、表 6-4、表 6-5 に示すように、操作系 SQL のアクセス制御を実施する。

表 6-3 ： ユーザ実表を対象とする操作系 SQL のアクセス規則

操作系 SQL を実行する DB ユーザ	操作系 SQL の種別			
	行検索	行挿入	行削除	行更新
操作の対象となるユーザ実表の所有者	○	○	○	○
操作の対象となるユーザ実表の SELECT 権限を持つ DB ユーザ	○	－	－	－
操作の対象となるユーザ実表の INSERT 権限を持つ DB ユーザ	－	○	－	－
操作の対象となるユーザ実表の DELETE 権限を持つ DB ユーザ	－	－	○	－
操作の対象となるユーザ実表の UPDATE 権限を持つ DB ユーザ	－	－	－	○
上記以外の DB ユーザ	×	×	×	×

○ ： 許可される

× ： 許可されない

－ ： 許可／不許可は定まらない

表 6-4 ： 大本となるユーザ実表がすべて所有者本人のものであるユーザビュー表を対象とする操作系 SQL のアクセス規則

操作系 SQL を実行する DB ユーザ	操作系 SQL の種別			
	行検索	行挿入	行削除	行更新
操作の対象となるユーザビュー表の所有者	○	○	○	○
操作の対象となるユーザビュー表の SELECT 権限を持つ DB ユーザ	○	－	－	－
操作の対象となるユーザビュー表の INSERT 権限を持つ DB ユーザ	－	○	－	－
操作の対象となるユーザビュー表の DELETE 権限を持つ DB ユーザ	－	－	○	－
操作の対象となるユーザビュー表の UPDATE 権限を持つ DB ユーザ	－	－	－	○
上記以外の DB ユーザ	×	×	×	×

○ ： 許可される （ただし、読込み専用ビューに対して行検索以外の操作を実行することはできない）
× ： 許可されない
－ ： 許可／不許可は定まらない

表 6-5 ： 大本となるユーザ実表に所有者本人以外のものが含まれるユーザビュー表を対象とする操作系 SQL のアクセス規則

操作系 SQL を実行する DB ユーザ	操作系 SQL の種別			
	行検索	行挿入	行削除	行更新
操作の対象となるユーザビュー表の所有者であり、かつそのユーザビュー表の基になるすべてのユーザ表の SELECT 権限を持つ DB ユーザ	○	－	－	－
操作の対象となるユーザビュー表の所有者であり、かつそのユーザビュー表の定義時以来そのユーザビュー表の基になるユーザ表の INSERT 権限を持ち続けている DB ユーザ	－	○	－	－
操作の対象となるユーザビュー表の所有者であり、かつそのユーザビュー表の定義時以来そのユーザビュー表の基になるユーザ表の DELETE 権限を持ち続けている DB ユーザ	－	－	○	－
操作の対象となるユーザビュー表の所有者であり、かつそのユーザビュー表の定義時以来そのユーザビュー表の基になるユーザ表の UPDATE 権限を持ち続けている DB ユーザ	－	－	－	○
上記以外の DB ユーザ	×	×	×	×

○ ： 許可される （ただし、読込み専用ビューに対して行検索以外の操作を実行することはできない）
× ： 許可されない
－ ： 許可／不許可は定まらない

＜ 注釈 ： ユーザビュー表の操作 ＞

ユーザビュー表に対する操作系 SQL の実行結果は、ユーザビュー表の基になるユーザ実表のデータ（行）に反映される。

＜ ユーザ実表の削除の規則 ＞

TOE は、ユーザ実表の削除（定義系 SQL の一つ）をその表の所有者と DBA 権限保持者に制限する。ユーザ実表の削除に伴い、その表の行はすべて削除される。

6.1.3. 識別･認証

＜識別･認証の概要＞

TOE は、TOE にアクセスする DB ユーザを識別し、その DB ユーザの本人確認を行う。識別･認証は、DB ユ

ーザが HiRDB サーバに接続する場合において、認可識別子とパスワードを用いて行なう。DB ユーザの接続要求は HiRDB クライアントから行われる。

SF.I&A.CON

TOE は、DB ユーザの接続要求を受け付けた場合、その DB ユーザを識別し、認証を行う。TOE は、各 DB ユーザを一意的に識別･認証できた場合、正当な DB ユーザとして接続を許可する。それ以前に、TOE は、いかなる動作も許可することはない。DB ユーザが接続に成功した場合に限り、TOE は、その DB ユーザを代行して動作するサーバプロセスを割り当てる。DB ユーザとサーバプロセスは、認可識別子によって関連付けられ、さらに認可識別子によってサーバプロセスと各種権限が関連付けられる。

TOE は、DB ユーザを代行して動作するサーバプロセスが、DB ユーザを代行して動作する他のサーバプロセスに干渉することを防ぎ、分離して動作させる。

SF.I&A.HOW

TOE は、次の通りの方法で、DB ユーザを識別･認証する。TOE は、指定された認可識別子が TOE に登録された有効な認可識別子の1つと完全一致することを確認することにより、DB ユーザの識別を行う。また、TOE は、DB ユーザにより指定されたパスワードが TOE に登録され識別された認可識別子のパスワードと完全一致することを確認することにより、DB ユーザの認証を行う。

パスワードは、次の条件を満たすものが設定可能であり、その範囲内でパスワードを変更することが可能である。

- n（パスワード最小文字数）文字以上 30 文字以下
- 半角文字（英大文字、英小文字、数字）で構成

＜注釈＞

パスワード最小文字数は、TOE のガイダンス文書に従い、6 以上 15 以下の値が DBA 権限保持者によって設定される。

SF.I&A.LCK

TOE は、連続認証失敗許容回数を制限する機能、即ち、DB ユーザによる同一の認可識別子を用いた認証の試行が、その制限回数（DBA 権限保持者によって、1 以上 10 以下の範囲で設定可能）を越えて連続して失敗した場合、その認可識別子をロックする機能を提供する。TOE は、ロックされている認可識別子を指定する接続要求を拒否する。TOE は、ロックした認可識別子を、ロック後、一定時間（ロック時間）経過後に自動的にロックを解除する。

＜注釈＞

連続認証失敗許容回数、およびロック時間は、TOE のガイダンス文書に従い、それぞれ 1 回以上 10 回以下、および 10 分以上が DBA 権限保持者によって設定される。

6.1.4. 利用者･権限管理

＜利用者･権限管理の概要＞

以下に示すセキュリティ属性、およびユーザ表の管理を特定の役割に制限する。

- 認可識別子
- パスワード
- DBA 権限
- スキーマ定義権限
- アクセス権限

また、以下に示すセキュリティパラメタの管理を DBA 権限保持者に制限する。

- パスワード最小文字数
- 連続認証失敗許容回数
- ロック時間

利用者･権限管理で取り扱われる情報は、ディクショナリ表で管理される。

SF.PRV.CTL

(1) 認可識別子およびパスワードの管理

TOE は、監査人を除く DB ユーザの登録と削除を DBA 権限保持者にのみ許可する。DB ユーザの登録は、認可識別子とパスワードを対で登録することで行う。DB ユーザの削除は、認可識別子とパスワードを削除することで行う。

TOE は、監査人を除くすべての DB ユーザのパスワードの変更を DBA 権限保持者に許可する。

また、TOE は、DB ユーザのパスワードを変更することをその DB ユーザ本人に許可する。

(2) DBA 権限の管理

TOE は、他の DB ユーザに対する DBA 権限の付与･取消しを DBA 権限保持者にのみ許可する。

(3) スキーマ定義権限の管理

TOE は、他の DB ユーザに対するスキーマ定義権限の付与･取消しを DBA 権限保持者にのみ許可する。

(4) ユーザ表の所有者の認可識別子およびアクセス権限の管理

TOE は、表 6-6 に示すように、ユーザ表を対象とする定義系 SQL の実行制御を実施する。なお、ユーザ表を定義すると同時にそのユーザ表の所有者の認可識別子が決定し、以後変更することはできない。ユーザ表の所有者の認可識別子は、ディクショナリ表で管理される。

表 6-6 ： ユーザ表を対象とする定義系 SQL の実行規則

定義系 SQL を実行する DB ユーザ	ユーザ表	定義系 SQL の種別	
		定義	削除
スキーマ所有者	本人が所有するユーザ表	○	○
DBA 権限保持者	他人が所有するユーザ表	×	○
上記以外	ユーザ表	×	×

○ ： 許可される

× ： 許可されない

＜ 注釈 ： ユーザビュー表の定義 ＞

スキーマ所有者は、本人の所有するユーザ表を基にユーザビュー表を定義して所有することができる。

スキーマ所有者は、他のスキーマ所有者の所有するユーザ表を基にユーザビュー表を定義して所有することもできるが、この場合は基になるユーザ表の SELECT 権限を必要とする。また、基になるユーザ表のアクセス権限が、定義するユーザビュー表の所有者が有するアクセス権限に反映される。

ユーザビュー表を定義する際、所有者の指定により、これを読込み専用ビューとすることができる。また、複数のユーザ表を結合して定義するユーザビュー表など、論理的に行検索以外の結果を基になるユーザ表に反映しかねるユーザビュー表は、TOE が読込み専用ビューとして定義する。読込み専用ビューに対する行検索以外の操作系 SQL は、一切実行することができない。

TOE は、ユーザ表のアクセス権限（SELECT 権限、INSERT 権限、DELETE 権限、UPDATE 権限）の他の DB ユーザに対する付与･取消しを、そのユーザ表を所有するスキーマ所有者にのみ許可する。TOE は、ユーザ表のアクセス権限の付与･取消しを許可する前に、実行者がそのユーザ表を所有するスキーマ所有者であることを確認する。

ユーザ表が定義された時点では、そのアクセス権限は制限的であり、そのユーザ表を所有するスキーマ所有者以外には一切与えられない（この規則を変更する手段は提供されない）。

＜ 注釈 ： ユーザビュー表への伝播 ＞

他人のユーザ表を基にしたユーザビュー表が定義されている場合、以下の規則が適用される。

- 基になるユーザ表の SELECT 権限が取消された場合、ユーザビュー表は自動的に削除される。
- 基になるユーザ表の INSERT 権限、DELETE 権限、UPDATE 権限が取消された場合、ユーザビュー表における所有者の有するアクセス権限も同様に取消される。

(5) パスワード最小文字数、連続認証失敗許容回数、およびロック時間の管理

TOE は、パスワード最小文字数、連続認証失敗許容回数、およびロック時間の設定、変更を DBA 権限保持者に制限する。

＜注釈＞

DBA 権限保持者は、TOE のガイダンス文書に従い、パスワード最小文字数は 6 文字以上に、連続認証失敗許容回数は 10 回以下に、ロック時間は 10 分以上に維持する責任を有する。

(6) ディクショナリ表の管理

TOE は、各 DB ユーザの認可識別子、パスワード、および各 DB ユーザに与えられた各種権限情報（DBA 権限、監査権限、スキーマ定義権限、アクセス権限、監査証跡表の参照権限）を、ディクショナリ表に格納し、維持する。TOE は、これらの情報を内部的に参照し、各 DB ユーザを代行して動作するサーバプロセスに関連付けることによって、アクセス制御、利用者･権限管理を実施する。

TOE は、スキーマ所有者の認可識別子、およびユーザ表の所有者の認可識別子をディクショナリ表に格納し、維持する。

＜注釈＞

監査人は、TOE のガイダンス文書に従って登録される。この際、監査権限は、監査人となる DB ユーザに付与される。TOE は、これ以降、監査権限の付与、取消しを行うことをどの利用者にも許可しない。

6.2. セキュリティ機能強度

確率的または順列的メカニズムに基づくセキュリティ機能は、**SF.I&A.HOW**、および **SF.I&A.LCK** である。これらのセキュリティ機能は、機能強度レベル SOF-基本を持つ。

6.3. 保証手段

本 ST で適用するセキュリティ保証要件とセキュリティの保証手段の対応を表 6-7 に示す。本 ST で適用するセキュリティ保証手段として、以下に示すドキュメントおよび製品を提供する。

表6-7 ： セキュリティ保証要件（EAL4 + ALC_FLR.1）とセキュリティ保証手段の対応表

セキュリティ保証要件	セキュリティ保証手段
ACM_AUT.1 **ACM_CAP.4** **ACM_SCP.2**	HiRDB 構成管理文書
ADO_DEL.2	HiRDB 配付文書
ADO_IGS.1	HiRDB Version 7 システム導入・設計ガイド HiRDB Version 7 システム定義 HiRDB Version 7 システム運用ガイド HiRDB Version 7 コマンドリファレンス HiRDB Version 7 UAP 開発ガイド HiRDB Version 7 SQL リファレンス HiRDB Version 7 メッセージ HiRDB Version 7 セキュリティガイド HiRDB/Single Server Version 7 リリースノート
ADV_FSP.2	HiRDB セキュリティ機能仕様書
ADV_HLD.2	HiRDB セキュリティ上位レベル設計書
ADV_IMP.1	HiRDB ソースコード
ADV_LLD.1	HiRDB セキュリティ下位レベル設計書
ADV_RCR.1	HiRDB セキュリティ機能仕様書 HiRDB セキュリティ上位レベル設計書 HiRDB セキュリティ下位レベル設計書
ADV_SPM.1	HiRDB セキュリティ方針モデル

AGD_ADM.1 **AGD_USR.1**	HiRDB Version 7 解説 HiRDB Version 7 システム導入･設計ガイド HiRDB Version 7 システム定義 HiRDB Version 7 システム運用ガイド HiRDB Version 7 コマンドリファレンス HiRDB Version 7 UAP 開発ガイド HiRDB Version 7 SQL リファレンス HiRDB Version 7 メッセージ HiRDB Version 7 セキュリティガイド HiRDB/Single Server Version 7 リリースノート
ALC_DVS.1	HiRDB 開発セキュリティ規程書
ALC_FLR.1	HiRDB セキュリティ欠陥修正規程書
ALC_LCD.1	HiRDB ライフサイクル定義書
ALC_TAT.1	HiRDB 構成管理文書 HiRDB ライフサイクル定義書
ATE_COV.2 **ATE_DPT.1** **ATE_FUN.1** **ATE_IND.2**	HiRDB セキュリティ機能テスト
AVA_MSU.2	HiRDB 誤使用分析書
AVA_SOF.1	HiRDB セキュリティ機能強度分析書
AVA_VLA.2	HiRDB 脆弱性分析書

7. PP 主張

本章では、PP 参照、PP 修正、PP 追加について記述する。

7.1. PP 参照

参照した PP はない。

7.2. PP 修正

PP への修正はない。

7.3. PP 追加

PP への追加はない。

8. 根拠

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について記述する。

8.1. セキュリティ対策方針根拠

セキュリティ対策方針は、TOE セキュリティ環境で規定した脅威に対抗するためのものであり、前提条件と組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対抗する脅威、実現する前提条件及び組織のセキュリティ方針の対応関係を表 8-1 に示す。

表 8-1 ： セキュリティ対策方針と前提条件、脅威、組織のセキュリティ方針の対応表

TOE セキュリティ環境 / セキュリティ対策方針	A.OS_ACCOUNT	A.REMOTE_OPERATION	A.SERVER_SOFTWARE	A.CLIENT_OF_SERVER	A.SERVER_HARDWARE	A.NETWORK	A.HiRDB_CLIENT	A.UAP	A.ADMINISTRATORS	A.PASSWORD	T.ILLEGAL_CONNECT	T.UNAUTHORIZED_ACCESS	T.UNAUTHORIZED_PERMISSION_MODIFY	P.ACCESS_PRIVILEGE	P.DATABASE_ADMINISTRATOR	P.AUDITOR	P.AUDIT_VIEWER	P.SECURITY_PARAMETER
O.I&A											○							○
O.ACCESS_CONTROL												○						
O.ACCESS_PRIVILEGE													○	○				
O.DATABASE_ADMINISTRATOR													○		○			
O.AUDIT																○	○	
OEN.SERVER_HARDWARE					○													
OEN.HiRDB_SERVER_CONFIG		○																
OEN.SERVER_SOFTWARE			○															
OEN.OS_ACCOUNT	○																	
OEN.CLIENT_OF_SERVER				○														
OEN.NETWORK						○												
OEN.HiRDB_CLIENT							○											

OEN.UAP								○										
OEN. ADMINISTRATORS									○									
OEN.SCHEMA_OWNER														○				
OEN.DATABASE_ADMINISTRATOR															○			
OEN.AUDITOR																○		
OEN.AUDIT_VIEWER																	○	
OEN.PASSWORD										○	○							
OEN.SECURITY_PARAMETER																		○

表 8-1 により、各セキュリティ対策方針は1つ以上の前提条件、脅威、または組織のセキュリティ方針に対応している。

次に、各脅威がセキュリティ対策方針で対抗できること、また前提条件･組織のセキュリティ方針がセキュリティ対策方針で実現できることを説明する。

① 前提条件

A.OS_ACCOUNT（OS のアカウント）：

この前提条件は、**OEN.OS_ACCOUNT** によって実現できる。

OEN.OS_ACCOUNT により、スーパユーザは、許可された管理者以外の者に対して HiRDB サーバの OS のアカウントを与えない。

A.REMOTE_OPERATION（リモート操作の制限）：

この前提条件は、**OEN.HiRDB_SERVER_CONFIG** によって実現できる。

OEN.HiRDB_SERVER_CONFIG により、HiRDB サーバにインストールされた OS へのリモートログインはできない。

A.SERVER_SOFTAWRE（HiRDB サーバにおけるソフトウェア構成）：

この前提条件は、**OEN. SERVER_SOFTWARE** によって実現できる。

OEN. SERVER_SOFTWARE により、HiRDB サーバには、OS、TOE、および SORT 以外のソフトウェアはインストールされない。

A.CLIENT_OF_SERVER（HiRDB サーバにおけるクライアント機能の制限）：

この前提条件は、**OEN.CLIENT_OF_SERVER** によって実現できる。

OEN.CLIENT_OF_SERVER により、HiRDB サーバにおけるクライアント機能は使用されない。

A.SERVER_HARDWARE（サーバにおけるハードウェア等の管理）：

この前提条件は、**OEN.SERVER_HARDWARE** によって実現できる。

OEN.SERVER_HARDWARE により、HiRDB サーバのためのハードウェアと周辺機器は、許可された管理者だけが入場できる場所に設置される。

A.NETWORK（ネットワーク）：

この前提条件は、**OEN.NETWORK** によって実現できる。

OEN.NETWORK により、ネットワークには、HiRDB サーバと HiRDB クライアント以外の機器は接続されない。よって、HiRDB サーバと HiRDB クライアント間の通信の秘匿性と完全性も、確保される。

A.HiRDB_CLIENT（HiRDB クライアント）：

この前提条件は、**OEN.HiRDB_CLIENT** によって実現できる。

OEN.HiRDB_CLIENT により、HiRDB クライアントでは、UAP と HiRDB SQL Executer 以外のネットワークを介して電文を送信できるソフトウェアの使用が禁止される。また、電文の送信先となる HiRDB サーバのポート番号を設定する環境変数には定められた値が設定され、変更がないように維持される。よって、この前提条件は実現される。

A.UAP（UAP の管理）：

この前提条件は、**OEN.UAP** によって実現できる。

OEN.UAP により、UAP は、TOE のガイダンスに従って開発されることにより、TOE で定められているプロトコルに従った電文のみを HiRDB サーバに送信する。また、XA 連携機能は使用されない。よって、この前提条件は実現される。

A. ADMINISTRATORS（許可された管理者）：

この前提条件は、**OEN. ADMINISTRATORS** によって実現できる。

OEN. ADMINISTRATORS により、許可された管理者は、HiRDB サーバおよび HiRDB クライアントに対して、悪意のある操作を行わない。

A.PASSWORD（パスワードの管理）：

この前提条件は、**OEN.PASSWORD** によって実現できる。

OEN.PASSWORD により、TOE を利用するためのパスワードは、DB ユーザ本人によって、他人に知られないように管理される。また、DB ユーザは、TOE のガイダンス文書に従って、適切なパスワードを設定し、適切な頻度でパスワード変更を行う。

② セキュリティ脅威

T.ILLEGAL_CONNECT（不正な接続）：

この脅威は、**O.I&A**、**OEN.PASSWORD** によって対抗される。

O.I&A により、TOE は、利用者が TOE に接続するときに識別･認証を実施することで、DB ユーザであ

ることを確認する。また、TOE は、DB ユーザに対して、本人のパスワードを変更する機能を提供する。さらに、TOE は、DB ユーザのパスワード長を一定文字数以上に維持し、同一の認可識別子による連続した認証の失敗が許容回数を上回った場合に、事前に設定された時間が経つまで、その認可識別子をロックする。このため、DB ユーザ本人以外からの不正な接続、およびその試みは困難となる。

OEN.PASSWORD により、DB ユーザは、自分自身のパスワードを管理し、他人に漏らさない。また、パスワードは適切なものが設定され、適切な頻度で変更される。このため、不正な利用者が他人のパスワードを知ることは困難である。

T.UNAUTHORIZED_ACCESS（権限外のアクセス）：

この脅威は、**O.ACCESS_CONTROL** によって対抗される。

O.ACCESS_CONTROL により、TOE は、DB ユーザに与えられた権限に従って、DB ユーザによる利用者データへのアクセスを制御する。

T.UNAUTHORIZED_PERMISSION_MODIFY（権限外の権限情報とパスワードの改ざん）：

この脅威は、**O.ACCESS_PRIVILEGE**、**O.DATABASE_ADMINISTRATOR** によって対抗される。

O.ACCESS_PRIVILEGE により、ユーザ表のアクセス権限を管理できるのは、そのユーザ表を所有するスキーマ所有者に制限される。

O.DATABASE_ADMINISTRATOR により、監査人以外の識別･認証情報、スキーマ定義権限、および DBA 権限を管理できるのは、DBA 権限保持者に制限される。

よって、適切な権限を持たない利用者が、自身や他人の権限情報とパスワードを改ざんすることはできない。

③ 組織のセキュリティ方針

P.ACCESS_PRIVILEGE（アクセス権限の管理）：

この組織のセキュリティ方針は、**O.ACCESS_PRIVILEGE**、**OEN.SCHEMA_OWNER** によって実現できる。

O.ACCESS_PRIVILEGE により、TOE は、スキーマ所有者に対して、本人が所有するユーザ表のアクセス権限を管理する機能を提供する。

OEN.SCHEMA_OWNER により、スキーマ所有者は、TOE のガイダンス文書に従って、本人が所有するユーザ表のアクセス権限を管理する。

P.DATABASE_ADMINISTRATOR（DBA 権限保持者）：

この組織のセキュリティ方針は、**O.DATABASE_ADMINISTRATOR**、**OEN.DATABASE_ADMINISTRATOR** によって実現できる。

O.DATABASE_ADMINISTRATOR により、TOE は、DBA 権限保持者に対して、監査人以外の識別･認証情報、スキーマ定義権限、および DBA 権限を管理する機能を提供する。

OEN.DATABASE_ADMINISTRATOR により、DBA 権限保持者は、TOE のガイダンス文書に従って、監査人以外の識別･認証情報、DBA 権限、およびスキーマ定義権限を管理する。

P.AUDITOR（監査人）：

この組織のセキュリティ方針は、**O.AUDIT**、**OEN.AUDITOR** によって実現できる。

O.AUDIT により、TOE は、セキュリティ機能に関する操作の中から、表単位および事象種別の単位で監査対象事象を選択させる機能を監査人に対して提供し、監査対象事象が発生した場合、それを監査データとして記録する。監査人は、監査データを検索し出力することができる。

OEN.AUDITOR により、監査人は、ユーザ表に格納されるデータの重要度に応じて監査対象事象を設定し、監査業務を実施する。また、監査証跡参照者を設ける場合には、監査人は信頼できる人物に対して、その役割を委任する。

P.AUDIT_VIEWER（監査証跡参照者）：

この組織のセキュリティ方針は、**O.AUDIT**、**OEN.AUDIT_VIEWER** によって実現できる。

O.AUDIT により、監査証跡参照者は、監査データを検索し出力することができる。

OEN.AUDIT_VIEWER により、監査証跡参照者は、監査人の指示に従って監査データをチェックし、不穏な事象を発見した場合には、これを監査人に報告する。

P.SECURITY_PARAMETER（セキュリティ変数）：

この組織のセキュリティ方針は、**O.I&A**、**OEN.SECURITY_PARAMETER** によって実現できる。

O.I&A により、TOE は、パスワード最小文字数、連続認証失敗許容回数、および認可識別子のロック時間を、事前に DBA 権限保持者によって設定された値に維持する。

OEN.SECURITY_PARAMETER により、DBA 権限保持者は、TOE のガイダンス文書に従って、パスワードの最小文字数、連続認証失敗許容回数、および認可識別子のロック時間をセキュアな値に維持する。

8.2. セキュリティ要件根拠

8.2.1. TOE セキュリティ機能要件根拠

TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 8-2 に示す。

表 8-2 ： TOE セキュリティ機能要件と TOE セキュリティ対策方針の対応関係

TOE セキュリティ対策方針 / TOE セキュリティ機能要件	O.I&A	O.ACCESS_CONTROL	O.ACCESS_PRIVILEGE	O.DATABASE_ADMINISTRATOR	O.AUDIT
FAU_GEN.1					○
FAU_GEN.2					○
FAU_SAR.1					○
FAU_SAR.2					○
FAU_SAR.3					○
FAU_SEL.1					○
FAU_STG.1					○
FAU_STG.4					○
FDP_ACC.1		○			
FDP_ACF.1		○			
FIA_AFL.1	○				
FIA_ATD.1	○	○	○	○	○
FIA_SOS.1	○				
FIA_UAU.2	○				
FIA_UID.2	○				
FIA_USB.1		○	○	○	○
FMT_MSA.1		○	○	○	
FMT_MSA.3		○			
FMT_MTD.1	○			○	○

FMT_SMF.1	○		○	○	○
FMT_SMR.1			○	○	○
FPT_RVM.1	○	○			○
FPT_SEP.1	○	○	○	○	○
FPT_STM.1					○

表 8-2 より、各 TOE セキュリティ機能要件が1つ以上の TOE セキュリティ対策方針に対応している。
次に、各 TOE セキュリティ対策方針が、TOE セキュリティ機能要件で実現できることを説明する。

O.I&A（TOE における識別･認証）：

このセキュリティ対策方針は、**FIA_AFL.1**、**FIA_ATD.1**、**FIA_SOS.1**、**FIA_UAU.2**、**FIA_UID.2**、**FMT_MTD.1**、**FMT_SMF.1**、**FPT_RVM.1**、**FPT_SEP.1** によって実現できる。

FIA_AFL.1 により、TOE は、一定回数の連続する認証の失敗を検出し、その認可識別子を一定時間使用できない状態にする。

FIA_ATD.1 により、TOE は、DB ユーザの識別に必要なセキュリティ属性（認可識別子）を維持する。

FIA_SOS.1 により、TOE は、秘密（パスワード）の品質尺度を維持する。

FIA_UAU.2 と **FIA_UID.2** により、TOE は、識別と認証が成功する前に接続を許可することはない。

FMT_MTD.1 により、TOE は、DB ユーザに対して本人のパスワードを変更する機能を提供し、連続認証失敗許容回数、パスワード最小文字数、およびロック時間の変更を、DBA 権限保持者に制限する。

FMT_SMF.1 により、TOE は認証データ（パスワード）の管理、および TSF データ（連続認証失敗許容回数、パスワード最小文字数）の管理を行う能力を持つ。

FPT_RVM.1 により、TOE は、利用者が TOE に接続する前に、識別･認証を実施する機能が呼び出され成功することを保証する。

FPT_SEP.1 により、TOE は、TSF 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 TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。

O.ACCESS_CONTROL（アクセス制御）：

このセキュリティ対策方針は、**FDP_ACC.1**、**FDP_ACF.1**、**FIA_ATD.1**、**FIA_USB.1**、**FMT_MSA.1**、**FMT_MSA.3**、**FPT_RVM.1**、**FPT_SEP.1** によって実現できる。

FDP_ACC.1 と **FDP_ACF.1** により、TOE は、DB ユーザのサーバプロセスとユーザ表間の操作に対して、DB ユーザに与えられたアクセス権限、または DBA 権限に基づいてアクセス制御を実施する。

FIA_ATD.1 と **FIA_USB.1** により、TOE は、DB ユーザに属するセキュリティ属性（認可識別子、アクセス権限、DBA 権限）とその DB ユーザを代行して動作するサブジェクトを関連付ける。

FMT_MSA.1 により、TOE は、ユーザ表のアクセス権限の付与と取消しを、ユーザ表の所有者に制限し、他人の DBA 権限の付与と取り消しを DBA 権限保持者に制限する。

FMT_MSA.3 により、TOE は、アクセス制御で使用するセキュリティ属性のデフォルト値を制限的とする。

FPT_RVM.1 により、TOE は、利用者データのアクセスが許可される前に、アクセス制御を実施する機能が呼び出され成功することを保証する。

FPT_SEP.1 により、TOE は、TSF 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 TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。

O.ACCESS_PRIVILEGE（アクセス権限の管理）：

このセキュリティ対策方針は、**FIA_ATD.1**、**FIA_USB.1**、**FMT_MSA.1**、**FMT_SMF.1**、**FMT_SMR.1**、**FPT_SEP.1** によって実現できる。

FIA_ATD.1 と **FIA_USB.1** により、TOE は、DB ユーザに属するセキュリティ属性（認可識別子、スキーマ定義権限）とその DB ユーザを代行して動作するサブジェクトを関連付ける。

FMT_MSA.1 により、TOE は、ユーザ表のアクセス権限の付与と取消しを、そのユーザ表を所有するスキーマ所有者に制限する。

FMT_SMF.1 により、TOE はセキュリティ管理（アクセス権限管理）機能を行う能力を持つ。

FMT_SMR.1 により、TOE は、スキーマ所有者の役割を維持し、利用者と関連付ける。

FPT_SEP.1 により、TOE は、TSF 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 TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。

O.DATABASE_ADMINISTRATOR（DBA 権限保持者）：

このセキュリティ対策方針は、**FIA_ATD.1**、**FIA_USB.1**、**FMT_MSA.1**、**FMT_MTD.1**、**FMT_SMF.1**、**FMT_SMR.1**、**FPT_SEP.1** によって実現できる。

FIA_ATD.1 と **FIA_USB.1** により、TOE は、DB ユーザに属するセキュリティ属性（DBA 権限）とその DB ユーザを代行して動作するサブジェクトを関連付ける。

FMT_MSA.1 により、TOE は、監査人以外の識別情報（認可識別子）、および他人の DBA 権限の管理を、DBA 権限保持者に制限する。

FMT_MTD.1 により、TOE は、監査人以外の認証情報（パスワード）、およびスキーマ定義権限の管理を、DBA 権限保持者に制限する。

FMT_SMF.1 により、TOE は、セキュリティ管理（識別･認証情報、スキーマ定義権限、DBA 権限の管理）機能を行う能力を持つ。

FMT_SMR.1 により、TOE は、DBA 権限保持者の役割を維持し、利用者と関連付ける。

FPT_SEP.1 により、TOE は、TSF 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 TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。

O.AUDIT（監査）：

このセキュリティ対策方針は、**FAU_GEN.1**、**FAU_GEN.2**、**FAU_SAR.1**、**FAU_SAR.2**、**FAU_SAR.3**、**FAU_SEL.1**、**FAU_STG.1**、**FAU_STG.4**、**FIA_ATD.1**、**FIA_USB.1**、**FMT_MTD.1**、**FMT_SMF.1**、**FMT_SMR.1**、**FPT_RVM.1**、**FPT_SEP.1**、**FPT_STM.1** によって実現できる。

FAU_GEN.1 により、TOE は、監査対象事象の監査データを生成する。表 5-1 に示すように、監査対象事象にはセキュリティ機能に関する操作がすべて含まれている。

FAU_GEN.2 により、TOE 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る。

FAU_SAR.1 により、TOE は、監査人、および監査証跡参照者が、監査データを読み出せるようにする。

FAU_SAR.2 により、TOE 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データの読み出しアクセスを禁止する。

FAU_SAR.3 により、TOE は、監査データを検索、並べ替えする機能を提供する。

FAU_SEL.1 により、TOE は、表単位および事象種別の単位で監査対象事象を選択する機能を提供する。

FAU_STG.1 により、TOE は、監査データを不正な削除から保護し、監査データの改変を防止する。

FAU_STG.4 により、TOE は、監査証跡が満杯になった場合、最も古くに格納された監査データへの上書きを行い、上書き開始を通知するメッセージを出力する。

FIA_ATD.1 と **FIA_USB.1** により、TOE は、DB ユーザに属するセキュリティ属性（監査権限、監査証跡表の参照権限）とその DB ユーザを代行して動作するサブジェクトを関連付ける。

FMT_MTD.1 により、TOE は、監査証跡表の参照権限、監査対象事象、および監査データの管理を、監査人に制限する。

FMT_SMF.1 により、TOE は、セキュリティ管理（監査証跡表の参照権限、監査対象事象、監査データの管理）機能を行う能力を持つ。

FMT_SMR.1 により、TOE は、監査人、および監査証跡参照者の役割を維持し、利用者と関連付ける。

FPT_RVM.1 により、TOE は、監査対象事象が発生した場合に、監査データを生成する機能が呼び出され成功することを保証する。

FPT_SEP.1 により、TOE は、TSF 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 TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。

FPT_STM.1 により、監査データの記録に必要な高信頼タイムスタンプが提供される。

8.2.2. 最小機能強度レベル根拠

「3.3.1 脅威エージェント」で述べたように、脅威エージェントの攻撃能力は低く、セキュリティ侵害の試みは一

時的なものであると想定される。したがって、最小機能強度レベルは SOF-基本が妥当である。

8.2.3. セキュリティ機能要件依存性

セキュリティ機能要件のコンポーネントの依存性を表 8-3 に示す。

表 8-3 ： セキュリティ機能要件のコンポーネントの依存性

セキュリティ機能要件（A） ＼ 依存されるコンポーネント（B）	FAU_GEN.1	FAU_SAR.1	FAU_STG.1	FDP_ACC.1	FDP_ACF.1	FIA_UAU.2	FIA_UID.2	FIA_ATD.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1
FAU_GEN.1														○
FAU_GEN.2	○						◎							
FAU_SAR.1	○													
FAU_SAR.2		○												
FAU_SAR.3		○												
FAU_SEL.1	○										○			
FAU_STG.1	○													
FAU_STG.4			○											
FDP_ACC.1					○									
FDP_ACF.1				○						○				
FIA_AFL.1						◎								
FIA_ATD.1														
FIA_SOS.1														
FIA_UAU.2							◎							
FIA_UID.2														
FIA_USB.1								○						
FMT_MSA.1				△								○	○	
FMT_MSA.3									○				○	
FMT_MTD.1												○	○	
FMT_SMF.1														
FMT_SMR.1							◎							
FPT_RVM.1														
FPT_SEP.1														

FPT_STM.1													

○ ： (A) が、CC パート 2 で規定されている依存コンポーネント (B) に依存する関係

◎ ： (A) が、CC パート 2 で規定されている依存コンポーネントの上位階層 (B) に依存する関係

△ ： (A) が、CC パート 2 で規定されている選択可能な依存コンポーネント (B) に依存する関係

表 8-3 より、TOE セキュリティ機能要件は、必要な依存関係をすべて満たしている。

8.2.4. セキュリティ機能要件相互補完性

前節の依存関係以外で、相互補完する機能要件について記述する。

＜バイパス防止＞

FPT_RVM.1 により、TSC 内の各機能の動作進行が許可される前に、識別･認証機能 (**FIA_UAU.2**、**FIA_UID.2**)、アクセス制御機能 (**FDP_ACC.1**、**FDP_ACF.1**) が呼び出され成功することが保証される。また、監査対象事象が発生した場合には、監査機能 (**FAU_GEN.1**) が呼び出され成功することが保証される。

＜改ざん防止＞

FPT_SEP.1 により、TSF は、信頼できないサブジェクトによる干渉と改ざんから保護される。したがって、これによりすべての TOE セキュリティ機能要件が支援される。

8.2.5. セキュリティ機能要件内部一貫性

各セキュリティ機能要件が内部的に一貫しており、矛盾しない根拠を記述する。

＜監査関連＞

セキュリティ監査 (FAU) に含まれる 8 つの機能要件は監査機能に閉じたものであり、依存性に関わる **FIA_UID.2**、**FMT_MTD.1**、**FPT_STM.1**、TSP の非バイパス性に関する **FPT_RVM.1**、および TSF ドメイン分離に関する **FPT_SEP.1** 以外の機能要件とは関連しない。

FIA_UID.2 (アクション前の利用者識別) は、**FAU_GEN.2** (利用者識別情報の関連付け) を補完するものであり、矛盾はない。

FMT_MTD.1 (TSF データの管理) には監査データの管理機能が含まれており、監査対象事象の登録･除外、監査データの削除を監査人が行うとの要件がある。これは、**FAU_SEL.1** (選択的監査)、**FAU_STG.1** (保護された監査証跡格納) を補完するものであり、矛盾はない。

FPT_STM.1 (高信頼タイムスタンプ) は、**FAU_GEN.1** (監査データ生成) を補完するものであり、矛盾はない。なお、**FAU_SEL.1** (選択的監査) は監査対象事象の取捨選択を許すため、**FAU_GEN.1** (監査データ生成) の要件に含まれる監査対象事象のすべては記録されないかもしれない。しかし、監査対象事象の設定権限を持つ監査人が運用環境に応じて必要な監査対象事象を設定することにより、監査記録の不備を原因とする脆弱性が生じることは防止される。

FPT_RVM.1 (TSP の非バイパス性) は、監査データの生成がバイパスされないための機能要件であり、矛盾はない。

FPT_SEP.1 (TSF ドメイン分離) は、セキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜アクセス制御関連＞

FDP_ACC.1、**FDP_ACF.1**、**FMT_MSA.1**、**FMT_MSA.3** はアクセス制御に関連する機能要件であり、**FMT_SMR.1**、**FPT_RVM.1**、**FPT_SEP.1** 以外の機能要件とは関連しない。

FDP_ACC.1（サブセットアクセス制御）と **FDP_ACF.1**（セキュリティ属性によるアクセス制御）では、サブジェクト、オブジェクト、SFP の名称を使用しているが、これらに矛盾はない。

FMT_MSA.1（セキュリティ属性の管理）で記述される役割はすべて **FMT_SMR.1**（セキュリティ役割）で定義されており、矛盾はない。

FPT_RVM.1（TSP の非バイパス性）は、アクセス制御がバイパスされないための機能要件であり、矛盾はない。

FPT_SEP.1（TSF ドメイン分離）は、セキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜識別･認証関連＞

識別と認証（FIA）に含まれる 6 つの機能要件は識別･認証に関わるものであり、**FAU_GEN.2**、**FMT_SMR.1**、**FPT_RVM.1**、**FPT_SEP.1** 以外の機能要件とは関連しない。

識別と認証（FIA）に含まれる 6 つの機能要件には、記述内容が重複する部分がない。したがって、これらの間に競合や矛盾はない。

FAU_GEN.2（利用者識別情報の関連付け）との関連については、＜監査関連＞で述べたように競合や矛盾はない。

FMT_SMR.1（セキュリティ役割）は利用者の役割を定義したものであり、これと重複する内容は識別と認証（FIA）に含まれる 6 つの機能要件には含まれていないため、競合や矛盾はない。

FPT_RVM.1（TSP の非バイパス性）は、識別･認証がバイパスされないための機能要件であり、矛盾はない。

FPT_SEP.1（TSF ドメイン分離）は、セキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜セキュリティ管理関連＞

セキュリティ管理（FMT）に含まれる 5 つの機能要件はセキュリティ管理に関わるものであり、このグループと他の機能要件との関係においては、**FPT_RVM.1**、**FPT_SEP.1** を除き、既に説明したように競合や矛盾はない。

FMT_MSA.1（セキュリティ属性の管理）、**FMT_MSA.3**（静的属性初期化）、**FMT_MTD.1**（TSF データの管理）では、セキュリティ属性および TSF データの管理を重複せずに規定しており、競合や矛盾はない。

FMT_SMF.1（管理機能の特定）はセキュリティ管理機能を特定するものであり、他の機能要件との競合や矛盾はない。

FMT_SMR.1（セキュリティ役割）は利用者の役割を定義したものであり、他の機能要件との競合や矛盾はない。

FPT_RVM.1（TSP の非バイパス性）は、アクセス制御、および識別･認証がバイパスされないための機能要件であり、矛盾はない。

FPT_SEP.1（TSF ドメイン分離）は、セキュリティドメインが干渉されないための機能要件であり、矛盾はない。

＜TSF 保護関連＞

TSF の保護（FPT）に含まれる 3 つの機能要件は TSF の保護に関わるものであり、このグループと他の機能要件との関係においては、既に説明したように競合や矛盾はない。

FPT_RVM.1（TSP の非バイパス性）、**FPT_SEP.1**（TSF ドメイン分離）は、**FPT_STM.1**（高信頼タイムスタンプ）は、これらの関係において、その内容から競合や矛盾は生じない。

8.2.6. セキュリティ管理機能根拠

表 5-7 より、各機能要件の管理機能と考えるアクションは、（後述）の例外を除き、本 TOE の管理機能によって満たされている。

次に、（後述）の例外について、その根拠を説明する。

＜**FAU_SEL.1**＞

TOE は、運用開始以降、監査権限の付与･取消しを行う機能を提供しない。

＜**FAU_STG.4**＞

TOE は、運用開始以降、監査格納失敗時にとられるアクション（上書き、メッセージ出力）を変更する機能を提供しない。

＜**FDP_ACF.1**＞

明示的なアクセスまたは拒否に基づく決定に使われる属性はない。

＜**FIA_AFL.1**＞

TOE は、認証失敗の事象においてとられるアクション（認可識別子のロック）を変更する機能を持たない。

＜**FIA_ATD.1**＞

利用者に対する追加のセキュリティ属性はない。

＜**FIA_USB.1**＞

デフォルトのサブジェクトのセキュリティ属性はない。

＜**FMT_MSA.3**＞

初期値を特定できる役割は存在しない。

TOE は、アクセス権限のデフォルト値の設定（制限的）を変更する機能を持たない。

＜**FMT_MTD.1**＞

TOE は、運用開始以降、監査権限の付与･取消しを行う機能を提供しない。

＜**FPT_STM.1**＞

TOE は、時間を変更しない。

8.2.7. セキュリティ保証要件根拠

TOE は、商用のデータベース製品であり、利用環境によってはセキュリティ上の高い信頼性が求められる。ただし、「3.3.1 脅威エージェント」で述べたように、脅威エージェントの攻撃能力は低く、セキュリティ侵害の試

みは一時的なものであると想定される。したがって、TOE の評価保証レベルは EAL4 を適用する。

また、本 ST では、EAL4 の保証要件の基本コンポーネントに加え、欠陥修正の手続きを重視することにより、ALC_FLR.1 コンポーネントを適用する。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係を表 8-4 に示す。

表 8-4 ： TOE セキュリティ機能と TOE セキュリティ機能要件の対応関係

TOE セキュリティ機能要件 / TOE セキュリティ機能	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_SAR.3	FAU_SEL.1	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FIA_AFL.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.2	FIA_UID.2	FIA_USB.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1
SF.AUD.GEN	○	○				○													○	○		○	○	○
SF.AUD.TBL			○	○	○		○					○							○	○			○	
SF.AUD.FIL								○															○	
SF.ACC.TBL									○	○												○	○	
SF.I&A.CON														○	○	○						○	○	
SF.I&A.HOW													○										○	
SF.I&A.LCK											○												○	
SF.PRV.CTL												○					○	○	○	○	○		○	

表 8-4 により、各 TOE セキュリティ機能が1つ以上の TOE セキュリティ機能要件に対応している。
次に、各 TOE セキュリティ機能要件が、TOE セキュリティ機能で実現できることを説明する。

FAU_GEN.1　監査データ生成

SF.AUD.GEN が要件を満たす。

＜根拠＞

SF.AUD.GEN により、TOE は、**FAU_GEN.1.1** で記述されるすべての監査対象事象の監査記録を生成することができる。

SF.AUD.GEN により、TOE は、**FAU_GEN.1.2** で記述されるすべての情報を記録する。

FAU_GEN.2　利用者識別情報の関連付け

SF.AUD.GEN が要件を満たす。

＜根拠＞

SF.AUD.GEN により、TOE は、生成する監査データにはその原因となった DB ユーザの認可識別子を含める。

FAU_SAR.1 監査レビュー

SF.AUD.TBL が要件を満たす。

＜根拠＞

SF.AUD.TBL により、監査人、および監査証跡参照者は、監査証跡表の監査データを検索することができる。

FAU_SAR.2 限定監査レビュー

SF.AUD.TBL が要件を満たす。

＜根拠＞

SF.AUD.TBL により、監査証跡表の監査データの検索は、監査人および監査証跡参照者にのみ許可され、その他の利用者が監査データに読み出しアクセスを行うことは禁止される。

FAU_SAR.3 選択可能監査レビュー

SF.AUD.TBL が要件を満たす。

＜根拠＞

SF.AUD.TBL により、TOE は、監査証跡表を行検索する機能を提供する。TOE は、行検索の機能により、任意の監査情報の大小関係や同値関係に基づいて、監査データを検索、並べ替えする能力を提供する。

FAU_SEL.1 選択的監査

SF.AUD.GEN が要件を満たす。

＜根拠＞

SF.AUD.GEN により、TOE は、事象種別、オブジェクト識別情報、および事象の結果（成功または失敗）に基づいて、監査対象事象を選択する機能を提供する。

FAU_STG.1 保護された監査証跡格納

SF.AUD.TBL が要件を満たす。

＜根拠＞

SF.AUD.TBL により、TOE は、監査証跡表の監査データの削除は監査人に制限し、監査データの改変はどの DB ユーザにも許可しない。

FAU_STG.4 監査データ損失の防止

SF.AUD.FIL が要件を満たす。

＜根拠＞

SF.AUD.FIL により、TOE は、監査証跡が満杯になった場合、最も古い監査記録が格納されている監査証跡ファイルを監査データの出力先（現用）とし、上書き開始を通知するメッセージを出力する。

FDP_ACC.1 サブセットアクセス制御

FDP_ACF.1 セキュリティ属性によるアクセス制御

SF.ACC.TBL が要件を満たす。

＜根拠＞

SF.ACC.TBL により、TOE は、**FDP_ACC.1.1** で記述される操作において、**FDP_ACF.1.1** で記述されるセキュリティ属性に基づき、**FDP_ACF.1.2** で記述されるアクセス制御の規則を実施する。

表 6-3、表 6-4、表 6-5、および＜ユーザ実表の削除の規則＞に示すアクセス規則は、**FDP_ACF.1.2** で記述される規則を満たす。

FIA_AFL.1 認証失敗時の取り扱い

SF.I&A.LCK が要件を満たす。

＜根拠＞

SF.I&A.LCK により、TOE は、管理者設定可能な連続認証失敗許容回数の同一認可識別子を指定する連続不成功認証試行を検出し、不成功な認証試行がそれを上回った場合、その認可識別子を一定時間ロックする機能を提供する。

FIA_ATD.1 利用者属性定義

SF.PRV.CTL、**SF.AUD.TBL** が要件を満たす。

＜根拠＞

SF.PRV.CTL、**SF.AUD.TBL** により、TOE は、各 DB ユーザに属する認可識別子、DBA 権限、スキーマ定義権限、アクセス権限、監査権限、および監査証跡表の参照権限を維持する機能を提供する。

FIA_SOS.1 秘密の検証

SF.I&A.HOW が要件を満たす。

＜根拠＞

SF.I&A.HOW により、TOE は、パスワードが管理者によって事前に設定された 6～15 内のパスワード最小文字数以上 30 文字以下の半角文字（英大文字、英小文字、数字）で構成されることを保証する。

FIA_UAU.2 アクション前の利用者認証

FIA_UID.2 アクション前の利用者識別

SF.I&A.CON が要件を満たす。

＜根拠＞

SF.I&A.CON により、TOE は、DB ユーザが識別･認証に成功して TOE に接続しない限り、その DB ユーザによる TOE の利用を許可することはない。

FIA_USB.1 利用者･サブジェクト結合

SF.I&A.CON が要件を満たす。

＜根拠＞

SF.I&A.CON により、TOE は、DB ユーザに付与された各種権限を、その DB ユーザを代行して動作するサーバプロセスに関連付ける。

FMT_MSA.1 セキュリティ属性の管理

SF.PRV.CTL が要件を満たす。

＜根拠＞

SF.PRV.CTL により、TOE は、認可識別子、アクセス権限、および DBA 権限の管理を適切な役割に制限する。

FMT_MSA.3 静的属性初期化

SF.PRV.CTL が要件を満たす。

＜根拠＞

SF.PRV.CTL により、TOE は、ユーザ表が定義された時点で、そのユーザ表のアクセス権限をそのユーザ表の所有者以外には一切与えない。また、ユーザ表を定義すると同時にそのユーザ表の所有者の認可識別子が決定し、以後変更することはできない。TOE は、これらの規則を変更する手段を提供しない。

FMT_MTD.1 TSF データの管理

SF.AUD.GEN、**SF.AUD.TBL**、**SF.PRV.CTL** が要件を満たす。

＜根拠＞

SF.AUD.GEN により、TOE は、監査対象事象の登録と除外を、監査人に制限する。

SF.AUD.TBL により、TOE は、監査証跡表の参照権限の管理、および監査データの削除を、監査人に制限する。

SF.PRV.CTL により、TOE は、監査人以外のパスワードの登録、削除、改変を DBA 権限保持者に許可し、DB ユーザには本人のパスワードの変更を許可する。また、スキーマ定義権限、パスワード最小文字数、連続認証失敗許容回数、およびロック時間の変更を DBA 権限保持者に制限する。

FMT_SMF.1 管理機能の特定

SF.AUD.GEN、**SF.AUD.TBL**、**SF.PRV.CTL** が要件を満たす。

＜根拠＞

SF.PRV.CTL により、TOE はセキュリティ属性の管理機能（**FMT_MSA.1**）を行う能力を持つ。

SF.AUD.GEN、**SF.AUD.TBL**、**SF.PRV.CTL** により、TOE は、TSF データの管理機能（**FMT_MTD.1**）を行う能力を持つ。

FMT_SMR.1 セキュリティ役割

SF.PRV.CTL が要件を満たす。

＜根拠＞

SF.PRV.CTL により、TOE は、各役割を維持するために必要な各種権限やユーザ表の所有者の認可識別子をディクショナリ表で管理し、DB ユーザと関連付ける。

FPT_RVM.1 TSP の非バイパス性

SF.AUD.GEN、**SF.I&A.CON**、**SF.ACC.TBL** が要件を満たす。

＜根拠＞

SF.AUD.GEN により、TOE は、監査対象事象の監査データを確実に採取（生成）する。

SF.I&A.CON により、TOE は、識別･認証に成功しない利用者に TOE への接続を許可することはない。

SF.ACC.TBL により、TOE は、アクセス制御をバイパスする手段を提供しない。

FPT_SEP.1 TSF ドメイン分離

SF.AUD.GEN 、 **SF.AUD.TBL** 、 **SF.AUD.FIL** 、 **SF.ACC.TBL** 、 **SF.I&A.CON** 、 **SF.I&A.HOW** 、 **SF.I&A.LCK**、**SF.PRV.CTL** が要件を満たす。

＜根拠＞

上記すべてのセキュリティ機能により、TOE は、セキュリティに関わるドメインと他のドメインを分離させる。

FPT_STM.1 高信頼タイムスタンプ

SF.AUD.GEN が要件を満たす。

＜根拠＞

SF.AUD.GEN により、TOE は、監査データを記録するのに必要なタイムスタンプを生成する機能を持つ。これにより、高信頼タイムスタンプを提供する。

8.3.2. セキュリティ機能強度根拠

この TOE において、確率的または順列的メカニズムに基づくセキュリティ機能は、**SF.I&A.HOW**、および **SF.I&A.LCK** である。これらのセキュリティ機能強度は、6.2 節において、SOF-基本を指定している。一方、5.1.2 項において、TOE の最小機能強度（TOE セキュリティ機能要件に対する機能強度）は、SOF-基本であることを述べており、両者は一致している。

8.3.3. 保証手段根拠

本節では、セキュリティ保証手段がセキュリティ保証要件に対して必要かつ十分であることを記述する。セキュリティ保証要件とセキュリティ保証手段の対応関係を表 6-7 に示す。

「表 6-7 ： セキュリティ保証要件（EAL4 + ALC_FLR.1）とセキュリティ保証手段の対応表」より、全てのセキュリティ保証手段が、何らかのセキュリティ保証要件のために必要であることが示される。

したがって、本 ST で適用するセキュリティ保証手段によって、セキュリティ保証要件を満たすことができる。

8.4. PP 主張根拠

参照した PP はない。