認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙押印済

評価対象

申請受付日（受付番号）	平成17年9月15日 (IT認証5056)
認証番号	C0171
認証申請者	株式会社 日立製作所
TOEの名称	HiRDB / Single Server Version 7
TOEのバージョン	07-03
PP適合	なし
適合する保証パッケージ	EAL4及び追加の保証コンポーネントALC_FLR.1
開発者	株式会社 日立製作所
評価機関の名称	株式会社電子商取引安全技術研究所　評価センター

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20年6月30日

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　鈴木　秀二

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 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「HiRDB / Single Server Version 7 07-03」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

1.1 はじめに

この認証報告書は、「HiRDB / Single Server Version 7 07-03」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所 評価センター（以下「評価機関」という。）が行った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ものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称： HiRDB / Single Server Version 7
バージョン： 07-03
開発者： 株式会社 日立製作所

1.2.2 製品概要

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

本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

1.2.3 TOEの範囲と動作概要

1.2.3.1 評価構成と TOE の範囲

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

図1-1 にクライアントーサーバ（C/S）型のシステム構成を示す。TOEの範囲は、図1-1におけるHiRDB / Single Server Version 7であり、それ以外の構成要素はTOEではない。

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

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

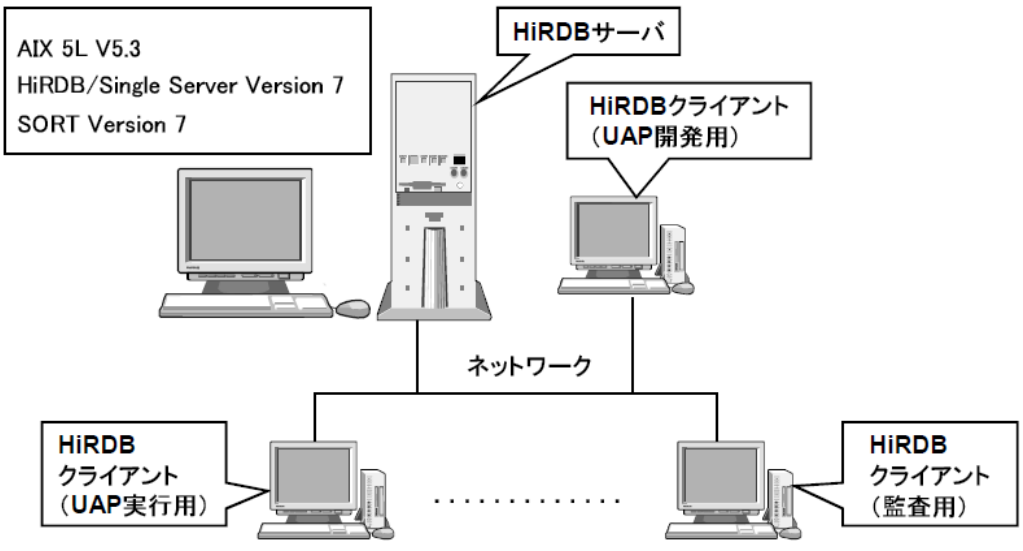


図1-1　クライアントーサーバ（C/S）型のシステム構成

1.2.3.2　評価構成の説明と動作概要

(1) 図1-1に示すシステムを構成する各端末の説明

【 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クライアントは、その用途により、UAP開発用、UAP実行用、監査用に分類される。

HiRDBクライアントは、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。HiRDBサーバによる実行結果をHiRDBクライアントは受信する。

(2) HiRDBサーバで使用されるソフトウェアの説明

＜ AIX 5L V5.3 ＞

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

＜ HiRDB / Single Server Version 7 ＞

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

＜ SORT Version 7 ＞

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

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

1.2.3.3 HiRDB サーバの OS に関連する役割

以下は、HiRDBサーバのOSで維持される利用者役割である。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)。

【 スーパユーザ 】

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

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

スーパユーザは、HiRDB管理者やDBユーザを兼任しても構わない。

【 HiRDB管理者 】

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

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

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

HiRDB管理者は、DBユーザとしてはDBA権限保持者を兼任する。

【 一般OSユーザ 】

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

TOEで維持される利用者役割のうち、スキーマ所有者、HiRDB管理者以外のDBA権限保持者、および監査人がTOEのコマンドを実行する場合、HiRDBサーバのOSにログインする必要がある。したがって、一般OSユーザのOSアカウン

トは、スキーマ所有者、HiRDB管理者以外のDBA権限保持者、および監査人に対して与えられるものであり、その他の者に対して与えられるものではない。

1.2.3.4 TOE に関連する役割

以下は、TOEで維持される利用者役割である。

【 DB ユーザ 】

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

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

表1-1　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。

＜ DBユーザに関する補足 ＞

DBユーザであるかどうかは、TOEにアクセス可能な認可識別子を持つかどうかで定義される。HiRDBクライアントを利用する者がDBユーザであるとは限らない。

例えば、UAPがTOEにアクセス可能な認可識別子とパスワードを保持していて、UAPを利用する者はその認可識別子とパスワードを知らなくてもUAPを通してTOEの機能を利用できる場合、その「UAPを利用する者」はDBユーザではない。その場合、そのパスワードが知られないように管理されなければならず、その管理をする者がDBユーザになる。

以下に示す役割はすべてDBユーザをも兼ねている。TOEの利用者はすべてDBユーザであり、以下に示す役割を兼ねていないDBユーザを「一般DBユーザ」と呼ぶ。

【 スキーマ所有者 】

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

スキーマ所有者が実施する主な業務を以下に示す。

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

【 DBA権限保持者 】

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

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

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

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

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

【 監査人 】

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

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

監査人は、必要であれば（大量に生成されるかもしれない監査データのチェッ

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

【 監査証跡参照者 】

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

1.2.3.5 UAP に関連する利用者役割

UAP に関連する各利用者役割について、以下に説明する。

【 UAP 管理者 】

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

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

【 UAP 利用者 】

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

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

1.2.3.6 役割に関するその他の定義

「許可された管理者」は、以下のいずれかの役割を持つ者と定義される。

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

- UAP管理者

1.2.4 TOEの機能

1.2.4.1 機能の説明

本TOEは、「1.2.3.2 評価構成の説明と動作概要」の【 HiRDBサーバ 】の項目で示した以下の機能を実現する。

(1) HiRDBサーバのコンソールから投入されたTOEのコマンドの処理。

(2) 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。

上記(1)は許可された管理者だけが使用することが想定された、TOEの運用管理のための機能である。本認証報告書での具体的な説明は割愛する。

上記(2)が本TOEの消費者が期待する機能である。本TOEは、「JISデータベース言語SQL X3005-1995」をエントリレベルでサポートしている。この機能について、データベースの構成(ユーザ表、ディクショナリ表、および監査データ)に基づいて以下に示す。

【 ユーザ表 】

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

{ ユーザ実表 }

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

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

- 行検索
- 行挿入
- 行削除
- 行更新

また、ユーザ実表を表定義変更することにより、ユーザ表定義情報の一部が変更される。

{ 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1-2に示す。

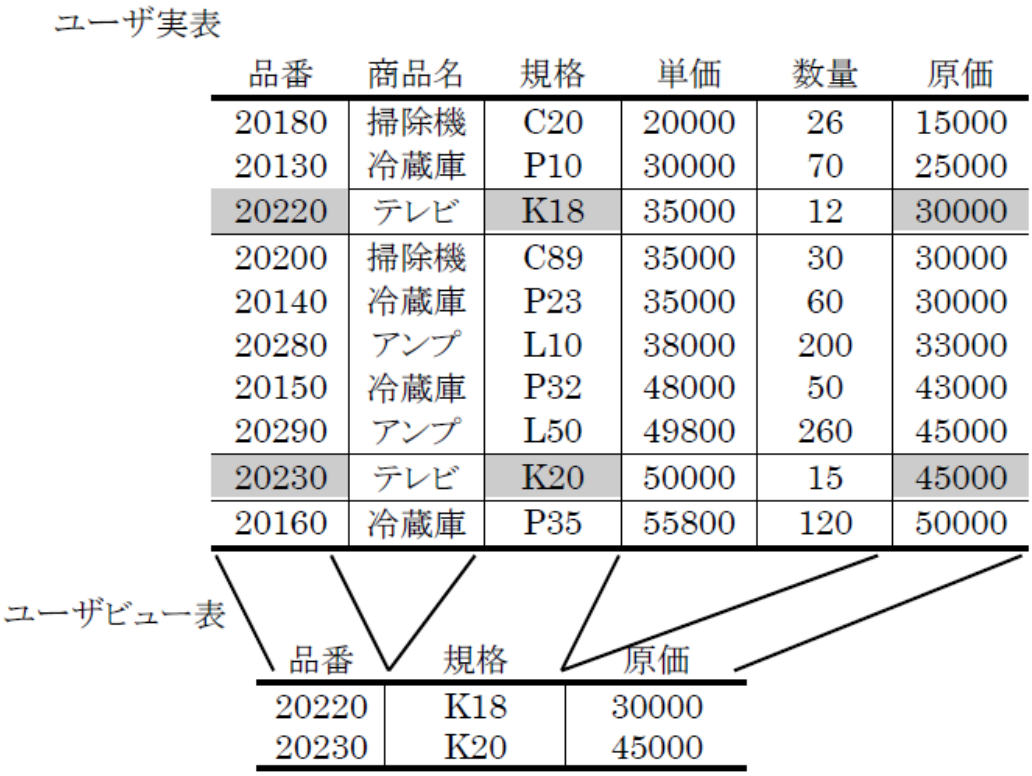


図1-2　ユーザビュー表と基になるユーザ実表との関係

ユーザビュー表を基に、さらにユーザビュー表を定義することも可能である。

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

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

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

- 大本となるユーザ実表がすべて所有者本人のものであるユーザビュー表

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

- 大本となるユーザ実表に所有者本人以外のものが含まれるユーザビュー表

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

【 ディクショナリ表 】

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

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

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

【 監査データ 】

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

＜ 監査証跡ファイル ＞

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

＜ 監査証跡表 ＞

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

1.3 評価の実施

認証機関が運営するITセキュリティ評価・認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「HiRDB Single Server セキュリティターゲット」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 ([5][8][11]のいずれか) 附属書B、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「HiRDB / Single Server Version 7 07-03 評価報告書」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、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、本TOE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。評価は、平成20年6月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEM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。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL4追加である。
追加の保証コンポーネントは、ALC_FLR.1である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。
脅威エージェントの攻撃能力は低く、セキュリティ侵害の試みは一時的なものであると想定される。したがって、最小機能強度レベルはSOF-基本が妥当である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能は、以下のとおりである。

【 識別・認証 】

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

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

【 利用者・権限管理 】

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

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

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

【 アクセス制御 】

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

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

【 監査 】

TOEは、利用者によって実行されるデータベース操作に関する情報（監査データ）を記録し、それらの情報を参照できる監査機能を提供する。この機能により、ある操作の結果や試行が問題となる場合は、それを実行した利用者の認可識別子を特定することができるため、その利用者にアカウンタビリティを要求することができる。

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

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

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

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

1.5.5 脅威

本TOEは、脅威エージェントとして以下を想定する。

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

上記の脅威エージェントは、いずれも高度な専門知識を持たず、攻撃用の特別な

ツールを利用することも無く、セキュリティ侵害を行う動機は強くないものとする。

本TOEは、表1-2に示す脅威を想定し、これに対抗する機能を備える。

表1-2　想定する脅威

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

1.5.6　組織のセキュリティ方針

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1-3に示す。

表1-3　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. ACCESS_PRIVILEGE	スキーマ所有者は、本人が所有するユーザ表のアクセス権限を管理しなければならない。
P.DATABASE_ADMINISTRATOR	DBA権限保持者は、監査人以外の識別・認証情報、DBA権限、およびスキーマ定義権限を管理しなければならない。
P.AUDITOR	監査人は、必要に応じ、セキュリティ機能に関する操作の中から監査対象事象を選択し、監査業務を実施しなければならない。監査証跡参照者を設ける場合は、監査人は信頼できる人物にその役割を委任しなければならない。
P.AUDIT_VIEWER	監査証跡参照者は、監査人の指示に従って監査データをチェックすることにより、監査人の業務を補佐しなければならない。
P.SECURITY_PARAMETER	DBA権限保持者は、パスワードの最小文字数、連続認証失敗許容回数、および認可識別子のロック時間をセキュアな値に維持しなければならない。

1.5.7 構成条件

本TOEは、図1-3の構成で動作する。

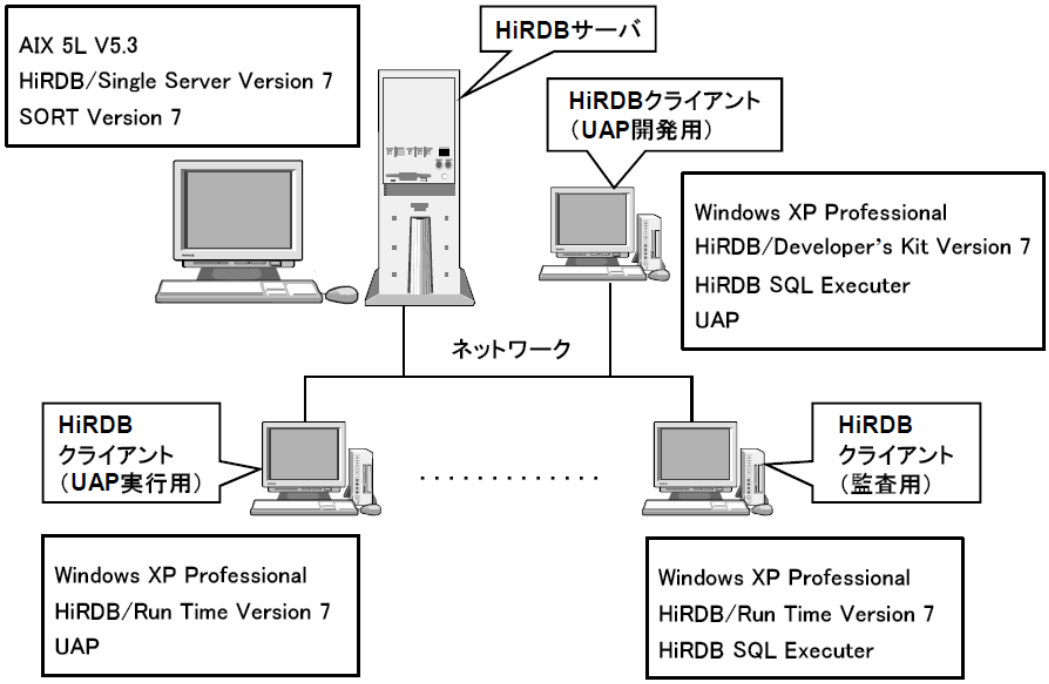


図1-3　TOEの動作環境

1.5.7.1 HiRDB サーバの構成

HiRDBサーバはAIX 5L V5.3が動作するマシンであり、以下のソフトウェアがインストールされる。

- AIX 5L V5.3
- HiRDB/Single Server Version 7 (本TOE)
- SORT Version 7

1.5.7.2 HiRDB クライアントの構成

HiRDBクライアントはWindows XP Professionalが動作するマシンである。HiRDBクライアントは複数台存在してもよく、各マシンはそれぞれの用途により3通りの構成が可能である。

HiRDBクライアントの構成の中にはUAPという要素が存在するが、UAPは特定の製品ではなく、TOEの機能を利用するアプリケーションプログラムの総称である。UAPは、HiRDB/Run Time Version 7またはHiRDB/Developer's Kit Version 7を介してTOEの機能を利用するように開発される。

UAP開発を用途とするHiRDBクライアントには、以下のソフトウェアがインストールされる。

- Windows XP Professional
- HiRDB/Developer's Kit Version 7
- HiRDB SQL Executer
- UAP

UAP実行を用途とするHiRDBクライアントには、以下のソフトウェアがインストールされる。

- Windows XP Professional
- HiRDB/Run Time Version 7
- UAP

監査を用途とするHiRDBクライアントには、以下のソフトウェアがインストールされる。

- Windows XP Professional
- HiRDB/Run Time Version 7
- HiRDB SQL Executer

1.5.7.3 ネットワークの構成

HiRDBサーバと各HiRDBクライアントは、他とは独立したネットワークにより接続される。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-4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1-4　TOE使用の前提条件

識別子	前提条件
A.OS_ACCOUNT	HiRDB サーバの OS のアカウントは、許可された管理者以外には与えられず、許可された管理者以外は HiRDB サーバの OS にログインできないものとする。
A.REMOTE_OPERATION	HiRDB サーバの OS には、HiRDB サーバ以外の端末からリモートログインすることはできないものとする。
A.SERVER_SOFTWARE	HiRDB サーバには、OS、TOE、および SORT 以外のソフトウェアはインストールされないものとする。

識別子	前提条件
A.CLIENT_OF_SERVER	HiRDB サーバにおけるクライアント機能は、使用されないものとする。
A.SERVER_HARDWARE	HiRDB サーバのためのハードウェアと周辺機器は、許可された管理者だけが入場できる場所に設置されるものとする。
A.NETWORK	HiRDB サーバには HiRDB クライアントだけが接続され、HiRDB サーバと HiRDB クライアント間の通信の秘匿性と完全性は、確保されているものとする。
A.HiRDB_CLIENT	HiRDB クライアントでは、UAP と HiRDB SQL Executer 以外のネットワークを介して電文を送信できるソフトウェアは使用されないものとする。また、電文の送信先となる HiRDB サーバのポート番号を設定する環境変数には定められた値が設定され、変更がないように維持されるものとする。
A.UAP	HiRDB クライアントで使用される UAP は、TOE で定められているプロトコルに従った電文のみを HiRDB サーバに送信するよう、TOE のガイダンスに従って開発されるものとする。また、XA 連携機能は使用されないものとする。
A.ADMINISTRATORS	許可された管理者は、HiRDB サーバおよび HiRDB クライアントに対して、悪意のある操作を行わない。
A.PASSWORD	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。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

- HiRDB Version 7 解説（UNIX(R) 用） 3000-6-271-30, 第4版
- HiRDB Version 7 システム導入・設計ガイド (UNIX(R)用) 3000-6-272-30, 第4版
- HiRDB Version 7 システム定義（UNIX(R)用） 3000-6-273-30, 第4版
- HiRDB Version 7 システム運用ガイド （UNIX(R) 用） 3000-6-274-30, 第4版
- HiRDB Version 7 コマンドリファレンス （UNIX(R) 用） 3000-6-275-30, 第4版
- HiRDB Version 7 UAP 開発ガイド （UNIX(R)/Windows(R) 用） 3000-6-276-30, 第4版

- HiRDB Version 7 SQL リファレンス （UNIX(R)/Windows(R) 用） 3000-6-277-30, 第4版
- HiRDB Version 7 メッセージ（UNIX(R)/Windows(R) 用） 3000-6-278-30, 第4版
- HiRDB Version 7 セキュリティガイド 3000-6-279-10, 第2版
- プログラムプロダクト P-1M62-1171 07-03-20 HiRDB/Single Server Version 7 リリースノート

2 評価機関による評価実施及び結果

2.1 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ている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 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17年9月に始まり、平成20年6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18年6月、平成20年1月及び平成20年2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・配付と運用・ライフサイクル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20年1月及び平成20年2月に開発者サイトで開発者のテスト環境を使用し、開発者が実施した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、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

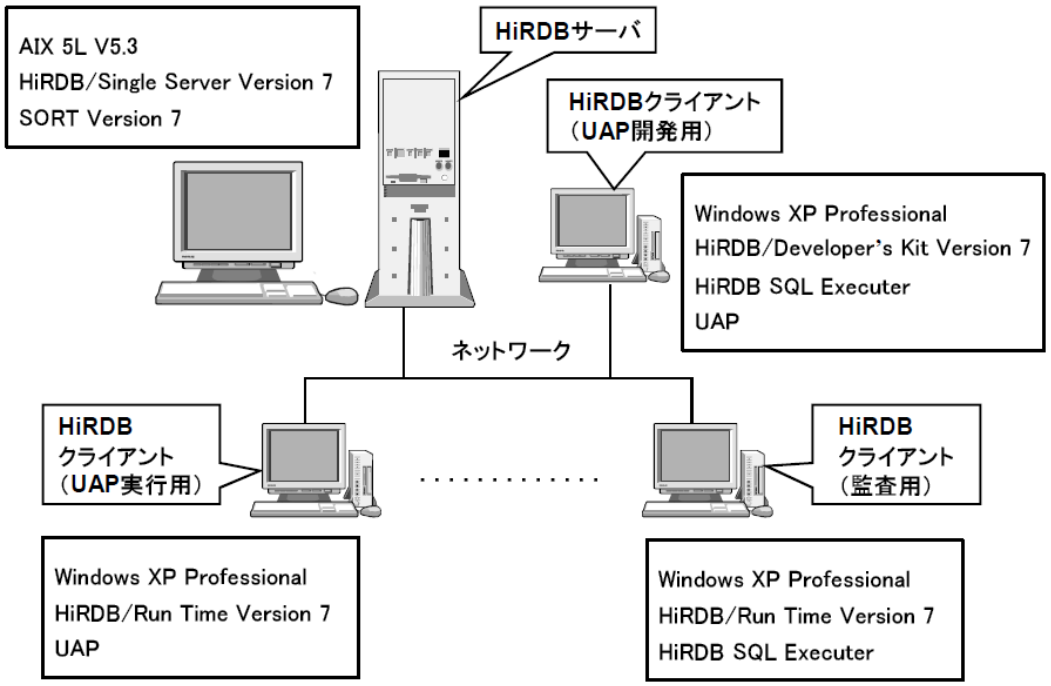
2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

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2-1に示す。



（補足） 上記に加え、各HiRDBクライアントには、テストのためのツールが導入された。
UAPとしては、開発者が作成したものが使用された。

図2-1　開発者テストの構成図

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a.テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストは、各HiRDBクライアントに導入されたツールを除いて、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。各HiRDBクライアントに導入されたツールが、STにおいて識別されている構成との一貫性に影響しないことは、評価者により検証された。

b.テスト手法

テストには、以下の手法が使用された。

①以下の方法でTOEの外部インタフェースを使用し、その応答を観察する。

- UAP、HiRDB SQL Executer、テストのためのツールを使用する。
- HiRDBサーバのシェルからコマンドを入力する。

c.実施テストの範囲

テストは開発者によって434項目実施されている。

カバレージ分析が実施され、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十分にテストされたことが検証されている。深

さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d.結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。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、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、図2-1に示した開発者テストと同様の構成である。ただし、UAPは評価者により再度作成された。

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a.テスト構成

評価者が実施したテストは、開発者テストと同様の構成で実施されている。

b.テスト手法

テストには、開発者テストと同様の手法が使用された。

c.実施テストの範囲

評価者が独自に考案したテストを12項目、開発者テストのサンプリングによるテストを284項目、計288項目のテストを実施した。

評価者が独自に考案したテストはCEMの4:ATE_IND.2-4、4:AVA_VLA.2-4、及び4:AVA_VLA.2-10の要求に従い考案された。特に、以下によりテストが導かれた。

① 開発者テストの厳密さを補足する。
② 開発者テストから評価者が持った懸念を解消する。
③ 脆弱性分析において、想定される脅威エージェントが悪用できる脆弱性がないことを確認する。

開発者テストのサンプリングは、CEMの4:ATE_IND.2-9で要求される観点に従い選択された。

d.結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本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。

3 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 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
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、ST及び評価報告書において、所見報告書及び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た。

4 結論

4.1 認証結果

提出された評価報告書、当該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EAL4及び保証コンポーネントALC_FLR.1に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE識別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。

ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。

ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**
ACM_AUT.1.1E	評価はワークユニットに沿って行われ、CMシステムが人為的誤りまたは怠慢による影響を受けないように、実装表現に対する変更が自動化ツールのサポートにより制御されていることを確認している。
ACM_AUT.1.1D	評価はワークユニットに沿って行われ、CM計画に記述されている自動化ツールと手順が使用されていることを確認している。
ACM_CAP.4.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理･追跡が可能な手続きが妥当であり正しく運用されていることを確認している。
ACM_SCP.2.1E	評価はワークユニットに沿って行われ、構成要素リストがCCによって要求される一連の要素を含んでいることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.2.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.2.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**

ADV_FSP.2.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.2.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.2.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境がないこと、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。
ADV_HLD.2.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_IMP.1.1E	評価はワークユニットに沿って行われ、実装表現がTSFを作成できる詳細レベルでTSFを明確に定義していること、開発者の提供した実装表現が十分足るものであること、それが内部的に一貫していることを確認している。
ADV_IMP.1.2E	評価はワークユニットに沿って行われ、実装表現のサブセットがその関連するTOEセキュリティ機能要件を正しく具体化したものであることを確認している。
ADV_LLD.1.1E	評価はワークユニットに沿って行われ、下位レベル設計が必要な説明情報を含み、内部的に一貫していること、モジュールの観点から記述されており、各モジュールの目的を記述していること、提供されるセキュリティ機能という観点でモジュール間の相互関係と依存性を定義していること、TSP実施機能の提供方法を記述していること、TSFモジュールのインタフェースと外部インタフェースを識別していること、各モジュールの使用法と目的を記述していること、そしてTSP実施モジュールとその他に区別できることを確認している。

ADV_LLD.1.2E	評価はワークユニットに沿って行われ、下位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であり、下位レベル設計が上位レベル設計の正しく完全な表現であることを、それらの対応分析により確認している。
ADV_SPM.1.1E	評価はワークユニットに沿って行われ、セキュリティ方針モデルが非形式的でありSTにおいて明示的方針をもたないこと、ST中のセキュリティ機能要件で表されたすべてのセキュリティ方針がモデル化されていること、セキュリティ方針モデルの規則や特性がモデル化されたTOEのセキュリティふるまいを明確に表していること、モデル化されたふるまいがセキュリティ方針と一貫し完全であること、セキュリティ方針を実装している機能仕様にてすべてのセキュリティ機能を識別していること、機能仕様の内容とセキュリティ方針モデルの実装として識別された機能の内容が一貫していることを確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
ライフサイクルサポート	**適切な評価が実施された**

ALC_DVS.1.1E	評価はワークユニットに沿って行われ、開発セキュリティ証拠資料がTOE開発環境のセキュア維持のための手段を記述しており、それが十分であること、その手段を実施した記録が生成されることを確認している。
ALC_DVS.1.2E	評価はワークユニットに沿って行われ、ALC_DVS.1.1Eで確認したセキュリティ手段が実施されていることを確認している。また、本評価時に行われたサイト訪問での調査方法も適切と判断される。
ALC_LCD.1.1E	評価はワークユニットに沿って行われ、使用されたライフサイクルモデルが開発者と保守手続きをカバーしており、その記述にある手続き、ツール、技法の使用が開発と保守に貢献していることを確認している。
ALC_TAT.1.1E	評価はワークユニットに沿って行われ、開発ツール証拠資料が明確であり、実装に用いられた開発ツールのステートメント及び実装依存オプションの意図を明確に定義していることを確認している。
ALC_FLR.1.1E	評価はワークユニットに沿って行われ、TOEの欠陥修正手続きについてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.2.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。
ATE_DPT.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが上位レベル設計に正確かつ完全に対応していること、テスト計画に示されたテスト手法がセキュリティ機能の検証に適切であること、テスト手順に示されるテスト条件、手順、期待される結果が各セキュリティ機能を適切にテストするものであることを確認している。

ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。
ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_MSU.2.1E	評価はワークユニットに沿って行われ、提供されたガイダンスがTOEのセキュアな運用に必要な情報を矛盾なく完全に記述していること、使用環境の前提事項、TOE以外のセキュリティ事項の要件がすべて明記されていること、ガイダンスの完全性を保証する手段を開発者が講じていることを確認している。
AVA_MSU.2.2E	評価はワークユニットに沿って行われ、提供されたガイダンスの管理者と利用者手続き、あるいはその他の手続き情報のみで、TOEを構成でき、TOEのセキュアな運用に関わる設定が行えることを確認している。
AVA_MSU.2.3E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEが非セキュアな状態に陥ったことを検出する手段及び対処方法を記述していることを確認している。

AVA_MSU.2.4E	評価はワークユニットに沿って行われ、提供されたガイダンスが、TOEの全ての操作モードにおいてのセキュアな操作を提供していることを確認している。
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.2.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.2.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。
AVA_VLA.2.3E	評価はワークユニットに沿って行われ、開発者がまだ扱っていない脆弱性の可能性を検査している。
AVA_VLA.2.4E	評価はワークユニットに沿って行われ、独立脆弱性分析に基づく侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテストの概要について報告がなされている。
AVA_VLA.2.5E	評価はワークユニットに沿って行われ、意図する環境においてTOEが低い攻撃力に対抗できることを侵入テストと脆弱性分析の結果から検査し、悪用され得る脆弱性及び残存脆弱性が存在しないことが報告されている。

4.2 注意事項

特になし。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用された用語を以下に示す。

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	本認証報告書では特に断わりがない限り、HiRDBサーバのOSを指す。
OSユーザ	HiRDBサーバのOSにログインする利用者。

SQL	リレーショナルデータベースの操作言語。SQLを用いることで、ユーザ表の定義やデータ操作など、リレーショナルデータベースに関する操作を機械可読なテキストとして記述できる。
UAP	利用者が開発するアプリケーションプログラム。
アクセス権限	ユーザ表のデータを操作するために必要な権限。アクセス権限は次に示す権限の総称であり、各権限はユーザ表毎にDBユーザに与えられる。 ● SELECT 権限 ● INSERT 権限 ● DELETE 権限 ● UPDATE 権限
オブジェクト	TOEの機能によって定義され、情報を内蔵するデータベースの構成要素。
監査証跡表	監査データの内容を参照するために使用される表。
監査証跡ファイル	監査対象事象の発生時に監査データが格納されるオブジェクト。
監査人	監査権限を持つDBユーザであり、監査業務を担当する。
行	表に格納される一件一件の各データのこと。 （別名 ： ロー、レコード）
行検索	表の行をさまざまな条件で検索する機能。操作系SQLの一種。
行更新	表の行の値を列単位で更新する機能。操作系SQLの一種。
行削除	表の行を削除する機能。操作系SQLの一種。
行挿入	表に行を追加する機能。操作系SQLの一種。
スキーマ	データベースの論理的構造単位（枠組）。単一のDBユーザ（スキーマ所有者）によりただ一つのスキーマが所有される。スキーマにはユーザ表が含まれる。

スキーマ所有者	スキーマを所有するDBユーザであり、所有するスキーマに含まれるユーザ表を所有し、管理する。スキーマを所有するには、スキーマ定義権限が必要である（スキーマ定義権限を持っていてもスキーマを所有していない場合は、スキーマ所有者には該当しない)。
スキーマ定義権限	スキーマを定義して、これを所有するのに必要な権限。
スーパユーザ	OS（UNIX）におけるシステム管理者。
制御系SQL	HiRDBサーバとの接続や切り離しを実行する場合に使用するSQL。
操作系SQL	表に格納されるデータを操作する場合に使用するSQL。
定義系SQL	ユーザ表をはじめとするオブジェクトの定義や削除を実行する場合に使用するSQL。
ディクショナリ表	DBユーザ、権限、およびユーザ表定義情報などを管理する表。
認可識別子	HiRDBサーバに接続するDBユーザを識別するための文字列。
表	リレーショナルデータベースの基本要素であり、論理的に行と列との2次元構造で表現されるデータが格納されるオブジェクト。表は、以下の３つに大別される。 ● ユーザ表 ● ディクショナリ表 ● 監査証跡表（別名 ： テーブル）
表定義変更	既に定義されているユーザ実表に列を追加するなど、ユーザ実表の定義内容を変更する機能。
ユーザ実表	実際に、利用者データとして行の集合が格納されるユーザ表。
ユーザビュー表	ユーザ表のデータから特定の行や列を選択して、新たに定義した仮想のユーザ表。ユーザビュー表は以下の２つに分類される。 ● 読込み専用ビュー ● 読込み専用ビュー以外のユーザビュー表

ユーザ表	スキーマ所有者が定義して所有する表であり、利用者データが格納される。ユーザ表は以下の２つに大別される。 ● ユーザ実表 ● ユーザビュー表
ユーザ表定義情報	ユーザ表の定義情報であり、以下の情報を含む。 ● 所有者の認可識別子 ● ユーザ表の種類 ● 列の定義情報
読込み専用ビュー	行検索だけが実行できるユーザビュー表。
列	表に格納される各レコード（行）に共通のデータ項目。 （別名 ： カラム、フィールド）

6 参照

[1] HiRDB Single Server セキュリティターゲット バージョン 2.20（2008年2月22日）株式会社 日立製作所

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[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1: 概説と一般モデル バージョン2.3 2005年8月 CCMB-2005-08-001 （平成17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2: セキュリティ機能要件 バージョン2.3 2005年8月 CCMB-2005-08-002 （平成17年12月翻訳第1.0版）

[10] 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: セキュリティ保証要件 バージョン2.3 2005年8月 CCMB-2005-08-003 （平成17年12月翻訳第1.0版）

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 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2.3 2005年8月 （平成17年12月翻訳第1.0版）

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] HiRDB / Single Server Version 7 07-03 評価報告書 第1.1版 2008年6月25日 株式会社電子商取引安全技術研究所 評価センター

JISEC

サーベイランス報告書

発行日 : 2012-10-12

資料番号 : SRP-C0171-01

下記評価対象について、ITセキュリティ認証等に関する要求事項(CCM-02) 8.1に基づき、サーベイランスが実施されたことを報告いたします。認証報告書と合わせて参照願います。

評価対象：

認証番号	C0171
認証申請者	株式会社 日立製作所
TOEの名称	HiRDB / Single Server Version 7
TOEのバージョン	07-03
PP適合	なし
適合する保証パッケージ	EAL4及び追加の保証コンポーネントALC_FLR.1
開発者	株式会社 日立製作所
評価機関の名称	株式会社電子商取引安全技術研究所 評価センター

サーベイランス管理番号： JISEC-SV12-002

サーベイランス実施報告：

- サーベイランス結果

評価機関により、本TOEを安全に調達者が利用することが可能であることが確認され、本TOEに対する認証は維持されます。

- サーベイランス概要

第三者からの情報提供により、HiRDB Version 8 体験版に識別・認証機能がバイパスされる脆弱性があることが判りました。

具体的には、利用者が識別・認証された後に、攻撃者がHiRDBサーバのあるポートにSQL実行のための不正な電文を送信することにより、既に識別・認証された利用者と同じ権限でSQLを実行できる可能性があります。

HiRDB Version 8 体験版は、本TOEの後継版の体験版となります。本TOEにも同様の脆弱性があることが懸念されるため、認証を維持することが適切かどうかを判断するために2012年5月から同年7月にかけてサーベイランスを実施しました。

サーベイランスの結果、本TOEにも同様の脆弱性の懸念があることが判りました。ただし、

STにおいて想定している運用環境では、攻撃者は自由に電文を送信することはできず、TOEに対して電文を送信するソフトウェアは限られているために脆弱性を悪用できないことが、評価機関の責任において当時の評価で検証済であることが示されました。

なお、この脆弱性の懸念については、開発者である株式会社 日立製作所より、ALC_FLR.1の保証要件にしたがって既に対策版が提供されており、対策版を入手することで回避することができるとの報告を受けています。

参考:ソフトウェア製品セキュリティ情報 HS10-014
http://www.hitachi.co.jp/Prod/comp/soft1/security/info/vuls/HS10-014/index.html

注意事項

未対策環境下において、脆弱性を悪用できないことの保証のためには、STに記載のとおり、「HiRDB Version7セキュリティガイド」に従って環境構築を行い、上記の「TOEに対して電文を送信するソフトウェア」が開発者の想定通りの電文の送信をすることが必要です。詳細を以下に示します。

TOEに対して電文を送信するソフトウェアはUAPとHiRDB SQL Executerであり、UAPはHiRDB/Run Time Version 7 またはHiRDB/Developer's Kit Version 7 を利用して電文を送信します。つまり、TOEに対して電文を送信するソフトウェアは、より正確には以下のものになります。

- HiRDB SQL Executer
- HiRDB/Run Time Version 7
- HiRDB/Developer's Kit Version 7

評価において、これらのソフトウェアは、TOEに対して開発者の想定通りの電文の送信をすることが仮定されています。この仮定によりこれらのソフトウェアからは脆弱性を悪用するような電文が発生しないということは、脆弱性を悪用できないことの根拠の一つとなります。

なお、仮にこれらのソフトウェアがTOEに対して想定外の電文の送信をする場合は、脆弱性の悪用につながることを否定できません。これらがTOEに対して想定外の電文の送信をしないことについては、評価による保証の対象ではなく、調達者が別途確信を得る必要があります。

以上