HITACHI
Inspire the Next

ノンストップデータベース

HiRDB Version 9 データベース暗号化機能

解説・手引・文法・操作書

3020-6-467-50

前書き

■ 対象製品

●適用 OS：HP-UX 11i V3(IPF)

P-1J62-3691 HiRDB Server with Additional Function Version 9 09-66

●適用 OS：AIX V7.1，AIX V7.2

P-1M62-3691 HiRDB Server with Additional Function Version 9 09-66

●適用 OS：Red Hat Enterprise Linux 6 (64-bit x86_64)

P-9W62-4691 HiRDB Server with Additional Function Version 9 09-66

●適用 OS：Windows Server 2008 R2，Windows Server 2008 (x64)，Windows Server 2012，Windows Server 2016，Windows 7 Professional (x64)，Windows 7 Enterprise (x64)，Windows 7 Ultimate (x64)，Windows 8 Pro (x64)，Windows 8 Enterprise (x64)，Windows 8.1 Pro (x64)，Windows 8.1 Enterprise (x64)，Windows 10 Pro (x64)，Windows 10 Enterprise (x64)

P-2962-9294 HiRDB Server with Additional Function Version 9 09-66

●適用 OS：Windows Server 2008，Windows Server 2012，Windows Server 2016，Windows 7 Professional，Windows 7 Enterprise，Windows 7 Ultimate，Windows 7 Professional (x64)，Windows 7 Enterprise (x64)，Windows 7 Ultimate (x64)，Windows 8 Pro，Windows 8 Enterprise，Windows 8 Pro (x64)，Windows 8 Enterprise (x64)，Windows 8.1 Pro，Windows 8.1 Enterprise，Windows 8.1 Pro (x64)，Windows 8.1 Enterprise (x64)，Windows 10 Pro，Windows 10 Enterprise，Windows 10 Pro (x64)，Windows 10 Enterprise (x64)

P-2462-9294 HiRDB Server with Additional Function Version 9(32) 09-66

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

その他記載の会社名，製品名などは，それぞれの会社の商標もしくは登録商標です。

HiRDB Server with Additional Function Version 9 は，EMC Corporation の RSA(R) BSAFE^{TM} ソフトウェアを搭載しています。

1. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

2. This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

3. This product includes software written by Tim Hudson (tjh@cryptsoft.com).

4.本製品には OpenSSL Toolkit ソフトウェアを OpenSSL License および Original SSLeay License に従い使用しています。OpenSSL License および Original SSLeay License は以下の通りです。

LICENSE ISSUES

==========

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
the OpenSSL License and the original SSLeay license apply to the toolkit.
See below for the actual license texts. Actually both licenses are BSD-style
Open Source licenses. In case of any license issues related to OpenSSL
please contact openssl-core@openssl.org.

OpenSSL License

/*

==========

* Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright

*
==========
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/
Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the copyright

* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
* must display the following acknowledgement:
* "This product includes cryptographic software written by
* Eric Young (eay@cryptsoft.com)"
* The word 'cryptographic' can be left out if the rouines from the library
* being used are not cryptographic related :-).
* 4. If you include any Windows specific code (or a derivative thereof) from
* the apps directory (application code) you must include an acknowledgement:
* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
*
* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
* copied and put under another distribution licence
* [including the GNU Public Licence.]
*/

■ 発行

2018 年 4 月　3020-6-467-50

変更内容

変更内容(3020-6-467-50)　HiRDB Server with Additional Function Version 9 09-66

追加・変更内容	変更個所
HiRDB ファイルシステム領域を暗号化する機能をサポートしました。 これによって，HiRDB を経由せずにファイルシステム領域を参照されることによる情報漏えいのリスクを低減できるようになります。	1.1，1.3，1.4.2，1.4.3，1.5，表 2-1，2.2.1(1)(a)，2.3.2，表 2-2，5.，6.1，6.2，6.3，6.4，6.5
HiRDB ファイルシステム領域を暗号化する機能をサポートしました。これに伴い，HiRDB のメモリ所要量に，暗号化 HiRDB ファイルシステム領域の機能を使用する場合のメモリ所要量の計算式を追加しました。	8.1.1（2）
HiRDB ファイルシステム領域を暗号化する機能をサポートしました。これに伴い，Windows 版 HiRDB で暗号化機能を使用する場合に変更が必要になる HiRDB のリソース数に関連する環境変数の見積もり式を追加しました。	10.
HiRDB ファイルシステム領域を暗号化する機能をサポートしました。これに伴い，次のメッセージを追加しました。 KFPI21505-I，KFPI21609-E，KFPI21681-I，KFPI21682-I，KFPI21683-I，KFPI21684-E，KFPI21685-E，KFPI21686-E，KFPI21687-E，KFPI21688-E，KFPI21689-E，KFPI21690-E	11.1
HiRDB ファイルシステム領域を暗号化する機能をサポートしました。これに伴い，「HiRDB ファイルシステムのエラーコード」を追加しました。 -1544	11.4
HiRDB ファイルシステム領域を暗号化する機能をサポートしました。これに伴い，次のコマンドのリターンコードを追加しました。 • pdmkekey • pdchekey	付録 D.5
HiRDB ファイルシステム領域を暗号化する機能をサポートしました。これに伴い，「暗号鍵ファイルが必要なコマンド」を追加しました。	付録 D.8
用語解説に次の項目を追加しました。 • 暗号化 HiRDB ファイルシステム領域 • 暗号鍵ファイル	付録 E
マニュアルの体裁を変更しました。	－

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(3020-6-467-40)　HiRDB Server with Additional Function Version 9 09-65

追加・変更内容
HiRDB のサポートプラットフォームに次の OS を追加しました。 • AIX V7.2

追加・変更内容
• Windows Server 2016

変更内容(3020-6-467-30)　HiRDB Server with Additional Function Version 9 09-60

追加・変更内容
BINARY 型（圧縮列も含めて）を暗号化できるようにしました。これに伴い，次の項目を追加，変更しました。 • CREATE TABLE および ALTER TABLE に圧縮指定を追加しました。 • RD エリアの容量見積もりを修正しました。 KFPA19640-E メッセージを変更しました。
HiRDB のメモリ所要量に，SQL 実行時に必要なメモリ所要量の計算式を追加しました。
データディクショナリ用 RD エリアの容量の見積もり式の，表の格納ページ数の計算方法を変更しました。
HiRDB のサポートプラットフォームに次の OS を追加しました。 • Linux 7 • Windows 10

変更内容(3020-6-467-20)　HiRDB Server with Additional Function Version 9 09-50

追加・変更内容
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，機能の説明を追加しました。
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，HiRDB システム定義 pd_tpyrced_key オペランドの説明を追加しました。
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，クライアント環境変数 PDTPYRCEDKEY を追加しました。
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，復号認証キー情報登録ユティリティ pdregtpyrcedkey を追加しました。
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，ディクショナリ表 SQL_TPYRCEDKEY 表を追加しました。
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，HiRDB のメモリ所要量の見積もりの変更点を追加しました。
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，データディクショナリ用 RD エリアの容量見積もりの変更点を追加しました。
特定 UAP に対する暗号化データの復号機能をサポートしました。これに伴い，次のメッセージを追加しました。 KFPA11552-E，KFPA11613-E，KFPA19621-E，KFPA19930-E，KFPD00032-W，KFPD00033-I，KFPD00034-W，KFPX21307-I，KFPX21308-E，KFPX21309-E，KFPX21310-I，KFPX21311-E，KFPX21312-W，KFPX21313-E また，次のメッセージを変更しました。 KFPA19644-E

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。なお，ここに記載されていない前提情報については，マニュアル「HiRDB Version 9 解説」（3020-6-450）を参照してください。

- P-1J62-3691 HiRDB Server with Additional Function Version 9
- P-1M62-3691 HiRDB Server with Additional Function Version 9
- P-9W62-3691 HiRDB Server with Additional Function Version 9
- P-2962-9294 HiRDB Server with Additional Function Version 9
- P-2462-9294 HiRDB Server with Additional Function Version 9

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 Server with Additional Function」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

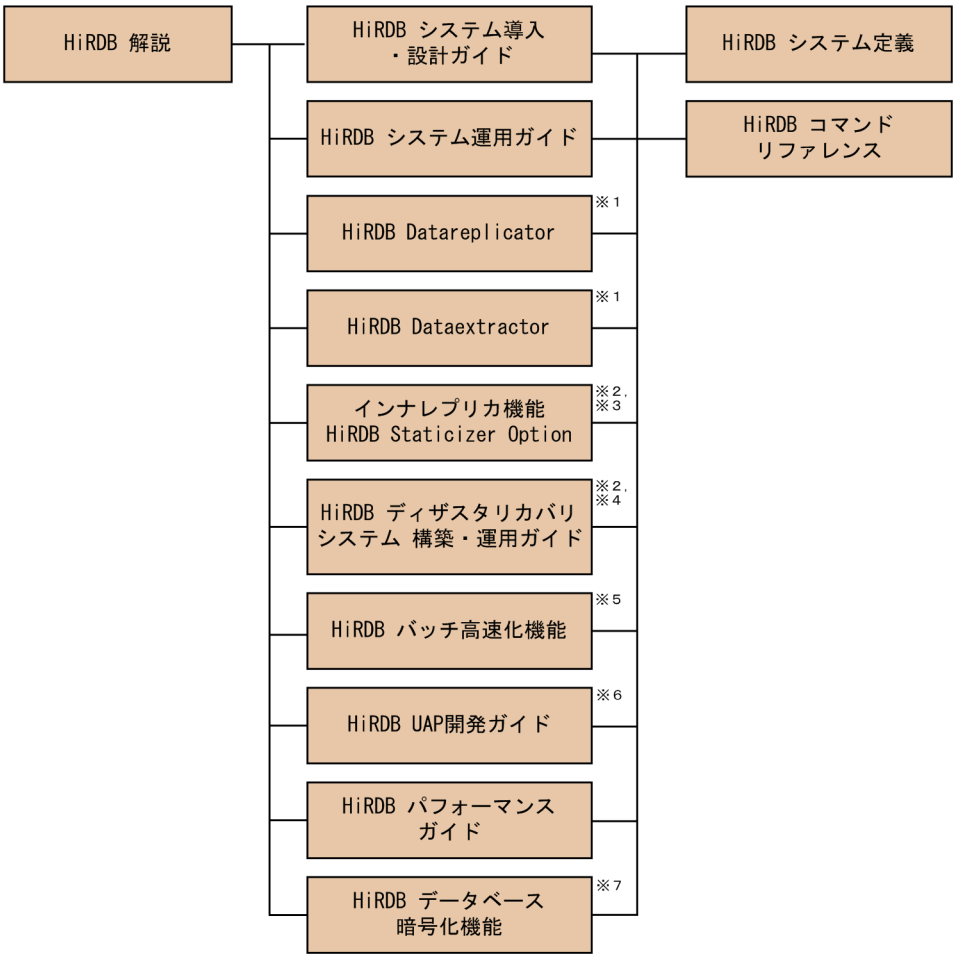
また，このマニュアルは，HiRDB のマニュアルを前提としていますので，あらかじめお読みいただくことをお勧めします。

■ 利用者ごとの関連マニュアル

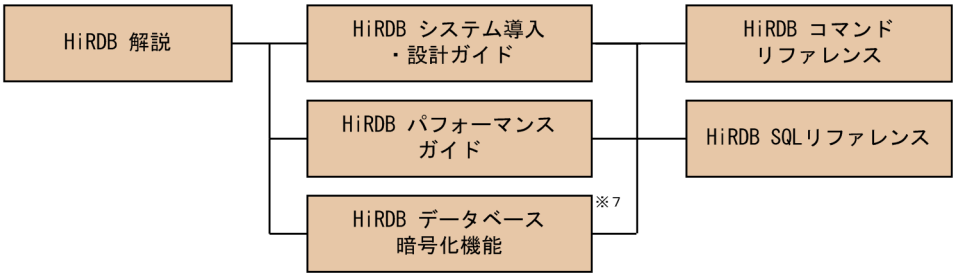
HiRDB のマニュアルをご利用になる場合，利用者ごとに次のようにお読みください。

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。

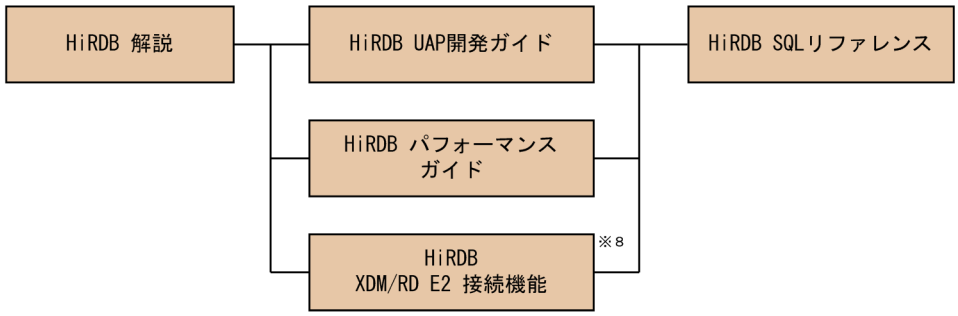
システム管理者が利用するマニュアル



表の作成者が利用するマニュアル



UAP作成者，およびUAP実行者が利用するマニュアル



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　データベース暗号化機能を使用する場合にお読みください。
注※８　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 Server with Additional Function Version 9	HiRDB/シングルサーバ	HiRDB または HiRDB Server with Additional Function
	HiRDB/パラレルサーバ	

■ 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。

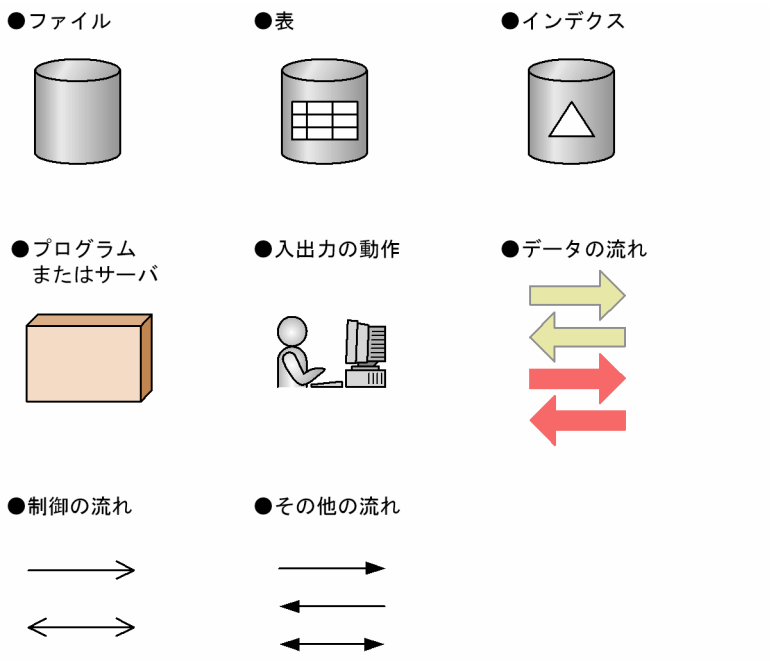
  Windows 版：%PDDIR%¥CLIENT¥UTL¥

  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。

■ 図中で使用している記号

このマニュアルの図中で使用している記号を次のように定義します。



■ このマニュアルで使用している記号

形式および説明で使用してい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 1 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 1 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。	

記　号	意　味	例
::=	::=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
～	この記号の後にユーザ指定値の属性を示します。	アドレスプリフィクス～<符号なし整数>((24～30))
＜　＞	ユーザ指定値の構文要素を示します。	
((　))	ユーザ指定値の指定範囲を示します。	

■ このマニュアルで使用している構文要素記号

このマニュアルで使用している構文要素記号を次に示します。

構文要素記号	意　　味
<英字>	アルファベット（A～Z，a～z）と下線（_）
<英字記号>	アルファベット（A～Z，a～z）と#，@，￥
<英数字>	英字と数字（0～9）
<英数字記号>	英字記号と数字
<符号なし整数>	数字
<符号なし 10 進数>※1	数字（0～9 の並び）ピリオド（.）数字（0～9 の並び）
<識別子>※2	先頭がアルファベットの英数字列
<文字列>	任意の文字の配列
<記号名称>	先頭が英字記号の英数字記号 UNIX 版の場合，￥は使用できません。
<パス名>※3	UNIX 版の場合：/，英数字，ピリオド（.），#，および@ Windows 版の場合：￥，英数字，ピリオド（.），空白，丸括弧，#，および@

注

すべて半角文字を使用してください。また，英字の大文字と小文字は区別されます。さらに，パス名は使用している OS に依存します。

注※1

ピリオドの前の数字がすべて 0 の場合，ピリオドより前の 0 を省略できます。また，ピリオドの後ろの数字がすべて 0 の場合，ピリオド以降を省略できます。

例 1 ：0.008 → .008

例 2 ：15.000 → 15

注※2

RD エリア名の場合は，先頭が英字記号で始まる英数字記号，下線（_），ハイフン（-），および空白となります。また，RD エリア名に空白が含まれる場合は，引用符（"）で囲んでください。

ホスト名の場合は，アルファベット（A～Z，a～z），数字，ピリオド（.），ハイフン（-），下線（_），および@で構成される文字列となります。

注※3

パス名に空白，または丸括弧を含む場合は，前後を引用符（"）で囲んでください。

なお，Windows 版の場合，コロン（：）をドライブ名に使用できます。

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。

データベースを暗号化する機能には，表定義時に列に対して暗号化を指定する方法と，HiRDB ファイルシステム領域作成時に，HiRDB ファイルシステム領域に暗号化指定する方法があります。HiRDB ファイルシステム領域に暗号化を指定する方法は「暗号化 HiRDB ファイルシステム領域」を参照してください。この節は表定義時に列に対して暗号化を指定する方法について説明します。

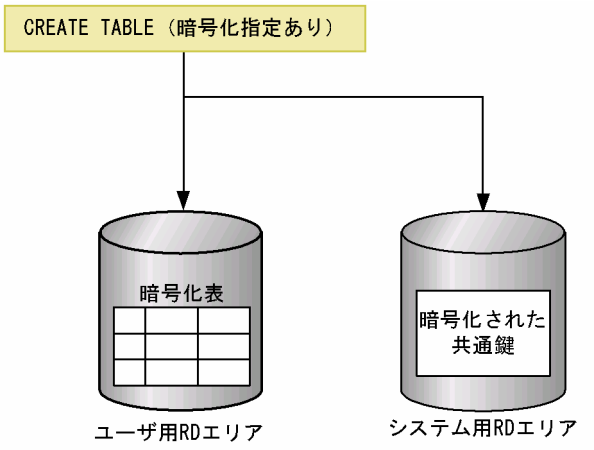
表定義時に列に対して暗号化の指定をすると，データベースへのデータ格納時に，その列のデータは暗号化されて格納されます。暗号化する列を**暗号化列**，暗号化列がある表を**暗号化表**といいます。なお，暗号化を指定しない列は，その表に暗号化列を含んでいても，暗号化しない状態でデータベースに格納されます。

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



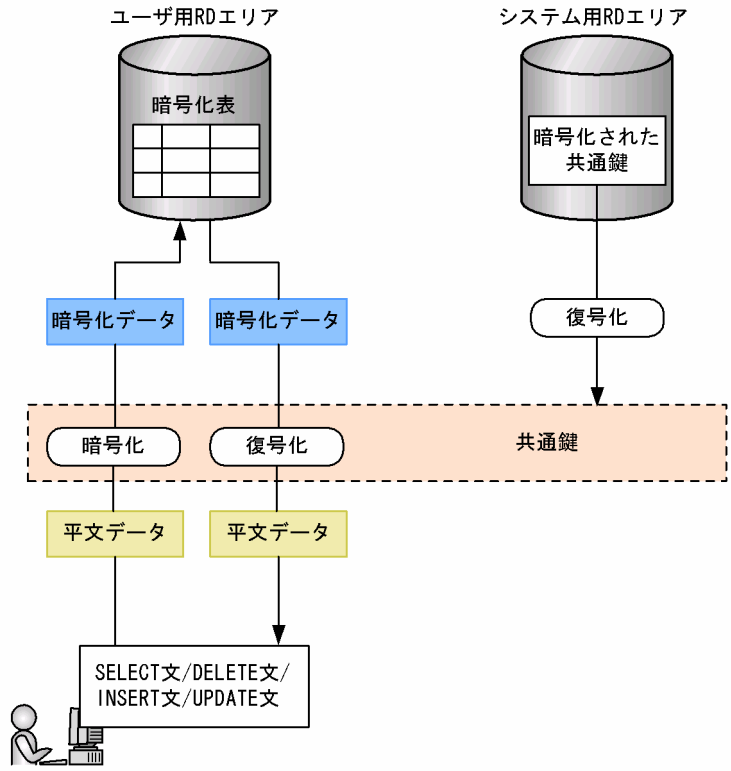
[説明]

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　特定 UAP に対する暗号化データの復号機能

特定 UAP に対する暗号化データの復号機能について説明します。

1.2.1　特定 UAP に対する暗号化データの復号機能の概要

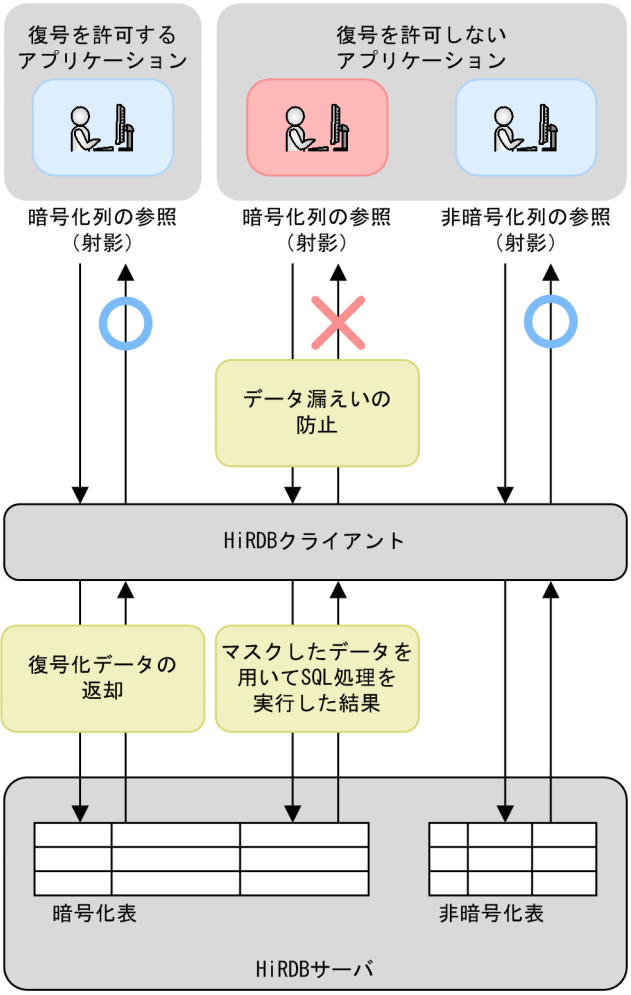
暗号化機能は，HiRDB ファイルシステム領域などのデータが格納されているファイルを直接参照するといった不正なアクセスから，データを守ることに有効です。HiRDB に接続したアプリケーションから SQL を実行し，暗号化列のデータを参照すると，平文データを受け取ることができます。

しかし，暗号化するデータには，特定のユーザだけにデータの復号を許可し，それ以外のユーザには平文データを参照させたくない場合があります。このような場合には，特定 UAP に対する暗号化データの復号機能が有効です。

特定 UAP に対する暗号化データの復号機能では，機密データの情報漏えいを防止するために，復号を許可するアプリケーションにだけ，暗号化列の平文データを返却します。復号を許可しないアプリケーションには，暗号化列のデータをマスクした値を返却します。HiRDB では，HiRDB システムに登録した復号認証キー情報の条件に一致するアプリケーションに対して復号を許可します。

特定 UAP に対する暗号化データの復号機能の概要を，次の図に示します。

図 1-3　特定 UAP に対する暗号化データの復号機能の概要



1.2.2　復号認証キー情報

復号認証キー情報について，説明します。

(1)　復号認証キー情報の構成要素

復号認証キー情報は，次の表に示す情報で構成されています。HiRDB システムに登録した復号認証キー情報の構成要素がすべて一致するアプリケーションに対して，復号を許可します。

表 1-1　復号認証キー情報の構成要素

構成要素	内容	一致する条件
IP アドレス	復号を許可するアプリケーションの実行マシンの IP アドレス。	アプリケーションを実行するマシンの IP アドレスが，HiRDB システムに登録した復号認証キー情報の IP アドレスと一致するか確認します。

構成要素	内容	一致する条件
認可識別子	復号を許可するアプリケーションの実行ユーザの認可識別子。 特定のマシンから，すべての実行ユーザに対して許可する場合は，PUBLIC を指定します。	アプリケーションを実行するユーザの認可識別子が，HiRDB システムに登録した復号認証キー情報の認可識別子と一致するか確認します。※1
復号認証キー	復号を許可する復号認証キー。	アプリケーションの実行環境に設定した復号認証キーに関するクライアント環境定義の内容が，HiRDB システムに登録した復号認証キー情報の復号認証キーと一致するか確認します。
有効期限	復号認証キー情報の有効期限。 無期限を指定することもできます。	アプリケーションが接続した時刻が，HiRDB システムに登録した復号認証キー情報の有効期限内であるかを確認します。※2

注※1

実行するユーザの認可識別子は，CONNECT または SET SESSION AUTORIZATION に指定した認可識別子になります。

注※2

復号の許可を判定する時刻は，CONNECT 要求受付時または SET SESSION AUTORIZATION 要求受付時の時刻になります。復号の許可は，CONNECT 要求受付時または SET SESSION AUTORIZATION 要求受付時に判定し，その接続が切り離されるか，または SET SESSION AUTORIZATION を実行するまで有効になります。

復号認証キー情報の登録には，次の規則があります。

- IP アドレスと，認可識別子の 1 つの組み合わせに対して，1 つの復号認証キーを登録できます。
- 認可識別子に PUBLIC を指定した場合も，IP アドレスと，PUBLIC という認可識別子の 1 つの組み合わせに対して，1 つの復号認証キーを登録できます。

(2) 復号認証キー情報の管理

復号認証キー情報は，ディクショナリ表で管理します。SQL_TPYRCEDKEY 表を参照することで，復号認証キー情報の IP アドレス，認可識別子および有効期限が確認できます。

SQL_TPYRCEDKEY 表を参照できるのは，DBA 権限所有者，および監査人だけです。ディクショナリ表の参照権限を設定した場合でも，SQL_TPYRCEDKEY 表に対する参照権限は同じです。ディクショナリ表の参照権限については，マニュアル「HiRDB Version 9 システム運用ガイド」の「ディクショナリ表の参照権限を設定するには」を参照してください。

1.2.3　実行結果の変更点

復号認証キー情報が一致する場合，暗号化表に対する実行結果は，特定 UAP に対する暗号化データの復号機能を使用していない場合と同じになります。ここでは，復号認証キー情報が一致しない場合に，実行結果が変わる内容について説明します。

(1)　検索 SQL の場合

データを検索する SQL 実行時の変更点について説明します。復号認証キー情報が一致しない場合の動作は，暗号化列の指定個所によって異なります。復号認証キー情報が一致しない場合の検索 SQL 実行結果を，次の表に示します。

表 1-2　復号認証キー情報が一致しない場合の検索 SQL 実行結果

暗号化列の指定個所	実行結果
WHERE 句中※1 ON 句中※1 HAVING 句中※1 副問合せ中※1※2	検索データなし(SQLCODE=100)になります。
上記以外	マスクした値を用いて SQL 処理を実行した結果を返却します。

注※1

導出表および内部導出表の導出列のうち，使用しない導出列を内部的に削除するため，暗号化列を含む値式を導出する導出列を指定しない場合，検索結果がデータなしにならないことがあります。

注※2

副問合せについては，マニュアル「HiRDB Version 9 SQL リファレンス」の「副問合せ」を参照してください。次に示す個所に暗号化列が含まれる場合も，副問合せ中に暗号化列を指定した場合と同様の検索結果になります。

- 導出表
- 内部導出表
- group by 句に列指定以外の値式を指定した場合，等価変換によって生成する導出表

暗号化列のデータをマスクする値を次の表に示します。

表 1-3　暗号化列のデータをマスクした値

暗号化列のデータ型	マスクにより出力されるデータ※
CHAR MCHAR VARCHAR MVARCHAR	半角アスタリスク(*)(0x2A)の値が定義長の長さ分連続するデータ列

暗号化列のデータ型	マスクにより出力されるデータ※
NCHAR NVARCHAR	半角アスタリスク(*)(0x2A)の値が定義長×2 の長さ分連続するデータ列
INTEGER SMALLINT	0
DECIMAL(m,n)	0.00...00 (小数点以下は n 個の 0) 符号部は正規化後の X'C'
FLOAT	+0.000000000000000E+00
SMALLFLT	+0.0000000E+00
DATE	0001-01-01
TIME	00:00:00
TIMESTAMP(p)	0001-01-01 00:00:00.0...0 (小数点以下は p 個の 0)
INTERVAL YEAR TO DAY	00000000.
INTERVAL HOUR TO SECOND	000000.
BINARY	0x00 (長さ 1 バイト)

注※

暗号化列のデータが NULL 値の場合，NULL 値を返却します。

(2) INSERT 文，UPDATE 文，DELETE 文の場合

INSERT 文，UPDATE 文，DELETE 文の SQL 実行時の変更点について説明します。復号認証キー情報が一致しない場合の動作は，暗号化列の指定個所によって異なります。復号認証キー情報が一致しない場合の更新 SQL 実行結果を，次の表に示します。

表 1-4　復号認証キー情報が一致しない場合の更新 SQL 実行結果

SQL 種別	更新対象表	更新対象列	更新対象列以外での暗号化列の指定	SQL 実行結果
INSERT	暗号化表	暗号化列	－	×
		非暗号化列	指定あり	×
			指定なし	○※1※2
	非暗号化表	非暗号化列	指定あり	×
			指定なし	○※2※3
UPDATE	暗号化表	暗号化列	－	×

SQL 種別	更新対象表	更新対象列	更新対象列以外での暗号化列の指定	SQL 実行結果
		非暗号化列	指定あり	×
			指定なし	○※2※3※4
	非暗号化表	非暗号化列	指定あり	×
			指定なし	○※2※3※4
DELETE	暗号化表	－	指定あり	×
			指定なし	○※2※4
	非暗号化表	－	指定あり	×
			指定なし	○※2※4

（凡例）

○：実行できます。

×：SQL エラー（KFPA19930-E）になります。

－：該当しません。

注※1

次の条件に該当する場合，SQL エラー（KFPA19930-E）となります。

- 暗号化列の列定義に with default を指定している。
- 暗号化列の列定義に DEFAULT 句を指定している。

注※2

更新対象表への操作を契機とするトリガを定義し，次の条件に該当する場合，SQL エラー（KFPA19930-E）となります。

- トリガ動作条件に暗号化列を指定している。
- トリガ SQL 中に新値相関名で修飾した暗号化列または旧値相関名で修飾した暗号化列を指定している。
- トリガ SQL で実行する操作系 SQL が SQL エラー（KFPA19930-E）を出力する条件に該当する。

注※3

更新対象表を参照表とする参照制約を定義し，被参照表の主キー構成列に暗号化列を含む場合，SQL エラー（KFPA19930-E）となります。

注※4

更新対象表を被参照表とする参照制約を定義し，参照表の外部キー構成列に暗号化列を含む場合，SQL エラー（KFPA19930-E）となります。

(3) ASSIGN LIST 文の場合

ASSIGN LIST 文の SQL 実行時の変更点について説明します。復号認証キー情報が一致しない場合の動作は，暗号化列の指定個所によって異なります。復号認証キー情報が一致しない場合の ASSIGN LIST 文実行結果を，次の表に示します。

表 1-5　復号認証キー情報が一致しない場合の ASSIGN LIST 文実行結果

リストの基表	暗号化列の指定	SQL 実行結果
暗号化表	指定あり	×
	指定なし	○
非暗号化表	－	○

（凡例）

○：実行できます。

×：SQL エラー（KFPA19930-E）になります。

－：該当しません。

(4) CALL 文の場合

CALL 文を実行した場合の実行可否および実行結果は，呼び出す SQL 手続き中で実行する操作系 SQL の実行可否および実行結果に依存します。

(5) EXECUTE 文，EXECUTE IMMEDIATE 文の場合

EXECUTE 文または EXECUTE IMMEDIATE 文を実行した場合の実行可否および実行結果は，EXECUTE 文または EXECUTE IMMEDIATE 文で実行する SQL の実行可否および実行結果に依存します。

(6) その他 SQL の場合

その他 SQL については，変更点はありません。

(7) ユティリティの場合

ユティリティについては，変更点はありません。

1.2.4 使用方法

特定 UAP に対する暗号化データの復号機能の使用方法について説明します。

(1) HiRDB システム定義の設定

HiRDB システム定義の pd_tpyrced_key オペランドに Y を指定します。pd_tpyrced_key オペランドの詳細は，「特定 UAP に対する暗号化データの復号機能に関するオペランド」を参照してください。

なお，pd_tpyrced_key オペランドが N の状態で作成したストアドプロシジャおよびトリガがある場合は，ALTER ROUTINE で再作成してください。

(2) 復号認証キー情報の登録

pdregtpyrcedkey ユティリティを実行して，復号認証キー情報を登録します。pdregtpyrcedkey ユティリティの詳細は，「復号認証キー情報登録ユティリティ（pdregtpyrcedkey）」を参照してください。

(3) クライアント環境変数の設定

復号を許可したいアプリケーションには，クライアント環境定義 PDTPYRCEDKEY に復号認証キーを指定してください。PDTPYRCEDKEY の詳細は，「クライアント環境定義の設定内容」を参照してください。

1.3　暗号化 HiRDB ファイルシステム領域

HiRDB ファイルシステム領域を暗号化する方法を説明します。

1.3.1　暗号化 HiRDB ファイルシステム領域の概要

暗号化 HiRDB ファイルシステム領域は，HiRDB ファイルのレコードの I/O 時に暗号化，復号する機能です。HiRDB ファイルのレコードの I/O 時に暗号化，復号することで，HiRDB 内部では通常の HiRDB ファイルと同じように使用できます。そのため，SQL を使用したデータベースへのアクセス時の機能的な制限はありません。また，OS ファイルを直接的に参照したときの機密情報の漏えいのリスクを低減できます。

1.3.2　暗号化 HiRDB ファイルシステム領域の使用方法の概要

暗号化 HiRDB ファイルシステム領域は，pdfmkfs に暗号化指定（-E）することで作成できます。暗号化 HiRDB ファイルシステム領域は，作成する HiRDB ファイルのレコード（ページ）データがレコード単位にすべて暗号化されます。暗号化，復号処理には pdmkekey コマンドで作成した暗号鍵ファイルが必要です。暗号鍵ファイルはユニットごとに作成し，システム定義の pd_ekey オペランドに暗号鍵ファイルの場所を指定します。

1.3.3　暗号化 HiRDB ファイルシステム領域の暗号化の方式

暗号化 HiRDB ファイルシステム領域は，暗号化アルゴリズムとして AES（Advanced Encryption Standard）を使用します。暗号化 HiRDB ファイルシステム領域の暗号鍵は次の 2 種類の 256 bit の暗号鍵を使用します。

- 暗号化 HiRDB ファイルシステム領域のデータを暗号化する暗号鍵。HiRDB ファイルごとに 1 つあり，暗号化して HiRDB 内で保持しています。
- 上記の暗号鍵を暗号化するための暗号鍵。暗号鍵ファイルの中にあります。

1.3.4　使用方法

暗号化 HiRDB ファイルシステム領域の使用方法について説明します。

(1)　暗号鍵ファイルの作成

暗号鍵ファイル作成コマンド（pdmkekey）で暗号鍵ファイルを作成します。暗号鍵ファイル作成コマンドの詳細は，「暗号鍵ファイル作成コマンド（pdmkekey）」を参照してください。

(2)　暗号化 HiRDB ファイルシステム領域の作成

pdfmkfs に暗号化指定（-E）で HiRDB ファイルシステム領域を作成します。暗号化指定のオプションの詳細は，「pdfmkfs （HiRDB ファイルシステム領域の初期設定)」を参照してください。

(3)　HiRDB システム定義の設定

HiRDB システム定義の pd_ekey オペランドに暗号鍵ファイルのパス名を指定します。pd_ekey オペランドの詳細は，「暗号化 HiRDB ファイルシステム領域に関するオペランド」を参照してください。

1.3.5　注意事項

1. 暗号化 HiRDB ファイルシステム領域は，特定 UAP に対する暗号化データの復号機能の対象にはなりません。特定 UAP に対する暗号化データの復号機能を使用する場合は，暗号化 HiRDB ファイルシステム領域に作成する表に対して暗号化表の指定をしてください。
2. pdlogunld コマンドおよび，自動ログアンロード機能の出力先に，暗号化 HiRDB ファイルシステム領域を指定している場合，HiRDB Datareplicator の「アンロードログファイルによるデータ連動回復」で，連動回復要バックアップファイルを使用した回復はできません。

1.4　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。

1.4.1　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
- Linux
- Windows

1.4.2　表定義時に列に対して暗号化を指定した場合に対象となる資源

表定義時に列に対して暗号化を指定した場合に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。

1.4.3　HiRDB ファイルシステム領域に暗号化を指定した場合に対象となる資源

暗号化を指定した HiRDB ファイルシステム領域の暗号化の対象となる資源を次に示します。

- 暗号化を指定した HiRDB ファイルシステム領域のレコードデータ
- 暗号化を指定した HiRDB ファイルシステム領域から pdfbkup で取得したバックアップファイル

HiRDB ファイルシステム領域の暗号化の指定は使用目的（pdfmkfs の-k）に関わらず，すべての HiRDB ファイルシステム領域に対して指定できます。

暗号化 HiRDB ファイルシステム領域は，ストレージを直接参照された場合に情報の漏えいを防止することを目的としています。そのため，暗号化の対象はストレージのデータだけで，メモリ中のデータおよび通信データは平文となります。

1.5 インストール

HiRDB Server with Additional Function 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 9 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 Server with Additional Function を HiRDB に変更する場合，HiRDB Server with Additional Function をアンインストールしてから HiRDB をインストールし直してください。
- HiRDB/パラレルサーバの場合，すべてのユニットに HiRDB Server with Additional Function をインストールしてください。HiRDB Server with Additional Function と HiRDB との混在はできません。
- UNIX 版 HiRDB Server with Additional Function の場合，HiRDB Server with Additional Function 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。
- UNIX 版 HiRDB Server with Additional Function を上書きインストールする場合，次の 2 つのバージョンを比較し，異なるときは HiRDB Data Convert Type1 Option も必ず上書きインストールしてください。

  ・インストールする HiRDB Data Convert Type1 Option のバージョン（インストーラの "Install Software."で表示される VR）

  ・インストール済みの HiRDB Data Convert Type1 Option のバージョン（インストーラの "List Installed Software."で表示される VR）
- 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 Server with Additional Function または HiRDB）を確認できます。

2 HiRDB システム定義

この章では，暗号化機能に関連する HiRDB システム定義について説明します。

2.1　オペランドの一覧

暗号化機能に関連する HiRDB システム定義のオペランド，および再開始時の変更可否の一覧を次の表に示します。

なお，ここでは，暗号化機能に関係するオペランドの説明だけを記載しています。そのほかの HiRDB システム定義の説明については，マニュアル「HiRDB Version 9 HiRDB システム定義」を参照してください。

表 2-1　暗号化機能に関連するオペランドの一覧

オペランド名	定義名							強制終了，異常終了後の変更可否	計画停止後の変更可否
	SYS	UNT	SVR	SDS	FES	DS	BES		
pd_tpyrced_key	○							○	○
pd_ekey	○	○						○	○

（凡例）

○：指定値を変更できます。

空白：該当しません。

SYS：システム共通定義

UNT：ユニット制御情報定義

SVR：サーバ共通定義

SDS：シングルサーバ定義

FES：フロントエンドサーバ定義

DS ：ディクショナリサーバ定義

BES：バックエンドサーバ定義

2.2　オペランドの形式

2.2.1　暗号化機能に関連するオペランドの形式

暗号化機能に関連するオペランドの形式について説明します。

(1)　特定 UAP に対する暗号化データの復号機能に関するオペランド

(a)　set 形式

[set pd_tpyrced_key= Y | N]

[set pd_ekey= "暗号鍵ファイル名"]

2.3　オペランドの説明

2.3.1　特定 UAP に対する暗号化データの復号機能に関するオペランド

◆　pd_tpyrced_key = Y | N

特定 UAP に対する復号化機能を使用するかどうかを指定します。

Y：

特定 UAP に対する復号化機能を使用します。

N：

特定 UAP に対する復号化機能を使用しません。

2.3.2　暗号化 HiRDB ファイルシステム領域に関するオペランド

◆　pd_ekey = "暗号鍵ファイル名"

～＜パス名＞((1024 文字以内))

暗号化 HiRDB ファイルシステム領域を使用する場合，pdmkekey コマンドで作成した暗号鍵ファイル名を絶対パスで指定します。

2.4 pdconfchk コマンドでチェックできるオペランド

暗号化機能に関連する HiRDB システム定義のオペランドについて，pdconfchk コマンドでチェックできるオペランドを次の表に示します。

表 2-2 pdconfchk コマンドでチェックできるオペランド

オペランド名	文法のチェック	ファイルのチェック	アクセス権限のチェック	重複指定のチェック	ホスト名のチェック	サーバマシン間のチェック
pd_tpyrced_key	○	×	×	×	×	○
pd_ekey	○	×	×	×	×	○

（凡例）

○：チェック対象です。

×：チェック対象外です。

文法のチェック：

オペランドの文法が正しいかチェックします。

ファイルのチェック：

システムログファイル，シンクポイントダンプファイル，およびステータスファイルの有無をチェックします。pdconfchk コマンドで-n オプションを指定した場合はファイルのチェックをしません。

アクセス権限のチェック：

HiRDB 管理者にファイルのアクセス権があるかを確認します。

UNIX 版の場合は，HiRDB 管理者に hosts ファイルのアクセス権があるかも確認します。

pdconfchk コマンドで-n オプションを指定した場合はアクセス権限のチェックをしません。

重複指定のチェック：

システムログファイル，シンクポイントダンプファイル，およびステータスファイルが重複していないかどうかをチェックします。

ホスト名のチェック：

ホスト名が hosts ファイルに記述されているかをチェックします。

サーバマシン間のチェック（HiRDB/パラレルサーバ限定）：

システムマネジャのサーバマシンを基準に，サーバマシン間の妥当性をチェックします。

3 クライアントの環境設定

この章では，暗号化機能に関連する HiRDB クライアントの環境設定について説明します。

3.1　クライアント環境定義の一覧

暗号化機能に関連するクライアント環境定義の一覧を次の表に示します。各環境変数の詳細は「クライアント環境定義の設定内容」を参照してください。

なお，ここでは，暗号化機能に関係するクライアント環境定義の説明だけを記載しています。そのほかのHiRDB クライアント環境定義の説明については，マニュアル「HiRDB Version 9 UAP 開発ガイド」の「クライアント環境定義（環境変数の設定）」を参照してください。

表 3-1　クライアント環境定義の一覧

環境変数名	機能	環境変数の分類
PDTPYRCEDKEY	復号認証キーを指定します。	特定 UAP に対する暗号化データの復号機能

3.2　クライアント環境定義の設定内容

3.2.1　暗号化機能に関連するクライアント環境定義の設定内容

(1)　PDTPYRCEDKEY=復号認証キー

～<文字列>((最大 30 バイト))

特定 UAP に対する暗号化データの復号機能を使用する場合，復号を許可するアプリケーションでは，この環境定義に復号認証キーを指定します。この環境定義を省略した場合，または復号認証キーが不一致の場合は，次の動作となります。

- 暗号化列の更新操作は，エラーになります。
- 暗号化列の検索結果は，マスクしたデータを返します。

特定 UAP に対する暗号化データの復号機能の詳細は，「特定 UAP に対する暗号化データの復号機能」を参照してください。

《留意事項》

1. 復号認証キーには，＜英数字記号＞，下線(_)およびハイフン(-)が指定できます。
2. この環境定義の設定値は，SQL トレースには出力しません。

3.3　Type4 JDBC ドライバで指定できるクライアント環境定義

JDBC ドライバで指定できるクライアント環境定義の一覧を次の表に示します。各環境変数の詳細は「クライアント環境定義の設定内容」を参照してください。

なお，ここでは，暗号化機能に関係するクライアント環境定義の説明だけを記載しています。そのほかのクライアント環境定義の説明については，マニュアル「HiRDB Version 9 UAP 開発ガイド」の「Type4 JDBC ドライバ」の「指定できるクライアント環境定義」を参照してください。

表 3-2　JDBC ドライバで指定できるクライアント環境定義の一覧

環境変数名	対応するシステムプロパティ※	機能	環境変数の分類
PDTPYRCEDKEY	HiRDB_for_Java_PDTPYRCEDKEY	復号認証キーを指定します。	特定 UAP に対する暗号化データの復号機能

注※

クライアント環境定義と同じ意味を持つ接続情報をシステムプロパティで指定できます。指定の優先順位については，マニュアル「HiRDB Version 9 UAP 開発ガイド」の「接続情報の優先順位」を参照してください。なお，内部ドライバの場合，システムプロパティの指定は無効です。

3.4　XDM/RD E2 接続機能使用時の環境変数の差異

XDM/RD E2 接続機能使用時の環境変数の差異を次の表に示します。各環境変数の詳細は「クライアント環境定義の設定内容」を参照してください。

なお，ここでは，暗号化機能に関係するクライアント環境定義の説明だけを記載しています。そのほかのクライアント環境定義の説明については，マニュアル「HiRDB Version 9 XDM/RD E2 接続機能」の「XDM/RD E2 接続機能使用時の環境変数の差異」を参照してください。

表 3-3　XDM/RD E2 接続機能使用時の環境変数の差異

環境変数	内容	Type4 JDBC ドライバ		差異の概要
		使用	不使用	
PDTPYRCEDKEY	復号認証キーを指定します。	×	×	－

（凡例）

×：

HiRDB 接続専用の環境変数です。サーバとして XDM/RD E2 を使用する場合は指定しても無視されますが，環境変数の文法チェックは行われます。

－：

特記事項はありません。

4 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。

4.1　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。

4.1.1　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 9 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〕
              〔圧縮指定〕
              〔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。
   ・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. 一時表の列には指定できません。
6. 予備列には指定できません。
7. 暗号化列の既定義型のデータ長については，「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)
```

4.1.2 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 9 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〕} 〕
        〔圧縮指定〕
```

```
        〔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. データが格納されている表の場合，切り出し列には指定できません。
3. 次のデータ型には指定できません。
   - BLOB 型
   - 抽象データ型

4.2　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。

4.2.1　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 9 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，「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。

5 コマンド

この章では，暗号化機能で使用するコマンドについて説明します。

5.1　復号認証キー情報登録ユティリティ（pdregtpyrcedkey）

5.1.1　pdregtpyrcedkey の形式と規則

(1)　機能

特定 UAP に対する暗号化データの復号機能を利用する場合に，復号を許可するための復号認証キー情報を登録・削除する機能です。

(2)　実行者

DBA 権限のあるユーザが実行できます。

(3)　形式

```
pdregtpyrcedkey　{-f 入力ファイル名 | -D}
```

(4)　引数

(a)　-f 入力ファイル名

登録または削除する復号認証キー情報を記述したファイル名を指定してください。ファイルの形式については(6)を参照してください。

(b)　-D

登録されているすべての復号認証キー情報を削除します。

(5)　規則

1. HiRDB の稼働中に実行してください。
2. 復号認証キー情報登録ユティリティは，シングルサーバまたはシステムマネジャがあるサーバマシンで実行してください。
3. 復号認証キーの登録対象の IP アドレスと認可識別子の組に対して復号認証キーがすでに登録されている場合は，復号認証キー情報を上書きします。
4. 登録されていない復号認証キーの削除を指定してもエラーにはなりません。
5. このユティリティを実行する前に，環境変数 PDUSER に DBA 権限のあるユーザの認可識別子およびパスワードを設定しておく必要があります。

(6) 入力ファイル形式

```
IPアドレス,{認可識別子 | PUBLIC},復号認証キー[,有効期限][;コメント]
   [1]              [2]          [3]        [4]       [5]
```

- 復号認証キー情報を登録したい場合は，[1]～[4]を一行で記述してください。
- 復号認証キー情報を削除したい場合は，[1][2]を一行で記述してください。
- セミコロン（;）以降，改行までに記述した文字列は，コメントと見なします。
- 行頭および行末とコンマ（,）直後の半角空白またはタブ文字の連続は，読み飛ばします。
- 復号認証キー情報を複数登録または削除したい場合は，複数行に分けて記述してください。複数行に分けて記述した場合は，ファイルの先頭から順に処理します。

[1]～[5]に記述する内容を次の表に示します。

表 5-1　入力ファイルの記述内容

番号	指定する情報	記述内容	記述形式
1	IP アドレス	登録または削除する復号認証キー情報の IP アドレスまたはネットワークアドレス	aaa.aaa.aaa.aaa[/bb]※1 • aaa ～<符号なし整数>(([[0]0]0～255)) • bb アドレスプリフィクス～<符号なし整数>((24～30))
2	認可識別子または PUBLIC※2	登録または削除する復号認証キー情報の認可識別子	マニュアル「HiRDB Version 9 SQL リファレンス」の「名前の指定」を参照してください。 ただし，ALL，HiRDB，MASTER は指定できません。
3	復号認証キー	登録する復号認証キー	次の文字から成る 30 文字以内の文字列 • 英大文字（A～Z，#，@，¥） • 英小文字（a～z） • 数字（0～9） • 下線（_） • ハイフン（-）
4	有効期限	登録する復号認証キー情報の有効期限	[YYYY-MM-DD[hh:mm:ss]]※3 • YYYY 年（0001～9999） • MM 月（01～12） • DD 日（01～該当する月の最終日） • hh

番号	指定する情報	記述内容	記述形式
			時（00～23） • mm 分（00～59） • ss 秒（00～59）
5	コメント	コメント文	改行コードを含まない任意の文字列

注※1

- IPv4（1 オクテットごとにピリオドで区切られた 10 進数）で記述してください。aaa の上位の無効数字 0 は除いてディクショナリ表に登録します。
- ネットワーク内の IP アドレスを一括して登録する場合は，bb にネットワーク部のビット数を指定し，aaa.aaa.aaa.aaa にネットワークアドレスを指定してください。ディクショナリ表には，指定したネットワーク中の IP アドレスごとに登録されます。ただし，ネットワークアドレスとブロードキャストアドレスは登録されません。IP アドレスの一括登録処理中にエラーが発生した場合は，一括登録前の状態に戻ります。

注※2

- すべての実行ユーザに対する復号認証キーを登録する場合は，PUBLIC を指定してください。
- CONNECT 権限のないユーザの認可識別子も登録できます。
- PUBLIC を指定して登録した復号認証キー情報を削除する場合は，PUBLIC を指定して削除してください。

注※3

hh:mm:ss を省略した場合は，23:59:59 を仮定します。有効期限を省略した場合は，無期限になります。

(7) 注意事項

1. 復号認証キー情報登録ユティリティのリターンコードを次に示します。

   0：正常終了

   4：正常終了（一部の登録・削除処理に失敗）

   8：異常終了

2. 復号認証キー情報登録ユティリティと PURGE TABLE 文を同時に実行した場合，排他の競合によって，どちらかが待ち状態になることがあります。これらの操作を同時に実行しないようにしてください。なお，検査保留状態を使用しない場合は，排他の競合は発生しません。検査保留状態を使用するかどうかは，HiRDB システム定義 pd_check_pending オペランドに指定します。詳細は，マニュアル「HiRDB Version 9 システム定義」のオペランドの説明を参照してください。

5.2　暗号鍵ファイル作成コマンド（pdmkekey）

5.2.1　pdmkekey の形式と規則

(1)　機能

暗号化 HiRDB ファイルシステム領域で使用する暗号鍵ファイルを作成します。

(2)　実行者

HiRDB 管理者が実行できます。

(3)　形式

```
pdmkekey 出力ファイル名
```

(4)　引数

(a)　出力ファイル名

作成する暗号鍵ファイル名を記述します。UNIX 版の場合，暗号鍵ファイルは 0600 のパーミッションで作成します。すでにファイルがある場合は，コマンドがエラーになります。

(5)　注意事項

1. 暗号鍵ファイル作成コマンドのリターンコードを次に示します。
   0：正常終了
   8：異常終了
2. HiRDB/パラレルサーバの場合，暗号鍵ファイル作成コマンドは各ユニットで実行できますが，次に示す機能を使用するときは，複数のユニットで同一の HiRDB ファイルシステム領域を参照します。そのため，1 つのユニットで作成した暗号鍵ファイルをそれぞれのユニットに配布してください。
3. 各機能との関係を次に示します。
   - 系切り替え機能
     ・スタンバイレス型系切り替え構成の場合
     現用系と予備系のユニットで同一の暗号鍵ファイルを使用します。
     ・1:1 スタンバイレス型系切り替え構成の場合
     正規 BES のユニットと代替 BES のユニットで同一の暗号鍵ファイルを使用します。
     ・影響分散スタンバイレス型系切り替えの場合
     同一の HA グループ内のユニットで同一の暗号鍵ファイルを使用します。

- 共用 RD エリア
  全 BES のユニットで同一の暗号鍵ファイルを使用します。
- ディザスタリカバリ機能
  メインサイトとリモートサイトで同一の暗号鍵ファイルを使用します。

5.3　暗号鍵ファイル変更コマンド（pdchekey）

5.3.1　pdchekey の形式と規則

(1)　機能

暗号化 HiRDB ファイルシステム領域で使用する暗号鍵ファイルを変更します。

(2)　実行者

HiRDB 管理者が実行できます。

(3)　形式

```
  pdchekey -p 旧暗号鍵ファイル名 -n 新暗号鍵ファイル名　{-f 入力ファイル名 | HiRDBファイルシステム領域名}
```

(4)　引数

(a)　-p 旧暗号鍵ファイル名

変更前の暗号鍵ファイルの名称を指定します。

(b)　-n 新暗号鍵ファイル名

変更後の暗号鍵ファイルの名称を指定します。

(c)　-f 入力ファイル名

暗号化 HiRDB ファイルシステム領域の名称リストを記述したファイルを指定します。

暗号化 HiRDB ファイルシステム領域の名称リストは 1 行に 1 つの HiRDB ファイルシステム領域のパス名を記述します。

(d)　HiRDB ファイルシステム領域名

暗号化 HiRDB ファイルシステム領域のパス名を指定します。直接指定できる HiRDB ファイルシステム領域のパス名は 1 つだけで，複数の HiRDB ファイルシステム領域のパス名を指定する場合は入力ファイルを使用してください。

(5) 規則

1. HiRDB が停止しているときに実行してください。HiRDB が起動しているときに実行した場合，暗号化 HiRDB ファイルシステム領域中の HiRDB ファイルにアクセスするサーバプロセスがアクセス時にエラーになり，RD エリアが障害閉塞することがあります。
2. 暗号鍵ファイル変更コマンドを実行中に，「付録 D.8 暗号鍵ファイルが必要なコマンド」に示すコマンドを同時に実行しないでください。

(6) 注意事項

1. 暗号鍵ファイル変更コマンドは，ユニット内のすべての暗号化 HiRDB ファイルシステム領域に対して実行してください。実行が漏れた暗号化 HiRDB ファイルシステム領域内の HiRDB ファイルは参照できなくなります。
2. pdfbkup コマンドでバックアップを取得した後に暗号鍵ファイルを変更した場合，バックアップファイル内のデータを参照するには古い暗号鍵ファイルが必要です。バックアップから戻す場合は，戻した後に暗号鍵ファイル変更コマンドで新しい暗号鍵に変更する必要があります。このため，暗号化 HiRDB ファイルシステム領域の HiRDB ファイルを pdfbkup コマンドでバックアップを取得する場合は，暗号鍵との対応を管理してください。
3. 暗号鍵ファイル変更コマンドのリターンコードを次に示します。

   0：正常終了

   8：異常終了

5.4　pdfmkfs（HiRDB ファイルシステム領域の初期設定）

5.4.1　pdfmkfs の形式と規則

暗号化 HiRDB ファイルシステム領域を使用するためのオプション（-E）について説明します。-E オプション以外の内容については，マニュアル「HiRDB Version 9 コマンドリファレンス」を参照してください。

(1)　形式

(a)　UNIX 版のキャラクタ型スペシャルファイルの場合

```
pdfmkfs -n HiRDBファイルシステム領域サイズ 〔-l 最大ファイル数〕
        〔-k 使用目的〕 〔-e 最大増分回数〕 〔-s セクタ長〕 〔-i〕 〔-a〕 〔-E〕
         キャラクタ型スペシャルファイル名
```

(b)　UNIX 版の通常ファイルの場合

```
pdfmkfs -n HiRDBファイルシステム領域サイズ 〔-l 最大ファイル数〕
        〔-k 使用目的〕 〔-e 最大増分回数〕 〔-i〕 〔-r〕 〔-a〕 〔-E〕
          通常ファイル名
```

(c)　Windows 版の場合

```
pdfmkfs -n HiRDBファイルシステム領域サイズ 〔-l 最大ファイル数〕
        〔-k 使用目的〕 〔-e 最大増分回数〕 〔-s セクタ長〕 〔-i〕 〔-r〕 〔-a〕 〔-E〕
          ファイル名
```

(2)　オプション

(a)　-E

HiRDB ファイルシステム領域内に作成する HiRDB ファイルのレコード（ページ）を暗号化する場合に指定します。

(3)　注意事項

1. UNIX 版で-E オプションを指定し，通常ファイルに新規に作成した場合，HiRDB ファイルシステム領域のパーミッションは 0600 になります。この HiRDB ファイルシステム領域に pdfls コマンドおよび

pdfstatfs コマンドを実行する場合は，HiRDB 管理者で実行する必要があります。指定した通常ファイルがすでにある場合，およびキャラクタ型スペシャルファイルに作成する場合は，パーミッションは変わりません。

5.5　pdfstatfs（HiRDB ファイルシステムの内容表示）

5.5.1　pdfstatfs の形式と規則

出力形式の HiRDB ファイルシステム領域の暗号化指定の表示について説明します。これ以外の内容については，マニュアル「HiRDB Version 9 コマンドリファレンス」を参照してください。

(1)　出力形式

(a)　-x 及び-y オプション省略時

```
 user area capacity         aa...a[kB]
 remain user area capacity  bb...b[kB]
[peak capacity              mm...m[kB]]
 available file size        cc...c[kB]
 available file count       dd...d
 current file count         ee...e
 remain file count          ff...f
 free area count            gg...g
 available expand count     hh...h
 current expand count       ii...i
[sector size                qq...q[Byte]]
 initialize area kind       jj...j
 initialize user id         kk...k
 initialize time            ll...l
 area auto expand           rr...r
[peak file count            ss...s]
[peak expand count          tt...t]
[limit expand count         uu...u]
[clear option               v]
[file system type           www]
[area encryption            xx...x]

[***** HiRDB file system area space information *****]
[offset[kB]     size[kB]  used/unused]
[  nn...n       oo...o      pp...p]
```

[説明]

xx...x：

pdfmkfs -E を指定し，「暗号化 HiRDB ファイルシステム領域」の機能を適用しているかを示します。

USE：適用

NOUSE：非適用

-A オプションを指定したときだけ表示されます。

(b) DAT 形式での出力形式（-x 及び-y オプション指定時）

```
”USER_AREA_CAPACITY”,”REMAIN_USER_AREA_CAPACITY”,”PEAK_CAPACITY”,
”AVAILABLE_FILE_SIZE”,”AVAILABLE_FILE_COUNT”,”CURRENT_FILE_COUNT”,
”REMAIN_FILE_COUNT”,”FREE_AREA_COUNT”,”AVAILABLE_EXPAND_COUNT”,
”CURRENT_EXPAND_COUNT”,”SECTOR_SIZE”,”INITIALIZE_AREA_KIND”,
”INITIALIZE_USER_ID”,”INITIALIZE_TIME”,”AREA_AUTO_EXPAND”,
”PEAK_FILE_COUNT”,”PEAK_EXPAND_COUNT”,”LIMIT_EXPAND_COUNT”,
”CLEAR_OPTION”,”FILE_SYSTEM_TYPE”,”AREA_ENCRYPTION” [CR]
aa...a,bb...b,mm...m,
cc...c,dd...d,ee...e,
ff...f,gg...g,hh...h,
ii...i,qq...q,”jj...j”,
”kk...k”,”ll...l”,”rr...r”,
ss...s,tt...t,uu...u,
”v”,”www”,”xx...x” [CR]
```

5.6　pdls【-d mem】（サーバの共用メモリの状態表示）

5.6.1　pdls【-d mem】の形式と規則

システム定義の pd_ekey オペランドを指定した場合の pdls -d mem コマンドの表示内容について説明します。これ以外の内容については，マニュアル「HiRDB Version 9 コマンドリファレンス」を参照してください。

(1)　出力形式

(a)　HP-UX，及び Linux，Windows の場合

```
HOSTNAME : aa...a(bbccdd)
SHM-ID  GET-SIZE  ACT-SIZE SHM-OWNER          POOL-ID
ee...e    ff...f    gg...g    hh...h           ii...i
   :         :         :         :               :
```

(b)　AIX（64 ビットモード）の場合

```
HOSTNAME : aa...a(bbccdd)
    SHM-ID             GET-SIZE      ACT-SIZE SHM-OWNER     POOL-ID
    ee...e               ff...f        gg...g    hh...h      ii...i
       :                    :             :         :           :
```

[説明]

hh...h ：

共用メモリを使用するプロセスの属性（8 文字以内）

共用メモリの種類	hh...h の内容
HiRDB ファイル管理用共用メモリ	IOS

ii...i ：

プール識別子（16 文字以内）

共用メモリの種類	ii...i の内容
HiRDB ファイル管理用共用メモリ	表示されません。

(2)　注意事項

1. システム定義 pd_ekey オペランドを指定している場合，pdls -d mem コマンドは HiRDB 管理者で実行してください。HiRDB 管理者以外で実行すると，コマンドがエラーになります。

6 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。

6.1　暗号化表の再編成

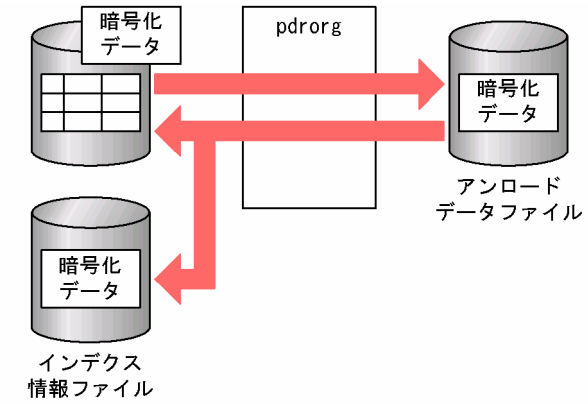
暗号化表に対して pdrorg を実行する場合の運用方法について説明します。

pdrorg での再編成については，マニュアル「HiRDB Version 9 システム運用ガイド」，およびマニュアル「HiRDB Version 9 コマンドリファレンス」を参照してください。

6.1.1　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 6-1　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。

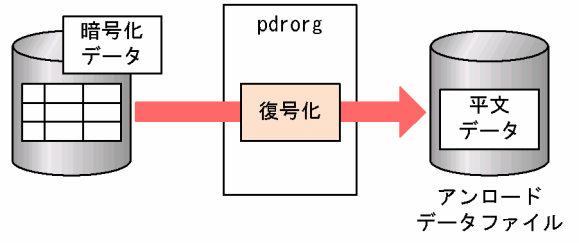
(2)　制限がある機能

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。

6.1.2　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 6-2　暗号化表のアンロードの概要



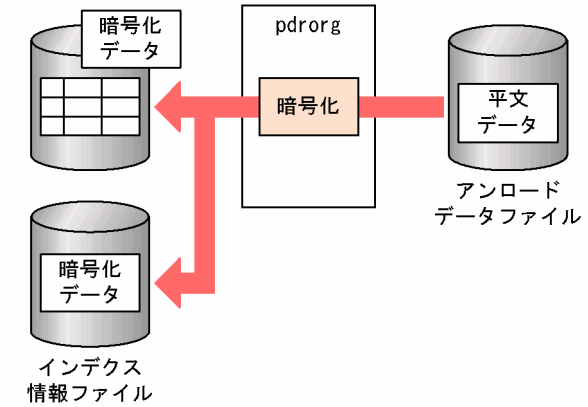
注意事項

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。

6.1.3　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 6-3　暗号化表のリロードの概要



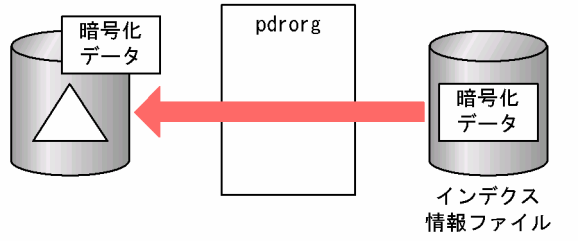
注意事項

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。

6.1.4　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。

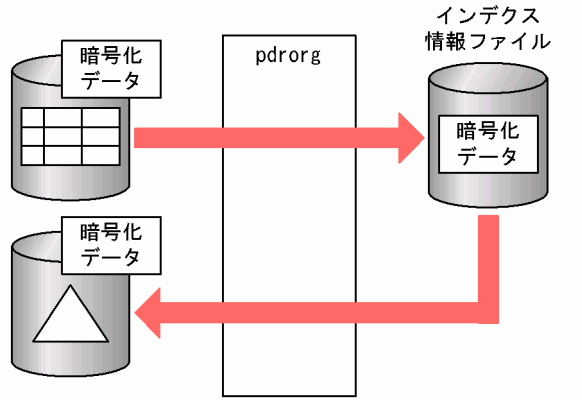
図 6-4　インデクス構成列に暗号化列を含むインデクスの一括作成の概要



6.1.5　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。

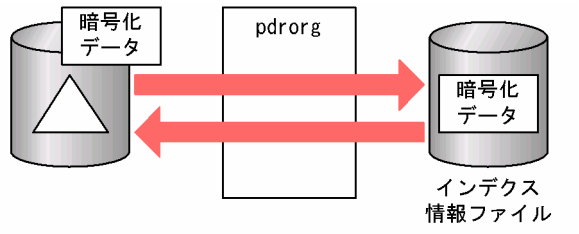
図 6-5　インデクス構成列に暗号化列を含むインデクスの再作成の概要



6.1.6　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 6-6　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



6.1.7　ディクショナリ表の再編成

暗号化機能を使用する場合は，ディクショナリ表が追加になります。ディクショナリ表の表識別子を指定してディクショナリ表の再編成を実行する場合に，追加になるディクショナリ表の表識別子について，次の表に示します。ディクショナリ表の再編成で指定する表識別子については，マニュアル「HiRDB Version 9 コマンドリファレンス」にある「データベース再編成ユティリティ（pdrorg）」の-t オプションの説明を参照してください。

表 6-1　ディクショナリ表の再編成で指定するディクショナリ表の表識別子

表識別子	備考
SQL_TPYRCEDKEY	なし

6.2　暗号化表の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 9 システム運用ガイド」，およびマニュアル「HiRDB Version 9 コマンドリファレンス」を参照してください。

6.2.1　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。

6.2.2　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。

6.3　暗号化表の運用時の注意事項

6.3.1　暗号化したデータベースを運用するときの注意事項

(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 9 コマンドリファレンス」を参照してください。

表 6-2　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 9 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 9 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 Server with Additional Function 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。

(5) 更新可能なオンライン再編成を実行したときに暗号化されないファイル

暗号化したデータベースに対して，更新可能なオンライン再編成を実行する場合，次に示すファイルに出力されるデータは暗号化されません。

- スキップ情報出力ファイル
- SQL トレース情報ファイル

スキップ情報出力ファイル，および SQL トレース情報ファイルについては，マニュアル「HiRDB Version 9 コマンドリファレンス」を参照してください。

6.4　暗号化表の制限される機能

暗号化表の場合に制限される機能を次に示します。

- データ連動（Version 8 08-05 より前の 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※

暗号化列が次のどれかに該当する場合，暗号化列の追加はできません。

- BLOB，または抽象データ型の列
- 繰返し列
- 予備列
- 切り出し列（表にデータが格納されている場合）

6.5　暗号化 HiRDB ファイルシステム領域の運用

暗号化 HiRDB ファイルシステム領域の運用について説明します。

6.5.1　使用方法

暗号化 HiRDB ファイルシステム領域の使用方法について説明します。

(1)　暗号鍵ファイル

暗号化 HiRDB ファイルシステム領域を使用するには，暗号鍵ファイルが必要になります。暗号鍵ファイルは暗号鍵ファイル作成コマンド（pdmkekey）で作成します。HiRDB/パラレルサーバの場合，暗号化 HiRDB ファイルシステム領域を使用するすべてのユニットで暗号鍵ファイルが必要になります。ユニット間で異なる暗号鍵ファイルを使用することもできますが，次の機能を使用する場合，複数のユニット間で同一の暗号化 HiRDB ファイルを使用するため，同一の暗号鍵ファイルを各ユニットに配置してください。

(a)　系切り替え機能

■ スタンバイレス型系切り替え構成の場合

現用系と予備系のユニットに同一の暗号鍵ファイルを配置します。

■ 1:1 スタンバイレス型系切り替え構成の場合

正規 BES のユニットと代替 BES のユニットに同一の暗号鍵ファイルを配置します。

■ 影響分散スタンバイレス型系切り替えの場合

同一の HA グループ内のユニットに同一の暗号鍵ファイルを配置します。

(b)　共用 RD エリア機能

すべての BES のユニットに同一の暗号鍵ファイルを配置します。

(c)　ディザスタリカバリ機能

メインサイトとリモートサイトに同一の暗号鍵ファイルを配置します。

(2)　システム定義

システム共通定義，またはユニット制御情報定義の pd_ekey に暗号鍵ファイルのパス名を指定します。パラレルサーバの場合は，暗号化 HiRDB ファイルシステム領域を使用するすべてのユニットで指定します。システム共通定義に指定する場合，暗号化 HiRDB ファイルシステム領域を使用しないユニットにも暗号鍵ファイルが必要になります。

(3) 暗号化 HiRDB ファイルシステム領域の作成

暗号化 HiRDB ファイルシステム領域は，pdfmkfs コマンドに暗号化指定（-E）で作成します。

(4) 初期構築時に暗号化 HiRDB ファイルシステム領域を使用する方法

初期構築時に暗号化 HiRDB ファイルシステム領域を作成する場合は，次の手順で作成します。

1. pdmkekey で暗号鍵ファイルを作成します。HiRDB/パラレルサーバの場合，必要なそれぞれのユニットで暗号鍵ファイルを作成するか，1 つのユニットで作成した暗号鍵ファイルを必要なユニットに配布します。
2. 暗号化する HiRDB ファイルシステム領域を，pdfmkfs コマンド（-E 指定）で作成します。
3. システム定義 pd_ekey に暗号鍵ファイルのパス名を指定します。
4. pdloginit および pdstsinit でシステムファイルを作成します。
5. pdstart で HiRDB を開始します。
6. pdinit で RD エリアを作成します。

(5) 構築後に暗号化 HiRDB ファイルシステム領域を使用する方法

1. HiRDB を停止※1 します。
2. pdmkekey で暗号鍵ファイルを作成します。HiRDB/パラレルサーバの場合，必要なそれぞれのユニットで暗号鍵ファイルを作成するか，1 つのユニットで作成した暗号鍵ファイルを必要なユニットに配布します。
3. 暗号化する HiRDB ファイルシステム領域を，pdfmkfs コマンド（-E 指定）で作成します。
4. システム定義 pd_ekey に暗号鍵ファイルのパス名を指定します。
5. システムファイルを暗号化する場合，pdloginit や pdstsinit でシステムファイルを作成し直します。※2
6. HiRDB を開始します。
7. pdmod で暗号化 HiRDB ファイルシステム領域に RD エリアを作成します。

注※1

システムファイルを暗号化 HiRDB ファイルシステム領域に作成し直す場合，必ず正常停止してください。

注※2

HiRDB Datareplicator を使用している場合，システムログファイルやステータスファイルを作成し直す前に HiRDB Datareplicator の初期化が必要になります。

(6) HiRDB 開始時

HiRDB を開始するとき（pdstart を実行するとき）は作成済みの暗号鍵ファイルを pd_ekey のパスに配置してから開始してください。

(7) 系切り替え構成

(a) スタンバイ型系切り替え（モニタモード）の場合

スタンバイ型系切り替え（モニタモード）は系が切り替わるときに pdstart が実行されるため，待機系のユニットに暗号鍵ファイルを配置しておく必要があります。

(b) スタンバイ型系切り替え（モニタモード）以外の場合

スタンバイ型系切り替え（モニタモード）以外の場合は，待機系を起動するときの pdstart 実行時に暗号鍵ファイルが必要になります。

6.5.2 バックアップ・アンロードログファイルの取得

次に示すファイルは，通常ファイルに出力すると，内容が平文で出力されます。

- pdcopy のバックアップファイル
- pdrorg のアンロードデータファイル
- pdlogunld のアンロードログファイル

これらのファイルを暗号化する場合，使用目的に UTL を指定した暗号化 HiRDB ファイルシステム領域に出力することで内容を暗号化し，ファイルの直接参照による情報漏えいのリスクを低減できます。

6.5.3 非暗号化 HiRDB ファイルシステム領域と暗号化 HiRDB ファイルシステム領域との変換

非暗号化 HiRDB ファイルシステム領域のファイルを暗号化する場合は次の手順で実施してください。暗号鍵ファイルの作成，システム定義の設定は別途実施し，HiRDB を起動してください。

(1) RD エリアの場合

(a) pdcopy を使用する場合

1. pdcopy で暗号化する RD エリアのバックアップを取得します。
2. pdfmkfs に-E を指定し，HiRDB ファイルシステム領域を作成し直します。
3. pdrstr で 1 のバックアップから RD エリアを回復します。

(b) pdrorg を使用する場合

1. pdrorg -k unld で暗号化する RD エリアのアンロードデータを取得します。
2. pdfmkfs に-E を指定し，HiRDB ファイルシステム領域を作成し直します。
3. pdmod の initialize rdarea 文で RD エリアを再初期化します。
4. pdrorg -k reld で 1 のアンロードデータを RD エリアに戻します。

(2) システムファイルの場合

1. HiRDB を正常停止します。
2. pdfmkfs に-E を指定し，HiRDB ファイルシステム領域を作成し直します。
3. pdloginit および pdstsinit でシステムファイルを作成し直します。
4. HiRDB を開始します。

HiRDB Datareplicator を使用している場合，システムログファイルおよびステータスファイルを作成し直す前に HiRDB Datareplicator の初期化が必要になります。

暗号化 HiRDB ファイルシステム領域から非暗号化 HiRDB ファイルシステム領域に変換する場合，上記と同様の手順で pdfmkfs に-E を指定しないで HiRDB ファイルシステム領域を作成することで実施できます。

6.5.4 暗号鍵ファイルの変更

暗号鍵ファイルは変更できます。暗号鍵ファイルの変更は暗号鍵ファイル変更コマンド（pdchekey）で実施します。パラレルサーバの場合，それぞれのユニットで実施します。変更は次の手順で実施します。

1. HiRDB を停止します。
2. pdmkekey で新しい暗号鍵ファイルを作成します。変更前の暗号鍵ファイルは 3 で使用するため，削除しないでください。
3. 次のコマンドで暗号鍵ファイルを変更します。入力ファイルにはそのユニットの暗号化 HiRDB ファイルシステム領域のリストを記述します。

```
pdchekey -p 旧暗号鍵ファイル -n 新暗号鍵ファイル -f 入力ファイル
```

4. システム定義 pd_ekey のファイルを新しい暗号鍵ファイルに置き換えます。
5. HiRDB を起動します。

<注意事項>

・3.の入力ファイルのリストに漏れがあると，未変更の HiRDB ファイルの操作でエラーになります。その場合は HiRDB を停止し，エラーになった未変更の HiRDB ファイルシステム領域に対して，再度 pdchekey を実施してください。

・pdchekey 実行前に pdfbkup で取得したバックアップファイルは古い暗号鍵で暗号化されています。このバックアップファイルから pdfrstr でリストアする場合，pdfrstr 実施後に pdfbkup 取得時の暗号鍵ファイルと現在の暗号鍵ファイルを使用し，pdchekey で暗号鍵ファイルを変更する必要があります。

7 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。

7.1　表定義

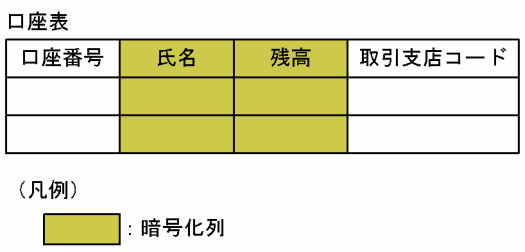
暗号化表は CREATE TABLE で定義します。

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 7-1　定義される暗号化表



7.2　データの格納

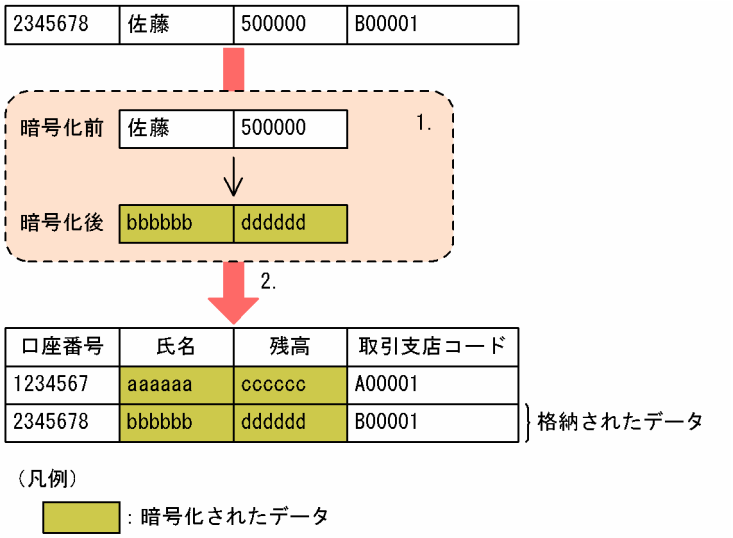
暗号化表へのデータの格納は，INSERT 文で行います。データの格納は pdload でも実行できますが，ここでは INSERT 文について説明します。

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 7-2　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。

7.3　データの検索

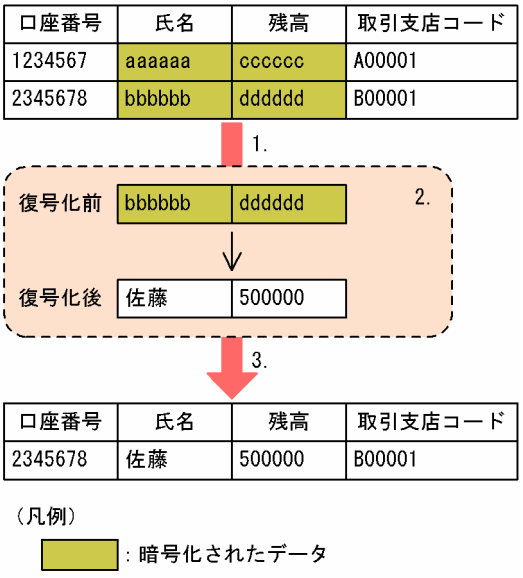
暗号化表のデータの検索は，SELECT 文で行います。

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 7-3　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。

8 HiRDB のメモリ所要量

この章では，暗号化機能を使用する場合に変更が必要になる HiRDB のメモリ所要量の見積もりについて説明します。

8.1　メモリ所要量の計算式

次の機能を使用する場合は，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「メモリ所要量の計算式」が変更になります。

8.1.1　メモリ所要量の計算式の詳細

(1)　特定 UAP に対する暗号化データの復号機能

特定 UAP に対する暗号化データの復号機能を使用する場合は，セキュリティ監査情報用バッファ用共用メモリの計算式に，復号認証キー情報用バッファのサイズを加算します。復号認証キー情報用バッファサイズの計算式を次に示します。なお，セキュリティ監査情報用バッファ用共用メモリはシングルサーバとフロントエンドサーバで使用します。

復号認証キー情報用バッファサイズの計算式

```
↑0.1＋MAX｛(key＋10000)，(key×1.2)｝×0.1↑
```

key：復号認証キー情報の数（ディクショナリ表 SQL_TPYRCEDKEY の行数）

(2)　暗号化 HiRDB ファイルシステム領域

(a)　プロセス固有領域

暗号化 HiRDB ファイルシステム領域の機能を使用する場合，暗号化 HiRDB ファイルシステム領域にアクセスプロセスでプロセス固有領域のメモリ使用量が増加します。次の値を加算してください。

HiRDB/パラレルサーバで，ユニット内に複数のサーバ（システムマネジャを除きます）がある場合は，サーバごとに計算してください。

- ユニットコントローラ全プロセスが使用するプロセス固有領域
  1024 キロバイト
- サーバプロセスが使用するプロセス固有領域
  (a ＋ b ＋ 4)×(512 ＋ c) (単位：キロバイト)

  a：
  pd_max_server_process の値

  b：
  pd_dfw_awt_process の値。定義を省略している場合は 1

  c：
  pd_log_dual_write_method に parallel を指定している場合：1024
  pd_log_dual_write_method に parallel を指定していない場合：0

(b) 共用メモリ

暗号化 HiRDB ファイルシステム領域の機能を使用する場合，共用メモリの使用量が 4096 バイト増加します。HiRDB/パラレルサーバの場合，ユニットごとに 4096 バイト加算してください。

8.2　SQL 実行時に必要なメモリ所要量の計算式

マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「SQL 実行時に必要なメモリ所要量の計算式」が変更になります。

8.2.1　暗号化表に対して操作系 SQL を実行する場合に必要なメモリ所要量の求め方

暗号化表に対して操作系 SQL を実行する場合に必要なメモリ所要量は，次に示す計算式で求めます。

計算式

```
共通部＋データ部＋インデクス情報部（単位：バイト）
```

(1)　共通部の求め方

共通部の求め方を次に示します。

計算式

```
●FIX指定のない表の場合
A＋8×a
●FIX指定の表の場合
A＋16×b
（単位：バイト）
```

A：64 ビットの場合 188，32 ビットの場合 146（バイト）

a：更新対象列数または検索対象列数（個）

b：表の構成列数（個）

(2)　データ部

データ部の求め方を次に示します。

計算式

```
●FIX指定のない表の場合（fi対象は暗号化列だけ）
          c
B×a＋Σ(fi＋Di)＋BIN
         i=1
●FIX指定の表の場合（UPDATEの場合は全構成列を更新する場合）
          a
B×b＋Σfi
         i=1
●FIX指定の表UPDATEで一部の列を更新する場合（fi対象は暗号化列だけ）
          c
B×b＋Σfi
```

i=1
（単位：バイト）

B：64 ビットの場合 20，32 ビットの場合 16（バイト）

D：NOT NULL 指定の場合 0，NOT NULL 指定でない場合 2（バイト）

a：更新対象列数または検索対象列数（個）

b：表の構成列数（個）

c：暗号化指定の列数（個）

f：RD エリア格納データ長（バイト）

分岐する場合は分岐データ長で算出してください。定義長 32001 以上の暗号化指定の BINARY 型の列，および定義長 256 以上の暗号化指定かつ圧縮指定の BINARY 型の列の場合 0 で計算します。

BIN：BINARY 用暗号化データ操作領域サイズ（バイト）

表に BINARY 型の列を定義している場合，BIN を次に示す表で求めます。該当する列が複数ある場合でも，一度だけ BIN を加算します。圧縮指定，または暗号化指定かつ圧縮指定の BINARY 型の列がある場合，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の次の個所を参照し，圧縮列用の領域サイズを求めてください。

- SQL 実行時に必要なメモリ所要量の計算式
- 圧縮列に対して操作系 SQL を実行する場合に必要なメモリ所要量の求め方

表 8–1　BIN の計算式

定義長 32001 以上の暗号化指定だけの BINARY 型の列	暗号化指定かつ圧縮指定の BINARY 型の列	圧縮指定だけの BINARY 型の列	BIN（バイト）
あり	あり	あり	G＋8
		なし	G×(E＋1)＋F＋8
	なし	あり	0
		なし	32000×E＋F
なし	あり	あり	G＋8
		なし	G×(E＋1)＋F＋8
	なし	あり	0
		なし	0

E：次に示すどれかの条件に該当する場合 2，該当しない場合 1

・SUBSTR 関数を使用している

・POSITION 関数を使用している

・後方削除更新をしている

F：SQL の実行対象となる圧縮表が格納されている RD エリアのページ長（バイト）

複数の RD エリアが対象になる場合は，最大のページ長で計算します。

G：最大の圧縮分割サイズまたは最大の定義長のどちらか小さい方のサイズ（バイト）

(3) インデクス情報部

インデクスを使用した検索および，インデクスを更新する場合，インデクス情報部を次に示す計算式で求めます。

計算式

```
8×(d＋e)
（単位：バイト）
```

d：操作対象インデクス数（個）

e：操作対象インデクスの構成列数の合計（個）

9 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。

9.1　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 9 システム導入・設計ガイド」を参照してください。

9.1.1　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「可変長文字列型のデータ長一覧」にあるデータ型の列についてだけ求めてください。

表 9-1　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		−

分類	データ型および条件				データ長（単位：バイト）
			上記以外		↑(2d + 1)÷16↑×16 + 3
		d≧128			6
	NVARCHAR(n) ノースプリットオプション指定あり	n≦127	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
		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)	n≦255			↑(d + 1)÷16↑×16 + 5
		n≧256	分岐する場合※		15

分類	データ型および条件			データ長（単位：バイト）
			分岐しない場合	↑(d + 1)÷16↑×16 + 9
	BINARY(n) 圧縮指定あり	n≧256	分岐する場合※	15
			分岐しない場合	↑(d + 1)÷16↑×16 + 17

（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。

注※

マニュアル「HiRDB Version 9 システム導入・設計ガイド」にある「表の格納ページ数の計算方法」の「計算式中で使用する変数」に記載されている SPN2 を求めるとき，Li を次の値で計算してください。

・定義長 32000 以下の場合

$Li = \uparrow(d + 1)\div 16\uparrow \times 16 + 8 + \alpha$

・定義長 32001 以上の場合かつ圧縮指定がない場合

$Li = d + \uparrow d \div \gamma \uparrow \times (9 + \alpha) + 16$

・定義長 32001 以上の場合かつ圧縮指定がある場合

$Li = \downarrow d \div \gamma \downarrow \times (\uparrow(\gamma + 9)\div 16\uparrow \times 16 + 8) + \mathrm{mod}(d, \gamma) + 32$

α：圧縮指定がある場合は 8，ない場合は 0

γ：圧縮指定がある場合は↓(圧縮分割サイズ)÷16↓×16－1，ない場合は 31999

表 9-2　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）

9.1.2　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 9-3　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
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。

9.2　データディクショナリ用 RD エリアの容量の見積もり

ここでは，暗号化機能を使用する場合に追加されるディクショナリ表の容量見積もりについて説明します。

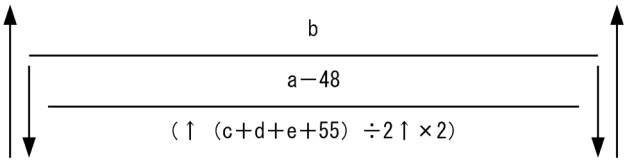
データディクショナリ用 RD エリアの容量見積もりについては，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「通常のデータディクショナリ用 RD エリアの容量の見積もり」を参照してください。

9.2.1　表の格納ページ数の計算方法

次の機能を使用する場合は，マニュアル「HiRDB Version 9 システム導入・設計ガイド」にある「通常のデータディクショナリ用 RD エリアの容量の見積もり」の「表の格納ページ数の計算方法」で求めたページ数に，該当する計算式の値を加算してください。

(1)　特定 UAP に対する暗号化データの復号機能

(a)　計算式 1

ディクショナリ表名	計算式
SQL_TPYRCEDKEY	 b a−48 （↑（c+d+e+55）÷2↑×2）

a：次に示すどちらかを代入します。

- pd_dbreuse_remaining_entries オペランドの指定値が ONLY_USER または NOTHING の場合
  データディクショナリ用 RD エリアのページ長−510（バイト）
- pd_dbreuse_remaining_entries オペランドの指定値が上記以外の場合
  データディクショナリ用 RD エリアのページ長（バイト）

b：復号認証キー情報の総数（個）

c：IP アドレスの長さの平均値（バイト）

d：認可識別子の長さの平均値（バイト）

e：復号認証キーの長さの平均値（バイト）

9.2.2　インデクスの格納ページ数の計算方法

次の機能を使用する場合は，マニュアル「HiRDB Version 9 システム導入・設計ガイド」にある「通常のデータディクショナリ用 RD エリアの容量の見積もり」の「インデクスの格納ページ数の計算方法」で求めたページ数に，該当するディクショナリ表のインデクス格納ページ数も加算してください。

(1)　特定 UAP に対する暗号化データの復号機能

インデクスの格納ページ数を求める計算式に代入する変数一覧を次の表に示します。

表 9-4　インデクスの格納ページ数を求める計算式に代入する変数一覧

表名	種別	キー長※2 (変数 g ※1)	キーの種類の個数 (変数 c ※1)	キーの重複数の平均値 (変数 d ※1)
SQL_TPYRCEDKEY	148	d + 7	復号認証キー情報数	1

d：認可識別子の長さの平均値（バイト）

注※1

マニュアル「HiRDB Version 9 システム導入・設計ガイド」にある「インデクスの格納ページ数の計算方法」の「計算式中で使用する変数」に記載されている変数のことです。

注※2

キー長は 4 バイト単位で切り上げになります。次に示す計算式で求めてください。

↑キー長÷4↑×4

10 リソース数に関連する環境変数の見積もり

この章では，Windows 版 HiRDB で暗号化機能を使用する場合に変更が必要になる HiRDB のリソース数に関連する環境変数の見積もりについて説明します。

10.1　見積もり式

10.1.1　見積もり式の詳細

次の機能を使用する場合は，マニュアル「HiRDB Version 9 システム導入・設計ガイド」の「見積もり式」が変更になります。

(1)　暗号化 HiRDB ファイルシステム領域

暗号化 HiRDB ファイルシステム領域の機能を使用する場合，共用メモリ使用数（PDUXPLSHMMAX）の計算式が変更になります。

●HiRDB/シングルサーバの場合

Max(4096，(5 ＋ h)×(e ＋ 50))

e：pd_max_server_process オペランドの値

h：↑(グローバルバッファが使用する共用メモリの総量※÷SHMMAX の値)↑

●HiRDB/パラレルサーバの場合

Max(4096，(5 ＋ z)×(g ＋ 50))

g：pd_max_server_process オペランドの値

z：↑(ユニット内のグローバルバッファが使用する共用メモリの総量※÷SHMMAX の値)↑

注※

グローバルバッファが使用する共用メモリについては，マニュアル「HiRDB Version 9 システム導入・設計ガイド」を参照してください。

11 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。

11.1　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 9 メッセージ」を参照してください。

KFPA11552-E

Unable to execute "aa....aa" due to lack of privilege　（A）

DBA 権限がないため，"aa....aa"に表示したユティリティを実行できません。

または，DBA 権限保持者のパスワードを HiRDB に登録していないため，"aa....aa"に表示したユティリティを実行できません。

aa....aa：実行できないユティリティ

- pdregtpyrcedkey

(S)処理を終了します。

(P)DBA 権限を取得してからこのユティリティを実行してください。または，DBA 権限保持者のパスワードを HiRDB に登録してから，このユティリティを実行してください。

KFPA11613-E

Unable to aa....aa for not empty table　（A）

データが格納されている表に対して，aa....aa に示す操作はできません。

aa....aa：誤った指定

add encrypted column into reserved column：予備列からの切り出しによる暗号化列の追加

(S)その SQL 文を無視します。

(P)データが格納されていない表に対して再度実行してください。または，PURGE TABLE 文で表中のすべてのデータを削除して，再度実行してください。なお，PURGE TABLE 文を実行するときは，障害に備えあらかじめバックアップを取得してください。

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 Server with Additional Function でないサーバが混在している状態で HiRDB Server with Additional Function の機能を使用している。

aa....aa：HiRDB Server with Additional Function でないサーバ名

(S)この SQL 文を無視します。

[対策]HiRDB Server with Additional Function の機能を使用する場合は，すべてのユニットで HiRDB Server with Additional Function 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。

KFPA19621-E

Unable to CREATE aa....aa TEMPORARY TABLE due to bb....bb, code=cc　（A）

bb....bb のため，一時表を定義できません。

aa....aa：GLOBAL

bb....bb：エラーに対する付加情報

cc：理由コード

(S)この SQL 文を無視します。

(P)理由コードおよびエラーに対する付加情報について次に示します。エラーの要因を取り除いて，SQL 文を修正し再度実行してください。

理由コード	エラーに対する付加情報	意味
02	encrypted table	暗号化表として定義しています。

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もしくは変更ができません。

aa....aa：

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，変更

(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

cc....cc：

encrypted column：暗号化列

(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。

KFPA19864-E

Unable to aa....aa MEMORY TABLE due to bb....bb, code=cc　（A）

bb....bb のため，メモリ DB 化対象表の設定ができません。

aa....aa：ALLOCATE

bb....bb：エラーに対する付加情報

cc：理由コード

理由コード（cc）	付加情報（bb....bb）	意味
08	encrypted table	暗号化表のため，メモリ DB 化対象表の設定ができません。

(S)この SQL 文を無視します。

(P)指定した表名が誤っている場合は，表名を見直して再度実行してください。表名が誤っていない場合，暗号化表はメモリ DB 化対象外にしてください。

KFPA19930-E

Unable to execute aa....aa statement for table "bb....bb"."cc....cc", due to invalid environment for INNER CONSTRUCTOR column　（A＋L）

暗号化列に関する環境に誤りがあるので表"bb....bb"."cc....cc"に対する aa....aa 文は実行できません。

aa....aa：実行しようとしたＳＱＬ文

- INSERT
- UPDATE
- DELETE
- ASSIGN LIST

bb....bb：認可識別子

cc....cc：表識別子またはビュー表識別子

(S)この SQL 文を無視します。

(P)HiRDB 管理者に連絡してください。

[対策]復号認証キー情報の一致条件を満たしているか確認してください。復号認証キー情報の一致条件を満たしている場合は，次のおそれがあります。

- 誤って復号認証キー情報の一致しない UAP から SQL を実行した。

- 誤って SQL 中に暗号化列を指定した。
- トリガや参照制約の制約動作によって，暗号化列を参照する SQL を実行した。
- ビュー定義に暗号化列を指定したビュー表を使用する SQL を実行した。
- 不正アクセスを受けた。
  不正アクセスを受けたおそれがあると判断した場合，ユーザ運用で不正アクセスがないか確認し対処してください。拡張 SQL エラー情報出力機能を使用している場合は，HiRDB サーバ側に出力した SQL エラーレポートファイルの内容から，KFPA19930-E が発生した SQL 実行時のクライアントの情報を確認できます。不正アクセスを受けていない場合，SQL 文の見直しを行ってください。

KFPD00032-W

Insufficient Audit definition buffer memory, size=aa....aa code=bb....bb completed size=cc....cc　（L）

セキュリティ監査情報用バッファの共用メモリが不足しました。

aa....aa：確保しようとしたサイズ（バイト）

bb....bb：エラーコード

cc....cc：確保したサイズ（バイト）

(S)処理を続行します。

(O)エラーコードに対するオペレータの処置を次に示します。性能を確保したい場合は次の処置をしてください。

エラーコード	要因の説明	オペレータの処置
05	HiRDB 稼働中，復号認証キー情報の登録が増えたため，すべての復号認証キー情報が復号認証キー情報用バッファに登録できませんでした。	HiRDB を再起動してください。

KFPD00033-I

Refresh aa....aa definition buffer completed　（L）

セキュリティ監査情報用バッファに，aa....aa で示す種別のすべての定義情報が登録されました。

aa....aa：定義情報の種別

Tpyrcedkey：復号認証キー情報

(S)処理を続行します。

KFPD00034-W

Unable to get aa....aa definition buffer space requirement,code=bb　（L）

ディクショナリアクセスエラーまたは通信障害が発生したため，セキュリティ監査情報用バッファ用共用メモリサイズの所要量が算出できませんでした。

aa....aa：エラー詳細

Tpyrcedkey：復号認証キー情報用バッファサイズの所要量が算出できませんでした。

bb：エラーコード

(S)オペレータの処置を参照してください。

(O)エラーコードに対するオペレータの処置を次に示します。

エラーコード	セキュリティ監査情報用バッファのサイズ指定	システムの処置	オペレータの処置
02	自動計算	aa....aa が Tpyrcedkey の場合，復号認証キー情報用バッファサイズが 0byte で続行します。	性能を確保したい場合は，エラーの要因を取り除いて，HiRDB を再開始してください。

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。

KFPI21505-I

Usage: pdfmkfs -n capacity [-l file_count] [-e expand_count] [-i] [-k area_kind] [-s sector_size] [-a] [-E] character_special_file pdfmkfs [-r] -n capacity [-l file_count] [-e expand_count] [-i] [-k area_kind] [-a] [-E] UNIX_regular_file　（E）

HiRDB ファイルシステム領域を初期設定するコマンド（pdfmkfs）の使用方法を示します。コマンドオプション，または引数が誤っている場合に出力されます。

(S)処理を終了します。

(O)コマンドの形式を修正して，再度実行してください。コマンドのオプションの組み合わせ可否については，マニュアル「HiRDB Version 9 コマンドリファレンス」を参照してください。

KFPI21609-E

aa....aa command unsupported　（E＋L）

未サポートのコマンドです。

aa....aa：コマンド名称

(S)処理を終了します。

[対策]必要な暗号化ライブラリがインストールされていません。HiRDB Data Convert Type1 Option のバージョンを確認してください。

KFPI21681-I

Usage: pdmkekey output_file　（E）

暗号鍵ファイル作成コマンド（pdmkekey）の使用方法を示します。引数が誤っている場合に出力されます。

(S)処理を終了します。

(O)コマンドの形式を修正して，再度実行してください。

KFPI21682-I

Usage: pdchekey -p old_key_file -n new_key_file {-f list_file¦HiRDB_file_system_area}　（E）

暗号鍵ファイル変更コマンド（pdchekey）の使用方法を示します。引数が誤っている場合に出力されます。

(S)処理を終了します。

(O)コマンドの形式を修正して，再度実行してください。

KFPI21683-I

Key change ended, file="aa....aa", code=b　（E＋L）

HiRDB ファイルシステム領域の暗号鍵の変更が終了しました。

aa....aa：暗号鍵を変更した HiRDB ファイル名称

b：コード

0：暗号鍵の変更に成功しました

4：暗号鍵がすでに変更済み，もしくは変更するファイルがないため，変更しませんでした。

8：暗号鍵の変更に失敗しました。

(S)処理を終了します。

[対策]コードが 8 の場合，直前のメッセージを参考にエラー要因を取り除き，再度 pdchekey コマンドで暗号鍵ファイルの変更を実施してください。

KFPI21684-E

Encryption function error occurred, code="aa....aa"　（E + L）

暗号化処理関数でエラーが発生しました。

aa....aa：内部情報

(S)処理を終了します。

[対策]保守員に連絡してください。

KFPI21685-E

Encryption key file invalid, reason="aa....aa"　（E + L）

暗号鍵ファイルが不正です。

aa....aa：理由

No definition：定義がありません。

Not found：暗号鍵ファイルが見つかりません。

Bad key：HiRDB ファイル作成時に作成した暗号鍵ファイルではないため，暗号鍵ファイルの暗号化キーで復号できません。

Bad format：指定した暗号鍵は，pdmkekey で作成した暗号鍵ファイルではありません。

(S)処理を終了します。

[対策]理由によって次の対処をしてください。

No definition：システム定義の pd_ekey オペランドを指定してください。

Not found：暗号鍵ファイルをシステム定義の pd_ekey オペランドのパスに配置してください。

Bad key：HiRDB ファイル作成時に作成した暗号鍵ファイルを指定しているか確認してください。

Bad format：pdmkekey で作成した暗号鍵ファイルを指定しているか確認してください。

KFPI21686-E

Specified backup file must be restored to aa....aa HiRDB file system area　（E＋L）

pdfrstr に指定したバックアップファイルは，aa....aa の HiRDB ファイルシステム領域にリストアしてください。

aa....aa：種別

encrypted：暗号化指定のある HiRDB ファイルシステム領域

unencrypted：暗号化指定のない HiRDB ファイルシステム領域

(S)処理を終了します。

[対策]HiRDB ファイルシステム領域をメッセージの種別に応じて HiRDB ファイルシステム領域を作成し直してください。

KFPI21687-E

Encryption key file aa....aa failed, code=bb....bb, file name="cc....cc"　（E＋L）

暗号鍵ファイルの操作に失敗しました。

aa....aa：操作

open：ファイルのオープン

write：ファイルの書き込み

read：ファイルの読み込み

fsync：ファイル書き込みの同期

close：ファイルのクローズ

bb....bb：内部コード

cc....cc：暗号鍵ファイル名称

ファイル名称が 150 文字を超える場合，ファイルの後ろから 150 文字を出力します。

(S)処理を終了します。

[対策]暗号鍵ファイルに指定したファイルがある場合は，異なるファイル名を指定してください。指定したファイルがない場合は，次のように対処してください。

操作が fsync の場合，内部コードが 5 のときは入出力エラーです。OS やハードウェアの情報に従って対策してください。内部コードが 5 以外のときは保守員に連絡してください。

操作が fsync 以外の場合，直前のメッセージに従って対処してください。

KFPI21688-E

List file aa....aa error occurred, code=bb....bb, file name="cc....cc"　（E＋L）

HiRDB ファイルシステム領域リストのファイルの操作で不正を検知しました。

aa....aa：理由

open：ファイルのオープンに失敗しました。

read ：ファイルの読み込みに失敗しました。

bb....bb：エラーコード

cc....cc：HiRDB ファイルシステム領域リストのファイル名

ファイル名称が 140 文字を超える場合，ファイルの後ろから 140 文字を出力します。

(S)処理を終了します。

[対策]理由が open の場合，ファイルがあるか確認してください。ファイルがある場合，または理由が read の場合，エラーコードから「システムコールのリターンコード」を参照し対処してください。

KFPI21689-E

HiRDB file system area operation error detected, code="aa....aa", line=bb....bb, file name="cc....cc"　（E ＋ L）

指定された HiRDB ファイルシステム領域の操作でエラーを検知しました。

aa....aa：理由

"long file name"：ファイル名が 165 文字を超えています。

"not encrypt file"：暗号化の指定のない HiRDB ファイルシステム領域です。

"encryption error"：暗号化や復号化の処理でエラーを検知しました。

"not found"：HiRDB ファイルシステム領域がありません。

"permission denied"：ファイルのアクセス権限がありません。

"open error"：ファイルのオープン数の上限を超えました。

"I/O error"：入出力エラーです。

"not HiRDB file system area"：HiRDB ファイルシステム領域ではありません。

"lock failed"：ロックセグメントが不足しています。

数値：HiRDB ファイルの操作でエラーになりました。

bb....bb：HiRDB ファイルシステム領域リストの行番号

HiRDB ファイルシステム領域名を指定した場合は，"*****"が表示されます。

cc....cc：HiRDB ファイルシステム領域名

ファイル名称が 90 文字を超える場合，ファイルの後ろから 90 文字を出力します。

ファイル名称が 255 文字を超える場合，166 文字目から 255 文字目までを出力します。

(S)処理を終了します。

[対策]理由によって次の対処をしてください。

long file name：

指定している HiRDB ファイルシステム領域の名称を確認してください。

not encrypt file：

指定する HiRDB ファイルシステム領域名に間違いがないか確認してください。間違いがない場合，変更する必要のない HiRDB ファイルシステム領域のためリストから削除してください。

encryption error：

保守員に連絡してください。

not found：

指定している HiRDB ファイルシステム領域の名称を確認してください。

permission denied：

指定している HiRDB ファイルの名称およびアクセス権を確認してください。HiRDB 管理者のアクセス権がない場合は，アクセス権を付与してください。

open error：

直前の KFPO00107-E メッセージの errno に対応した処置をしてください。UNIX 版の場合は，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見積もりを参照してください。オペレーティングシステムパラメタの値が不足している場合は上限値を上げてください。それぞれの OS では，次の値を見直してください。

- HP-UX の場合
  nfile，maxfiles_lim
- AIX の場合
  nofiles_hard
- Linux の場合
  NR_FILE，NR_OPEN

I/O error：

KFPO00107-E メッセージの errno に対応した処置をしてください。KFPO00107-E が出力されていない場合は保守員に連絡してください。

not HiRDB file system area：

指定している HiRDB ファイルの名称を確認してください。正しい場合は HiRDB ファイルシステム領域が壊れているおそれがあります。指定したファイルに対して pdfls コマンドを実行し，HiRDB ファイルシステム領域が壊れていないか調査してください。

lock failed：

KFPO00107-E メッセージの errno に対応した処置をしてください。errno が 46（ENOLCK）の場合は OS のロックセグメントが不足しています。マニュアル「HiRDB Version 9 システム導入・設計ガイド」OS のオペレーティングシステムパラメタの見積もりを参照し，上限値を上げてください。HP-UX の場合は，nflock を見直してください。

その他の OS の場合は，ロックを使用しているほかのプロセスの終了を待って，再度実行してください。

上記対策を実行しても問題が解決しない場合は保守員に連絡してください。

数値：

HiRDB ファイルシステムに対するアクセス要求から返されるエラーコードを参照し，対処してください。

KFPI21690-E

Encryption key file operation error detected, reson="aa....aa", code="bb....bb", file="cc....cc"　（E + L）

暗号鍵ファイルの操作でエラーを検知しました。

aa....aa：理由

open：オープン処理でエラーが発生しました。

read：読み込み処理でエラーが発生しました。

Bad key：暗号鍵が不正です。

Bad format：形式が不正です。

bb....bb：open，read 時のエラーコード

理由が open，read 以外の場合，"**"を出力します。

cc....cc：暗号鍵ファイル名

暗号鍵ファイル名が 100 文字を超える場合，ファイル名の後ろから 100 文字を出力します。

(S)処理を終了します。

[対策]理由によって次の対処をしてください。

open,read：エラーコードからシステムコールのリターンコード参照し，対処してください。

Bad key：正しい暗号鍵ファイルを指定しているか確認してください。

Bad format：正しい暗号鍵ファイルを指定しているか確認してください。

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 Server with Additional Function でないサーバが混在している状態で HiRDB Server with Additional Function の機能を使用している。

aa....aa：HiRDB Server with Additional Function 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 Server with Additional Function 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 Server with Additional Function の機能を使用する場合は，すべてのユニットで HiRDB Server with Additional Function 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，1 つだけ指定してください。

KFPT00017-E

aa....aa : Error occurred in bb....bb library function call, reason = cc....cc, inf = dd....dd　（L）

暗号化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：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：エラー発生ライブラリ名

encryption：暗号化ライブラリ

cc....cc：エラー理由

LIBRARY LOAD FAILURE：暗号化ライブラリのロードに失敗しました。

INSUFFICIENT MEMORY：暗号化機能の処理中にメモリ不足が発生しました。

dd....dd：エラー情報

- cc....cc が LIBRARY LOAD FAILURE の場合
  ライブラリ名称：libacon1.xx※
- cc....cc が INSUFFICIENT MEMORY の場合
  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。
- 上記以外の場合
  ********となります。

注※
xx は拡張子を示します。

(S)処理を終了します。

(O)システム管理者に連絡してください。

[対策]

- cc....cc が LIBRARY LOAD FAILURE の場合
  pdadmvr コマンドを実行して，HiRDB の種類が"Plus-facilities"であるかを確認してください。HiRDB の種類が"Plus-facilities"である場合は，保守員に連絡してください。HiRDB の種類が"Plus-facilities"でない場合は，HiRDB Server with Additional Function のセットアップが完了したあとに，コマンドを再実行してください。
- cc....cc が INSUFFICIENT MEMORY の場合
  同時実行しているプロセス数を減らすなどして使用できるメモリに余裕を持たせてから，コマンドを再実行してください。

上記の対策方法で対策できない場合は，保守員に連絡してください。

KFPT00018-E

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

暗号化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：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：エラー発生ライブラリ名
encryption：暗号化ライブラリ

cc....cc：エラーが発生した暗号化ライブラリ関数の名称

dd....dd：暗号化ライブラリ関数のリターンコード

ee....ee：保守情報 1

ff....ff：保守情報 2

(S)異常終了します。

(O)保守員に連絡してください。

KFPX21307-I

Usage: pdregtpyrcedkey {-f filename¦-D}　（S）

pdregtpyrcedkey のオプションの指定形式に誤りがあります。

(S)処理を終了します。

(O)オプションの指定形式を確認して，pdregtpyrcedkey を再度実行してください。

KFPX21308-E

Unable to open file,due to aa....aa　（E）

aa....aa が原因で指定されたファイルを開くことができません。

aa....aa：エラー原因

- no file：ファイルが存在しません。
- no permission on file：ファイルを開く権限がありません。
- system call error with errno エラーコード：システムコールエラーが発生しました。

(S)処理を終了します。

(O)エラーの原因を取り除き，pdregtpyrcedkey を再度実行してください。

KFPX21309-E

Invalid aa....aa in line bb....bb of input file　（E）

入力ファイルの bb....bb 行目の項目 aa....aa の形式に次のどれかの誤りがあります。

aa....aa：エラーの項目

IP address：IP アドレス

- nnn.nnn.nnn.nnn[/mm]の形式でない。
- nnn が 0～255 の範囲外である。

- mm が 24～31 の範囲外である。

authorization identifier：認可識別子

- 認可識別子に使用できない文字を記述している。
- 30 文字を超えている。

key：復号認証キー

- 使用できない文字（A～Z,a～z,0～9,@,#,¥,_,-以外）を記述している。
- 30 文字を超えている。

date：有効期限

- YYYY-MM-DD hh:mm:ss または YYYY-MM-DD の形式で記述していない。
- 年，月，日，時，分，秒に指定できない範囲の値を指定している。

bb....bb：エラー行の行番号

(S)処理を続行します。

(O)エラーの原因を取り除き，pdregtpyrcedkey を再度実行してください。

KFPX21310-I

pdregtpyrcedkey terminated　（S）

すべての復号認証キー情報の登録または削除処理が終了しました。

(S)処理を終了します。

KFPX21311-E

Error occurred in line aa....aa,bb....bb　（E）

pdregtpyrcedkey を実行中に入力ファイルの aa....aa 行目で bb....bb のエラーが発生しました。

aa....aa：エラーが発生した入力ファイルの行番号

bb....bb：エラー詳細メッセージ

(S)処理を終了します。

(O)エラー詳細メッセージ中のメッセージ ID を参照して，エラーの原因を取り除き，pdregtpyrcedkey を再度実行してください。

KFPX21312-W

pdregtpyrcedkey terminated incompletely　（S）

復号認証キー情報の登録または削除処理が終了しましたが，一部の登録または削除が完了していません。

(S)処理を終了します。

(O)すでに出力されている KPFX21309-E メッセージを参照して，入力ファイル中の登録または削除に失敗した復号認証キー情報を修正し，pdregtpyrcedkey を再度実行してください。

KFPX21313-E

Error occurred during execution of pdregtpyrcedkey, aa....aa　（E）

pdregtpyrcedkey を実行中にエラーが発生しました。

aa....aa：エラー詳細メッセージ

(S)処理を終了します。

(O)エラー詳細メッセージ中のメッセージ ID を参照して，エラーの原因を取り除き，pdregtpyrcedkey を再度実行してください。

11.2　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 9 メッセージ」を参照してください。

表 11–1　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。

11.3 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 9 メッセージ」を参照してください。

表 11–2 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

11.4　HiRDB ファイルシステムのエラーコード

暗号化機能を使用する場合に出力される HiRDB ファイルシステムのエラーコードを次の表に示します。その他の HiRDB ファイルシステムのエラーコードについては，マニュアル「HiRDB Version 9 メッセージ」を参照してください。

表 11–3　暗号化機能を使用する場合に出力される HiRDB ファイルシステムのエラーコード

エラーコード	内容	対策
-1544	入出力エラー，または暗号化・復号処理でエラーが発生しました。	イベントログ（UNIX 版の場合は syslogfile）の KFPO00107-E メッセージの errno に対応した処置，または KFPI メッセージに対応した処置をしてください。 KFPO00107-E，または KFPI メッセージが出力されていない場合は保守員に連絡してください。

付録

付録 A　予約語

付録 A.1　暗号化機能を使用したときの予約語

(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 Server with Additional Function

(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追加および変更となります。

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，およびビュー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，およびビュー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，およびビュー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，およびビュー表の場合はナル値となります。

付録 B.3　追加されるディクショナリ表

暗号化機能を使用する場合に追加されるディクショナリ表について説明します。

(1)　SQL_TPYRCEDKEY

この表では，復号認証キー情報を管理します（1 行で 1 復号認証キー情報分）。

なお，この表を参照できるのは，DBA 権限所有者，および監査人だけです。

SQL_TPYRCEDKEY 表の内容を次の表に示します。

表 B-1　SQL_TPYRCEDKEY 表の内容

項番	列名	データ型	内容
1	IP_ADDR	VARCHAR(15)	復号を許可するマシンの IP アドレス。
2	GRANTEE	VARCHAR(30)，または MVARCHAR(30)※	復号を許可する実行ユーザの認可識別子，または'PUBLIC'。
3	LIMITED_TIME	CHAR(14)	復号認証キー情報の有効期限 (YYYYMMDDHHMMSS)。 無期限の場合はナル値となります。
4	REG_TIME	CHAR(14)	復号認証キー情報の登録時刻 (YYYYMMDDHHMMSS)。

注※

データベース初期設定ユティリティ，またはデータベース構成変更ユティリティの dictionary datatype オペランドで，データ型をどちらにするか設定してください。

付録 B.4　追加されるディクショナリ表の参照権限

暗号化機能を使用する場合に追加されるディクショナリ表の，参照権限について説明します。次に示すユティリティの制御文で limited を指定すると，ディクショナリ表の参照権限を設定できます。

- データベース初期設定ユティリティの define system 文の dicinf オペランド
- データベース構成変更ユティリティの alter system 文の dicinf オペランド

dicinf オペランドの指定値と，暗号化機能を使用する場合に追加されるディクショナリ表の参照権限について，次の表に示します。

ディクショナリ表の参照権限については，マニュアル「HiRDB Version 9 システム運用ガイド」の「ディクショナリ表の参照権限を設定するには」を参照してください。

表 B–2　dicinf オペランドの指定値とディクショナリ表の参照権限

ディクショナリ表	dicinf オペランドの指定値					
	limited			unlimited		
	DBA 権限保持者	監査人	一般ユーザ	DBA 権限保持者	監査人	一般ユーザ
SQL_TPYRCEDKEY	○	○	×	○	○	×

（凡例）

○：すべての列を参照できます。

×：すべての列を参照できません。

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　ユティリティ

暗号化機能で使用するユティリティの仕様について説明します。

付録 D.1　ユティリティの排他制御モード

暗号化機能で使用するユティリティの排他制御モードについて，次の表に示します。その他のコマンドおよびユティリティの排他制御モードについては，マニュアル「HiRDB Version 9 コマンドリファレンス」の「コマンド実行時の排他制御モード」を参照してください。

表中で使用している排他制御モードを次に示します。

PR：共用モードの排他が掛かります。

EX：排他モードの排他が掛かります。

SR：意図共用モードの排他が掛かります。

SU：意図排他モードの排他が掛かります。

表 D-1　復号認証キー情報登録ユティリティの排他制御モード

実行環境	資源					
	ディクショナリ表	ディクショナリ表				
		行	前処理表	表	RD エリア	
					表用	インデクス用
復号認証キー情報登録ユティリティ	EX	PR※1/EX※2	PR※1※3	SR※1/SU※2	SR※1/SU※2	SR※1/SU※2

注※1

ディクショナリ表(SQL_USERS)に排他を掛けます。

注※2

ディクショナリ表(SQL_TPYRCEDKEY)に排他を掛けます。

注※3

一時的に排他を掛けます。

付録 D.2　排他資源数の見積もり

暗号化機能で使用するユティリティを実行するときに必要とする排他資源数の概算式を示します。その他のコマンドおよびユティリティの排他資源数の見積もりについては，マニュアル「HiRDB Version 9 システム定義」の「排他資源数の見積もり」を参照してください。

(1)　復号認証キー情報登録ユティリティ（pdregtpyrcedkey）

(a)　HiRDB/シングルサーバの場合

7＋登録または削除対象の復号認証キー情報数
インデクスキー値排他を使用している場合に加算します。
　＋1＋登録または削除対象の復号認証キー情報数

(b)　HiRDB/パラレルサーバの場合（ディクショナリサーバ）

7＋登録または削除対象の復号認証キー情報数
インデクスキー値排他を使用している場合に加算します。
　＋1＋登録または削除対象の復号認証キー情報数

付録 D.3　RD エリアの状態による実行可否

暗号化機能で使用するユティリティの RD エリアの状態による実行可否を次の表に示します。その他のコマンドおよびユティリティの実行可否については，マニュアル「HiRDB Version 9 コマンドリファレンス」の「コマンド実行時の RD エリアの状態」を参照してください。

表中で使用している凡例を次に示します。

○：実行できます。

×：実行できません。

－：該当しません。

表 D-2　RD エリアの状態によるユティリティの実行可否（オープン契機が INITIAL の場合）（1/3）

ユティリティ	閉塞なし		コマンド閉塞		参照可能閉塞	
	オープン	クローズ	オープン	クローズ	オープン	クローズ
復号認証キー情報登録ユティリティ	○	×	×	×	×	×

表 D-3　RD エリアの状態によるユティリティの実行可否（オープン契機が INITIAL の場合）（2/3）

ユティリティ	参照可能バックアップ閉塞		更新可能バックアップ閉塞	障害閉塞	
	オープン	クローズ	オープン	オープン	クローズ
復号認証キー情報登録ユティリティ	×	×	○	×	×

表 D–4　RD エリアの状態によるユティリティの実行可否（オープン契機が INITIAL の場合）（3/3）

ユティリティ	ログレス閉塞		同期化閉塞		オン中再編成閉塞	
	オープン	クローズ	オープン	クローズ	オープン	クローズ
復号認証キー情報登録ユティリティ	×	×	−	−	−	−

表 D–5　RD エリアの状態によるユティリティの実行可否（オープン契機が DEFER または SCHEDULE の場合）（1/3）

ユティリティ	閉塞なし		コマンド閉塞		参照可能閉塞	
	オープン	クローズ	オープン	クローズ	オープン	クローズ
復号認証キー情報登録ユティリティ※	−	−	−	−	−	−

表 D–6　RD エリアの状態によるユティリティの実行可否（オープン契機が DEFER または SCHEDULE の場合）（2/3）

ユティリティ	参照可能バックアップ閉塞		更新可能バックアップ閉塞	障害閉塞	
	オープン	クローズ	オープン	オープン	クローズ
復号認証キー情報登録ユティリティ※	−	−	−	−	−

表 D–7　RD エリアの状態によるユティリティの実行可否（オープン契機が DEFER または SCHEDULE の場合）（3/3）

ユティリティ	ログレス閉塞		同期化閉塞		オン中再編成閉塞	
	オープン	クローズ	オープン	クローズ	オープン	クローズ
復号認証キー情報登録ユティリティ※	−	−	−	−	−	−

注※

対象となるディクショナリ表用 RD エリアのオープン契機が，DEFER または SCHEDULE になることはないため，該当しない。

付録 D.4　ユティリティの最大同時実行数

暗号化機能で使用するユティリティの最大同時実行数を次の表に示します。その他のユティリティの最大同時実行数については，マニュアル「HiRDB Version 9 コマンドリファレンス」の「ユティリティの最大同時実行数」を参照してください。

表 D–8　ユティリティの最大同時実行数

ユティリティ	最大同時実行数
復号認証キー情報登録ユティリティ（pdregtpyrcedkey）	1

付録 D.5　リターンコード一覧

暗号化機能で使用するユティリティのリターンコードを次の表に示します。その他のコマンドおよびユティリティのリターンコードについては，マニュアル「HiRDB Version 9 コマンドリファレンス」の「コマンドのリターンコード一覧」を参照してください。

表 D-9　リターンコード一覧

コマンド名	出力メッセージ		リターンコード	内容
	メッセージ ID	コード		
pdregtpyrcedkey	−	−	0	正常終了
			4	警告終了
			8	異常終了
pdmkekey	−	−	0	正常終了
			8	異常終了
pdchekey	KFPI21607-I	0	0	正常終了
		8	8	異常終了

（凡例）

−：メッセージ，またはコードは出力されません。

付録 D.6　UAP からの実行可否

暗号化機能で使用するユティリティの UAP からの実行可否を次の表に示します。その他のコマンドおよびユティリティの実行可否については，マニュアル「HiRDB Version 9 UAP 開発ガイド」の「コマンド実行可否」を参照してください。

表 D-10　UAP からのコマンド実行可否

コマンド名	内容	COMMAND EXECUTE からの実行可否	CALL COMMAND からの実行可否
pdregtpyrcedkey	復号認証キー情報の登録	○	○

（凡例）

○：UAP から実行できます。

付録 D.7　ログ適用サイトでの実行可否

ログ同期方式のリアルタイム SAN レプリケーションを適用している場合の，暗号化機能で使用するユティリティのログ適用サイトでの実行可否を次の表に示します。その他のコマンドおよびユティリティの実行

可否については，マニュアル「HiRDB Version 9 ディザスタリカバリシステム　構築・運用ガイド」の「ログ適用サイトでの HiRDB のコマンド実行可否」を参照してください。

表 D–11　ログ適用サイトでのコマンド実行可否

コマンド名	内容	ログ適用サイトでのコマンド実行可否
pdregtpyrcedkey	復号認証キー情報の登録	×

（凡例）

×：実行しないでください。実行した場合の動作は保証されません。

付録 D.8　暗号鍵ファイルが必要なコマンド

暗号化 HiRDB ファイルシステム領域にアクセスするときにシステム定義の pd_ekey オペランドに示すパスに暗号鍵ファイルを配置する必要があるコマンドを次の表に示します。暗号鍵ファイルがない場合，pdstart コマンドは起動処理がエラーになります。pdstart コマンド以外のコマンドは暗号化 HiRDB ファイルシステム領域に作成した HiRDB ファイルを操作するときにエラーになります。

表 D–12　暗号鍵ファイルが必要なコマンド

コマンド名	暗号鍵ファイルが必要になる条件
pdbkupls	バックアップファイルを暗号化 HiRDB ファイルシステム領域に作成している
pdcat	暗号化 HiRDB ファイルシステム領域に作成しているステータスファイルの内容を表示する
pdchpathf	暗号化 HiRDB ファイルシステム領域のパス名を変更する
pdconfchk	暗号化 HiRDB ファイルシステム領域のステータスファイル，シンクポイントダンプファイル，システムログファイルをシステム定義に指定している
pdlogchg	暗号化 HiRDB ファイルシステム領域にシステムログファイルを作成している
pdloginit	暗号化 HiRDB ファイルシステム領域にシステムログファイルもしくはシンクポイントダンプファイルを作成する
pdlogls	表示対象のファイルを暗号化 HiRDB ファイルシステム領域に作成している
pdlogrm	削除するファイルが暗号化 HiRDB ファイルシステム領域に作成されている
pdlogucat	暗号化 HiRDB ファイルシステム領域にシステムログファイルを作成している
pdlogunld	暗号化 HiRDB ファイルシステム領域に作成したシステムログファイルをアンロードするか，出力先に暗号化 HiRDB ファイルシステム領域を指定する
pdstart	システム定義の pd_ekey オペランドを指定している
pdstedit	暗号化 HiRDB ファイルシステム領域に作成したシステムログファイルを入力ファイルに指定する
pdstsinit	暗号化 HiRDB ファイルシステム領域にステータスファイルを作成する

コマンド名	暗号鍵ファイルが必要になる条件
pdstsrm	暗号化 HiRDB ファイルシステム領域に作成したステータスファイルを削除する

付録 E　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 HiRDB ファイルシステム領域

データを暗号化する指定をした HiRDB ファイルシステム領域のことです。この領域に作成した HiRDB ファイルのデータは暗号化されます。

暗号鍵ファイル

暗号化 HiRDB ファイルシステム領域で使用する暗号鍵を格納したファイルです。

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