認 証 報 告 書

独立行政法人情報処理推進機構
理事長　藤江　一正

原紙押印済

評価対象

申請受付日（受付番号）	平成23年7月11日 (IT認証1361)
認証番号	C0351
認証申請者	株式会社日立製作所
TOEの名称	HiRDB Server Version 9 (Linux版)
TOEのバージョン	09-01
PP適合	なし
適合する保証パッケージ	EAL2及び追加の保証コンポーネントALC_FLR.2
開発者	株式会社日立製作所
評価機関の名称	みずほ情報総研株式会社 情報セキュリティ評価室

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。

平成24年5月21日

技術本部
セキュリティセンター 情報セキュリティ認証室
技術管理者　山里　拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 3.1 Release 3
② Common Methodology for Information Technology Security Evaluation Version 3.1 Release 3

評価結果：合格

「HiRDB Server Version 9 (Linux版)」は、独立行政法人情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約

この認証報告書は、株式会社日立製作所が開発した「HiRDB Server Version 9 (Linux 版) バージョン 09-01」(以下「本 TOE」という。) についてみずほ情報総研株式会社 情報セキュリティ評価室 (以下「評価機関」という。) が平成 24 年 5 月に完了した IT セキュリティ評価に対し、その内容の認証結果を申請者である株式会社日立製作所に報告するとともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット (以下「ST」という。) を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、政府の調達者及び一般消費者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL2 及び追加の保証コンポーネント ALC_FLR.2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE 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。

本 TOE はクライアントサーバ形態で使用される。サーバ側システムを HiRDB サーバ、クライアント側システムを HiRDB クライアントと呼ぶ。本 TOE は、HiRDB サーバにインストールされるソフトウェアであり、データベースにアクセスする機能を提供する。本 TOE に、HiRDB クライアントにインストールされるソフトウェアは含まれない。通常、DB ユーザは 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アクセスする。

本 TOE は、主なセキュリティ機能性として以下の機能性を持つ。

- DB ユーザを識別・認証してアクセス制御することで、データベースへの不正アクセスを防止する。

- 許可された DB ユーザによるデータベースへのアクセスを記録することで、データベースへのアクセスの説明責任を支援する。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する脅威及び前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本TOEは､以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

データベースへのアクセスが不正に行われ、データベース内のデータが不正に暴露されたり改ざんされたりすることを脅威とする。

この脅威に対抗するため､TOE は DB ユーザを識別認証し､その DB ユーザがアクセスしようとしているユーザ表に対して許可された操作のみができるようにする。また、不正操作が行われたことを示す監査データを監査人、監査証跡参照者が参照できるようにする。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

- 信頼できる許可管理者により､ガイダンス文書に従って管理が行われることを想定する。
- Parallel Server の構成の場合は､HiRDB サーバは 2 台であることを想定する。
- HiRDB サーバでは、OS と TOE のみが動作することを想定する。
- HiRDB サーバに対しては信頼できる者のみが物理的にアクセスできるような環境で運用することを想定する。Parallel Server の構成の場合に HiRDB サーバ同士の通信のためのネットワークも同様の環境に置かれることを想定する。
- HiRDB クライアントから TOE へのアクセスは、必ず正しい方法で作られた UAP または HiRDB SQL Executer Version 9 を介して行われ、その通信内容の改変や盗聴は防止される環境を想定する。これは、HiRDB クライアントが接続されるネットワークにおいても、ネットワークは保護され、不正なプログラムは動作させることはできないような管理が要求されることを意味する。

1.1.3 免責事項

本 TOE は、Parallel Server の構成の場合、HiRDB サーバが複数の構成で動作する。ただし、本評価の対象となったのは HiRDB サーバが 2 台の場合のみである。つまり、HiRDB サーバが 3 台以上の構成の場合は、本評価による保証の対象外である。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証申請手続等に関する規程」[2]、「IT セキュリティ評価機関承認申請手続等に関する規程」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 24 年 5 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、所見報告書、及び関連する評価証拠資料を検証し、本 TOE の評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC（[4][5][6]または[7][8][9]）及び CEM（[10][11]のいずれか）に照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

2 TOE識別

本 TOE は、以下のとおり識別される。

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

製品が評価･認証を受けた本 TOE であることを、消費者は以下の方法によって確認することができる。

TOE は CD-ROM で配付される。CD-ROM には部品番号が記載され、同梱される明細書に部品番号に対応する TOE の名称とバージョンが記載される。消費者は、明細書に記載される TOE の名称とバージョンにより、評価･認証を受けた本 TOE であることを確認できる。

インストールされたソフトウェアが評価･認証を受けたバージョンであるかどうかについては、DBA 権限保持者が HiRDB サーバのコンソールからバージョン確認のコマンドを利用することによっても確認できる。

3 セキュリティ方針

本章では、本 TOE が脅威に対抗するために採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は、DB ユーザからの SQL による指示に従い、データベースへのアクセスを実施する。

本 TOE は、DB ユーザを識別・認証し、DB ユーザがデータベース内のユーザ表に対して実施しようとしている操作が許可されているものかどうかを確認し、許可されている場合のみ操作ができるようにする。そうすることで、データベース内のユーザ表に関して、不正なデータの暴露や改ざんが行われることを防止する。

本 TOE は、セキュリティに関連する操作が行われた場合に、そのことを示す監査データを生成する。生成された監査データは、監査人、または監査証跡参照者が参照できるようにする。

本 TOE は、これらのセキュリティ機能を管理するための機能を提供し、そのような機能は信頼できる許可管理者のみが利用できるようにする。

なお、本 TOE は、以下の役割を想定する。以下の役割のうち、DBA 権限保持者とスキーマ所有者と監査人をまとめて「許可管理者」という。

(1) DB ユーザ

本 TOE にアクセスし、SQL を実行する権限を持つ。

(2) DBA 権限保持者

DB ユーザであり、TOE 全体の管理の権限(監査に関するものは除く)を持つ。

(3) スキーマ所有者

DB ユーザであり、スキーマに対して割り当てられる所有者である。そのスキーマの管理権限を持つ。

(4) 監査人

DB ユーザであり、監査データを読み出す権限を持ち、さらに監査に関する設定や管理の権限も持つ。

(5) 監査証跡参照者

DB ユーザであり、監査データを読み出す権限を持つ。監査に関する設定や管理の権限は持たない。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、表 3-1 に示す脅威を想定し、これに対抗する機能を備える。

後述する前提条件により、HiRDB サーバ、HiRDB クライアント、これらを接続するネットワークは十分に管理された環境に置かれる。そのため、悪意を持つ者の想定は、例えば HiRDB クライアント上の UAP をリモートから利用して TOE にアクセスする者となる。

表3-1　想定する脅威

識別子	脅威
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to user data for which they are not authorized according to the TOE security policy. (注) TOE security policyは、ユーザ表ごとにどのDBユーザのどの操作が許可されるかを定めることができるということを表す。
T.TSF_COMPROMISE	A malicious user or process may cause configuration data to be inappropriately accessed (viewed, modified or deleted).
T.UNIDENTIFIED_ACTIONS	Failure of the authorized administrator to identify and act upon unauthorized actions may occur.

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

⑴ 脅威「T.MASQUERADE」への対抗

本 TOE は、本 TOE を利用しようとする者を識別・認証することで、異なる DB ユーザになりすまして利用することを防止する。

⑵ 脅威「T.UNAUTHORIZED_ACCESS」への対抗

識別・認証された DB ユーザがユーザ表に対して操作を実施しようとするとき、本 TOE は、DB ユーザの識別情報と、ユーザ表ごとに設定できるアクセス許可の情報(表に対して、どの DB ユーザのどの操作が許可されるか)をもとに、DB ユーザがユーザ表に対して実施しようとする操作が許可されているかどうかを判定する。その結果、許可されている場合にのみ操作を許可する。

⑶ 脅威「T.TSF_COMPROMISE」への対抗

識別・認証された DB ユーザがセキュリティに関係するデータに対して操作を実施しようとするとき、本 TOE は、DB ユーザの役割をもとに、操作が許可されているかどうかを判定する。その結果、許可されている場合にのみ操作を許可する。

⑷ 脅威「T.UNIDENTIFIED_ACTIONS」への対抗

本 TOE は、セキュリティに関連する操作が行われたことを示す監査データを生成する。さらに、監査人及び監査証跡参照者に対し監査データを参照する機能を提供し、記録された監査データに対してはいかなる変更も許さず、監査人以外が削除できないようにする。それによって、不正な操作が行われた場合に検出できるようにする。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 TOE の利用に当たって要求される組織のセキュリティ方針を表 3-2 に示す。

表3-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
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.

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表 3-2 に示す組織のセキュリティ方針を満たす機能を具備する。

⑴ 組織のセキュリティ方針「P.ACCOUNTABILITY」への対応

本 TOE は、P.ACCOUNTABILITY で具体的に特定された監査事象を記録する。さらに、記録された監査データに対してはいかなる変更も許さず、監査人以外が削除できないようにする。これらにより、P.ACCOUNTABILITY を満たす。

⑵ 組織のセキュリティ方針「P.ROLES」への対応

本 TOE は、DB ユーザと役割の関連付けをする機能を提供する。一部(例えば許可管理者ではない DB ユーザであっても本人には許可されるパスワードの変更)を除く管理機能の利用は、許可管理者のみに許可することにより、P.ROLES を満たす。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 に示す。これらの前提条件が満たされない場合、本 TOE のセキュリティ機能が有効に動作することは保証されない。

表4-1 前提条件

識別子	前提条件
A.NO_EVIL	Administrators are non-hostile, appropriately trained, and follow all administrator guidance. (注) 環境がこの前提条件を満たすかどうかの判断のために、以下の事項に注意する必要がある。 ● TOEと通信できるのはHiRDB SQL Executer Version 9 とUAPのみとなるように、HiRDBクライアントおよびネットワークの管理が必要である。 ● HiRDBクライアントとTOEの通信に対して盗聴や改ざんが行われないように、HiRDBクライアントおよびネットワークの管理が必要である。 ● コマンドインタフェースからコマンドを使用する際には、ガイダンスに記載されている使用方法に従う必要がある。
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. (注) 具体的には、TOEの動作に必要なIT環境(つまり、OSのみ)が許容される。

識別子	前提条件
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。
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。 (注) UAPがTOEにアクセスする際には必ずHiRDB/Run Time Version 9を介してアクセスするように、UAPが作られなければならないことを意味する。

4.2 運用環境と構成

本 TOE の構成は、Single Server (図 4-1)と Parallel Server (図 4-2) の 2 通りある。

本 TOE は、信頼できる者のみが物理的にアクセス可能な環境に置かれた HiRDB サーバに導入される。Parallel Server の構成の場合に HiRDB サーバ同士の通信のためのネットワークも同様の環境に置かれる。

本 TOE は、通信内容の改変や盗聴が防止されるように管理されたネットワークを介して接続されたクライアントから利用される。クライアントも、不正なプログラムは動作させることはできないような管理の下で利用される。

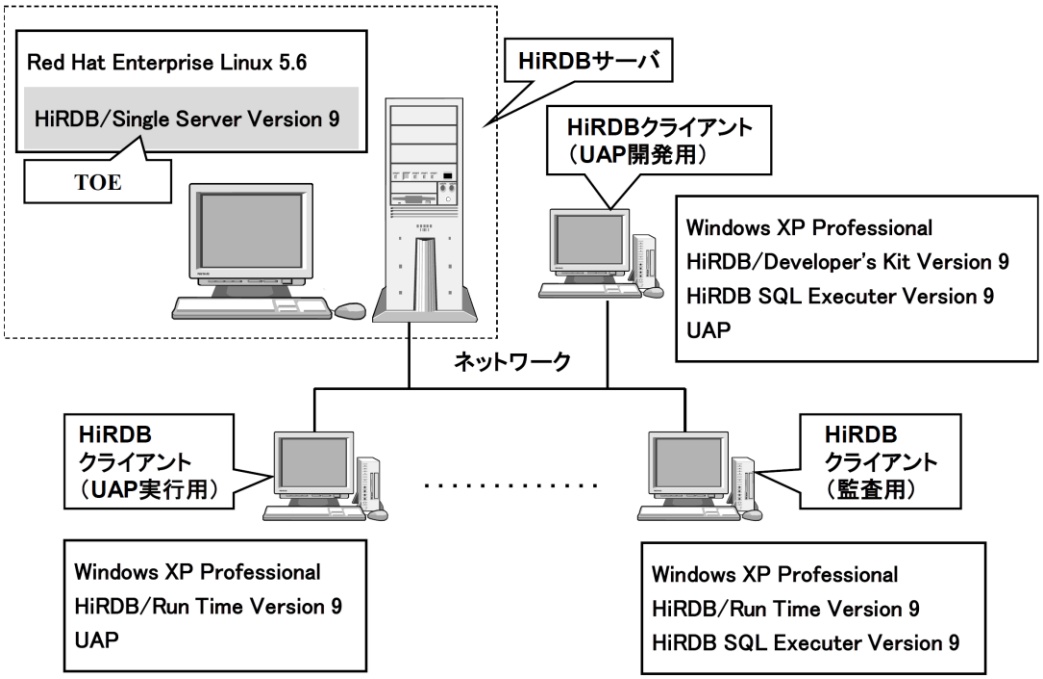

図 4-1 TOE の運用環境(Single Server の構成)

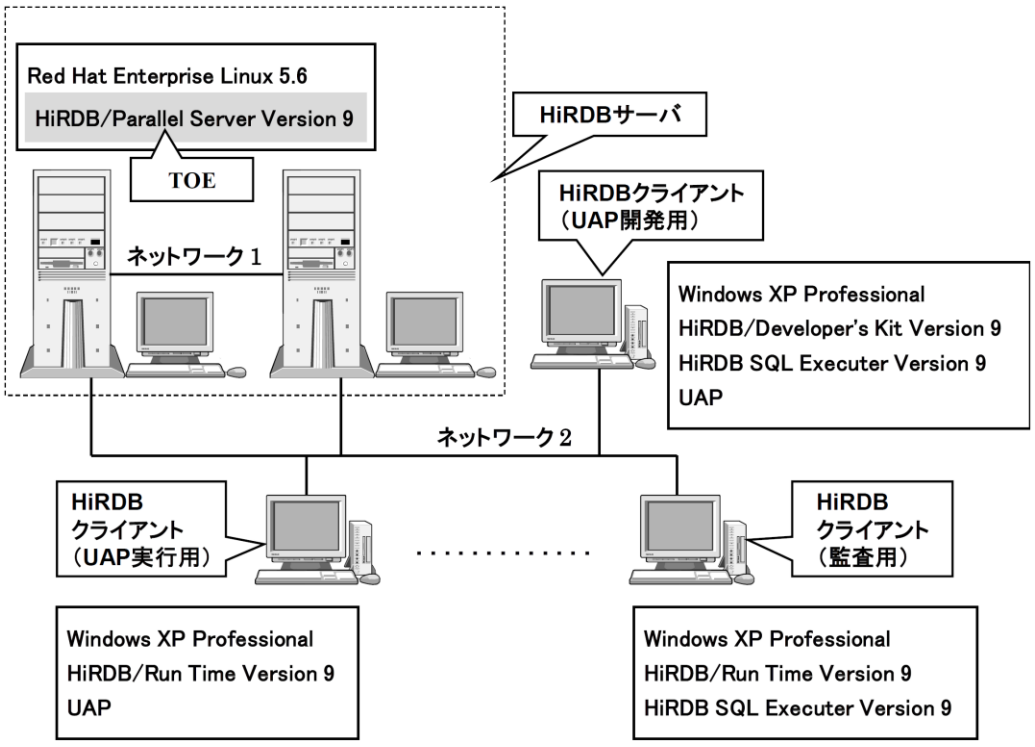

図 4-2 TOE の運用環境(Parallel Server の構成)

運用環境を構成する要素について以下に示す。

(1) HiRDB サーバ

OS は Red Hat Enterprise Linux 5.6 であり、ハードウェアはこの OS が動作する BladeSymphony、HA8000 シリーズ等の AT 互換機である。

HiRDB サーバに TOE がインストールされる。

Single Server の構成では HiRDB サーバは 1 台であり、Parallel Server の構成では HiRDB サーバは 2 台である。

(2) ネットワーク

HiRDB サーバと HiRDB クライアントは、IPv4 のネットワークで接続される。

Parallel Server の構成では、HiRDB サーバ同士を接続する IPv4 のネットワーク(図 4-2 のネットワーク 1)も必要となる。HiRDB サーバ同士を接続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ネットワーク(図 4-2 のネットワーク 2)とは異なるネットワークである。

(3) HiRDB クライアント

OS は Windows XP Professional であり、ハードウェアはこの OS が動作する BladeSymphony、HA8000 シリーズ等の AT 互換機である。

HiRDB クライアントに以下のソフトウェアがインストールされる。

- HiRDB / Run Time Version 9 09-01

  株式会社日立製作所のソフトウェア製品である。

  UAP や HiRDB SQL Executer Version 9 が TOE にアクセスするために必要となるソフトウェアであり、全ての HiRDB クライアントで利用される。

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

  株式会社日立製作所のソフトウェア製品である。

  UAP の開発のため、UAP 開発用の HiRDB クライアントで利用される。

- HiRDB SQL Executer Version 9

  株式会社日立製作所のソフトウェア製品である。

TOE と対話形式で、SQL の発行とその結果の確認ができるソフトウェアであり、UAP 開発用と監査用の HiRDB クライアントで利用される。

- UAP

  TOE の機能を利用するアプリケーションプログラムで、UAP 管理者によって作成される。

なお、本構成に示されている TOE 以外のソフトウェア及びハードウェアの信頼性は本評価の範囲ではない（十分に信頼できるものとする）。

4.3 運用環境におけるTOE範囲

TOE 範囲に関して、特に注意すべき事項はない。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成（サブシステム）を説明する。

5.1 TOE境界とコンポーネント構成

TOE の主な構成(Parallel Server の構成の場合)を図 5-1 に示す。HiRDB サーバのハードウェアと OS(Red Hat Enterprise Linux 5.6)、HiRDB クライアントのハードウェアとソフトウェアは TOE の範囲ではない。

1 台の HiRDB サーバで処理が完結しない場合(処理に必要なデータがもう片方の HiRDB サーバにある場合、もう片方の HiRDB サーバとデータの整合性をとる必要がある場合)は、ネットワーク 1 を介してもう片方の HiRDB サーバとの連携が行われる。

Single Server の構成の場合には、HiRDB サーバは 1 台であり、図 5-1 のネットワーク 1 に該当するネットワークはない。Single Server の構成の場合には全ての処理が 1 台の HiRDB サーバで完結する。

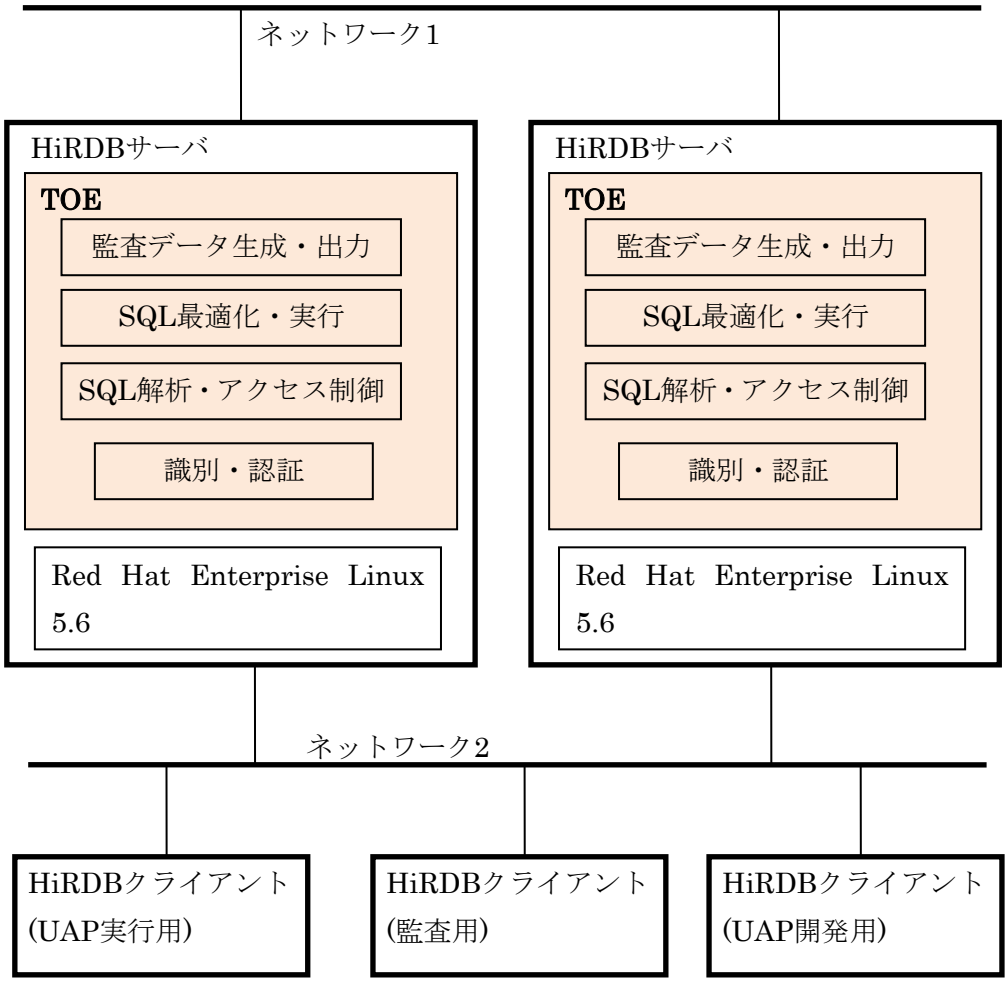

図 5-1　TOE 境界と構成

TOE を構成する主なコンポーネントについて説明する。

(1) 識別・認証のコンポーネント

HiRDB クライアントからの接続要求を受け、利用者の識別・認証を行う。識別・認証が成功すると、接続が確立された状態となる。接続が確立された状態であれば、HiRDB クライアントから SQL を受け取り、SQL 解析・アクセス制御のコンポーネントへ渡す。

(2) SQL 解析・アクセス制御のコンポーネント

SQL を受け取り、構文の解析を行う。DB ユーザの識別情報に基づいて、SQL により実施しようとしている操作が許可されている操作かどうかを判定する。許可されていると判定した場合には SQL 最適化・実行のコンポーネントを使って SQL を実行する。

(3) SQL 最適化・実行のコンポーネント

SQL から効率的な内部処理実行手順を生成し、実行する。

(4) 監査データ生成・出力のコンポーネント

上記の各コンポーネントで監査対象事象が発生した場合、監査データが監査データ生成・出力のコンポーネントに渡される。監査データ生成・出力のコンポーネントによって監査データの出力が行われる。

5.2 IT環境

本 TOE は、Red Hat Enterprise Linux 5.6 がインストールされた AT 互換機で動作し、HiRDB クライアントからネットワークを介して利用される。

HiRDB クライアント(UAP 実行用)からは、消費者の想定する業務等のために、ネットワークを介して TOE が利用される。

HiRDB クライアント(監査用)からは、ネットワークを介して TOE の監査機能が利用される。

HiRDB クライアント(UAP 開発用)では UAP の開発が行われ、テストのためにネットワークを介して TOE が利用される。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

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

7 評価機関による評価実施及び結果

7.1 評価方法

評価は、CC パート 3 の保証要件について、CEM に規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告された。評価報告書では、本TOEの概要と、CEMのワークユニットごとの評価内容及び判断結果を説明する。

7.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成 23 年 7 月に始まり、平成 24 年 5 月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成 24 年 1 月に開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成 24 年 1 月に開発者サイトで開発者のテスト環境を使用し、開発者テストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。

これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

7.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(1) 開発者テスト環境

開発者が実施したテストの構成を図 7-1 と図 7-2 に示す。

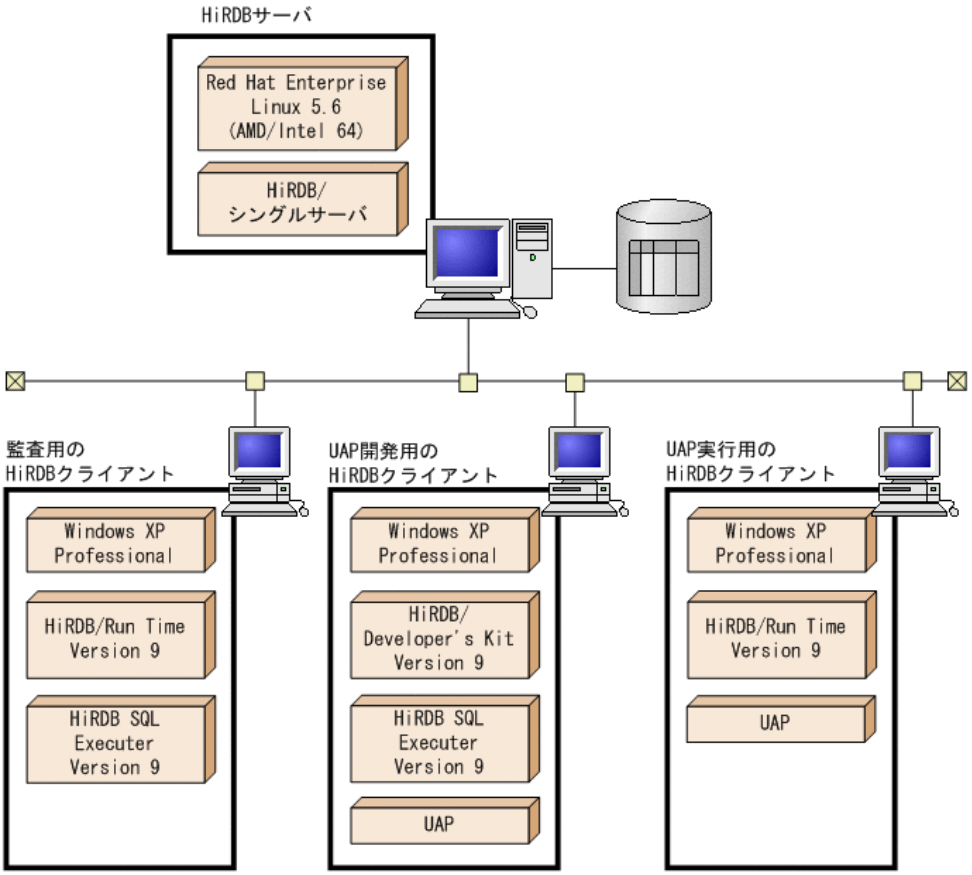

図 7-1　開発者テストの構成図 (Single Server の構成)

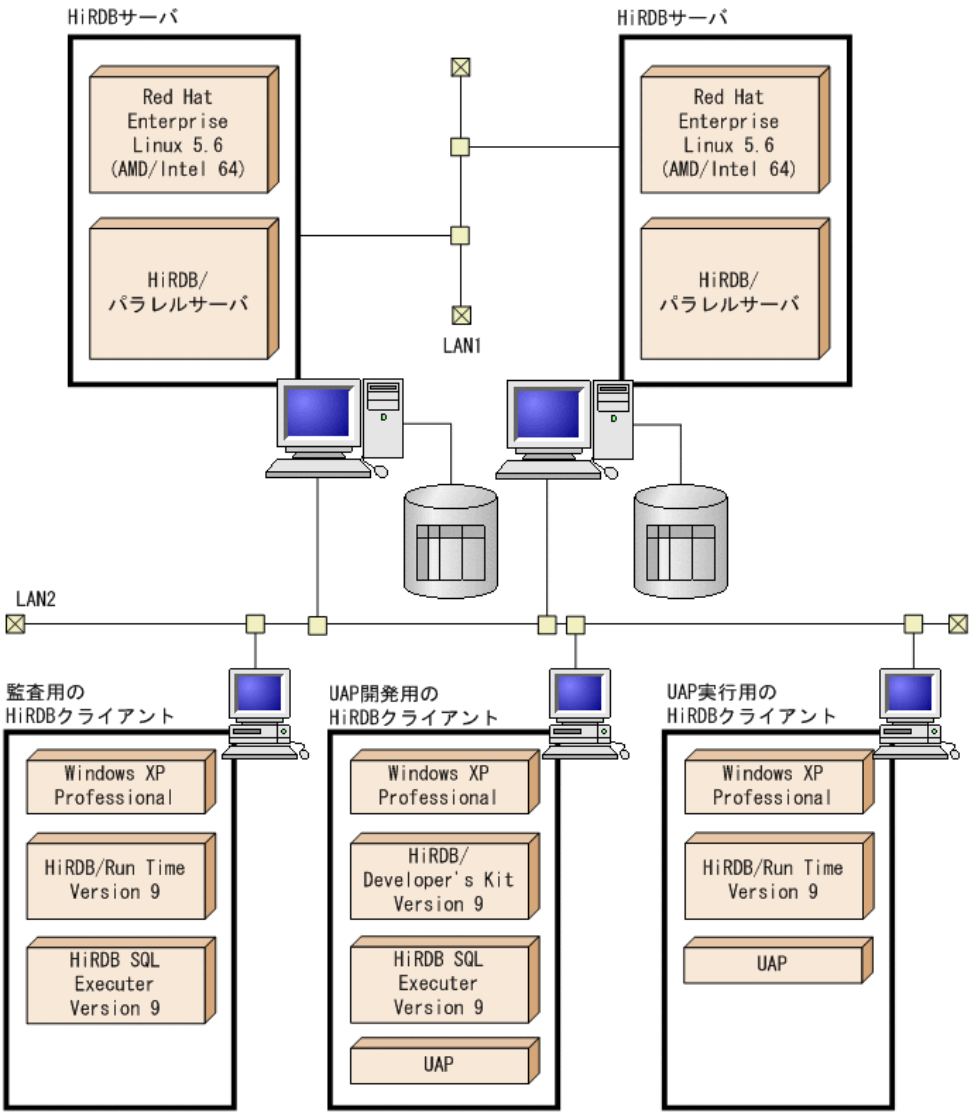

図 7-2　開発者テストの構成図 (Parallel Server の構成)

開発者テストが対象とした TOE は以下のとおりである。本 TOE には、Single Server の構成と Parallel Server の構成が存在し、双方がテストの対象となった。

表7-1　TOEの構成 (Single Server の構成)

図7-1の表記	意味
HiRDB / シングルサーバ	HiRDB Server Version 9 バージョン09-01 の、Single Server の構成。

表7-2　TOEの構成 (Parallel Server の構成)

図7-2の表記	意味
HiRDB / パラレルサーバ	HiRDB Server Version 9 バージョン09-01 の、Parallel Server の構成。

開発者テストの構成における TOE 以外の要素は以下のとおりである。

表7-3　TOEの構成 (Single Server, Parallel Server の構成共通)

図7-1の表記	意味
Red Hat Enterprise Linux 5.6 (AMD/Intel 64)	HiRDBサーバのOS。 TOEの動作環境となる。
Windows XP Professional	クライアントのOS。
HiRDB / Run Time Version 9	UAP やHiRDB SQL Executer Version 9がTOEにアクセスするために必要となるソフトウェア。
HiRDB SQL Executer Version 9	TOEと対話形式で、SQLの発行とその結果の確認ができるソフトウェア。
HiRDB Developer's Kit Version 9	UAPの開発環境。(テスト実施時には使われない)
UAP	テスト用に作成されたUAP。

開発者テストは本 ST において識別されている TOE 構成と同一の TOE テスト環境で実施されている。

(2) 開発者テスト概説

開発者テストの概説は以下のとおりである。

a) テスト概要

開発者テストの概要は、以下のとおりである。

＜開発者テスト手法＞

SQL インタフェースに対しては、SQL 文を送信して結果を確認するためのツール(図 7-1 と図 7-2 の UAP)が使用された。

コマンドインタフェースに対しては、HiRDB サーバのコンソールからコマンドを入力して結果の観察が行われた。

SQL インタフェースやコマンドインタフェースからはテストが困難なもの(例えば、バイパス経路が存在しないことの確認)に対しては、ソースコードのレビューにより代替された。

＜開発者テストツール＞

開発者テストにおいては、テストツールとして、テスト用 UAP が使用された。UAP 管理者が作成する UAP による TOE の利用方法をカバーするように設計されており、テストツールと TOE の通信内容の妥当性が開発者により確認されている。

＜開発者テストの実施内容＞

SQL インタフェースに対しては、テスト用 UAP を介して、手動またはスクリプトによって TOE に対して SQL 文が送信された。テスト用 UAP によって TOE の応答を観察し、期待される結果との照合が行われた。

コマンドインタフェースに対しては、HiRDB サーバのコンソールからコマンドを入力し、応答を観察し、期待される結果との照合が行われた。

ソースコードのレビューに関しては、レビューの方法(例えば、特定の処理が行われる部分で必ず特定の関数が使われるなど)が明示され、それに従ったレビューが行われた。

b) **開発者テストの実施範囲**

開発者テストは開発者によって2247項目実施された。カバレージ分析によって、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースがテストされたかどうかが確認され、テストが十分でない部分は独立テストで補われた。

c) **結果**

評価者は、開発者テストの実施方法、実施項目の正当性を確認し、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.3.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト（以下「独立テスト」という。）を実施した。評価者が実施した独立テストを以下に説明する。

(1) **独立テスト環境**

評価者が実施した独立テストの構成は、開発者テストと同じ構成(図 7-1、図 7-2)である。TOE および TOE 以外の要素も、開発者テストと同じもの(表 7-1、表 7-2、表 7-3)が使われた。

また、ここで用いられたテスト用 UAP は開発者のものを利用しているが、テスト用 UAP の仕様確認及び動作試験と校正は評価者によって実施されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が､開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

独立テストは、セキュリティ機能のふるまいに関係するSQLインタフェース、コマンドインタフェースに対して、以下のように考案された。

＜独立テストの観点＞

①開発者テストのサンプリングの観点で、開発者が実施したテストから、すべてのセキュリティ機能が含まれ、かつインタフェースの種別とテスト手法がすべて含まれるようにテスト項目を抽出し、開発者と同じテストを実施する。

② 開発者テストの不十分な点を補う。

③ 開発者テストとは異なる状態やパラメタで同様のテストを実施し、テストの厳密さを補う。

④ 開発者テストで結果の観察が不十分な点を補う。

b) 独立テスト概要

評価者が実施した独立テストの概要は以下のとおりである。

＜独立テスト手法＞

開発者テストと同じ手法で実施された。

＜独立テストツール＞

開発者テストと同じツールが使用された。

＜独立テストの実施内容＞

独立テストは、サンプリング 520 項目と評価者によって考案された 15 項目が実施された。

独立テストの観点とそれに対応したテスト内容を表 7-4 に示す。

表7-4 実施した独立テスト

観点	テスト概要
①	開発者が実施したテスト項目から、テストの観点に基づいてテスト項目を抽出して開発者と同じテストを実施し、開発者と同じ結果が得られることを確認する。実施したテストは2247項目中、520項目である。
②	パスワードとして使える文字種が仕様通りであるかどうかについて、開発者テストを補足する。
	認証に関するパラメタについて、設定不可能となる境界値や誤動作の懸念される値(負数など)の設定を試みて、正しく拒否されることを確認する。 テストは2項目考案された。
③	以下の場合において、表定義が正しく拒否されることを確認する。 ● 別ユーザのユーザ表定義を試みる。この試みは、開発者テストとは異なる役割のユーザで行う。 ● 別ユーザ(開発者テストでは同一ユーザ)のすでに存在するユーザ表と同じ識別のユーザ表の定義を試みる。
	アクセス権限の付与が正しくできることを確認する。 この試みは、開発者テストとは異なる役割のユーザで行う。
	不正にDBA権限付与を試み、拒否されることを確認する。この試みは、開発者テストとは異なる役割のユーザで行う。
	不正にスキーマ定義を試み、拒否されることを確認する。この試みは、開発者テストとは異なる役割のユーザで行う。
	一人のDBユーザのアクセス権限を複数同時に剥奪した場合、正しく剥奪されることを確認する。
	監査データの生成について、以下のように開発者テストの補足をする。 ● 開発者テストでは監査データの生成が確認されていないような事象に対するテストを実施する。 ● 事象の成功/不成功の監査データを生成するかどうかの設定に関するテストを実施する。 テストは2項目考案された。
	監査証跡表に対する不正なアクセス権限の付与が、一人のDBユーザに複数の権限を同時に付与しようとした場合にも拒否されることを確認する。
	アカウントロックが以下の場合でも正しく動作することを確認する。 ● 別のクライアントからの試行も合わせて、認証の不成功回数が閾値を超えた場合。 ● 異なるSQL文による試行も合わせて、認証の不成功回数が閾値を超えた場合。

観点	テスト概要
③	以下の場合でも正しく認証が失敗することを確認する。 ● 正しいパスワードに1文字追加した文字列をパスワードとして入力した場合。
	SQLインタフェースからの実行が拒否されるべき機能について、開発者テストとは異なるパラメタで確認する。
④	監査証跡の上書きが発生した場合に記録される監査記録の内容が適切であることを確認する。
	SQLの実行の際に識別認証されているかどうかのチェックがTOEによって行われているかどうかについて、開発者テストで観察されているかどうかに懸念があった。(HiRDBクライアント側で同様のチェックが動作するため) そのため、識別認証されているかどうかのチェックがTOEで実装されていることを、ソースコードのレビューで確認する。
	DBユーザからTOEへの接続数が増えていく際に、HiRDBサーバ上に待機しているプロセスの個数を超えると新たにプロセスが作られるというふるまいがある。そのふるまいが開発者テストで観察されているかどうかに懸念があった。そのため、新たにプロセスが作られる前後のプロセスの状況を観察し、正しくプロセスが作られることを確認する。

c) **結果**

評価者が実施したすべての独立テストは正しく完了し、評価者は TOE のふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) **懸念される脆弱性**

評価者は、提供された証拠資料や公知の情報より、潜在的な脆弱性を探索し、侵入テストを必要とする以下の脆弱性を識別した。

① 公知の脆弱性が、TOEの悪用に結びつくことが懸念される。(なお、公知の情報の探索から得られた潜在的な脆弱性に対しては、本案件には該当しない、または想定の環境での悪用手段がないことが判断された。そのため、さらなる探索が必要かどうかの観点でのテストのみ行われた。)

② セキュリティ機能のバイパスの懸念がないかどうかの探索が各証拠資料に対して行われた。その結果、侵入テストが必要となる以下のような懸念が検出された。

②-1. パスワードの文字数の上限があるという仕様から、それを超える入力に対する誤動作(例えば、認証失敗の回数のカウントをバイパスできること)が懸念される。

③ セキュリティ機能の改ざんの懸念がないかどうかの探索が各証拠資料に対して行われた。その結果、侵入テストが必要となる以下のような懸念が検出された。

③-1. 仕様上はユーザ表の大きさの制限はあるものの、開発者の想定を超えて大きなユーザ表が定義されようとした場合に予期しない動作をすることが懸念される。
③-2. 一般的に、アプリケーションの動作中の電源断が予期しない影響を引き起こすことがあり、特にスタートアップ、クローズダウンの際の懸念が大きい。
③-3. HDD上の表の領域やメモリを資源として扱う仕様から、これらの資源が枯渇した場合に予期しない動作をすることが懸念される。
③-4. TOEの仕様上、同じユーザ表に対する競合する操作が考えられる。同じユーザ表に対する異なる権限の操作の競合については動作の検証が十分でなく、予期しない動作をすることが懸念される。
③-5. 複数のプロセスが連携して動作するという仕様から、一部のプロセスが欠けた場合に予期しない動作をすることが懸念される。

上記以外に、パスワードなどのメカニズムが打ち負かされる懸念、盗聴によるセキュリティ侵害の懸念、安全でない状態が気づかれずに使われる懸念についての探索が行われた。これらの探索からは、侵入テストを要する懸念は見つからなかった。

b) 侵入テストの概要

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

評価者が実施した侵入テストの構成は、開発者テストと同じ構成(図 7-1、図 7-2)である。TOE および TOE 以外の要素も、開発者テストと同じもの(表 7-1、表 7-2、表 7-3)が使われた。

加えて、検査用の PC が別途用意され、以下のツールが使用された。

- Nessus 4.4.1
  ネットワーク上のサービスポートでの既知の脆弱性についてその潜在の可能性を検出するツールである。
  脆弱性データベースは 2012 年 1 月 20 日現在最新のものが使用された。

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7-5 に示す。

表7-5　侵入テスト概要

脆弱性	テスト概要
①	NessusをHiRDBサーバに対して実施し、悪用され得るポートやさらに分析が必要なポートがないかどうかを確認した。
②-1	パスワードの最大文字数を超える入力が可能ではないことを、ソースコードのレビューで確認した。
③-1	列の個数の制限を超えるユーザ表の作成を試み、予期しないふるまいをすることがないかどうかを確認した。
③-2	スタートアップ、クローズダウン中の電源断により、予期しないふるまいをすることがないかどうかを確認した。
③-3	ユーザ表の領域やメモリが枯渇した状態とし、予期しないふるまいをすることがないかどうかを確認した。
③-4	異なる権限で同一のユーザ表に対して競合する操作を実施することで、予期しないふるまいをすることがないかどうかを確認した。
③-5	HiRDB上のTOEのプロセスを一部停止させ、予期しないふるまいをすることがないかどうかを確認した。

c) 結果

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

7.4 評価構成について

Parallel Server の構成の場合、評価構成は HiRDB サーバが 2 台の場合である。

7.5 評価結果

評価者は、評価報告書をもって本 TOE が CEM のワークユニットすべてを満たしていると判断した。

評価では以下について確認された。

- PP適合：なし
- セキュリティ機能要件：　コモンクライテリア　パート2　拡張
- セキュリティ保証要件：　コモンクライテリア　パート3　適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

- EAL2パッケージのすべての保証コンポーネント
- 追加の保証コンポーネントALC_FLR.2

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.6 評価者コメント/勧告

評価者勧告は特にない。

8 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。

④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。

⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。認証機関は、本 ST 及び評価報告書において、認証レビューで指摘された問題点が解決されていることを確認し、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本 TOE が CC パート 3 の EAL2 及び保証コンポーネント ALC_FLR.2 に対する保証要件を満たすものと判断する。

8.2 注意事項

本 TOE を Parallel Server の構成で利用する場合には、HiRDB サーバが 3 台以上の構成は本評価による保証の対象外であることに注意すべきである。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

HiRDB セキュリティターゲット バージョン 5.22　2012 年 3 月 19 日　株式会社日立製作所

11 用語

本報告書で使用された CC に関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation（セキュリティ評価基準）
CEM	Common Methodology for Information Technology Security Evaluation（セキュリティ評価方法）
EAL	Evaluation Assurance Level（評価保証レベル）
PP	Protection Profile（プロテクションプロファイル）
ST	Security Target（セキュリティターゲット）
TOE	Target of Evaluation（評価対象）
TSF	TOE Security Functionality（TOEセキュリティ機能）

本報告書で使用された TOE に関する略語を以下に示す。

DBA	DataBase Administrator
UAP	User Application Program
U.S.GPP	U.S. Government Protection Profile for Database Management Systems Version 1.3

本報告書で使用された用語の定義を以下に示す。

DBA権限保持者	DBユーザであり、TOE全体の管理の権限(監査に関するものは除く)を持つ。
DBユーザ	本TOEにアクセスし、SQLを実行する権限を持つ。
SQL インタフェース	ネットワークを介してTOEに接続し、SQLを実行するためのインタフェース。
UAP	TOEの機能を利用するアプリケーションプログラムで、UAP管理者によって作成される。
UAP管理者	UAPの開発と保守に責任を有する者。
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
監査証跡参照者	DBユーザであり、監査データを読み出す権限を持つ。監査に関する設定や管理の権限は持たない。

監査人	DBユーザであり、監査データを読み出す権限を持ち、さらに監査に関する設定や管理の権限も持つ。
許可管理者	DBA権限保持者、スキーマ所有者、監査人の総称。
コマンドインタフェース	HiRDBサーバのコンソールからTOEの管理をするためのインタフェース。
スキーマ所有者	DBユーザであり、スキーマに対して割り当てられる所有者である。そのスキーマの管理権限を持つ。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成24年3月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成24年3月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成24年3月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-001, (平成21年12月, 翻訳第1.0版)

[8] 情報技術セキュリティ評価のためのコモンクライテリア パート2: セキュリティ機能コンポーネント, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-002, (平成21年12月, 翻訳第1.0版)

[9] 情報技術セキュリティ評価のためのコモンクライテリア パート3: セキュリティ保証コンポーネント, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] 情報技術セキュリティ評価のための共通方法: 評価方法, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] HiRDB セキュリティターゲット バージョン 5.22　2012年3月19日　株式会社日立製作所

[13] HiRDB Server Version 9 評価報告書 第2版, 2012年5月10日, みずほ情報総研株式会社 情報セキュリティ評価室