HITACHI
Inspire the Next

ノンストップデータベース

HiRDB Version 9 セキュリティガイド

解説・手引書

3020-6-459

■対象製品

●適用 OS：HP-UX 11i V2(IPF)，HP-UX 11i V3(IPF)
P-1J62-3591 HiRDB Server Version 9 09-01
●適用 OS：AIX 5L V5.2，AIX 5L V5.3，AIX V6.1
P-1M62-3591 HiRDB Server Version 9 09-01
●適用 OS：Solaris 8，Solaris 9，Solaris 10
P-9D62-3591 HiRDB Server Version 9 09-01
●適用 OS：Red Hat Enterprise Linux AS 4(AMD64 & Intel EM64T)，Red Hat Enterprise Linux ES 4(AMD64 & Intel EM64T)，Red Hat Enterprise Linux 5 (AMD/Intel 64)
P-9W62-3591 HiRDB Server Version 9 09-01
●適用 OS：Windows Server 2003 x64 Editions，Windows Server 2008 R2，Windows Server 2008 (x64)，Windows XP x64 Edition，Windows Vista Ultimate (x64)，Windows Vista Business (x64)，Windows Vista Enterprise (x64)，Windows 7 Professional (x64)，Windows 7 Enterprise (x64)，Windows 7 Ultimate (x64)
P-2962-9194 HiRDB Server Version 9 09-01
これらのプログラムプロダクトのほかにもこのマニュアルをご利用になれる場合があります。詳細は「リリースノート」でご確認ください。
これらの製品は，ISO9001 および TickIT の認証を受けた品質マネジメントシステムで開発されました。

■ ISO/IEC 15408 の認証

次に示す製品は，ISO/IEC 15408 に基づき EAL2 の認証を取得しました。
・P-9W62-3591 HiRDB Server Version 9 09-01（適用 OS：Red Hat Enterprise Linux 5 (AMD/Intel 64)）
なお，この認証は，製品そのものを保証しているのではなく，ISO/IEC 15408 による評価結果がその保証要件を満たしていることを意味するものです。
また，この製品を認証取得製品として使用するためには，最初にこのマニュアルを参照してシステムを構築・運用する必要があります。

■輸出時の注意

本製品を輸出される場合には，外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上，必要な手続きをお取りください。
なお，ご不明な場合は，弊社担当営業にお問い合わせください。

■商標類

■発行

2012 年 4 月　3020-6-459

■著作権

変更内容

変更内容 (3020-6-459)　HiRDB Version 9 09-01

追加・変更内容	変更個所
データロードを実行する場合，HiRDB 管理者と監査人が共同で実行するように記述を変更しました。	1.3.4(2)，4.2.2，7.3.1(3)
ISO/IEC 15408 の評価構成システムの OS を，AIX 5L V5.3 から Red Hat Enterprise Linux 5.6 (AMD/Intel 64) に変更しました。	2.2.4(1)，2.2.4(2)，5.3.1

単なる誤字・脱字などはお断りなく訂正しました。

変更内容 (3020-6-359-10)　HiRDB Version 8 08-04

追加・変更内容
マシンの設置および管理上の条件に，次の内容を追加しました。 • UAP の開発や実行についての説明 • 故障などの理由によって，一部のマシンの電源を切る場合の説明
HiRDB/ パラレルサーバの ISO/IEC 15408 評価構成システムのシステム構成を変更しました（マシン 2 のディクショナリサーバをマシン 1 へ移動しました)。
SQL 実行時の注意事項を追加しました。
システムジェネレータを使用する場合の注意として，HiRDB/ パラレルサーバで接続するホストについての説明を追加しました。
HiRDB システム定義の指定値の確認として，pd_sql_command_exec_users オペランドの説明を追加しました。
連続認証失敗許容回数とアカウントロック期間の設定に，アカウントロック状態解除時の確認についての説明を追加しました。
運用コマンド実行時の注意事項を追加しました。
HiRDB クライアントの設置場所に，次の内容を追加しました。 • ランタイムを経由しない電文についての説明 • HiRDB クライアントの OS アカウントについての説明 また，HiRDB クライアントで使用することを禁止しているハードウェアおよびソフトウェアについて，具体的な対策を追加しました。

はじめに

このマニュアルは，HiRDB システムのセキュリティ対策について説明したものです。

■対象読者

HiRDB システムの管理者，および HiRDB システム（データベース）の利用者の方を対象としています。
また，このマニュアルは次に示す知識があることを前提に説明しています。

HiRDB システムの管理者

- UNIX，Linux，または Windows のシステム管理の基礎的な知識
- HiRDB のシステム管理の基礎的な知識
- SQL の基礎的な知識

HiRDB システム（データベース）の利用者

- SQL の基礎的な知識

■マニュアルの構成

このマニュアルは，次に示す章から構成されています。

第 1 章　HiRDB のセキュリティ対策の概要
セキュリティ対策の考え方と HiRDB のセキュリティ機能について説明しています。

第 2 章　セキュアなシステムを構築するための条件
セキュアなシステムを構築するために必要な条件について説明しています。

第 3 章　HiRDB のセキュリティ設計
ユーザの管理，パスワードの管理，データベースのアクセス管理，およびリムーバブルメディアの管理について説明しています。

第 4 章　監査による利用状況の確認
監査で確認する項目と監査の手順について説明しています。

第 5 章　HiRDB の環境設定（UNIX の場合）
UNIX 版の HiRDB の環境設定方法について説明しています。

第 6 章　HiRDB の環境設定（Windows の場合）
Windows 版の HiRDB の環境設定方法について説明しています。

第 7 章　セキュアな環境を維持するための運用
セキュアな環境を維持するために必要な操作について説明しています。

第 8 章　HiRDB クライアントの管理
HiRDB クライアントの管理方法について説明しています。

■関連マニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

HiRDB（UNIX 用マニュアル）

- HiRDB Version 9 解説（UNIX(R) 用）（3000-6-451）
- HiRDB Version 9 システム導入・設計ガイド（UNIX(R) 用）（3000-6-452）
- HiRDB Version 9 システム定義（UNIX(R) 用）（3000-6-453）
- HiRDB Version 9 システム運用ガイド（UNIX(R) 用）（3000-6-454）
- HiRDB Version 9 コマンドリファレンス（UNIX(R) 用）（3000-6-455）

HiRDB（Windows 用マニュアル）

- HiRDB Version 9 解説（Windows(R) 用）（3020-6-451）
- HiRDB Version 9 システム導入・設計ガイド（Windows(R) 用）（3020-6-452）
- HiRDB Version 9 システム定義（Windows(R) 用）（3020-6-453）
- HiRDB Version 9 システム運用ガイド（Windows(R) 用）（3020-6-454）
- HiRDB Version 9 コマンドリファレンス（Windows(R) 用）（3020-6-455）

HiRDB（Windows，UNIX 共通マニュアル）

- HiRDB Version 9 UAP 開発ガイド（3020-6-456）
- HiRDB Version 9 SQL リファレンス（3020-6-457）
- HiRDB Version 9 メッセージ（3020-6-458）

なお，本文中で使用している HiRDB Version 9 のマニュアル名は，（UNIX(R) 用）または（Windows(R) 用）を省略して表記しています。使用しているプラットフォームに応じて UNIX 用または Windows 用のマニュアルを参照してください。

■読書手順

このマニュアルは，次の表に従ってお読みいただくことをお勧めします。

章または節タイトル		ユーザの種類	
		HiRDB システムの管理者	HiRDB システムの利用者
1. HiRDB のセキュリティ対策の概要		○	
2. セキュアなシステムを構築するための条件		○	
3. HiRDB のセキュリティ設計	3.1 ユーザの管理	○	
	3.2 パスワードの管理	○	○
	3.3 データベースのアクセス管理	○	
	3.4 データを格納したリムーバブルメディアの管理	○	
4. 監査による利用状況の確認		○	
5. HiRDB の環境設定（UNIX の場合）		○※	

章または節タイトル	ユーザの種類	
	HiRDB システムの管理者	HiRDB システムの利用者
6. HiRDB の環境設定（Windows の場合）	○※	
7. セキュアな環境を維持するための運用	○	
8. HiRDB クライアントの管理	○	○

（凡例）

○：必ず読んでいただきたい内容です。

注※ HiRDB の環境設定については，使用しているプラットフォームに応じて UNIX または Windows のどちらかを選択してお読みください。

■このマニュアルでの表記

このマニュアルでは製品名称および名称について次のように表記しています。ただし，それぞれのプログラムについての表記が必要な場合はそのまま表記しています。

製品名称または名称	表記	
HiRDB Server Version 9	HiRDB/ シングルサーバ	HiRDB または HiRDB サーバ
	HiRDB/ パラレルサーバ	
HiRDB/Developer's Kit Version 9	HiRDB/ Developer's Kit	HiRDB クライアント
HiRDB/Run Time Version 9	HiRDB/Run Time	
HiRDB Advanced High Availability Version 9	HiRDB Advanced High Availability	
HiRDB Control Manager	HiRDB CM	
HiRDB Control Manager - Agent	HiRDB CM Agent	
HiRDB Control Manager - Server	HiRDB CM Server	
HiRDB Control Manager - Console	HiRDB CM Console	
システムマネジャ	MGR	
フロントエンドサーバ	FES	
ディクショナリサーバ	DS	
バックエンドサーバ	BES	
HP-UX 11i V2 (IPF)	HP-UX または HP-UX (IPF)	
HP-UX 11i V3 (IPF)		
AIX 5L V5.2	AIX 5L	AIX
AIX 5L V5.3		

製品名称または名称	表記	
AIX V6.1	AIX V6.1	
Linux(R)	Linux	
Red Hat Enterprise Linux(R) AS 4(AMD64 & Intel EM64T)	Linux AS 4	Linux
Red Hat Enterprise Linux(R) AS 4(x86)		
Red Hat Enterprise Linux(R) ES 4(AMD64 & Intel EM64T)	Linux ES 4	
Red Hat Enterprise Linux(R) ES 4(x86)		
Red Hat Enterprise Linux(R) 5.1 Advanced Platform (x86)	Linux 5.1	
Red Hat Enterprise Linux(R) 5.1 (x86)		
Red Hat Enterprise Linux(R) 5.1 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.1 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.2 Advanced Platform (AMD/Intel 64)	Linux 5.2	
Red Hat Enterprise Linux(R) 5.2 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.3 Advanced Platform (AMD/Intel 64)	Linux 5.3	
Red Hat Enterprise Linux(R) 5.3 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.4 Advanced Platform (AMD/Intel 64)	Linux 5.4	
Red Hat Enterprise Linux(R) 5.4 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.6 (AMD/Intel 64)	Linux 5.6	
Red Hat Enterprise Linux(R) AS 4(AMD64 & Intel EM64T)	Linux (EM64T)	
Red Hat Enterprise Linux(R) ES 4(AMD64 & Intel EM64T)		
Red Hat Enterprise Linux(R) 5.1 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.1 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.2 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.2 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.3 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.3 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.4 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.4 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.6 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.1 Advanced Platform (x86)	Linux 5 (x86)	Linux 5
Red Hat Enterprise Linux(R) 5.1 (x86)		

製品名称または名称	表記	
Red Hat Enterprise Linux(R) 5.1 Advanced Platform (AMD/Intel 64)	Linux 5 (AMD/Intel 64)	
Red Hat Enterprise Linux(R) 5.1 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.2 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.2 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.3 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.3 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.4 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.4 (AMD/Intel 64)		
Red Hat Enterprise Linux(R) 5.6 (AMD/Intel 64)		
Microsoft(R) Windows(R) 2000 Professional Operating System	Windows 2000	
Microsoft(R) Windows(R) 2000 Server Operating System		
Microsoft(R) Windows(R) 2000 Datacenter Server Operating System		
Microsoft(R) Windows(R) 2000 Advanced Server Operating System		
Microsoft(R) Windows(R) 2000 Advanced Server Operating System	Windows 2000 Advanced Server	
Microsoft(R) Windows Server(R) 2003, Standard Edition	Windows Server 2003 Standard Edition	Windows Server 2003
Microsoft(R) Windows Server(R) 2003, Enterprise Edition	Windows Server 2003 Enterprise Edition	
Microsoft(R) Windows Server(R) 2003, Standard x64 Edition	Windows Server 2003 Standard x64 Edition	
Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition	Windows Server 2003 Enterprise x64 Edition	
Microsoft(R) Windows Server(R) 2003 R2, Standard Edition	Windows Server 2003 R2	
Microsoft(R) Windows Server(R) 2003 R2, Enterprise Edition		
Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition		
Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition		
Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition	Windows Server 2003 R2 x64 Editions	

製品名称または名称	表記	
Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition		
64 ビットバージョン Microsoft(R) Windows Server(R) 2003, Enterprise Edition	Windows Server 2003 (IPF)	
Microsoft(R) Windows Server(R) 2008 Standard	Windows Server 2008 Standard	Windows Server 2008
Microsoft(R) Windows Server(R) 2008 Enterprise	Windows Server 2008 Enterprise	
Microsoft(R) Windows Server(R) 2008 R2 Standard (x64)	Windows Server 2008 R2	
Microsoft(R) Windows Server(R) 2008 R2 Enterprise (x64)		
Microsoft(R) Windows Server(R) 2008 R2 Datacenter (x64)		
Microsoft(R) Windows Server(R) 2008 Standard (x64)	Windows Server 2008 (x64)	
Microsoft(R) Windows Server(R) 2008 Enterprise (x64)		
Microsoft(R) Windows Server(R) 2003, Standard x64 Edition	Windows Server 2003 x64 Editions	Windows (x64)
Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition		
Microsoft(R) Windows Server(R) 2003 R2, Standard x64 Edition		
Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition		
Microsoft(R) Windows(R) XP Professional x64 Edition	Windows XP x64 Edition	
64 ビットバージョン Microsoft(R) Windows Server(R) 2003, Enterprise Edition	Windows Server 2003 (IPF)	Windows(IPF)
Microsoft(R) Windows(R) XP Professional x64 Edition	Windows XP x64 Edition	Windows XP
Microsoft(R) Windows(R) XP Professional Operating System	Windows XP Professional	
Microsoft(R) Windows(R) XP Home Edition Operating System	Windows XP Home Edition	
Microsoft(R) Windows Vista(R) Home Basic	Windows Vista Home Basic	Windows Vista
Microsoft(R) Windows Vista(R) Home Premium	Windows Vista Home Premium	
Microsoft(R) Windows Vista(R) Ultimate	Windows Vista Ultimate	
Microsoft(R) Windows Vista(R) Business	Windows Vista Business	
Microsoft(R) Windows Vista(R) Enterprise	Windows Vista Enterprise	

製品名称または名称	表記	
Microsoft(R) Windows Vista(R) Home Basic (x64)	Windows Vista (x64)	
Microsoft(R) Windows Vista(R) Home Premium (x64)		
Microsoft(R) Windows Vista(R) Ultimate (x64)		
Microsoft(R) Windows Vista(R) Business (x64)		
Microsoft(R) Windows Vista(R) Enterprise (x64)		
Microsoft(R) Windows(R) 7 Home Premium	Windows 7 Home Basic	Windows 7
Microsoft(R) Windows(R) 7 Professional	Windows 7 Professional	
Microsoft(R) Windows(R) 7 Enterprise	Windows 7 Enterprise	
Microsoft(R) Windows(R) 7 Ultimate	Windows 7 Ultimate	
Microsoft(R) Windows(R) 7 Home Premium (x64)	Windows 7 (x64)	
Microsoft(R) Windows(R) 7 Professional (x64)		
Microsoft(R) Windows(R) 7 Enterprise (x64)		
Microsoft(R) Windows(R) 7 Ultimate (x64)		

- Windows Server 2003 および Windows Server 2008 を総称して Windows Server と表記します。また，Windows 2000，Windows XP，Windows Server，Windows Vista，および Windows 7 を総称して Windows と表記します。
- HiRDB 運用ディレクトリのパスを $PDDIR と表記します。Windows の場合は %PDDIR% と表記します。

■このマニュアルで使用する略語

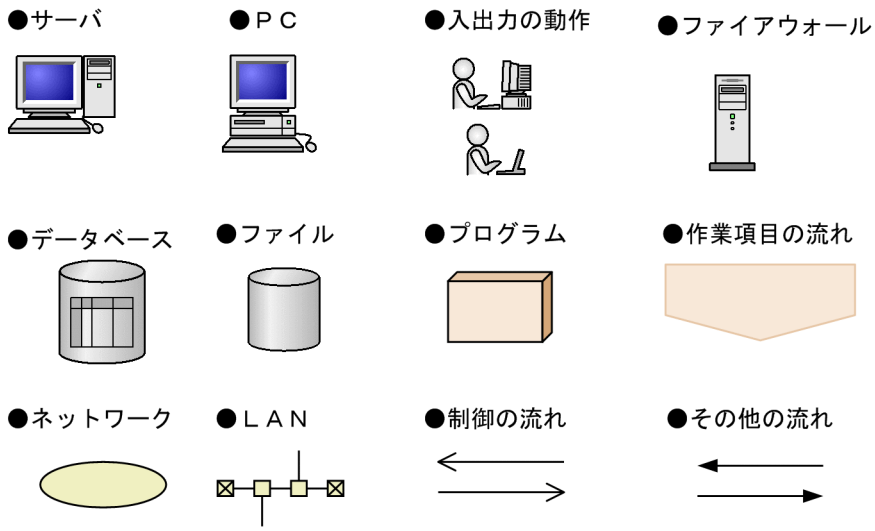
このマニュアルで使用する英略語の一覧を次に示します。

英略語	英字の表記
CD-ROM	Compact Disc - Read Only Memory
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
IPF	Itanium(R) Processor Family
LAN	Local Area Network
OS	Operating System
PC	Personal Computer
PP	Program Product

英略語	英字の表記
RD	Relational Database
UAP	User Application Program

■図中で使用する記号

このマニュアルの図中で使用する記号を次のように定義します。



■このマニュアルで使用する記号

このマニュアルで使用する記号を次に示します。ここで説明する記号は，説明のための記号なので実際には記述しないでください。

記号	意味
〔 〕	この記号で囲まれている項目は省略できます。 （例）pdbuffer 〔-p〕 これは，pdbuffer と指定するか，または pdbuffer -p と指定することを示します。
…	この記号の直前の項目を繰り返して指定できます。 （例）pdbuffer -r RD エリア名 〔, RD エリア名〕… これは，-r オプションの RD エリア名を繰り返し指定できることを示します。
|	この記号で区切られた項目は選択できます。 （例）pdlogadfg -d {sys | spd} これは，-d オプションに sys か spd のどちらかを指定できることを示します。
{ }	この記号で囲まれている複数の項目のうちから，一つを選択できます。 （例）pdbuffer 〔{-r RD エリア名 | -i 認可識別子 . インデクス識別子 | -o}〕 これは，-r RD エリア名，-i 認可識別子 . インデクス識別子，-o の三つのオプションのうち，どれか一つを指定することを示します。

■セキュリティ関連の情報について

(株)日立製作所 ソフトウェア事業部が開発・提供する，ソフトウェア製品のセキュリティに関する情報については，下記 URL で提供しています。HiRDB に関するセキュリティ上の問題が明らかになった場合には，こちらのサイトで情報を提供しますので，定期的なチェックをお願いします。

http://www.hitachi.co.jp/Prod/comp/soft1/security/

■ HiRDB の技術的なお問い合わせについて

サポートサービス契約を結んでいるユーザは，サポートサービスにお問い合わせください。サポートサービス契約を結んでいないユーザは，担当の営業，SE，または下記 URL の「お問い合わせ：ミドルウェア」からお問い合わせください。

http://www.hitachi.co.jp/Prod/comp/soft1/ask/index.html

目次

1 HiRDB のセキュリティ対策の概要

この章では，セキュリティ対策の考え方と HiRDB のセキュリティ機能について説明します。

1.1 このマニュアルの使い方

ここでは，このマニュアルの目的と使い方について説明します。

(1) このマニュアルの目的

HiRDB システムのセキュリティを強化する必要がある場合にこのマニュアルをお読みください。

マニュアル「HiRDB Version 9 システム導入・設計ガイド」にもシステムの構築方法が説明されていますが，セキュリティを強化し，よりセキュアなシステムを構築する場合は，このマニュアルで説明している操作に従って，システムを構築・運用してください。

(2) このマニュアルの読み方

このマニュアルの 1 章～ 4 章はシステムを構築する前にお読みください。5 章または 6 章は HiRDB の環境設定時に，7 章は運用時にお読みください。また，8 章は HiRDB クライアントの環境設定および運用のときにお読みください。

このマニュアルでは操作方法（ユティリティ，コマンド，SQL の使い方など）を説明していません。詳細な操作方法については，次に示すマニュアルの該当個所を参照させています。

- HiRDB Version 9 解説
- HiRDB Version 9 システム導入・設計ガイド
- HiRDB Version 9 システム定義
- HiRDB Version 9 システム運用ガイド
- HiRDB Version 9 コマンドリファレンス
- HiRDB Version 9 UAP 開発ガイド
- HiRDB Version 9 SQL リファレンス

特に次の表に示すマニュアルと関係が深いため，該当個所も併せてお読みいただくことをお勧めします。

また，システム定義，コマンド，クライアント環境定義，SQL などは，HiRDB のマニュアルに記載されていないものは使用しないでください。

表 1-1 このマニュアルと関係の深いマニュアル

マニュアル名	該当個所	内容
HiRDB Version 9 システム運用ガイド	機密保護機能	DBA 権限，スキーマ定義権限，CONNECT 権限，および表のアクセス権限について説明しています。
	CONNECT 関連セキュリティ機能	パスワードのセキュリティ対策（パスワードの禁止条件の設定および連続認証失敗許容回数の設定）について説明しています。
	セキュリティ監査機能	監査情報の取得方法について説明しています。
HiRDB Version 9 SQL リファレンス	定義系 SQL の GRANT	権限を与える SQL について説明しています。
	定義系 SQL の CREATE AUDIT	監査対象イベントを定義する SQL について説明しています。

1.2 セキュリティ対策の考え方

ここでは，セキュリティ対策の重要性とセキュリティ上の脅威について説明します。

(1) セキュリティ対策の重要性

システムのセキュリティ対策が十分でないと，顧客情報などの機密性の高い情報が漏えいしたり，改ざんされたりするおそれがあります。このような事態が発生すると，組織の社会的信用は失墜し，大きな経済的損失を招きます。このように，システムのセキュリティ対策を怠ると，大きなビジネス上のリスクが生じる可能性があります。システムの管理者はこのようなビジネス上のリスクを回避するために，機密性の高い情報を管理しているシステムのセキュリティを強化する必要があります。

(2) 管理者が認識しておく必要があるセキュリティ上の脅威

システムの管理者は次に示すようなセキュリティ上の脅威を認識し，それに対して十分な対策を行う必要があります。

- データへの不正なアクセス
- データの漏えい，改ざん，破壊
- システムの不正利用

これらの脅威は組織外（インターネット）だけではなく，組織内にも存在します。組織内に存在するセキュリティ上の脅威を次に示します。

- 権限の範囲を超えたデータへの不正なアクセス
- 組織内の人間によるデータの持ち出し（漏えい，改ざん，破壊も含む）
- 権限の範囲を超えたシステムの不正利用

(3) 必要なセキュリティ対策

(2) で説明したセキュリティ上の脅威に対して，管理者は次に示すようなセキュリティ対策を行う必要があります。

- ファイアウォールなどのセキュリティ機器による対策
- マシンルームの設置などによる物理的対策
- 使用するソフトウェアのセキュリティ対策
- セキュリティ面の管理・運用ルールの設定による対策
- 利用者のセキュリティ教育などによる人的対策

ポイント

システムのセキュリティ対策は，HiRDB だけでなく，OS やネットワークなども含めて包括的に行う必要があります。HiRDB だけでセキュリティ対策を行っても，期待したセキュリティ効果が得られません。また，ソフトウェアやハードウェアのセキュリティ対策だけではなく，利用者のセキュリティ教育なども必要です。
また，システムの利用者全員（管理者も含む）がセキュリティ対策を継続して行うことが重要です。

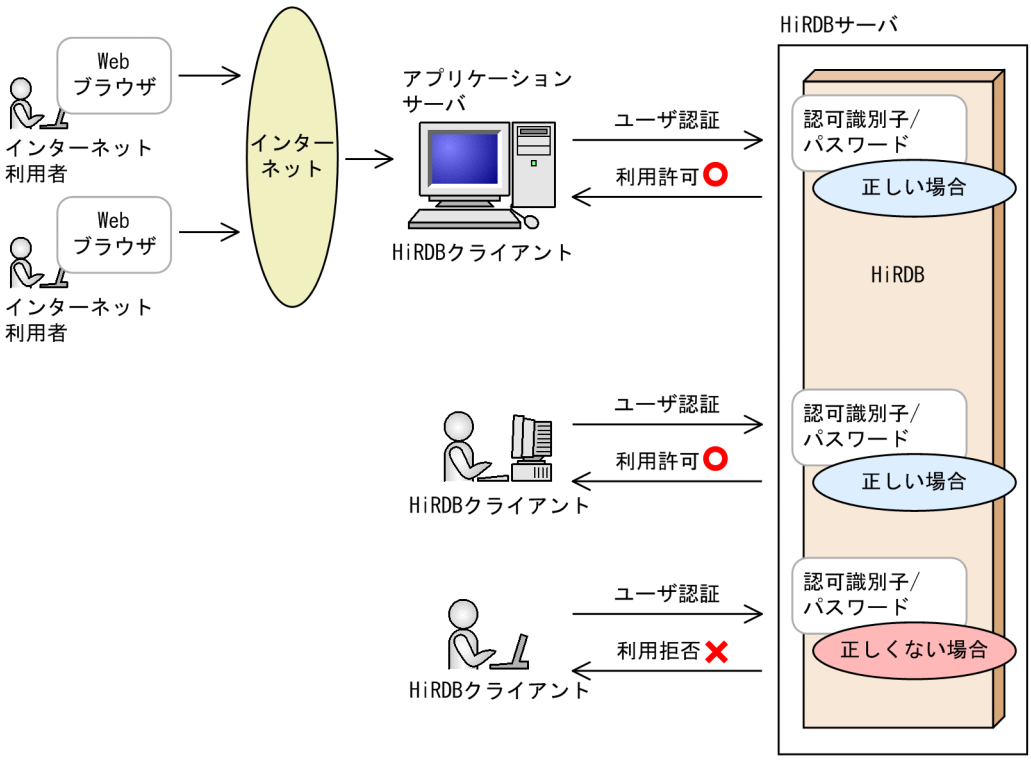
1.3　HiRDB のセキュリティ機能

ここでは，HiRDB のセキュリティ機能について説明します。

1.3.1　ユーザ認証

HiRDB では**認可識別子**と**パスワード**を使用してユーザ認証を行います。HiRDB はユーザ認証によって正規の利用者かどうかを確認し，第三者による HiRDB の不正利用を防止しています。HiRDB を利用するときに使用する認可識別子とパスワードが正しい場合は HiRDB の利用が許可され，正しくない場合は HiRDB の利用が拒否されます。
HiRDB のユーザ認証の仕組みを次の図に示します。

図 1-1　HiRDB のユーザ認証の仕組み



説明

- 正しい認可識別子とパスワードを使用した場合は，HiRDB の利用が許可されます。認可識別子またはパスワードに誤りがある場合は，HiRDB の利用が拒否されます。
- アプリケーションサーバを使用している場合，インターネット利用者の操作の延長で，アプリケーションサーバから HiRDB に対して SQL が発行されます。この

場合，通常はアプリケーションサーバの HiRDB クライアントを利用する，データベース利用者に与えられている認可識別子とパスワードでユーザ認証が行われます。

参考

- パスワードの不正入力によってユーザ認証に連続して失敗した場合，その認可識別子に対して HiRDB の利用を一定期間禁止できます。詳細については，「3.2.4　アカウントの不正使用対策」を参照してください。
- HiRDB のコマンドおよびユティリティを実行する場合，OS アカウントによって識別されます（HiRDB のユーザ認証は行われません）。
- アプリケーションサーバは ISO/IEC 15408 の評価構成に含まれません。ISO/IEC 15408 の評価構成となるシステムについては，「2.2.4　ISO/IEC 15408 の評価を行ったシステム構成」を参照してください。

1.3.2　権限による操作の制御

HiRDB を利用（操作）するには**権限**が必要になります。与えられた権限によって実行できる操作が制御されています。利用者ごとに目的に応じた権限を与えることで，不正な操作が行われる可能性を低くできます。

HiRDB の権限の種類を表 1-2 に，権限の種類と実行できる操作を表 1-3 に示します。

参考

- 表のアクセス権限はここでいう権限に含まれていません。表のアクセス権限については，「1.3.3　データベースのアクセス制御」を参照してください。
- 表 1-2 に示す権限を持っている HiRDB の利用者を HiRDB **ユーザ**といいます。

表 1-2　HiRDB の権限の種類

権限の種類	説明
DBA 権限	監査人以外の HiRDB ユーザを管理するために必要な権限です。この権限があると，ほかの HiRDB ユーザに権限（DBA 権限，スキーマ定義権限，および CONNECT 権限）を与えたり，削除したりできます。また，ほかの HiRDB ユーザが所有する表を削除できます。 なお，DBA 権限は，スキーマ定義権限と CONNECT 権限を含んでいます。つまり，DBA 権限を有するということは，スキーマ定義権限および CONNECT 権限を有するということです。したがって，スキーマを定義して表を定義できます。
スキーマ定義権限	スキーマを定義するために必要な権限です。スキーマを定義すると，表を定義できます。ただし，スキーマを定義するには CONNECT 権限も必要になります。

権限の種類	説明
CONNECT 権限	HiRDB を利用するために必要な権限です。CONNECT 権限がない利用者は HiRDB を利用できません。 また，表の所有者から表のアクセス権限を与えてもらうと，その表に対してアクセスできるようになります。
監査権限	HiRDB システムの監査をするために必要な権限です。この権限を有する HiRDB ユーザを**監査人**といいます。監査人の登録時に，監査権限，CONNECT 権限，およびスキーマ定義権限が同時に与えられます。 監査権限は HiRDB 管理者から与えてもらいます。

参考

これらの権限の詳細（権限の説明と実行できる操作）については，次に示すマニュアルを参照してください。

- 「HiRDB Version 9 システム運用ガイド」には，これらの権限の説明がされています。
- 「HiRDB Version 9 コマンドリファレンス」には，各コマンドおよびユティリティ実行時に必要な権限が説明されています。
- 「HiRDB Version 9 SQL リファレンス」には，権限を付与または削除する SQL（REVOKE，GRANT）と SQL 実行時に必要な権限が説明されています。

表 1-3　権限の種類と実行できる操作

権限の種類	操作			
	権限の付与および削除	表の定義	表へのアクセス	監査
DBA 権限	○	○	○※1	×
スキーマ定義権限	×	○※2	×	×
CONNECT 権限	×	×	○※1	×
監査権限	×	○	○※1	○

（凡例）

○：実行できます。

×：実行できません。

注※ 1

表にアクセスするには，その表に対するアクセス権限が必要になります。アクセス権限については，「1.3.3　データベースのアクセス制御」を参照してください。

注※ 2

表を定義するには，スキーマを定義する必要があります。スキーマを定義するには，スキーマ定義権限と CONNECT 権限が必要になります。

1.3.3　データベースのアクセス制御

HiRDB では，**表のアクセス権限**によってデータベースのアクセス制御が行われています。表のアクセス権限がないと，その表にあるデータにアクセスできません。アクセス権限を適切に管理することによって，データの機密性を高め，セキュリティを強化できます。

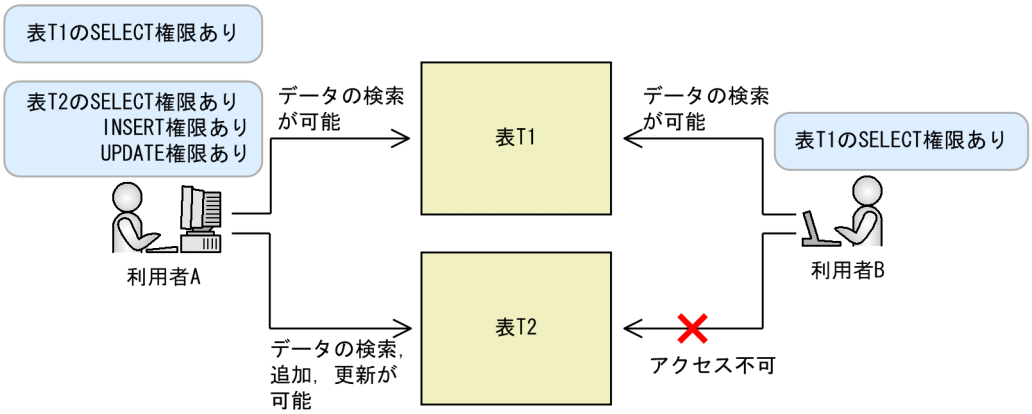
表のアクセス権限には次の表に示す種類があります。権限の種類によって，表に対して実行できる操作が異なります。

表 1-4　表のアクセス権限の種類

表のアクセス権限の種類	表に対してできる操作
SELECT 権限	表のデータを検索（SELECT）できます。
INSERT 権限	表にデータを追加（INSERT）できます。
DELETE 権限	表のデータを削除（DELETE）できます。
UPDATE 権限	表のデータを更新（UPDATE）できます。

表のアクセス権限によるデータベースのアクセス制御を次の図に示します。

図 1-2　表のアクセス権限によるデータベースのアクセス制御



説明

利用者 A と利用者 B の表の操作の実行可否を次に示します。

利用者	操作対象の表	操作内容	実行可否
利用者 A	表 T1	データの検索（SELECT）	○
		データの追加（INSERT）	×
		データの削除（DELETE）	×
		データの更新（UPDATE）	×

利用者	操作対象の表	操作内容	実行可否
	表 T2	データの検索（SELECT）	○
		データの追加（INSERT）	○
		データの削除（DELETE）	×
		データの更新（UPDATE）	○
利用者 B	表 T1	データの検索（SELECT）	○
		データの追加（INSERT）	×
		データの削除（DELETE）	×
		データの更新（UPDATE）	×
	表 T2	データの検索（SELECT）	×
		データの追加（INSERT）	×
		データの削除（DELETE）	×
		データの更新（UPDATE）	×

（凡例）
○：実行できます。
×：実行できません。

表のアクセス権限の詳細については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

1.3.4 監査

システムの不正利用がないか，組織のセキュリティポリシーに従った運用が行われているかなど，HiRDB のセキュリティ機能が意図したとおりに働いているかを定期的に確認（監査）する必要があります。この監査のために必要な情報を**セキュリティ監査機能**を使用して取得できます。この情報には，だれが，いつ，どのオブジェクトに対してどのような操作をしたか，またそのとき使用した権限や，その操作（イベント）が成功したかどうかが記録されます。

ポイント

監査は 1.3.1 ～ 1.3.3 で説明したセキュリティ機能と異なり，直接的なセキュリティ効果はありません。ただし，このあとの「(1) 監査の目的」で説明するように，総合的にセキュリティ効果を高めています。特に組織内の脅威に対して監査は有効な手段であると考えられます。

セキュリティ監査機能の詳細については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

(1) 監査の目的

監査の目的を次に示します。

● 不審なアクセスがないかを確認する
データベースに対して不審なアクセスが行われていないかを確認します。

● 利用者の不正行為に対する抑止効果をねらう
監査を実施していることを組織内にアナウンスすると，組織内の悪意を持った利用者の次に示す行為を心理的に抑止できると考えられます。

- 不正にデータベースにアクセスする
- データを改ざんする
- データを持ち出す

また，正当な利用者に対しても，システムの正しい使い方についての注意を促す効果が期待できます。

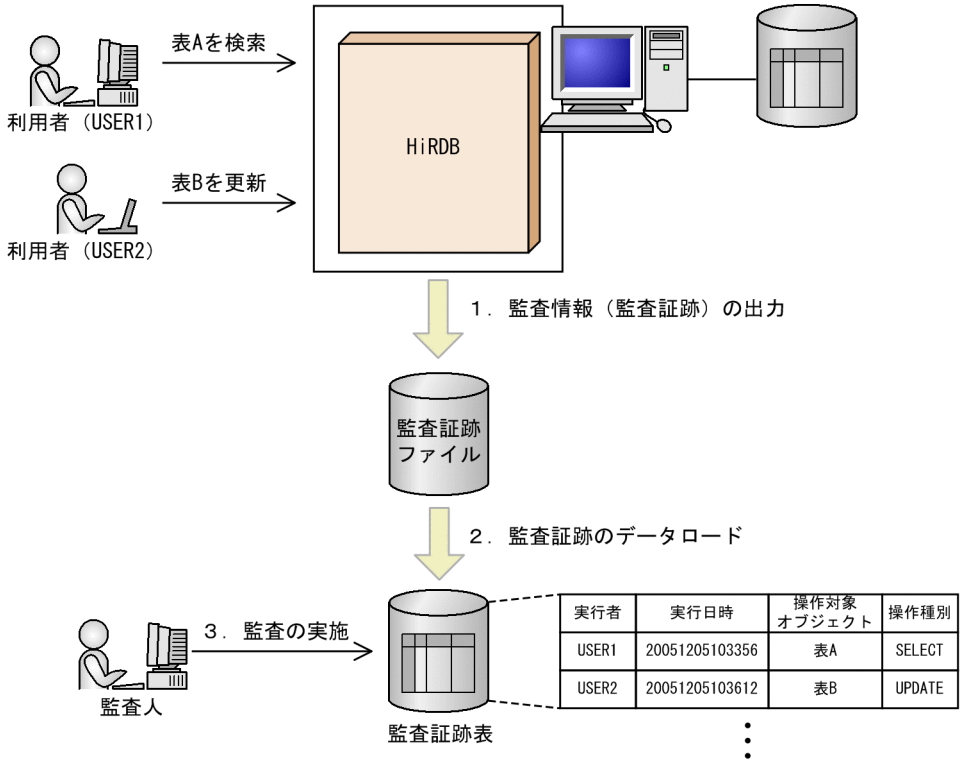
● セキュリティポリシーに従った運用が行われているかを確認する
パスワードの定期変更や，与えられた権限に沿った操作など，組織のセキュリティポリシーに従った運用が行われているかを確認します。

● セキュリティ上のリスクを分析する
監査結果からセキュリティ上のリスクを分析し，それをセキュリティ対策に反映します。

(2) 監査情報の出力と参照方法

利用者の操作によって監査情報の取得対象となるイベントが発生した場合に，監査情報が出力されます。**監査人**はその監査情報を参照して監査を実施します。監査情報の出力と参照方法の概要を次の図に示します。

図 1-3 監査情報の出力と参照方法の概要



説明

1. 利用者の操作によって監査情報取得対象イベントが発生した場合，監査情報（**監査証跡**）が監査証跡ファイルに出力されます。
2. 監査情報を SQL で検索できるようにするために，監査証跡ファイルの内容を**監査証跡表**にデータロードします。データロードは HiRDB 管理者と監査人が共同で実行します。
3. SQL で監査証跡表を検索し，監査情報を確認します。

参考

監査証跡表の改ざんを防止するために，監査証跡表へのデータの追加および更新（INSERT および UPDATE）はできなくなっています。データの削除（DELETE）は監査人だけが実行できます。

2 セキュアなシステムを構築するための条件

この章では，セキュアなシステムを構築するために必要な条件について説明します。

2.1 セキュアなシステムに必要な条件

システムのセキュリティを強固にするには，HiRDB のセキュリティ機能を使用するだけではなく，システム構成，マシンの設置場所，OS，ネットワークなどとあわせてセキュリティ対策する必要があります。これらのうちの一つでも対策が十分でないと，その部分がセキュリティ上の弱点となります。したがって，セキュアなシステムを構築するためには，次に示すことに対して十分な検討・対策を行う必要があります。

- システム構成の条件が満たされている
- HiRDB サーバの設置場所のセキュリティが守られている
- OS に必要な条件が満たされている
- ネットワークに必要な条件が満たされている

各項目の詳細については，次節以降で順に説明していきます。

2.2　システム構成の条件

ここでは，セキュアなシステムを構築・運用するために必要なシステム構成の条件について説明します。

なお，ISO/IEC 15408 の評価は，「2.2.4　ISO/IEC 15408 の評価を行ったシステム構成」に示すシステム構成下で行われました。

2.2.1　マシンの設置および管理上の条件

セキュアなシステムを構築し，運用するためには次のことを守ってください。

- 不要なソフトウェアはインストールしないでください。インストールするソフトウェアの数が多くなるほど，システムの管理や，セキュリティ対策が複雑になるため，セキュリティ上のリスクが高くなります。
- 通常の業務で使用するマシンとは別に，監査業務で使用するマシンを設置してください。監査業務で使用するマシンと通常の業務で使用するマシンを一緒にすると，監査情報が漏れるなどのセキュリティ上のリスクが高くなります。
- 故障などの理由によって，HiRDB/ パラレルサーバを構成する一部のマシンの電源を切る場合，そのマシンから他マシンへのログインの許可を取り消してください。HiRDB/ パラレルサーバを構成するマシン以外からのログイン（IP アドレスの詐称）を，確実に排除することが目的です。

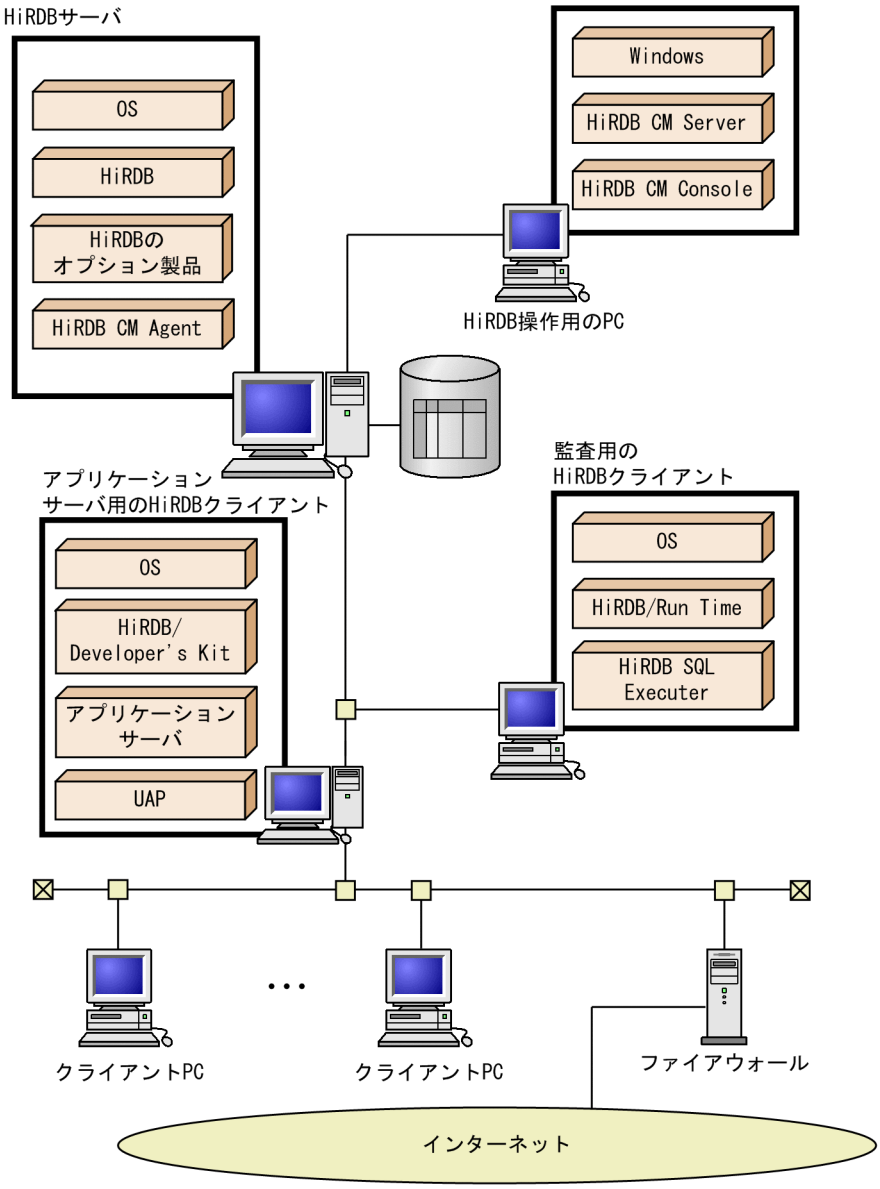
2.2.2　アプリケーションサーバを使用した三階層型システムを構築する場合

アプリケーションサーバを使用した三階層型システムを構築する場合，次のことを守ってください。

- アプリケーションサーバを構築したマシンは HiRDB クライアントとして動作しますが，この HiRDB クライアントは HiRDB サーバと同じレベルで管理してください。

アプリケーションサーバを使用した三階層型システムの構成例を次の図に示します。

図 2-1 アプリケーションサーバを使用した三階層型システムの構成例



説明

組織内のデータベース利用者が，クライアント PC を操作してアプリケーションサーバ上の UAP を利用します。この操作の延長で，アプリケーションサーバから HiRDB サーバに対して SQL が発行されてデータベースをアクセスします。クライアント PC からは，データベースに直接アクセスできないようにしてください。

2.2.3　クライアントサーバ型システムを構築する場合

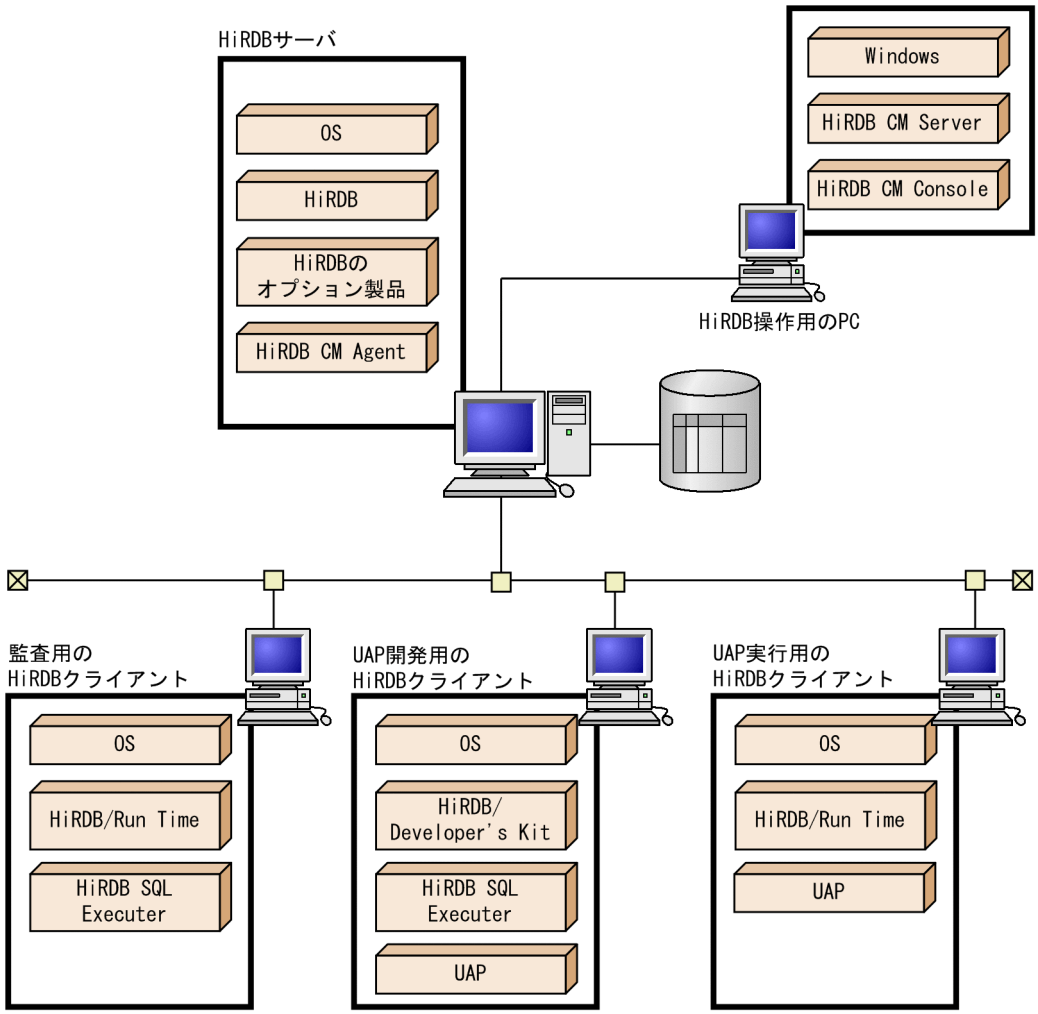
クライアントサーバ型システムを構築する場合，次のことを守ってください。

- 実際の作業にあった HiRDB クライアントを各データベース利用者に与えてください。

UAP 管理者には UAP 開発用の HiRDB クライアント（HiRDB/Developer's Kit）を，UAP 実行者には UAP 実行用の HiRDB クライアント（HiRDB/Run Time）を与えてください。UAP の実行だけを行うデータベース利用者に，UAP 開発用の HiRDB クライアントを与えないでください。

クライアントサーバ型システムの構成例を次の図に示します。

図 2-2　クライアントサーバ型システムの構成例



説明

組織内のデータベース利用者が，HiRDB SQL Executer または UAP を実行し，HiRDB クライアントからデータベースにアクセスします。

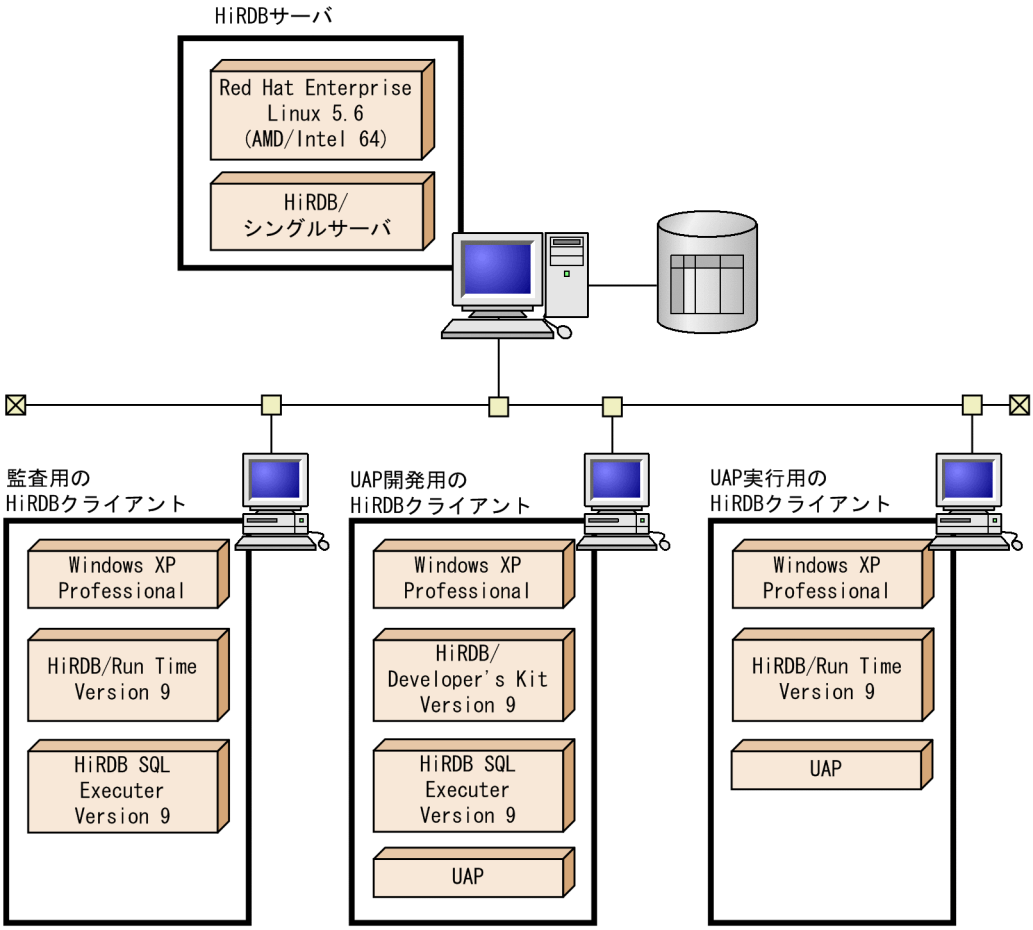
2.2.4 ISO/IEC 15408 の評価を行ったシステム構成

ISO/IEC 15408 の評価はここで説明する条件下で行われました。

(1) システム構成

ISO/IEC 15408 の評価は図 2-3 および図 2-4 に示すシステム構成で行われました。ISO/IEC 15408 の評価構成システム（HiRDB/ シングルサーバの場合）を図 2-3 に，ISO/IEC 15408 の評価構成システム（HiRDB/ パラレルサーバの場合）を図 2-4 に示します。

図 2-3 ISO/IEC 15408 の評価構成システム（HiRDB/ シングルサーバの場合）



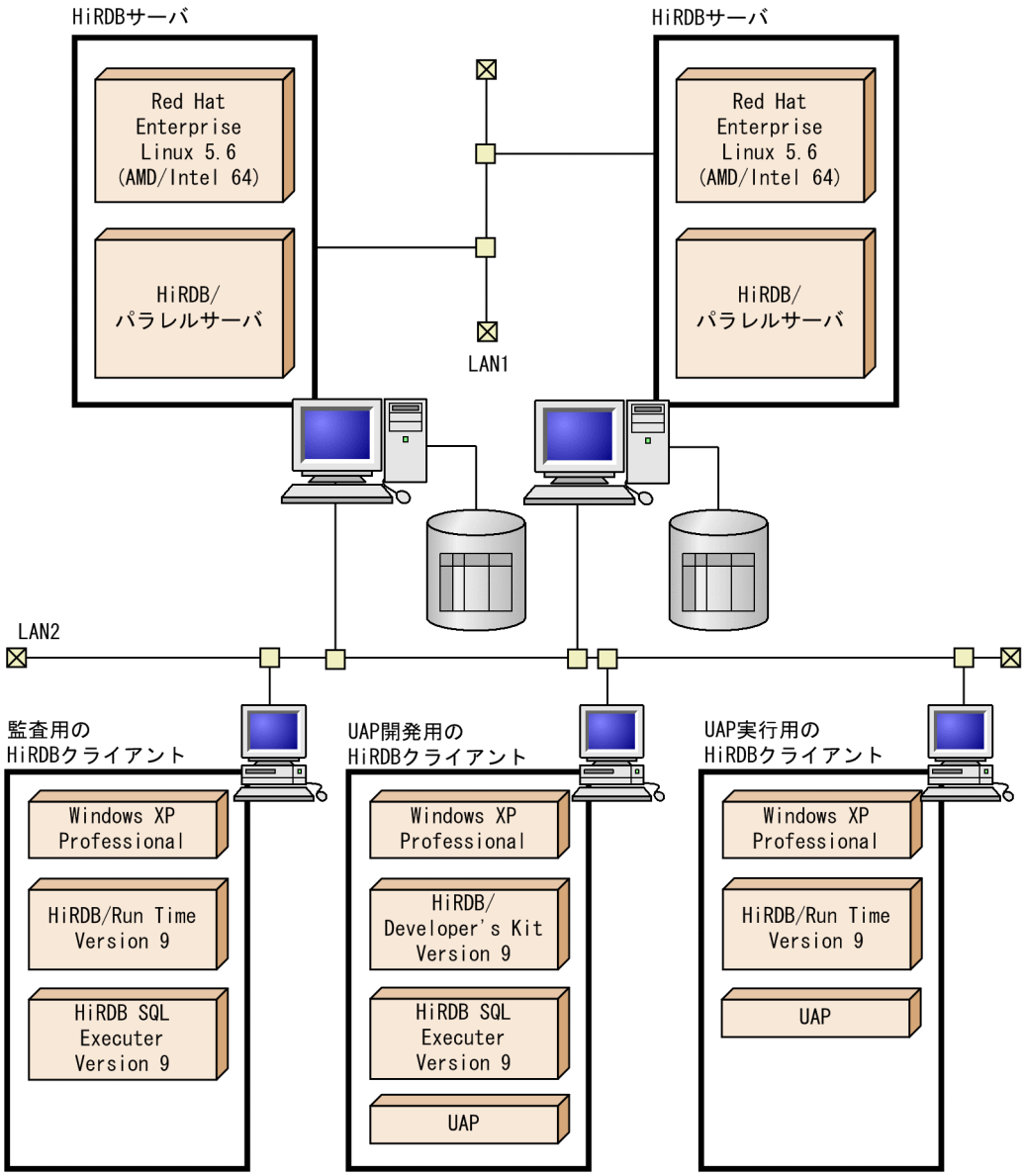
説明

- 監査用，UAP 開発用，および UAP 実行用の 3 台の HiRDB クライアントを設置

し，各 HiRDB クライアントから HiRDB SQL Executer Version 9 または UAP を実行して HiRDB のデータベースにアクセスします。

- 監査用の HiRDB クライアントを設置し，その HiRDB クライアントで監査人が監査情報を検索します。
- UAP 開発用と UAP 実行用の HiRDB クライアントを設置し，それぞれの HiRDB クライアントで UAP を開発，実行します。

図 2-4　ISO/IEC 15408 の評価構成システム（HiRDB/ パラレルサーバの場合）



説明

- HiRDB/ パラレルサーバは 2 台のマシンで構成されています。マシン 1 のユニットにはシステムマネジャ，フロントエンドサーバ，ディクショナリサーバ，およびバックエンドサーバが定義されています。マシン 2 のユニットにはフロントエンドサーバ，およびバックエンドサーバが定義されています。
- HiRDB サーバを構成するマシン間で使用するローカルエリアネットワーク（LAN1）と，HiRDB クライアントと HiRDB サーバ間で使用するローカルエリアネットワーク（LAN2）は，異なるローカルエリアネットワークを使用しています。
  LAN1 は HiRDB/ パラレルサーバを構成するマシン 1 とマシン 2 を，LAN2 は HiRDB サーバと HiRDB クライアントを接続するためのものです。
- 監査用，UAP 開発用，および UAP 実行用の 3 台の HiRDB クライアントを設置し，各 HiRDB クライアントから HiRDB SQL Executer Version 9 または UAP を実行して HiRDB のデータベースにアクセスします。
- 監査用の HiRDB クライアントを設置し，その HiRDB クライアントで監査人が監査情報を検索します。
- UAP 開発用と UAP 実行用の HiRDB クライアントを設置し，それぞれの HiRDB クライアントで UAP を開発，実行します。

（2）HiRDB サーバのソフトウェア構成

ISO/IEC 15408 の評価を行ったときの HiRDB サーバのソフトウェア構成を次の表に示します。

表 2-1　HiRDB サーバのソフトウェア構成

使用したソフトウェア	説明
OS	Red Hat Enterprise Linux 5.6 (AMD/Intel 64) を使用しました。
HiRDB	次に示す製品を使用しました。 • P-9W62-3591 HiRDB Server Version 9 09-01

（3）HiRDB クライアントのソフトウェア構成

監査用，UAP 開発用，および UAP 実行用の HiRDB クライアントを設置しました。
ISO/IEC 15408 の評価を行ったときの HiRDB クライアントのソフトウェア構成を次の表に示します。

表 2-2　監査用の HiRDB クライアントのソフトウェア構成

使用したソフトウェア	説明
OS	Windows XP Professional を使用しました。
HiRDB/Run Time Version 9	UAP を実行するために必要な製品です。また，HiRDB SQL Executer Version 9 の前提製品です。HiRDB/Run Time Version 9 は，次に示す製品を使用しました。 • P-2662-1194 HiRDB/Run Time Version 9 09-01

使用したソフトウェア	説明
HiRDB SQL Executer Version 9	HiRDB SQL Executer Version 9 を使用すると，PC の画面から SQL を実行し，その結果を確認できます。監査証跡表を検索するツールとして使用します。HiRDB SQL Executer Version 9 は，次に示す製品を使用しました。 • R-F15427-197 HiRDB SQL Executer 09-01

表 2-3　UAP 開発用の HiRDB クライアントのソフトウェア構成

使用したソフトウェア	説明
OS	Windows XP Professional を使用しました。
HiRDB/Developer's Kit Version 9	UAP を開発するために必要な製品です。UAP の実行もできます。また，HiRDB SQL Executer Version 9 の前提製品です。HiRDB/Developer's Kit Version 9 は，次に示す製品を使用しました。 • P-2662-1294 HiRDB/Developer's Kit Version 9 09-01
HiRDB SQL Executer Version 9	HiRDB SQL Executer Version 9 を使用すると，PC の画面から SQL を実行し，その結果を確認できます。UAP を開発するときのツールとして使用します。HiRDB SQL Executer Version 9 は，次に示す製品を使用しました。 • R-F15427-197 HiRDB SQL Executer 09-01

表 2-4　UAP 実行用の HiRDB クライアントのソフトウェア構成

使用したソフトウェア	説明
OS	Windows XP Professional を使用しました。
HiRDB/Run Time Version 9	UAP を実行するために必要な製品です。HiRDB/Run Time Version 9 は，次に示す製品を使用しました。 • P-2662-1194 HiRDB/Run Time Version 9 09-01

2.3 HiRDB サーバの設置場所の条件

ここでは，HiRDB サーバの設置場所の条件について説明します。HiRDB クライアントの設置場所については，「8.1.1 HiRDB クライアントの設置」を参照してください。

2.3.1 セキュアエリアの確保

(1) セキュアエリアとは

システムやネットワークのセキュリティをいくら強化しても，HiRDB サーバを設置するマシンルームの出入りが自由になっていると，管理者以外の人間が HiRDB サーバを不正に操作したり，データを持ち出したりするおそれがあります。

したがって，セキュアなシステムを構築するには，システム環境だけではなく，HiRDB サーバを設置する場所の管理にも注意を払う必要があります。人の入退室管理が行われ，不正な物理的アクセスから保護されたエリア（これを**セキュアエリア**といいます）を確保し，このエリア内に HiRDB サーバを設置してください。

参考

セキュアエリアとするマシンルームを施錠したり，監視カメラを設置したり，警備員を配置したりするとセキュリティ効果が高くなります。

(2) セキュアエリアに設置する機器

セキュアエリアには，次に示すマシンとその周辺機器を設置してください。

- HiRDB サーバ用のマシン
- アプリケーションサーバ用のマシン（三階層型システムの場合）

セキュアエリアは，許可された人（スーパユーザ※，HiRDB 管理者，DBA 権限保持者，表の所有者，および監査人）だけが入場できるように管理してください。

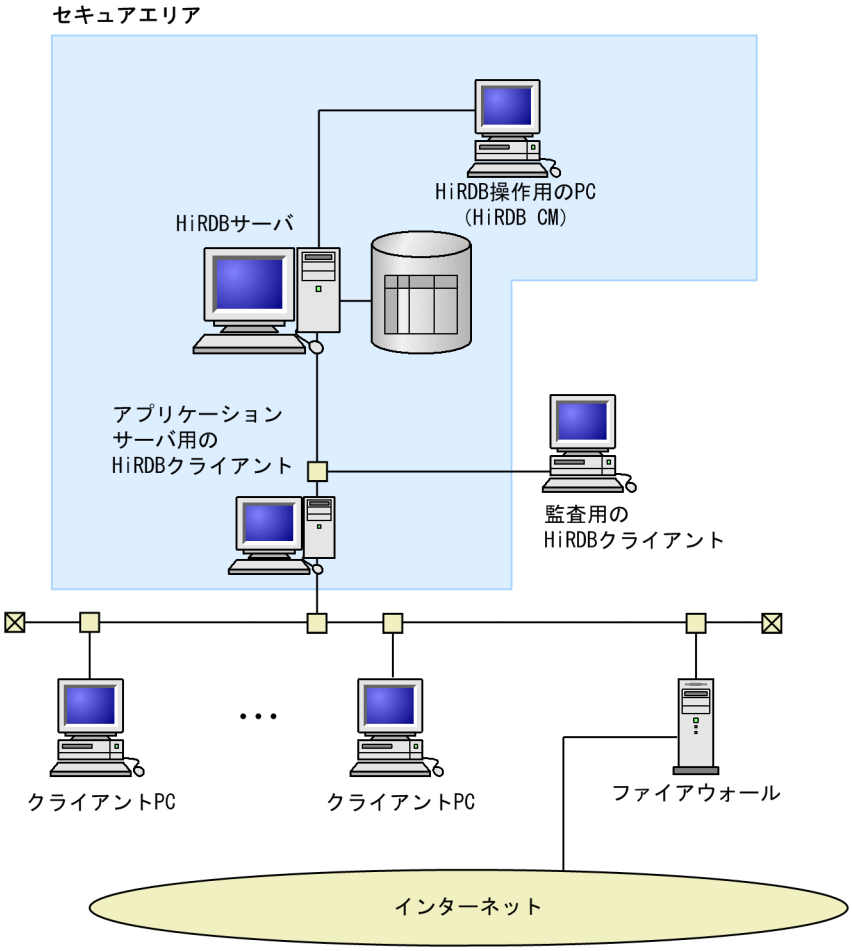
注※

使用するシステムが Windows の場合，Administrator 権限を持つマシンの管理者となります。

なお，HiRDB CM を使用して HiRDB を操作する場合，HiRDB CM Server，HiRDB CM Console をインストールしたマシンをセキュアエリア内に設置するなどの対策を行い，HiRDB サーバがそのマシンから不正操作されることがないようにしてください。

アプリケーションサーバを使用した三階層型システムと，クライアントサーバ型システムのセキュアエリアを次の図に示します。

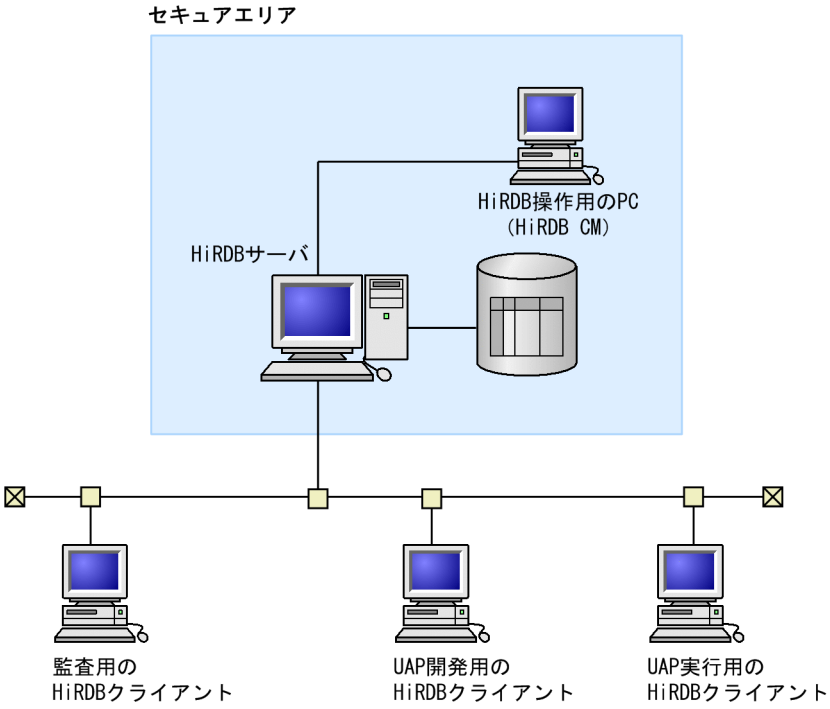
図 2-5　アプリケーションサーバを使用した三階層型システムのセキュアエリア



注

HiRDB/ パラレルサーバの場合は，HiRDB/ パラレルサーバを構成するすべてのマシンをセキュアエリア内に設置してください。

図 2-6 クライアントサーバ型システムのセキュアエリア



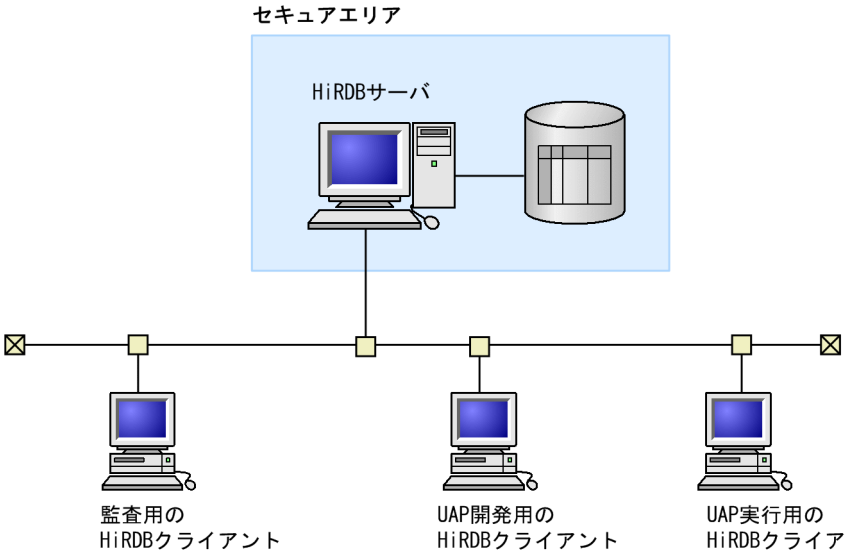
注

HiRDB/ パラレルサーバの場合は，HiRDB/ パラレルサーバを構成するすべてのマシンをセキュアエリア内に設置してください。

(3) ISO/IEC 15408 の評価構成時のセキュアエリア

セキュアエリアには HiRDB サーバ用のマシンだけを設置します。ISO/IEC 15408 の評価構成時のセキュアエリアを次の図に示します。

図 2-7　ISO/IEC 15408 の評価構成時のセキュアエリア



注

HiRDB/ パラレルサーバの場合は，HiRDB/ パラレルサーバを構成するすべてのマシンをセキュアエリア内に設置してください。

セキュアエリアは，許可された人（スーパユーザ，HiRDB 管理者，DBA 権限保持者，表の所有者，および監査人）だけが入場できるように管理されています。

2.3.2　リムーバブルメディアの管理

データベースのバックアップファイルなどを格納したリムーバブルメディアをセキュアエリアから持ち出せないように管理してください。特に，バックアップファイルなどの重要なデータを格納したリムーバブルメディアは，キャビネットなどに格納して施錠するなど，厳重に管理してください。

データを格納したリムーバブルメディアの管理方法については，「3.4　データを格納したリムーバブルメディアの管理」を参照してください。

2.4 OS に必要な条件

ここでは，セキュアなシステムを構築するときに必要な OS の条件について説明します。

2.4.1 OS アカウントの管理

HiRDB サーバ用のマシンの OS アカウントを管理する必要があります。

(1) OS アカウントを与えるユーザ

OS アカウントはむやみに与えないで，許可された管理者に対してだけ与えてください。スーパユーザは，許可された次の管理者に OS アカウントを与えてください。

- HiRDB 管理者
- DBA 権限保持者
- 表の所有者
- 監査人

ポイント

- 不特定多数の人に OS アカウントを与えると，OS アカウントを不正利用されるリスクが高くなります。
- 不要になった OS アカウントはすぐに削除してください。不要になった OS アカウントをそのままにしておくと，その OS アカウントを使用してシステムを不正利用されるリスクが高くなります。

(2) パスワードの管理

OS アカウントのパスワードは，ほかの人に知られないように各ユーザが管理してください。各ユーザは，パスワードに推測されにくい文字列を設定し，適切な頻度でパスワードを変更する必要があります。

2.4.2 リモートログインの設定（UNIX 限定）

HiRDB サーバへのリモートログインを許可すると，管理者以外の人間によって HiRDB が不正利用されるリスクが高くなるため，リモートログインを禁止してください。ただし，システム構成によっては，リモートログインを許可する必要があります。その場合は，必要なマシンからのリモートログインだけを許可するようにしてください。

参考

HiRDB サーバ以外のマシンからリモートログインして HiRDB のユティリティまたはコマンドが実行できると，その分 HiRDB が不正利用されるリスクが高くなるため，リモートログインを禁止します。

(1) HiRDB/ シングルサーバの場合

HiRDB サーバへのリモートログインを禁止してください。スーパユーザはリモートログインができないように OS の設定を行ってください。

(2) HiRDB/ パラレルサーバの場合

HiRDB/ パラレルサーバを構成するマシン間のリモートログインは許可してください。それ以外のマシンからのリモートログインは禁止してください。

参考

HiRDB のコマンドの中には，リモートシェル機能を使用して各マシンで実行するコマンドがあります。このため，HiRDB/ パラレルサーバを構成するマシン間でリモートログインを許可する必要があります。

(3) IP アドレスを引き継がない高速系切り替え機能を使用する場合

IP アドレスを引き継がない高速系切り替え機能を使用する場合，現用系の情報を予備系に転送するためにリモートシェル機能を使用します。このため，現用系のマシンと予備系のマシン間のリモートログインは許可してください。それ以外のマシンからのリモートログインは禁止してください。

2.4.3 マシンに設定される時刻の管理

HiRDB サーバ用のマシンに設定されている時刻を正しく管理してください。

HiRDB では，システムログファイル，ステータスファイルなどのファイル中に，日付・時間の情報を格納しています。この情報は，HiRDB の再開始時などに利用しているため，時刻を変更すると，統計情報が正しく表示されない，再開始が失敗する，データベースが回復できないなどの問題が発生することがあります。したがって，テストなどでしかたなく日時を変更する場合以外は，時刻が変更されないように適切に管理してください。

2.5 ネットワークに必要な条件

ここでは，セキュアなシステムを構築するときに必要なネットワークの条件について説明します。

2.5.1 ローカルエリアネットワークに必要な条件

HiRDB クライアントと HiRDB サーバ間の通信，および HiRDB/ パラレルサーバを構成するマシン間の通信は，次に示すすべての条件を満たすローカルエリアネットワークを使用してください。

- ローカルエリアネットワークを構成する機器とケーブルは，無断でアクセスできないように管理されている
- ホスト名やポート番号などのネットワークの設定が正確に行われている
- HiRDB クライアントから HiRDB サーバに対して不正な電文が送信されないように，ネットワーク構成の情報を適切に管理し，安定した運用が実施されている

これらの条件が守られていないと，通信の秘匿性や完全性が失われる可能性があります。例えば，データの漏えいや改ざんなどが発生したり，不正な電文を HiRDB サーバで受信したり，電文が相手に届かなかったりする可能性があります。

参考

ISO/IEC 15408 の評価は，ローカルエリアネットワークに HiRDB サーバおよび HiRDB クライアント用のマシン以外の機器を接続しない環境で行われました。

2.5.2 インターネットに接続する場合に必要な条件

HiRDB サーバと HiRDB クライアントを接続しているローカルエリアネットワークがインターネットに接続している場合，ファイアウォールを設置してインターネットから HiRDB サーバに直接アクセスできないようにしてください。

また，ローカルエリアネットワークを構成する機器とケーブルは，無断でアクセスできないように管理してください。

ポイント

ファイアウォールを通過させるパケットは必要最低限としてください。通過させるパケットを多くするほど（通過させるパケットのセキュリティレベルを下げるほど），その分セキュリティ上のリスクが高くなります。

参考

ISO/IEC 15408 の評価は，外部接続（インターネット接続）をしない環境で行われました。

3 HiRDB のセキュリティ設計

この章では，ユーザの管理，パスワードの管理，データベースのアクセス管理，およびリムーバブルメディアの管理について説明します。

3.1 ユーザの管理

ここでは，ユーザの役割分担とユーザに権限を与えるときの方針について説明します。

3.1.1 ユーザ管理の重要性

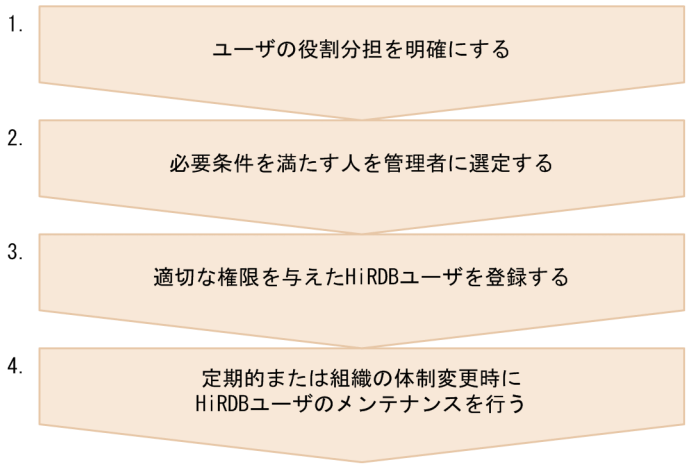
ユーザの管理はセキュリティ対策で最も重要なことの一つです。2 章で説明したセキュアなシステムを構築するための条件を満たし，HiRDB のセキュリティ機能を使用しても，ユーザ管理が十分にできていないと期待したセキュリティ効果が得られません。システムのセキュリティを強化するにはユーザの役割分担を明確にし，目的に合った権限を与えてユーザを管理する必要があります。ユーザ管理の手順を次の図に示します。

ポイント

ユーザの役割分担を明確にしないで必要以上に権限を与えると，それがセキュリティ上の弱点になる可能性があります。ユーザの管理が十分に行われていない場合，次に示すことが発生するリスクが高くなります。

- 権限を不正使用し，機密データへの不正アクセスを行う
- 架空の HiRDB ユーザを登録し，その HiRDB ユーザの認可識別子を使用して不正行為を行う

図 3-1 ユーザ管理の手順



説明

1. ユーザの役割分担については，「3.1.2(1) ユーザの役割と主な作業項目」を参照してください。
2. 各ユーザに必要な条件については，「3.1.2(2) 各ユーザの選定基準」を参照してください。

3. 管理者および利用者に適切な権限を与えて HiRDB ユーザとして登録してください。権限を与えるときの方針については,「3.1.3 権限を与えるときの方針」を参照してください。
4. 定期的または組織の体制変更時に HiRDB ユーザのメンテナンス（HiRDB ユーザの追加，HiRDB ユーザの削除，HiRDB ユーザの権限変更など）を行ってください。

3.1.2 ユーザの役割分担

ユーザの役割とその作業について説明します。

(1) ユーザの役割と主な作業項目

HiRDB では，次の表に示すユーザがシステムを構築，運用，または利用することを想定しています。

表 3-1 ユーザの役割と主な作業項目

ユーザの役割		人数	必要な権限	主な作業項目
システムを管理する人	スーパユーザ	1 名	―※1	• OS アカウントの登録 • OS の環境設定および管理 • HiRDB サーバのインストール
	HiRDB 管理者	1 名	DBA 権限	• HiRDB の環境設定 • HiRDB の管理・運用 • 監査人の登録（監査権限の付与）
権限を管理する人	DBA 権限保持者	1 名以上	DBA 権限	• 権限（DBA 権限，スキーマ定義権限，および CONNECT 権限）の管理 • パスワードの管理ルールの設定
表を管理する人	表の所有者	1 名以上	スキーマ定義権限 CONNECT 権限	• 表の定義 • 表へのデータロード • 表のアクセス権限の管理
データベースを利用する人	データベース利用者	1 名以上	CONNECT 権限	• データの検索，更新，挿入，および削除
監査を実施する人	監査人※2	1 名	監査権限	• 監査の実施 • セキュリティ監査機能の環境設定 • 監査証跡表へのデータロード

（凡例）―：該当しません。

注※ 1

スーパユーザは OS の権限であり，HiRDB の権限ではありません。

注※ 2

監査人は 1 名だけですが，監査を補佐する人（HiRDB ユーザ）を追加できます。その場合，監査人は監査を補佐する人に監査証跡表の SELECT 権限を与えてください。

参考

- HiRDB 管理者が有する DBA 権限と DBA 権限保持者が有する DBA 権限に機能差はありません。操作できる範囲に違いはありません。
- HiRDB 管理者はスーパユーザと同様に OS アカウントによって識別されます。
- 権限によって実行できるコマンドおよび SQL が異なります。詳細については，「HiRDB Version 9 コマンドリファレンス」，および「HiRDB Version 9 SQL リファレンス」を参照してください。
- HiRDB/ パラレルサーバの場合，ユーザの役割は各マシン共通です。

(2) 各ユーザの選定基準

(1) でユーザの役割と主な作業項目を説明しました。各ユーザに割り当てられた作業内容によって，必要とされる技能および知識が異なります。必要な技能および知識を有する人を選定してください。必要な技能または知識がない人を選定した場合，OS または HiRDB の運用・操作を誤り，それがセキュリティ上のリスクにつながる可能性があります。また，スーパユーザ，HiRDB 管理者，DBA 権限保持者，表の所有者，UAP 管理者，および監査人は，利用組織内で信頼できる人を選定してください。

各ユーザに必要な技能および知識を次の表に示します。

表 3-2 各ユーザに必要な技能および知識

ユーザの種類	ユーザに必要な技能および知識
スーパユーザ	ソフトウェアのインストールおよび環境設定をマニュアルの記載内容に従って適切に行える知識や，技能を有する人をスーパユーザに選定してください。 スーパユーザに必要な知識を次に示します。 • UNIX，Linux，または Windows のシステム管理の基礎的な知識 • HiRDB の環境設定に関する基礎的な知識 • セキュリティに関する基礎的な知識 これらの知識や技能が不足している場合は，OS または HiRDB の教育を受けるなどの対策を行ってください。 スーパユーザは，HiRDB 管理者やデータベース利用者を兼任できます。

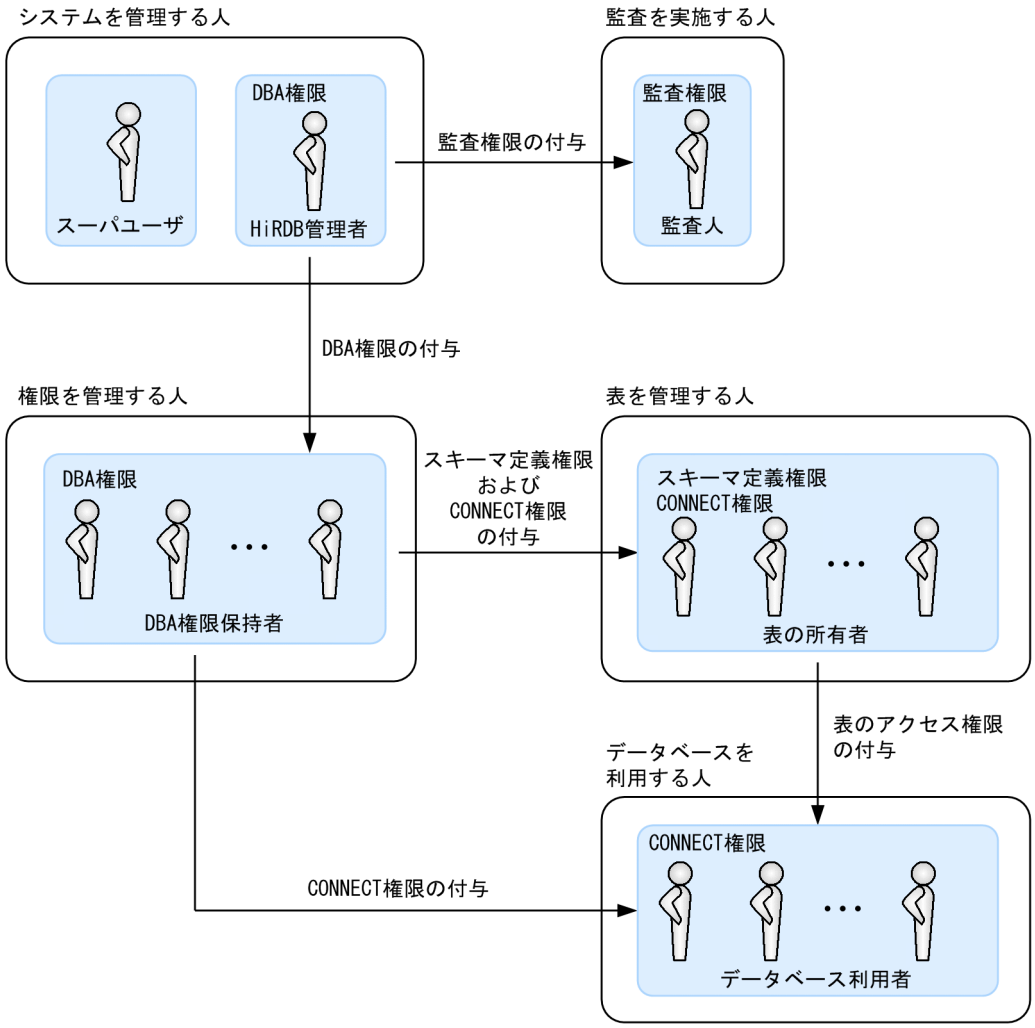
ユーザの種類	ユーザに必要な技能および知識
HiRDB 管理者	HiRDB の環境設定および運用・操作をマニュアルの記載内容に従って適切に行える知識や，技能を有する人を HiRDB 管理者に選定してください。 HiRDB 管理者に必要な知識を次に示します。 • UNIX，Linux，または Windows のシステム管理の基礎的な知識 • HiRDB の環境設定および操作に関する基礎的な知識 • HiRDB のユティリティおよびコマンドに関する基礎的な知識 • SQL の基礎的な知識 • セキュリティに関する基礎的な知識 これらの知識や技能が不足している場合は，OS または HiRDB の教育を受けるなどの対策を行ってください。 HiRDB 管理者は，DBA 権限保持者を兼任することになります。監査人は兼任できません。
DBA 権限保持者	HiRDB の各種権限（DBA 権限，スキーマ定義権限，および CONNECT 権限）をマニュアルの記載内容に従って適切に管理できる知識や，技能を有する人を DBA 権限保持者に選定してください。DBA 権限保持者に必要な知識を次に示します。 • HiRDB の権限に関する基礎的な知識 • HiRDB の操作に関する基礎的な知識 • SQL の基礎的な知識 • セキュリティに関する基礎的な知識 これらの知識や技能が不足している場合は，HiRDB の教育を受けるなどの対策を行ってください。 DBA 権限保持者は，表の所有者を兼任できます。監査人は兼任できません。
表の所有者	所有する表のアクセス権限をマニュアルの記載内容に従って適切に管理できる知識や，技能を有する人を表の所有者に選定してください。表の所有者に必要な知識を次に示します。 • HiRDB の権限に関する基礎的な知識 • HiRDB のユティリティおよびコマンドに関する基礎的な知識 • SQL の基礎的な知識 • セキュリティに関する基礎的な知識 これらの知識や技能が不足している場合は，HiRDB の教育を受けるなどの対策を行ってください。
データベース利用者	HiRDB サーバに対して適切なアクセスを行える知識や，技能を有する人をデータベース利用者に選定してください。データベース利用者に必要な知識を次に示します。 • PC の基本操作の知識 • セキュリティに関する基礎的な知識 これらの知識や技能が不足している場合は，セキュリティに関する教育を受けるなどの対策を行ってください。 なお，SQL を使ってデータベースにアクセスする利用者は，さらに SQL の基礎的な知識が必要になります。 次のユーザはデータベース利用者であり，データベース利用者以外の役割も兼任できます。 • UAP 管理者 HiRDB クライアントで実行する UAP の開発と保守を行う人です。また，UAP 実行者の管理も担います。 • UAP 実行者 HiRDB クライアントで実行する UAP を操作する人です。

ユーザの種類	ユーザに必要な技能および知識
監査人	マニュアルの記載内容に従って監査を適切に行う知識や，技能を有する人を監査人に選定してください。監査人に必要な知識を次に示します。 • HiRDB の権限に関する基礎的な知識 • HiRDB の操作に関する基礎的な知識 • HiRDB のユティリティおよびコマンドに関する基礎的な知識 • SQL の基礎的な知識 • セキュリティに関する基礎的な知識 これらの知識や技能が不足している場合は，HiRDB の教育を受けるなどの対策を行ってください。 監査人は，DBA 権限保持者（HiRDB 管理者を含む）を兼任できません。

（3） 権限付与の流れ

HiRDB のインストール後，最初に登録される HiRDB ユーザは HiRDB 管理者です。HiRDB 管理者には自動的に DBA 権限が与えられているため，最初は HiRDB 管理者がほかの HiRDB ユーザに対して権限を与えます。HiRDB 管理者登録後の権限付与の流れを次の図に示します。

図 3-2　HiRDB 管理者登録後の権限付与の流れ



参考

- DBA 権限をほかの HiRDB ユーザに与えないで，HiRDB 管理者だけが有するようにしても問題はありません。
- HiRDB 管理者用に設定される認可識別子については，UNIX の場合は「5.5　HiRDB の環境設定を行う」を，Windows の場合は「6.4　簡易セットアップツールを実行する」を参照してください。

3.1.3　権限を与えるときの方針

DBA 権限保持者が HiRDB ユーザの登録を行い，その HiRDB ユーザに必要な権限を与えます。ここでは，権限を与えるときの方針について説明します。

(1) 権限管理の原則

権限管理の原則を次に示します。

- 必要以上の権限を与えると，それがセキュリティ上の弱点となる可能性があります。したがって，決められた役割に従って必要最小限の権限を与えるようにしてください。
- 権限が不要になった場合は（組織内で人の異動があったときなど），すぐに権限を削除するか，または変更してください。その HiRDB ユーザがいなくなる場合はその HiRDB ユーザ（認可識別子）を削除してください。
- 必要のない HiRDB ユーザを登録して権限を与えないでください。

(2) DBA 権限を与えるときの方針

HiRDB ユーザの権限を管理する人に DBA 権限を与えます。

DBA 権限を与えるときの方針

DBA 権限があると，権限を追加（削除および変更も含む）したり，ほかの HiRDB ユーザが所有している表を削除したりできます。また，DBA 権限はスキーマ定義権限および CONNECT 権限を包括しているため，表の定義もできます。このように大変利便性が良いため，多くの HiRDB ユーザに DBA 権限を与えてしまいがちです。しかし，DBA 権限はほかの HiRDB ユーザの表を削除したり，権限を削除したりできる強力な権限です。このため，悪意を持った HiRDB ユーザがこの権限を有するとセキュリティ上のリスクが非常に高くなります。したがって，DBA 権限を与えるときは利便性を考えないで，セキュリティ面だけを考えて判断するようにしてください。

DBA 権限を与える方法

DBA 権限保持者が，定義系 SQL の GRANT を実行してほかの HiRDB ユーザに DBA 権限を与えます。

ほかの HiRDB ユーザの DBA 権限を削除する場合は，定義系 SQL の REVOKE を実行します。

(3) スキーマ定義権限を与えるときの方針

表を定義し，所有・管理する人にスキーマ定義権限および CONNECT 権限を与えます。

参考

スキーマを定義するにはスキーマ定義権限と CONNECT 権限の両方が必要になります。スキーマ定義権限および CONNECT 権限を与えてもらったあとにスキーマを定義し，表を定義すると，表の所有者になります。

なお，権限は CONNECT 権限，スキーマ定義権限の順に与えてください。逆にした場合，SQL の実行時にエラーとなります。

スキーマ定義権限を与えるときの方針

表を定義し，所有・管理する人だけにスキーマ定義権限を与えてください。それ以外の人にはスキーマ定義権限を与えないでください。

スキーマ定義権限を与える方法

DBA 権限保持者が，定義系 SQL の GRANT を実行してほかの HiRDB ユーザにスキーマ定義権限を与えます。
ほかの HiRDB ユーザのスキーマ定義権限を削除する場合は，定義系 SQL の REVOKE を実行します。

(4) CONNECT 権限を与えるときの方針

データの検索，更新，追加，および削除を行うデータベースの利用者に CONNECT 権限を与えます。ただし，データベースの利用者がデータをアクセスするには，表の所有者に表のアクセス権限を与えてもらう必要があります。

CONNECT 権限を与えるときの方針

データベースの利用者だけに CONNECT 権限を与えてください。必要のない HiRDB ユーザを登録し，CONNECT 権限を与えないようにしてください。

CONNECT 権限を与える方法

DBA 権限保持者が，定義系 SQL の GRANT を実行してほかの HiRDB ユーザに CONNECT 権限を与えます。
ほかの HiRDB ユーザの CONNECT 権限を削除する場合は，定義系 SQL の REVOKE を実行します。REVOKE 実行時の注意事項については，「7.9.1 CONNECT 権限を取り消す場合」を参照してください。

(5) 監査権限を与えるときの方針

監査を実施する人に監査権限を与えて監査人として登録します。

監査権限を与えるときの方針

- システムの利用者（管理者を含む）を監査人にしないでください。利用者を監査人にすると，監査の不正工作がやりやすくなるため，不正行為が行われるリスクが高くなります。
- 監査人には，監査証跡表以外の表のアクセス権限を極力与えないでください。

監査権限の制限

- DBA 権限保持者（HiRDB 管理者を含む）は監査人になれません。
- 監査人の監査権限は削除できません。
- 一度登録した監査人の認可識別子は変更できません。

参考

- DBA 権限は最も強力な権限であるため，DBA 権限と監査権限の両方を有する人が不正行為を行った場合，それをチェックすることが難しくなります。そのため，DBA 権限保持者を監査人にはできない仕組みになっています。
- 監査人を変更する場合，既存の監査人の認可識別子をそのまま引き継いで，パスワードを変更する運用としてください。このとき，すぐにパスワードを変更してください。

監査権限を与える方法

HiRDB 管理者がデータベース構成変更ユティリティの create auditor 文で監査人を登録します（監査権限を与えます）。

3.2 パスワードの管理

ここでは，アカウントの不正使用を防止するために必要なパスワードの管理方法について説明します。

3.2.1 パスワードの管理ルールの設定

HiRDB では認可識別子とパスワードによってユーザ認証を行い，第三者によるシステムの不正利用を防止しています。このため，パスワードを第三者に不正使用されない（盗まれない）ことが重要になります。

DBA 権限保持者はパスワードの管理ルールを設定し，HiRDB ユーザにそのルールを徹底させて，パスワードのセキュリティを強化してください。パスワードの管理ルールを次の表に示します。

ポイント

DBA 権限保持者が HiRDB ユーザを登録するときに，その HiRDB ユーザの初期パスワードを設定します。そのあと，各 HiRDB ユーザが自分のパスワードを次の表に示すルールに従って管理（変更）します。

表 3-3 パスワードの管理ルール

パスワードの管理ルール	説明
パスワードを秘密にする	HiRDB ユーザにパスワードの守秘義務を与えて，それを守らせてください。
パスワードを記録しない	パスワードを記録すると，パスワードがほかの人に盗まれる可能性が高くなるため，HiRDB ユーザにパスワードを記録させないようにし，それを守らせてください。
パスワードを定期的に変更する	HiRDB ユーザにパスワードの定期変更義務を与えて，それを守らせてください。 DBA 権限保持者はどのくらいの期間でパスワードを変更するかを決めてください。パスワードの変更履歴は監査情報に記録されるため，パスワードの定期変更義務が守られているかどうかを監査で確認できます。
推測されにくいパスワードを作成する	HiRDB ユーザがパスワードを変更するときに，推測しやすい簡単なパスワードを作成しないようにさせてください。 DBA 権限保持者はパスワードの作成規則（パスワードを何文字以上にするか，パスワードに英字と数字を混ぜるかなど）を設定し，HiRDB ユーザにその規則を守らせてください。パスワードの作成規則は，「3.2.2 パスワードの例」を参考にして決めてください。

参考

パスワードを忘れてしまった場合，および連続認証失敗アカウントロック状態になった場合，HiRDB ユーザはその旨を DBA 権限保持者に連絡してください。連絡を受けた DBA 権限保持者は，必ず本人かどうかを確認した上で対処してください。

3.2.2 パスワードの例

悪いパスワードの例と良いパスワードの例を説明します。

(1) パスワードに使用できる文字列

パスワードに使用できる文字列を次に示します。

- 英大文字：A ～ Z，#，@，¥
- 英小文字：a ～ z
- 数字：0 ～ 9

パスワードにはこれらの文字列を指定できますが，先頭は英字（英大文字または英小文字）を指定する必要があります。

(2) 悪いパスワードの例

悪いパスワードの例を次の表に示します。

表 3-4 悪いパスワードの例

禁止項目	説明およびパスワードの例
わかりやすい単語をパスワードに使用する	固有名称，簡単な単語や文字列などは使用しないでください。 （例）hirdb，eigyo，keiri
英字 1 文字と，同じ数字の組み合わせをパスワードに使用する	先頭が英字 1 文字で，その後ろが同じ数字のパスワードは使用しないでください。 （例）a11111，z99999
推測しやすいパスワードを使用する	認可識別子と同じ文字列のパスワードを使用しないでください。また，個人情報（自分の名前，家族の名前，生年月日，電話番号など）をパスワードに使用しないでください。 （例）SUZUKI，masaru，S521024 パスワードの文字列中に認可識別子を使用することを禁止できます。詳細については，「3.2.3 パスワードの禁止条件の設定」を参照してください。
英字だけのパスワードを使用する	英字だけのパスワードを使用しないでください。特に同じ文字を並べただけ，またはアルファベット順に並べただけのパスワードは絶対に使用しないでください。 （例）aaaaaa，ABCDEFG，dbmanual，GRNPJXRD パスワードを英大文字だけまたは英小文字だけで作成することを禁止できます。詳細については，「3.2.3 パスワードの禁止条件の設定」を参照してください。

(3) 良いパスワードの例

良いパスワードの例を次の表に示します。

表 3-5 良いパスワードの例

推奨項目	説明およびパスワードの例
パスワードの文字数を多くする	8 文字以上のパスワードを作成してください。ただし，長過ぎるパスワードは覚えることが難しいため，適切な長さにしてください。 （例）Gth47ADb，F#36Qjls パスワードの最低文字数を設定できます。詳細については，「3.2.3 パスワードの禁止条件の設定」を参照してください。
英字と数字を混ぜたパスワードを使用する	パスワードには英字と数字を混ぜてください。英大文字と英小文字を混ぜるとさらに効果が上がります。 （例）Gth47ADb，F#36Qjls

ポイント

覚えられるパスワードを使用してください。パスワードが覚えられないためにパスワードを記録したりすると，パスワードがほかの人に盗まれる可能性が高くなります。

3.2.3 パスワードの禁止条件の設定

パスワードの禁止条件を設定できます。禁止条件に該当するパスワードの認可識別子を**パスワード無効アカウントロック状態**にし，HiRDB を利用できないようにします。

参考

- パスワード無効アカウントロック状態になった場合，DBA 権限保持者が定義系 SQL の GRANT で，該当する HiRDB ユーザのパスワードを変更してください。禁止条件に該当しないパスワードに変更すれば，パスワード無効アカウントロック状態が解除されます。
- 定義系 SQL の DROP CONNECTION SECURITY FOR PASSWORD を実行すると，全ユーザのパスワード無効アカウントロック状態が解除されます。そのため，DROP CONNECTION SECURITY FOR PASSWORD を実行した場合は，再度パスワードの禁止条件の設定（CREATE CONNECTION SECURITY FOR PASSWORD）をしてください。

パスワードに設定できる禁止条件を次に示します。

- 決められた文字数（バイト数）以下のパスワードを禁止する
- パスワードの文字列中に認可識別子を使用することを禁止する
- パスワードを英大文字だけまたは英小文字だけで作成することを禁止する

CONNECT 関連セキュリティ機能を使用してパスワードの禁止条件を設定します。CONNECT 関連セキュリティ機能については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

3.2.4 アカウントの不正使用対策

パスワードを推測して何度も入力し，アカウントを不正使用する試みに対しても対策する必要があります。この不正行為の対策として，CONNECT 関連セキュリティ機能を使用して**連続認証失敗許容回数**と**アカウントロック期間**を設定します。CONNECT 関連セキュリティ機能については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

(1) 連続認証失敗許容回数とは

パスワードの不正入力によってユーザ認証に連続して失敗したときに，失敗回数が連続認証失敗許容回数を超えると，その認可識別子を**連続認証失敗アカウントロック状態**にし，HiRDB を利用できないようにします。

例えば，連続認証失敗許容回数を 3 と設定した場合，パスワードの不正入力によって 4 回連続でユーザ認証に失敗すると，その認可識別子は連続認証失敗アカウントロック状態になり，HiRDB を利用できなくなります。

(2) アカウントロック期間とは

連続認証失敗アカウントロック状態とする期間をアカウントロック期間といいます。例えば，アカウントロック期間を 1 時間とした場合，連続認証失敗アカウントロック状態が 1 時間続きます。1 時間を過ぎると連続認証失敗アカウントロック状態が解除されて，その認可識別子で HiRDB を利用できるようになります。

ポイント

連続認証失敗許容回数とアカウントロック期間はセキュリティポリシーに合わせた値にしてください。例えば，連続認証失敗許容回数を 10 回と極端に多くしたり，アカウントロック期間を 10 分と極端に短くしたりすると，それがセキュリティ上の弱点になる可能性があります。

3.3 データベースのアクセス管理

ここでは，表のアクセス権限の管理方針，およびディクショナリ表の参照権限の設定方法について説明します。

3.3.1 表のアクセス権限の管理方針

「1.3.3 データベースのアクセス制御」で説明したように，表のアクセス制御は**表のアクセス権限**によって管理されています。表のアクセス権限は表の所有者が管理し，ほかの HiRDB ユーザにアクセス権限を与えたり，アクセス権限を削除したりします。表の所有者は次に示す管理方針に従って表のアクセス権限を管理してください。

(1) 必要な HiRDB ユーザだけに必要なアクセス権限を与える

表をアクセスする必要がある HiRDB ユーザだけにアクセス権限を与えてください。例えば，組織のグループ（部，課など）内の全員が表をアクセスする必要がないのに，グループ内の全員にアクセス権限を与えるようなことはしないでください。必要以上の人にアクセス権限を与えると，データが改ざんされたり，データが漏えいしたりするリスクが高くなります。

(2) 目的に合ったアクセス権限を与える

目的に合ったアクセス権限を与えてください。例えば，検索だけを行う HiRDB ユーザには SELECT 権限だけを与えてください。UPDATE 権限や DELETE 権限などの不要なアクセス権限を与えると，データが改ざんされるリスクが高くなります。

また，必要に応じてアクセス権限の種類（SELECT 権限，INSERT 権限，DELETE 権限，UPDATE 権限）を変更してください。

ポイント

与えるアクセス権限は必要最小限にしてください。

(3) 不要になったアクセス権限をすぐに削除する

組織内の人の異動などによって，表にアクセスする必要がなくなる HiRDB ユーザが生じた場合，その HiRDB ユーザのアクセス権限をすぐに削除してください。アクセス権限をそのままにしておくと，そのアクセス権限を利用したデータの改ざんまたは漏えいが発生するリスクが高くなります。

参考

定義系 SQL の GRANT でアクセス権限を与えて，REVOKE でアクセス権限を削除します。

3.3.2 ディクショナリ表の参照権限の設定

ディクショナリ表には，認可識別子，表名，表の所有者，HiRDB ユーザが持っている権限などの重要な情報が格納されています。不特定多数の HiRDB ユーザがこれらの情報を参照できると，それがセキュリティ上の弱点になる可能性があります。したがって，HiRDB 管理者は**ディクショナリ表の参照権限**を設定し，一般の HiRDB ユーザ（DBA 権限保持者および監査人以外の HiRDB ユーザ）がディクショナリ表内の重要な情報を参照できないようにしてください。

ディクショナリ表の参照権限の設定については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

参考

- ディクショナリ表の参照権限を設定しない場合，一般の HiRDB ユーザは DBA 権限保持者と同程度の情報を参照できます。
- 認可識別子，および各 HiRDB ユーザが持っている DBA 権限，監査権限，およびスキーマ定義権限については，ディクショナリ表の参照権限を設定するかどうかに関係なく，一般の HiRDB ユーザは参照できません。

3.4 データを格納したリムーバブルメディアの管理

バックアップデータなどをリムーバブルメディア（以下，メディアと表記します）に格納して保管する場合，そのメディアを不正使用されないように管理する必要があります。ここでは，データを格納したメディアの管理方法について説明します。

(1) メディア管理の重要性

システムのセキュリティをいくら強化しても，データを格納したメディアの管理が行われていないと，メディアを盗まれてデータが漏えいしたり，メディアを不正使用されてデータが改ざんされたりするおそれがあります。そのため，データを格納したメディアが不正使用されないように管理する必要があります。

ポイント

守る必要があるデータは，ハードディスク上のデータだけではありません。データを格納したメディアも同様に守る必要があります。データが漏えいする原因は，ハードディスク上のデータが盗まれるケースよりも，メディアが盗まれるケースの方が多いと考えられます。

(2) 管理ルールの設定

メディアの管理ルールの例を次の表に示します。これを参考にしてデータを格納したメディアの管理ルールを設定してください。

表 3-6 メディアの管理ルールの例

メディアの管理ルール	説明
メディア管理の責任者を決める	メディア管理の責任者を決めてください。責任者は管理対象のメディアの一覧を作成し，それを使用してメディアを管理してください。
管理対象とするデータを決める	組織のセキュリティポリシーに従って管理対象とするデータを決めてください。バックアップデータ，アンロードデータ，アンロードログなどの重要なデータは必ず管理対象にしてください。
セキュアエリア内でメディアを管理する	メディアはセキュアエリア内で管理し，セキュアエリア外に持ち出せないようにしてください。また，キャビネットなどに格納して施錠するなど，厳重に管理してください。
メディアの使用記録を取る	メディアを使用する場合，使用者や，使用時刻などの使用記録を取ってください。
メディアが無くなっていないかを定期的に確認する	メディアが無くなっていないかを定期的に確認してください。
読み込み専用のメディアにデータを格納する	データの上書きを防止するために，読み込み専用のメディアにデータを格納してください。
メディアごとに管理番号入りのシールをはる	メディアの差し替えを防止するために，メディアごとに管理番号入りのシールをはるなどしてください。

メディアの管理ルール	説明
メディアの廃棄方法を決める	廃棄したメディアが不正使用されないように廃棄方法を決めてください。
利用者全員に教育を実施する	メディアの管理が重要なセキュリティ対策になっていることを利用者全員に教育してください。

4 監査による利用状況の確認

この章では，監査で確認する項目と監査の手順について説明します。

4.1 監査で確認する項目

1 章～ 3 章でシステムのセキュリティ対策について説明してきました。それに基づいて実施したセキュリティ対策が意図したとおりに機能しているかを監査で確認する必要があります。ここでは，一般的な監査の例として，各項目について説明します。

4.1.1 HiRDB の不正利用が行われていないかを確認する

HiRDB の不正利用が行われていないかを監査で確認します。ここで説明する考え方に基づいて確認してください。

(1) ユーザ認証時に発生したエラーをチェックする

ユーザ認証時に発生したエラーをチェックして，不正なアクセスが試されていないかを確認します。この場合，次に示すことを監査情報で確認します。

- ユーザ認証エラーを起こした認可識別子
- ユーザ認証エラーを起こした日時

この監査情報を基に，この操作を行ったのが本人かどうか確認してください。本人が否定した場合，第三者による HiRDB への不正なアクセスが試された可能性があります。

ポイント

エラーの回数が多い（特に連続して失敗している場合）認可識別子は不正アクセスが試されている可能性があります。このような認可識別子を重点的にチェックします。

4.1.2 権限の不正利用が行われていないかを確認する

権限の不正利用が行われていないかを監査で確認します。ここで説明する考え方に基づいて確認してください。

(1) 権限がないため操作エラーになったケースをチェックする

必要な権限がないため，操作エラーになったケースをチェックします。この場合，次に示すことを監査情報で確認します。

- 操作エラーを起こした認可識別子
- 操作エラーを起こした日時
- 変更しようとした情報

この監査情報を基に，この操作を行ったのが本人かどうか確認してください。本人が否定した場合，成り済ましによる不正な操作が試された可能性があります。この場合，該当する認可識別子のパスワードをすぐに変更してください。

ポイント

- 権限の変更や，パスワードの変更などの重要な操作でエラーが発生した場合，その操作についてはチェックが必要になると考えられます。
- 操作エラーの回数が多い認可識別子を重点的にチェックします。

4.1.3 表の不正アクセスが行われていないかを確認する

表の不正アクセスが行われていないかを監査で確認します。ここで説明する考え方に基づいて確認してください。

(1) 表のアクセスエラーをチェックする

表のアクセス権限がないため，アクセスエラーになったケースがないかをチェックします。この場合，次に示すことを監査情報で確認します。

- アクセスエラーを起こした認可識別子
- アクセスエラーを起こした日時
- アクセスを試みた表と操作種別

この監査情報を基に，この操作を行ったのが本人かどうか確認してください。本人が否定した場合，成り済ましによる不正なアクセスが試された可能性があります。この場合，該当する認可識別子のパスワードをすぐに変更してください。

ポイント

- 顧客情報などの重要なデータを格納している表のアクセスエラーを重点的にチェックします。
- アクセスを試みたデータの機密度が高いほど，またはアクセスを試みた回数が多いほどチェックが必要になると考えられます。

(2) 想定外のアクセスをチェックする

次に示すような想定外のアクセスが行われている場合はチェックが必要になります。

- 業務時間外（アクセスが行われないはずの時間帯）にアクセスが発生した場合
- 実際のアクセス頻度が想定していたアクセス頻度を大幅に上回った場合

この場合，アクセス権限の設定が適切でない，または正しい使用者であっても組織の方針が守られていない可能性があります。また，なりすましによる不正なアクセスが行われている可能性もあります。

4.1.4 パスワードの定期変更が行われているかを確認する

HiRDB ユーザにはパスワードの定期変更義務があります。この義務が守られているかどうかを監査で確認します。ここで説明する考え方に基づいて確認してください。

(1) パスワードの前回変更日時をチェックする

パスワードの前回変更日時を監査情報でチェックします。この場合，次に示すことを監査情報で確認します。

- パスワードの変更を行った認可識別子
- パスワードの変更を行った日時

例えば，30 日以内にパスワードを変更するルールを設定した場合，30 日以内にパスワードを変更した HiRDB ユーザをこれらの情報で確認します。それ以外の HiRDB ユーザはパスワードの定期変更義務を果たしていません。この場合，本人にパスワードをすぐに変更するように連絡してください。

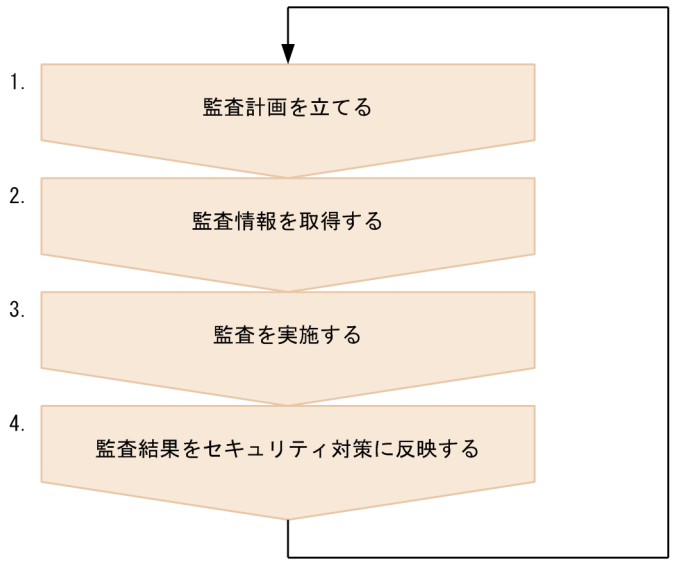
4.2　監査の手順

ここでは，監査の手順と各手順の作業内容について説明します。

4.2.1　監査の流れ

監査の流れを次の図に示します。監査人はこの流れに基づいて監査を実施してください。

図 4-1　監査の流れ



説明

1. 組織のセキュリティポリシーに基づいて監査計画を立てください。また，「4.1 監査で確認する項目」も参考にしてください。
2. 監査計画に従って必要な監査情報を取得してください。詳細については，「4.2.2 監査情報の取得」を参照してください。
3. 監査計画に従って監査を実施してください。詳細については，「4.2.3　監査の実施」を参照してください。
4. 監査結果からセキュリティ上のリスクを分析し，それをセキュリティ対策に反映してください。また，監査の結果を監査計画に反映してください。

ポイント

監査を効率的に行うためには監査目的を明確にし，そのために必要な監査情報を取得する必要があります。明確な目的がないままむやみに監査情報を取得すると，監査に掛かる時間が増加し，的確な監査ができなくなるおそれがあります。

4.2.2 監査情報の取得

セキュリティ監査機能を使用し，次に示す手順で監査情報を取得します。

手順

1. セキュリティ監査機能の環境設定（監査証跡表の作成など）をしてください。この作業は HiRDB 管理者が行います。
2. 取得する監査情報を定義系 SQL の CREATE AUDIT で選択してください。この作業は監査人が行います。ここで選択した監査対象イベントが発生すると監査情報が監査証跡ファイルに出力されます。
3. セキュリティ監査機能を使用して運用を開始してください。この作業は HiRDB 管理者と監査人が実行します。なお，pdload コマンドを実行する場合，-u オプションには監査人の認可識別子を指定してください。コマンドを実行すると，パスワード入力要求のメッセージが表示されるため，監査人が自身のパスワードを入力してください。
4. 監査証跡ファイルに出力された監査情報を監査証跡表にデータロードしてください。この作業は監査人が行います。

各作業の詳細，およびセキュリティ監査機能によって取得される監査情報については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

●現在の取得対象イベントを知る方法

監査情報の取得対象イベントを追加，変更，または削除する場合，現在の取得対象イベントをディクショナリ表（SQL_AUDITS 表）で確認してください。CREATE AUDIT の設定値と SQL_AUDITS 表の関係を次に示します。

```
CREATE AUDIT
   AUDITTYPE {PRIVILEGE | EVENT | ANY}    ...1
   FOR 操作種別     ...2
   選択オプション     ...3
   WHENEVER {SUCCESSFUL | UNSUCCESSFUL | ANY}    ...4
```

説明

1. AUDIT_TYPE 列で設定値を確認できます。
2. EVENT_TYPE，および EVENT_SUBTYPE 列で設定値を確認できます。
3. OBJECT_TYPE，OBJECT_SCHEMA，および OBJECT_NAME 列で設定値を確認できます。
4. ANY_VALID，SUCCESSFUL_VALID，および UNSUCCESSFUL_ANY_VALID 列で設定値を確認できます。

● HiRDB の強制終了または異常終了時の監査情報

HiRDB が強制終了または異常終了したとき，強制終了または異常終了についての監査情報は取得されません。また，強制終了または異常終了の直前の監査ログが取得されないこともあります（詳細については，「7.3.1(2)pd_aud_async_buff_size および pd_aud_async_buff_count」を参照してください）。

注意事項

HiRDB が強制終了または異常終了した場合，HiRDB 管理者は強制終了または異常終了したことを監査人に連絡してください。HiRDB が強制終了または異常終了したあとの監査は不要となります。

HiRDB の強制終了または異常終了時の監査については，次の表に示す情報を基に実施してください。

表 4-1 HiRDB の強制終了または異常終了時の監査情報

実行したコマンド	監査情報
pdstop -f	このコマンドを実行したときに KFPS01850-I メッセージが出力されます。このメッセージを監査情報としてください。
pdstop -f -q	このコマンドを実行してもメッセージは出力されません。 HiRDB を終了する操作（異常終了も含む）を行っていないのに HiRDB が停止している場合は，このコマンドが実行された可能性があります。 また，HiRDB が稼働中かどうかは pdls -d svr コマンドで確認できます。
pdstop -f -x ホスト名 pdstop -f -u ユニット識別子	このコマンドを実行したときに，コマンド指示で終了したユニットのマシンに KFPS01841-I メッセージが出力されます。このメッセージを監査情報としてください。
pdstop -f -s サーバ名	このコマンドを実行したときに KFPS01843-I メッセージが出力されます。このメッセージを監査情報としてください。
pdstop -f -u ユニット識別子 -s サーバ名	このコマンドを実行したときに，実行系には KFPS01843-I メッセージが出力され，待機系には KFPS05621-I メッセージが出力されます。
pdstop -z	システムマネジャがあるユニットには KFPS01850-I メッセージが出力され，システムマネジャがないユニットには KFPS01841-I メッセージが出力されます。なお，pdstop -z コマンドは，コマンドを実行したユニットだけ強制終了します。
pdstop -z -q	このコマンドを実行してもメッセージは出力されません。 HiRDB を終了する操作（異常終了も含む）を行っていないのに HiRDB が停止している場合は，このコマンドが実行された可能性があります。 また，HiRDB が稼働中かどうかは pdls -d svr コマンドで確認できます。
pdstop -z -c	このコマンドを実行したときに KFPS01841-I メッセージが出力されます。このメッセージを監査情報としてください。
pdstop -z -s サーバ名	このコマンドを実行したときに，実行系には KFPS01843-I メッセージが出力され，待機系には KFPS05621-I メッセージが出力されます。

4.2.3 監査の実施

監査情報は監査証跡表に格納されているため，SQL で検索できます。HiRDB SQL Executer または監査情報を検索するための UAP を作成し，監査情報を調査してください。

また，監査結果からセキュリティ上のリスクを分析し，それをセキュリティ対策および監査計画に反映してください。

参考

- 監査証跡表の SELECT 権限は監査人だけが持っています。監査を補佐する人（HiRDB ユーザ）を追加した場合，監査人はその HiRDB ユーザに対して監査証跡表の SELECT 権限を与えてください。監査人は，利用組織内で信頼できる人を，監査を補佐する人として選任する必要があります。
- 監査を補佐する人は，監査人の指示に従って監査データをチェックしてください。このとき，不穏な事象を発見した場合には，監査人に報告してください。
- 監査証跡表の改ざんを防止するために，監査証跡表のデータ更新（INSERT および UPDATE）はだれにもできないようになっています。データの削除（DELETE）は監査人だけが実行できるようになっています。

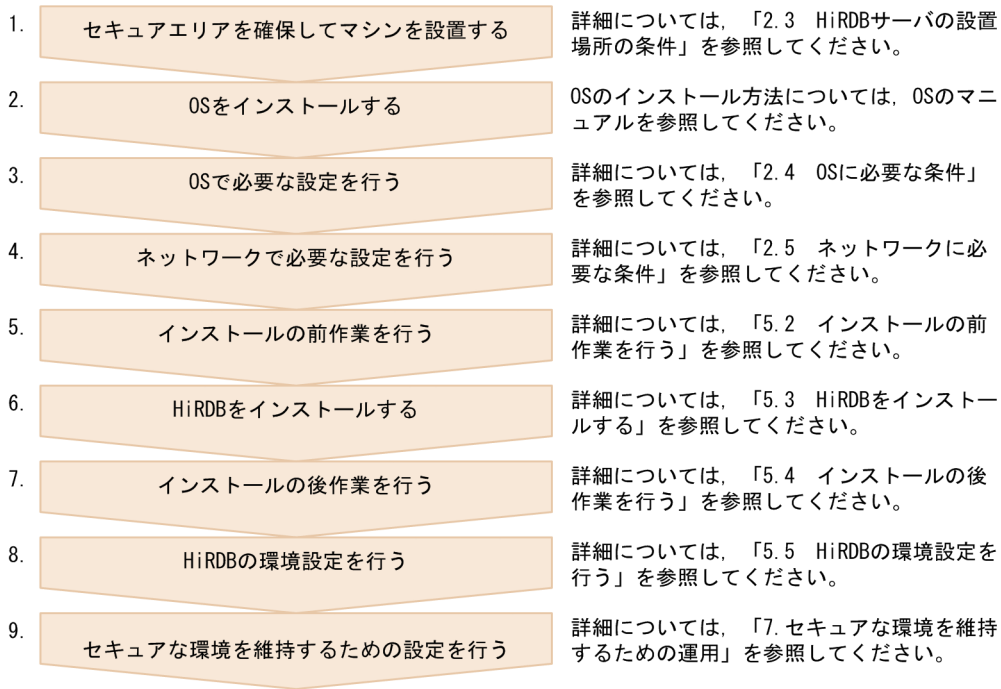
5 HiRDB の環境設定（UNIX の場合）

この章では，UNIX 版の HiRDB の環境設定方法について説明します。

5.1　環境設定手順

セキュアなシステムを構築する場合は，「HiRDB Version 9 システム導入・設計ガイド」で説明している環境設定手順ではなく，ここで説明している手順に従って HiRDB サーバの環境設定を行ってください。HiRDB サーバの環境設定手順を次の図に示します。

図 5-1　HiRDB サーバの環境設定手順（UNIX の場合）



5.2 インストールの前作業を行う

ここでは，HiRDB をインストールする前に行う作業について説明します。

5.2.1 OS アカウントを登録する

実行者　スーパユーザ

次に示す HiRDB ユーザの OS アカウントを登録してください。これら以外のユーザに OS アカウントを与えないでください。

- HiRDB 管理者
- DBA 権限保持者
- 表の所有者
- 監査人

ポイント

必要以上の人間に OS を利用する権利を与えると，その分システムが不正利用されるリスクが高くなります。

OS アカウントのパスワードは，ほかの人に知られないように各ユーザが管理してください。各ユーザは，パスワードに推測されにくい文字列を設定し，適切な頻度でパスワードを変更する必要があります。

5.2.2 オペレーティングシステムパラメタを変更する

実行者　スーパユーザ

オペレーティングシステムパラメタ（カーネルパラメタ）を変更してください。変更内容については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「OS のオペレーティングシステムパラメタの確認・変更」を参照してください。

5.2.3 HiRDB グループを設定する

実行者　スーパユーザ

HiRDB 専用のグループを設定してください。HiRDB グループを設定すると，グループ以外のユーザが HiRDB ファイルシステム領域や，HiRDB 運用ディレクトリ下のファイルなどにアクセスすることを拒否できます。

グループの設定方法については，OS のマニュアルを参照してください。

5.2.4 インストールディレクトリを作成する

実行者　スーパユーザ

ルートパーティションを圧迫しないように，HiRDB をインストールする前に次に示すインストールディレクトリをあらかじめ作成しておきます。

- /opt/HiRDB_S（HiRDB/ シングルサーバの場合）
- /opt/HiRDB_P（HiRDB/ パラレルサーバの場合）

このインストールディレクトリは，ファイルシステムを圧迫しないように専用のディスクパーティションに作成することをお勧めします。HiRDB はここで作成したインストールディレクトリ下にインストールされます。ディスクパーティションについては，OS のマニュアルを参照してください。

なお，HiRDB/ パラレルサーバの場合は，HiRDB/ パラレルサーバを構成するすべてのマシンにインストールディレクトリを作成してください。

5.2.5 ディレクトリの空き容量を確認する

実行者　スーパユーザ

HiRDB をインストールする前に，次のディレクトリの空き容量を確認してください。

- インストールディレクトリ
- /tmp ディレクトリ

必要な空き容量については，リリースノートを参照してください。

5.3 HiRDB をインストールする

ここでは，HiRDB のインストール方法について説明します。

5.3.1 HiRDB のインストール

実行者　スーパユーザ

インストール CD-ROM に格納されている日立 PP インストーラを起動して，HiRDB をインストールしてください。HiRDB/ パラレルサーバの場合は，HiRDB/ パラレルサーバを構成するすべてのマシンに HiRDB をインストールしてください。

注意事項

インストールを実行する前に次に示すことを確認してください。

- デバイスファイル名や CD-ROM のマウントディレクトリは，OS，ハードウェア，またはシステムの環境によって異なるため，OS のマニュアルや，システムの環境などを確認してからインストールを実行してください。
- 日立 PP インストーラ実行時の言語種別と実行するターミナルの言語を一致させてください。
- Linux 版の場合，日立 PP インストーラ実行時には，ncurses パッケージを使用します。次のコマンドを実行し，ncurses パッケージがインストールされていることを確認してください。
  （コマンド実行例）
  #rpm -q --qf '%{NAME}-%{ARCH}¥n' ncurses
  （コマンド実行結果）
  ncurses パッケージがインストールされている場合：
  　ncurses-x86_64
  ncurses パッケージがインストールされていない場合：
  　package ncurses is not installed
  ncurses パッケージがインストールされていない場合，必要に応じて関連パッケージも含めてインストールを実施してください。インストール完了後，日立 PP インストーラを起動してください。

Linux 版の HiRDB のインストール手順を次に示します。

手順

1. **CD-ROM をマウントする**
   次に示すコマンドを実行してください。ただし，自動マウントされている場合は，この操作は不要になります。

```
mount -r -o mode=0544 /dev/cdrom /mnt/cdrom
```

下線部分のデバイスファイル名や CD-ROM のマウントディレクトリ名は，使用している環境によって異なります。使用する環境に合わせてファイル名を変更してください。

2. **インストールを開始する**
次に示すコマンドを実行してください。CD-ROM セットアッププログラムが日立 PP インストーラを起動します。

```
/mnt/cdrom/x64lin/setup /mnt/cdrom
```

下線部分は CD-ROM のマウントディレクトリ名を指定します。
CD-ROM のディレクトリ名やファイル名は，使用している環境によって異なります。OS の ls コマンドを実行して，表示されたファイル名に合わせて変更してください。

3. **メインメニューで［I］を指定する**
メインメニューで［I］を指定すると，インストール画面が表示されます。

4. **インストールする製品をカーソルで選択する**
インストールする製品をカーソルで選択し，スペースキーを押します。このとき，複数の製品を選択できます。選択した製品の左側には，<@> が表示されます。

5. **［I］を指定する**
［I］を指定すると，最下行にインストールを確認する次のメッセージが表示されます。

```
Install PP? (y: install,  n: cancel)==>
```

6. **［y］または［Y］を指定する**
［y］または［Y］を指定するとインストールが開始されます。
［n］または［N］を指定するとインストールが中止されます。［Q］を指定すると，メインメニューに戻ります。

7. **インストール処理が終了したら，［Q］を指定する**
最下行にインストール終了を示す次のメッセージが表示されたら，［Q］を指定します。

```
Installation completed.
```

8. **メインメニューで［L］を選択する**
該当するマシンにインストールされている PP の一覧が表示されます。この画面で，インストールした HiRDB が意図したバージョンであるかを確認してください。意図したバージョンでない場合は，HiRDB をアンインストールして，再度正しいバージョンの HiRDB をインストールしてください。また，メインメニューで［P］を選択すると，インストール済み PP 一覧が /tmp/hitachi_PPLIST ディレクトリに出力されます。

9. **メインメニューで［Q］を指定する**
   メインメニューで［Q］を指定し，インストールを終了してください。

5.4 インストールの後作業を行う

ここでは，HiRDB をインストールしたあとに行う作業について説明します。

5.4.1 HiRDB 運用ディレクトリを作成する

実行者　HiRDB 管理者

HiRDB を OS に登録する前に HiRDB 運用ディレクトリを作成してください。作成方法については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「HiRDB 運用ディレクトリの作成」を参照してください。

5.4.2 HiRDB を OS に登録する

実行者　スーパユーザ

pdsetup コマンドを実行して HiRDB を OS に登録してください。HiRDB を OS に登録する方法については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「HiRDB および付加 PP の OS への登録」を参照してください。

5.4.3 環境変数を設定する

実行者　HiRDB 管理者

HiRDB 管理者の環境に環境変数を設定してください。設定方法については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「環境変数の設定」を参照してください。

! 注意事項

環境変数を格納するファイルのアクセス権はほかのユーザに与えないでください。

5.4.4 リモートシェル実行環境を設定する

次に示すシステムを構築する場合にリモートシェル実行環境を設定してください。

- HiRDB/ パラレルサーバの場合
  HiRDB/ パラレルサーバを構成するマシン間のリモートログインを許可してください。それ以外のマシンからのリモートログインは禁止してください。
- IP アドレスを引き継がない高速系切り替え機能を使用する場合
  現用系のマシンと予備系のマシン間のリモートログインを許可してください。それ以外のマシンからのリモートログインは禁止してください。

リモートシェル実行環境の設定方法については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「リモートシェル実行環境の設定」を参照してください。

前記以外のシステムの場合は，リモートシェル実行環境を設定しないでください。リモートシェル実行環境を設定すると，第三者によってシステムが不正利用されるおそれがあるため，セキュリティ上のリスクが高くなります。

5.5 HiRDB の環境設定を行う

実行者　HiRDB 管理者

HiRDB 管理者は次に示すどちらかの方法で HiRDB の環境設定を行ってください。

- 簡易セットアップツールを使用する方法
- コマンドを使用する方法

各環境設定方法のメリット，デメリットについては，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「HiRDB の環境設定の概要」を参照してください。

(1) 簡易セットアップツールを使用する場合

簡易セットアップツールを使用した環境設定については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「簡易セットアップツールによる環境設定」を参照してください。

注意事項

1. HiRDB サーバ用のマシンとは別に，簡易セットアップツール実行用のマシンを準備する必要があります。簡易セットアップツール実行用のマシンはセキュアエリア内に設置して管理するようにしてください。このマシンをセキュアエリア外に設置すると，管理者以外の人間に HiRDB が不正利用されるリスクが高くなります。
2. 簡易セットアップツールを実行すると，HiRDB 管理者用の認可識別子とパスワードが次のように設定されます。
   ・認可識別子：OS アカウントのユーザ名
   ・パスワード：OS アカウントのパスワード
   パスワードが OS アカウントのパスワードと同じになるため，定義系 SQL の GRANT でパスワードを変更してください。
   なお，ここで設定された HiRDB 管理者用の認可識別子は変更できません。

(2) コマンドを使用する場合

コマンドを使用した環境設定については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「コマンドによる環境設定」を参照してください。

注意事項

データベース初期設定ユティリティを実行するときに，-u オプションで HiRDB 管理者用の認可識別子を，-p オプションでパスワードを設定してください。このオプションを指定しないと，HiRDB 管理者用の認可識別子とパスワードが次のように設定されます。

- 認可識別子：OS アカウントのユーザ名（root 権限がある場合は root）
- パスワード：OS アカウントのユーザ名（root 権限がある場合は root）

この場合，パスワードが認可識別子と同じになるため，定義系 SQL の GRANT でパスワードを変更してください。
なお，ここで設定された HiRDB 管理者用の認可識別子は変更できません。

6 HiRDB の環境設定（Windows の場合）

この章では，Windows 版の HiRDB の環境設定方法について説明します。

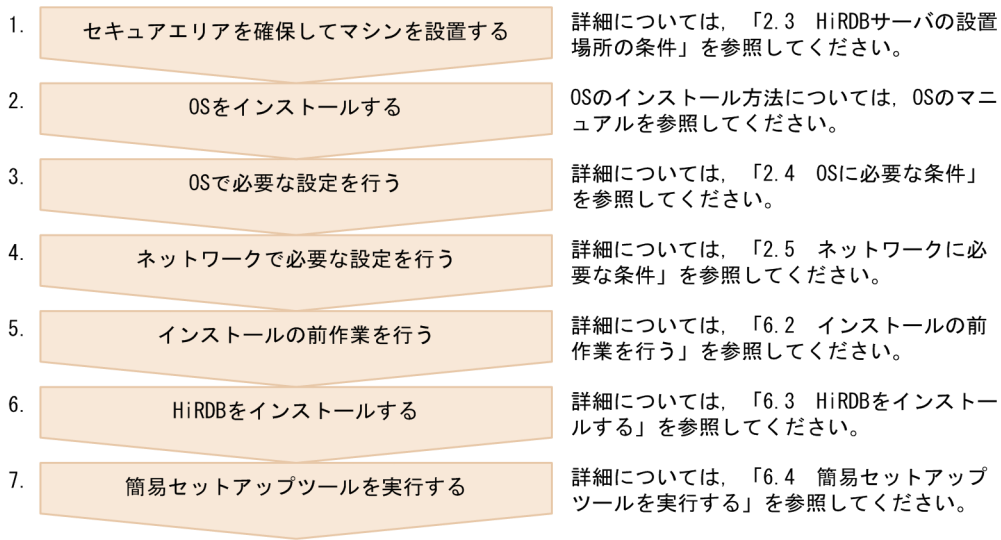
6.1　環境設定手順

参考

Windows 版の HiRDB は ISO/IEC 15408 の評価構成ではありません。

セキュアなシステムを構築する場合は，マニュアル「HiRDB Version 9 システム導入・設計ガイド」で説明している環境設定手順ではなく，ここで説明している手順に従って HiRDB サーバの環境設定を行ってください。HiRDB サーバの環境設定手順を次の図に示します。

図 6-1　HiRDB サーバの環境設定手順（Windows の場合）



6.2 インストールの前作業を行う

HiRDB をインストールする前に次の作業を行います。

- サーバマシン環境の確認
- HiRDB 管理者の登録
- OS 環境ファイルの設定

各作業の詳細については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「インストール前に必要な作業」を参照してください。

6.3 HiRDB をインストールする

HiRDB のインストール方法については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「HiRDB のインストール手順」および「インストール後の作業」を参照してください。

6.4 簡易セットアップツールを実行する

実行者　HiRDB 管理者

簡易セットアップツールを使用して HiRDB の環境設定を行います。簡易セットアップツールを使用した環境設定については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「簡易セットアップツールによる環境設定」を参照してください。

注意事項

1. ほかのマシン（HiRDB サーバ用のマシン以外）で簡易セットアップツールを実行する場合，そのマシンはセキュアエリア内に設置して管理するようにしてください。簡易セットアップツールを実行するマシンをセキュアエリア外に設置すると，管理者以外の人間に HiRDB が不正利用されるリスクが高くなります。
2. 簡易セットアップツールを実行すると，HiRDB 管理者用の認可識別子とパスワードが次のように設定されます。
   ・認可識別子：root
   ・パスワード：root
   パスワードが認可識別子と同じになるため，定義系 SQL の GRANT でパスワードを変更してください。
   なお，ここで設定された HiRDB 管理者用の認可識別子は変更できません。

7 セキュアな環境を維持するための運用

この章では，セキュアな環境を維持するために必要な操作について説明します。

7.1 HiRDB システム定義の指定値を確認する

実行者　HiRDB 管理者

HiRDB のセキュリティを強化するために，次の表に示す HiRDB システム定義のオペランドを指定してください。

表 7-1　セキュリティを強化するために指定するオペランド

オペランド	指定する理由
pd_connect_errmsg_hide = Y	ユーザ認証エラーが発生したときのメッセージに，認可識別子に関する情報を出力しないようにするため。
pd_security_host_group	セキュリティ上のリスクを軽減するため。

注意事項

- システム構成変更コマンド（pdchgconf コマンド）を使用しない場合，HiRDB システム定義を変更するには pdstop コマンドで HiRDB を一度終了する必要があります。pdstop コマンドの実行時，pdstop コマンドの処理が完了するまでコマンドを入力したウィンドウを閉じないでください。ウィンドウを閉じると，pdstop コマンドが強制終了するため，共用資源の整合性が保てなくなり，HiRDB が異常終了します。
  pdstop 以外のコマンドおよびユティリティについても同様に，実行中にウィンドウを閉じないでください。
- pd_sql_command_exec_users オペランドは指定しないでください。
- ユーザ認証エラーが発生したときの KFPA19632-E メッセージに，認可識別子に関する情報を出力しないようにするため，pd_connect_errmsg_hide オペランドには Y を指定してください。Y を指定した場合，KFPA19632-E メッセージに認可識別子の情報が出力されないため，指定した認可識別子を第三者に知られる可能性を低減できます。

7.2　ディクショナリ表の参照権限を設定する

実行者　HiRDB 管理者

データベース構成変更ユティリティの alter system 文で，ディクショナリ表の参照権限を設定してください。

ディクショナリ表の参照権限を設定したあとに，データベース利用者のアカウントでディクショナリ表を検索し，実際にディクショナリ表が参照できないことを確認してください。

参考

データベース初期設定ユティリティの define system 文でもディクショナリ表の参照権限を設定できます。したがって，コマンドを使用して HiRDB の環境設定を行う場合は，データベース初期設定ユティリティ実行時（「5.5(2) コマンドを使用する場合」の作業時）に設定できます。

7.3 監査情報の取得準備をする

実行者 HiRDB 管理者および監査人

セキュリティ監査機能の環境設定を行ってください。セキュリティ監査機能の環境設定については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

セキュリティ監査機能の環境設定での注意事項を次に示します。

7.3.1 システム定義の指定値

（1）pd_audit

HiRDB の開始と同時に監査証跡を取得するため，pd_audit オペランドには Y を指定してください。

（2）pd_aud_async_buff_size および pd_aud_async_buff_count

HiRDB が強制終了または異常終了した場合，直前の監査ログが失われることがあります。そのため，HiRDB の強制終了はできる限り実行しないようにしてください。

pd_aud_async_buff_size オペランドおよび pd_aud_async_buff_count オペランドに小さな値を指定すると，監査証跡の損失を防げる可能性が高くなりますが，それに比例して性能も劣化します。これらのオペランドの指定値については，性能との兼ね合いを考慮して決定してください。

万が一，HiRDB が強制終了または異常終了した場合，最大，pd_aud_async_buff_size オペランドの指定値× pd_aud_async_buff_count オペランドの指定値分の監査ログが失われるおそれがあります。

（3）pd_aud_no_standby_file_opr

pd_aud_no_standby_file_opr オペランドには forcewrite（デフォルト値）を指定してください。ただし，forcewrite を指定した場合，既存の監査証跡ファイルがスワップ先となるため，既存のファイルが上書きされることがあります。既存のファイルがスワップ先となった場合は，KFPS05706-W メッセージが出力されます。KFPS05706-W メッセージが出力された場合，HiRDB 管理者は，データロード待ちの監査証跡ファイルをデータロードしてください。このとき，pdload コマンドの -u オプションには監査人の認可識別子を指定してください。コマンドを実行すると，パスワード入力要求のメッセージが表示されるため，監査人が自身のパスワードを入力してください。

7.3.2 監査人のパスワード変更

監査人の登録が終了したあと，監査人は定義系 SQL の GRANT AUDIT でパスワードを変更してください。

7.3.3 SQL の指定値

CREATE AUDIT で監査対象イベントを定義する場合，AUDITTYPE オペランドには EVENT または ANY を指定してください。

7.4 パスワードのセキュリティ対策を行う

ここでは，HiRDB の CONNECT 関連セキュリティ機能を使用したパスワードのセキュリティ対策について説明します。

7.4.1 パスワードの禁止条件を設定する

実行者　DBA 権限保持者

定義系 SQL の CREATE CONNECTION SECURITY で，パスワードの禁止条件を設定してください。パスワードの禁止条件を設定する方法については，マニュアル「HiRDB Version 9 システム運用ガイド」の「パスワードの文字列制限」を参照してください。

パスワードの禁止条件を設定したあとに，パスワードの変更テストを行ってください。条件に違反したパスワードを指定して GRANT を実行し，その操作がエラーになるか確認してください。

7.4.2 連続認証失敗許容回数とアカウントロック期間を設定する

実行者　DBA 権限保持者

定義系 SQL の CREATE CONNECTION SECURITY で，連続認証失敗許容回数とアカウントロック期間を設定してください。連続認証失敗許容回数とアカウントロック期間を設定する方法については，マニュアル「HiRDB Version 9 システム運用ガイド」を参照してください。

連続認証失敗許容回数とアカウントロック期間を設定したあとに，ユーザ認証テストを行ってください。クライアント環境定義の PDUSER オペランドに，不正なパスワードを指定して UAP を実行してみてください。ユーザ認証不正を何度か繰り返して，アカウントロック状態になるか確認してください。

なお，アカウントロック状態を解除するには，アカウントロック期間を過ぎるか，または pdacunlck コマンドで解除するかの二つの方法があります。pdacunlck コマンドは HiRDB 管理者だけが実行できるため，HiRDB 管理者の認可識別子で前記のテストを行わないでください。HiRDB 管理者の認可識別子がアカウントロック状態になると，pdacunlck コマンドが実行できなくなるため，アカウントロック期間が過ぎるまでアカウントロック状態を解除できなくなります。

ポイント

pdacunlck コマンドを実行してアカウントロック状態を解除する場合は，そのアカウントを持つ本人からの要求であることを必ず確認してください。パスワードの入力ミスが本人によるものでない場合，第三者による HiRDB への不正なアクセスが試された可能性があります。

7.5 ユーザを登録して権限を与える

ここでは，HiRDB ユーザを登録して権限を与える方法について説明します。

7.5.1 DBA 権限を与える

実行者 DBA 権限保持者

権限を管理する HiRDB ユーザに DBA 権限を与えてください。定義系 SQL の GRANT で，必要な HiRDB ユーザに対してだけ DBA 権限を与えてください。

なお，DBA 権限を最初に持っているのは HiRDB 管理者です。したがって，まず HiRDB 管理者がほかの HiRDB ユーザに DBA 権限を与えてください。

（例）

認可識別子が DBA001 の HiRDB ユーザを登録し，その HiRDB ユーザに DBA 権限を与えます。初期パスワードには TC201asD を設定します。

```
GRANT DBA TO DBA001 IDENTIFIED BY "TC201asD"
```

注意事項

登録された HiRDB ユーザは，定義系 SQL の GRANT で初期パスワードを変更してください。

7.5.2 スキーマ定義権限を与える

実行者 DBA 権限保持者

表を定義し，所有・管理する HiRDB ユーザにスキーマ定義権限を与えてください。定義系 SQL の GRANT で，必要な HiRDB ユーザに対してだけスキーマ定義権限を与えてください。

なお，表を定義し，所有・管理する HiRDB ユーザには，CONNECT 権限とスキーマ定義権限が必要になります。権限は CONNECT 権限，スキーマ定義権限の順に与えてください。逆にした場合，SQL の実行時にエラーとなります。

（例）

認可識別子が SCH001 の HiRDB ユーザを登録し，その HiRDB ユーザに CONNECT 権限とスキーマ定義権限を与えます。初期パスワードには TC356knH を設定します。

```
GRANT CONNECT TO SCH001 IDENTIFIED BY "TC356knH"
GRANT SCHEMA TO SCH001
```

注意事項

登録された HiRDB ユーザは，定義系 SQL の GRANT で初期パスワードを変更してください。

7.5.3 CONNECT 権限を与える

実行者　DBA 権限保持者

表をアクセスする HiRDB ユーザに CONNECT 権限を与えてください。定義系 SQL の GRANT で，必要な HiRDB ユーザに対してだけ CONNECT 権限を与えてください。

（例）

認可識別子が USR001 の HiRDB ユーザを登録し，その HiRDB ユーザにスキーマ定義権限を与えます。初期パスワードには TC277reZ を設定します。

```
GRANT CONNECT TO USR001 IDENTIFIED BY "TC277reZ"
```

注意事項

登録された HiRDB ユーザは，定義系 SQL の GRANT で初期パスワードを変更してください。

7.6 ユーザ用 RD エリアを作成する

実行者 HiRDB 管理者

データベース構成変更ユティリティの create rdarea 文で，表を格納するユーザ用 RD エリアを作成してください。RD エリアの作成方法については，マニュアル「HiRDB Version 9 システム運用ガイド」の「RD エリアを作成する方法（RD エリアの追加）」を参照してください。

なお，ユーザ用 RD エリアを作成する前に，pdfmkfs コマンドで RD エリア用の HiRDB ファイルシステム領域を作成する必要があります。RD エリア用の HiRDB ファイルシステム領域の作成方法については，マニュアル「HiRDB Version 9 システム運用ガイド」の「HiRDB ファイルシステム領域を作成（初期設定）する方法」を参照してください。

参考

データベース初期設定ユティリティの create rdarea 文でもユーザ用 RD エリアを作成できます。したがって，コマンドを使用して HiRDB の環境設定を行う場合は，データベース初期設定ユティリティ実行時（「5.5(2) コマンドを使用する場合」の作業時）にユーザ用 RD エリアを作成できます。

7.7　表を作成してアクセス権限を与える

実行者　スキーマ定義権限保持者（表の所有者）

次に示す手順で表を作成し，その表をアクセスする HiRDB ユーザにアクセス権限を与えてください。

手順

1. 定義系 SQL の CREATE SCHEMA でスキーマを定義してください。
2. 定義系 SQL の CREATE TABLE で表を定義してください。
3. データベース作成ユティリティで表にデータロードを行ってください。
4. 表をアクセスする HiRDB ユーザに，定義系 SQL の GRANT でアクセス権限を与えてください。

表の作成方法の詳細については，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「データベースの作成」を参照してください。

7.8 運用コマンド実行時の注意事項

ここでは，HiRDB の運用コマンドを実行する時の注意事項について説明します。次に示す注意事項に従わないで運用コマンドを実行した場合，HiRDB のセキュアな環境が維持できなくなるおそれがあります。

（1） pdaudend

pdaudend コマンドを実行する場合は，その正当性を確認してください。原則として，コマンドでの監査証跡の取得開始および停止は，緊急時以外は実行しないでください。

（2） pdaudswap

pdaudswap コマンドを実行する場合は，データロード済みの監査証跡ファイルがあること，または監査証跡ファイル数が上限（pd_aud_max_generation_num の値）に達していないことを確認してください。

スワップ先にできるファイルがなく，データロード待ちの監査証跡ファイルにスワップした場合，そのファイルに格納されていた監査証跡は上書きされ，内容が失われます。

（3） pdfbkup

pdfbkup コマンドを実行する場合は，すでに使用されている HiRDB ファイルシステム領域を退避先に指定しないよう注意してください。

（4） pdfmkfs

pdfmkfs コマンドを実行する場合は，すでに使用されている HiRDB ファイルシステム領域を誤って初期設定しないよう注意してください。

（5） pdfrm

pdfrm コマンドを実行する場合は，すでに使用されている HiRDB ファイルを誤って削除しないよう注意してください。

（6） pdfrstr

pdfrstr コマンドを実行する場合は，バックアップファイルに退避した HiRDB ファイルの用途と，リストア後の HiRDB ファイルの用途が一致していることを確認してください。また，古いバックアップファイルでリストアしないよう注意してください。

（7） pdinit

pdinit コマンドを実行すると，ディクショナリ表で管理される定義系 SQL の実行結果はすべて消去されます。データベースを再構築する以外の目的で，pdinit コマンドを実行しないでください。

(8) pdrorg

ディクショナリ表の再編成がリロードの段階でエラーになった場合を除き，ディクショナリ表のリロードはしないでください。また，ディクショナリ表のリロードをする場合は，再編成でのエラーの原因を取り除いた上で，その時に生成されたアンロードデータファイルを使用してください。

(9) pdstop

pdstop コマンドを実行して HiRDB を強制終了させると，監査証跡ファイルに出力されていないバッファ上の監査証跡の内容は失われます。HiRDB を強制終了させる必要がある場合は，直前に pdaudswap コマンドを実行し，バッファ上の監査証跡の内容を監査証跡ファイルに出力してください。

7.9 SQL 実行時の注意事項

7.9.1 CONNECT 権限を取り消す場合

定義系 SQL の REVOKE で CONNECT 権限を取り消す場合，取り消すユーザが接続していない状態で行ってください。接続中のユーザの CONNECT 権限は取り消せないことがあります。接続中のユーザの CONNECT 権限を取り消した場合は，取り消したユーザの接続が切れたあとにディクショナリ表（SQL_USERS）を参照して，CONNECT 権限が取り消されていることを確認してください。

CONNECT 権限の取り消し手順の例を次に示します。

手順

1. REVOKE を実行する DBA 権限保持者が HiRDB に接続します。
2. pdchprc コマンドで最大起動プロセス数を 1 にします。ただし，HiRDB/ パラレルサーバの場合は，上記の DBA 権限保持者が接続しているフロントエンドサーバの最大起動プロセス数を 1 にして，ほかのフロントエンドサーバの最大起動プロセス数を 0 にしてください。
3. 接続中のユーザが上記の DBA 権限保持者だけになるまで待ちます。なお，接続中のユーザは，pdls -d act コマンドで確認できます。また，問題がなければ，接続中の UAP やユティリティを pdcancel コマンドで強制終了させてもかまいません。
4. HiRDB/ パラレルサーバの場合，接続しないフロントエンドサーバを停止します（REVOKE を実行するフロントエンドサーバだけ稼働している状態にしてください）。
5. REVOKE を実行して，不要な CONNECT 権限を取り消します。
6. ディクショナリ表（SQL_USERS）を参照して，CONNECT 権限が取り消されていることを確認します。
7. pdchprc コマンドで変更した最大起動プロセス数を元に戻します。なお，HiRDB/ パラレルサーバの場合は，停止したフロントエンドサーバを開始してから戻してください。

7.9.2 スキーマを削除する場合

定義系 SQL の DROP SCHEMA でスキーマを削除しても，与えたアクセス権限はそのまま残ります。同じスキーマおよび表を再定義すると，改めてアクセス権限を与えなくても再利用できてしまいます。これを避けるためには，明示的に REVOKE でアクセス権限を取り消す必要があります。スキーマ削除とアクセス権限取り消しの順序は問いません。

なお，スキーマは表の所有者および DBA 権限保持者が削除できますが，アクセス権限を

削除できるのは表の所有者だけです。

8 HiRDB クライアントの管理

この章では，HiRDB クライアントの管理方法について説明します。

8.1 HiRDB クライアントの環境設定

8.1.1 HiRDB クライアントの設置

HiRDB サーバの設置場所のセキュリティが強化されていても，HiRDB サーバのデータベースを利用する HiRDB クライアントの設置場所の管理が不適切であると，第三者による成り済ましなどによって，データが持ち出されたり，改ざんされたりするおそれがあります。このため，セキュアなシステムを構築する場合には，HiRDB クライアントの環境構築と運用にも注意する必要があります。HiRDB クライアントが次に示す環境で使用されるように管理してください。

- HiRDB クライアントは，ネットワークの管理者が管理しているローカルエリアネットワーク環境下に設置します。
- HiRDB クライアント用のマシンにはスクリーンセーバーにパスワード保護を掛けて，第三者に使用されないようにします。
- HiRDB クライアントには，不要なソフトウェアをインストールしないようにしてください。具体的には，次の対策を徹底してください。
  - ネットワーク盗聴ソフトのインストール防止
  - バイナリエディタ，デバッガなどの，UAP を改ざんする可能性があるツールのインストール禁止
- HiRDB クライアントでは，UAP と HiRDB SQL Executer から HiRDB サーバに電文を送信できるようにしてください。
- HiRDB クライアントでは，設定済みのクライアント環境定義の内容をむやみに変更することを禁止します。なお，クライアント環境定義の PDUSER については，HiRDB クライアントから UAP を実行するたびに認可識別子とパスワードを設定してください。さらに，UAP の実行が完了したら，PDUSER の認可識別子とパスワードを削除してください。
- HiRDB/Developer's Kit または HiRDB/Run Time に含まれるランタイムを経由しない電文を HiRDB サーバに送信する UAP や，マニュアルに記載されていない機能を使用した UAP の開発と使用を禁止します。
- クライアント環境定義 PDNAMEPORT には，システム定義の pd_name_port オペランドの値を設定し，変更しないように維持してください。また，クライアント環境定義 HiRDB_PDNAMEPORT についても，同様に pd_name_port オペランドの値を設定し，変更しないように維持してください。
- マルチフロントエンドサーバ構成で高速接続機能を使用する場合，クライアント環境定義 PDSERVICEPORT には，システム定義の pd_service_port オペランドの値を設定し，変更しないように維持してください。なお，高速接続機能を使用しない場合は，クライアント環境定義 PDSERVICEPORT には値を設定しないでください。
- HiRDB クライアントの OS アカウントは，データベース利用者以外には与えないでください。具体的には，次の対策を徹底してください。

- UAP 開発用の HiRDB クライアントの OS アカウントは，管理下にある UAP 開発者だけに付与する。
- 監査用の HiRDB クライアントの OS アカウントは，監査人だけに付与する。
- 各アカウントには業務に必要な権限だけを付与する。

8.1.2 HiRDB クライアントのインストール

HiRDB クライアントのインストールおよび環境設定については，マニュアル「HiRDB Version 9 UAP 開発ガイド」の「クライアントの環境設定」を参照してください。なお，HiRDB クライアントをインストールする場合，セットアップ方法として「標準」，「コンパクト」，または「カスタム」を選択できます。

注意事項

HiRDB クライアント用のマシンは，HiRDB のデータベースに対して問題のあるソフトウェアが実行されないように管理する必要があります。インストールするソフトウェアの数が多くなるほど，システムの管理やセキュリティ対策が複雑になるため，セキュリティ上のリスクが高くなります。

参考

- ISO/IEC 15408 の評価は，セットアップ方法「コンパクト」でインストールした HiRDB クライアントで行われました。
- HiRDB クライアントは，セキュアエリア外に設置できますが，適切に管理されている必要があります。HiRDB クライアントの管理については，「8.1.1　HiRDB クライアントの設置」を参照してください。

8.2 出力情報の管理

HiRDB クライアントから実行する UAP で障害が発生した場合，トラブルシュート情報が出力されます。ここでは，出力される情報の管理について説明します。

UAP 実行時に障害が発生した場合，トラブルシュート機能を利用して障害要因を調査します。このトラブルシュート機能で出力されるファイルの内容には，認可識別子，HiRDB サーバの情報，HiRDB が内部的に管理している情報などが含まれている場合があります。これらの出力情報が第三者によって参照されると，セキュリティ上の弱点になる可能性があります。そのため，トラブルシュート機能で出力されるファイルが，不正に使用されないように管理する必要があります。

UAP 実行者（データベース利用者）は，トラブルシュート機能で出力されるトレースファイル，ログファイルなどの格納先ディレクトリに対して参照権限を設定するなど，ファイルの内容が第三者に漏れないように管理してください。

トラブルシュート機能で出力されるファイルと，格納先ディレクトリの設定方法を次の表に示します。なお，トラブルシュート機能の詳細については，マニュアル「HiRDB Version 9 UAP 開発ガイド」を参照してください。

表 8-1 トラブルシュート機能で出力されるファイルと，格納先ディレクトリの設定方法

トラブルシュート機能の種類	出力されるファイル	格納先ディレクトリの設定方法
SQL トレース機能	SQL トレースファイル	クライアント環境定義の PDCLTPATH
エラーログ機能	エラーログファイル	クライアント環境定義の PDCLTPATH
拡張 SQL エラー情報出力機能	エラーログファイル	クライアント環境定義の PDCLTPATH
	SQL エラーレポートファイル※	pd_uap_exerror_log_dir オペランド
UAP 統計レポート機能	UAP 統計レポートファイル	クライアント環境定義の PDCLTPATH
コマンドトレース機能	コマンドトレースファイル	クライアント環境定義の PDCLTPATH
SQL トレース動的取得機能	SQL トレースファイル	クライアント環境定義の PDCLTPATH
再接続トレース機能	再接続トレースファイル	クライアント環境定義の PDCLTPATH
HiRDB SQL Tuning Advisor 用アクセスパス情報ファイル	アクセスパス情報ファイル	クライアント環境定義の PDTAAPINFPATH

注※ SQL エラーレポートファイルは，HiRDB サーバ側に出力されます。

索引

き

け

さ

し

す

せ

そ

て

に

ね

は

ひ

ま

め

や

ゆ

よ

り

れ

ろ

わ