HITACHI
Inspire the Next

スケーラブルデータベースサーバ

HiRDB Version 8 データベース暗号化機能

解説・手引・文法・操作書

3020-6-367-43

■ 対象製品

●適用 OS：HP-UX 11i V2(IPF)，HP-UX 11i V3(IPF)

P-1J62-1681 HiRDB/Single Server Plus Version 8(64) 08-05，08-51※1

P-1J62-1881 HiRDB/Parallel Server Plus Version 8(64) 08-05，08-51※1

●適用 OS：AIX 5L V5.1，AIX 5L V5.2，AIX 5L V5.3，AIX V6.1，AIX V7.1

P-1M62-1681 HiRDB/Single Server Plus Version 8(64) 08-05，08-51※1

P-1M62-1881 HiRDB/Parallel Server Plus Version 8(64) 08-05，08-51※1

●適用 OS：Red Hat Enterprise Linux AS 3(AMD64 & Intel EM64T)※2, Red Hat Enterprise Linux AS 4(AMD64 & Intel EM64T)，Red Hat Enterprise Linux ES 4(AMD64 & Intel EM64T)，Red Hat Enterprise Linux 5 Advanced Platform (AMD/Intel 64)，Red Hat Enterprise Linux 5 (AMD/Intel 64)

P-9W62-1283 HiRDB/Single Server Plus Version 8(64) 08-05，08-51※1

P-9W62-1483 HiRDB/Parallel Server Plus Version 8(64) 08-05，08-51※1

●適用 OS：Windows 2000，Windows Server 2003，Windows Server 2008，Windows XP，Windows Vista，Windows 7

P-2462-7284 HiRDB/Single Server Plus Version 8 08-05，08-51※1

P-2462-7484 HiRDB/Parallel Server Plus Version 8 08-05，08-51※1

●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-2962-7284 HiRDB/Single Server Plus Version 8(64) 08-05，08-51※1

P-2962-7484 HiRDB/Parallel Server Plus Version 8(64) 08-05，08-51※1

注※1　08-51 は，08-05 の修正版のバージョン・リビジョン番号です。

注※2　動作環境としては，Intel EM64T にだけ対応しています。

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。

■ 輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、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

2016 年 9 月 3020-6-367-43

■ 著作権

変更内容

変更内容(3020-6-367-43)　HiRDB Plus Version 8 08-05，08-51

追加・変更内容	変更個所
リリースノートのマニュアル訂正を反映しました。	－

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(3020-6-367-42)　HiRDB Plus Version 8 08-05，08-51

追加・変更内容
(1)前提プラットフォーム [訂正前] 前提プラットフォームは次のどれかになります。 • HP-UX(IPF) • AIX • Windows 2000 • Windows XP • Windows Server • Windows Vista Business，Windows Vista Enterprise，または Windows Vista Ultimate [訂正後] 前提プラットフォームは次のどれかになります。 • HP-UX(IPF) • AIX • Windows 2000 • Windows XP • Windows Server • Windows Vista Business，Windows Vista Enterprise，または Windows Vista Ultimate • Linux(EM64T)
インストール [訂正前] 注意 • HiRDB Plus がインストールされているサーバマシンに，HiRDB を上書きインストールしないでください。 • HiRDB/パラレルサーバの場合，すべてのユニットに HiRDB Plus をインストールしてください。HiRDB Plus と HiRDB との混在はできません。 • UNIX 版 HiRDB Plus の場合，HiRDB Plus をアンインストールするときは，先に HiRDB Data Convert Type1 Option をアンインストールしてから，HiRDB をアンインストールしてください。 • pdadmvr コマンドで，サーバマシンにインストールされている HiRDB の種類（HiRDB Plus または HiRDB）を確認できます。 [訂正後] 注意 • HiRDB Plus がインストールされているサーバマシンに，HiRDB を上書きインストールしないでください。 • HiRDB/パラレルサーバの場合，すべてのユニットに HiRDB Plus をインストールしてください。HiRDB Plus と HiRDB との混在はできません。 • UNIX 版 HiRDB Plus の場合，HiRDB Plus をアンインストールするときは，先に HiRDB Data Convert Type1 Option をアンインストールしてから，HiRDB をアンインストールしてください。 • pdadmvr コマンドで，サーバマシンにインストールされている HiRDB の種類（HiRDB Plus または HiRDB）を確認できます。

追加・変更内容
• UNIX 版 HiRDB Plus をインストールする場合は，HiRDB 本体と HiRDB Data Convert Type1 Option を両方一緒にインストールしてください。 また，HiRDB 本体と HiRDB Data Convert Type1 Option を別々にインストールする場合は，HiRDB 本体をインストールしたあとに HiRDB Data Convert Type1 Option をインストールしてください。 HiRDB Data Convert Type1 Option だけのインストールはできません。

変更内容(3020-6-367-20)　HiRDB Plus Version 8 08-05

追加・変更内容
ALTER TABLE で暗号化列の追加，および削除をできるようにしました。
次のメッセージを変更しました。 KFPA19640-E

変更内容(3020-6-367-10)　HiRDB Plus Version 8 08-04

追加・変更内容
HiRDB の稼働プラットフォームに Windows Server 2008 を追加しました。
DECIMAL 型の精度を拡張し，38 けたまで定義できるようになりました。また，精度 20 けた以上の DECIMAL 型の列にインデクスを定義できるようにしました。これに伴い，表の格納ページ数の計算方法，およびインデクスの格納ページ数の計算方法を変更しました。
SQLSTATE を細分化できるようにしました。これに伴い，SQLSTATE を追加しました。

はじめに

このマニュアルは，次に示す製品の機能と使い方について説明したものです。

- P-1J62-1681 HiRDB/Single Server Plus Version 8(64)
- P-1J62-1881 HiRDB/Parallel Server Plus Version 8(64)
- P-1M62-1681 HiRDB/Single Server Plus Version 8(64)
- P-1M62-1881 HiRDB/Parallel Server Plus Version 8(64)
- P-2462-7284 HiRDB/Single Server Plus Version 8
- P-2462-7484 HiRDB/Parallel Server Plus Version 8

以降，このマニュアルでは，上記の製品を総称して「HiRDB」または「HiRDB Plus」と表記します。

■ 対象読者

HiRDB を使って，暗号化されたリレーショナルデータベースシステムを構築または運用する方々を対象にしています。

このマニュアルの記述は，次に示す知識があることを前提にしています。

- UNIX，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

また，このマニュアルは，HiRDB のマニュアルを前提としていますので，あらかじめお読みいただくことをお勧めします。

■ 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（Windows 用マニュアル）

- HiRDB Version 8 解説（Windows(R)用）（3020-6-351）
- HiRDB Version 8 システム導入・設計ガイド（Windows(R)用）（3020-6-352）
- HiRDB Version 8 システム定義（Windows(R)用）（3020-6-353）
- HiRDB Version 8 システム運用ガイド（Windows(R)用）（3020-6-354）
- HiRDB Version 8 コマンドリファレンス（Windows(R)用）（3020-6-355）
- HiRDB ファーストステップガイド（Windows(R)用）（3020-6-054）

HiRDB（UNIX 用マニュアル）

- HiRDB Version 8 解説（UNIX(R)用）（3000-6-351）
- HiRDB Version 8 システム導入・設計ガイド（UNIX(R)用）（3000-6-352）
- HiRDB Version 8 システム定義（UNIX(R)用）（3000-6-353）
- HiRDB Version 8 システム運用ガイド（UNIX(R)用）（3000-6-354）
- HiRDB Version 8 コマンドリファレンス（UNIX(R)用）（3000-6-355）
- インナレプリカ機能 HiRDB Staticizer Option Version 8（3000-6-363）
- HiRDB Version 8 ディザスタリカバリシステム　構築・運用ガイド（3000-6-364）
- HiRDB ファーストステップガイド（UNIX(R)用）（3000-6-254）

HiRDB（Windows，UNIX 共通マニュアル）

- HiRDB Version 8 UAP 開発ガイド（3020-6-356）

- HiRDB Version 8 SQL リファレンス（3020-6-357）
- HiRDB Version 8 メッセージ（3020-6-358）
- HiRDB Version 8 セキュリティガイド（3020-6-359）
- HiRDB Version 8 XDM/RD E2 接続機能（3020-6-365）
- HiRDB Version 8 バッチ高速化機能（3020-6-368）
- HiRDB データ連動機能 HiRDB Datareplicator Version 8（3020-6-360）
- HiRDB データ連動拡張機能 HiRDB Datareplicator Extension Version 8（3020-6-361）
- データベース抽出・反映サービス機能 HiRDB Dataextractor Version 8（3020-6-362）
- HiRDB 全文検索プラグイン HiRDB Text Search Plug-in Version 8（3020-6-375）
- HiRDB XML 拡張機能 HiRDB XML Extension Version 8（3020-6-376）

なお，本文中で使用している HiRDB Version 8 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。

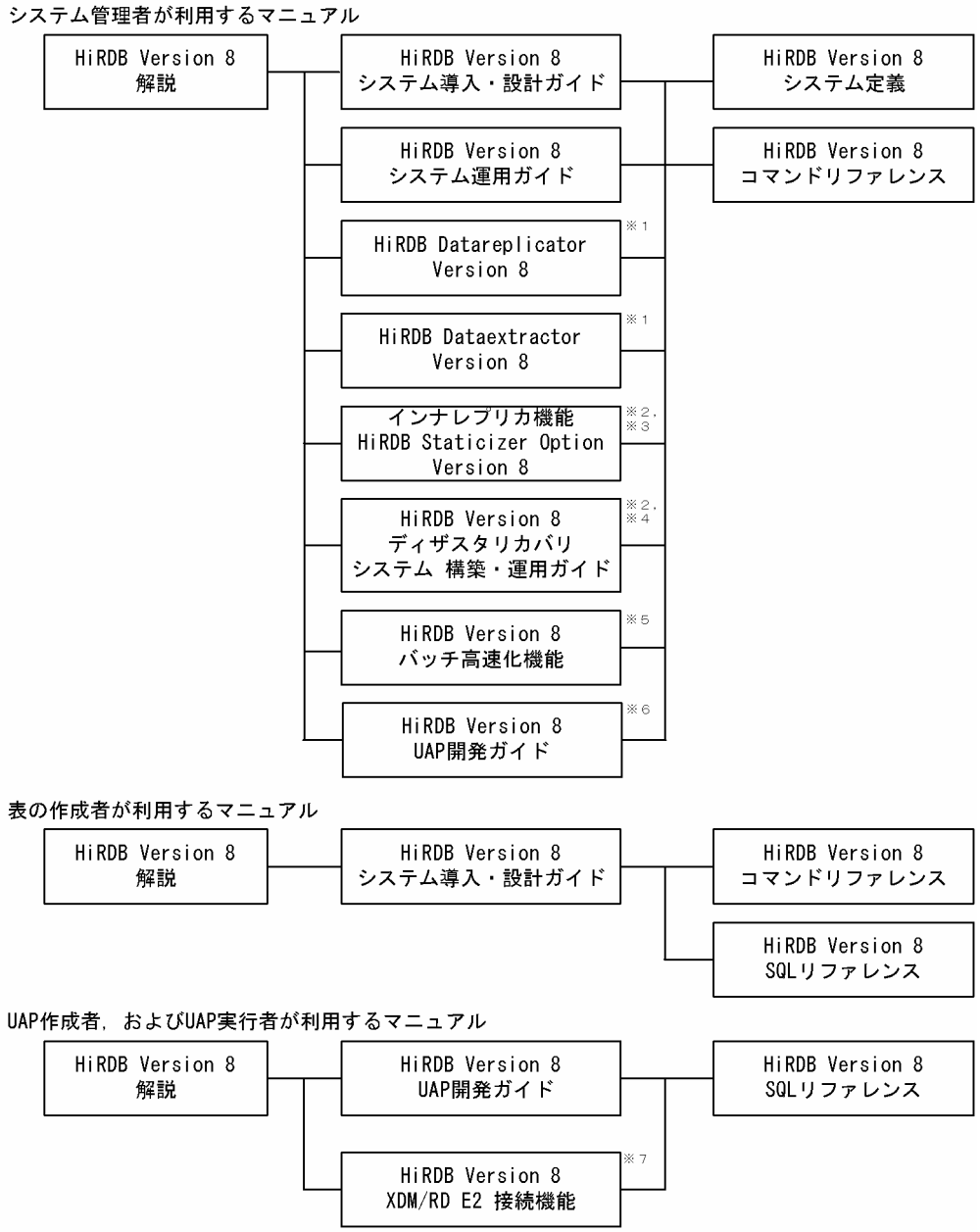
関連製品

- HiRDB External Data Access Version 8（3020-6-366）

■ 利用者ごとの関連マニュアル

HiRDB のマニュアルをご利用になる場合，利用者ごとに次のようにお読みください。

また，より理解を深めるために，左側のマニュアルから順にお読みいただくことをお勧めします。



注※１　レプリケーション機能を使用してデータ連携をする場合にお読みください。
注※２　UNIX用マニュアルです。Windows用はありません。
注※３　インナレプリカ機能を使用する場合にお読みください。
注※４　ディザスタリカバリシステムを構築する場合にお読みください。
注※５　インメモリデータ処理によるバッチ高速化を行う場合にお読みください。
注※６　OLTPシステムと連携する場合は必ずお読みください。
注※７　XDM/RD E2 接続機能を使用して，XDM/RD E2のデータベースを操作する場合にお読みください。

■ 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/Single Server Plus Version 8	HiRDB/シングルサーバ	HiRDB または HiRDB Plus

製品名称または名称	表記	
HiRDB/Single Server Plus Version 8(64)		
HiRDB/Parallel Server Plus Version 8	HiRDB/パラレルサーバ	
HiRDB/Parallel Server Plus Version 8(64)		
HiRDB/Single Server Version 8	HiRDB/シングルサーバ	HiRDB または HiRDB サーバ
HiRDB/Single Server Version 8(64)		
HiRDB/Parallel Server Version 8	HiRDB/パラレルサーバ	
HiRDB/Parallel Server Version 8(64)		
HiRDB/Developer's Kit Version 8	HiRDB/Developer's Kit	HiRDB クライアント
HiRDB/Developer's Kit Version 8(64)		
HiRDB/Run Time Version 8	HiRDB/Run Time	
HiRDB/Run Time Version 8(64)		
HiRDB Datareplicator Version 8	HiRDB Datareplicator	
HiRDB Dataextractor Version 8	HiRDB Dataextractor	
HiRDB Text Search Plug-in Version 8	HiRDB Text Search Plug-in	
HiRDB XML Extension Version 8	HiRDB XML Extension	
HiRDB Spatial Search Plug-in Version 3	HiRDB Spatial Search Plug-in	
HiRDB Staticizer Option Version 8	HiRDB Staticizer Option	
HiRDB LDAP Option Version 8	HiRDB LDAP Option	
HiRDB Advanced Partitioning Option Version 8	HiRDB Advanced Partitioning Option	
HiRDB Advanced High Availability Version 8	HiRDB Advanced High Availability	
HiRDB Non Recover Front End Server Version 8	HiRDB Non Recover FES	
HiRDB Disaster Recovery Light Edition Version 8	HiRDB Disaster Recovery Light Edition	
HiRDB Accelerator Version 8	HiRDB Accelerator	
HiRDB External Data Access Version 8	HiRDB External Data Access	
HiRDB External Data Access Adapter Version 8	HiRDB External Data Access Adapter	
HiRDB Adapter for XML - Standard Edition	HiRDB Adapter for XML	
HiRDB Adapter for XML - Enterprise Edition		
HiRDB Control Manager	HiRDB CM	
HiRDB Control Manager Agent	HiRDB CM Agent	
Hitachi TrueCopy	TrueCopy	
Hitachi TrueCopy basic		

製品名称または名称	表記	
TrueCopy		
TrueCopy remote replicator		
JP1/Automatic Job Management System 2	JP1/AJS2	
JP1/Automatic Job Management System 2 - Scenario Operation	JP1/AJS2-SO	
JP1/Cm2/Extensible SNMP Agent	JP1/ESA	
JP1/Cm2/Extensible SNMP Agent for Mib Runtime		
JP1/Cm2/Network Node Manager	JP1/NNM	
JP1/Integrated Management - Manager	JP1/Integrated Management または JP1/IM	
JP1/Integrated Management - View		
JP1/Magnetic Tape Access	EasyMT	
EasyMT		
JP1/Magnetic Tape Library	MTguide	
JP1/NETM/Audit - Manager	JP1/NETM/Audit	
JP1/NETM/DM	JP1/NETM/DM	
JP1/NETM/DM Manager		
JP1/Performance Management	JP1/PFM	
JP1/Performance Management - Agent Option for HiRDB	JP1/PFM-Agent for HiRDB	
JP1/Performance Management - Agent Option for Platform	JP1/PFM-Agent for Platform	
JP1/Performance Management/SNMP System Observer	JP1/SSO	
JP1/VERITAS NetBackup BS v4.5	NetBackup	
JP1/VERITAS NetBackup v4.5		
JP1/VERITAS NetBackup BS V4.5 Agent for HiRDB License	JP1/VERITAS NetBackup Agent for HiRDB License	
JP1/VERITAS NetBackup V4.5 Agent for HiRDB License		
JP1/VERITAS NetBackup 5 Agent for HiRDB License		
OpenTP1/Server Base Enterprise Option	TP1/EE	
Virtual-storage Operating System 3/Forefront System Product	VOS3/FS	VOS3
Virtual-storage Operating System 3/Leading System Product	VOS3/LS	
Extensible Data Manager/Base Extended Version 2 XDM 基本プログラム XDM/BASE E2	XDM/BASE E2	
XDM/Data Communication and Control Manager 3 XDM データコミュニケーションマネジメントシステム XDM/DCCM3	XDM/DCCM3	
XDM/Relational Database	XDM/RD	XDM/RD

製品名称または名称	表記	
リレーショナルデータベースシステム XDM/RD		
XDM/Relational Database Extended Version 2 リレーショナルデータベースシステム XDM/RD E2	XDM/RD E2	
VOS3 Database Connection Server	DB コネクションサーバ	
BEA WebLogic Server	WebLogic Server	
DB2 Universal Database for OS/390 Version 6	DB2	
DNCWARE ClusterPerfect（Linux 版）	ClusterPerfect	
Microsoft(R) Office Excel	Microsoft Excel または Excel	
Microsoft(R) Visual C++(R)	Visual C++または C++言語	
Oracle8i	ORACLE	
Oracle9i		
Oracle 10g		
Sun Java™ System Directory Server	Sun Java System Directory Server またはディレクトリサーバ	
HP-UX 11i V2 (IPF)	HP-UX または HP-UX (IPF)	
HP-UX 11i V3 (IPF)		
AIX 5L V5.1	AIX 5L	AIX
AIX 5L V5.2		
AIX 5L V5.3		
AIX V6.1	AIX V6.1	
AIX V7.1	AIX V7.1	
Linux(R)	Linux	
Red Hat Linux	Red Hat Linux	Linux
Red Hat Enterprise Linux	Red Hat Enterprise Linux	
Red Hat Enterprise Linux AS 3 (IPF)	Linux (IPF)	
Red Hat Enterprise Linux AS 4 (IPF)		
Red Hat Enterprise Linux 5.1 Advanced Platform (Intel Itanium)		
Red Hat Enterprise Linux 5.1 (Intel Itanium)		
Red Hat Enterprise Linux 5.2 Advanced Platform (Intel Itanium)		
Red Hat Enterprise Linux 5.2 (Intel Itanium)		
Red Hat Enterprise Linux AS 3(AMD64 & Intel EM64T)	Linux (EM64T)	

製品名称または名称	表記	
Red Hat Enterprise Linux AS 4(AMD64 & Intel EM64T)		
Red Hat Enterprise Linux ES 4(AMD64 & Intel EM64T)		
Red Hat Enterprise Linux 5.1 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux 5.1 (AMD/Intel 64)		
Red Hat Enterprise Linux 5.2 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux 5.2 (AMD/Intel 64)		
Red Hat Enterprise Linux AS 4(AMD64 & Intel EM64T)	Linux AS 4	
Red Hat Enterprise Linux AS 4(x86)		
Red Hat Enterprise Linux ES 4(AMD64 & Intel EM64T)	Linux ES 4	
Red Hat Enterprise Linux ES 4(x86)		
Red Hat Enterprise Linux 5.1 Advanced Platform (x86)	Linux 5.1	Linux 5
Red Hat Enterprise Linux 5.1 (x86)		
Red Hat Enterprise Linux 5.1 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux 5.1 (AMD/Intel 64)		
Red Hat Enterprise Linux 5.1 Advanced Platform (Intel Itanium)		
Red Hat Enterprise Linux ES 4(x86)		
Red Hat Enterprise Linux 5.2 Advanced Platform (x86)	Linux 5.2	
Red Hat Enterprise Linux 5.2 (x86)		
Red Hat Enterprise Linux 5.2 Advanced Platform (AMD/Intel 64)		
Red Hat Enterprise Linux 5.2 (AMD/Intel 64)		
Red Hat Enterprise Linux 5.2 Advanced Platform (Intel Itanium)		
Red Hat Enterprise Linux 5.2 (Intel Itanium)		
turbolinux 7 Server for AP8000	Linux for AP8000	
Microsoft(R) Windows NT(R) Workstation Operating System Version 4.0	Windows NT	
Microsoft(R) Windows NT(R) Server Network Operating System Version 4.0		
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	

製品名称または名称	表記	
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	
Microsoft(R) Windows Server(R) 2003 R2, Enterprise x64 Edition		
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	
Microsoft(R) Windows Server(R) 2003, Enterprise x64 Edition	Windows Server 2003 (IPF)	Windows(IPF)
Microsoft(R) Windows(R) XP Professional x64 Edition	Windows XP x64 Edition	Windows XP

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

製品名称または名称	表記
Microsoft(R) Windows(R) 7 Professional (x64)	Windows 7 Professional (x64)
Microsoft(R) Windows(R) 7 Enterprise (x64)	Windows 7 Enterprise (x64)
Microsoft(R) Windows(R) 7 Ultimate (x64)	Windows 7 Ultimate (x64)
シングルサーバ	SDS
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

- 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。
- TCP/IP が規定する hosts ファイル（UNIX の場合/etc/hosts ファイルも含む）を hosts ファイルと表記します。hosts ファイルとは通常，Windows の場合は%windir%¥system32¥drivers¥etc¥hosts のことです。

■ 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
ACK	Acknowledgement
ADM	Adaptable Data Manager
ADO	ActiveX Data Objects
ADT	Abstract Data Type
AP	Application Program
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
BES	Back End Server
BLOB	Binary Large Object
BMP	Basic Multilingual Plane
BOM	Byte Order Mark
CD-ROM	Compact Disc - Read Only Memory
CGI	Common Gateway Interface
CLOB	Character Large Object

英略語	英字の表記
CMT	Cassette Magnetic Tape
COBOL	Common Business Oriented Language
CORBA	Common ORB Architecture
CPU	Central Processing Unit
CSV	Comma Separated Values
DAO	Data Access Object
DAT	Digital Audio Taperecorder
DB	Database
DBM	Database Module
DBMS	Database Management System
DDL	Data Definition Language
DF for Windows NT	Distributing Facility for Windows NT
DF/UX	Distributing Facility / for UNIX
DIC	Dictionary Server
DLT	Digital Linear Tape
DML	Data Manipulate Language
DNS	Domain Name System
DOM	Document Object Model
DS	Dictionary Server
DTD	Document Type Definition
DTP	Distributed Transaction Processing
DWH	Data Warehouse
EUC	Extended UNIX Code
EX	Exclusive
FAT	File Allocation Table
FD	Floppy Disk
FES	Front End Server
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GUI	Graphical User Interface
HBA	Host Bus Adapter

英略語	英字の表記
HD	Hard Disk
HTML	Hyper Text Markup Language
ID	Identification number
IP	Internet Protocol
IPF	Itanium(R) Processor Family
JAR	Java Archive File
Java VM	Java Virtual Machine
JDBC	Java Database Connectivity
JDK	Java Developer's Kit
JFS	Journaled File System
JFS2	Enhanced Journaled File System
JIS	Japanese Industrial Standard code
JP1	Job Management Partner 1
JRE	Java Runtime Environment
JTA	Java Transaction API
JTS	Java Transaction Service
KEIS	Kanji processing Extended Information System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LIP	Loop Initialization Process
LOB	Large Object
LRU	Least Recently Used
LTO	Linear Tape-Open
LU	Logical Unit
LUN	Logical Unit Number
LVM	Logical Volume Manager
MGR	System Manager
MIB	Management Information Base
MRCF	Multiple RAID Coupling Feature
MSCS	Microsoft Cluster Server
MSFC	Microsoft Failover Cluster

英略語	英字の表記
NAFO	Network Adapter Fail Over
NAPT	Network Address Port Translation
NAT	Network Address Translation
NIC	Network Interface Card
NIS	Network Information Service
NTFS	New Technology File System
ODBC	Open Database Connectivity
OLAP	Online Analytical Processing
OLE	Object Linking and Embedding
OLTP	On-Line Transaction Processing
OOCOBOL	Object Oriented COBOL
ORB	Object Request Broker
OS	Operating System
OSI	Open Systems Interconnection
OTS	Object Transaction Service
PC	Personal Computer
PDM II E2	Practical Data Manager II Extended Version 2
PIC	Plug-in Code
PNM	Public Network Management
POSIX	Portable Operating System Interface for UNIX
PP	Program Product
PR	Protected Retrieve
PU	Protected Update
RAID	Redundant Arrays of Inexpensive Disk
RD	Relational Database
RDB	Relational Database
RDB1	Relational Database Manager 1
RDB1 E2	Relational Database Manager 1 Extended Version 2
RDO	Remote Data Objects
RiSe	Real time SAN replication
RM	Resource Manager

英略語	英字の表記
RMM	Resource Manager Monitor
RPC	Remote Procedure Call
SAX	Simple API for XML
SDS	Single Database Server
SGML	Standard Generalized Markup Language
SJIS	Shift JIS
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SQL	Structured Query Language
SQL/K	Structured Query Language / VOS K
SR	Shared Retrieve
SU	Shared Update
TCP/IP	Transmission Control Protocol / Internet Protocol
TM	Transaction Manager
TMS-4V/SP	Transaction Management System - 4V / System Product
UAP	User Application Program
UOC	User Own Coding
VOS1	Virtual-storage Operating System 1
VOS3	Virtual-storage Operating System 3
VOS K	Virtual-storage Operating System Kindness
WS	Workstation
WWW	World Wide Web
XDM/BASE E2	Extensible Data Manager / Base Extended Version 2
XDM/DF	Extensible Data Manager / Distributing Facility
XDM/DS	Extensible Data Manager / Data Spreader
XDM/RD E2	Extensible Data Manager / Relational Database Extended Version 2
XDM/SD E2	Extensible Data Manager / Structured Database Extended Version 2
XDM/XT	Extensible Data Manager / Data Extract
XFIT	Extended File Transmission program
XML	Extensible Markup Language

■ パス名の表記

- パス名の区切りは「¥」で表記しています。UNIX 版 HiRDB を使用している場合はマニュアル中の「¥」を「/」に置き換えてください。ただし，Windows 版と UNIX 版でパス名が異なる場合は，それぞれのパス名を表記しています。
- HiRDB 運用ディレクトリのパスを%PDDIR%と表記します。ただし，Windows 版と UNIX 版でパス名が異なるため，それぞれを表記する場合，UNIX 版は$PDDIR と表記します。例を次に示します。

  Windows 版：%PDDIR%¥CLIENT¥UTL¥

  UNIX 版：$PDDIR/client/lib/
- Windows のインストールディレクトリのパスを%windir%と表記します。

■ ログの表記

●Windows 版の場合

Windows のイベントビューアで表示されるアプリケーションログをイベントログと表記します。イベントログは，次の方法で参照できます。

〈手順〉

1.［スタート］－［プログラム］－［管理ツール（共通）］－［イベントビューア］を選択します。

2.［ログ］－［アプリケーション］を選択します。

アプリケーションログが表示されます。「ソース」の列が「HiRDBSingleServer」または「HiRDBParallelServer」になっているのが HiRDB が出力したメッセージです。

なお，セットアップ識別子を指定してインストールした場合は，「HiRDBSingleServer」または「HiRDBParallelServer」にセットアップ識別子が付いた名称となります。

●UNIX 版の場合

OS のログを syslogfile と表記します。syslogfile は，/etc/syslog.conf でログ出力先に指定しているファイルです。一般的には，次のファイルが syslogfile となります。

OS	ファイル
HP-UX	/var/adm/syslog/syslog.log
Solaris	/var/adm/messages または/var/log/syslog
AIX	/var/adm/ras/syslog
Linux	/var/log/messages

■ Windows の操作説明で使う表記

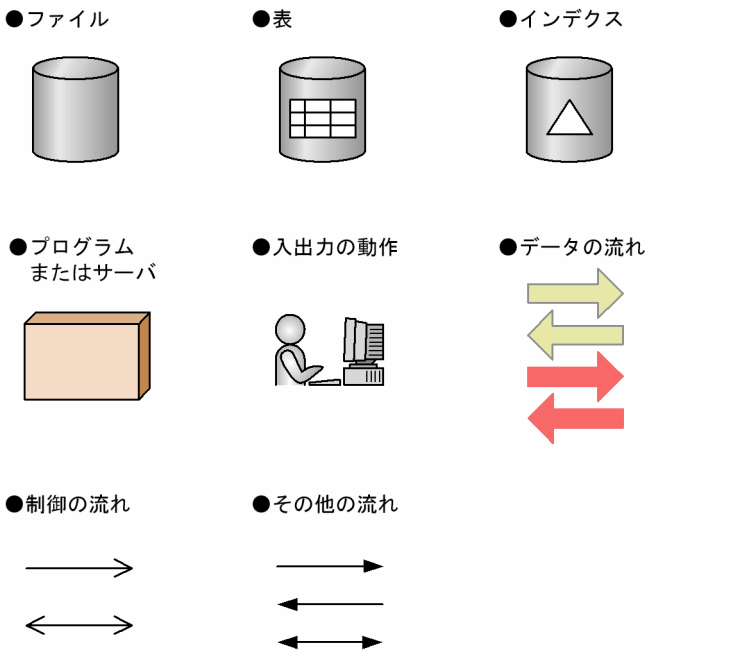
Windows の操作説明で使う記号を次に示します。

記　号	意　味
[　]	ボタンやテキストボックスなど，画面に表示されている要素を示します。
[　] －[　]	画面に表示されるメニューやアイコンなどを選択する操作を示します。

Windows の用語「ディレクトリ」と「フォルダ」は，「ディレクトリ」に統一して表記しています。

■ 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

形式および説明で使用する記号を次に示します。ここで説明する文法記述記号は，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	例
{ }	この記号で囲まれた複数の項目のうちから一つを選択することを示します。	{：埋込み変数｜？パラメタ} 埋込み変数，または？パラメタのどちらかを選択して記述します。
〔 〕	この記号で囲まれた項目は省略できることを意味します。 複数の項目が並べて記述されている場合は，すべてを省略するか，記号 { } と同じくどれか一つを選択します。	〔{ALL ｜ DISTINCT}〕 すべてを省略するか，ALL，または DISTINCT のどちらかを選択して指定します。すべてを省略した場合は，ALL を指定したときと同じ処置をします。
_(下線)	記号〔 〕で囲まれた複数項目のうち 1 項目に対して使用し，括弧内のすべての項目を省略したときシステムがとる標準値を示します。	
…	この記号の直前に示された項目を繰り返し複数個指定できることを示します。	(列名〔，列名〕…) 列名を繰り返し複数個指定できます。そのとき，列名の前と後ろを記号（ ）で囲みます。
（ ）	記号（ ）で囲まれた項目は，（ ）を省略しないでそのまま記述することを示します。	
::=	::=の左にあるものを右にあるもので定義することを示します。	表名::=〔認可識別子.〕表識別子

■ このマニュアルで使用する計算式の記号

このマニュアルで使用する計算式の記号の意味を次に示します。

記号	内容
↑　↑	計算結果の値の小数点以下を切り上げることを意味します。 （例）↑34÷3↑の計算結果は 12 となります。
↓　↓	計算結果の値の小数点以下を切り捨てることを意味します。 （例）↓34÷3↓の計算結果は 11 となります。

■ Windows のパス名に関する注意

- パス名を絶対パスで指定する場合はドライブ名を指定してください。

（例）C:¥win32app¥hitachi¥hirdb_s¥spool¥tmp

- コマンドの引数，制御文ファイル，および HiRDB システム定義ファイル中に空白または丸括弧を含むパス名を指定する場合は，前後を引用符（"）で囲んでください。

（例）pdinit -d "C:¥Program Files(x86)¥hitachi¥hirdb_s¥conf¥mkinit"

ただし，バッチファイルもしくはコマンドプロンプト上で set コマンドを使用して環境変数を設定する場合，またはインストールディレクトリを指定する場合は引用符は不要です。引用符で囲むと，引用符も環境変数の値に含まれます。

（例）set PDCLTPATH=C:¥Program Files¥hitachi¥hirdb_s¥spool

- HiRDB はネットワークドライブのファイルを使用できないため，HiRDB のインストール，および環境構築はローカルドライブで行ってください。また，ユティリティの入出力ファイルなども，ローカルドライブ上のファイルを使用してください。
- パス名には，ショートパス名（例えば，C:¥PROGRA~1 など）は使用しないでください。

■ KB（キロバイト）などの単位表記について

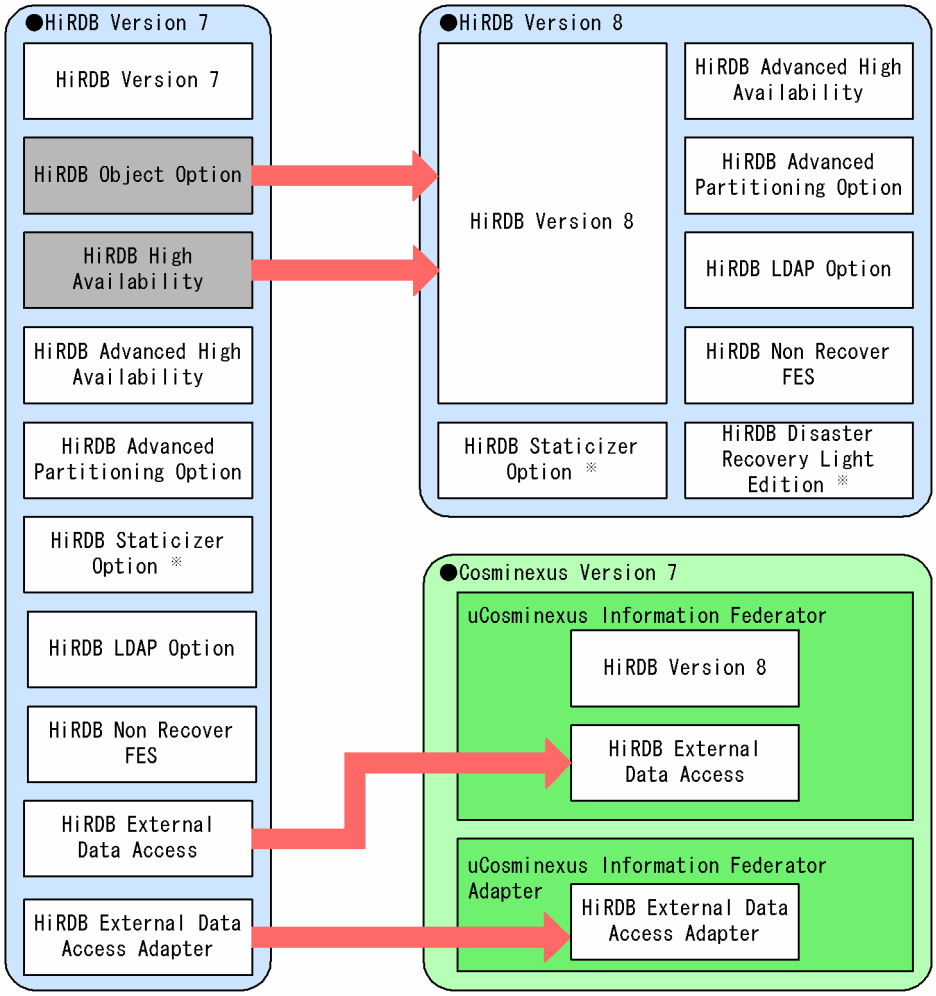
1KB（キロバイト），1MB（メガバイト），1GB（ギガバイト），1TB（テラバイト）はそれぞれ 1,024 バイト，$1{,}024^2$ バイト，$1{,}024^3$ バイト，$1{,}024^4$ バイトです。

■ Version 7 と Version 8 の製品体系の違い

HiRDB Version 8 では，HiRDB Version 7 までオプション製品（HiRDB Object Option および HiRDB High Availability）で提供していた機能を HiRDB の標準機能としました。それに伴い，オプション製品が廃止になりました。

また，Version 8 以降，HiRDB External Data Access および HiRDB External Data Access Adapter は HiRDB シリーズではなく，Cosminexus Version 7 シリーズとなりました。

HiRDB Version 7 と Version 8 の製品体系の違いを次に示します。



注※　UNIX版でだけ使用できる製品です。

目次

1 概要

この章では，データベース暗号化機能の概要について説明します。

1.1　データベース暗号化機能とは

データベース暗号化機能を使用すると，不正な利用者が HiRDB のデータを直接参照したときでも，機密情報を守ることができます。データベースのセキュリティを強化する場合に有効となる機能です。

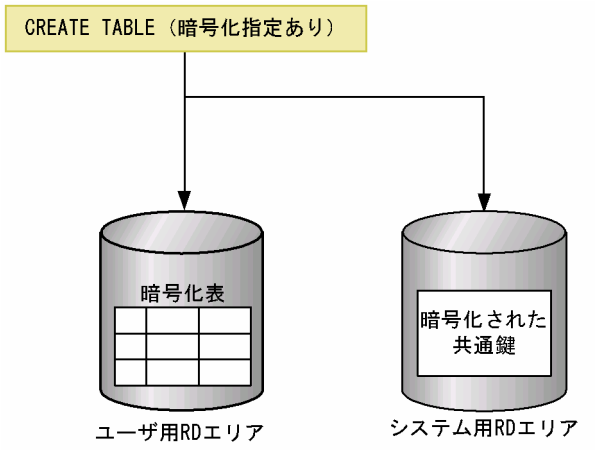
データベース暗号化機能を使用する場合は，表定義時に列に対して暗号化の指定をします。暗号化の指定をすることで，データベースへのデータ格納時に，その列のデータは暗号化されて格納されます。暗号化する列を**暗号化列**，暗号化列がある表を**暗号化表**といいます。なお，暗号化を指定しない列は，その表に暗号化列を含んでいても，暗号化しない状態でデータベースに格納されます。

以降，このマニュアルでは，データベース暗号化機能を**暗号化機能**と表記します。

1.1.1　暗号化表の定義の概要

暗号化表の定義の概要を次の図に示します。

図 1-1　暗号化表の定義の概要



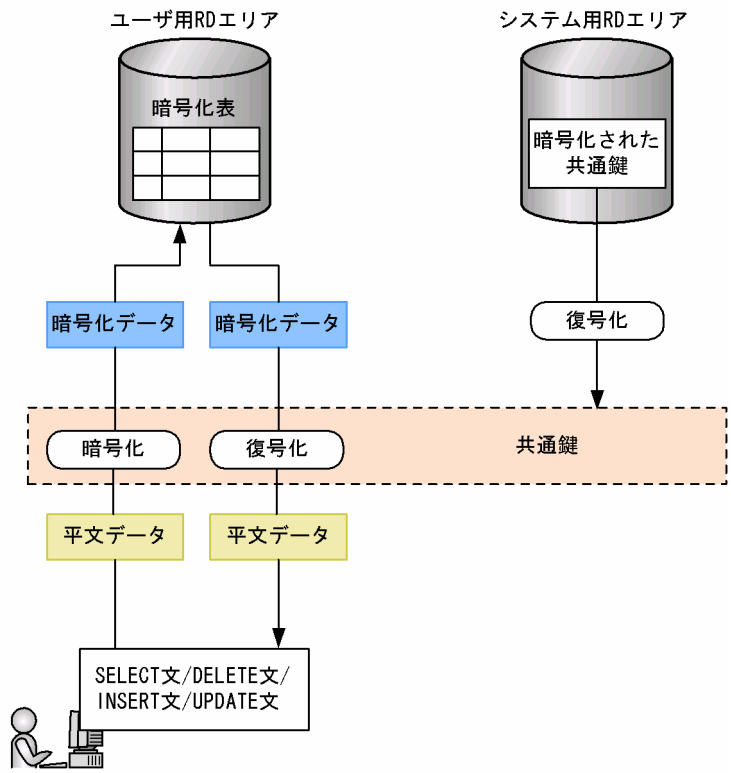
[説明]

暗号化指定ありの CREATE TABLE を実行することで，暗号化表を定義できます。このとき，暗号化および復号化で使用する共通鍵も作成され，暗号化した状態でシステム用 RD エリアに格納されます。

1.1.2　暗号化表の操作の概要

暗号化表の操作の概要を次の図に示します。

図 1-2　暗号化表の操作の概要



[説明]

暗号化列に対して SQL を実行する場合，共通鍵を使用して送信時の平文データを暗号化し，暗号化列に暗号化データを格納します。また，暗号化列のデータを取得する場合は，共通鍵を使用して暗号化データを復号化し，平文データで受け取ることができます。

1.1.3　暗号化列の暗号化の方式

HiRDB は，暗号化アルゴリズムとして AES（Advanced Encryption Standard）を使用します。AES は電子政府推奨の暗号化アルゴリズムで，それまで使われてきた DES よりも暗号化の強度を上げ，さらに暗号化および復号化の高速化を実現しています。

AES で暗号化する情報は，一定のブロック長（128bit）でなければなりません。HiRDB では，128bit のブロック長のデータを，鍵長 192bit の共通鍵で暗号化します。このブロック長に満たないデータ，またはこのブロック長を超えるデータを，一定のブロック長に合わせるアルゴリズムが必要になります。一定のブロック長に合わせるアルゴリズム（これをパディングといいます）として，PKCS #5 v1.5(RFC1424)を使用します。

暗号化する情報は，ブロック長 128bit にパディングされたあと，AES で暗号化して表に格納されます。そのため，第三者が表の物理ファイルである HiRDB ファイルを直接参照したとしても，暗号化した列の解読は難しくなります。

1.2　前提条件

暗号化機能を使用する場合の前提条件について説明します。

(1)　前提プラットフォーム

前提プラットフォームは次のどれかになります。

- HP-UX(IPF)
- AIX
- Windows 2000
- Windows XP
- Windows Server
- Windows Vista Business，Windows Vista Enterprise，または Windows Vista Ultimate
- Linux(EM64T)

(2)　対象となる資源

暗号化の対象となる資源を次に示します。

- システム用 RD エリア※1
- ユーザ用 RD エリア
- システムログファイル
- アンロードログファイル
- pdcopy でのバックアップファイル
- pdrorg でのアンロードデータファイル※2
- pdrorg でのインデクス情報ファイル

注※1

共通鍵だけ暗号化されます。

注※2

-k オプションに rorg を指定した場合だけ，表のデータを暗号化してアンロードデータファイルを作成します。ただし，-g オプションを指定している，または UOC を利用している場合は，暗号化されません。

1.3　インストール

HiRDB Plus をインストールする場合，HiRDB および HiRDB Data Convert Type1 Option をインストールします。インストールおよびアンインストールについては，マニュアル「HiRDB Version 8 システム導入・設計ガイド」を参照してください。

! 注意事項

- HiRDB Plus がインストールされているサーバマシンに，HiRDB を上書きインストールしないでください。
- HiRDB/パラレルサーバの場合，すべてのユニットに HiRDB Plus をインストールしてください。HiRDB Plus と HiRDB との混在はできません。
- UNIX 版 HiRDB Plus の場合，HiRDB Plus をアンインストールするときは，先に HiRDB Data Convert Type1 Option をアンインストールしてから，HiRDB をアンインストールしてください。
- pdadmvr コマンドで，サーバマシンにインストールされている HiRDB の種類（HiRDB Plus または HiRDB）を確認できます。
- UNIX 版 HiRDB Plus をインストールする場合は，HiRDB 本体と HiRDB Data Convert Type1 Option を両方一緒にインストールしてください。

  また，HiRDB 本体と HiRDB Data Convert Type1 Option を別々にインストールする場合は，HiRDB 本体をインストールしたあとに HiRDB Data Convert Type1 Option をインストールしてください。

  HiRDB Data Convert Type1 Option だけのインストールはできません。

2 定義

この章では，データベースを暗号化するときの暗号化表の定義，および暗号化表のインデクスの定義について説明します。

2.1　暗号化表の定義

暗号化表は，CREATE TABLE で定義します。また，ALTER TABLE で暗号化列を追加できます。

2.1.1　CREATE TABLE（表定義）

暗号化表を定義する場合の CREATE TABLE について説明します。

なお，ここでは，CREATE TABLE の暗号化に関係する説明だけ記載しています。そのほかの CREATE TABLE の説明については，マニュアル「HiRDB Version 8 SQL リファレンス」を参照してください。

(1)　形式

```
表要素：：＝｛列定義｜表制約定義｝

  列定義：：＝列名 データ型〔ARRAY ［最大要素数］〕
             〔NO SPLIT〕
             〔｛列データ抑制指定｜〔列回復制約〕
                 {IN ｛LOB列格納用RDエリア名
                       ｜（LOB列格納用RDエリア名）
                       ｜（（LOB列格納用RDエリア名）
                           〔，（LOB列格納用RDエリア名）｝…）
                       ｜マトリクス分割LOB列格納用RDエリア指定｝
                   ｜抽象データ型定義内LOB格納用RDエリア指定｝｝〕
             〔プラグイン指定〕
             〔DEFAULT句〕
             〔列制約…〕
             〔更新可能列属性〕
             〔暗号化指定〕

    列データ抑制指定：：＝〔SUPPRESS〕

    暗号化指定：：＝INNER CONSTRUCTOR 〔OF TYPE1〕
```

(2)　オペランド

列データ抑制指定：：＝〔SUPPRESS〕

暗号化表の場合，SUPPRESS を指定しても無効となります（エラーにはなりません）。

暗号化指定：：＝ INNER CONSTRUCTOR 〔OF TYPE1〕

HiRDB が組み込んでいる暗号ライブラリを使用して，列を暗号化する場合に指定します。

このオペランドを指定すると，データの暗号化，および復号化に使用する共通鍵が生成されます。

なお，OF TYPE1 は指定してもしなくても意味は変わりません。

暗号化指定の規則を次に示します。

1. 繰返し列には指定できません。
2. 次のデータ型には指定できません。
   - BINARY 型
   - BLOB 型
   - 抽象データ型
3. 次の分割キー構成列には指定できません。
   - 格納条件指定
   - 境界値指定
   - マトリクス分割（ハッシュ関数の対象となる列を除きます）
4. クラスタキー構成列には指定できません。

5. 暗号化列の既定義型のデータ長については，「5.1.1　表の格納ページ数の計算方法」を参照してください。

(3)　使用例

暗号化表を定義する場合の CREATE TABLE の例を次に示します。

暗号化表として，在庫表（ZAIKO）を定義します。このとき，単価（TANKA）列を暗号化します。

```
CREATE TABLE ZAIKO
        (SCODE CHAR(4),
         SNAME NCHAR(8),
         COL NCHAR(1),
         TANKA INTEGER INNER CONSTRUCTOR OF TYPE1,
         ZSURYO INTEGER)
```

2.1.2　ALTER TABLE（表定義変更）

暗号化列を追加する場合の ALTER TABLE について説明します。

なお，ここでは，ALTER TABLE の暗号化に関係する説明だけ記載しています。そのほかの ALTER TABLE の説明については，マニュアル「HiRDB Version 8 SQL リファレンス」を参照してください。

(1)　形式

```
列追加定義：：＝
    ADD 列名 データ型〔ARRAY ［最大要素数］〕 〔NO SPLIT〕
        〔〔列回復制約1〕
          {LOB列格納用RDエリア指定
            ｜マトリクス分割LOB列格納用RDエリア指定
            ｜抽象データ型定義内LOB格納用RDエリア指定
              〔プラグイン指定〕
            ｜マトリクス分割LOB属性格納用RDエリア指定
              〔プラグイン指定〕}〕
        〔DEFAULT句〕
        {〔NULL｜NOT NULL〔WITH DEFAULT〕〕
          ｜｛〔NOT NULL〕 WITH DEFAULT〕}
        〔更新可能列属性〕
        〔暗号化指定〕
        〔WITH PROGRAM〕

  暗号化指定：：＝ INNER CONSTRUCTOR 〔OF TYPE1〕
```

(2)　オペランド

暗号化指定：：＝ INNER CONSTRUCTOR 〔OF TYPE1〕

指定した暗号化ライブラリを使用して列データを暗号化します。

このオペランドを指定すると，データの暗号化，および復号化に使用する共通鍵が生成されます。

なお，OF TYPE1 は指定してもしなくても意味は変わりません。

暗号化指定についての規則を次に示します。

1. 繰返し列には指定できません。
2. 次のデータ型には指定できません。
   - BINARY 型
   - BLOB 型
   - 抽象データ型

2.2　暗号化表のインデクスの定義

暗号化表のインデクスは，CREATE INDEX 形式 1 で定義します。

2.2.1　CREATE INDEX 形式 1（インデクス定義）

暗号化表のインデクスを定義する場合の，CREATE INDEX 形式 1 について説明します。

なお，ここでは，CREATE INDEX 形式 1 の暗号化に関係する説明だけ記載しています。そのほかの CREATE INDEX 形式 1 の説明については，マニュアル「HiRDB Version 8 SQL リファレンス」を参照してください。

(1)　規則

1. 複数列インデクスを定義する場合，暗号化列と繰返し列は混在できません。
2. 暗号化列のインデクスのキー長については，「5.1.2　インデクスの格納ページ数の計算方法」を参照してください。

3 運用

この章では，暗号化したデータベースの運用方法について説明します。

3.1　再編成

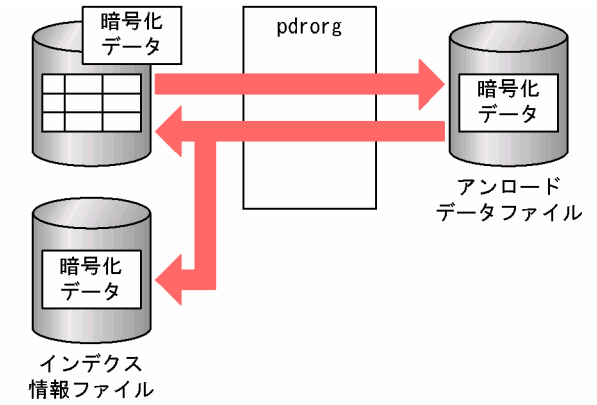
暗号化表に対して pdrorg を実行する場合の運用方法について説明します。

pdrorg での再編成については，マニュアル「HiRDB Version 8 システム運用ガイド」，およびマニュアル「HiRDB Version 8 コマンドリファレンス」を参照してください。

3.1.1　暗号化表の再編成

暗号化表の再編成では，暗号化されているデータをいったんファイルに退避し，そのファイルのデータを再度表に格納します。表中のデータの復号化および暗号化は行われません。暗号化表の再編成の概要を次の図に示します。

図 3-1　暗号化表の再編成の概要



(1)　アンロードデータファイルに出力するデータの形式

暗号化表の再編成の場合，暗号化データがアンロードデータファイルに出力されます。ただし，次のどちらかの条件を満たす場合は，平文データが出力されます。

- UOC を使用する場合
- -g オプションを指定する場合※

注※

HiRDB/パラレルサーバでのスキーマ単位の再編成の場合，-g オプションが仮定されます。

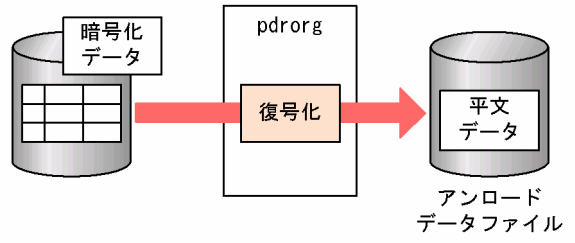
(2)　制限がある機能

暗号化表を再編成する場合，option 文の spacelvl オペランドを指定して空白変換をすることができません。空白変換をする必要がある場合は，アンロードとリロードを分けて実行し，リロード時に option 文の spacelvl オペランドを指定してください。

3.1.2　暗号化表のアンロード

暗号化表のアンロードでは，表中のデータが復号化され，平文データがアンロードデータファイルに出力されます。暗号化表のアンロードの概要を次の図に示します。

図 3-2　暗号化表のアンロードの概要



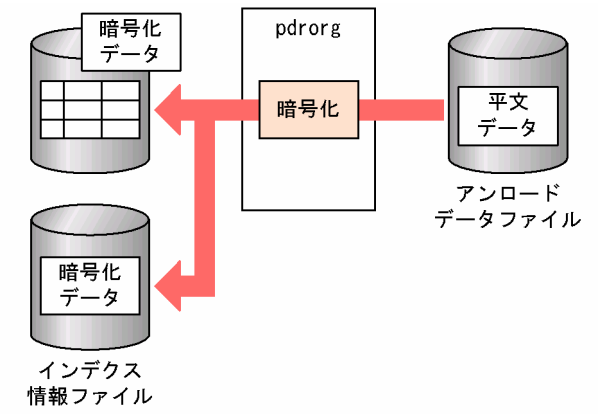
! 注意事項

暗号化表をアンロードする場合，-b オプションに指定したインデクスのインデクス構成列に暗号化列を含んでいると，暗号化した状態のデータのキー順となります。

3.1.3　暗号化表のリロード

暗号化表のリロードでは，アンロードデータファイルの平文データが暗号化され，表には暗号化データが格納されます。暗号化表のリロードの概要を次の図に示します。

図 3-3　暗号化表のリロードの概要



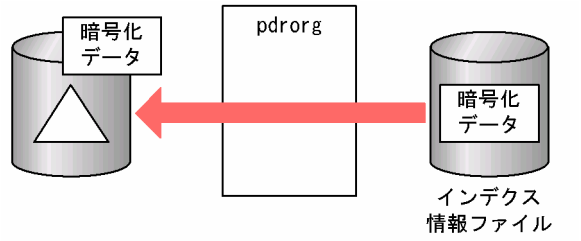
! 注意事項

再編成（-k rorg）で作成したアンロードデータファイルを使用して，別表へデータを移行する（リロードする）ことはできません。暗号化表のデータを別表に移行する場合は，アンロード（-k unld）で作成したアンロードデータファイルを使用して，リロードしてください。

3.1.4　インデクス構成列に暗号化列を含むインデクスの一括作成

インデクス構成列に暗号化列を含むインデクスを一括作成する場合，インデクスに格納するキーデータは暗号化したままソートされ，ソートしたキーデータでインデクスを作成します。インデクス構成列に暗号化列を含むインデクスの一括作成の概要を次の図に示します。

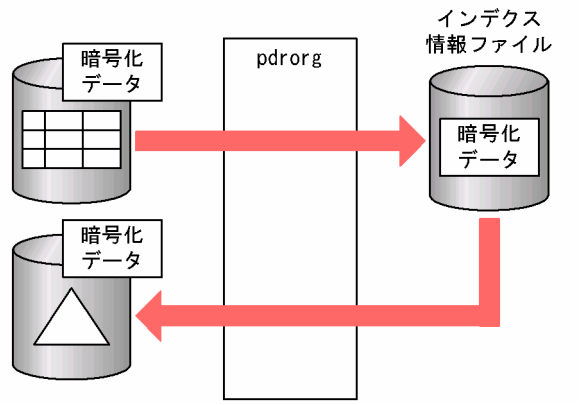
図 3-4　インデクス構成列に暗号化列を含むインデクスの一括作成の概要



3.1.5　インデクス構成列に暗号化列を含むインデクスの再作成

インデクス構成列に暗号化列を含むインデクスを再作成する場合，暗号化されたインデクスのインデクス構成列（キーデータ）が，暗号化した状態でインデクス情報ファイルに出力されます。出力されたキーデータは，暗号化した状態でソートされ，ソートされたキーデータでインデクスを再作成します。インデクス構成列に暗号化列を含むインデクスの再作成の概要を次の図に示します。

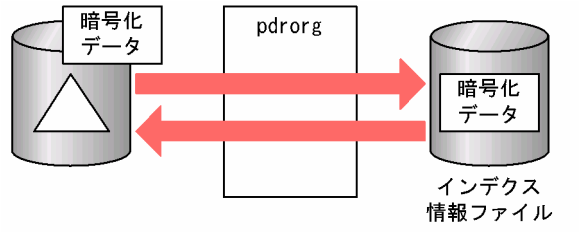
図 3-5　インデクス構成列に暗号化列を含むインデクスの再作成の概要



3.1.6　インデクス構成列に暗号化列を含むインデクスの再編成

インデクス構成列に暗号化列を含むインデクスを再編成する場合，暗号化されたインデクスのインデクス構成列（キーデータ）が，暗号化した状態でインデクス情報ファイルに出力され，出力されたキーデータでインデクスを再作成します。インデクス構成列に暗号化列を含むインデクスの再編成の概要を次の図に示します。

図 3-6　インデクス構成列に暗号化列を含むインデクスの再編成の概要



3.2　バックアップと回復

暗号化表を含むデータベースの，pdcopy でのバックアップと pdrstr での回復の注意事項について説明します。

pdcopy でのバックアップと pdrstr での回復については，マニュアル「HiRDB Version 8 システム運用ガイド」，およびマニュアル「HiRDB Version 8 コマンドリファレンス」を参照してください。

3.2.1　データベースのバックアップ

暗号化表定義時に作成される共通鍵がシステム用 RD エリアにない場合，その暗号化表のデータは復号化できません。このため，pdcopy でバックアップを取得する場合，暗号化表があるユーザ用 RD エリア以外にも，共通鍵を含むシステム用 RD エリアも同時に取得する必要があります。

3.2.2　データベースの回復

システム用 RD エリアに障害が発生して，暗号化表のデータを復号化できなくなった場合，バックアップを入力情報として pdrstr でデータベースを回復してください。

3.3　運用時の注意事項

(1)　暗号化した場合の処理時間

表を暗号化すると，暗号化および復号化の処理があるため，その分処理速度が遅くなります。性能が劣化する可能性があるため，暗号化する列は必要最低限にしてください。また，SQL を作成する場合，暗号化列はなるべく比較述語（=），または IN 述語（IN）で判定するようにしてください。

暗号化しない場合は，インデクスは昇順または降順になることが保証されますが，暗号化する場合は保証されなくなるため，述語によっては，インデクスのサーチ条件によるインデクスのサーチ範囲の絞り込みができなくなり，性能が劣化します。同様の理由によって，ORDER BY 処理方式，およびグループ分け処理方式で，インデクスを使用した高速な処理方式が選択できなくなります。

(a)　インデクスのサーチ範囲の絞り込み適用可否

暗号化列に対するインデクスのサーチ範囲の絞込み適用可否を次の表に示します。サーチ条件については，マニュアル「HiRDB Version 8 コマンドリファレンス」を参照してください。

表 3-1　暗号化列に対するインデクスのサーチ範囲の絞込み適用可否

述語	非暗号化列での適用可否	暗号化列での適用可否
比較述語（=）	○	○
比較述語（=以外）	○※1	×
NULL 述語（IS NULL）	○	○
NULL 述語（IS NOT NULL）	○※2	○※2
IN 述語（IN）	○	○
IN 述語（NOT IN）	×	×
LIKE 述語	○※3	×
XLIKE 述語	×	×
BETWEEN 述語	○※4	×
EXISTS 述語	－	－
構造化繰返し述語	○	－
限定述語	○※5	○※5
論理述語	○	－

（凡例）

○：絞込みを適用します。

×：絞込みを適用しません。

－：暗号化列は，データ比較に使用しないか，または指定できません。

注※1

<>，^=，および!=は，絞込みを適用しません。

注※2

列に定義した単一列インデクスを利用しない場合，絞込みを適用しません。

注※3

NOT LIKE の場合は絞込みを適用しません。

注※4

NOT BETWEEN の場合は絞込みを適用しません。

注※5

=ANY，および=SOME の場合だけ，絞込みを適用します。

(b)　選択されない ORDER BY 処理方式

暗号化列を含む ORDER BY 処理で，選択できなくなる処理方式を次に示します。ORDER BY 処理方式の種類については，マニュアル「HiRDB Version 8 コマンドリファレンス」を参照してください。

- SORT CANCEL BY INDEX
- SORT CANCEL BY INDEX(LIMIT SCAN)

(c)　選択されないグループ分け処理方式

暗号化列を含むグループ分け処理で，選択できなくなる処理方式を次に示します。グループ分け処理方式の種類については，マニュアル「HiRDB Version 8 コマンドリファレンス」を参照してください。

- SORT CANCEL BY INDEX
- SORT CANCEL BY INDEX{SET SCAN}
- IMPLICIT SORT CANCEL BY INDEX{SET FUNCTION SCAN}
- IMPLICIT MIN-MAX INDEX

(2)　暗号化表の移行

HiRDB Plus で作成した暗号化表は HiRDB には移行できません。

(3)　DECIMAL 型の暗号化列を検索した場合の符号部の扱い

DECIMAL 型の列を暗号化した場合，システム共通定義の pd_dec_sign_normalize オペランドの指定値に関係なく，正の符号はすべて X'C'に変換します。このため，符号に X'F'を指定してデータを格納した場合でも，検索結果の符号は必ず X'C'になります。

(4)　強制的にコストベース最適化モード 2 を適用する SQL

SQL 中に暗号化列が含まれる場合，強制的にコストベース最適化モード 2 が適用されます。例を次に示します。

例

```
SELECT C1,C2 FROM T3
```

注　下線部分が該当個所です。C2 は暗号化列です。

3.4　制限される機能

暗号化表の場合に制限される機能を次に示します。

- 更新可能なオンライン再編成
- データ連動（HiRDB Datareplicator）
- プラグインからの操作
- 表定義の変更（ALTER TABLE）での暗号化列の追加（ADD 列名）※，および暗号化列の RD エリア追加（ADD RDAREA）
- 表のリバランス（pdrbal）

注※

暗号化列が次のどちらかに該当する場合，暗号化列の追加はできません。

- BINARY，BLOB，または抽象データ型の列
- 繰返し列

4 使用例

この章では，暗号化表の定義，データの格納，および検索の例について説明します。

4.1　表定義

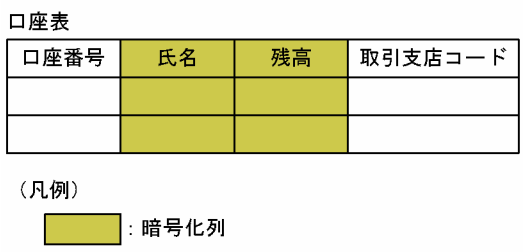
暗号化表は CREATE TABLE で定義します。

CREATE TABLE の例：

```
CREATE TABLE 口座(口座番号 CHAR(10),
                  氏名 NVARCHAR(20) INNER CONSTRUCTOR OF TYPE1,
                  残高 INT INNER CONSTRUCTOR OF TYPE1,
                  取引支店コード CHAR(10));
```

上記の CREATE TABLE を実行すると，次の図のような暗号化表が定義されます。

図 4-1　定義される暗号化表



4.2　データの格納

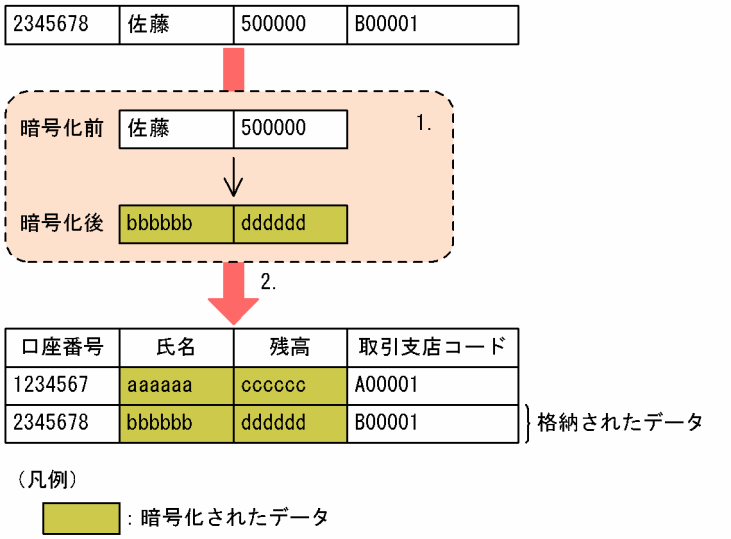
暗号化表へのデータの格納は，INSERT 文で行います。データの格納は pdload でも実行できますが，ここでは INSERT 文について説明します。

INSERT 文の例：

```
INSERT INTO 口座 VALUES ('2345678',N'佐藤',500000,'B00001');
```

上記の INSERT 文を実行すると，次の図のように暗号化表にデータが格納されます。

図 4-2　暗号化表へのデータの格納



[説明]

1. 口座表へ格納するデータのうち，暗号化列へ格納するデータだけ暗号化を行います。
2. 1.で暗号化したデータ，およびそのほかのデータを口座表に格納します。口座表の暗号化列は暗号化データ，暗号化列以外の列は平文データとなります。

4.3　データの検索

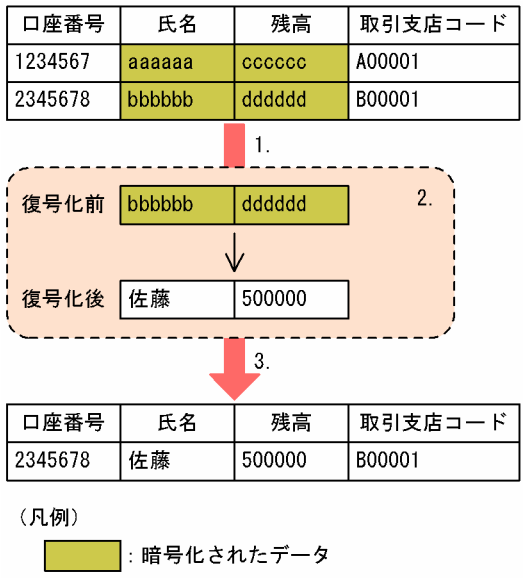
暗号化表のデータの検索は，SELECT 文で行います。

SELECT 文の例：

```
SELECT * FROM 口座 WHERE 氏名 = N'佐藤';
```

上記の SELECT 文を実行すると，次の図のように暗号化表のデータを検索します。

図 4-3　暗号化表のデータの検索



[説明]

1. 探索条件中の暗号化列と比較する条件を暗号化し，暗号化列のデータと一致する行を口座表から取得します。
2. 1.で取得した行のうち，暗号化列のデータを復号化します。
3. 検索結果はすべて平文データとなります。

5 RD エリアの容量見積もり

この章では，暗号化機能を使用する場合に変更となる RD エリアの容量見積もりについて説明します。

5.1　ユーザ用 RD エリア

暗号化機能を使用する場合，ユーザ用 RD エリアの容量見積もりの「表の格納ページ数の計算方法」および「インデクスの格納ページ数の計算方法」が変更となります。ユーザ用 RD エリアの容量の見積もりについては，マニュアル「HiRDB Version 8 システム導入・設計ガイド」を参照してください。

5.1.1　表の格納ページ数の計算方法

暗号化機能を使用すると，データ長の部分が変更になります。暗号化列のデータ長一覧を次の表に示します。また，列のデータ長の平均値を求める場合は，表 5-2 にあるデータ型の列についてだけ求めてください。

表 5-1　暗号化列のデータ長一覧

分類	データ型および条件				データ長（単位：バイト）
数値データ	INTEGER				16
	SMALLINT				16
	LARGE DECIMAL(m,n)				↑(↑(m + 1)÷2↑+1)÷16↑×16
	FLOAT または DOUBLE PRECISION				16
	SMALLFLT または REAL				16
文字データ	CHARACTER(n)				↑(n + 1)÷16↑×16
	VARCHAR(n)	d≦255	繰返し列の要素		−
			上記以外		↑(d + 1)÷16↑×16 + 3
		d≧256			6
	VARCHAR(n) ノースプリットオプション指定あり	n≦255	抽象データ型の属性		−
			繰返し列の要素		−
			上記以外		↑(d + 1)÷16↑×16 + 3
		n≧256	分岐する場合		6
			分岐しない場合	抽象データ型の属性	−
				繰返し列の要素	−
				上記以外	↑(d + 1)÷16↑×16 + 3
各国文字データ	NCHAR(n)または NATIONAL CHARACTER(n)				↑(2n + 1)÷16↑×16
	NVARCHAR(n)	d≦127	繰返し列の要素		−
			上記以外		↑(2d + 1)÷16↑×16 + 3
		d≧128			6
	NVARCHAR(n)	n≦127	抽象データ型の属性		−

分類	データ型および条件				データ長（単位：バイト）
	ノースプリットオプション指定あり		繰返し列の要素		－
			上記以外		↑(2d + 1)÷16↑×16 + 3
		n≧128	分岐する場合		6
			分岐しない場合	抽象データ型の属性	－
				繰返し列の要素	－
				上記以外	↑(2d + 1)÷16↑×16 + 3
混在文字データ	MCHAR(n)				↑(n + 1)÷16↑×16
	MVARCHAR(n)	d≦255	繰返し列の要素		－
			上記以外		↑(d + 1)÷16↑×16 + 3
		d≧256			6
	MVARCHAR(n) ノースプリットオプション指定あり	n≦255	抽象データ型の属性		－
			繰返し列の要素		－
			上記以外		↑(d + 1)÷16↑×16 + 3
		n≧256	分岐する場合		6
			分岐しない場合	抽象データ型の属性	－
				繰返し列の要素	－
				上記以外	↑(d + 1)÷16↑×16 + 3
日付データ	DATE				16
時刻データ	TIME				16
日間隔データ	INTERVAL YEAR TO DAY				16
時間隔データ	INTERVAL HOUR TO SECOND				16
時刻印データ	TIMESTAMP(n)				16
長大データ	BLOB				－
バイナリデータ	BINARY(n)				－

（凡例）

m，n：正の整数

d：実際のデータ長（文字数）

－：暗号化列に指定できません。

表 5-2　可変長文字列型のデータ長一覧

データ型		データ長
VARCHAR(n)	d≧256	↑(d+1)÷16↑×16+2
	ノースプリットオプション指定あり	0
NVARCHAR(n)	d≧128	↑(2d+1)÷16↑×16+2
	ノースプリットオプション指定あり	0
MVARCHAR(n)	d≧256	↑(d+1)÷16↑×16+2
	ノースプリットオプション指定あり	0

（凡例）

n：正の整数

d：実際のデータ長（文字数）

5.1.2　インデクスの格納ページ数の計算方法

暗号化機能を使用すると, インデクスのキー長の部分が変更になります。暗号化列のインデクスのキー長一覧を次の表に示します。

表 5-3　暗号化列のインデクスのキー長一覧

データ型	キー長（単位：バイト）					
	各列のキー長の合計が 255 バイト以下である場合			各列のキー長の合計が 256 バイト以上である場合		
	単一列インデクスを構成する列	複数列インデクスを構成する列		単一列インデクスを構成する列	複数列インデクスを構成する列	
		構成列が固定長だけの場合	構成列に可変長を含む場合		構成列が固定長だけの場合	構成列に可変長を含む場合
INTEGER	16	17	18	−	17	19
SMALLINT	16	17	18	−	17	19
LARGE DECIMAL(m,n)	↑(↑(m+1)÷2↑+1)÷16↑×16	↑(↑(m+1)÷2↑+1)÷16↑×16+1	↑(↑(m+1)÷2↑+1)÷16↑×16+2	−	↑(↑(m+1)÷2↑+1)÷16↑×16+1	↑(↑(m+1)÷2↑+1)÷16↑×16+3
FLOAT	16	−	−	−	−	−
SMALLFLT	16	−	−	−	−	−
CHAR(n)	↑(n+1)÷16↑×16	↑(n+1)÷16↑×16+1	↑(n+1)÷16↑×16+2	↑(n+1)÷16↑×16	↑(n+1)÷16↑×16+1	↑(n+1)÷16↑×16+3
VARCHAR(n)	↑(a+1)÷16↑×16+1	−	↑(a+1)÷16↑×16+2	↑(a+1)÷16↑×16+2	−	↑(a+1)÷16↑×16+3
NCHAR(n)	↑(2×n+1)÷16↑×16	↑(2×n+1)÷16↑×16+1	↑(2×n+1)÷16↑×16+2	↑(2×n+1)÷16↑×16	↑(2×n+1)÷16↑×16+1	↑(2×n+1)÷16↑×16+3

データ型	キー長（単位：バイト）					
	各列のキー長の合計が 255 バイト以下である場合			各列のキー長の合計が 256 バイト以上である場合		
	単一列インデクスを構成する列	複数列インデクスを構成する列		単一列インデクスを構成する列	複数列インデクスを構成する列	
		構成列が固定長だけの場合	構成列に可変長を含む場合		構成列が固定長だけの場合	構成列に可変長を含む場合
NVARCHAR(n)	↑(2×b+1)÷16↑×16+1	－	↑(2×b+1)÷16↑×16+2	↑(2×b+1)÷16↑×16+2	－	↑(2×b+1)÷16↑×16+3
MCHAR(n)	↑(n+1)÷16↑×16	↑(n+1)÷16↑×16+1	↑(n+1)÷16↑×16+2	↑(n+1)÷16↑×16	↑(n+1)÷16↑×16+1	↑(n+1)÷16↑×16+3
MVARCHAR(n)	↑(a+1)÷16↑×16+1	－	↑(a+1)÷16↑×16+2	↑(a+1)÷16↑×16+2	－	↑(a+1)÷16↑×16+3
DATE	16	17	18	－	17	19
TIME	16	17	18	－	17	19
TIMESTAMP	16	17	18	－	17	19
INTERVAL YEAR TO DAY	16	17	18	－	17	19
INTERVAL HOUR TO SECOND	16	17	18	－	17	19

（凡例）

m，n：正の整数

a：実際のデータ長

b：実際の文字数

－：該当しません。

6 メッセージ

この章では，暗号化機能を使用する場合に出力されるメッセージ，アボートコード，および SQLSTATE について説明します。

6.1 メッセージの詳細

暗号化機能を使用する場合に出力されるメッセージについて説明します。

メッセージの記述形式，およびこのマニュアルに記載されていない HiRDB のメッセージについては，マニュアル「HiRDB Version 8 メッセージ」を参照してください。

KFPA19334-E

HiRDB Server type inconsistency occurred, server=aa....aa （A）

HiRDB のサーバ種別に不整合が発生しました。次の原因が考えられます。

- HiRDB Plus でないサーバが混在している状態で HiRDB Plus の機能を使用している。

aa....aa：HiRDB Plus でないサーバ名

(S)この SQL 文を無視します。

[対策]HiRDB Plus の機能を使用する場合は，すべてのユニットで HiRDB Plus のセットアップを行ってください。

KFPA19516-E

Error occurred in encryption library function call, reason=aa....aa, inf=bb....bb （A）

暗号ライブラリ関数の呼び出し処理でエラーが発生しました。

aa....aa：エラー理由

INSUFFICIENT MEMORY：

暗号化機能の処理中にメモリ不足が発生しました。

bb....bb：

確保しようとした領域の大きさ（単位：バイト）です。領域の大きさが特定できない場合，********となります。

(S)この SQL 文を無視します。ただし，ユティリティを実行している場合は処理を終了します。

(P)再度実行してください。再度このエラーが発生する場合は，HiRDB 管理者に連絡してください。

[対策]同時実行しているプロセス数を減らして，使用できるメモリに余裕を持たせてください。

KFPA19640-E

Unable to bb....bb table due to specification "INNER CONSTRUCTOR" for aa....aa （A）

aa....aa に示す列を暗号化列に指定しているため，表定義，または暗号化列の追加ができません。

aa....aa：

column of BINARY type：BINARY 型の列

column of BLOB type：BLOB 型の列

column of abstract data type：抽象データ型の列

multi-value column：繰返し列

cluster key column：クラスタキー構成列

divided key column：キーレンジ分割の分割キー構成列

bb....bb：

create：表定義

alter：暗号化列の追加

(S)この SQL 文を無視します。

(P)SQL 文を修正し，再度実行してください。

KFPA19641-E

Unable to create index due to including both encrypted column and multi-value column （A）

インデクス構成列に，暗号化列と繰返し列が混在するため，インデクスを定義できません。

(S)この SQL 文を無視します。

(P)SQL 文を修正し，再度実行してください。

KFPA19644-E

Unable to drop column on aa....aa ."bb....bb" due to cc....cc （A）

指定した列が暗号化列であるため，列の削除ができません。

aa....aa：認可識別子

bb....bb：表識別子

(S)この SQL 文を無視します。

(P)列名を見直して，再度実行してください。

KFPD00037-E

Error occurred in encryption library function call, func=aa....aa, errno=bb....bb (cc....cc, dd....dd)
（L）

暗号ライブラリ関数の呼び出し処理でエラーが発生しました。

aa....aa：エラーが発生した暗号ライブラリ関数の名称

bb....bb：暗号ライブラリ関数のリターンコード

cc....cc：保守情報 1

dd....dd：保守情報 2

(S)異常終了します。

[対策]保守員に連絡してください。

KFPL10008-E

Unable to specified option spacelvl in Control file when encrypted table （E＋L）

暗号化表を再編成する場合，option 文の spacelvl オペランドに 1 および 3 は指定できません。

(S)処理を終了します。

(O)次のどちらかの対処をしてください。

- option 文の spacelvl オペランドを指定しないで再実行してください。
- 表の再編成（-k rorg）ではなく，アンロード（-k unld）とリロード（-k reld）に分けて pdrorg を実行してください。このとき，リロード時に option 文の spacelvl オペランドを指定してください。

KFPL15320-E

Unable to reload due to DB data encrypted in unload file , table=aa....aa."bb....bb" （E＋L）

アンロードデータファイル中のデータが暗号化されているため，表 aa....aa."bb....bb"へのリロードができません。

aa....aa：認可識別子

bb....bb：表識別子

(S)処理を終了します。

(O)表の再編成（-k rorg）時にエラーが発生した場合，リロード（-k reld）ではなく，表の再編成（-k rorg）を再度実行してください。また，エラー発生時に出力されたアンロードデータファイルは，暗号化されているためデータの移行ができません。pdrorg でデータを移行する場合は，再度，移行元でアンロード（-k unld）をしてアンロードデータファイルを作成してください。

KFPL25223-E

Error occurred in encryption library function call, reason=aa....aa, inf=bb....bb　（E＋L）

暗号ライブラリ関数の呼び出し処理でエラーが発生しました。

aa....aa：エラー理由

INSUFFICIENT MEMORY：

暗号化機能の処理中に，メモリ不足が発生しました。

bb....bb：確保しようとした領域の大きさ（単位：バイト）です。領域の大きさが特定できない場合，********となります。

(S)処理を終了します。

(O)再度実行してください。再度このエラーが発生する場合は，HiRDB 管理者に連絡してください。

[対策]同時実行しているプロセス数を減らして，使用できるメモリに余裕を持たせてください。

KFPL25224-E

HiRDB Server type inconsistency occurred, server=aa....aa　（E＋L）

HiRDB のサーバ種別に不整合が発生しました。次の原因が考えられます。

- HiRDB Plus でないサーバが混在している状態で HiRDB Plus の機能を使用している。

aa....aa：HiRDB Plus でないサーバ名

HiRDB/パラレルサーバの場合，システムマネジャのユニットで HiRDB Plus をセットアップしていない状態で，次のユティリティを実行したときは「MGR」が出力されます。

- pdload
- pdrorg
- pdrbal
- pdreclaim
- pdpgbfon

(S)処理を終了します。

(O)HiRDB のサーバ種別に不整合がないか，HiRDB 管理者に確認してください。

[対策]HiRDB Plus の機能を使用する場合は，すべてのユニットで HiRDB Plus のセットアップを行ってください。

KFPL25362-E

Unable to rorg rebalancing table, because encrypted column include fix HASH partitioning key columns （E＋L）

FIX ハッシュ分割表の構成列に暗号化列が含まれているため，リバランス表を再編成できません。

(S)処理を終了します。

(O)-g オプションを指定して pdrorg を再実行してください。また，unload 文を複数指定している場合は，一つだけ指定してください。

KFPT02016-E

aa....aa:unable to execute Online DB Reorganization, reason=bb....bb,resource kind=cc....cc,name=dd....dd （E＋L）

更新可能なオンライン再編成を実行できません。

aa....aa：コマンド名（KFPT00001-E の埋め込み文字中のコマンド名を参照してください）

bb....bb：理由

"encrypted table"：暗号化列を含む表が定義されています。

cc....cc：資源種別

table：表

dd....dd：適用条件を満足していない資源名称

資源種別が table の場合："認可識別子"."表識別子"

(S)処理を続行します。

(O)HiRDB 管理者に連絡してください。

[対策]資源名称で出力されている表の構成列の定義内容を確認し，次のどちらかの処置をしてください。

- 資源名称で出力された表を，更新可能なオンライン再編成対象外の別の RD エリアに定義してください。
- 資源名称で出力された表の列構成を，暗号化列を含まない構成に変更してください。

6.2　アボートコード

暗号化機能を使用する場合に出力されるアボートコードを次の表に示します。その他のアボートコードについては，マニュアル「HiRDB Version 8 メッセージ」を参照してください。

表 6-1　暗号化機能を使用する場合に出力されるアボートコード

アボートコード	原因	対策
Pae2260	暗号ライブラリの関数呼び出し処理で，内部矛盾を検知しました。	%PDDIR%¥spool 下のファイルを退避し，保守員に連絡してください。
Pd00031	暗号ライブラリから不正なリターンコードが返りました。	%PDDIR%¥spool 下のファイルを退避して，直前に出力された KFPD00008-E または KFPD00037-E のメッセージの内容とともに，保守員に連絡してください。
Phm6010	暗号ライブラリから不正なリターンコードが返りました。	%PDDIR%¥spool 下のファイルを退避して，直前に出力された KFPH26001-I のメッセージの内容とともに，保守員へ連絡してください。
Pu20002	暗号ライブラリの関数呼び出し処理で，内部矛盾を検知しました。	%PDDIR%¥spool 下のファイルを退避し，保守員に連絡してください。

6.3　SQLSTATE

暗号化機能を使用する場合に出力される SQLSTATE を次の表に示します。その他の SQLSTATE については，マニュアル「HiRDB Version 8 メッセージ」を参照してください。

表 6–2　暗号化機能を使用する場合に出力される SQLSTATE

SQLSTATE	意味	SQLCODE
0A506	HiRDB のサーバ種別に不整合が発生しました。詳細については KFPA19334-E メッセージを参照してください。	-1334
40DJE	暗号化表の定義に誤りがあります。 詳細については KFPA19640-E メッセージを参照してください。	-1640
40DJF	暗号化列と繰返し列を組み合わせた複数列インデクスは定義できません。 詳細については KFPA19641-E メッセージを参照してください。	-1641
40DJG	列が削除できません。 詳細については KFPA19644-E メッセージを参照してください。	-1644
42J19	詳細については KFPA19640-E メッセージを参照してください。	-1640
42J20	詳細については KFPA19641-E メッセージを参照してください。	-1641
54010	詳細については KFPA19516-E メッセージを参照してください。	-1516
54011	詳細については KFPA19644-E メッセージを参照してください。	-1644

付録

付録 A　予約語

(1)　SQL の予約語

暗号化機能を使用すると，次の表に示す予約語が追加となります。

表 A-1　SQL の予約語

予約語	SQL92	SQL99	UNIFY	XDM/RD	HiRDB
ENCRYPT	－	－	－	－	○

（凡例）

○：予約語です。

－：予約語ではありません。

SQL92：ISO SQL 1992

SQL99：ISO SQL 1999

UNIFY：UNIFY2000

XDM/RD：XDM/RD E2

HiRDB：HiRDB Plus Version 8

(2)　SQL 予約語削除機能で削除できる予約語

暗号化機能を使用した場合の，SQL 予約語削除機能で削除できる予約語，および削除したときに使用できなくなる機能を次の表に示します。

表 A-2　削除できる予約語

予約語	使用できなくなる機能
INNER	• 結合表 INNER JOIN • 暗号化機能

付録 B　ディクショナリ表

暗号化機能を使用すると，ディクショナリ表の一部の内容が変更となります。

付録 B.1　列の値が格納されるディクショナリ表

(1)　SQL_TABLES

列名	データ型	内容
N_CONSTRUCTOR_COLUMN	SMALLINT	暗号化列数。 暗号化表以外，ビュー表，および外部表の場合はナル値になります。
CONSTRUCTOR_TYPE	CHAR(1)	暗号ライブラリ製品種別。 B：HiRDB に組み込まれた暗号ライブラリ ナル値：上記以外 暗号化表以外，ビュー表，および外部表の場合はナル値になります。

(2)　SQL_COLUMNS

列名	データ型	内容
CONSTRUCTOR_TYPE	CHAR(1)	暗号ライブラリ製品種別。 B：HiRDB に組み込まれた暗号ライブラリ ナル値：上記以外 暗号化列以外の列，ビュー表，および外部表の場合はナル値になります。

付録 B.2　列の内容が変更となるディクショナリ表

(1)　SQL_COLUMNS

列名	データ型	内容
SUPPRESS_INF	CHAR(1)	データ抑制指定有無。 Y：指定あり ナル値：指定なし データ抑制を指定していない表，暗号化表，ビュー表，および外部表の場合はナル値となります。

付録 C　作業表用ファイル

暗号化機能を使用する場合，作業表用ファイルを必要とする SQL が追加されます。

作業表用ファイルは，SELECT 文で複数の表を結合して検索する場合や，CREATE INDEX を実行する場合など，特定の SQL 実行時に使用されます。追加される「作業表を必要とする SQL」を次に示します。

- SELECT 文で ORDER BY 句に暗号化列を指定する場合

付録 D　用語解説

暗号化機能で使用している用語について説明します。

（ア行）

暗号化指定

暗号化表を定義するときに，暗号化する列に対して指定するオプションのことです。暗号化指定ありで表を定義すると，共通鍵が生成されます。

暗号化表

暗号化列がある表のことをいいます。

暗号化表は，CREATE TABLE（暗号化指定あり）で定義できます。

暗号化列

暗号化した列のことをいいます。

CREATE TABLE で暗号化表を定義する場合，列定義に暗号化指定があると，その列が暗号化列となります。

（カ行）

共通鍵

データの暗号化，および復号化に使用する鍵のことです。

共通鍵の情報は，システム用 RD エリアに格納されます。

索引

り

れ