ＳＴ確認報告書

評価対象

申請受付年月日（受付番号）	**平成16年 2月 3日（ST確認4031）**
ＳＴ確認申請者	**株式会社日立製作所**
ＳＴの名称	HiRDB **セキュリティターゲット**
ＳＴのバージョン	Version 1.3
ＰＰ適合	**なし**
適合する保証要件	ASE（ST**評価**）**クラス** （TOE**の保証パッケージは**EAL3**適合**）
ＳＴ開発者	**株式会社日立製作所　ソフトウェア事業部**
評価実施機関の名称	**電子商取引安全技術研究組合研究所**

上記のSTについての評価は、以下のとおりであることを確認したので報告します。

平成16年6月18日

独立行政法人情報処理推進機構
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　田渕　治樹

評価基準等：「セキュリティターゲットの確認業務実施規程」で定める下記の規格に基づいて評価された。

① ISO/IEC 15408:1999　Information technology - Security techniques – Evaluation criteria for IT security
② JIS X 5070(2000) セキュリティ技術 ― 情報技術セキュリティの評価基準
③ Common Criteria for Information Technology Security Evaluation Version 2.1
④ JIS TR X 0049(2001) 情報技術セキュリティ評価のための共通方法
⑤ Common Methodology for Information Technology Security Evaluation Version 1.0
⑥ CCIMB Interpretation-0210
⑦ 認証機関が公開する③、⑤及び⑥の翻訳文書

評価結果：合格

「HiRDB セキュリティターゲット」は、独立行政法人情報処理推進機構が定めるセキュリティターゲットの確認業務実施規程に従い、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。

その他：なし

目次

1 全体要約

1.1 はじめに

このST確認報告書は、「HiRDB セキュリティターゲット」[1]（以下「本ST」という。）について電子商取引安全技術研究組合研究所（以下「評価実施機関」という。）が行ったセキュリティ評価に対し、その内容の確認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ST確認報告書の読者は、本書とともに、対応する本ST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、本STにおいて詳述されている。

本ST確認報告書は、本STに対する確認結果を示すものであり、対応するTOEのいかなる実装についても言及していないことに留意されたい。

1.2 評価製品

1.2.1 製品名称

本STが対象とする製品は、以下のとおりである。なお、TOEの正確な範囲は、「1.2.3 TOEの範囲」で定義される。

- 名称: HiRDB / Single Server Version 7
- バージョン: 07
- リビジョン: 02
- 開発者: 株式会社日立製作所 ソフトウェア事業部

1.2.2 製品概要

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る。HiRDB / Single Server Version 7はデータベースサーバとして、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。利用者はネットワークを介しクライアントからHiRDB / Single Server Version 7に対してSQLを発行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。またHiRDB / Single Server Version 7は、格納された情報へのアクセスに対し、そのアクセスを許可された利用者に制限する機能を提供する。

HiRDB / Single Server Version 7はクライアント/サーバのネットワーク環境で使用する。データベースを配置するHiRDB / Single Server Version7のデータベースサーバ側システム(HiRDBサーバ)とサーバにSQLを発行するアプリケーションが実行されるクライアント側システム（HiRDBクライアント）の利用環境を図1に示す。

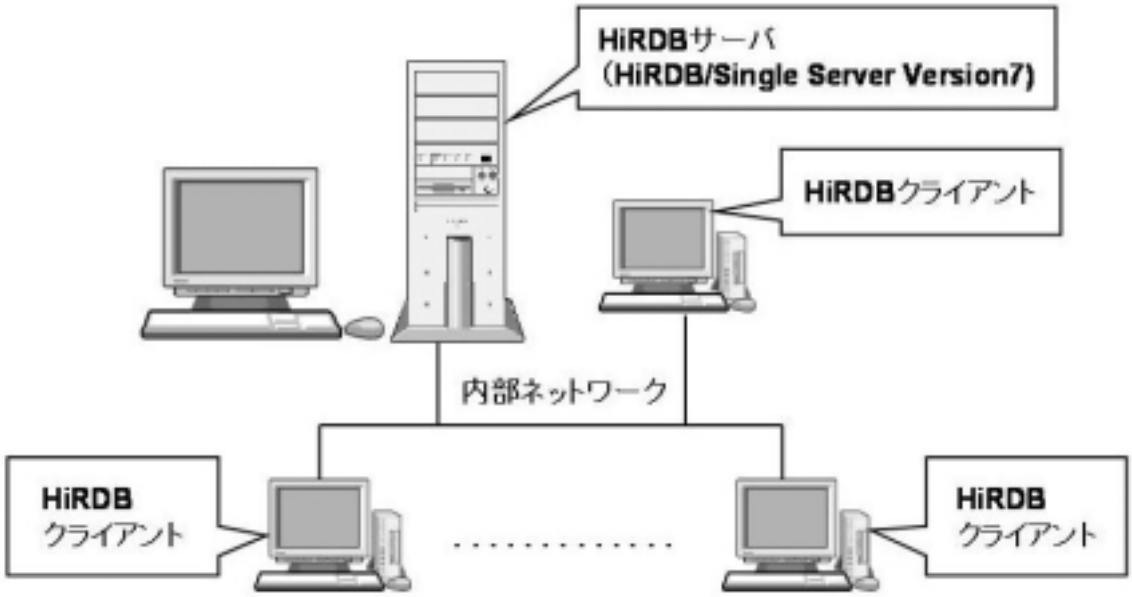

図1　HiRDBの利用環境

1.2.3 TOEの範囲

製品であるHiRDB / Single Server Version 7はHiRDBサーバにインストールされるソフトウェアである。HiRDBサーバにはHiRDB / Single Server Version 7のほかOSおよびレコードソートプログラム(SORT Version 6)が搭載される。HiRDBサーバおよびHiRDBクライアントの構成については「2 TOE構成」で述べる。

HiRDB / Single Server Version 7は大別すると、「HiRDB本体」、「ユーザ表を操作するユティリティ」、「監査データを操作するユティリティ」、「その他のユティリティおよび運用コマンド」の4つのモジュールから構成される。このうち、「その他のユティリティおよび運用コマンド」はデータベースのバックアップおよびTOEの開始・終了を実施するもので、本TOE管理者が直接的に操作する機能であり、TOEの資産アクセスに関与しないため、TOEの範囲外とする。TOEの３つのモジュールについて述べる。

- HiRDB 本体

  HiRDB / Single Server Version 7 が提供するメイン機能は SQL であり、その SQL の機能を有する部分が HiRDB 本体である。以下に SQL の概略を定義系、操作系、制御系の３つに分類して説明する。

  1)　定義系 SQL

定義系 SQL とは、ユーザ表（1.2.4 TOE の動作概要に記述）を定義したり、削除したりする場合に使用する SQL である。通常のサービスで使用する操作系 SQL とは異なり、事前に行うデータベースの論理的な構築やその変更時に用いる SQL が定義系 SQL である。また、DB ユーザ(HiRDB / Single Server Version 7 に接続する利用者)の登録・削除および各種権限の与奪を行う機能や、監査の対象とする事象を選択する機能も定義系 SQL に含まれる。

2) 操作系 SQL

操作系 SQL とは、表に格納されるデータを操作する場合に使用する SQL である。通常のサービスでは、操作系 SQL を駆使することで、データ（行）の参照や更新が行われる。基本的な操作系 SQL の機能は、行検索・行挿入・行削除・行更新である。

3) 制御系 SQL

制御系 SQL とは、HiRDB / Single Server Version 7 との接続や切り離しを実行する場合に使用する SQL である。SQL の機能を利用するには、DB ユーザは HiRDB / Single Server Version 7 に接続する必要がある。HiRDB / Single Server Version 7 との接続は制御系 SQL の CONNECT 文を実行することで行われる。DB ユーザが HiRDB / Single Server Version 7 に接続するとその DB ユーザのセションが確立（開始）される。確立されたセションにおいて HiRDB / Single Server Version 7 との切り離しが行われた場合、そのセションは終了する。DB ユーザはセションが確立されている間でのみ、CONNECT 文を除く SQL の実行を要求することができる。

DB ユーザが HiRDB / Single Server Version 7 に接続するには HiRDB / Single Server Version 7 によって行われる「識別・認証」をパスしなければならない。

- ユーザ表を操作するユティリティ

本ユティリティは、HiRDB サーバの OS が提供するシェルからコマンドを入力することにより起動され、定義系 SQL を実行する。ユーザ表を操作するユティリティは、OS ユーザであれば制限なく起動することができる。ただし HiRDB / Single Server Version 7 は、ユーザ表を操作するユティリティを実行する利用者に対して、識別・認証、およびユーザ表の操作に必要な権限のチェックを実施する。

- 監査データを操作するユティリティ

本ユティリティは、HiRDBサーバのOSが提供するシェルからコマンドを入力することにより起動され、監査証跡ファイルの監査データを監査証跡表に登録する。監査データを操作するユティリティは、OSユーザであれば制限なく起動することができる。ただし、HiRDB / Single Server Version 7は、監査データを操作するユティリティを実行する利用者に対して、識別・認証、および監査データの操作に必要な権限のチェックを実施する。

1.2.4 TOEの動作概要

(1) TOEの利用方法

HiRDB / Single Server Version 7は、クライアントサーバ形態で使用される（「図1　HiRDBの利用環境」を参照）。HiRDB / Single Server Version 7がインストールされる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 / Single Server 7に接続し、データベースにアクセスする端末をHiRDBクライアントと呼ぶ。

HiRDBクライアントから発行されるSQLに応じてHiRDBサーバは構築されたデータベースの操作を行う。HiRDBサーバに構築されるデータベースは、ユーザ表、ディクショナリ表、監査データで構成される。HiRDB利用者はHiRDBクライアントからSQLを発行することでユーザ表の操作（行検索、行挿入、行削除、行更新）を依頼する。HiRDBサーバは、その操作の対象となるユーザ表において、操作要求をしたDBユーザの操作権限を検査し、要求を実行あるいは拒否する。

以下、データベースの構成要素とその操作について説明する。

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（ユーザ表を含むデータベースの論理的構造単位で、スキーマ上に表などのオブジェクトを作成する）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二次元の表形式であり、横方向に並ぶ一式のデータを行、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、行検索、行挿入、行削除、行更新の４つである。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木目の細かいアクセス制御を実施することが可能である。ユーザビュー表とその基になるユーザ実表との基本的な関係の例

を図 2に示す。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2　ユーザ実表とユーザビュー表

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。

① [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。

② [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。

2) ディクショナリ表

ディクショナリ表とは HiRDB / Single Server Version 7 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、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、削除される。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（監査人の補佐）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 評価実施

HiRDB セキュリティターゲットのセキュリティ評価は、認証機関として運営するITセキュリティ評価・認証プログラムに基づき、公表文書「セキュリティターゲットの評価・確認申請等の手引き (平成15年10月)」[2]、「セキュリティターゲット評価実施機関に対する要求事項 (平成14年4月)」[3]、「セキュリティターゲットの確認申請者・登録者に対する要求事項 (平成14年4月)」[4]に規定された内容に従い、評価実施機関によって実施された。

本評価の目的は、申請者から提出された本STが、CCパート1 ([5][8][11][14]のいずれか)附属書C、CCパート2（[6][9][12][15]のいずれか）の機能要件及びCCパート3

（[7][10][13][16]のいずれか）のASEクラスの規定を満たし、セキュリティ機能設計の基本文書として技術的に妥当なものであるかどうかを評価することである。ただし、ASEクラスの規定の中で、TOE評価と関連する要求事項については、評価の項目に含まれていない。なお、評価方法は、CEMパート2（[17][18][19]のいずれか）に準拠する。また、CC及びCEMの各パートは補足([21][22])の内容を含む。

認証機関は、評価実施機関である電子商取引安全技術研究組合研究所が実施するSTの評価を監督し、ST評価が所定の手続きに沿って行われたことを確認した。評価は、平成16年5月の評価実施機関による「ST評価報告書」[20]の提出をもって完了し、同報告書に基づき、認証機関は本ST確認報告書を作成した。

1.4 報告概要

1.4.1 PP適合

適合するPPはない。

1.4.2 EAL

本STが規定するTOEの評価保証レベルは、EAL3適合である。

1.4.3 セキュリティ機能強度

本STにおいてTOEに要求される最小機能強度レベルは、SOF-基本である。

1.4.4 セキュリティ機能

TOEは、以下のセキュリティ機能を有する。

- 識別・認証

  DBユーザがHiRDB / Single Server Version 7に接続するには、HiRDB / Single Server Version 7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 / Single Server Version 7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HiRDB / Single Server Version 7に登録されているものと一致する場合、HiRDB / Single Server Version 7はそのDBユーザの接続を許可する。

  HiRDB / Single Server Version 7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、HiRDB / Single Server Version 7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、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、HiRDB / Single Server Version 7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、および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、各種オブジェクト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。

  ① 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。

  ② 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。

  ③ データベース管理者である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。

1.4.5 脅威

TOEは、表1に示す脅威を想定し、これに対抗する機能を備える。

表1　想定する脅威

識別子	脅威
T.ILLEGAL_CONNECT （不正な接続）	不正な利用者が、TOEに接続し、SQLを実行することによって、利用者データを暴露・改ざん・削除するかもしれない。
T.UNAUTHORIZED_ACCESS （権限外のアクセス）	正当な利用者（DBユーザ）が、TOEに接続し、SQLを実行することによって、本来は権限のない利用者データを暴露・改ざん・削除するかもしれない。
T.UNAUTHORIZED_PERMISSION_MODIFY （権限外の利用者・権限情報の改ざん）	正当な利用者（DBユーザ）が、TOEに接続し、SQLを実行することによって、自身や他の利用者の利用者・権限情報を改ざんして、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。
T.AUDIT_TRAIL_DESTRUCTION （監査データの改ざん）	監査データが改ざん、または不当に削除されることにより、TOEに対する不当なアクセスの試みが検出できなくなり、不正な利用者による利用者データを暴露・改ざん・削除する被害が発生し、拡大するかもしれない。

1.4.6 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2に示す。

表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. ACCESS_PRIVILEGE （アクセス権限の管理）	スキーマ所有者は、本人が所有するユーザ表のアクセス権限を適切に管理しなければならない。
P.DATABASE_ADMINISTRATOR （DBA権限保持者）	DBA権限保持者は、監査人以外の識別・認証情報、DBA権限、およびスキーマ定義権限を適切に管理しなければならない。なお、DBA権限保持者が監査人を兼任してはならない。
P.AUDITOR （監査人）	監査人は、監査対象事象を適切に設定し、監査業務を適切に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適切な人物にその役割を委任しなければならない。
P.AUDIT_VIEWER （監査証跡参照者）	監査証跡参照者は、監査人の指示に従って監査データをチェックすることにより、監査人の業務を補佐しなければならない。
P.ACCOUNTABILITY （説明責任）	正当な利用者（DBユーザ）は、TOEのアクセスについて説明責任を負わなければならない。
P.SECURITY_PARAMETER （セキュリティ変数）	DBA権限保持者は、パスワードの最小文字数、連続認証失敗許容回数、および認可識別子のロック時間をセキュアな値に維持しなければならない。

1.4.7 構成条件

本TOEの利用環境については「図1　HiRDBの利用環境」を参照のこと。HiRDBサーバにおいて本TOEと協調して動作するために必要なソフトウェアの構成条件を表3に、HiRDBサーバのソフトウェア構成図を図3に示す。なお、サーバにおいて必要となるハードウェアおよびスペックについては「2 TOE構成」を参照のこと。

表3　HiRDBサーバの構成条件

ソフトウェア	説明
AIX 5L V5.2	HiRDBサーバに搭載されるOS
HiRDB / Single Server Version 7	RDB管理システムソフトウェア製品（本TOE）
SORT Version6	レコードの整列・選択・集約のためのユティリティプログラム。HiRDB / Single Server Version 7へソート機能を提供する。

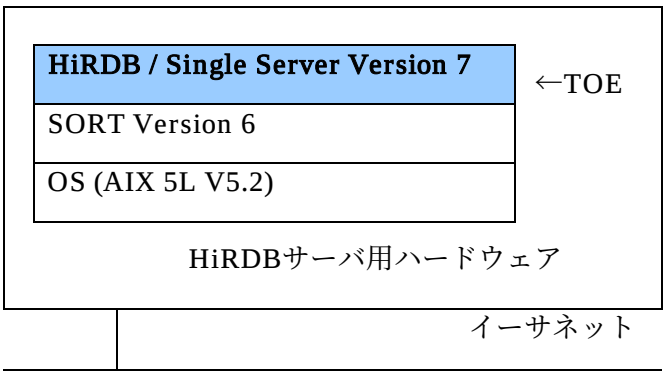

図3　HiRDBサーバソフトウェア構成図

1.4.8 動作環境の前提条件

TOEを使用する環境において有する前提条件を表4に示す。

これらの前提条件が満たされない場合、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　TOE使用の前提条件

識別子	前提条件
TOEの意図する使用法	
A.HiRDB_SERVER_CONFIG （HiRDBサーバの設定）	HiRDBサーバのために使用されるソフトウェアは、適切にインストール、設定、および運用管理が行われるものとする。
A.OS_ACCOUNT （OSのアカウント）	HiRDBサーバのOSのアカウントは、許可された管理者（HiRDB管理者、DBA権限保持者、監査人、スキーマ所有者）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。OSのアカウントのパスワードは、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.REMOTE_OPERATION （リモート操作の制限）	HiRDBサーバのOSには、HiRDBサーバ以外の端末からリモートログインすることはできないものとする。また、HiRDB / Single Server Version 7のユティリティと運用コマンドは、HiRDBサーバ以外の端末からは実行できないものとする。
物理的管理	
A.HiRDB_SERVER_HARDWARE （ハードウェアの管理）	HiRDBサーバのためのハードウェアと周辺機器は、許可された管理者（HiRDB管理者、DBA権限保持者、監査人、スキーマ所有者）だけが入場できる場所に設置されるものとする。また、HiRDBサーバのためのハードウェアと周辺機器は、その構成に変更がないように管理され、かつ正常に動作し続けるように管理されているものとする。さらに、HiRDBサーバに必要なバックアップ等のための記憶媒体は、許可された管理者だけが入場できる場所からは持ち出されないように管理されているものとする。
接続環境	
A.NETWORK （ネットワーク）	内部ネットワークは外部からのアクセスに対して完全に守られており、その秘匿性と保全性は確保されているものとする。
人的条件	
A.HiRDB_ADMINISTRATOR （HiRDB管理者）	HiRDB管理者は、怠慢なく、HiRDBサーバに対して悪意のある操作や誤操作を行わないようHiRDBサーバの管理に責任を持つ。
A.OS_USERS （一般OSユーザ）	OSのアカウントを持つDBA権限保持者、監査人、およびスキーマ所有者は、HiRDBサーバに対して悪意のある操作や誤操作を行わないようHiRDBサーバの使用に責任を持つ。
A.PASSWORD （パスワードの管理）	DBユーザのパスワードは、他人に知られないように本人によって管理される。パスワードは推測されにくいものが設定され、適切な頻度で変更される。
A.ORDINARY_USERS （一般DBユーザ）	一般DBユーザは、データベースの安全な利用方法についての技能と知識を有し、それを用いてデータベースの操作を行う

1.5 ST確認に関わる注意事項

ST確認は、CCで規定された評価の全過程から、ST評価の部分だけを抜き出した評価に基づいて行われるものである。したがって、ST評価を規定したASEクラスの要件の中で、TOE評価と関連する事項についてはST評価の対象になっていない。また、ASEクラス以外の保証クラスに属する事項、例えば、STの記載事項がそのとおりに設計されTOEに実装されているかどうか、TOEに悪用可能な脆弱性が残っていないかどうか、あるいはTOEの製造・配付が安全な手続きに基づいて行われているかなども評価の範囲外である。これら評価対象外の事項については確認も行われていないことに、本報告書の読者は留意すべきである。

ST確認は、TOEに対する、潜在的なものを含めたあらゆるセキュリティ上の脅威が完全に対策されていることを保証するものではない。評価完了後にTOEやそのIT環境にあらたな脅威が発見される可能性は常に考慮されるべきであり、TOE利用者は、TOEに関わる最新のセキュリティ関連情報に継続的な注意を払うことが必要である。

STの中で前提条件として記述されたものは、TOEを安全に使用する上での必須事項である。これらの条件が満たされないと、TOEのセキュリティ機能は、期待される効果を発揮することができない。前提条件を満たすためのTOEの安全な運用管理は、TOE利用者の責務である。

本ST確認報告書は、認証機関が該当するTOEを保証し、その使用を推奨することを意図したものではない。

2 TOE構成

2.1 TOEの動作に必要なハードウェア

TOEはソフトウェア製品であり、HiRDBサーバ上に搭載され、他のソフトウェアと協調して動作する。このHiRDBサーバのハードウェアおよび仕様を表5に示す。

表5　HiRDBサーバのハードウェア

ハードウェア	仕様
本体	日立 EP8000シリーズ （ディスプレイ、キーボード、マウス、CD-ROMを含む）
CPU	POWER3-Ⅱ 333MHz以上
メモリ	512MB以上
ハードディスク	18.2GB以上

3 評価実施機関による評価結果

評価は、CCパート3のASEクラスの規定に基づき、CEMパート2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、ST評価報告書[20]において報告されている。ST評価報告書には、TOEの概要説明、CEMパート2のワークユニットごとの評価内容及び判断が記載されている。各ワークユニットの評価作業において発見された問題点及びその対処の経過・結果も記載されている。

評価実施機関が評価中に発見した問題点は、すべて開発者による見直しが行われ、最終的に全ての問題点が解決されている。

総合判定は、「合格」である。

4 結論

4.1 ST確認実施

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

① 評価実施機関が評価作業中に指摘した所見報告書の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正しくSTに反映されていること。

③ 提出されたSTの内容を確認し、関連する評価者アクションエレメントが本評価報告書で示されたように評価されていること。

④ 本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 本評価報告書に示された評価者の評価方法がCEMに準拠していること。

これらの確認において発見された問題事項を認証レビューとして記載し、評価実施機関に送付した。

認証機関は、本ST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。

4.2 ST確認結果

提出されたST評価報告書及び所見報告書を検証した結果、認証機関は本STがCCパート3に規定されたASEクラスの保証要件を満たしていることを確認した。

評価実施機関の実施した各評価者アクションエレメントについて、確認結果を表6にまとめる。

表6　評価者アクションエレメント確認結果

評価者アクションエレメント	確認結果
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然と一貫性のあることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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概説が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明記され、それらが脅威、組織のセキュリティ、前提条件へ遡れ、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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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理路整然とし、完結しており、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。
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結しており、理路整然とし、かつ一貫していることを確認している。また、当評価に至るまでなされた指摘(所見報告書)も適切と判断される。

4.3 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
DBA	Data Base Administrator
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation

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	DBA権限を持つDBユーザ。DBユーザ、DBA権限およびスキーマ定義権限を管理する。
DBユーザ	HiRDB / Single Server Version 7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HiRDB / Single Server Version 7の管理・運用業務を担う管理者。
HiRDBクライアント	HiRDBサーバに対してSQLを発行するアプリケーションが実行されるクライアント側システム。
HiRDBサーバ	HiRDB / Single Server Version 7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では特に断りがない限り、HiRDBサーバのOSを示す。
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。

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、各権限はユーザ表ごとに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	HiRDB / Single Server Version 7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1件1件の各データ。（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ユーザによりただひと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。
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。
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 セキュリティターゲット　2004年5月28日　Version 1.3 株式会社日立製作所

[2] セキュリティターゲットの評価・確認申請等の手引き 平成15年10月 独立行政法人 製品評価技術基盤機構 適合性評価センター

[3] セキュリティターゲット 評価実施機関に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－ST評価要求－02

[4] セキュリティターゲットの確認申請者・登録者に対する要求事項 平成14年4月 独立行政法人 製品評価技術基盤機構 適合性評価センター 適合－部門－ST申請要求－02

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.1 August 1999 CCIMB-99-031

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.1 August 1999 CCIMB-99-032

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.1 August 1999 CCIMB-99-033

[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2.1 1999年8月 CCIMB-99-031

[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2.1 1999年8月 CCIMB-99-032

[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2.1 1999年8月 CCIMB-99-033

[11] ISO/IEC 15408-1 Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model ISO/IEC15408-1: 1999(E)

[12] ISO/IEC 15408-2 Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements ISO/IEC15408-2: 1999(E)

[13] ISO/IEC 15408-3 Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements ISO/IEC15408-3: 1999(E)

[14] JIS X 5070-1: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第1部: 総則及び一般モデル

[15] JIS X 5070-2: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第2部: セキュリティ機能要件

[16] JIS X 5070-3: 2000 セキュリティ技術－情報技術セキュリティの評価基準－第3部: セキュリティ保証要件

[17] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part2: Evaluation Methodology Version 1.0 August 1999

[18] 情報技術セキュリティ評価のための共通方法論 CEM-99/045 パート2: 評価方法論 バージョン1.0 1999年8月
[19] JIS TR X 0049: 2001 情報技術セキュリティ評価のための共通方法
[20] ST評価報告書 1.2版 2004年5月31日 DUT-ETRST-0001-02 電子商取引安全技術研究組合研究所
[21] CCIMB Interpretations-0210
[22] 補足-0210