VERITAS NetBackup™ Encryption 3.4

System Administrator's Guide

（日本語版）

2000 年 10 月
P/N 30-000089-011

VERITAS

免責事項

本書に記載されている情報は、予告なしに変更される場合があります。VERITAS Software Corporation は、本書に関して、商品性や特定目的に対する適合性の黙示保証などの一切の保証を行いません。VERITAS Software Corporation は、本書に含まれるエラーや本書の提供、遂行、または使用に伴う付随的または間接的な損害に対して一切の責任を負わないものとします。

著作権

Printed in the USA, November 2000.

VERITAS NetBackup Encryption System Administrator's Guide

VERITAS Software Corporation
1600 Plymouth St.
Mountain View, CA 94043
電話 650–335–8000
ファックス 650–335–8050
www.veritas.com

目次

まえがき

本書では、VERITAS NetBackup Encryption のインストール、設定、および使用方法を説明します。*NetBackup Encryption System Administrator's Guide* 本書内では、VERITAS NetBackup は NetBackup、VERITAS NetBackup Encryption は NetBackup Encryption と表します。

対象読者

本書では、NetBackup Encryption を設定する システム管理者を対象としています。また、ユーザが NetBackup の管理や使用方法に関する十分な知識を持っていることを前提とします。

本書の構成

- 第 1 章 「はじめに」では、製品の概要を説明します。
- 第 2 章 「マスタサーバでのインストール」では、NetBackup Encryption のインストール方法を説明します。
- 第 3 章 「設定」NetBackup Encryption を使用するためのシステムの構成方法を説明します。この情報は NetBackup Windows NT/2000 Server と UNIX system administrator's guide 内のシステム構成方法の説明を補足するのもです。
- 付録 A 「コマンド」では、暗号をインストールしたり、設定するために必要なコマンドを説明します。

関連マニュアル

- *NetBackup System Administrator's Guide - Windows NT/2000*

  Windows NT/2000 システム上での NetBackup の設定方法や管理方法が説明されています。
- *NetBackup System Administrator's Guide - UNIX*

  UNIX システム上での NetBackup の設定方法や管理方法が説明されています。

表記規則

本書で採用している一般的な表記規則について説明します。

一般の表記規則

表 1. 一般の表記規則

表記	用途
英字等幅フォント太字	入力する文字。例: **cd** と入力して、ディレクトリを変更してください。
英字等幅フォント	パス、コマンド、ファイル名、および出力。例: デフォルトのインストール ディレクトリは /opt/VRTSxx です。
『』	ドキュメントなどのタイトル。
「」	章や項目のタイトル、強調する用語。
英字ゴシック体（斜体）	プレースホルダーテキストまたは変数。例: *filename* には、実際のファイル名を指定してください。
英字ゴシック体（斜体以外）	フィールド名、メニュー項目など、グラフィカルユーザインタフェース（GUI）のオブジェクト。例: ［**パスワード**］フィールドに、パスワードを入力してください。

「注」と「注意」の違い

注 「注」では、製品をより使いやすくするための情報や、問題の発生を防ぐための情報について説明します。

注意 「注意」では、データ損失のおそれがある状態について説明します。

キーの組み合わせ

キーボードからコマンドを入力する場合、複数のキーを同時に使用することがあります。たとえば、Ctrl キーを押しながら別のキーを押す場合などが考えられます。このようなコマンドを示す場合は、次のように、各キーをプラス記号（+）でつないで表記します。

Ctrl+T を押します。

コマンドの用法

コマンドの用法を示す場合によく使用される表記を、以下に示します。

角かっこ［ ］

かっこ内のコマンド ライン コンポーネントは、必要に応じて指定可能なオプションです。

垂直バーまたはパイプ（|）

ユーザーが選択可能なオプションの引数を区切る場合に使用します。たとえば、次に示すコマンドでは、ユーザーが *arg1* または *arg2* のいずれかを使用できることを示します。

```
command arg1|arg2
```

テクニカル サポート

この製品に関するシステム要件、サポートされているプラットフォーム、サポートされている周辺機器、テクニカル サポートから入手できる最新のパッチなどの最新情報については、弊社の Web サイトをご利用ください。

http://www.veritas.com/jp（日本語）

http://www.veritas.com/（英語）

製品に関するサポートは、VERITAS テクニカル サポートまでお問い合わせください。

電話: (03)3509-9210

FAX : (03)5532-8209

VERITAS カスタマ サポートへのお問い合わせの際は、次の電子メール アドレスもご利用いただけます。

support.jp-es@veritas.com

はじめに 1

NetBackup Encryption は、ファイルレベルにおけるバックアップやアーカイブの暗号化を提供します。この製品は、NetBackup 本体とは別々に購入する必要があります。NetBackup Encryption には、以下のように 2 つのバージョンがあります。

- Encryption with 40-bit DES
- Encryption with 56-bit DES (40 ビット DES を含む)

注 本書で説明している CRYPT_OPTION、CRYPT_STRENGTH、CRYPT_LIBPATH、および CRYPT_KEYFILE 設定オプションは UNIX および Macintosh クライアント上では bp.conf ファイル内にあり、Microsoft Windows クライアント上ではレジストリ内にあります。また、Windows NT/2000 NetBackup サーバ上で NetBackup の管理インタフェースを使用し、リモートでオプションを設定することもできます。これらのオプションは、［**クライアントのプロパティ**］ダイアログボックスの **[暗号]** タブで設定することがきます（詳しくは、*NetBackup System Administrator's Guide - Windows NT/2000* を参照してください）。

用語

NetBackup Encryption を理解したり、使用する上で役に立つ用語を以下に説明します。

DES

DES（Data Encryption Standard）は共通キーを使用したブロック暗号方式を採用しています。この方式では、データの暗号化や暗号の解読に同一のシークレット暗号キーを使用します。NetBackup Encryption はバックアップを暗号化するのに、DES を使用します。

56 ビット DES キー

標準の DES 暗号キーは、56 ビット長です。

40 ビット DES キー

40 ビットの DES キーは、常にゼロに設定されている 16 ビットを除いては、56 ビット DES キーと同一のものです。

キーファイル

キーファイルとは、NetBackup Encryption クライアント上に存在するファイルのことです。キーファイル内のデータはDESキーを生成するのに使用されます。このDES キーはクライアントのバックアップファイルを暗号化するのに使用されます。キーファイルのパス名は、クライアントのCRYPT_KEYFILE設定オプションで定義されます。キーファイルを作成したり更新するには、NetBackupマスタサーバ上で`bpinst`コマンドを使用するか、またはクライアント上で`bpkeyfile`コマンドを使用してパスフレーズを指定します。

パスフレーズ

パスフレーズとは、パスワードと同様のものですが、通常はパスワードよりも長いものです。NetBackupでは、DES暗号キーを生成するために、パスフレーズのチェックサムを実行します。NetBackupが使用するパスフレーズは0から63の文字列を含むことができます。システム間の互換性に関する問題を防ぐために、パスフレーズに使用する文字は、表示可能なASCII文字に限定してください。つまりASCII照合順序では、スペース（コード32）からチルダ（コード126）までの文字です。

NetBackupパスフレーズ

NetBackupパスフレーズは、クライアントのキーファイル内にあるデータを生成するのに使用されます。キーファイル内のデータは、DESキーを生成するのに使用されます。また、このDES キーはクライアントのバックアップファイルを暗号化するのに使用されます。クライアントのキーファイル用にNetBackupパスフレーズを更新するには、マスタサーバで`bpinst`コマンドに`-passphrase_prompt`オプションを指定、またはクライアントで`bpkeyfile`コマンドに`-change_netbackup_pass_phrase`オプションを指定します。

キーファイルパスフレーズ

キーファイルパスフレーズは、DESキーを生成するのに使用されます。このDESキーは、NetBackupクライアント上でキーファイルを暗号化するのに使用されます。標準のキーファイルパスフレーズを使用する以外に、クライアント上で`bpkeyfile`コマンドに`-change_key_file_pass_phrase`オプションを指定することで、独自のキーファイルパスフレーズを使用することができます。

標準キーファイルパスフレーズ

標準キーファイルパスフレーズは、NetBackupプログラムにハードコードされています。標準キーファイルパスフレーズを使用して作成したDESキーでキーファイルを暗号化した場合には、NetBackupプログラムはキーファイルの暗号を自動的に解読し、読み取ることができます。

技術的な概要

バックアップやリストアの実行中における、NetBackup Encryption処理の仕組みを以下で説明します。

暗号化バックアップの仕組み

サーバは、バックアップを暗号化するかどうかを判断するのに、クラス属性を使用します。次に、サーバがクライアント上のbpcdプロセスへ接続し、バックアップを開始して、バックアップ要求へ暗号化クラス属性を渡します。クライアントは、渡された暗号化クラス属性とクライアント上の設定内のCRYPT_OPTIONを比較します。

- クラス属性がyesで、CRYPT_OPTIONがREQUIREDまたは、ALLOWEDの場合には、クライアントは、暗号化バックアップを実行します。
- クラス属性がyesで、CRYPT_OPTIONがDENIEDの場合には、クライアントは、バックアップを実行しません。
- クラス属性がnoで、CRYPT_OPTIONがALLOWEDまたは、DENIEDの場合には、クライアントは、非暗号化バックアップを実行します。
- クラス属性がnoで、CRYPT_OPTIONがREQUIREDの場合には、クライアントは、バックアップを実行しません。

以下の表には、上記の各状況におけるバックアップの実行タイプが示されています。

	暗号化クラス属性	
CRYPT_OPTION	Yes	No
REQUIRED	暗号化	バックアップを実行しない
ALLOWED	暗号化	非暗号化
DENIED	バックアップを実行しない	非暗号化

以下に、バックアップを暗号化するために、あらかじめ必要な条件を説明します。

- CRYPT_LIBPATH設定エントリで指定したクライアント上のディレクトリに暗号化ソフトウェアがロードされている必要があります。
- 暗号化ソフトウェアは40ビットDESライブラリを含む必要があります。40ビットDESライブラリの名前は、libvdes40.*extention*です。*extention*(拡張子)はプラットフォームよっては異なりますが、通常はso、sl、またはdllです。
- CRYPT_STRENGTH設定オプションがDES_56に設定されている場合は、暗号化ソフトウェアは56ビットDESライブラリも含む必要があります。56ビットDESライブラリの名前は、libvdes56.*extention*です。*extention*(拡張子)はプラットフォームよっては異なりますが、通常はso、sl、またはdllです。

- キーファイルは、CRYPT_KEYFILE設定オプションで指定した通りに存在する必要があります。キーファイルは、マスタサーバからbpinstコマンド、または、クライアントからbpkeyfileコマンドを使用してNetBackupパスフレーズを指定すると作成されます。

上記の条件が揃い、バックアップ処理が開始されると、以下の状況が発生します。

1. クライアントがキーファイルから最新のデータを取り出し、現在の時間（バックアップ時間）とマージさせてDESキーを生成します。40ビットDESキーの場合は、キーの16ビット分は常にゼロに設定されます。

2. バックアップされる各ファイルに関して：
   - クライアントは、暗号化されたtarヘッダを作成します。このヘッダには、暗号化に使用したDESキーのチェックサムが含まれています。
   - クライアントは、DESキーを使用して暗号化されたファイルデータを書き込みます。

注 暗号化されるものはファイルのデータのみです。ファイル名や属性は暗号化されません。

3. サーバはクライアントからファイル名、属性、およびデータを読み取り、サーバ上のバックアップイメージへ書き込みます。この際、サーバはデータの暗号化や暗号の解読を実行しません。サーバ上のバックアップイメージに含まれるものは、バックアップ時間、およびバックアップの暗号化有無を示すフラグです。

暗号化リストアの仕組み

サーバはバックアップイメージを使用してバックアップの暗号化の有無を判断します。次に、サーバはクライアント上のbpcdプロセスへ接続してリストアを開始します。サーバはリストア要求されたバックアップイメージに書き込まれている暗号化フラグとバックアップ時間をクライアントへ渡します。

以下に、暗号化したバックアップをリストアするために、あらかじめ必要な条件を説明します。

- CRYPT_LIBPATH設定オプションで指定したクライアント上のディレクトリに暗号化ソフトウェアがロードされている必要があります。
- 暗号化ソフトウェアは40ビットDESライブラリを含む必要があります。40ビットDESライブラリの名前は、libvdes40.*extention*です。*extention*（拡張子）はプラットフォームよっては異なりますが、通常はso、sl、またはdllです。
- CRYPT_STRENGTH設定オプションがDES_56に設定されている場合は、暗号化ソフトウェアは56ビットDESライブラリも含む必要があります。56ビットDESライブラリの名前は、libvdes56.*extention*です。*extention*（拡張子）はプラットフォームよっては異なりますが、通常はso、sl、またはdllです。
- キーファイルは、CRYPT_KEYFILE設定オプションで指定した通りに、存在する必要があります。キーファイルは、マスタサーバからbpinstコマンド、または、クライアントからbpkeyfileコマンドを使用してNetBackupパスフレーズを指定する際に作成されます。

上記の条件が揃い、リストア処理が開始されると、以下の状況が発生します。

1. サーバはファイル名、属性、および暗号化されたファイルデータをリストア先クライアントへ送信します。

2. クライアントはクライアント上のキーファイルデータを取り出し、現在の時間（バックアップ時間）とマージさせ、1つまたは複数の40ビットDESキーを生成します。56ビットDESライブラリが使用できる環境では、クライアントは、1つまたは複数の56ビットDESキーも生成します。

3. クライアントが暗号化された`tar`ヘッダを読み取り、ヘッダ内のチェックサムとDESキーのチェックサムを比較します。チェックサムが一致すると、DESキーを使用してファイルデータの暗号を解読します。

4. この場合は 、DESキーが使用可能なときは、暗号化されたファイルデータが解読されファイルがクライアント上にリストアされます。DESキーが使用できないときは、ファイルはリストアされずに、エラーメッセージが生成されます。

マスタサーバでのインストール 2

クライアントへインストールする前に、NetBackup Encryption を UNIX または Windows NT/2000 NetBackup マスタサーバへインストールする必要があります。マスタサーバへのインストール後、クライアント上へインストールし、第3 章の 「設定」に説明されているように、暗号化に関する必要な設定を行います。

インストール必要条件

クライアント上のファイルに対して暗号化バックアップを実行するには、マスタサーバで NetBackup 3.4 サーバソフトウェアが実行されている必要があります。なお、NetBackup Encryption がインストール可能なプラットフォームのリストについては、NetBackup Release Notes を参照してください。

UNIX NetBackup マスタサーバにインストールする

1. NetBackup UNIX マスタサーバに root ユーザとしてログインします。
2. 以下のコマンドを実行し、NetBackup Encryption (40 または 56 ビット) のライセンスキーを登録します。

   ```
   /usr/openv/netbackup/bin/admincmd/get_license_key
   ```

3. NetBackup Encryption ソフトウェア (40 または 56 ビット) を含んでいる CD を CD ドライブへ挿入します。
4. 作業ディレクトリを CD-ROM ディレクトリに変更します。

   ```
   cd /cd_rom_directory
   ```

   cd_rom_directory は CD-ROM へアクセスすることのできるパスです。プラットフォームによっては、ディレクトリをマウントする必要があります。

5. NetBackup Encryption をインストールするには、以下のコマンドを実行します。

   ./install

インストールする NetBackup Encryption のバージョンが表示されます。続行を促すプロンプトが表示される場合は、y を入力します。

6. クライアント上にソフトウェアをインストールします。

   たいていの NetBackup クライアントの場合、マスタサーバからクライアントへ暗号化ソフトウェアをプッシュすることができます。詳しくは、「マスタサーバから設定する」（11 ページ）を参照してください。

   ただし、クライアントがサーバからの書き込みを許可している必要があります。つまり、UNIX や Macintosh クライアント上では、`bp.conf` ファイルから `DISALLOW_SERVER_WRITES` エントリを削除してください。また、Microsoft Windows クライアント上では、[NetBackup **設定**] ダイアログボックスの［**一般**］タブで **[サーバ主動のリストアを有効化]** ボックスを選択する必要があります（このダイアログボックスを開くには、クライアントユーザインタフェースの **[アクション]** メニュー上で **[設定]** を選択します）。

   クライアントがサーバからの書き込みを許可しないように設定されている場合は、「クライアント上で NetBackup Encryption を設定する」（15 ページ）に説明されている方法を実行してください。

Windows NT/2000 NetBackup マスタサーバにインストールする

1. Windows NT/2000 NetBackup サーバで Administrator としてログインします。

2. 以下の操作を実行し、NetBackup Encryption (40 または 56 ビット) のライセンスキーを登録します。

   a. NetBackup 管理ウィンドウで **[ヘルプ]** をクリックします。

   b. **[ヘルプ]** メニューで **[ライセンス キー]** を選択します。

      [NetBackup **ライセンス キー**] ダイアログ ボックスが表示されます。**[現在のライセンス]** フィールドには、登録済みのライセンス キーが表示されます。

   c. 新しいキーを登録するには、新規ボタンをクリックし、表示される **[ライセンス キーの追加]** ダイアログ ボックスの **[新しいライセンス キー]** フィールドにライセンスを入力します。

   新しく追加したキーが [NetBackup **ライセンス キー**] ダイアログ ボックスの［**現在のライセンス**］フィールドに表示されます。

3. NetBackup Encryption の CD-ROM を CD-ROM ドライブに挿入します。

4. 自動再生機能が使用可能な場合は、AutoRun プログラムを使用して以下のことを実行することができます。

- CD-ROM を参照する。
- プログラムをシステムへ追加したりシステムから削除する。
- NetBackup Encryption for Windows NT/2000 Readme ファイルを表示する。
- NetBackup Encryption for Windows NT/2000 をインストールする。

5. 自動再生機能が使用できない場合は、**[スタート]** メニューから **[ファイル名を指定して実行]** を選択し、以下のように入力して [OK] をクリックします。

   D:\NTCrypt\Setup.exe

   D:\ は、お使いの CD-ROM ドライブです。

6. インストールアプリケーションの指示に従って操作を進めます。

7. クライアント上へソフトウェアをインストールします。

   たいていの NetBackup クライアントの場合、マスタサーバからクライアントへ暗号化ソフトウェアをプッシュすることができます。詳しくは、「マスタサーバから設定する」（11 ページ）を参照してください。

   ただし、クライアントがサーバからの書き込みを許可している必要があります。つまり、UNIX や Macintosh クライアント上では、bp.conf ファイルから DISALLOW_SERVER_WRITES エントリを削除してください。また、Microsoft Windows クライアント上では、[NetBackup **設定**] ダイアログボックスの [**一般**] タブで **[サーバ主動のリストアを有効化]** ボックスを選択する必要があります（このダイアログボックスを開くには、クライアントユーザインタフェース内の **[アクション]** メニュー上で **[設定]** をクリックします）。

   クライアントがサーバからの書き込みを許可しないように設定されている場合は、「クライアント上で NetBackup Encryption を設定する」（15 ページ）に説明されている方法を実行してください。

設定 3

この章では、NetBackup Encryptionの設定方法や以下の項目を説明します。

- マスタサーバから設定する
- クライアント上でNetBackup Encryptionを設定する
- NetBackupクラスで暗号化を設定する
- その他のキーファイルセキュリティについて（UNIXクライアントのみ）

注 この章で説明しているCRYPT_OPTION、CRYPT_STRENGTH、CRYPT_LIBPATH、およびCRYPT_KEYFILET設定オプションはUNIXおよびMacintoshクライアント上ではbp.confファイルに設定されています。また、Microsoft Windowsクライアント上ではレジストリに設定されています。さらに、Windows NT/2000 NetBackupサーバ上でNetBackupの管理インタフェースを使用し、リモートでクライアントのオプションを設定することもできます。これらのオプションは、［**クライアントのプロパティ**］ダイアログボックスの**[暗号]**タブで設定することがきます（詳しくは、*NetBackup System Administrator's Guide - Windows NT/2000*を参照してください）。

マスタサーバから設定する

マスタサーバからbpinstコマンドを実行することにより、NetBackupクライアントの暗号化環境を設定することができます。その際、以下の条件があらかじめ必要です。

- NetBackup Encryptionクライアントソフトウェアが、第2章の「マスタサーバでのインストール」で説明されているように、マスタサーバ上の適切なディレクトリにインストールされている必要があります。
- NetBackupクライアントソフトウェアが、NetBackup Encryptionをサポートするプラットフォーム上で実行されている必要があります（NetBackup Release Notesを参照）。
- NetBackupクライアントがNetBackup 3.4以降を実行している必要があります。
- クライアント上のNetBackup設定がサーバからの書き込みを許可している必要があります。

  サーバからの書き込み許可を有効に設定するには、UNIXやMacintoshクライアントでは、bp.confファイルからDISALLOW_SERVER_WRITESエントリを削除してください。

また、Microsoft Windows クライアント上では、［NetBackup **設定**］ダイアログボックスの［**一般**］タブで **[サーバ主動のリストアを有効化]** ボックスを選択する必要があります（このダイアログボックスを開くには、クライアントユーザインタフェースの **[アクション]** メニュー上で **[設定]** を選択します）。

クライアントがサーバからの書き込みを許可しないように設定されている場合は、書き込みを許可するように現在の設定を一時的に変更するか、「クライアント上で NetBackup Encryption を設定する」（15 ページ）に説明されている方法を実行してください。

bpinst コマンドはマスタサーバの NetBackup bin ディレクトリに存在します。

- Windows NT/2000 サーバの場合には、bin ディレクトリは以下の通りです。

  install_path¥NetBackup¥bin

- UNIX サーバの場合には、bin ディレクトリは以下の通りです。

  /usr/openv/netbackup/bin

bpinst コマンドで使用できるオプションの詳細については、付録 A の bpinst コマンドの説明を参照してください。以下のセクションで、bpinst の使用方法を紹介します。

bpinst コマンド使用する際、通常はクライアント名を指定します。ただし、-class_names オプションを使用する場合は、クライアント名の代りにクラス名を指定します。このオプションを使用すると、指定したクラス内のすべてのクライアントに設定が影響します。

クライアントをまだ設定していない場合は、以下をお読みください。

bpinst -CRYPT を使用し、暗号化をまだ設定していないクライアントを設定する場合は、まず bpinst コマンドを使用して暗号化ライブラリをクライアントへプッシュします。その後、別の bpinst コマンドを使用して暗号化パスフレーズを設定します。以下に例を示します：

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client clientname1
bpinst -CRYPT -passphrase_prompt clientname1
```

同じコマンドライン上で -client_libraries と -passphrase_prompt の両方の引数を指定すると、パスフレーズの設定は失敗します。これは、暗号化ライブラリがクライアント上でまだ使用できないのが理由です。

NetBackup Encryption ソフトウェアをクライアントへプッシュする

注 NetBackup Release Notes のサポートされるプラットフォームのセクションで、暗号化をサポートしている NetBackup クライアントが定義されています。

bpinst コマンドで -client_libraries オプションを使用してマスタサーバから NetBackup クライアントへ暗号化ソフトウェアをコピーすることができます。

client1 および client2 へクライアントソフトウェアをインストールする場合には、以下のコマンドを（一行で）入力します。

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client client1
client2
```

NetBackup クラスの client1 および client2 内のすべてのクライアントへクライアントソフトウェアをインストールする場合には、以下のコマンドを（一行で）入力します。

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client -class_names
class1 class2
```

Windows NT/2000 マスターサーバでは、以下のコマンドを入力します。

```
bpinst.exe -CRYPT -client_libraries ignore client1 client2
bpinst.exe -CRYPT -client_libraries ignore class_names client1
client2
```

注 Windows NT/2000 マスターサーバで -client_libraries オプションを使用する場合には、必ず引数 ignore を一緒に使用してください。

NetBackup Encryption 設定をクライアントへプッシュする

bpinst コマンドで -crypt_option と -crypt_strength オプションを使用し、暗号化に関連した設定を NetBackup クライアント上にプッシュすることができます。

- -crypt_option オプションを使用する場合で、クライアントが暗号化バックアップを許可しない場合は、（denied）を指定します。クライアントが暗号化バックアップを許可する場合は、（allowed）を指定します。クライアントが暗号化バックアップを必要とする場合は、（required）を指定します。
- -crypt_strength オプションでは、クライアントが暗号化バックアップ用に使用する DES キー長（40 または 56）を指定します。

NetBackup クラス class1 および class2 内にあるすべてのクライアントを 56 ビット DES キーを使用して暗号化することが要求する場合には、UNIX NetBackup マスタサーバから以下のコマンドを（一行で）入力します。

```
bpinst -CRYPT -crypt_option required -crypt_strength 56
-class_names class1 class2
```

class1 および class2 が 40 ビット DES キーを使用した暗号化バックアップまたは非暗号化バックアップのいずれかを許可するように設定する場合には、Windows NT/2000 NetBackup マスタサーバから以下のコマンドを（一行で）入力します。

```
bpinst.exe -CRYPT -crypt_option allowed -crypt_strength 40 client1
client2
```


暗号化パスフレーズをクライアントへプッシュする

bpinstコマンドで-passphrase_promptまたは-passphrase_stdinオプションを使用してパスフレーズをNetBackupクライアントへ送信することができます。NetBackupクライアントは、キーファイル内のデータを作成したり、更新するのに、パスフレーズを使用します。キーファイルには、クライアントがDESキーを生成するために使用するデータが含まれています。なお、DESキーはバックアップを暗号化するために使用されます。

- -passphrase_promptオプションを使用する場合は、0から63文字のパスフレーズの入力を要求するプロンプトがターミナルで表示されます。パスフレーズ用に入力した文字列は画面には表示されません。パスフレーズを入力後に、入力した文字列が正しいかを確認するために、再度同じパスフレーズを入力する必要があります。
- -passphrase_stdinオプションを使用する場合は、標準入力でパスフレーズを二回入力する必要があります。一般的に、-passphrase_promptオプションの方が-passphrase_stdinよりも確固なセキュリティを持ちますが、bpinstをシェルスクリプト内で使用する場合には、-passphrase_stdinのほうが便利に実行できます。

標準入力を使用してUNIX NetBackupマスタサーバからclient1というクライアント用にパスフレーズを入力する場合は、以下のようにコマンドを入力します。

```
bpinst -CRYPT -passphrase_stdin client1 <<EOF
パスフレーズを入力します
パスフレーズを入力します
EOF
```

Windows NT/2000 NetBackupマスタサーバからclient2というクライアント用にパスフレーズを入力する場合は、以下のようにコマンドを入力します。

```
bpinst.exe -CRYPT -passphrase_prompt client2
Enter new NetBackup pass phrase: ********************
Re-enter new NetBackup pass phrase: ********************
```

新しいパスフレーズを入力することもできます。NetBackupクライアントは、キーファイル内に古いパスフレーズに関する情報を保持しているので、新しいパスフレーズを入力しても、古いパスフレーズで生成されたDESキーを使用して暗号化されたデータをリストアすることができます。

注意 古いものを含めた、パスフレーズは決して忘れないでください。クライアントのキーファイルが破損したり、無くなった場合には、キーファイルを再作成するのに、前のパスフレーズを含めたすべてのパスフレーズが必要になります。正しいキーファイルを再作成できない場合には、古いパスフレーズを使用して暗号化されたファイルをリストアすることはできなくなります。

多数のクライアント用に同一のパスフレーズを使用するかどうかを決める必要があります。同一のパスフレーズを使用すると、単一のbpinstコマンドで、各クライアント用にパスフレーズを設定することができるので大変便利です。また、同一のパスフレーズを使用するクライアント間で代替クライアントリストア処理を実行することができます。

注 代替クライアントリストア処理を実行しない場合には、各クライアント用に異なるパスフレーズを指定してください。この場合には、各クライアントごとに個別のbpinstコマンドを実行する必要があります。

NetBackup クラスで暗号化属性を設定する

各NetBackupクラスには暗号化属性が含まれています。

- 暗号化属性を有効に設定すると、NetBackupサーバはクラス内のNetBackupクライアントが暗号化バックアップを実行するように要求します。
- 暗号化属性を無効に設定すると、NetBackupサーバはクラス内のNetBackupクライアントが暗号化バックアップを実行するようには要求しません。

クラス用の暗号化属性を設定するには、NetBackup管理インタフェースを使用します。

また、bpinstコマンドを使用してNetBackupクラス用の暗号化属性を有効または無効に設定することもできます。複数のクラス用の属性を設定する場合には、この方法を使用すると大変便利です。

UNIX NetBackupマスタサーバからclass1とclass2用の暗号化属性を有効に設定する場合は、以下のようにコマンドを入力します。

```
bpinst -CRYPT -class_encrypt 1 -class_names class1 class2
```

1を指定すると、暗号化属性を有効に設定します（0は無効に設定します）。

クライアント上で NetBackup Encryption を設定する

Microsoft WindowsとUNIXクライアントの場合には、以下のトピックで説明するように、NetBackup Encryptionをクライアント上で直接設定することができます。

注 Macintoshクライアントの場合は、マスタサーバからNetBackup Encryptionを設定する必要があります。クライアント上で直接設定することはできません。

NetBackup Encryption ソフトウェアを入手する

クライアントがサーバに書き込み許可を与えていない場合は、マスタサーバの管理者からNetBackup Encryptionソフトウェアを入手する必要があります。UNIXやMacintoshクライアントでは、bp.confファイルにDISALLOW_SERVER_WRITESエントリが存在している場合には、サーバからの書き込みが許可されません。また、Microsoft Windowsクライアントでは、［NetBackup **管理**］ダイアログボックス（このダイアログボックスを開くには、クライアントユーザインタフェース内の**[アクション]**メニュー上で**[設定]**をクリックします）の［**一般**］タブで**[サーバ主動のリストアを有効化]**ボックスが選択されている場合は、サーバからの書き込みが許可されません。

特に指定しない限り、NetBackup Encryptionクライアントソフトウェアはマスタサーバの以下のディレクトリにインストールされています。

- Windows NT/2000マスタサーバ：

  install_path¥lib¥client

- UNIXマスタサーバ：

  /usr/openv/lib/client

クライアントディレクトリには、NetBackup Encryptionがサポートするさまざまなハードウェアプラットフォームに相当するハードウェアディレクトリ名が含まれています。ハードウェアディレクトリには、NetBackup Encryptionがサポートするさまざまなオペレーティングシステムに相当するオペレーティングシステムディレクトリ名が含まれています。オペレーティングシステムディレクトリには、ハードウェアやオペレーティングシステム用のNetBackupライブラリが含まれています。

ライブラリをマスタサーバからクライアント上の適切なディレクトリへコピーしてます。

クライアント上のディレクトリを指定するには、クライアント上でCRYPT_LIBPATH設定を使用します。

Microsoft Windowsクライアントのデフォルトディレクトリ：

install_path¥NetBackup¥bin

UNIXクライアントのデフォルトディレクトリ：

/usr/openv/lib

クライアントがSolaris 2であり、FTP経由でUNIX NetBackupマスタサーバからNetBackup Encryptionを取得することができる環境では、以下のコマンドを入力します：

```
cd /usr/openv
mkdir lib
cd lib
ftp master
ftp> cd /usr/openv/lib/client/Sun4/Solaris2
ftp> binary
ftp> mget *
ftp> quit
```

ライブラリ名：

libvdes40.*extension*
libvdes56.*extension*

.extension（拡張子）はプラットフォームよっては異なりますが、通常はso、sl、またはdllです。40ビットDESキーを使用する場合は、libvdes40.*extension*が必要です。56ビットDESキーを使用する場合は、libvdes40.*extension*とlibvdes56.*extension*の両方が必要です。

NetBackup Encryption設定オプションを管理する

NetBackupクライアントには、4つの暗号化に関連した設定オプションがあります。これらのオプションがクライアント用に正しく設定されていることを確認してください。

`CRYPT_OPTION = option`

NetBackupクライアント上で暗号化オプションを定義します。*option*に設定できる値は以下です：

`denied|DENIED`

クライアントが暗号化バックアップを許容しないように設定します。サーバが暗号化バックアップを要求すると、その要求はエラーとして扱われます。この値はこのオプションのデフォルト値です。

`allowed|ALLOWED`

クライアントが暗号化バックアップや非暗号化バックアップを許容するように設定します。

`required|REQUIRED`

クライアントが暗号化バックアップを要求するように設定します。サーバが非暗号化バックアップを要求すると、その要求はエラーとして扱われます。

`CRYPT_STRENGTH = strength`

NetBackupクライアント上の暗号化の*strength*（ビット長）を定義します。以下に、*strength*に設定できる値の例を示します：

`des_40|DES_40`

40ビットDESの暗号化を指定します。この値はこのオプションのデフォルト値です。

`des_56|DES_56`

56ビットDESの暗号化を指定します。

`CRYPT_LIBPATH = directory_path`

NetBackupクライアント上で暗号化ライブラリを含むディレクトリを指定します。

以下は、UNIXシステムにおけるデフォルト値です：

`/usr/openv/lib/`

以下は、Windows NT/2000、98、および95システムにおけるデフォルト値です：

install_path¥NetBackup¥bin¥

install_pathはNetBackupのインストール場所です。デフォルト値は`C:\VERITAS`です。

`CRYPT_KEYFILE = file_path`

NetBackupクライアント上で暗号キーを含むファイルを指定します。

以下は、Windows NT/2000、98、および95システムにおけるデフォルト値です：

install_path¥NetBackup¥bin¥keyfile.dat

以下は、UNIXシステムにおけるデフォルト値です：

/usr/openv/netbackup/keyfile

NetBackup暗号キーファイルを管理する

暗号化バックアップやリストアを実行するファイルが存在している各NetBackupクライアントにはキーファイルが必要です。キーファイルには、クライアントがDESキーを生成するために使用するデータが含まれています。このDESキーはバックアップを暗号化するために使用されます。

キーファイルを管理するには、クライアント上でbpkeyfileコマンドを使用します。詳細については、付録Aのbpkeyfileコマンドを参照してください。

キーファイルがまだ存在していない場合は、まずキーファイルを作成します。ファイル名は、CRYPT_KEYFILE設定オプションで指定したファイル名と同一にする必要があります。

- Windows NT/2000、98、および95システムにおけるデフォルトのキーファイル名：

  install_path¥NetBackup¥bin¥keyfile.dat

- UNIXシステムにおけるデフォルトのキーファイル名：

  /usr/openv/netbackup/keyfile

次に、キーファイルの暗号化方法を決定する必要があります。キーファイルは、キーファイルパスフレーズから生成されたDESキーによって暗号化されます。通常は、NetBackupアプリケーションにハードコードされた標準のキーファイルを使用しますが、より確固なセキュリティを追加する場合は、独自のキーファイルパスフレーズを使用します。詳細については、「その他のキーファイルセキュリティについて（UNIXクライアントのみ）」（20ページ）を参照してください。

注 「その他のキーファイルセキュリティについて（UNIXクライアントのみ）」（20ページ）に説明されているような、独自のキーファイルパスフレーズを使用して、より確固な保護対策を実施する必要がない場合は、新しいキーファイルパスフレーズを入力しないでください。代りに、標準キーパスフレーズを使用し、新しいNetBackupパスフレーズを入力してください（以下を参照）。

さらに、使用するNetBackupパスフレーズを決定する必要があります。NetBackupパスフレーズはキーファイル内に保存されているデータを生成するのに使用されます。NetBackup はこのデータを使用してバックアップを暗合化するためのDESキーを生成します。

標準キーファイルパスフレーズで暗号化されたデフォルトのキーファイルをUNIXクライアント上で作成する場合は、以下のコマンドを入力します：

```
bpkeyfile /usr/openv/netbackup/keyfile
Enter new key file pass phra se:(標準キーファイルパスフレーズ)
Re-enter new key file pass ph rase:(標準キーファイルパスフレーズ)
Enter new NetBackup pass phrase: **********************
```

```
Re-enter new NetBackup pass phrase: **********************
```

新しいパスフレーズを入力することもできます。NetBackup クライアントは、キーファイル内に古いパスフレーズに関する情報を保持しているので、新しいパスフレーズを入力しても、古いパスフレーズで生成された DES キーを使用して暗号化されたデータをリストアすることができます。新しい NetBackup パスフレーズを入力するには、`bpkeyfile` コマンドで `-change_netbackup_pass_phrase` または `-cnbpp` オプションを使用します。

Windows NT/2000 クライアント上で新しい NetBackup パスフレーズを入力する場合は、以下のコマンドを入力します :

```
bpkeyfile.exe -cnbpp install_path¥NetBackup¥bin¥keyfile.dat
Enter old key file pass phra se:(標準キーファイルパスフレーズ)
Enter new NetBackup pass phrase: **********
Re-enter new NetBackup pass phrase: **********
```

注意 古いものを含めた、パスフレーズは決して忘れないでください。クライアントのキーファイルが破損したり、無くなった場合には、キーファイルを再作成するのに、前のパスフレーズを含めたすべてのパスフレーズが必要になります。正しいキーファイルを再作成できない場合には、古いパスフレーズを使用して暗号化されたファイルをリストアすることはできなくなります。

キーファイルへのアクセス権はクライアントマシンの管理者のみが所有するようにしてください。すなわち、UNIX クライアントでは、ファイルの所有者が root で、モードが 600、およびファイルが NFS マウントが可能なファイルシステム上に存在しないことです。

キーファイルのバックアップの必要性も考慮に入れる必要があります。暗号化したバックアップに関しては、キーファイルがクライアント上に既に存在している場合にだけキーファイルをリストアすることができるので、キーファイルのバックアップはあまり意味を持ちません。

また、クライアントのキーファイルの非暗号化バックアップを実行する NetBackup クラスの作成も考慮に入れる必要があります。キーファイルを緊急リストアする場合に大変効果的です。ただしこの場合、あるクライアントの暗号化されていないキーファイルが他のクライアント上にリストアされる可能性があります。

キーファイルをバックアップから除くように設定するには、キーファイルのパス名をクライアントの除外リストへ追加する必要があります。

NetBackup クラスで暗号化を設定する

各 NetBackup クラスには暗号化属性が含まれています。この属性はマスタサーバ上で設定する必要があります。詳細については、「マスタサーバから設定する」（11 ページ）を参照してください。

その他のキーファイルセキュリティについて（UNIX クライアントのみ）

このセクションは、UNIX クライアントのみに適用できます。ここで説明されている追加セキュリティはWindows NT/2000、98、95、およびMacintosh クライアントでは利用できません。

クライアントもファイルを暗号化するために必要なキーファイルはDESキーを使用して暗号化されます。このDESキーは、キーファイルパスフレーズから生成されます。特に指定しない限り、NetBackup にハードコードされた標準キーファイルパスフレーズを使用して生成されたDESキーを使用してキーファイルを暗号化します。

標準パスフレーズを使用すると、非暗号化バックアップやリストアと同様に、自動化した暗号化バックアップやリストアを実行することができます。

ただし、特権を持たないユーザがクライアントのキーファイルへのアクセス権を取得すると、そのユーザが、バックアップに使用している暗号キーを解読したり、そのキーを利用して暗号化されたバックアップをリストアすることが可能になります。このような恐れがあるので、クライアントの管理者だけがキーファイルへのアクセスを持つようにしてください。

更に保護を確固にするために、独自のキーファイルパスフレーズを使用し、キーファイルを暗号化するのためのDESキーを生成することもできます。この場合、特権を持たないユーザがクライアントのキーファイルへのアクセス権を取得した場合でも、そのキーを利用してクライアントの暗号化したバックアップをリストアすることはより困難になります。

独自のキーファイルパスフレーズを使用する場合は、バックアップやリストアは以前のように自動化されません。以下に、独自のキーファイルパスフレーズを使用すると、UNIX NetBackup クライアント上でどのようなことが生じるかを説明します。

NetBackup サーバがクライアント上でバックアップやリストアを開始するときは、クライアント上のbpcdデーモンへ接続して要求を発行します。

通常は、bpcdはクライアント上の/etc/inetd.confファイルで設定されており、inetdデーモンを使用して起動されます。

暗号化バックアップやリストアを実行するには、bpcdがキーファイルの暗号を解読してそのファイルを読み取る必要があります。

標準キーファイルパスフレーズを使用する場合は、bpcdがキーファイルの暗号を自動的に解読することができます。bpcdを起動するのに、通常のinetdメソッドが使用されます。

独自のキーファイルパスフレーズを使用する場合は、bpcd がキーファイルの暗号を自動的に解読することはできず、inetdメソッドを使用することはできません。その際は、以下に説明にしたがって、bpcdをスタンドアロンプログラムとして起動する必要があります。

bpcdをスタンドアロンプログラムとして実行する

1. /etc/inetd.confファイルのbpcdエントリを削除するかコメントアウトします。bpcdエントリは以下のようなエントリです。

   ```
   bpcd stream tcp nowait root /usr/openv/netbackup/bin/bpcd bpcd
   ```

2. inetd が設定ファイルを再度読み取るように強制的に実行します。inetd に設定ファイルを強制的に再度読み込みさせる方法は、プラットフォームによって異なります。最も簡単な方法は、システムをリブートすることです。

3. キーファイルパスフレーズを変更します。bpkeyfile コマンドで -change_key_file_pass_phrase （または -ckfpp）オプションを使用します。例：

```
bpkeyfile -ckfpp /usr/openv/netbackup/keyfile
Enter old key file pass phrase:（標準キーファイルパスフレーズ）
Enter new key file pass phrase:（標準キーファイルパスフレーズ）
******
Re-enter new key file pass phrase:（標準キーファイルパスフレーズ）
******
```

プロンプトで「Return」キーを入力すると、標準キーファイルパススルーが使用されます。

4. bpcd をスタンドアロンプログラムとして起動します。起動するには、bpcd コマンドで -keyfile オプションを使用し、入力が要求されたら、新しいキーファイルパスフレーズを入力します。

```
bpcd -keyfile
Please enter key file pass phrase: ******
```

bpcd がバックグランドで実行され、NetBackup サーバからの要求を待ちます。

bpkeyfile コマンドと -ckfpp オプションを使用してキーファイルパスフレーズを変更することができます。新しいキーファイルパスフレーズは bpcd を次回起動すると有効になります。

bpkeyfile コマンドと -cnpp オプションを使用して NetBackup パスフレーズ（バックアップを暗号化するのに使用する DES キーを作成するのに使用）を変更することができます。ただし、新しい NetBackup パスフレーズは 現在の bpcd プロセスを強制終了し、再開するまで有効にはなりません。

bpcd を強制終了する

bpcd を強制終了するには、ps コマンドを使用して、プロセス ID を検索し、検出したプロセス ID に対して kill コマンドを発行します。その後、ps コマンドを再度実行して bpcd が強制終了されていることを確認します。通常の UNIX クライアント用には、ps コマンドで -e 引数を使用します。Solaris 4 や Auspex クライアント用には、ps コマンドで -ax 引数を使用します。

Solaris 2 クライアントから bpcd 強制終了する場合は以下のようにコマンドを実行します:

```
ps -e | grep bpcd
   148 ?        0:22 bpcd
kill 148
ps -e | grep bpcd
```


Auspex クライアントから bpcd 強制終了する場合は以下のようにコマンドを実行します:

```
ps -ax | grep bpcd
   389 ?  S     6:46  0:22 bpcd
kill 389
ps -ax | grep bpcd
```

コマンド A

この符録では、NetBackup Encryption 製品に特定なコマンドについて説明します。

コマンドの説明には、以下の表記規則を採用します。

- 角かっこ［ ］は、かっこ内のコマンドラインコンポーネントが必要に応じて指定可能なオプションであることを意味します。たとえば、あるコマンドが以下の形式を持つ場合：

  ```
  command [arg1]
  ```

  この場合、ユーザは arg1 を選択するか引数を省略することができます。

- 垂直バーまたはパイプ（| ）は、ユーザが選択可能なオプションの引数を区切る場合に使用します。たとえば、あるコマンドが以下の形式を持つ場合：

  ```
  command [arg1 | arg2]
  ```

  この場合、ユーザは arg1 または arg2 のいずれかを使用できます（両方は不可）。または引数を省略することができます。

- 斜体は、ユーザが指定する情報であることを示します。たとえば、以下のコマンドでは、ユーザが *directory* を指定します：

  ```
  -client_libraries directory
  ```


bpinst(1M)

名前

bpinst は -CRYPT オプションと一緒に使用すると、NetBackup Encryption をインストールしたり、設定することができます。

用法

```
bpinst -CRYPT [-client_libraries directory] [-crypt_option
        option] [-crypt_strength strength] [-passphrase_prompt
        |-passphrase_stdin] [-verbose] [ [-class_encrypt 0 |
        1] -class_names] name1 [name2 ... nameN]
```

注　このコマンドを使用するには、NetBackup Encryption が必要です。NetBackup Encryption は別途に購入してください。

説明

注　bpinst -CRYPT を使用して、まだ暗号化に関する設定を実行していないクライアント上で暗号化を設定する場合は、まずはじめに、bpinst コマンドを使用してクライアントへ暗号化ライブラリをプッシュし、その後別の bpinst コマンドで暗号化パスフレーズを設定してください。
例：

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client
clientname1

bpinst -CRYPT -passphrase_prompt clientname1
```

同じコマンドラインで -client_libraries と -passphrase_prompt の両方の引数を指定すると、暗号化ライブラリがクライアント上ではまだ利用できる状態ではないため、パスフレーズの設定に失敗します。

bpinst は、-CRYPT オプションと一緒に使用して、暗号化をサポートする NetBackup クライアント上に NetBackup Encryption をインストールしたり、暗号化の環境を設定することができます。UNIX では、コマンドは /usr/openv/netbackup/bin ディレクトリにあります。Windows NT/2000 では、コマンドは、*install_path*¥NetBackup¥bin ディレクトリにあります。

このコマンドを使用する前に、*NetBackup Encryption System Administrator's Guide* の第 2 章で説明されているように、まずサーバ上に暗号化ソフトウェアをインストールしてください。インストール後は、マスタサーバ上で bpinst -CRYPT を実行し、クライアン

トへの NetBackup Encryption のインストールおよび設定を実行します。このコマンドを実行するだけで、選択したクライアントへ必要なファイルをコピーし、さらにクライアントとサーバの両方で、必要な設定の変更を実行することができます。

注　DISALLOW_SERVER_FILE_WRITES NetBackup 設定オプションがクライアントで設定されていないことを確認してください。この設定オプションが設定されていると、サーバはクライアントへソフトウェアをインストールまたは設定することができません。

---

bpinst -CRYPT を使用して、class40 という名前のクラス内のすべての UNIX クライアントへ暗号化ソフトウェアをインストールし、必要な環境を設定するには、以下のように（一行で）入力します。

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client -crypt_option
allowed -crypt_strength des_40 -passphrase_prompt -class_encrypt 1
-class_names class40
```

上記のコマンドラインは -class_encrypt オプションを使用し、クラス用の暗号化属性を設定します。また、暗号化属性は、NetBackup 管理ユーティリティを使用して設定することもできます。

bpinst -CRYPT で使用できるオプションの説明については、オプション項を参照してください（特に、-passphrase_prompt オプションに注意してください）。

注　マスタサーバホストにインストールされているクライアント用の暗号化を設定することもできます。

オプション

-CRYPT　bpinst コマンドを使用して暗号化をインストールまたは設定する場合は、必ず、このオプションを一番目のオプションとして指定する必要があります。順序を変更したり、このオプションを省略しないでください。

-client_libraries *directory*

NetBackup クライアント上へ暗号化ライブラリをインストールします。このオプションでは、クライアント暗号化ライブラリを含むマスタサーバ上のディレクトリを指す必要があります：

UNIX サーバ上のライブラリディレクトリ：

install_path/lib/client

（デフォルトでは、install_path は /usr/openv です。）

Windows NT/2000 サーバ上でのライブラリディレクトリ：

ignore

-crypt_option *option*

NetBackup クライアントの CRYPT_OPTION 設定エントリを設定します。-crypt_option を指定しない場合は、クライアントは暗号化バックアップか非暗号化バックアップのいずれかを許可します（以下の ALLOWED を参照）。

option に指定できる値を以下に示します：

DENIED | denied | -1

クライアントが暗号化バックアップを許可しないように指定します。サーバが暗号化バックアップを要求すると、その要求はエラーとして扱われます。このオプションは、暗号用に設定されていないクライアントに対するデフォルト設定です。

ALLOWED | allowed | 0

クライアントが暗号化バックアップまたは非暗号化バックアップを許可するように指定します。この値はデフォルト値です。

REQUIRED |required | 1

クライアントが暗号化バックアップを要求するように指定します。サーバが非暗号化バックアップを要求すると、その要求はエラーとして見なされます。

-crypt_strength *strength*

NetBackup クライアント上の CRYPT_STRENGTH 設定エントリを設定します。このオプションを設定しない場合は、クライアント上の CRYPT_STRENGTH 設定エントリは変更されません。

strength に指定できる値：

DES_40 | des_40 | 40

40 ビット DES 暗号を指定します。このオプションは、暗号用に設定されていないクライアントに対するデフォルト設定です。

DES_56 | des_56 | 56

56 ビット DES 暗号を指定します。

-passphrase_prompt | -passphrase_stdin

注意　古いものを含めた、パスフレーズは決して忘れないでください。クライアントのキーファイルが破損したり、無くなった場合には、キーファイルを再作成するのに、前のパスフレーズを含めたすべてのパスフレーズが必要になります。正しいキーファイルを再作成できない場合には、古いパスフレーズを使用して暗号化されたファイルをリストアすることはできなくなります。

NetBackup はパスフレーズを使用して、各クライアント上のキーファイル内に保存するデータを作成します。作成後、NetBackup はそのキーファイル内のデータを使用して暗号キーを作成します。この暗号キーは、バックアップデータの暗号化および暗号の解読に必要なものです。

-passphrase_prompt オプションはパスフレーズの入力を要求するプロンプトを表示します。パスフレーズの文字は、実際に入力する際は表示されません。

-passphrase_stdin オプションは標準入力からパスフレーズを読み取ります。パスフレーズは 二回入力する必要があります。このオプションでは、パスフレーズが表示されるので、-passphrase_prompt オプションの方がこのオプションよりも確実なセキュリティを持ちますが、bpinst -CRYPT をシェルスクリプト内で使用する場合には、このオプションの方が便利です。

NetBackup は、bpinst -CRYPT で指定したすべてのクライアント用にパスフレーズを使用します。各クライアント用に異なるパスフレーズを指定する場合は、各クライアントごとに異なる bpinst -CRYPT コマンドを入力してください。

パスフレーズを指定すると、bpinst -CRYPT はクライアント上でキーファイルを作成または更新します。パスフレーズから生成される暗号キーは次のバックアップ用に使用されます。古い暗号キーは、前のバックアップのリストア用に、キーファイル内に保存されます。

-passphrase_prompt または-passphrase_stdin オプションを指定しない場合は、クライアント上のキーファイルは変更されません。

-verbose 各クライアントの現在の暗号に関する設定を表示します。また各クライアント上のインストール状況や再設定状況も表示されます。

-class_names

names で指定した名前が NetBackup クラス名であることを指定します。

-class_names オプションを使用する場合は、bpinst -CRYPT が、指定した各クラス内のすべてのクライアントをインストールし、設定します。-class_names オプションを省略した場合は、名前は NetBackup クライアント名として扱われます。

-class_encrypt 0 | 1

NetBackup クラス用に暗号化クラス属性を設定します。
-class_encrypt オプションを使用する場合には、-class_names オプションを使用する必要があります。
指定できる値：

0 は暗号化属性を無効（または無効の状態のままに設定）にするので、このクラスではサーバはクライアント用に暗号化を要求しません。この値は、暗号化用に設定されていないクラスに対するデフォルト値です。

1 は暗号化属性を設定するので、このクラスでは、サーバはクライアントに暗号化を要求します。

このオプションを指定しない場合は、クラス用の暗号化属性は変更されません。

name1 [*name2 ... nameN*]

-class_names オプションの使用状況によりますが、1 つまたは複数の NetBackup クライアント名またはクラス名を指定します。
-class_names オプションを省略した場合は、名前は NetBackup クライアント名として扱われます。

例

例 1

クライアントへのインストールやクライアントの設定を実行する前に、NetBackup マスタサーバ上に暗号化ライブラリをインストールする必要があります。ライブラリを mars という名前の NetBackup クライアントへインストールするには、以下のようにコマンドを（一行で）入力します。

UNIX の場合：

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client mars
```

Windows NT/2000 の場合：

```
bpinst.exe -CRYPT -client_libraries ignore mars
```

例 2

UNIX クライアント上で class40 という名前のクラスに 40 ビット DES 暗号をインストールし、設定するには、以下のようにコマンドを（一行で）入力します。

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client -crypt_option
allowed -crypt_strength des_40 -class_encrypt 1 -passphrase_prompt
-client_names class40
```

このコマンドは、-passphrase_prompt オプションを含むので、パスフレーズの入力を要求するプロンプトが表示されます。

```
Enter new NetBackup pass phrase: **********************
Re-enter new NetBackup pass phrase: **********************
```

例 3

strong という名前の NetBackup クライアントが、56 ビット DES 暗号を必ず使用するように指定するには、以下のようにコマンドを（一行で）入力します。

```
bpinst -CRYPT -crypt_option required -crypt_strength des_56 strong
```

例 4

strong という名前のクライアントの設定リストを表示するには、以下のようにコマンドを入力します。

```
bpinst -CRYPT -verbose strong
BPCD protocol version 3.1.0 on client strong
```

```
40-bit library version is 3.1.0.40 on client strong
56-bit library version is 3.1.0.56 on client strong
BPCD platform is sgi5 for client strong
Current configuration entries are:
CRYPT_KEYFILE = /usr/openv/netbackup/keyfile
CRYPT_LIBPATH = /usr/openv/lib
CRYPT_OPTION = 1
CRYPT_STRENGTH = 56
About to update 40-bit DES library for client strong
No update of 40-bit DES library required for client strong
About to update 56-bit DES library for client strong
No update of 56-bit DES library required for client strong
About to update NetBackup configuration for client strong
No update of NetBackup configuration required for client strong
About to update NetBackup pass phrase for client strong
No update of NetBackup pass phrase required for client strong
```

注

- `bpinst -CRYPT` がネットワークを介してクライアントへ送信するパスフレーズは、NetBackup40 ビット DES キーで暗号化されます。
- 各 NetBackup クライアント上のキーファイルは、NetBackup DES キーで暗号化されます。クライアントの設定状況によって、キー長 (40 ビットまたは 56 ビット) が異なります。キーファイルへのアクセスは、管理者に限定してください。UNIX クライアントでは、キーファイルの所有者は root で、モードは 600 に設定してください。またキーファイルを NFS を介してエクスポートできないように設定してください。
- パスフレーズは決して忘れないようにしてください。障害回復を実行する際には、`bpinst -CRYPT`を使用してクライアント上でキーファイルを再生成する必要がある場合があります。たとえば、orca という名前の NetBackup クライアントが暗号化バックアップを実行中に何らかの障害が発生し、orca のファイルが消失したとします。このような状況では、バックアップをリストアするために、クライアント上で暗号化ソフトウェアをインストールして設定する必要があります。

  以下に、暗号を使用した環境での基本的な障害回復の手段を示します（オペレーティングシステムと NetBackup のリストアについての詳細は、NetBackup Troubleshooting Guide を参照してください)。以下の例では、NetBackup クライアント名として orca を使用しています。

1. orca 上で OS を再インストールします。
2. orca 上で NetBackup クライアントソフトウェアを再インストールし、再設定します。
3. 以下のコマンド（一行）を実行し、orca 上で暗号を再インストールし、再設定します。

```
bpinst -CRYPT -client_libraries /usr/openv/lib/client -crypt_option
allowed -passphrase_prompt orca
Enter new NetBackup pass phrase: **********************
Re-enter new NetBackup pass phrase: **********************
```

ここで入力するパスフレーズは、orca で使用した一番初めのものです。

4. orca 上で使用した各パスフレーズ用に `bpinst -CRYPT` を連続して実行します。

```
# bpinst -CRYPT -passphrase_prompt orca
Enter new NetBackup pass phrase: **********************
Re-enter new NetBackup pass phrase: **********************
```

5. バックアップしたファイルを orca へリストアします。

ファイル

UNIX:

- UNIX サーバコマンド
  `/usr/openv/netbackup/bin/bpinst`
- クライアントライブラリを持つ UNIX サーバディレクトリ
  `/usr/openv/lib/client/`
- UNIX クライアント暗号ラ化イブラリ
  `/usr/openv/lib/libvdes*.*`
- UNIX クライアント暗号化キーファイル
  `/usr/openv/netbackup/keyfile`
- UNIX クライアント暗号化キーファイルユーティリティ
  `/usr/openv/netbackup/bpkeyfile`

Windows NT/2000、98、または 95:

- Windows NT/2000 サーバコマンド
  install_path¥NetBackup¥bin¥bpinst.exe
- クライアントライブラリを持つ Windows NT/2000 サーバディレクトリ
  install_path¥lib¥client¥
- Windows NT/2000、98、または 95 クライアント 暗号キーファイル
  install_path¥NetBackup¥bin¥keyfile.dat
- Windows NT/2000、98、または 95 クライアント暗号ライブラリ

install_path¥bin¥libvdes*.dll

- Windows NT/2000、98、または 95 クライアント暗号キーファイルユーティリティ
  install_path¥bin¥bpkeyfile.exe

Macintosh:

- Macintosh クライアント暗号ライブラリ
  :System Folder:Extensions:libvdes*.dll
- Macintosh client クライアント 暗号キーファイル
  :System Folder:Preferences:NetBackup:keyfile

bpkeyfile(1)

名前

bpkeyfile は NetBackup 用の暗号化キーファイルユーティリティです。

用法

```
bpkeyfile [-stdin] [-change_key_file_pass_phrase]
          [-change_netbackup_pass_phrase] [-display] key_file_path
```

使用制限

bpkeyfile コマンドは NetBackup Encryption オプションとだけに使用できます。

説明

bpkeyfile は、DES 暗号キーを生成するのに使用する情報を含むファイルを作成または更新します。この情報は、ユーザが提供する NetBackup パスフレーズに基づいて生成されます。キーファイルはユーザが提供するキーファイルパスフレーズによって暗号化されます。

NetBackup クライアントソフトウェアは、キーファイル内の情報から計算した暗号を使用してバックアップ中にファイルを暗号化し、リストア中にファイルの暗号を解読します。

ファイルが存在する場合は、現在のキーファイルパスフレーズの入力を要求するプロンプトが表示されます。

-change_key_file_pass_phrase を指定する場合は、新しいキーファイルパスフレーズの入力を要求するプロンプトが表示されます。空のパスフレーズを入力した場合は、標準キーパスフレーズが使用されます。

標準キーパスフレーズを使用する場合は、bpcd を自動的に実行することができます。独自のキーファイルパスフレーズを使用する場合は、*NetBackup Encryption System Administrator's Guide* の 第 3 章の「その他のキーファイルセキュリティについて (UNIX クライアントのみ)」で説明されているように、bpcd を -keyfile 引数と一緒に実行してください。

オプション

-stdin　標準入力からパスフレーズを読み取ります。特に指定しない限り、bpkeyfile はターミナル入力からパスフレーズを読み取ります。

-change_key_file_pass_phrase (or -ckfpp)
キーファイルを暗号化するのに使用するパスフレーズを変更します。

-change_netbackup_pass_phrase (or -cnpp)
クライアント上の NetBackup バックアップやアーカイブを暗号化するのに使用するパスフレーズを変更します。

`-display`
キーファイルに関する情報を表示します。

key_file_path
`bpkeyfile` によって作成されたり、更新されるキーファイルのパスを指定します。

注

NetBackup が使用するパスフレーズは 0 から 63 の文字列を含むことができます。システム間での互換性の問題を防ぐために、パスフレーズ内の文字には表示可能な ASCII 文字に限定してください。つまり、ASCII 照合順序のスペース（コード 32）からチルダ（コード 126）までの文字です。

ファイル

UNIX:

`/usr/openv/netbackup/keyfile`

（UNIX クライアント暗号キーファイル）

Windows NT/2000、98、または 95：

install_path¥NetBackup¥bin¥keyfile.dat

（Windows NT/2000、98、または 95 クライアント暗号キーファイル）