HiRDB

セキュリティターゲット

2012/03/19

Version 5.22

株式会社 日立製作所

「HiRDB 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	2011/05/25	Ver 5.00	新規作成
2	2011/05/31	Ver 5.01	U.S.政府 PP の記述の引用ほか内部レビュー結果反映
3	2011/06/14	Ver 5.02	CC 記述の英語化ほか内部レビュー結果反映
4	2011/06/21	Ver 5.03	内部レビュー結果反映
5	2011/06/27	Ver 5.04	内部レビュー結果反映
6	2011/07/08	Ver 5.05	内部レビュー結果反映
7	2011/08/28	Ver 5.06	評価機関からの指摘反映
8	2011/09/11	Ver 5.07	評価機関からの指摘反映
9	2011/10/07	Ver 5.08	評価機関からの指摘反映
10	2011/10/19	Ver 5.09	評価機関からの指摘反映
11	2011/10/31	Ver 5.10	評価機関からの指摘反映
12	2011/11/03	Ver 5.11	評価機関からの指摘反映
13	2011/11/08	Ver 5.12	評価機関からの指摘反映
14	2011/11/14	Ver 5.13	評価機関からの指摘反映
15	2012/01/09	Ver 5.14	評価機関からの指摘反映
16	2012/01/17	Ver 5.15	評価機関からの指摘反映
17	2012/02/03	Ver 5.16	評価機関からの指摘反映
18	2012/02/16	Ver 5.17	評価機関からの指摘反映
19	2012/02/29	Ver 5.18	評価機関からの指摘反映
20	2012/03/05	Ver 5.19	評価機関からの指摘反映
21	2012/03/06	Ver 5.20	評価機関からの指摘反映
22	2012/03/07	Ver 5.21	評価機関からの指摘反映
23	2012/03/19	Ver 5.22	評価機関からの指摘反映
24			

■ 商標類

・ AIX は，米国およびその他の国における International Business Machines Corporation の商標です。

・ Red Hat は，米国およびその他の国で Red Hat, Inc.の登録商標若しくは商標です。

・ Solaris は，Oracle Corporation およびその子会社，関連会社の米国 およびその他の国における登録商標または商標です。

・ 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 ST は, HiRDB Server Version 9 (Linux 版)に対するセキュリティ要件を記述する。
本 ST は,「2.2 PP 主張, パッケージ主張」に記述しているとおり, プロテクションプロファイル(PP)への適合は主張していない。一方で, DBMS 向けのプロテクションプロファイルとしては,「U.S. Government Protection Profile Database Management Systems, Version 1.3(以降, U.S.GPP)」が認証されており, 現在の商用 DBMS 製品に対する共通的なセキュリティ要件が規定されている。
本 ST においては当該 U.S.GPP を参照し, 記述のレベルを可能な限り合わせることとした。

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

1.1. ST参照

ST 名称	:	HiRDB セキュリティターゲット
ST バージョン	:	5.22
識別名	:	HiRDB-ST-5.22
発行日	:	2012 年 3 月 19 日
作成者	:	株式会社 日立製作所

1.2. TOE参照

TOE 名称	:	HiRDB Server Version 9 (Linux 版)
TOE バージョン	:	09
TOE リビジョン	:	01
開発者	:	株式会社 日立製作所

1.3. TOE概要

1.3.1. TOEの使用法及び主要なセキュリティ機能の特徴

評価対象である HiRDB Server Version 9 (Linux 版)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, クライアントーサーバ(C/S)形態で使用される。HiRDB Server Version 9 (Linux 版)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。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

1.3.1.1. 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。

1.3.1.2. 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。

1.3.1.3. 識別・認証

DB ユーザが SQL インタフェースを使用し，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。

1.3.1.4. 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。

1.3.2. TOE種別

この ST で記述される TOE 種別は，データベース管理システム(DBMS)である。

1.3.3. TOEに必要なTOE以外のハードウェア/ソフトウェア

TOE はクライアントーサーバ(C/S)形態で使用される。HiRDB サーバを構成する各マシンと HiRDB クライアントを構成する各マシンは，IPv4 を用いた LAN で接続される。

1.3.3.1. HiRDBサーバを構成するTOE以外のハードウェア/ソフトウェア

(1) 評価構成における適用OS

- Red Hat Enterprise Linux 5.6

(2) 適用機種

下記シリーズ中で適用 OS が稼動する機種

- BladeSymphony
- HA8000 シリーズ
- 上記以外の PC/AT 互換機

1.3.3.2. HiRDBクライアントを構成するTOE以外のハードウェア/ソフトウェア

(1) 評価構成における適用OS

- Windows XP Professional

(2) 適用機種

下記シリーズ中で適用 OS が稼動する機種

- BladeSymphony
- HA8000 シリーズ
- 上記以外の PC/AT 互換機

(3) その他のソフトウェア

- HiRDB / Run Time Version 9 09-01
- HiRDB / Developer's Kit Version 9 09-01

1.4. TOE記述

1.4.1. 製品概要

1.4.1.1. 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。

TOE は HiRDB Server Version 9 (Linux 版)であり，構成として，HiRDB / Single Server と HiRDB / Parallel Server がある。業務要件に応じて，インストール時にいずれかの構成を選択する。

- HiRDB / Single Server は，小規模から大規模まで幅広いデータベースに対応する，オンライン業務のレスポンスを重視したデータベースサーバである。1 台のマシンでデータベースサーバを構成する。
- HiRDB / Parallel Server は，中規模から大規模のデータベースに対応する，大量アクセス・大量データ処理を重視した，エンタープライズモデルのデータベースサーバである。特に負荷分散が必要な場合に使用する。

1.4.1.2. 製品の用途

HiRDB Server Version 9 (Linux 版)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。

1.4.1.3. 評価構成

HiRDB / Single Server, HiRDB / Parallel Server, それぞれをインストールしたクライアントーサーバ(C/S)型のシステム構成を図 1.4-1，図 1.4-2 に示す。いずれのシステム構成でも，組織内の特定の従業員が HiRDB クライアントで HiRDB SQL Executer Version 9 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。

図 1.4-1 のネットワークは，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。

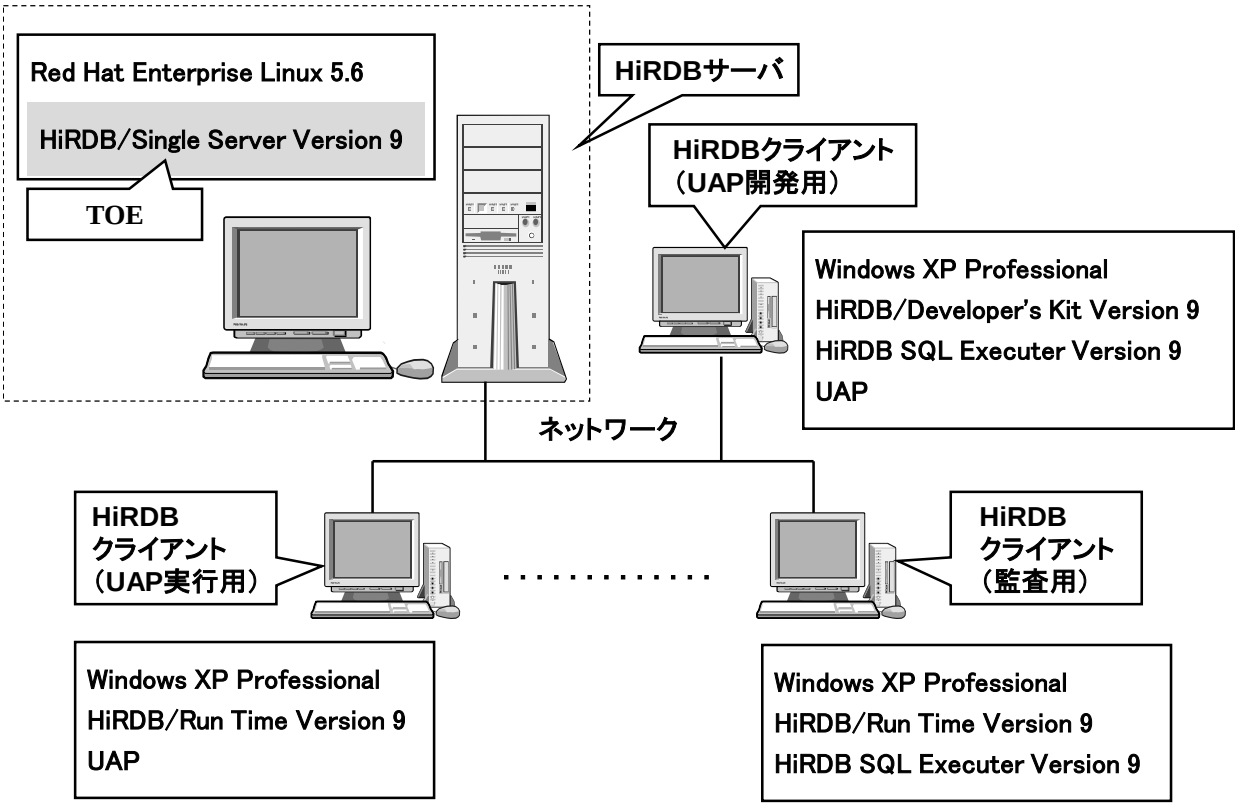

図 1.4-1 ： クライアントーサーバ（C/S）型のシステム構成(HiRDB / Single Server)

図 1.4-2 のネットワーク 1 は HiRDB / Parallel Server を構成する各マシン間を，ネットワーク 2 は HiRDB / Parallel Server と HiRDB クライアントを接続するためのものであり，各ネットワークには他のコンピュータは接続されないものとする。

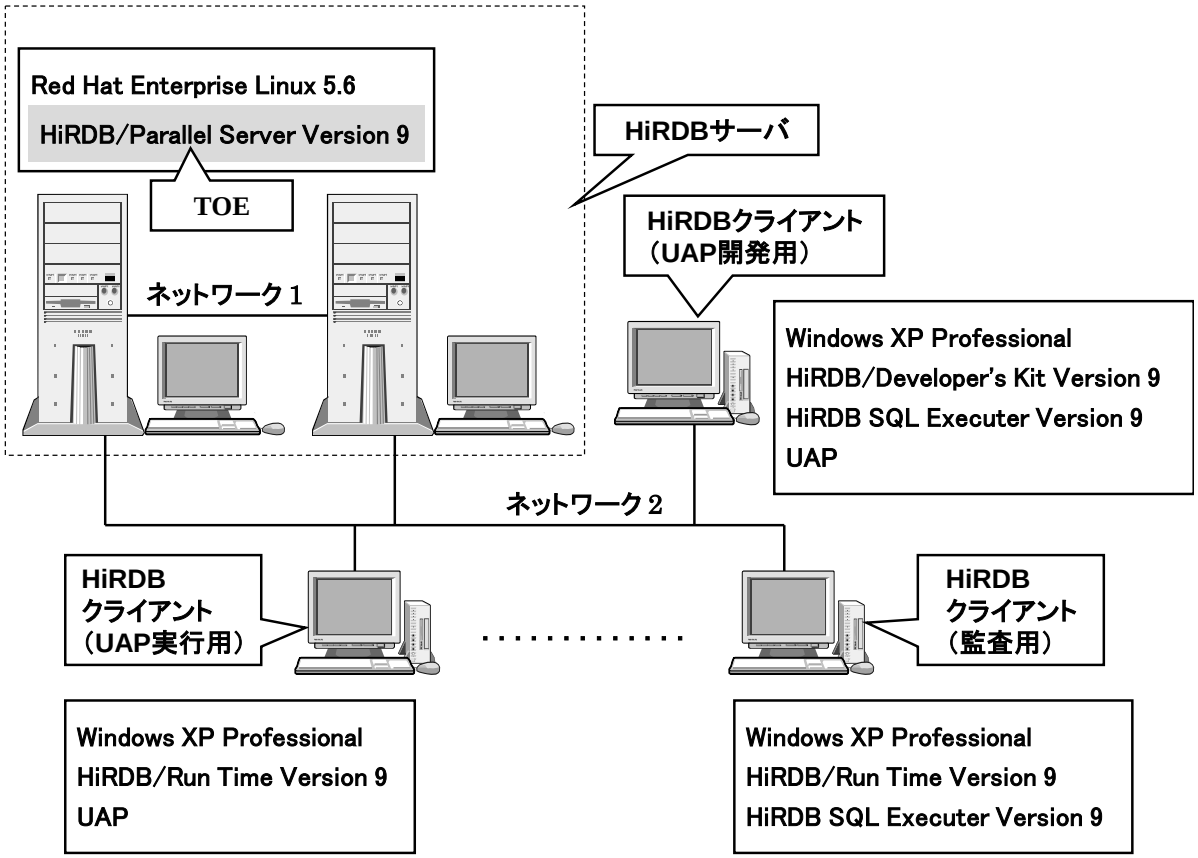

図 1.4-2 ： クライアントーサーバ(C/S)型のシステム構成(HiRDB / Parallel Server)

(1) マシン構成

以下に，図 1.4-1 および図 1.4-2 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。

(2) ソフトウェア構成

次に，図 1.4-1 および図 1.4-2 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】

《Red Hat Enterprise Linux 5.6》
Red Hat Enterprise Linux 5.6 は HiRDB サーバに搭載される OS である。Red Hat Enterprise Linux 5.6 は TOE 外である。

《HiRDB Server Version 9 (Linux 版)》
HiRDB Server Version 9 (Linux 版)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。

【HiRDB クライアント】

《Windows XP Professinaol》
Windows XP Professinaol 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 Professinaol は TOE 外である。

《HiRDB / Developer's Kit Version 9》
HiRDB / Developer's Kit Version 9 は，HiRDB / Run Time Version 9 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 9 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 9 は TOE 外である。

《HiRDB SQL Executer Version 9》
HiRDB SQL Executer Version 9 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 Version 9 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 Version 9 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 Version 9 は TOE 外である。

《HiRDB / Run Time Version 9》
HiRDB / Run Time Version 9 は，UAP もしくは HiRDB SQL Executer Version 9 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 9 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 9 は TOE 外である。

1.4.1.4. 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。

(1) 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 1.4-3 に示す。

ユーザ実表

品番	商品名	規格	単価	数量	原価
20180	掃除機	C20	20000	26	15000
20130	冷蔵庫	P10	30000	70	25000
20220	テレビ	K18	35000	12	30000
20200	掃除機	C89	35000	30	30000
20140	冷蔵庫	P23	35000	60	30000
20280	アンプ	L10	38000	200	33000
20150	冷蔵庫	P32	48000	50	43000
20290	アンプ	L50	49800	260	45000
20230	テレビ	K20	50000	15	45000
20160	冷蔵庫	P35	55800	120	50000

ユーザビュー表

品番	規格	原価
20220	K18	30000
20230	K20	45000

図 1.4-3 ： 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，データ操作毎のアクセス可否は，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。

(2) 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。

(3) 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。

1.4.2. TOEの物理的範囲

1.4.2.1. TOEを構成するソフトウェア

- HiRDB Server を構成する以下のいずれか
  - HiRDB / Single Server
  - HiRDB / Parallel Server

1.4.2.2. TOEを構成するガイダンス文書

- HiRDB Version 9 セキュリティガイド (3020-6-459)

- HiRDB Version 9 セキュリティガイドが参照する各マニュアル(8.4 参照)

1.4.3. TOEの論理的範囲

TOE の論理構成は,「1.4.1.3 評価構成」を参照のこと。
評価対象とするセキュリティ機能は以下である。

- 監査
- アクセス制御
- 識別・認証
- 利用者・権限管理

1.4.4. TOE関連の利用者役割

TOE に関連する利用者役割を説明する。

1.4.4.1. 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。なお, これらの利用者役割は, HiRDB サーバを構成する各マシンの OS において同様に維持される(OS アカウントを持つ)。

(1) 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。

(2) 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, 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。
HiRDB 管理者は, 一般的に, DB ユーザとして DBA 権限保持者を兼任する。

(3) 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。

「1.4.4.2 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。一般OSユーザのOSアカウントは，ログインのために，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。

1.4.4.2. 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。

(1) 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 1.4-1 に示す。なお，「アクセス権限」とは，表 1.4-1 で示す各権限の総称として用いられる用語である。

表 1.4-1 ： 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。

(2) 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

(3) 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。

(4) 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 SELECT 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。

(5) 監査証跡参照者

監査証跡参照者は監査証跡表の SELECT 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。

1.4.4.3. 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。

(1) 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 だけが利用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。

(2) 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。

1.4.4.4. 管理者と利用者役割の関係

1. 管理者(administrator)は，以下のいずれか，あるいは複数の，利用者役割をもつ利用者である。
   - スーパーユーザ

- HiRDB 管理者
- DBA 権限保持者
- 監査人
- スキーマ所有者

2. 許可管理者(authorized administrator)は, 以下のいずれか, あるいは複数の, TOE によって維持される利用者役割をもつ利用者である。
   - DBA 権限保持者
   - 監査人
   - スキーマ所有者

1.4.4.5. 利用者と利用者役割の関係

1. 利用者(user)は, 以下のいずれか, あるいは複数の, 利用者役割をもつ。
   - DB ユーザ
   - UAP 管理者
   - UAP 利用者
2. 許可利用者(authorized user)は, 以下の利用者役割をもつ利用者である。
   - DB ユーザ

2. 適合主張

2.1. CC適合主張

本 ST は以下の CC に適合している。

- ST が適合主張する CC のバージョン
  - Part 1: Introduction and general model
    July 2009 Version 3.1 Revision 3 Final
  - Part 2: Security functional components
    July 2009 Version 3.1 Revision 3 Final
  - Part 3: Security assurance components
    July 2009 Version 3.1 Revision 3 Final
- CC Part 2 に対する適合
  - CC Part 2 extended
- CC Part 3 に対する適合
  - CC Part 3 conformant

2.2. PP主張，パッケージ主張

2.2.1. PP主張

本 ST が適合主張する PP はない。

2.2.2. パッケージ主張

本 ST の評価保証レベルは EAL2 Augmented である。
追加されるセキュリティ保証要件は ALC_FLR.2 である。

2.3. 主張根拠

2.3.1. PP適合主張根拠

本 ST は PP 適合を主張しないが，参照する U.S.GPP の TOE 種別とは一貫している。

3. セキュリティ課題定義

本章では，脅威，前提条件，組織のセキュリティ方針について記述する。

3.1. 脅威

U.S. GPP と同じ脅威を Table 3.1-1 に示す。なお，U.S.GPP と同じ脅威については，具体的な内容を追記することにより補足する。

Table 3.1-1 :Applicable Threats

Threat	Definition
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.TSF_COMPROMISE	A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.

3.2. 組織のセキュリティ方針

U.S. GPP と同じ組織のセキュリティ方針を Table 3.2-1 に示す。

Table 3.2-1 :Applicable Policies

Policy	Definition
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE. ✧ 具体的には，DB ユーザのオブジェクト(ユーザ表)に対するアクセスを対象としなければならない。また，アクセス制御に関連する設定変更(パスワード，DBA 権限，スキーマ定義権限，アクセス権限，監査証跡表の SELECT 権限)も対象としなければならない。
P.ROLES	The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.

3.3. 前提条件

U.S. GPP と同じ前提条件を Table 3.3-1 に，追加した前提条件を Table 3.3-2 に示す。なお，U.S.GPP と同じ前提条件については，具体的な内容を追記することにより補足する。

Table 3.3-1 :Applicable Assumptions[1]

Assumption	Definition
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance.
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS. ✧ 具体的には，TOE の動作に必要な IT 環境が許容される。
A.PHYSICAL	It is assumed that appropriate physical security is provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information. ✧ 具体的には，許可されない人からの物理的な攻撃に対抗できるように，セキュアに管理されたサーバルームのサーバに TOE を設置することが要求される。TSF データ，利用者データは，TOE が設置されるサーバに保存されるため，セキュアなサーバ管理が要求される。サーバ間のネットワークもサーバルーム内へ設置されるなど，物理的な攻撃から保護されることが要求される。

Table 3.3-2 :Applicable Assumptions[2]

Assumption	Definition
A.PASSWORD	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。
A.UAP	HiRDB クライアントで利用される UAP は，TOE ガイダンスに従って，プロトコル，送信方式，連携方式が信頼できる形式であることが確認できたものでなければならない。

4. セキュリティ対策方針

本章では, TOE のセキュリティ対策方針, 運用環境のセキュリティ対策方針, およびセキュリティ対策方針の根拠について記述する。

4.1. TOEのセキュリティ対策方針

U.S. GPP と同じ TOE のセキュリティ対策方針を Table 4.1-1, 追加した TOE のセキュリティ対策方針を Table 4.1-2 に示す。なお, U.S.GPP と同じ TOE のセキュリティ対策方針については, 具体的な内容を追記することにより補足する。

Table 4.1-1 :Security Objectives[1]

Objective Name	Objective Definition
O.ACCESS_HISTORY	The TOE will store and retrieve information (to authorized users) related to previous attempts to establish a session.
O.ADMIN_ROLE	The TOE will provide authorized administrator roles to isolate administrative actions.
O.AUDIT_GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users. ✧ 具体的には, DB ユーザのオブジェクト(ユーザ表)に対するアクセスを対象としなければならない。また, アクセス制御に関連する設定変更(パスワード, DBA 権限, スキーマ定義権限, アクセス権限, 監査証跡表の SELECT 権限)も対象としなければならない。
O.MANAGE	The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. ✧ 具体的には, 管理権限を持つ各役割に応じて, 以下の管理機能を提供しなければならない。なお, 一般 DB ユーザは, 管理権限を持たないが自身のパスワード管理機能を提供しなければならない。 [DBA 権限保持者] DB ユーザの管理, DB ユーザに付与されるアクセス権限

Objective Name	Objective Definition
	の管理(付与, 取り消し), 認証機能の設定(連続失敗回数, ロック, パスワード構成文字)に関する機能 [監査人] 監査イベントの管理, 監査証跡表に対するアクセス権限の管理(付与, 取り消し)に関する機能 [スキーマ所有者] ユーザ表に対するアクセス権限の管理(付与, 取り消し), デフォルト所有者の設定に関する機能
O.MEDIATE	The TOE must protect user data in accordance with its security policy. ✧ 具体的には, 利用者データ(ユーザ表)への許可されないアクセスを制限しなければならない。また, アクセス制御に利用される TSF データ(ディクショナリ表)は, 分散されたコンポーネント間で一貫していなければならない。
O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to the TOE.

Table 4.1-2 :Security Objectives[2]

Objective Name	Objective Definition
O.AUDIT_PROTECTION	TOE は監査データを保護しなければならない。
O.AUDIT_REVIEW	TOE は監査データを評価するのに要求されるアクセス権を保持する利用者が, 監査データをレビューする手段を提供しなければならない。

4.2. 運用環境のセキュリティ対策方針

U.S. GPP と同じ運用環境のセキュリティ対策方針を Table 4.2-1, 追加した運用環境のセキュリティ対策方針を Table 4.2-2 に示す。なお, U.S.GPP と同じ運用環境のセキュリティ対策方針については, 具体的な内容を追記することにより補足する。

Table 4.2-1 : Environmental Security Objectives[1]

Environmental Objective Name	Environmental Objective Definition
OE.NO_EVIL	Sites using the TOE shall ensure that authorized administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.NO_GENERAL_ PURPOSE	There will be no general-purpose computing capabilities (e.g.,

Environmental Objective Name	Environmental Objective Definition
	compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration and support of the DBMS. ✧ 具体的には，1.3.3 に示す TOE の動作に必要なハードウェア/ソフトウェアのサーバ環境が対応する。
OE.PHYSICAL	Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed, and transmitted information. ✧ 具体的には，適切に管理されたサーバルームに，適切に管理されたサーバとネットワークを配置し，その中に TOE インストールすることにより物理的な攻撃から保護される環境を構築することが必要とされる。

Table 4.2-2 ： Environmental Security Objectives[2]

Environmental Objective Name	Environmental Objective Definition
OE.PASSWORD	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。
OE.UAP	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。 ● 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た UAP だけが利用される。

4.3. TOEのセキュリティ対策方針根拠

TOE のセキュリティ対策方針によって対抗される脅威，及び実施される組織のセキュリティ方針と，その根拠を Table 4.3-1 に示す。なお，U.S.GPP と同じ脅威，同じ TOE のセキュリティ対策方針に対する追記に応じて，TOE のセキュリティ対策方針根拠についても，具体的な内容を追記することにより補足する。また，U.S.GPP に **O.AUDIT_REVIEW** および **O.AUDIT_PROTECTION** を追加することにより，組織のセキュリティ対策方針を強化している。根拠をそれぞれ**太字**で示す。

Table 4.3-1 :Rationale for TOE Security Objectives

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
T.MASQUERADE A user or process may	**O.TOE_ACCESS** The TOE will provide	**O.TOE_ACCESS** mitigates this threat by controlling the logical

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
masquerade as another entity in order to gain unauthorized access to data or TOE resources.	mechanisms that control a user's logical access to the TOE.	access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.
T.TSF_COMPROMISE A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).	**O.MANAGE** The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. ✧ 具体的には，管理権限を持つ各役割に応じて，以下の管理機能を提供しなければならない。なお，一般 DB ユーザは，管理権限を持たないが自身のパスワード管理機能を提供しなければならない。	**O.MANAGE** is necessary because an access control policy is specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
	[DBA 権限保持者] DB ユーザの管理, DB ユーザに付与されるアクセス権限の管理(付与, 取り消し), 認証機能の設定(連続失敗回数, ロック, パスワード構成文字)に関する機能 [監査人] 監査イベントの管理, 監査証跡表に対するアクセス権限の管理(付与, 取り消し)に関する機能 [スキーマ所有者] ユーザ表に対するアクセス権限の管理(付与, 取り消し), デフォルト所有者の設定に関する機能	
T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	**O.MEDIATE** The TOE must protect user data in accordance with its security policy. ✧ 具体的には, 利用者データ(ユーザ表)への許可されないアクセスを制限しなければならない。また, アクセス制御に利用される TSF データ(ディクショナリ表)は, 分散されたコンポーネント間で一貫していなければならない。	**O.MEDIATE** ensures that all accesses to user data are subject to mediation, unless said data has been specifically identifies as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker’s opportunity to conduct a man-in-the-middle and/or password guessing attack successfully is greatly reduced. Lastly, the TSF will ensure that

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
		all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc to the administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.
	O.ACCESS_HISTORY The TOE will store and retrieve information (to authorized users) related to previous attempts to establish a session.	**O.ACCESS_HISTORY** is important to mitigate this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without their knowledge.
T.UNIDENTIFIED_ACTIONS Failure of the authorized administrator to identify and act upon unauthorized actions may occur.	**O.MANAGE** The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	The threat of an authorized administrator failing to know about malicious audit events produces the objectives of the authorized administrator having the capability to use the mechanisms (**O.MANAGE**) to review audit records.

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
	✧ 具体的には，管理権限を持つ各役割に応じて，以下の管理機能を提供しなければならない。なお，一般 DB ユーザは，管理権限を持たないが自身のパスワード管理機能を提供しなければならない。 [DBA 権限保持者] DB ユーザの管理，DB ユーザに付与されるアクセス権限の管理(付与，取り消し)，認証機能の設定(連続失敗回数，ロック，パスワード構成文字)に関する機能 [監査人] 監査イベントの管理，監査証跡表に対するアクセス権限の管理(付与，取り消し)に関する機能 [スキーマ所有者] ユーザ表に対するアクセス権限の管理(付与，取り消し)，デフォルト所有者の設定に関する機能	
P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE. ✧ 具体的には，DB ユーザのオブジェクト(ユーザ表)に対するアクセスを対象としなければならない。また，アクセス制御に関連する設定変	**O.AUDIT_GENERATION** The TOE will provide the capability to detect and create records of security relevant events associated with users. ✧ 具体的には，DB ユーザのオブジェクト(ユーザ表)に対するアクセスを対象としなければならない。また，アクセス制御に関連する設定変更(パスワード，	**O.AUDIT_GENERATION** addresses this policy by providing the authorized administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the

Threat/Policy	Objectives Addressing the Threat/Policy	Rationale
更(パスワード, DBA 権限, スキーマ定義権限, アクセス権限, 監査証跡表の SELECT 権限)も対象としなければならない。	DBA 権限, スキーマ定義権限, アクセス権限, 監査証跡表の SELECT 権限)も対象としなければならない。	administrator's ID is recorded when any security relevant change is made to the TOE (e.g., access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).
	O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	**O.TOE_ACCESS** supports this policy by requiring the TOE to identify and authenticate all authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users.
	O.AUDIT_REVIEW TOE は監査データを評価するのに要求されるアクセス権を保持する利用者が, 監査データをレビューする手段を提供しなければならない。	**許可管理者に監査データ情報を選択的にレビューする機能を提供する。**
	O.AUDIT_PROTECTION TOE は監査データを保護しなければならない。	**許可されていないアクセスや監査情報の消失から監査証跡を保護し, 脅威に対抗する。**
P.ROLES The TOE shall provide an authorized administrator role for secure administration of the TOE. This role shall be separate and distinct from other authorized users.	**O.ADMIN_ROLE** The TOE will provide authorized administrator roles to isolate administrative actions.	The TOE has the objective of providing an authorized administrator role for secure administration. The TOE may provide other roles as well, but only the role of authorized administrator is required (**O.ADMIN_ROLE**).

4.4. 運用環境のセキュリティ対策方針根拠

U.S. GPP と同じ運用環境のセキュリティ対策方針によって充足される前提条件と, その根拠を Table 4.4-1 に示

す。なお，U.S.GPP と同じ前提条件，同じ運用環境のセキュリティ対策方針に対する追記に応じて，運用環境のセキュリティ対策方針根拠についても，具体的な内容を追記することにより補足する。
また，追加した運用環境のセキュリティ対策方針によって充足される前提条件と，その根拠を Table 4.4-2 に示す。

Table 4.4-1 :Rational for IT Environmental Objectives[1]

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.NO_EVIL Administrators are non-hostile, appropriately trained, and follow all administrator guidance.	**OE.NO_EVIL** Sites using the TOE shall ensure that authorized administrators are non-hostile, are appropriately trained and follow all administrator guidance.	All authorized administrators are trustworthy individuals, having background investigations commensurate with the level of data being protected, have undergone appropriate admin training, and follow all admin guidance.
A.NO_GENERAL_PURPOSE There are no general-purpose computing or storage repository capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration and support of the DBMS. ✧ 具体的には，TOE の動作に必要な IT 環境が許容される。	**OE.NO_GENERAL_PURPOSE** There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration and support of the DBMS. ✧ 具体的には，1.3.3 に示す TOE の動作に必要なハードウェア/ソフトウェアのサーバ環境が対応する。	The DBMS server must not include any general-purpose commuting or storage capabilities. This will protect the TSF data from malicious processes.
A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT	**OE.PHYSICAL** Physical security will be provided within the domain for the value of the IT assets protected by the TOE and the value of the stored, processed,	The TOE, the TSF data, and protected user data is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include

Assumption	Environmental Objective Addressing the Assumption	Rationale
environment. ✧ 具体的には，許可されない人からの物理的な攻撃に対抗できるように，セキュアに管理されたサーバルームのサーバに TOE を設置することが要求される。TSF データ，利用者データは，TOE が設置されるサーバに保存されるため，セキュアなサーバ管理が要求される。サーバ間のネットワークもサーバルーム内へ設置されるなど，物理的な攻撃から保護されることが要求される。	and transmitted information. ✧ 具体的には，適切に管理されたサーバルームに，適切に管理されたサーバとネットワークを配置し，その中に TOE インストールすることにより物理的な攻撃から保護される環境を構築することが必要とされる。	unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment.

Table 4.4-2 :Rational for IT Environmental Objectives[2]

Assumption	Environmental Objective Addressing the Assumption	Rationale
A.PASSWORD 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。	**OE.PASSWORD** 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。	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。
A.UAP HiRDB クライアントで利用される UAP は，TOE のガイダンスに従って，プロトコル，送信方式，連携方式が信頼できる形式であることが確認できたものでなければならない。	**OE.UAP** 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。 ● 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	UAP は，TOE のガイダンスに従って利用されることにより，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。

Assumption	Environmental Objective Addressing the Assumption	Rationale
	開発された UAP だけが利用される。	

5. 拡張コンポーネント定義

5.1. セキュリティ機能要件

本 ST では，既存コンポーネントで表現できない以下の 3 つの拡張コンポーネントを定義する。既存コンポーネントを拡張しているため，コンポーネント識別情報のファミリ名の後ろに，「_(EXT)」を追加することにより，既存のコンポーネント名との対応を明確にするとともに，その上位概念としての関係を示した。

- FMT_MSA_(EXT).3
- FPT_TRC_(EXT).1
- FTA_TAH_(EXT).1

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are not italicized.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments to be filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:].

5.1.1. Static attribute initialization (**FMT_MSA_(EXT).3**)

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA_(EXT).3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection, choose one of: *restrictive, permissive, [assignment: other property]*] default values for security attributes that are used to enforce the SFP.

5.1.2. Internal TSF consistency (**FPT_TRC_(EXT).1**)

Hierarchical to: No other components.

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_TRC_(EXT).1.1 The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state in a timely manner.

Application Note: In general, it is impossible to achieve complete, constant consistency of TSF data that is distributed to remote portions of a TOE because distributed portions of the TSF may be active at different times or disconnected from one another. This requirement attempts to address this

situation in a practical manner by acknowledging that there will be TSF data inconsistencies but that they will be corrected without undue delay. For example, a TSF could provide timely consistency through periodic broadcast of TSF data to all TSF nodes maintaining replicated TSF data. Another example approach is for the TSF to provide a mechanism to explicitly probe remote TSF nodes for inconsistencies and respond with action to correct the identified inconsistencies. Application Note: This requirement is trivially met if the TOE does not contain physically separated components.

5.1.3. TOE access history (**FTA_TAH_(EXT).1**)

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAH_(EXT).1.1	Upon successful session establishment, the TSF shall store and retrieve the [selection: *date, time, method, location*] of the last successful session establishment to the user.
FTA_TAH_(EXT).1.2	Upon successful session establishment, the TSF shall store and retrieve the [selection: *date, time, method, location*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

5.2. セキュリティ保証要件

本 ST では, 拡張コンポーネントを定義しない。

5.3. セキュリティ要件根拠

5.3.1. セキュリティ機能要件定義根拠

5.3.1.1. Static attribute initialization (**FMT_MSA_(EXT).3**)

The CC does not allow the ST author to specify restrictive values that are not modifiable. This extended requirement eliminates the element FMT_MSA.3.2 from the component FMT_MSA.3 and makes the component more secure by requiring the security attributes of the objects on creation to be restrictive and not allowing any user to be able of override the restrictive default values.

5.3.1.2. Internal TSF consistency (**FPT_TRC_(EXT).1**)

FPT_TRC_(EXT).1 has been created to require timely consistency of replicated TSF data. Although there is a Common Criteria Requirement that attempts to address this functionality, it falls short of the needs of the environment in this ST.

Specifically, FPT_TRC.1.1 states "The TSF shall ensure that TSF data is consistent when replicated

between parts of the TOE." In the widely distributed environment of this ST's TOE, this is an infeasible requirement. For TOEs with a very large number of components, 100 percent TSF data consistency is not achievable and is not expected at any specific instant in time.

Another concern lies in FPT_TRC.1.2 that states that when replicated parts of the TSF are "disconnected", the TSF shall ensure consistency of the TSF replicated data upon "reconnection". Upon first inspection, this seems reasonable, however, when applying this requirement it becomes clear that it dictates specific mechanisms to determine when a component is "disconnected" from the rest of the TSF and when it is "reconnected". This is problematic in this ST 's environment in that it is not the intent of the authors to dictate that distributed TSF components keep track of connected/disconnected components.

In general, to meet the needs of this ST, it is acceptable to only require a mechanism that provides TSF data consistency in a timely manner after it is determined that it is inconsistent.

5.3.1.3. TOE access history (**FTA_TAH_(EXT).1**)

This ST does not require the TOE to contain a client. Therefore, the ST cannot require the client to display a message. This requirement has been modified to require the TOE to store and retrieve the access history instead of displaying it.

6. セキュリティ要件

本章では，セキュリティ機能要件，セキュリティ保証要件，セキュリティ要件根拠について記述する。

6.1. 用語定義

セキュリティ機能要件およびセキュリティ保証要件で用いる用語の定義を表 6.1-1 に示す。

表 6.1-1 :用語定義

用語	定義
サブジェクト (subject)	オブジェクトに対して操作を実行する TOE の能動的なエンティティ ● サーバプロセス
オブジェクト (object)	情報を格納または受信し，サブジェクトによる操作の実行対象となる TOE 内の受動的なエンティティ ● ユーザ表 ● ディクショナリ表 ● 監査証跡ファイル ● 監査証跡表
操作 (operation)	サブジェクトによってオブジェクトに対し実行される特定のタイプのアクション ● 表定義・表削除 ● 行挿入・行削除・行更新・行参照 ● ファイル出力 その他のアクション ● 認可識別子の登録・削除 ● パスワード登録・変更・削除 ● 権限の付与・取消し ● パスワード最小文字数の変更 ● ロック時間の変更 ● 連続認証失敗許容回数の変更 ● 最大同時接続数の変更
セキュリティ属性 (security attribute)	サブジェクト，利用者(外部 IT 製品を含む)，オブジェクト，情報，セッション，及び/または資源の特性であり，SFR の定義及び SFR の実施においてその値が使用される ● DB ユーザの認可識別子 ● DBA 権限 ● スキーマ定義権限 ● 監査権限 ● アクセス権限

	下記は U.S. GPP で定義されたセキュリティ属性であり，上記のセキュリティ属性に対応する。 ● Security-relevant database roles 　➢ DBA 権限 　➢ スキーマ定義権限 　➢ 監査権限
外部エンティティ (external entity)	TOE の外部にあって TOE と対話することができる人間または IT のエンティティ ● HiRDB 管理者 ● DB ユーザ ● TOE の下で稼働する OS

6.2. セキュリティ機能要件

機能コンポーネントを Table 6.2-1 に示す。
U.S. GPP に含まれない SFR は**太字**で示す。

Table 6.2-1 :Security Functional Requirements

Functional Class	Functional Components	Functional Components Description
Security Audit	**FAU_GEN.1**	**Audit data generation**
	FAU_GEN.2	**User identity association**
	FAU_SAR.1	**Security audit review**
	FAU_SAR.2	**Restricted audit review**
	FAU_SAR.3	**Selectable audit review**
	FAU_SEL.1	**Selective audit**
	FAU_STG.1	**Protected audit trail storage**
	FAU_STG.4	**Prevention of audit data loss**
User data protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	**Security attribute based access control**
Identification and authentication	**FIA_AFL.1**	**Authentication failure handling**
	FIA_ATD.1	User attribute definition
	FIA_SOS.1	**Verification of secrets**
	FIA_UAU.2	**User authentication before any action**
	FIA_UID.2	**User identification before any action**
	FIA_USB.1	**User-subject binding**
Security management	FMT_MOF.1	Management of security functions behavior

Functional Class	Functional Components	Functional Components Description
	FMT_MSA.1	Management of security attributes
	FMT_MSA_(EXT).3	Static attribute initialization
	FMT_MTD.1(1)	Management of TSF data
	FMT_MTD.1(2)	**Management of TSF data**
	FMT_REV.1(1)	Revocation (user attributes)
	FMT_REV.1(2)	Revocation (subject, object attributes)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of the TSF	**FPT_STM.1**	**Reliable time stamps**
	FPT_TRC_(EXT).1	Internal TSF consistency
TOE access	FTA_TAH_(EXT).1	TOE access history

機能要件の操作(**selection**, **assignment**, **refinement**, **iteration**)について, 表記方法を以下に示す。

- selection は,「[*選択した内容*]」のように*斜体*で表記する。
- assignment は,「[割付した内容]」のように表記する。
- refinement は,「Refinement: **詳細化した内容**」のように**太字**を使用して表記する。
- iteration は,「コンポーネント名(n)」のように表記する。
- 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。

6.2.1. Security Audit(FAU)

6.2.1.1. Audit data generation (**FAU_GEN.1**)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified*] level of audit; and

c) [Start-up and shutdown of the DBMS; Auditable events listed in Table 6.2-2 and Table 6.2-3].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 6.2-2 and Table 6.2-3 below].

Table 6.2-2 :Auditable Events[1]

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.2	None	
FDP_ACC.1	None	
FIA_ATD.1	None	
FMT_MOF.1	None	
FMT_MSA.1	None	
FMT_MSA_(EXT).3	None	
FMT_MTD.1	None	
FMT_REV.1(1)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_REV.1(2)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_SMF.1	Use of the management functions	Identity of the administrator performing these functions
FMT_SMR.1	None	
FPT_TRC_(EXT).1	None	
FTA_TAH_(EXT).1	None	

Table 6.2-3 :Auditable Events[2]

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_GEN.1	なし	
FAU_SAR.1	監査記録からの情報の読み出し 〔監査証跡表の行検索〕	監査証跡表の識別情報
FAU_SAR.2	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	なし	
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the authorized administrator that made the change to the audit configuration

Security Functional Requirement	Auditable Event(s)	Additional Audit Record Contents
FAU_STG.1	なし	
FAU_STG.4	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_ACF.1	Successful requests to perform an operation on an object covered by the SFP	The identity of the subject performing the operation
FIA_AFL.1	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〕	認可識別子
FIA_SOS.1	TSF による, テストされた秘密の拒否または受け入れ 〔パスワードの登録・変更〕	
FIA_UAU.2	認証メカニズムのすべての使用 〔接続〕	認可識別子
FIA_UID.2	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〕	認可識別子
FIA_USB.1	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) 〔接続〕	認可識別子
FPT_STM.1	なし	

6.2.1.2. User identity association (**FAU_GEN.2**)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3. Security audit review (**FAU_SAR.1**)

FAU_SAR.1.1 The TSF shall provide [監査人, 監査証跡参照者] with the capability to read [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] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4. Restricted audit review (**FAU_SAR.2**)

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.5. Selectable audit review (**FAU_SAR.3**)

FAU_SAR.3.1 The TSF shall provide the ability to apply [検索, 並べ替え] of audit data based on [監査データの任意の情報の大小関係や同値関係].

6.2.1.6. Selective audit (**FAU_SEL.1**)

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [*object identity*,*event type*],
b) [success of auditable security events,failure of auditable security events].

6.2.1.7. Protected audit trail storage (**FAU_STG.1**)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [*prevent*] unauthorised modifications to the stored audit records in the audit trail.

6.2.1.8. Prevention of audit data loss (**FAU_STG.4**)

FAU_STG.4.1 The TSF shall [*overwrite the oldest stored audit records*] and [上書き開始を通知するメッセージ出力のアクション] if the audit trail is full.

6.2.2. User data protection(FDP)

6.2.2.1. Subset access control (**FDP_ACC.1**)

FDP_ACC.1.1 The TSF shall enforce the [HiRDB Access Control policy] on [all subjects, all objects and all operations among them].

6.2.2.2. Security attribute based access control (**FDP_ACF.1**)

FDP_ACF.1.1 The TSF shall enforce the [HiRDB Access Control policy] to objects based on the following:

- [the authorized user identity associated with a subject;
- access operations implemented for objects; and
- object identity].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

[The HiRDB Access Control policy mechanism shall, either by explicit authorized user action or by default, provide that controlled objects are protected from unauthorized access according to the following ordered rules:

a) If the requested mode of access is denied to that authorized user, deny access;
b) If the requested mode of access is permitted to that authorized user, permit access;
c) Else, deny access

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [no additional rules].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [no additional explicit denial rules].

6.2.3. Identification and authentication（FIA）

6.2.3.1. Authentication failure handling (**FIA_AFL.1**)

FIA_AFL.1.1 The TSF shall detect when [*an administrator configurable positive integer within*[1～10]] unsuccessful authentication attempts occur related to [同一認可識別子を指定する連続した識別・認証試行].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [*met*], the TSF shall [以下のアクション].

【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。

6.2.3.2. User attribute definition (**FIA_ATD.1**)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [以下のセキュリティ属性]

【セキュリティ属性】

- Database user identifier
- Security-relevant database roles
- アクセス権限

6.2.3.3. Verification of secrets (**FIA_SOS.1**)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [以下の品質尺度].

【品質尺度】

- 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)

6.2.3.4. User authentication before any action (**FIA_UAU.2**)

FIA_UAU.2.1 **Refinement: When using SQL interface,** the TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.5. User identification before any action (**FIA_UID.2**)

FIA_UID.2.1 **Refinement: When using SQL interface,** the TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.6. User-subject binding (**FIA_USB.1**)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**FIA_ATD.1.1** に指定されたセキュリティ属性].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [以下の規則].

【規則】

なし

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [以下の規則].

【規則】

なし

6.2.4. Security management（FMT）

6.2.4.1. Management of security functions behavior (**FMT_MOF.1**)

FMT_MOF.1.1 The TSF shall restrict the ability to [*disable and enable*] the functions [監査される事象の指定に関連する以下の機能] to [DBA 権限保持者]:

【機能】

- 連続認証失敗を制限するロック機能
- パスワード構成文字を制限する機能.

6.2.4.2. Management of security attributes (**FMT_MSA.1**)

FMT_MSA.1.1 The TSF shall enforce the [HiRDB Access Control policy] to restrict the ability to [*[manage]*] the security attributes [all] to [DBA 権限保持者, 監査人, スキーマ所有者].

6.2.4.3. Static attribute initialization (**FMT_MSA_(EXT).3**)

FMT_MSA_(EXT).3.1 The TSF shall enforce the [HiRDB Access Control policy] to provide restrictive default values for security attributes that are used to enforce the SFP.

6.2.4.4. Management of TSF data (**FMT_MTD.1(1)**)

FMT_MTD.1.1(1) The TSF shall restrict the ability to [*[select]*] the [auditable events] to [監査人].

6.2.4.5. Management of TSF data (**FMT_MTD.1(2)**)

FMT_MTD.1.1(2) The TSF shall restrict the ability to [*[以下の操作]*] the [以下の TSF データ] to [以下の役割].

#	TSF データ	操作	役割
1	DB ユーザのパスワード	本人のパスワード登録・変更・削除	DB ユーザ
2		監査人を除く他人のパスワード登録・変更・削除	DBA 権限保持者
3	連続認証失敗許容回数	設定または解除	DBA 権限保持者
4	パスワード最小文字数	設定または解除	DBA 権限保持者
5	ロック時間	設定または解除	DBA 権限保持者

6.2.4.6. Revocation (**FMT_REV.1(1)**)

FMT_REV.1.1(1) The TSF shall restrict the ability to revoke [security attributes] associated with the [*users*] under the control of the TSF to [DBA 権限保持者].

FMT_REV.1.2(1) The TSF shall enforce the rules [以下の規則].

【規則】

- 監査人のスキーマを除き，スキーマに表がない場合に限り，当該スキーマ定義権限を取り消すことができる。
- 自分自身以外の DBA 権限を取り消すことができる。
- 監査人以外の，DBA 権限，およびスキーマを持たないユーザの CONNECT 権限を取り消すことができる。
- CONNECT 権限を取り消すと，スキーマ定義権限も取り消される。

6.2.4.7. Revocation (**FMT_REV.1(2)**)

FMT_REV.1.1(2) The TSF shall restrict the ability to revoke [security attributes] associated with the [*objects*] under the control of the TSF to [スキーマ所有者].

FMT_REV.1.2(2) The TSF shall enforce the rules [以下の規則].

【規則】

- 他人に付与したアクセス権限を取り消すことができる。

6.2.4.8. Specification of Management Functions (**FMT_SMF.1**)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [TSF によって提供される以下のセキュリティ管理機能].

【セキュリティ管理機能】

- 認可識別子の登録，削除
- DBA 権限保持者によるパスワード登録，変更，削除
- DB ユーザ本人によるパスワード登録，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
- 監査証跡表の SELECT 権限の付与，取消し
- アクセス権限の付与，取り消し
- 監査対象事象の登録，削除
- 連続認証失敗を制限するロック機能の開始，停止
  - 連続認証失敗許容回数の設定，解除
  - ロック時間の設定，解除
- パスワード構成文字を制限する機能の開始，停止
  - パスワード最小文字数の設定，解除

6.2.4.9. Security roles (**FMT_SMR.1**)

FMT_SMR.1.1 The TSF shall maintain the roles [以下の許可された識別された役割].

【役割】

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

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.5. Protection of the TSF（FPT）

6.2.5.1. Reliable time stamps (**FPT_STM.1**)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2.5.2. Internal TSF consistency (**FPT_TRC_(EXT).1**)

FPT_TRC_(EXT).1.1 The TSF shall ensure that TSF data is consistent between parts of the TOE by providing a mechanism to bring inconsistent TSF data into a consistent state in a timely manner.

6.2.6. TOE access（FTA）

6.2.6.1. TOE access history (**FTA_TAH_(EXT).1**)

FTA_TAH_(EXT).1.1 Upon successful session establishment, the TSF shall store and retrieve the [*date and time*] of the last successful session establishment to the user.

FTA_TAH_(EXT).1.2 Upon successful session establishment, the TSF shall store and retrieve the [*date and time*] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

6.3. セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 Augmented であり，追加する保証コンポーネント ALC_FLR.2 である。該当する保証コンポーネントを Table 6.3-1 に示す。

Table 6.3-1 : Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description

Assurance Class	Assurance Components	Assurance Components Description
Development	**ADV_ARC.1**	Architectural Design with domain separation and non-bypassability
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic design
Guidance Documents	**AGD_OPE.1**	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life Cycle Support	**ALC_CMC.2**	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	**Flaw Reporting Procedures**
Tests	**ATE_COV.1**	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – conformance
Vulnerability Assessment	**AVA_VAN.2**	Vulnerability analysis

6.4. セキュリティ要件根拠

6.4.1. セキュリティ機能要件根拠

U.S. GPP と同じセキュリティ要件によって実現される TOE のセキュリティ対策方針と，その根拠を Table 6.4-1 に示す。また，追加したセキュリティ要件によって実現される TOE のセキュリティ対策方針と，その根拠を Table 6.4-2 に示す。なお，U.S.GPP と同じ TOE のセキュリティ対策方針に対する追記に応じて，セキュリティ機能要件根拠についても，具体的な内容を追記することにより補足する。

Table 6.4-1 :Rationale for TOE Security Requirements[1]

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS_HISTORY The TOE will store and retrieve information (to authorized users) related to previous attempts to establish a session.	**FTA_TAH_(EXT).1**	The TOE must be able to store and retrieve information about previous unauthorized login attempts and the number times the login was attempted every time the user logs into their account. The TOE must also store the last successful

Objective	Requirements Addressing the Objective	Rationale
		authorized login. This information will include the date, time, method, and location of the attempts. When appropriately displayed, this will allow the user to detect if another user is attempting to access their account. These records should not be deleted until after the user has been notified of their access history. (**FTA_TAH_(EXT).1**)
O.ADMIN_ROLE The TOE will provide authorized administrator roles to isolate administrative actions.	**FMT_SMR.1**	The TOE will establish, at least, an authorized administrator role. The ST writer may choose to specify more roles. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions. (**FMT_SMR.1**)
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users. ✧ 具体的には, DB ユーザのオブジェクト(ユーザ表)に対するアクセスを対象としなければならない。また, アクセ	**FAU_GEN.1**	**FAU_GEN.1** defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit

Objective	Requirements Addressing the Objective	Rationale
ス制御に関連する設定変更(パスワード, DBA 権限, スキーマ定義権限, アクセス権限, 監査証跡表の SELECT 権限)も対象としなければならない。		record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to U.S. GPP.
	FAU_GEN.2	**FAU_GEN.2** ensures that the audit records associate a user identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID.
	FAU_SEL.1	**FAU_SEL.1** allows the administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism.
O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	**FMT_MOF.1**	**FMT_MOF.1** requires that the ability to use particular TOE capabilities be restricted to the administrator.
	FMT_MSA.1	**FMT_MSA.1** requires that the ability to perform operations on security attributes be restricted to particular roles.
	FMT_MSA_(EXT).3	**FMT_MSA_(EXT).3** requires that default values used for

Objective	Requirements Addressing the Objective	Rationale
✧ 具体的には，管理権限を持つ各役割に応じて，以下の管理機能を提供しなければならない。なお，一般DBユーザは，管理権限を持たないが自身のパスワード管理機能を提供しなければならない。 [DBA 権限保持者] DB ユーザの管理，DB ユーザに付与されるアクセス権限の管理(付与，取り消し)，認証機能の設定(連続失敗回数，ロック，パスワード構成文字)に関する機能 [監査人] 監査イベントの管理，監査証跡表に対するアクセス権限の管理(付与，取り消し)に関する機能 [スキーマ所有者] ユーザ表に対するアクセス権限の管理(付与，取り消し)，デフォルト所有者の設定に関する機能		security attributes are restrictive.
	FMT_MTD.1(1)	**FMT_MTD.1(1)** requires that the ability to manipulate TOE content is restricted to administrators.
	FMT_REV.1(1) **FMT_REV.1(2)**	**FMT_REV.1** restricts the ability to revoke attributes to the administrator.
	FMT_SMF.1	**FMT_SMF.1** identifies the management functions that are available to the authorized administrator.
	FMT_SMR.1	**FMT_SMR.1** defines the specific security roles to be supported.
O.MEDIATE The TOE must protect user data in accordance with its security policy. ✧ 具体的には，利用者データ(ユーザ表)への許可されないアクセスを制限しなければならない。また，アクセス制御に利用される TSF デ	**FDP_ACC.1**	The **FDP** requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation takes place in the TOE. **FDP_ACC.1** defines the Access Control policy that will be enforced on a list of subjects acting on the behalf of users

Objective	Requirements Addressing the Objective	Rationale
ータ(ディクショナリ表)は，分散されたコンポーネント間で一貫していなければならない。		attempting to gain access to a list of named objects. All the operation between subject and object covered are defined by the TOE's policy.
	FDP_ACF.1	**FDP_ACF.1** defines the security attribute used to provide access control to objects based on the TOE's access control policy.
	FPT_TRC_(EXT).1	Replicated TSF data that specifies attributes for access control must be consistent across distributed components of the TOE. The requirement is to maintain consistency of replicated TSF data.
O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	**FIA_ATD.1**	**FIA_ATD.1** defines the attributes of users, including a user ID that is used by the TOE to determine a user's identity and enforce what type of access the user has to the TOE.

Table 6.4-2 :Rationale for TOE Security Requirements[2]

Objective	Requirements Addressing the Objective	Rationale
O.AUDIT_GENERATION The TOE will provide the capability to detect and create records of security relevant events associated with users. ✧ 具体的には，DB ユーザのオブジェクト(ユーザ表)に対	**FPT_STM.1**	TOE は，監査データの記録に必要な高信頼タイムスタンプを提供する。

Objective	Requirements Addressing the Objective	Rationale
するアクセスを対象としなければならない。また，アクセス制御に関連する設定変更(パスワード，DBA 権限，スキーマ定義権限，アクセス権限，監査証跡表の SELECT 権限)も対象としなければならない。		
O.AUDIT_PROTECTION TOE は監査データを保護しなければならない。	**FAU_STG.1**	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	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。
O.AUDIT_REVIEW TOE は監査データを評価するのに要求されるアクセス権を保持する利用者が，監査データをレビューする手段を提供しなければならない。	**FAU_SAR.1**	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	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	TOE は，監査データを検索，並べ替えする機能を提供する。
O.MANAGE The TOE will provide all the functions and facilities necessary to support the authorized administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	**FMT_MTD.1(2)**	TOE は，DB ユーザ本人のパスワード変更以外において，TSF データに対する操作を管理者に制限する。

Objective	Requirements Addressing the Objective	Rationale
O.TOE_ACCESS The TOE will provide mechanisms that control a user's logical access to the TOE.	**FIA_AFL.1**	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_SOS.1	TOE は，秘密（パスワード）の品質尺度を維持する。
	FIA_UAU.2	TOE は，認証が成功する前に接続を許可することはない。
	FIA_UID.2	TOE は，識別が成功する前に接続を許可することはない。
	FIA_USB.1	TOE は，DB ユーザに属する **FIA_ATD.1** に指定されたセキュリティ属性とその 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。

6.4.2. セキュリティ機能要件依存性

セキュリティ機能要件の依存性を Table 6.4-3 に示す。

Table 6.4-3 :Functional Requirement Dependencies

セキュリティ機能要件	CC の依存性	ST の依存性	Satisfied
FAU_GEN.1	**FPT_STM.1**	**FPT_STM.1**	Satisfied
FAU_GEN.2	**FAU_GEN.1** **FIA_UID.1**	**FAU_GEN.1** **FIA_UID.2**	Satisfied
FAU_SAR.1	**FAU_GEN.1**	**FAU_GEN.1**	Satisfied
FAU_SAR.2	**FAU_SAR.1**	**FAU_SAR.1**	Satisfied
FAU_SAR.3	**FAU_SAR.1**	**FAU_SAR.1**	Satisfied
FAU_SEL.1	**FAU_GEN.1** **FMT_MTD.1**	**FAU_GEN.1** **FMT_MTD.1(1)**	Satisfied
FAU_STG.1	**FAU_GEN.1**	**FAU_GEN.1**	Satisfied
FAU_STG.4	**FAU_STG.1**	**FAU_STG.1**	Satisfied
FDP_ACC.1	**FDP_ACF.1**	**FDP_ACF.1**	Satisfied
FDP_ACF.1	**FDP_ACC.1** **FMT_MSA.3**	**FDP_ACC.1** **FMT_MSA_(EXT).3**	Satisfied
FIA_AFL.1	**FIA_UAU.1**	**FIA_UAU.2**	Satisfied

セキュリティ機能要件	CC の依存性	ST の依存性	Satisfied
FIA_ATD.1	なし	なし	N/A
FIA_SOS.1	なし	なし	N/A
FIA_UAU.2	**FIA_UID.1**	**FIA_UID.2**	Satisfied
FIA_UID.2	なし	なし	N/A
FIA_USB.1	**FIA_ATD.1**	**FIA_ATD.1**	Satisfied
FMT_MOF.1	**FMT_SMF.1** **FMT_SMR.1**	**FMT_SMF.1** **FMT_SMR.1**	Satisfied
FMT_MSA.1	[**FDP_ACC.1** or **FDP_IFC.1**] **FMT_SMF.1** **FMT_SMR.1**	**FDP_ACC.1** **FMT_SMF.1** **FMT_SMR.1**	Satisfied
FMT_MSA_(EXT).3	**FMT_MSA.1** **FMT_SMR.1**	**FMT_MSA.1** **FMT_SMR.1**	Satisfied
FMT_MTD.1(1)	**FMT_SMF.1** **FMT_SMR.1**	**FMT_SMF.1** **FMT_SMR.1**	Satisfied
FMT_MTD.1(2)	**FMT_SMF.1** **FMT_SMR.1**	**FMT_SMF.1** **FMT_SMR.1**	Satisfied
FMT_REV.1(1)	**FMT_SMR.1**	**FMT_SMR.1**	Satisfied
FMT_REV.1(2)	**FMT_SMR.1**	**FMT_SMR.1**	Satisfied
FMT_SMF.1	なし	なし	N/A
FMT_SMR.1	**FIA_UID.1**	**FIA_UID.2**	Satisfied
FPT_STM.1	なし	なし	N/A
FPT_TRC_(EXT).1	**FPT_ITT.1**	**FPT_ITT.1**	TSF データ(ディクショナリ表)はサーバ内で複製されるため，暴露や改ざんに対して，**OE.PHYSICAL** により IT 環境で保護されるため，考慮する必要がない。
FTA_TAH_(EXT).1	なし	なし	N/A

Table 6.4-3 より，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。

6.4.3. 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，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 EAL2 を適用する。
また，本 ST では，EAL2 の保証要件の基本コンポーネントに加え，欠陥修正および欠陥報告の手続きを重視することにより，ALC_FLR.2 コンポーネントを適用する。

7. TOE要約仕様

7.1. TOEセキュリティ機能

本節では，TOE セキュリティ機能，および TOE がどのように「6.2 セキュリティ機能要件」で記述した各セキュリティ機能要件を満足しているかを記述する。

7.1.1. 監査(SF.AUD)

7.1.1.1. 機能概要

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。

7.1.1.2. 監査データ生成(**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，OS 機構を利用し，タイムスタンプを生成する機能を実現する(**FPT_STM.1**)。

監査機能の起動および終了は，HiRDB 管理者によって制御される。

表 7.1-1 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 7.1-1 で示す監査対象事象の発生時に監査データを採取する(**FAU_GEN.1**)。

TOE は，表 7.1-1 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(**FMT_SMF.1**)。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(**FAU_SEL.1**)(**FMT_MTD.1(1)**)。

監査データには，以下の監査情報が含まれる。

- 事象の日付・時刻（タイムスタンプを使用する）
- 監査対象事象（例えば，”アクセス権限の付与”）
- 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(**FAU_GEN.2**)，および

接続通番）

- 事象の結果（成功または失敗）
- SQL コードまたは終了コード

また，監査対象事象毎に追加される監査情報は，表 7.1-1 に示す通りである。

表 7.1-1 :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	HiRDB の起動	監査機能の設定値
	HiRDB の終了	なし
	監査機能の起動と終了	なし
	監査証跡ファイルのスワップ	なし
	監査証跡表の行検索，行削除	監査証跡表の識別情報
	監査対象事象の選択	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 SELECT 権限の付与	監査証跡表の SELECT 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

事象種別	監査対象事象	追加される監査情報
	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 SELECT 権限の取消し	監査証跡表のSELECT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

セション確立の試みにおいて接続に関する監査データが，日付と時刻を含めて格納される(**FTA_TAH_(EXT).1**(store))。

■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。

7.1.1.3. 監査証跡表(**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(**FAU_SAR.3**)。監査証跡表の監査データの検索，並べ替えは，監査証跡表の SELECT 権限をもつ，監査人および監査証跡参照者にのみ許可され(**FAU_SAR.1**)，それ以外の利用者には許可されない(**FAU_SAR.2**)。セション確立の試みにおいて格納された接続に関する監査データは，最終アクセス日時を含め，監査証跡表から読み出すことができる(**FTA_TAH_(EXT).1**(retrieve))。TOE は，監査証跡表の SELECT 権限の付与・取消しを実行可能とし(**FMT_SMF.1**)，監査人にのみ許可する(**FMT_MSA.1**)。
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，

監査証跡表の DELETE 権限をもつ，監査人に対してのみ許可される(**FAU_STG.1.1**)。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(**FAU_STG.1.2**)。

7.1.1.4. 監査証跡ファイル(**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メッセージログファイルに出力する(**FAU_STG.4**)。

7.1.2. アクセス制御(SF.ACC)

7.1.2.1. 機能概要

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。

7.1.2.2. 定義制御(**SF.ACC.DEF**)

TOE は，ユーザ表の定義（定義系 SQL の一つ）をスキーマ所有者に制限する(**FDP_ACC.1**)(**FDP_ACF.1**)。ユーザ表を定義したスキーマ所有者は，その表の所有者となる。

TOE は，ユーザ表の削除（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(**FDP_ACC.1**)(**FDP_ACF.1**)。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。

7.1.2.3. 表アクセス制御(**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。

TOE は，表 7.1-2 ，－ : その権限では許可されない

表 7.1-3 ，－ : その権限では許可されない

表 7.1-4 に示すように，操作系 SQL のアクセス制御を実施する(**FDP_ACC.1**)(**FDP_ACF.1**)。

表 7.1-2 : 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

－ ： その権限では許可されない

表 7.1-3 ： 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

－ ： その権限では許可されない

表 7.1-4 ： 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

－ ： その権限では許可されない

■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。

7.1.3. 識別・認証(SF.I&A)

7.1.3.1. 機能概要

TOE は，SQL インタフェースを使用し 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。

7.1.3.2. 接続(SF.I&A.CON)

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 SELECT 権限）を維持する(**FIA_ATD.1**)(**FMT_SMR.1**)。

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し，セションを確立する。それ以前に，TOE は，いかなる動作も許可することはない(**FIA_UAU.2**)(**FIA_UID.2**)。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，DB ユーザに属するセキュリティ属性を関連付ける(**FIA_USB.1**)。セション中の DB ユーザを変更した場合は，サーバプロセスへの関連付けも同時に変更する。

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。

7.1.3.3. 認証失敗(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(**FIA_AFL.1**)。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，認可識別子のロックを，ロック後，一定時間（ロック時間）経過後に自動的に解除する。また，コマンドによるロック解除を HiRDB 管理者のみ許可する。

7.1.4. 利用者・権限管理(SF.PRV)

7.1.4.1. 機能概要

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
- 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。

7.1.4.2. 利用者・権限管理(SF.PRV.CTL)

(1) 認可識別子およびパスワードの管理

TOE は，DB ユーザの登録と削除を実行可能とし(**FMT_SMF.1**)，監査人を除く DB ユーザを対象として DBA 権限保持者にのみ実行を許可する(**FMT_MSA.1**)。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，DB ユーザのパスワードの変更を実行可能とし(**FMT_SMF.1**)，DBA 権限保持者および DB ユーザ本人に許可する(**FMT_MTD.1(2)**)。

パスワードは，次の条件を満たすものが設定可能(**FIA_SOS.1**)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。

- 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
- 半角文字（英大文字，英小文字，数字）で構成

(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・取消しを実行可能とし(**FMT_SMF.1**)，DBA 権限保持者にのみ許可する(**FMT_MSA.1**)(**FMT_REV.1(1)**)。

(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・取消しを実行可能とし(**FMT_SMF.1**)，DBA 権限保持者にのみ許可する(**FMT_MSA.1**)(**FMT_REV.1(1)**)。

(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 7.1-5 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(**FMT_MSA_(EXT).3**)。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 7.1-5 ： 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・取消しを実行可能とし(**FMT_SMF.1**)，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(**FMT_MSA.1**)(**FMT_REV.1(2)**)。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)(**FMT_MSA_(EXT).3**)。

■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，解除を実行可能とし(**FMT_SMF.1**)，DBA 権限保持者に制限する(**FMT_MOF.1**)(**FMT_MTD.1(2)**)。

(6) ディクショナリ表の管理

TOE は，TSF データである管理情報をディクショナリで管理する。

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SELECT権限）を，ディクショナリ表に格納する。
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。
ディクショナリ表データは，アクセス性能向上のため，ディクショナリ情報用の各種バッファに複製される。TOE はディスクおよびバッファに存在するデータの一貫性を保証する(**FPT_TRC_(EXT).1**)。

■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。

8. 付録

8.1. 用語

本 ST で用いる用語を表 8.1-1 に示す。

表 8.1-1 :用語一覧

用語	説明
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。
SQL インタフェース	SQL を使用する TOE へのアクセス手段。TOE による識別・認証を必要とする。
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利用される。
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
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。
管理者 (administrator)	TOE の一部あるいは全てを管理する権限を特に与えられ, アクションが TSP に影響を及ぼすかもしれない利用者。管理者は、TSP の部分を越える能力を提供する特権

	を備えているかもしれない。
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。
許可利用者 (authorized user)	SFR に従って操作を実行することができる TOE 利用者。
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)
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。
利用者(user)	TOE の外部にあって TOE と対話することができる人間または IT エンティティ。
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）

8.2. 略語

本 ST で用いる略語を以下に示す。

CC	Common Criteria
PP	Protection Profile
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

8.3. 参照

本 ST で用いる参照ドキュメントを以下に示す。

U.S. GPP	U.S. Government Protection Profile for Database Management Systems Version 1.3

8.4. ガイダンス文書

HiRDB Version 9 セキュリティガイド (3020-6-459)が参照する各マニュアルを以下に示す。

- HiRDB Version 9 解説（UNIX(R)用）(3000-6-451-10)
- HiRDB Version 9 システム導入・設計ガイド（UNIX(R)用）(3000-6-452-10)
- HiRDB Version 9 システム定義（UNIX(R)用）(3000-6-453-10)
- HiRDB Version 9 システム運用ガイド（UNIX(R)用）(3000-6-454-10)

- HiRDB Version 9 コマンドリファレンス(UNIX(R)用) (3000-6-455-10)
- HiRDB Version 9 UAP 開発ガイド (3020-6-456-10)
- HiRDB Version 9 SQL リファレンス (3020-6-457-10)
- HiRDB Version 9 メッセージ (3020-6-458-10)