Symantec NetBackup™ セキュリティおよび暗号化ガイド

UNIX、Windows および Linux

リリース 7.7

Symantec

Symantec NetBackup™ セキュリティおよび暗号化ガイド

法的通知と登録商標

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec、Symantec ロゴ、Checkmark ロゴ、Veritas、Veritas ロゴは Symantec Corporation またはその関連会社の、米国およびその他の国における商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

本書に記載する製品は、使用、コピー、頒布、逆コンパイルおよびリバースエンジニアリングを制限するライセンスに基づいて頒布されています。Symantec Corporation からの書面による許可なく本書を複製することはできません。

Symantec Corporation が提供する技術文書は Symantec Corporation の著作物であり、Symantec Corporation が保有するものです。保証の免責: 技術文書は現状有姿のままで提供され、Symantec Corporation はその正確性や使用について何ら保証いたしません。技術文書またはこれに記載される情報はお客様の責任にてご使用ください。本書には、技術的な誤りやその他不正確な点を含んでいる可能性があります。Symantec は事前の通知なく本書を変更する権利を留保します。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商業用コンピュータソフトウェアと見なされ、場合に応じて、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202「Rights in Commercial Computer Software or Commercial Computer Software Documentation」、その後継規制の規定により制限された権利の対象となります。米国政府によるライセンス対象ソフトウェアおよび資料の使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

目次

第 1 章 NetBackup セキュリティの強化 12

NetBackup セキュリティおよび暗号化について 13
NetBackup セキュリティの実装レベル 13
世界レベルのセキュリティ 14
企業レベルのセキュリティ 15
データセンターレベルのセキュリティの概要 17
NetBackup アクセス制御 (NBAC) 17
世界レベル、企業レベルおよびデータセンターレベルの統合 22
NetBackup セキュリティの実装形式 23
オペレーティングシステムのセキュリティ 25
NetBackup セキュリティの脆弱性 25
NetBackup の標準セキュリティ 26
Media Server Encryption Option (MSEO) セキュリティ 27
クライアント側の暗号化セキュリティ 28
マスターサーバー、メディアサーバーおよび GUI での NBAC によるセキュリティ 30
すべてに NBAC を使用したセキュリティ 32
すべての NetBackup セキュリティ 33

第 2 章 セキュリティの配置モデル 36

ワークグループ 37
単一のデータセンター 37
複数のデータセンター 37
NetBackup を使用するワークグループ 38
標準の NetBackup を使用する単一のデータセンター 41
MSEO (Media Server Encryption Option) を使用する単一のデータセンター 44
クライアント側の暗号化を使用する単一のデータセンター 47
マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンター 49
すべてに NBAC を使用する単一のデータセンター 53
すべてのセキュリティが実装された単一のデータセンター 57
標準的な NetBackup を使用する複数のデータセンター 61
MSEO (Media Server Encryption Option) を使用する複数のデータセンター 65

クライアント側の暗号化を使用する複数のデータセンター 71
マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンター 76
すべてに NBAC を使用する複数のデータセンター 82
すべての NetBackup セキュリティを使用する複数のデータセンター 87

第 3 章 ポートセキュリティ 94

NetBackup TCP/IP ポートについて 94
NetBackup のデーモン、ポート、通信について 96
NetBackup の標準ポート 96
NetBackup マスターサーバーの外部接続ポート 97
NetBackup メディアサーバーの外部接続ポート 98
NetBackup 企業メディア管理 (EMM)サーバーの送信ポート 99
クライアントの外部接続ポート 100
Windows 管理コンソールおよび Java サーバーの外部接続ポート 100
Java コンソールの外部接続ポート 101
MSDP ポートの使用について 102
Cloud ポートの使用について 102
NetBackup と相互運用する製品のためのポートの追加情報 102
ポートの構成について 107
ランダムなポートの割り当ての有効化または無効化 108
NetBackup サーバーまたはクライアントのファイアウォール接続オプションの指定 109
接続元コンピュータから接続先コンピュータのファイアウォール接続オプションを指定する 112
構成ファイルのポート情報の編集 114
クライアント接続オプションの更新 115
vm.conf ファイルの Media Manager ポート設定の更新 115
NDMP バックアップのポート要件 118
サードパーティの製品とともに NetBackup を使う場合の既知のファイアウォールの問題 118

第 4 章 NetBackup 操作の監査 120

NetBackup の監査について 120
現在の監査設定の表示 123
NetBackup マスターサーバーでの監査の構成 123
監査レポートでのユーザーの識別情報 125
拡張監査について 126
拡張監査の有効化 127
拡張監査の設定 128
拡張監査でのメディアサーバーへの接続 128

NetBackup ドメイン間でのサーバー変更 128
サーバーの変更を NBAC または拡張監査と一緒に使った場合の設定要件 130
拡張監査の無効化 131
ホストプロパティの変更の監査 131
監査記録の保持とバックアップ 132
監査レポートの表示 132
-reason または -r option コマンドラインの使用 136
nbaudit ログの動作 137
監査エラーの監査アラート通知 138

第 5 章 アクセス制御のセキュリティ 140

NetBackup のアクセス制御について 140
ユーザー管理 141
ユーザー認証 143
Java インターフェース認証でのアクセス制御と拡張監査の影響 143

第 6 章 NetBackup アクセス制御セキュリティ (NBAC) 145

NetBackup アクセス制御 (NBAC) の使用について 149
NetBackup のアクセス管理 151
NBAC (NetBackup アクセス制御) 構成について 152
NetBackup アクセス制御 (NBAC) の構成 152
NBAC の構成の概要 153
スタンドアロンのマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成 154
クラスタでの高可用性の NetBackup マスターサーバーのインストール 155
クラスタ化されたマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成 155
メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成 156
クライアントでのアクセス制御のインストールおよび構成 158
ブローカーと Windows リモートコンソール間の信頼関係の確立 160
NBAC の構成コマンドの概略 160
NetBackup アクセス制御 (NBAC) のアップグレード 165
NetBackup ホットカタログバックアップへの認証データベースおよび認可データベースの追加について 165
NetBackup の古いバージョンがリモートコンピュータにインストールされているルートブローカーを使っている場合の NetBackup のアップグレード 165
NetBackup 7.0 より前のメディアサーバーおよびクライアントコンピュータの NetBackup アクセス制御 (NBAC) の構成 170
［アクセス制御 (Access Control)］ホストプロパティの手動構成 171

NetBackup 管理インフラストラクチャと setuptrust コマンドの統合 172
setuptrust コマンドの使用 173
マスターサーバーおよびメディアサーバーのホストプロパティへのアクセス 174
［アクセス制御 (Access Control)］ホストプロパティ 174
［ネットワーク設定 (Network Settings)］タブ 175
［認証ドメイン (Authentication Domain)］タブ 176
［認可サービス (Authorization Service)］タブ 178
クライアントのホストプロパティへのアクセス 179
クライアントの［アクセス制御 (Access Control)］ホストプロパティダイアログボックス 180
クライアントの［認証ドメイン (Authentication Domain)］タブ 181
クライアントの［ネットワーク設定 (Network Settings)］タブ 182
アクセス管理のトラブルシューティングのガイドライン 182
NetBackup Authentication and Authorization の構成とトラブルシューティング 183
NBAC の問題のトラブルシューティング 189
UNIX の検証手順について 190
UNIX マスターサーバーの検証 191
UNIX メディアサーバーの検証 194
UNIX クライアントの検証 196
UNIX マスターサーバーが存在する複合環境での検証項目 198
複合環境の UNIX マスターサーバーのマスターサーバーでの検証項目 200
複合環境の UNIX マスターサーバーのメディアサーバーでの検証項目 200
複合環境の UNIX マスターサーバーのクライアントでの検証項目 202
Windows マスターサーバーが存在する複合環境での検証項目 203
複合環境の Windows マスターサーバーのマスターサーバーでの検証項目 206
複合環境の Windows マスターサーバーのメディアサーバーでの検証項目 206
複合環境の Windows マスターサーバーのクライアントでの検証項目 208
Windows での検証項目 209
Windows マスターサーバーでの検証項目 211
Windows メディアサーバーでの検証項目 215
Windows クライアントでの検証項目 217
アクセス管理ユーティリティの使用 219
nbac_cron ユーティリティについて 220
nbac_cron ユーティリティの使用 220
NetBackup へアクセス可能なユーザーの決定について 222
個々のユーザー 223
ユーザーグループ 224

NetBackup のデフォルトユーザーグループ 225
ユーザーグループの構成 227
新しいユーザーグループの作成 227
既存のユーザーグループのコピーによる新しいユーザーグループの作成 228
ユーザーグループの名前の変更 228
[一般 (General)]タブ 229
[ユーザー (Users)]タブ 229
[ユーザー (Users)]タブの[定義されているユーザー (Defined Users)]ペイン 230
[ユーザー (Users)]タブの[割り当て済みのユーザー (Assigned Users)]ペイン 231
ユーザーグループへの新しいユーザーの追加 231
ユーザーグループおよびユーザーの定義について 231
新しいユーザーとしてのログオン 233
ユーザーグループへのユーザーの割り当て 233
[アクセス権 (Permissions)]タブ 234
認可オブジェクトおよび権限について 234
権限の付与 236
NetBackup ユーザーグループの特定のユーザー権限の表示 237
認可オブジェクト 238
メディアの認可オブジェクトの権限 239
ポリシーの認可オブジェクトの権限 239
ドライブの認可オブジェクトの権限 240
レポートの認可オブジェクトの権限 240
NBU_Catalog の認可オブジェクトの権限 241
ロボットの認可オブジェクトの権限 241
ストレージユニットの認可オブジェクトの権限 242
ディスクプールの認可オブジェクトの権限 242
バックアップおよびリストアの認可オブジェクトの権限 243
ジョブの認可オブジェクトの権限 244
サービスの認可オブジェクトの権限 244
ホストプロパティの認可オブジェクトの権限 245
ライセンスの認可オブジェクトの権限 245
ボリュームグループの認可オブジェクトの権限 246
ボリュームプールの認可オブジェクトの権限 246
デバイスホストの認可オブジェクトの権限 247
セキュリティの認可オブジェクトの権限 247
ファットサーバーの認可オブジェクトの権限 248
ファットクライアントの認可オブジェクトの権限 248
Vault の認可オブジェクトの権限 249
サーバーグループの認可オブジェクトの権限 249
キー管理システム (kms) グループの認可オブジェクトの権限 249

第 7 章 格納データの暗号化セキュリティ 251
格納データの暗号化に関する用語 253
格納データの暗号化に関する制限事項 253
暗号化セキュリティについて考慮する際の質問 255
NetBackup 格納データの暗号化オプション 256
暗号化オプションの比較 256
オプション 1 - NetBackup クライアントの暗号化 257
暗号化を使用したバックアップの実行について 257
バックアップの暗号化の選択について 258
標準暗号化を使用したバックアップ処理 258
レガシー暗号化を使用したバックアップ処理 259
NetBackup 標準暗号化を使用したリストア処理 260
NetBackup レガシー暗号化を使用したリストア処理 261
暗号化セキュリティのインストール前提条件 262
UNIX 版 NetBackup サーバーへの暗号化のインストール 262
Windows 版 NetBackup サーバーへの暗号化のインストール 263
UNIX 版 NetBackup クライアントへの暗号化のローカルインストールについて 263
Windows 版 NetBackup クライアントへの暗号化のローカルインストールについて 263
クライアントでの標準暗号化の構成について 263
標準暗号化の構成オプションの管理 264
NetBackup 暗号化鍵ファイルの管理 265
サーバーからの標準暗号化の構成について 266
クライアントノードでの暗号化鍵ファイルの作成について 266
鍵ファイルの作成 267
鍵ファイルのリストアの推奨する実施例 268
鍵ファイルのパスフレーズを保護するための手作業による保存 268
鍵ファイルの自動バックアップ 268
暗号化されたバックアップファイルの、異なるクライアントへのリストア 269
クライアントでの標準暗号化の直接的な構成について 270
ポリシーでの標準暗号化属性の設定 270
NetBackup サーバーからのクライアントの暗号化設定の変更 270
レガシー暗号化の構成について 271
サーバーからのレガシー暗号化の構成について 271
レガシー暗号化構成オプション 272
クライアントへのレガシー暗号化構成のプッシュインストールについて 274
クライアントへのレガシー暗号化パスフレーズのプッシュインストールについて 275
レガシー暗号化鍵ファイルの管理 276
別のクライアントで作成されたレガシー暗号化が使用されたバックアップのリストア 278

ポリシーでのレガシー暗号化属性の設定について 279
サーバーからのクライアントのレガシー暗号化設定の変更 280
UNIX 版クライアントのレガシー鍵ファイルの追加によるセキュリティの向上 280
bpcd -keyfile コマンドの実行 281
UNIX クライアントでの bpcd の終了 282
オプション 2 - メディアサーバーの暗号化 282
メディアサーバー暗号化オプション管理 283

第 8 章 格納するデータのキーマネージメントサービス 284

FIPS (連邦情報処理標準) 287
FIPS 対応 KMS について 287
キーマネージメントサービス (Key Management Service: KMS) の概要 289
KMS の注意事項 290
KMS の操作原理 294
暗号化テープへの書き込みの概要 294
暗号化テープの読み取りの概要 295
KMS の用語 295
KMS のインストール 297
KMS の NBAC との使用 301
HA クラスタに使用する KMS のインストールについて 301
クラスタでの KMS サービスの有効化 302
KMS サービスの監視の有効化 302
KMS サービスの監視の無効化 303
監視対象リストからの KMS サービスの削除 303
KMS の構成 303
キーデータベースの作成 304
キーグループとキーレコードについて 305
キーグループの作成について 306
キーレコードの作成について 306
キーレコードの状態の概要 307
キーレコードの状態に関する注意事項 308
キーレコードの prelive 状態 309
キーレコードの active 状態 309
キーレコードの inactive 状態 309
キーレコードの deprecated 状態 310
キーレコードの terminated 状態 310
KMS データベースファイルのバックアップについて 310
すべてのデータファイルのリストアによる KMS のリカバリについて 311
KMS データファイルのみのリストアによる KMS のリカバリ 311
データ暗号化キーの再生成による KMS のリカバリ 311

KMS データファイルのバックアップに関する問題 312
KMS データベースファイルのバックアップソリューション 313
キーレコードの作成 313
主要グループからのキーのリスト 314
KMS と連携するための NetBackup の構成 315
NetBackup および KMS のキーレコード 315
テープ暗号化を使用するための Netbackup の設定例 316
暗号化への KMS の使用について 318
暗号化テープバックアップの実行例 319
暗号化バックアップの確認例 319
KMS 暗号化イメージのインポートについて 320
KMS データベースの要素 320
空の KMS データベースの作成 321
KPK ID および HMK ID の重要性 321
HMK および KPK の定期的な更新について 322
KMS キーストアおよび管理者キーのバックアップ 322
コマンドラインインターフェース (CLI) コマンド 322
CLI の使用方法のヘルプ 324
新しいキーグループの作成 324
新しいキーの作成 325
キーグループの属性の変更 325
キーの属性の変更 326
キーグループの詳細の取得 326
キーの詳細の取得 327
キーグループの削除 328
キーの削除 328
キーのリカバリ 329
KMS データベースからのキーのエクスポートと KMS データベースへの
キーのインポートについて 329
キーのエクスポート 330
キーのインポート 331
ホストマスターキー (HMK) の変更 333
ホストマスターキー (HMK) ID の取得 333
キーの保護キー (KPK) ID の取得 334
キーの保護キー (KPK) の変更 334
キーストアの統計の取得 334
KMS データベースの静止 334
KMS データベースの静止解除 335
キーの作成オプション 335
KMS のトラブルシューティング 336
バックアップが暗号化されていない問題の解決方法 336
リストアが復号化されない問題の解決方法 337

トラブルシューティングの例 - active キーレコードが存在しない場合のバックアップ 337
トラブルシューティングの例 - 不適切なキーレコード状態でのリストア 341

索引 343

1

NetBackup セキュリティの強化

この章では以下の項目について説明しています。

- NetBackup セキュリティおよび暗号化について
- NetBackup セキュリティの実装レベル
- 世界レベルのセキュリティ
- 企業レベルのセキュリティ
- データセンターレベルのセキュリティの概要
- NetBackup アクセス制御 (NBAC)
- 世界レベル、企業レベルおよびデータセンターレベルの統合
- NetBackup セキュリティの実装形式
- オペレーティングシステムのセキュリティ
- NetBackup セキュリティの脆弱性
- NetBackup の標準セキュリティ
- Media Server Encryption Option (MSEO) セキュリティ
- クライアント側の暗号化セキュリティ
- マスターサーバー、メディアサーバーおよび GUI での NBAC によるセキュリティ
- すべてに NBAC を使用したセキュリティ
- すべての NetBackup セキュリティ

NetBackup セキュリティおよび暗号化について

NetBackup のセキュリティと暗号化は NetBackup のマスターサーバー、メディアサーバー、接続クライアントですべての NetBackup 操作を保護します。また、サーバーとクライアントが動作しているオペレーティングシステムも保全されます。バックアップデータは暗号化処理と Vault 処理によって保護されます。ネットワークで送信される NetBackup データは安全な専用ネットワークポートによって保護されます。

NetBackup セキュリティおよび暗号化の各レベルと実装について、次のトピックで説明します。

p.13 の「NetBackup セキュリティの実装レベル」を参照してください。

p.17 の「NetBackup アクセス制御 (NBAC)」を参照してください。

p.25 の「オペレーティングシステムのセキュリティ」を参照してください。

p.26 の「NetBackup の標準セキュリティ」を参照してください。

p.27 の「Media Server Encryption Option (MSEO) セキュリティ」を参照してください。

p.28 の「クライアント側の暗号化セキュリティ」を参照してください。

p.30 の「マスターサーバー、メディアサーバーおよび GUI での NBAC によるセキュリティ」を参照してください。

p.32 の「すべてに NBAC を使用したセキュリティ」を参照してください。

p.33 の「すべての NetBackup セキュリティ」を参照してください。

NetBackup セキュリティの実装レベル

NetBackup セキュリティの実装において、世界レベルは非常に広義な概念であり、エンタープライズレベルではより詳細化します。データセンターレベルではセキュリティは固有のものになります。

表 1-1 は NetBackup セキュリティレベルがどのように実装することができるか示します。

表 1-1 NetBackup セキュリティの実装レベル

セキュリティレベル	説明
世界レベル	Web サーバーアクセスと、発送されたり Vault に格納されたりする暗号化されたテープを指定します
企業レベル	内部ユーザーおよびセキュリティ管理者を指定します
データセンターレベル	NetBackup 操作を指定します

世界レベルのセキュリティ

世界レベルのセキュリティでは、外部ユーザーはファイアウォールで保護されている企業の Web サーバーにアクセスでき、暗号化されたテープを発送したりオフサイト Vault に格納したりできます。世界レベルのセキュリティは企業レベルおよびデータセンターのレベルを網羅します。

図 1-1　　世界レベルのセキュリティのスコープ

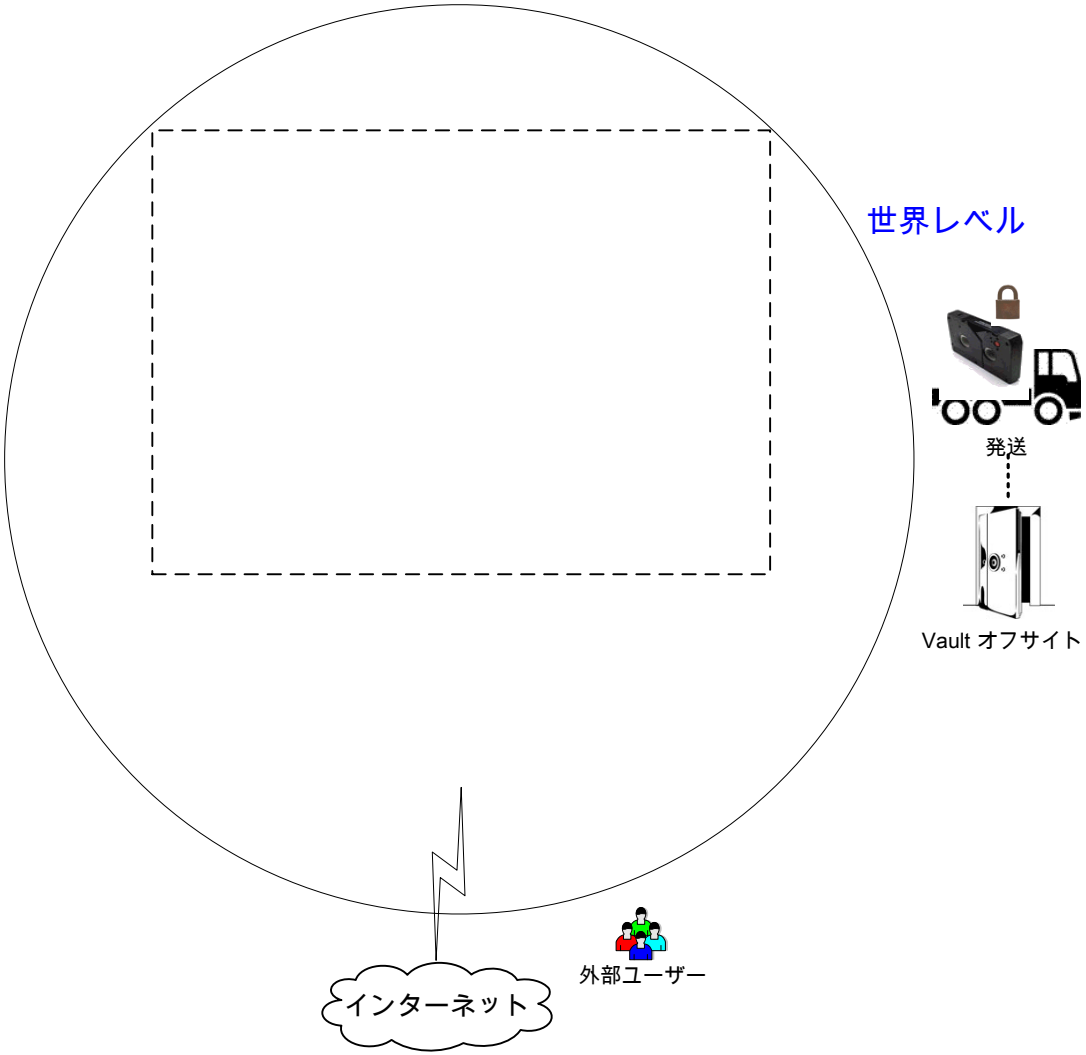


表 1-2　世界レベルのセキュリティの種類

型	説明
世界レベルの外部ユーザー	外部ユーザーはファイアウォールで保護されている Web サーバーにアクセスできます。NetBackup ポートへのアクセスは外部ファイアウォールによって遮断されるため、外部ユーザーはインターネットから NetBackup の機能にアクセスしたり、機能を使用したりすることはできません。
世界レベルのインターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。HTTP ポートを使用してファイアウォールを通過することで、インターネットから企業の Web サーバーにアクセスできます。
世界レベルの WAN	WAN (ワイドエリアネットワーク) は、セキュリティの概要の図には表示されていません。WAN は、地理的に分散している NetBackup のデータセンターをリンクするために使用される専用の高速接続です。
世界レベルのトランスポート	トランスポートトラックにより、暗号化されたクライアントテープがセキュリティ保護されたオフサイト Vault 施設に運ばれます。
世界レベルのオフサイト Vault	暗号化されたテープが現在のデータセンター以外の安全なストレージ機能で管理できることを示します。

企業レベルのセキュリティ

企業レベルのセキュリティは NetBackup セキュリティの実装のうちより目に見える部分を含んでいます。企業レベルには、内部ユーザー、セキュリティ管理者、データセンターレベルが含まれます。

図 1-2　企業レベルのセキュリティのスコープ

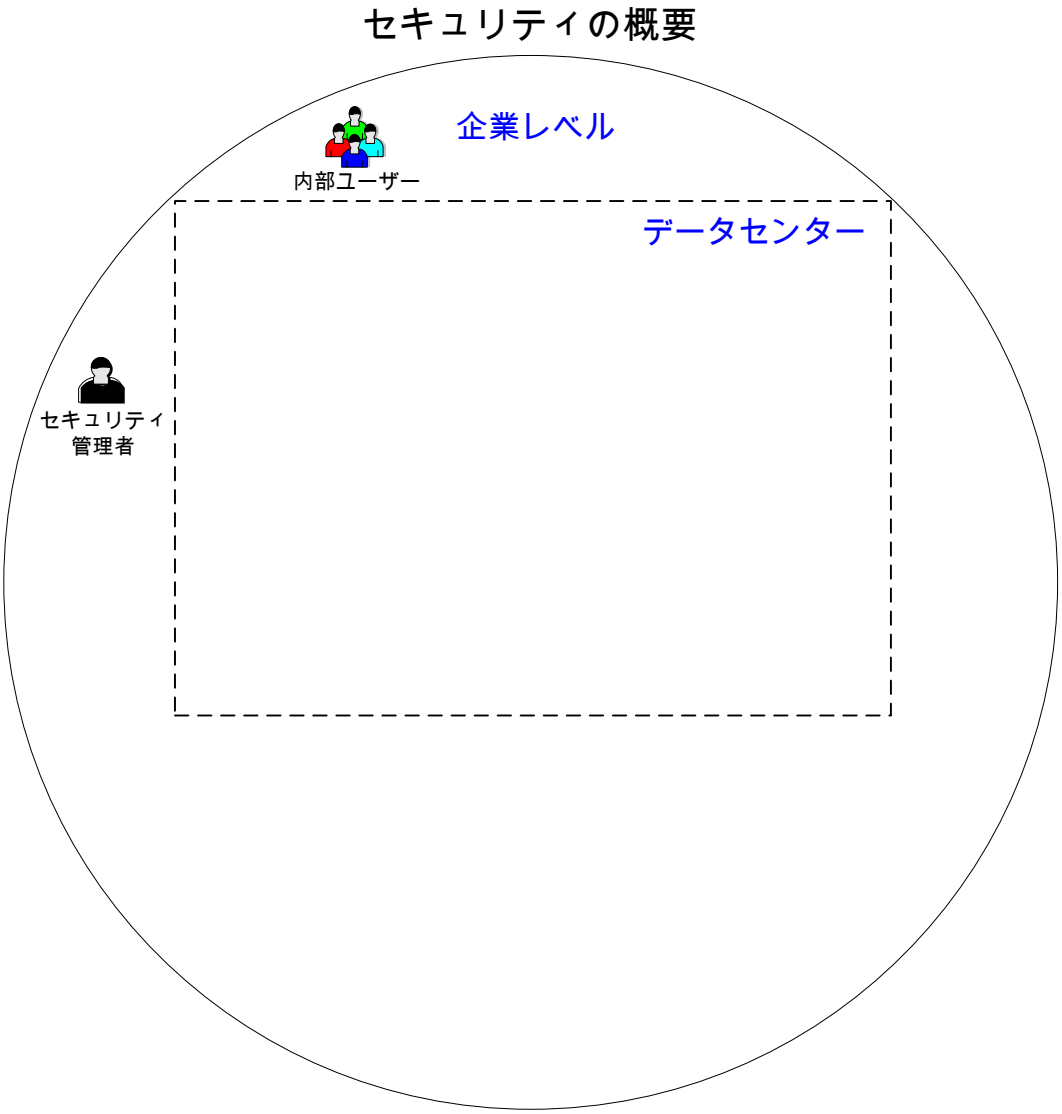


表 1-3　企業レベルのセキュリティの種類

型	説明
内部ユーザー	データセンター内部からの NetBackup 機能へのアクセスおよび機能の使用を許可されるユーザーを示します。通常、内部ユーザーには、データベース管理者、バックアップ管理者、オペレータ、一般のシステムユーザーなどが混在しています。
セキュリティ管理者	データセンター内部から NetBackup セキュリティ機能に対してアクセスおよび管理を行う管理者権限が付与されているユーザーを示します。

データセンターレベルのセキュリティの概要

データセンターレベルのセキュリティは NetBackup セキュリティ機能の中心です。データセンターレベルのセキュリティは、ワークグループ、単一のデータセンター、または複数のデータセンターで構成される場合があります。

表 1-4 はデータセンターレベルのセキュリティ固有の展開モデルを説明します。

表 1-4　データセンターレベルのセキュリティのための展開モデル

型	説明
ワークグループ	完全に内部で NetBackup を使用する小規模な (50 未満の) システムグループ。
単一のデータセンター	中規模から大規模な (50 を超える) ホストのグループを示し、DMZ 内のホストをバックアップできます。
複数のデータセンター	2 つ以上の地域にまたがる、中規模から大規模な (50 を超える) ホストのグループを示します。WAN によって接続できます。この構成には、バックアップ対象の DMZ 内のホストを含めることもできます。

p.13 の「NetBackup セキュリティの実装レベル」を参照してください。

NetBackup アクセス制御 (NBAC)

NetBackup アクセス制御 (NBAC) 機能は、NetBackup に NetBackup Product Authentication and Authorization を組み込んで、マスターサーバー、メディアサーバー、およびクライアントのセキュリティを高めます。

p.13 の「NetBackup セキュリティおよび暗号化について」を参照してください。

次に、NBAC に関する重要事項を示します。

- 認証および認可は組み合わせて使用します。

- NBAC は信頼できるソースからの認証 ID を使用して、関連のあるパーティを確実に識別します。これらの ID に基づき、NetBackup 操作に対するアクセスが決定されます。NetBackup 7.1 のリリースでは、セキュリティサービスが組み込まれていることに注意してください。

メモ: 7.0 より前の NetBackup バージョンのメディアサーバーとクライアントでは、ICS インストールディスク上の NetBackup Product Authentication and Authorization インストールキットから追加のコンポーネントが必要です。NetBackup 7.0 には、AT と AZ 用のクライアントがすでに含まれています。

- NetBackup Product Authentication and Authorization は、ルートブローカー、認証ブローカー、認可エンジン、および GUI で構成されています。
- Oracle、Oracle Archiver、DB2、Informix、Sybase、SQL Server、SAP および EV Migrator は NBAC でサポートされません。
- NBAC はアプライアンスでサポートされません。
- NetBackup カタログバックアップは NBAC でサポートされます。

次の表は、セキュリティで使われる NetBackup コンポーネントを記述したものです。

表 1-5 セキュリティで使われる NetBackup コンポーネント

コンポーネント	説明
ルートブローカー	データセンターのインストールでは、NetBackup 7.6 マスターサーバーがルートブローカーです。別のルートブローカーを使うためのプロビジョニングは必要ありません。ルートブローカー間の信頼を許可することをお勧めします。 **メモ:** 7.0 より前の NetBackup インストールでは 1 つのルートブローカーのみがデータセンターのインストールに必要でした。ルートブローカーは、認証ブローカーと組み合わせて使用することもできました。 ルートブローカーは認証ブローカーを認証します。ルートブローカーはクライアントを認証しません。
認証ブローカー	マスターサーバー、メディアサーバー、GUI およびクライアントのそれぞれにクレデンシャルを設定して認証します。認証ブローカーは、コマンドプロンプトを操作するユーザーも認証します。データセンターのインストールでは、複数の認証ブローカーを配置できます。認証ブローカーをルートブローカーと組み合わせて使用することもできます。
認可エンジン	マスターサーバーおよびメディアサーバーと通信して、認証済みユーザーの権限を決定します。これらの権限によって、指定したサーバーで利用可能な機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。データセンターのインストールには、認可エンジンが 1 つのみ必要です。認可エンジンは WAN を介して通信し、複数のデータセンター環境にある他のメディアサーバーを認可します。

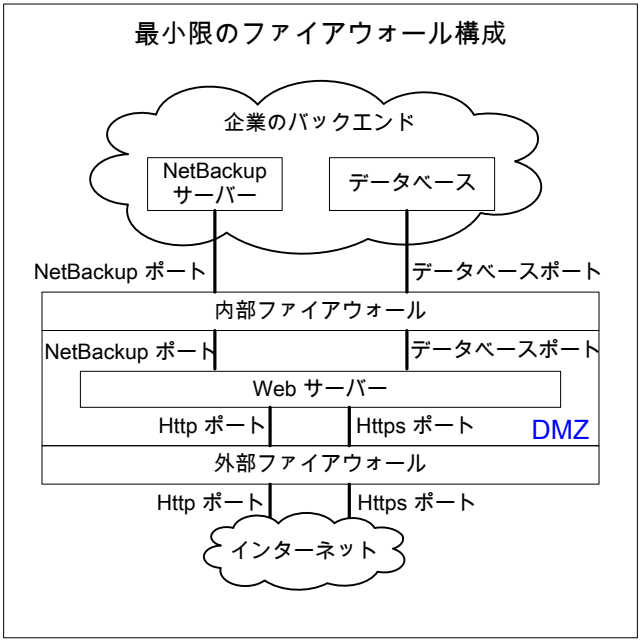
コンポーネント	説明
GUI	認証ブローカーからクレデンシャルを受信するリモート管理コンソールを示します。GUI は受け取ったクレデンシャルを使用して、クライアント、メディアサーバーおよびマスターサーバーの機能へのアクセス権を取得できます。
MSEO	メディアサーバーによってテープに書き込まれるデータを暗号化 (格納データの暗号化) するソフトウェア装置である MSEO (Media Server Encryption Option) を指定します。MSEO ではクライアント側の暗号化が代行されるため、クライアントの CPU 処理負荷を軽減できます。
マスターサーバー	ルートブローカー、認証ブローカー、GUI、認可エンジン、メディアサーバーおよびクライアントと通信します。
NetBackup 管理者	データセンター内部から NetBackup 機能に対してアクセスおよび管理を行う管理者権限が付与されているユーザーを示します。
メディアサーバー	マスターサーバー、ルートブローカー、認証ブローカー、認可エンジン、MSEO および 1 から 6 までのクライアントと通信します。メディアサーバーは、クライアント 5 の暗号化されていないデータと、クライアント 6 の暗号化されたデータをテープに書き込みます。
クライアント	クライアント 1 から 4 までは、標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。クライアント 6 は、クライアント側で暗号化を行う形式のクライアントで、同じく DMZ に配置されています。いずれの形式のクライアントもマスターサーバーによって管理され、クライアントのデータはメディアサーバーによってテープにバックアップされます。クライアント 5 および 6 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5 は http ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。
テープ	NetBackup のテープセキュリティは、次の機能を追加することによって強化できます。 ■ クライアント側の暗号化 ■ MSEO (Media Server Encryption Option) ■ 蓄積データの暗号化 暗号化されていないデータおよび暗号化されているデータのテープはデータセンターで作成されます。1 から 5 までのクライアントの場合は、暗号化されていないテープデータが書き込まれ、データセンターのオンサイトに格納されます。クライアント 6 の場合は、暗号化されたテープが書き込まれ、ディザスタリカバリ保護に使用するためオフサイト Vault に発送されます。

コンポーネント	説明
暗号化	NetBackup の暗号化は、次のようにセキュリティを高めることができます。 ■ データの機密性が向上する ■ すべてのデータを効果的に暗号化することによって、物理テープの損失がそれほど重大ではなくなる ■ 最もよい危険軽減方法である 暗号化についての詳細 p.255 の「暗号化セキュリティについて考慮する際の質問」を参照してください。
回線上のデータセキュリティ	マスターサーバー、メディアサーバー、クライアント間の通信、およびポートを使用してファイアウォールを通過する通信と WAN を介した通信が含まれます。 ポートについての詳細 p.94 の「NetBackup TCP/IP ポートについて」を参照してください。 NetBackup では、次の手段を使用して、回線上のデータのセキュリティを強化することができます。 ■ NetBackup アクセス制御 (NBAC) ■ 従来の NetBackup デーモンは NBAC が有効な場合に認証を使用する ■ CORBA デーモンは完全に暗号化されたチャネルを使用して機密性を確保し、データの整合性を提供する ■ ファイアウォール ■ NetBackup とそのほかの製品での未使用ポートの無効化 p.108 の「ランダムなポートの割り当ての有効化または無効化」を参照してください。 ■ PBX および VNETD の専用ポートを使用して NetBackup セキュリティを強化する ■ ファイアウォールを介してアクセスを監視および許可する中央ポートセット

コンポーネント	説明
ファイアウォールセキュリティ	NetBackup のファイアウォールサポートはセキュリティを高めるうえで役立ちます。 ファイアウォールのセキュリティに関する重要事項を次に示します。 ■ NetBackup でファイアウォールおよび侵入検知保護を使用することをお勧めします。 ■ NetBackup の観点では、ファイアウォール保護は一般的なネットワークセキュリティに関連します。ファイアウォール保護では、泥棒がピッキングを試みる「ドアロック」の可能性を減らすことに重点が置かれます。NFS、telnet、FTP、電子メールなどに使用されるポートをブロックをすると有効な場合があります。これらのポートは必ずしも NetBackup に必要ではなく、迷惑なアクセスの侵入口となる可能性があります。 ■ マスターサーバーを最大限に保護してください。 ■ ファイアウォールには、次に示すように内部ファイアウォールおよび外部ファイアウォールがあります。 　■ 内部ファイアウォール - NetBackup は、DMZ 内の Web サーバークライアント 5 と暗号化クライアント 6 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、内部ファイアウォールを通過して DMZ とのデータ通信を行うことができます。HTTP ポートは外部ファイアウォールで開かれており、内部ファイアウォールを通過できません。 　■ 外部ファイアウォール - 外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
非武装地帯 (DMZ)	非武装地帯 (DMZ) は、次のようにセキュリティを高めます。 ■ DMZ は、特定のホストが使用できるポート数が高度に制御される、制限された領域です。 ■ DMZ は、外部ファイアウォールと内部ファイアウォールの間に存在します。この例での共通領域は、Web サーバーです。外部ファイアウォールでは、HTTP (標準) および HTTPS (セキュリティ保護) の Web ポートを除いたすべてのポートがブロックされます。内部ファイアウォールでは、NetBackup ポートおよびデータベースポートを除いたすべてのポートがブロックされます。DMZ を使用することで、内部の NetBackup サーバーおよびデータベース情報に外部インターネットからアクセスすることができなくなります。 DMZ は、内部ファイアウォールと外部ファイアウォールの間の Web サーバークライアント 5 および暗号化クライアント 6 に対して「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 図 1-3 に、DMZ を持つ内部ファイアウォールと外部ファイアウォールの例を示します。

次の図は DMZ を持つ内部ファイアウォールと外部ファイアウォールの例を示します。

図 1-3　ファイアウォールおよび DMZ の例

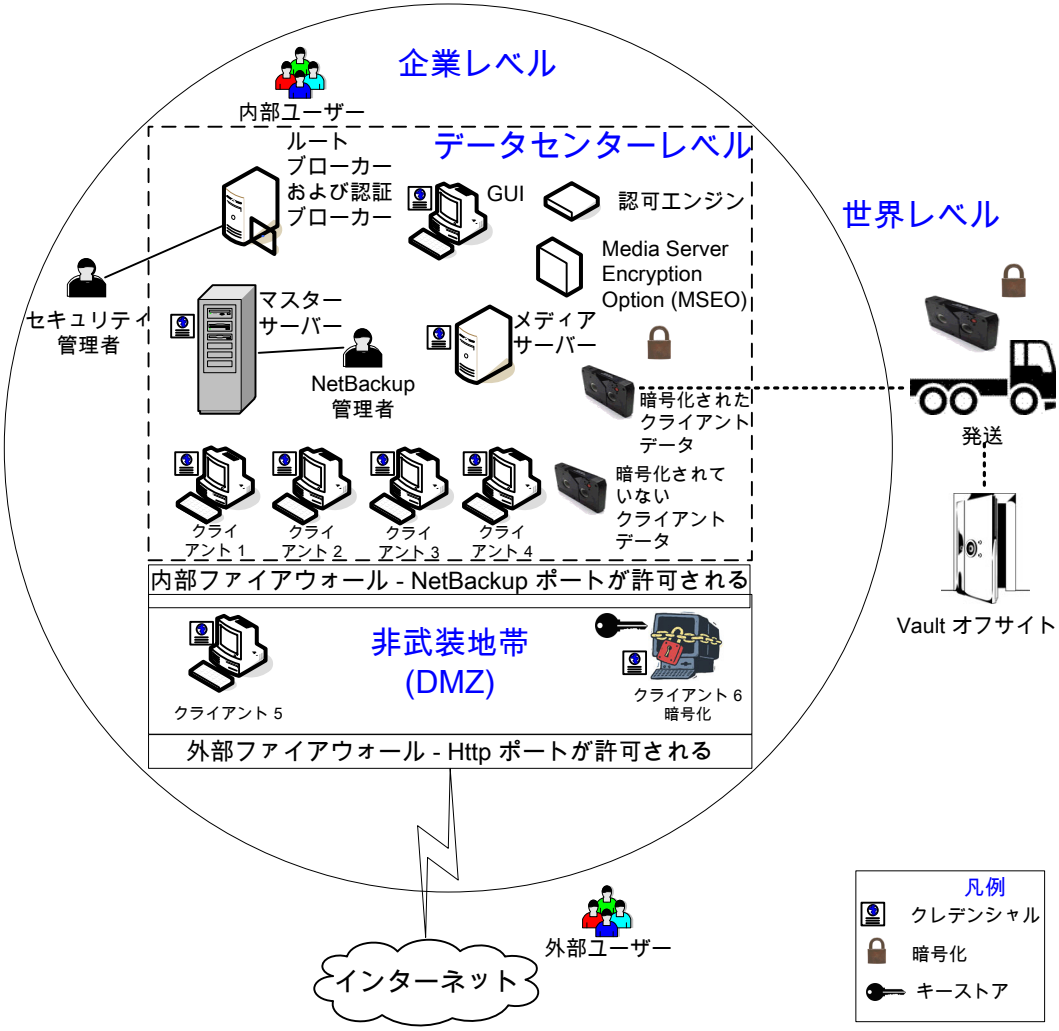


世界レベル、企業レベルおよびデータセンターレベルの統合

世界レベル、企業レベルおよびデータセンターレベルを統合したモデルは、完全に機能する標準的な NetBackup の操作が行われる領域を示します。一番外側の世界レベルでは、外部ユーザーはファイアウォールで保護されている企業の Web サーバーにアクセスすることができ、暗号化されたテープは発送されてオフサイト Vault に格納されます。その内側の企業レベルでは、内部ユーザー、セキュリティ管理者およびデータセンターレベルに関連する機能が実行されます。最も内側のデータセンターレベルでは、ワークグループ、単一のデータセンターまたは複数のデータセンターから NetBackup セキュリティの主要な機能が実行されます。

次の図に、世界レベル、企業レベルおよびデータセンターレベルの統合モデルを示します。

図 1-4　世界レベル、企業レベルおよびデータセンターレベルの統合



NetBackup セキュリティの実装形式

次の図に、NetBackup セキュリティの実装形式、特徴、複雑さのレベル、およびセキュリティの配置モデルを示します。

表 1-6 セキュリティの実装形式

セキュリティの実装形式	特徴	複雑さのレベル	セキュリティの配置モデル
p.25 の「オペレーティングシステムのセキュリティ」を参照してください。	■ オペレーティングシステムに依存 ■ システムコンポーネントに依存	システムによって異なる	ワークグループ 単一のデータセンター 複数のデータセンター
p.26 の「NetBackup の標準セキュリティ」を参照してください。	■ root または管理者として管理 ■ データは暗号化されない	低	NetBackup を使用するワークグループ 標準の NetBackup を使用する単一のデータセンター 標準的な NetBackup を使用する複数のデータセンター
p.27 の「Media Server Encryption Option (MSEO) セキュリティ」を参照してください。	■ メディアサーバーの暗号化 ■ クライアントからメディアサーバーへのトラフィックは暗号化されない ■ メディアサーバーの CPU のパフォーマンスに影響を与える可能性がある ■ 鍵の保管	低	MSEO (Media Server Encryption Option) を使用する単一のデータセンター MSEO (Media Server Encryption Option) を使用する複数のデータセンター
p.28 の「クライアント側の暗号化セキュリティ」を参照してください。	■ データはクライアント上で暗号化される ■ 暗号化されたデータは回線を介して送信される ■ クライアントの CPU のパフォーマンスに影響を与える可能性がある ■ 鍵の保管	中	クライアント側の暗号化を使用する単一のデータセンター クライアント側の暗号化を使用する複数のデータセンター
p.30 の「マスターサーバー、メディアサーバーおよび GUI での NBAC によるセキュリティ」を参照してください。	■ NBAC によってマスターサーバーおよびメディアサーバーへのアクセスに対して認可が行われる ■ NBAC によってマスターサーバーおよびメディアサーバーへアクセスするシステムおよびユーザーが認証される	中	マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンター マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンター

セキュリティの実装形式	特徴	複雑さのレベル	セキュリティの配置モデル
p.32 の「すべてに NBAC を使用したセキュリティ」を参照してください。	■ NBAC によってシステム全体の認可が行われる ■ NBAC によってシステム全体の認証が行われる(サーバー、クライアント、およびユーザー)	高	すべてに NBAC を使用する単一のデータセンター すべてに NBAC を使用する複数のデータセンター
p.33 の「すべての NetBackup セキュリティ」を参照してください。	■ すべての NetBackup セキュリティ形式を統合 ■ 例の図および説明では、すべてのセキュリティ機構が統合されている	最高	すべてのセキュリティが実装された単一のデータセンター すべての NetBackup セキュリティを使用する複数のデータセンター

オペレーティングシステムのセキュリティ

マスターサーバー、メディアサーバー、およびクライアントにおけるオペレーティングシステムのセキュリティは、次の対策を行うことにより強化できます。

- オペレーティングシステムのパッチをインストールする
  オペレーティングシステムのパッチには、最高レベルのシステムの整合性を維持するために OS に適用するアップグレードが含まれます。ベンダーが指定するレベルのアップグレードおよびパッチを常に適用してください。
- 安全なファイアウォール手順に従う
- 最小権限で管理を行う
- root ユーザーを制限する
- IPSEC (IP を介したセキュリティプロトコル) ハードウェアを適用する
- 外部に接続するアプリケーションの未使用ポートを無効にする
- 安全な基盤で NetBackup を実行する
- オペレーティングシステムが危険にさらされているかどうかの確認に最先端の手法を使用する
- すべてのオペレーティングシステムに同じセキュリティを実装する
- 異機種が混在する環境で、NBAC を使用して様々なシステム間での完全な相互運用性を実現する

NetBackup セキュリティの脆弱性

NetBackup セキュリティの潜在的な脆弱性に備えて、次の保護手段を検討してください。

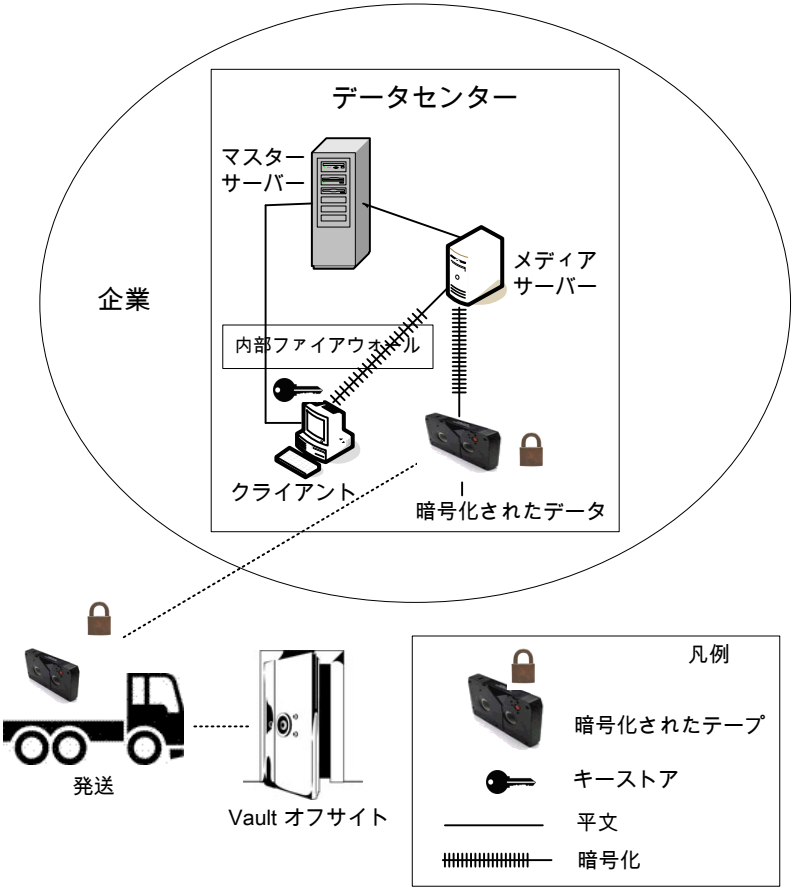
- 次に適用する NetBackup メンテナンスパッチで完全な NetBackup 更新を行う
- 累積的な NetBackup 更新を行う
- シマンテック社の Web サイトで潜在的なセキュリティの脆弱性に関する情報を参照する
  www.symantec.com/avcenter/security/SymantecAdvisories.html または www.symantec.com/security
- 潜在的なセキュリティの脆弱性に関して次のアドレスに電子メールで問い合わせる
  secure@symantec.com

NetBackup の標準セキュリティ

NetBackup の標準セキュリティには、オペレーティングシステムおよびデータセンターのハードウェアコンポーネントから提供されるセキュリティのみが含まれます。認可済みの NetBackup ユーザーが root または管理者として管理を行います。クライアントデータは暗号化されません。マスターサーバー、メディアサーバーおよびクライアントはすべてローカルの企業のデータセンター内で動作します。暗号化されていないデータは通常オンサイトに格納されるため、ディザスタリカバリ計画を実行できない可能性が比較的高くなります。オフサイトに送信されたデータは、傍受された場合に機密性が違反される可能性があります。

次の図は NetBackup の標準の構成例を示します。

図 1-5　　標準的な NetBackup



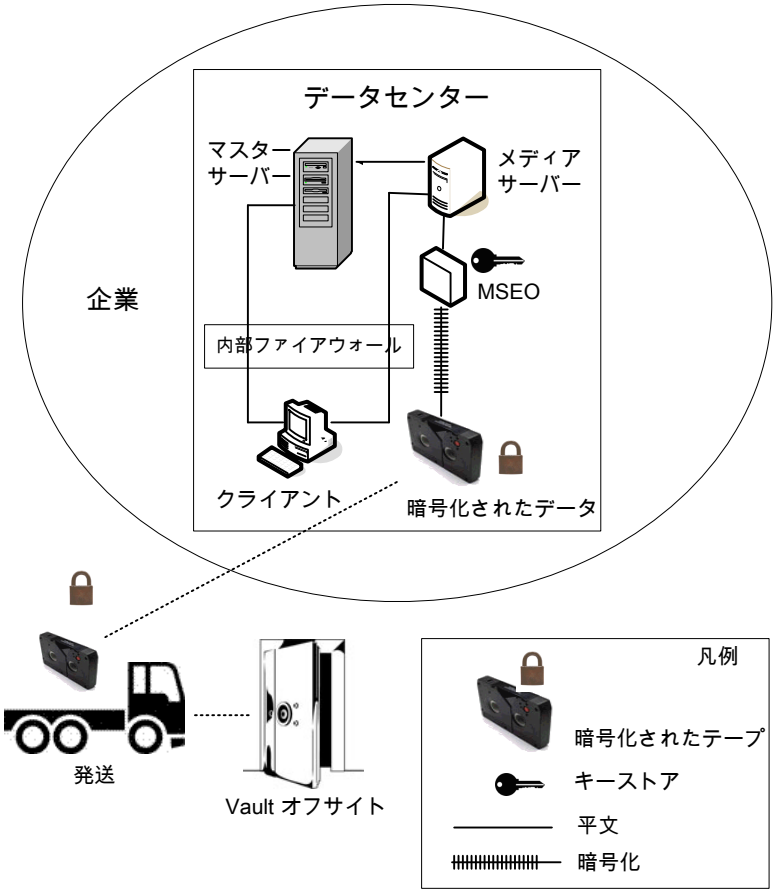
Media Server Encryption Option (MSEO) セキュリティ

Media Server Encryption Option (MSEO) セキュリティ形式は、クライアントレベルのデータ暗号化ソリューションを提供します。暗号化されたテープデータが発送されてオフサイト Vault に格納されるため、全体的なディザスタリカバリでデータが損失する危険性が減少します。マスターサーバー、メディアサーバー、MSEO およびクライアントはすべてローカルの企業のデータセンター内で動作します。MSEO は個々のクライアントの CPU 集中処理を軽減できます。これは、暗号化処理がメディアサーバーに移行されるためで、クライアント側で暗号化した場合の MSEO に比べて処理が軽減されます。ただし、MSEO はメディアサーバーの CPU のパフォーマンスに影響を与える可能性があります。MSEO からテープへのトラフィックは暗号化されます。クライアントからメディアサーバー

へのトラフィックは暗号化されません。暗号化されたデータに将来アクセスできるように、MSEO デバイス上に鍵を保管しておく必要があります。

次の図に、Media Server Encryption Option (MSEO) の構成例を示します。

図 1-6 Media Server Encryption Option (MSEO)



クライアント側の暗号化セキュリティ

クライアント側の暗号化セキュリティを使用すると、テープ上のデータだけでなく回線を経由するデータの機密性も確保されます。この暗号化によって、組織内での回線の消極的な盗聴の危険性を軽減できます。テープをオフサイトに移動する際のデータ流出の危険性が軽減されます。暗号化鍵はクライアント上に置かれます。クライアントとメディアサーバー間の回線上のデータ通信は暗号化されます。クライアントによるデータの暗号化では、CPU に処理が集中する可能性があります。

次のバックアップポリシー形式では、クライアントの暗号化オプションの使用がサポートされます。

- AFS
- DB2
- DataStore
- DataTools-SQL-BackTrack
- Informix-On-BAR
- LOTUS_NOTES
- MS-Exchange
- MS-SharePoint
- MS-SQL-Server
- MS-Windows
- Oracle
- PureDisk-Export
- SAP
- Split-Mirror
- Standard
- Sybase

次のバックアップポリシー形式では、クライアントの暗号化オプションはサポートされません。これらのポリシー形式の場合、ポリシー属性インターフェースの暗号化のチェックボックスを選択できません。

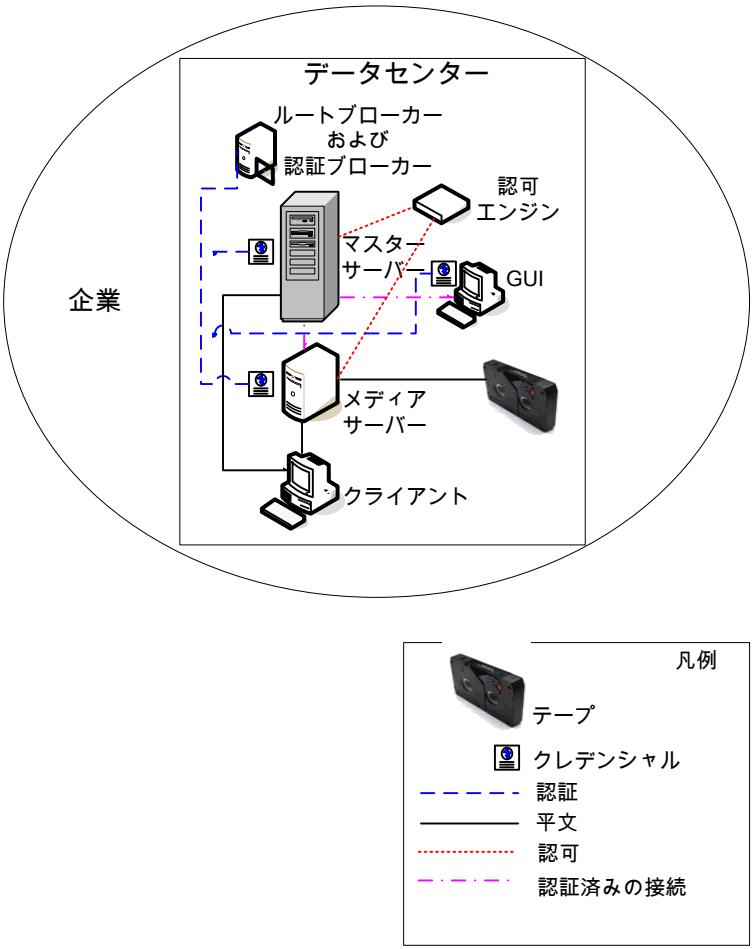
- FlashBackup
- FlashBackup-Windows
- NDMP
- NetWare
- OS/2
- Vault

Media Server Encryption Option は、データがテープに書き込まれる時点で適用され、一覧にあるすべてのポリシー形式で使うことができます。ただし、NDMP ポリシーは例外です。このポリシーでは、NDMP サーバーからデータが NDMP 形式で直接書き込まれます。Media Server Encryption Option は、バックアップが通常のメディアサーバーを使ってテープに書き込まれるリモート NDMP ではサポートされます。

VMS と OpenVMS のクライアントはクライアントの暗号化オプションをサポートしないことに注意してください。これらのクライアントは標準のポリシー形式を使用します。

次の図はクライアント側の暗号化の構成例を示します。

図 1-7　クライアント側の暗号化



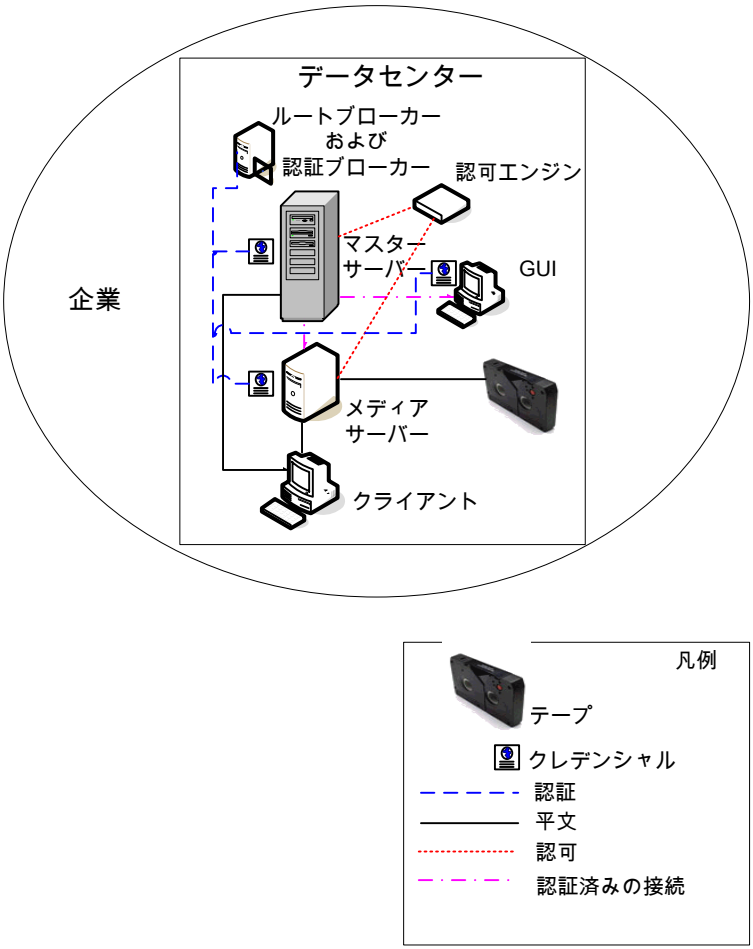
マスターサーバー、メディアサーバーおよび GUI での NBAC によるセキュリティ

マスターサーバー、メディアサーバーおよび GUI での NBAC によるセキュリティ方式では、認証ブローカーが使用されます。ブローカーは、マスターサーバー、メディアサーバー

および GUI にクレデンシャルを提供します。このデータセンターの例では、マスターサーバーおよびメディアサーバーで NetBackup アクセス制御を使用して、NetBackup へのアクセスを部分的に制限しています。また、この例では、root 以外のユーザーが NetBackup を管理することもできます。NBAC はサーバーと GUI 間で使用できるように構成されます。root 以外のユーザーは、オペレーティングシステムを使用して NetBackup にログオンできます。NetBackup の管理には、UNIX パスワードまはた Windows のローカルドメインを使用します。また、グローバルユーザーリポジトリ (NIS/NIS+ または Active Directory) を使って NetBackup を管理することもできます。さらに、NBAC を使用して、特定のユーザーに対して NetBackup へのアクセスレベルを制限することもできます。たとえば、日常的な操作の制御と、新しいポリシーやロボットの追加といった環境構成を分離することもできます。

次の図に、マスターサーバーおよびメディアサーバー構成での NBAC の例を示します。

図 1-8　マスターサーバーおよびメディアサーバー上の NBAC



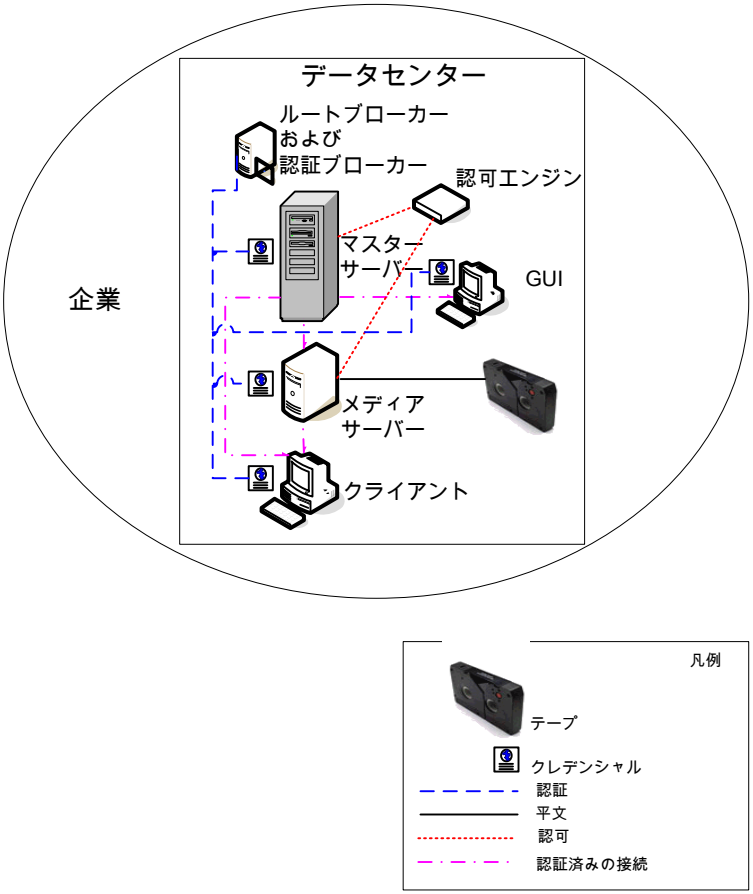
すべてに NBAC を使用したセキュリティ

すべてに NBAC を使用したセキュリティ方式では、認証ブローカーを使用して、マスターサーバー、メディアサーバー、およびクライアントにクレデンシャルを提供します。この環境は、マスターサーバー、メディアサーバーおよび GUI 上の NBAC モデルに非常によく似ています。主な相違点は、NetBackup 環境に含まれるすべてのホストがクレデンシャルを使用して確実に識別される点です。また、root 以外の管理者が、構成可能なアクセスレベルに基づいて NetBackup クライアントを管理できる点も異なります。ユーザー識別情報は、Windows の Active Directory または UNIX の NIS などのグローバルリポジトリに存在する場合があります。また、識別情報は、認証ブローカーをサポートするホスト

上のローカルのリポジトリ (UNIX のパスワード、Windows のローカルドメイン) に存在する場合もあります。

次の図は NBAC の完全な構成例を示します。

図 1-9 すべてに NBAC を使用



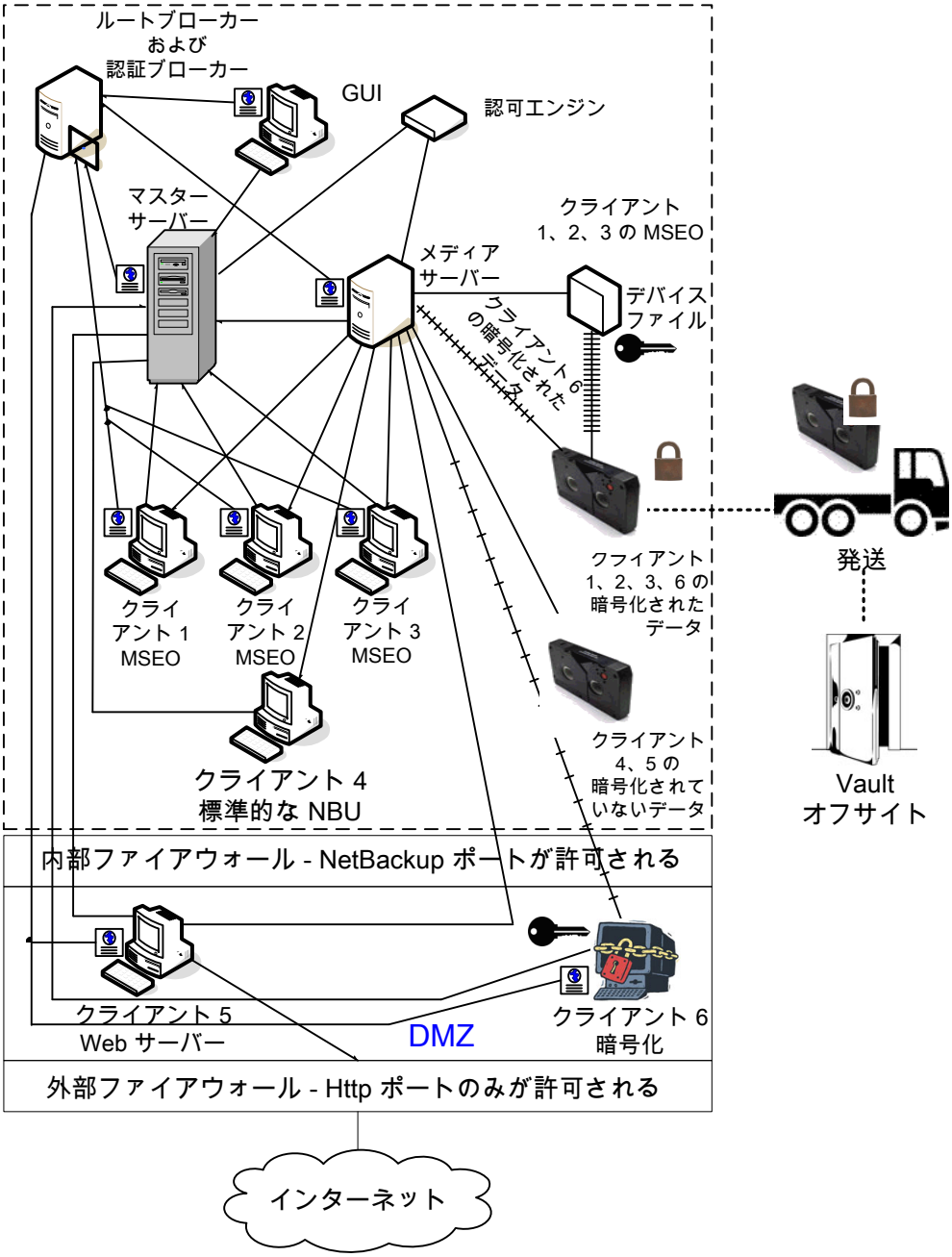
すべての NetBackup セキュリティ

すべての NetBackup セキュリティでは、すべてのセキュリティが統合されます。これは、非常に高度な環境で、様々なクライアントに対して異なる要件が存在します。クライアントの要件によっては、ホスト以外での暗号化が必要になることもあります (ホストのリソースが不足している場合やデータベースのバックアップ時など)。また、クライアントの要件によっては、ホスト上のデータの機密性を確保するためにホストでの暗号化が必要になることも

あります。NBAC をセキュリティ構成に追加することで、NetBackup 内で管理者、オペレータ、およびユーザーを分離することができます。

次の図に、すべての NetBackup セキュリティが実装された例を示します。

図 1-10　すべての NetBackup セキュリティ



2

セキュリティの配置モデル

この章では以下の項目について説明しています。

- ワークグループ
- 単一のデータセンター
- 複数のデータセンター
- NetBackup を使用するワークグループ
- 標準の NetBackup を使用する単一のデータセンター
- MSEO (Media Server Encryption Option) を使用する単一のデータセンター
- クライアント側の暗号化を使用する単一のデータセンター
- マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンター
- すべてに NBAC を使用する単一のデータセンター
- すべてのセキュリティが実装された単一のデータセンター
- 標準的な NetBackup を使用する複数のデータセンター
- MSEO (Media Server Encryption Option) を使用する複数のデータセンター
- クライアント側の暗号化を使用する複数のデータセンター
- マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンター
- すべてに NBAC を使用する複数のデータセンター
- すべての NetBackup セキュリティを使用する複数のデータセンター

ワークグループ

ワークグループは、内部で NetBackup を使用する小規模な (50 未満の) システムグループです。

例のワークグループは次の項に示されています。

- p.38 の「NetBackup を使用するワークグループ」を参照してください。

単一のデータセンター

単一のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。

単一のデータセンターの例については、次の項を参照してください。

- p.41 の「標準の NetBackup を使用する単一のデータセンター」を参照してください。
- p.44 の「MSEO (Media Server Encryption Option) を使用する単一のデータセンター」を参照してください。
- p.47 の「クライアント側の暗号化を使用する単一のデータセンター」を参照してください。
- p.49 の「マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンター」を参照してください。
- p.53 の「すべてに NBAC を使用する単一のデータセンター」を参照してください。
- p.57 の「すべてのセキュリティが実装された単一のデータセンター」を参照してください。

複数のデータセンター

複数のデータセンターには、中規模から大規模な (50 を超える) ホストのグループが含まれます。ホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。

複数のデータセンターの例については、次の項を参照してください。

- p.61 の「標準的な NetBackup を使用する複数のデータセンター」を参照してください。
- p.65 の「MSEO (Media Server Encryption Option) を使用する複数のデータセンター」を参照してください。
- p.71 の「クライアント側の暗号化を使用する複数のデータセンター」を参照してください。

- p.76 の「マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンター」を参照してください。
- p.82 の「すべてに NBAC を使用する複数のデータセンター」を参照してください。
- p.87 の「すべての NetBackup セキュリティを使用する複数のデータセンター」を参照してください。

NetBackup を使用するワークグループ

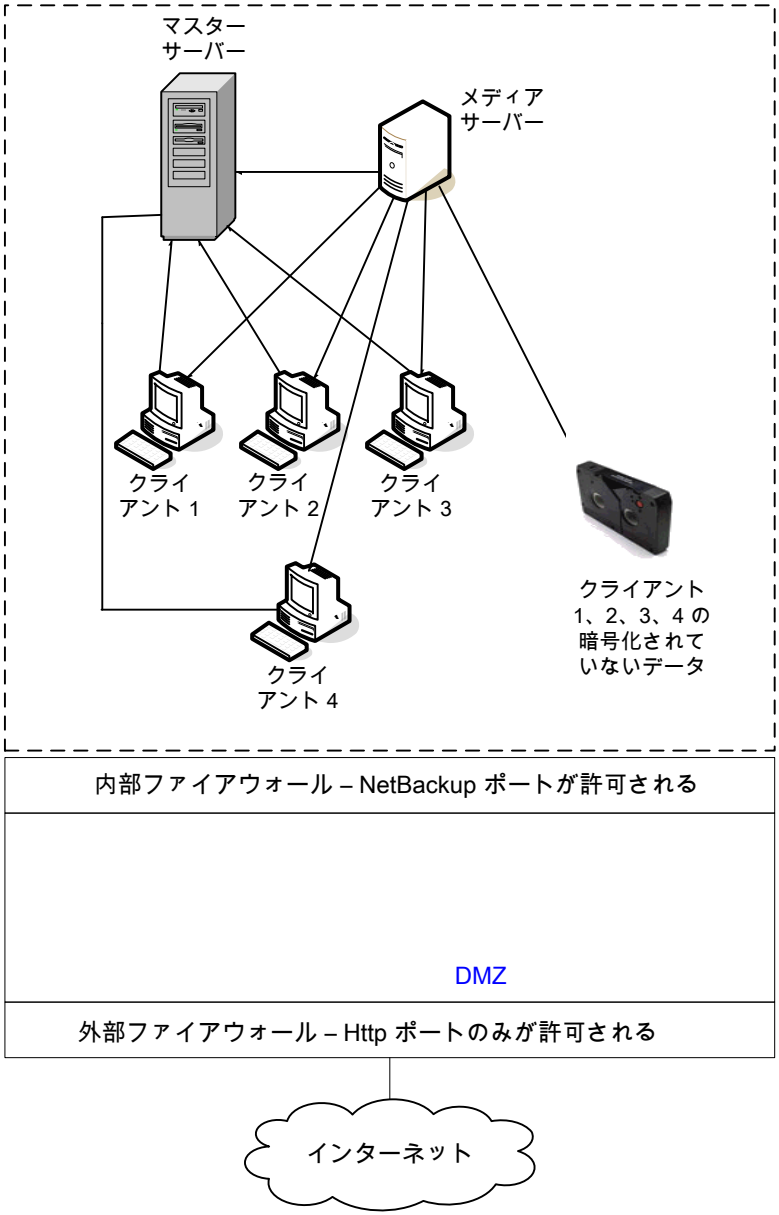
NetBackup を使用するワークグループは、小規模な (50 未満の) システムグループです。このワークグループは NetBackup を内部で使います。通常、この構成には NIS、Active Directory などの統一されたネーミングサービスはありません。DNS、WINS のような信頼できるホストネーミングサービスを持たないこともあります。通常、この構成は大規模な企業でのテストラボや、小規模な企業の環境で使用されます。

NetBackup を使用するワークグループには、次の特徴があります。

- NetBackup サーバーの数が非常に少ない
- コンピュータ環境が小規模である
- 外部に接続する装置が実装されていない

図 2-1 に、NetBackup を使用するワークグループの例を示します。

図 2-1　NetBackup を使用するワークグループ



次の表に、ワークグループで使われる NetBackup の構成要素を示します。

表 2-1 ワークグループで使われる NetBackup の構成要素

構成要素	説明
マスターサーバー	メディアサーバーおよびクライアント 1、2、3、4 と通信します。
メディアサーバー	マスターサーバーおよびクライアント 1、2、3、4 と通信します。また、クライアント 1、2、3、4 の暗号化されていないデータのテープへの書き込みを管理します。
テープ	クライアント 1、2、3、4 の暗号化されていないバックアップデータが格納されます。
クライアント	クライアント 1、2、3、4 は、マスターサーバーで管理される標準的な NetBackup クライアントです。これらのクライアントには、メディアサーバーによってテープにバックアップされる暗号化されていないデータが存在します。
内部ファイアウォール	NetBackup が DMZ 内のクライアントにアクセスすることを許可します。選択された NetBackup ポートおよび他のアプリケーションポート(可能な場合)のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、インターネットから内部ファイアウォールを通過できません。内部ファイアウォールは、ワークグループ配置モデルでは使用されません。この例では、内部ファイアウォールにアクセスするクライアントが存在しないため、内部ファイアウォールを通過する NetBackup ポートを開く必要はありません。 **メモ:** この例では、内部ファイアウォールの外側にクライアントは存在しません。このため、内部ファイアウォールを通過する NetBackup ポートを開く必要はありません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している NetBackup クライアントに「安全な」操作領域を提供します。DMZ で操作を行う可能性のあるクライアントには、標準的な NetBackup クライアントまたは暗号化を行う NetBackup クライアントのいずれかを使用する Web サーバー NetBackup クライアントがあります。DMZ 内のクライアントは、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバー NetBackup クライアントは、一般的な HTTP ポートを使用して、外部ファイアウォールからのインターネットへの接続を受信できます。ワークグループ配置モデル内のクライアントは、DMZ にアクセスできません。
外部ファイアウォール	外部ユーザーは、一般的に HTTP ポートを経由してインターネットから外部ファイアウォールを通過して、DMZ 内にある Web サーバー NetBackup クライアントにアクセスできます。内部ファイアウォールを通過して通信を行うクライアント向けに開かれた NetBackup ポートは、外部ファイアウォールを通過してインターネットにアクセスすることはできません。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ワークグループ配置モデル内のクライアントでは、インターネットは使用されません。 **注意:** NetBackup クライアントは、DMZ の外側に配置したり、インターネット上に直接配置したりしないでください。外部ファイアウォールを使用して、常に NetBackup ポートを外部からブロックする必要があります。

標準の NetBackup を使用する単一のデータセンター

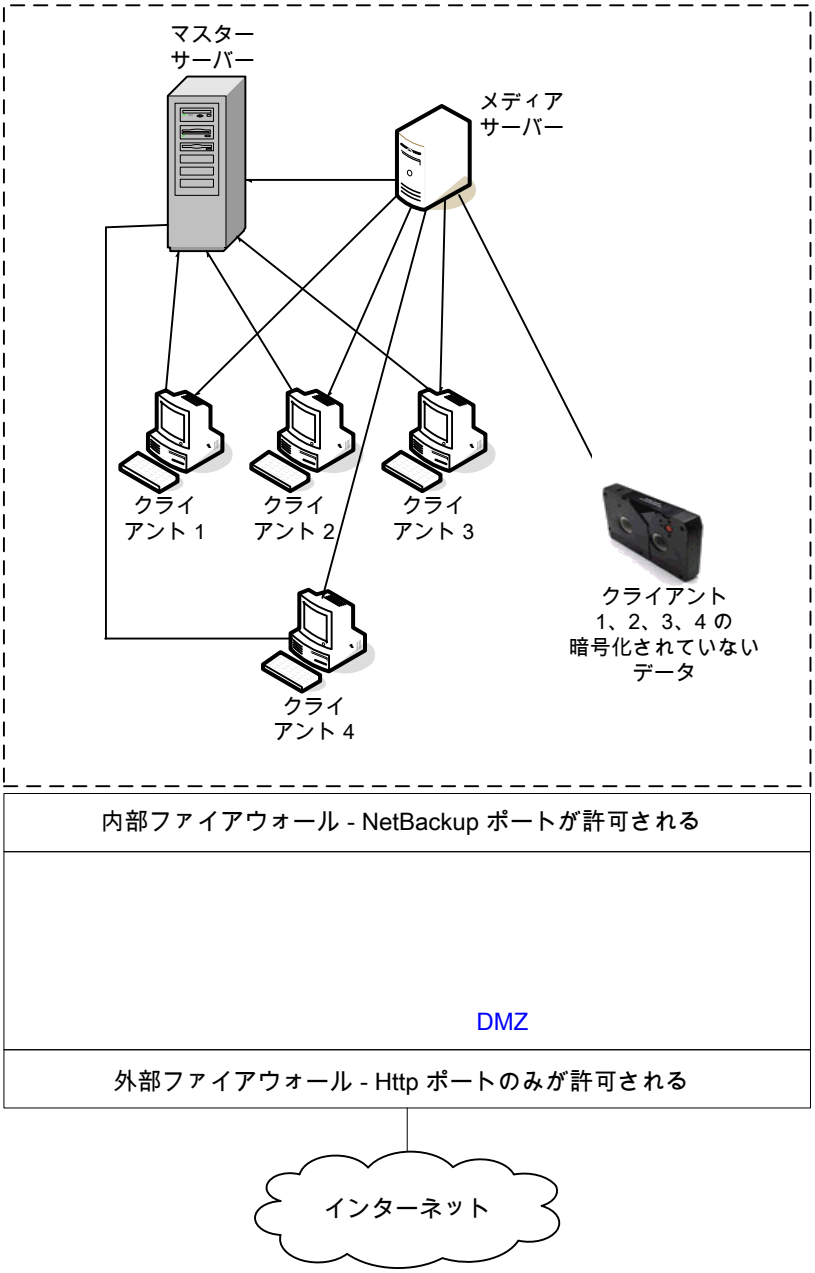
標準的な NetBackup を使用する単一のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。単一のデータセンターには、内部専用のホストと、DMZ を介してインターネットに展開するホストの両方が含まれます。通常、この構成には、ホスト向けの中央集中型ネーミングサービス (DNS、WINS など) が含まれます。また、ユーザー向けの中央集中型ネーミングサービス (NIS、Active Directory など) も含まれます。

標準の NetBackup を使用する単一のデータセンターには、次の特徴があります。

- 外部に接続するホストがある
- 通常、中央集中型ネーミングサービスが存在する
- ホスト数が 50 を超える
- 最も単純な構成で、NetBackup の一般的な知識のみが必要である
- NetBackup ユーザー用に使用される標準的な構成である
- バックアップ時に、回線上でデータの消極的な妨害が行われる危険性がほとんどない

図 2-2 に、標準の NetBackup を使用する単一のデータセンターの例を示します。

図 2-2　　標準の NetBackup を使用する単一のデータセンター



次の表に、標準的なNetBackupを使用する単一のデータセンターで使われるNetBackupの構成要素を示します。

表 2-2　標準的な NetBackup を使用する単一のデータセンターにおける NetBackup の構成要素

構成要素	説明
マスターサーバー	メディアサーバー、標準的な NetBackup クライアント 4 および DMZ 内の Web サーバー NetBackup クライアント 5 と通信します。
メディアサーバー	マスターサーバー、標準的な NetBackup クライアント 4 および DMZ 内の Web サーバー NetBackup クライアント 5 と通信します。メディアサーバーは、クライアント 4、5 の暗号化されていないデータのテープへの書き込みを管理します。
テープ	クライアント 4、5 の暗号化されていないバックアップデータが格納されます。
クライアント	クライアント 4 は標準的な NetBackup 形式であり、クライアント 5 は Web サーバー形式です。これらのクライアントはどちらもマスターサーバーによって管理され、それらの暗号化されていないデータはメディアサーバーによってテープにバックアップされます。クライアント 4 は、データセンター内に存在します。クライアント 5 は、DMZ 内に存在します。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。照合を行うすべての NetBackup 通信は、暗号化されていない状態で回線を介して送信されることに注意してください。
内部ファイアウォール	NetBackup は、DMZ 内の Web サーバー NetBackup クライアント 5 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、インターネットから内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している NetBackup クライアント 5 Web サーバーに「安全な」操作領域を提供します。DMZ 内のクライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。
外部ファイアウォール	外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートはクライアント 5 に対して開かれており、内部ファイアウォールを通過して通信が行われます。 **注意:** NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。外部ファイアウォールでは、クライアント 5 に対する HTTP ポートだけが開かれており、インターネットに接続することができます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットを介した接続を受信できます。

MSEO (Media Server Encryption Option) を使用する単一のデータセンター

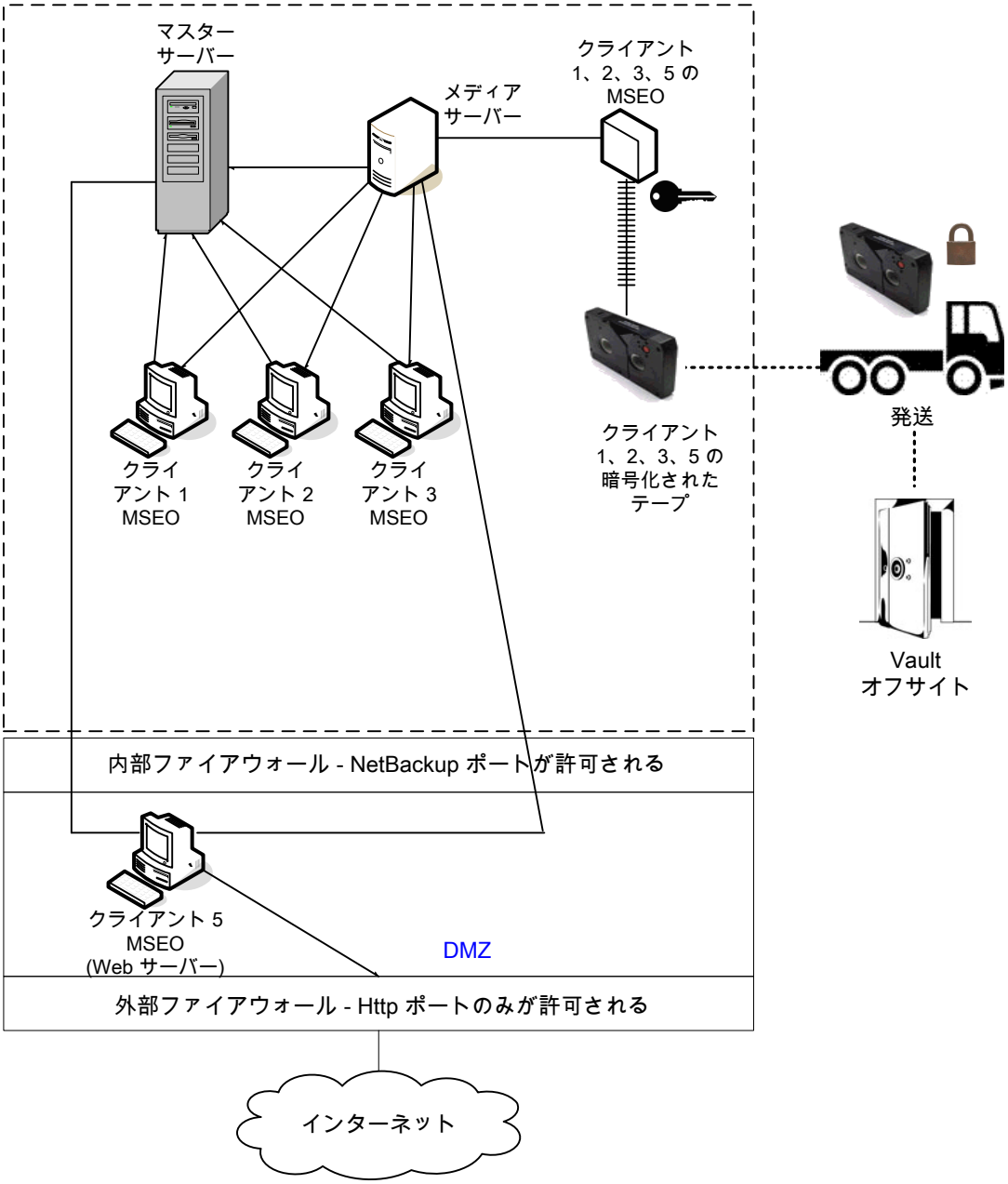
MSEO (Media Server Encryption Option) を使用する単一のデータセンターの例には、通常、50 を超えるホストが含まれます。外部に接続するすべてのホストは、MSEO (Media Server Encryption Option) を使用します。この例では、クライアントはすべてのホストに対して MSEO オプションを使用しています。

MSEO (Media Server Encryption Option) を使用する単一のデータセンターには、次の特徴があります。

- MSEO は NetBackup における新しいオプションである
- オフサイトに発送されたデータを保護する
- 回線からのデータの消極的な妨害は許容リスクであるため、データは暗号化されずにクライアントから送信される
- 単一障害点と同様、鍵の管理と暗号化は 1 か所で管理される高可用性クラスタを使用すると便利です。
- 同時に複数のクライアントを処理するために、堅牢なメディアサーバーが必要である
- 暗号化されたテープをオフサイトに送る必要があるが、CPU に負荷がかかるクライアントの暗号化処理を軽減させる場合に有効である
- データを戻すには鍵が必要である。鍵を失うと、データも失われます。(暗号化の章の鍵の共有バックアップに関する情報を参照してください。)

図 2-3 に、MSEO を使用する単一のデータセンターの例を示します。

図 2-3 MSEO を使用する単一のデータセンター



次の表に、MSEO を使用する単一のデータセンターで使われる NetBackup の構成要素を示します。

表 2-3 MSEO を使用する単一のデータセンターで使用される NetBackup の構成要素

構成要素	説明
マスターサーバー	メディアサーバー、MSEO クライアント 1、2、3 および DMZ 内の MSEO Web サーバークライアント 5 と通信します。
メディアサーバー	マスターサーバー、MSEO クライアント 1、2、3 および DMZ 内の MSEO Web サーバークライアント 5 と通信します。また、メディアサーバーは、クライアント 1、2、3、5 の暗号化されたデータのテープへの書き込みを可能にする MSEO デバイスと通信します。
MSEO	MSEO ハードウェア装置は、個々のクライアントでの暗号化処理による負荷を軽減させるため、クライアント 1、2、3、5 の暗号化されたデータを生成します。この暗号化されたデータは、テープに書き込まれます。MSEO 装置を使用することで、クライアント側で暗号化を行う場合と比較して、個々のクライアントの CPU パフォーマンスが向上します。
テープ	MSEO によって暗号化されたクライアント 1、2、3、5 のバックアップデータが格納されます。暗号化されたテープは、ディザスタリカバリ保護用にオフサイト Vault に発送されます。 **メモ:** データを復号化するには、そのデータの暗号化に使用した鍵が利用可能である必要があります。
トランスポート	トランスポートトラックにより、暗号化されたテープがセキュリティ保護されたオフサイト Vault 施設に運ばれます。輸送中にテープが失われた場合でも、データセンターの管理者は、データの漏洩リスクを軽減することができます。データの漏洩は、データの暗号化により軽減されます。
オフサイト Vault	ディザスタリカバリ保護を支援するデータセンターとは異なる場所にある安全な保管施設を提供します。
クライアント	クライアント 1、2、3 は MSEO 形式であり、クライアント 5 は Web サーバー形式 (MSEO オプションも使用) です。どちらの形式もマスターサーバーによって管理でき、暗号化されたデータがテープにバックアップされます。バックアップは、MSEO ハードウェア装置が接続されたメディアサーバーによって実行されます。クライアント 1、2、3 は、データセンター内に存在します。クライアント 5 は、DMZ 内に存在します。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。
内部ファイアウォール	NetBackup は、これを使用して、DMZ 内のクライアント 5 Web サーバーにアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。

構成要素	説明
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している Web サーバークライアント 5 に「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。
外部ファイアウォール	外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

クライアント側の暗号化を使用する単一のデータセンター

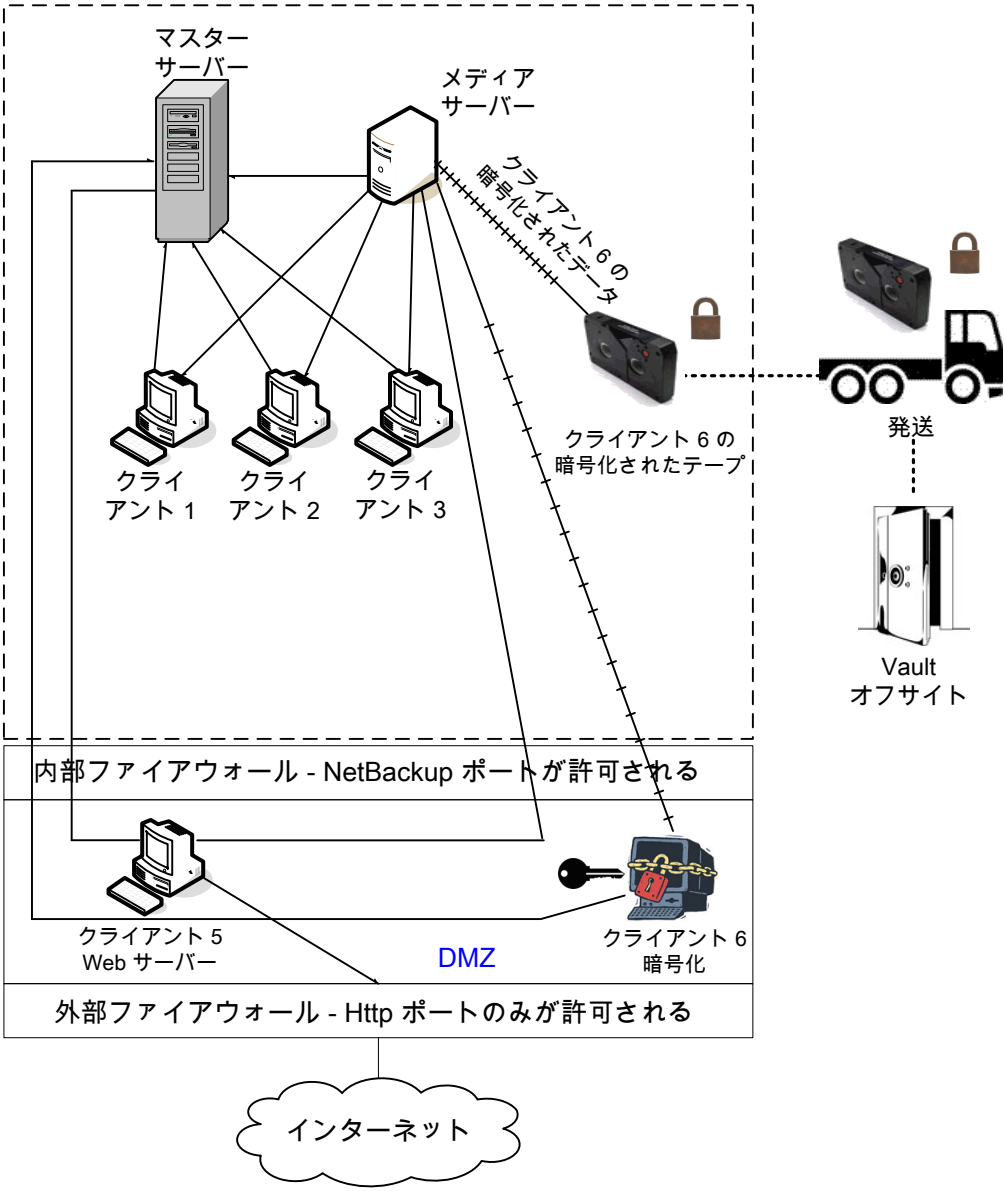
クライアント側の暗号化を使用する単一のデータセンターの例では、クライアント側の暗号化によって、テープ上のデータだけでなく回線を経由するデータの機密性も確保されます。クライアント側の暗号化によって、組織内での回線の消極的な盗聴の危険性が軽減されます。テープをオフサイトに移動する際のデータ流出の危険性が軽減されます。このデータセンターモデルでは、中規模から大規模 (50 を超える) の管理対象ホストに対応できます。データセンター内および DMZ 内のクライアントは、ホストおよびユーザー識別情報に中央集中型ネーミングサービスを使うことができます。

クライアント側の暗号化を使用する単一のデータセンターには、次の特徴があります。

- オフサイトデータの保護に役立つ
- クライアントからのデータが暗号化されるため、回線でのデータの消極的な妨害が防止される
- 鍵の管理はクライアントに分散される
- NetBackup 独自の暗号化オプションが使用される
- 暗号化処理にはクライアントの CPU が使用される
- データを戻すには鍵が必要である。鍵を失うと、データも失われます。
- オフサイトでテープをスキャンする必要がある場合または回線上での機密性が必要な場合に有効である

図 2-4 に、クライアント側の暗号化を使用する単一のデータセンターの例を示します。

図 2-4 クライアント側の暗号化を使用する単一のデータセンター



次の表に、クライアント側の暗号化を使用する単一のデータセンターで使われる NetBackup の構成要素を示します。

表 2-4 クライアント側の暗号化を使用する単一のデータセンターにおける NetBackup の構成要素

構成要素	説明
非武装地帯 (DMZ)	Web サーバークライアント 5 および暗号化クライアント 6 に対して「安全な」操作領域を提供します。これらのクライアントは、内部ファイアウォールと外部ファイアウォールの間に存在します。DMZ 内の Web サーバークライアント 5 と暗号化クライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 と暗号化クライアント 6 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。DMZ 内の暗号化クライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。
外部ファイアウォール	外部ユーザーは、Web サーバークライアント 5 および暗号化クライアント 6 にアクセスできます。これらのクライアントは HTTP ポートを経由してインターネットから DMZ 内にアクセスできます。NetBackup ポートは Web サーバークライアント 5 と暗号化クライアント 6 に対して開かれており、内部ファイアウォールを通過して通信が行われます。ただし、NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 と暗号化クライアント 6 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。外部ファイアウォールによって、クライアント 5、6 のインターネット上での双方向の通信が制限されます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンター

マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンターの例では、マスターサーバーとメディアサーバー上で NetBackup のアクセス制御を使用します。この構成では、NetBackup へのアクセスを部分的に制限し、root 以外のユーザーが NetBackup を管理できるようになっています。NBAC はサーバーと GUI 間で実行できるように構成されます。root 以外のユーザーはオペレーティングシステム (UNIX のパスワードまたは Windows のローカルドメイン) またはグローバルユーザーリポジトリ (NIS/NIS+ または Active Directory) を使用して NetBackup にログインし、NetBackup を管理することができます。NBAC を使用して、特定のユーザーに対して NetBackup へのアクセスレベルを制限することもできます。たとえば、日常的な操作の制御と、新しいポリシーやロボットの追加といった環境構成を分離することもできます。

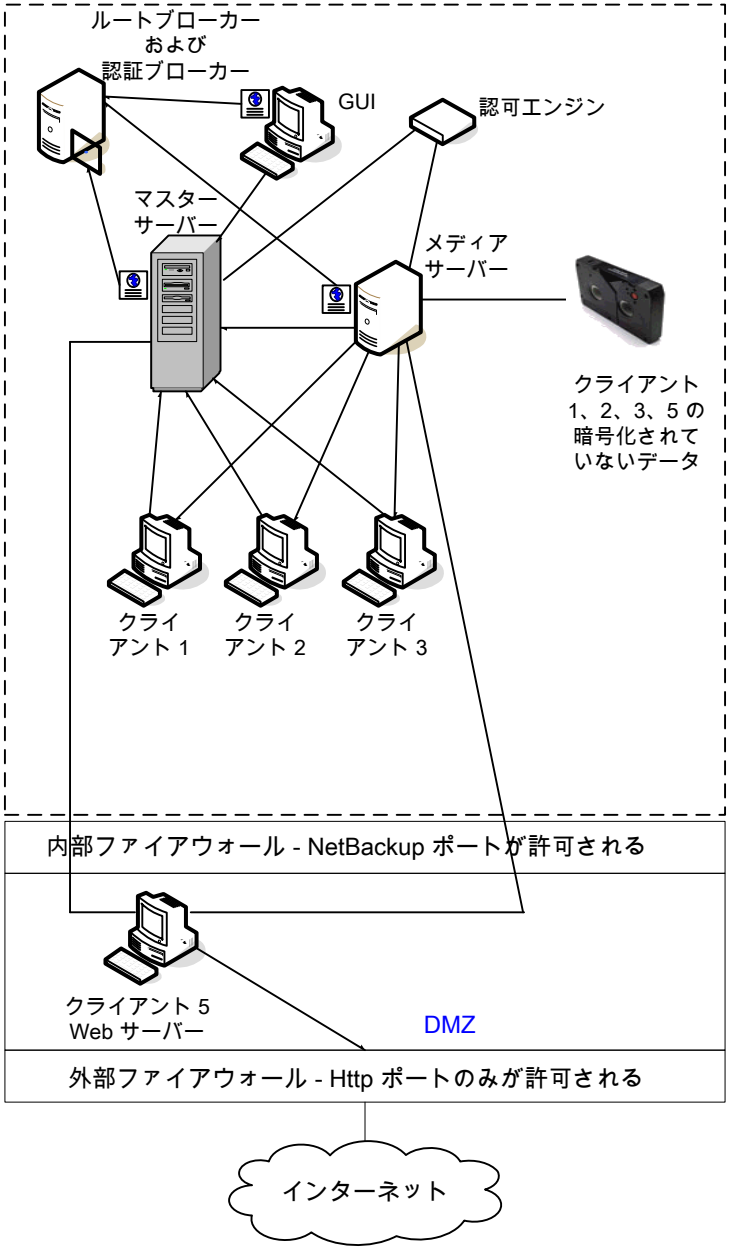
マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンターには、次の特徴があります。

- root 以外のユーザーを管理する

- Windows のユーザー ID を使用して UNIX を管理する
- UNIX アカウントを使用して Windows を管理する
- 特定のユーザーの操作を分離および制限する
- クライアントホストの root ユーザーまたは管理者はローカルクライアントのバックアップとリストアを実行できる
- 他のセキュリティ関連のオプションと組み合わせることができる
- すべてのサーバーが NetBackup バージョン 5.x 以上である必要がある

図 2-5 に、マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンターの例を示します。

図 2-5 マスターサーバーとメディアサーバーでNBACを使用する単一のデータセンター



次の表に、マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンターで使われる NetBackup の構成要素を示します。

表 2-5 マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンターにおける NetBackup の構成要素

構成要素	説明
マスターサーバー	メディアサーバー、ルートブローカーおよび認証ブローカーと通信します。また、認可エンジン、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) とも通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。 CLI または GUI がマスターサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。次に、デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
メディアサーバー	マスターサーバー、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) と通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。メディアサーバーによって、クライアント 1、2、3、5 の暗号化されていないデータのテープへの書き込みが可能になります。 CLI または GUI がメディアサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。次に、デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
GUI	このリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびマスターサーバーの機能へのアクセス権を取得します。
ルートブローカー	認証ブローカーを認証しますが、クライアントを認証しません。この例では、ルートブローカーおよび認証ブローカーは同じコンポーネントとして示されています。
認証ブローカー	マスターサーバー、メディアサーバーおよび GUI に対してそれぞれクレデンシャルを設定し、認証します。コマンドプロンプトが使われる場合、認証ブローカーはユーザーも認証します。
認可エンジン	マスターサーバーおよびメディアサーバーと通信して、認証済みユーザーの権限を決定します。これらの権限によって、ユーザーが利用できる機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。必要となる認可エンジンは 1 つだけです。 **メモ:** 認可エンジンは、デーモンプロセスとしてマスターサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	クライアント 1、2、3、5 の暗号化されていないバックアップデータが格納されます。
クライアント	クライアント 1、2、3 は標準の NetBackup 形式であり、クライアント 5 は Web サーバー形式です。どちらの形式もマスターサーバーによって管理され、暗号化されていないデータがメディアサーバーを介してテープにバックアップされます。クライアント 1、2、3 は、データセンター内に存在します。クライアント 5 は、DMZ 内に存在します。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。

構成要素	説明
内部ファイアウォール	NetBackup は、DMZ 内の Web サーバークライアント 5 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している Web サーバークライアント 5 に「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。
外部ファイアウォール	外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートはクライアント 5 に対して開かれており、内部ファイアウォールを通過して通信が行われます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。クライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。クライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

すべてに NBAC を使用する単一のデータセンター

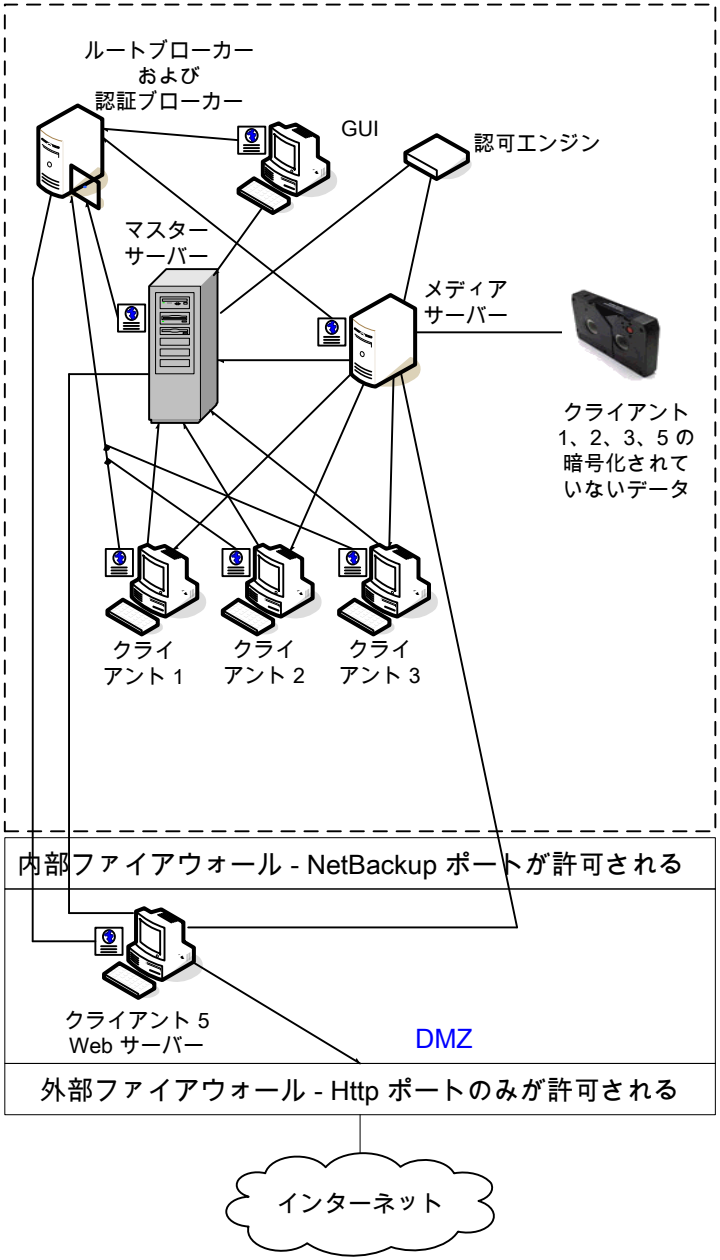
すべてに NBAC を使用する単一のデータセンターの環境は、マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンターによく似ています。主な相違点は、NetBackup 環境に含まれるすべてのホストがクレデンシャルを使用して確実に識別される点です。また、root 以外の管理者が、構成可能なアクセスレベルに基づいて NetBackup クライアントを管理できる点も異なります。ユーザー識別情報は、Windows の Active Directory または UNIX の NIS などのグローバルリポジトリに存在する場合があります。また、識別情報は、認証ブローカーをサポートするホスト上のローカルのリポジトリ (UNIX のパスワード、Windows のローカルドメイン) に存在する場合もあります。

すべてに NBAC を使用する単一のデータセンターには、次の特徴があります。

- マスターサーバーとメディアサーバーで NBAC を使用する単一のデータセンターの場合の特徴と類似している (クライアントの root ユーザーまたは管理者についての項目は除く)
- クライアントシステムでは、ローカルバックアップとリストアを行うために root 以外または管理者以外のユーザーが設定される場合がある (デフォルト設定)
- この環境では、NetBackup に含まれるすべてのホストの信頼できる識別が容易である
- すべてのホストは NetBackup バージョン 5.0 以上である必要がある

図 2-6 に、すべてに NBAC を使用する単一のデータセンターの例を示します。

図 2-6 すべてに NBAC を使用する単一のデータセンター



次の表に、すべてに NBAC を使用する単一のデータセンターで使われる NetBackup の構成要素を示します。

表 2-6 すべてにNBACを使用する単一のデータセンターにおけるNetBackupの構成要素

構成要素	説明
マスターサーバー	メディアサーバー、ルートブローカーおよび認証ブローカーと通信します。また、認可エンジン、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) とも通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。 CLI または GUI がマスターサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
メディアサーバー	マスターサーバー、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) と通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。メディアサーバーによって、クライアント 1、2、3、5 の暗号化されていないデータのテープへの書き込みが可能になります。 CLI または GUI がメディアサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
GUI	このリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびマスターサーバーの機能へのアクセス権を取得します。
ルートブローカー	認証ブローカーを認証しますが、クライアントを認証しません。図 2-6 では、ルートブローカーおよび認証ブローカーは同じコンポーネントとして示されています。
認証ブローカー	マスターサーバー、メディアサーバー、GUI、クライアントおよびユーザーに対してそれぞれクレデンシャルを設定し、認証します。
認可エンジン	マスターサーバーおよびメディアサーバーと通信して、認証済みユーザーの権限を決定します。また、認可エンジンには、ユーザーグループおよび権限が格納されます。必要となる認可エンジンは 1 つだけです。 **メモ:** 認可エンジンは、デーモンプロセスとしてマスターサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	クライアント 1、2、3、5 の暗号化されていないバックアップデータが格納されます。

構成要素	説明
クライアント	クライアント 1、2、3 は標準の NetBackup 形式であり、クライアント 5 は Web サーバー形式です。認証ブローカーからクレデンシャルを受信すると、クライアント 1、2、3、5 は NetBackup Product Authentication Service ドメインに認証されます。標準サーバー形式と Web サーバー形式はどちらもマスターサーバーによって管理され、暗号化されていないデータがメディアサーバーを介してテープにバックアップされます。クライアント 1、2、3 は、データセンター内に存在します。クライアント 5 は、DMZ 内に存在します。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。
内部ファイアウォール	NetBackup は、DMZ 内の Web サーバークライアント 5 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	内部ファイアウォールと外部ファイアウォールの間に存在している Web サーバークライアント 5 に「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。
外部ファイアウォール	外部ユーザーは HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートはクライアント 5 に対して開かれており、内部ファイアウォールを通過して通信が行われます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。クライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。クライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

すべてのセキュリティが実装された単一のデータセンター

すべてのセキュリティが実装された単一のデータセンターの例は、前述のすべての例を組み合わせたものです。これは、非常に高度な環境で、様々なクライアントに対して異なる要件が存在します。クライアントの要件によっては、ホスト以外での暗号化が必要になることもあります (ホストのリソースが不足している場合やデータベースのバックアップ時など)。また、クライアントの要件によっては、ホスト上のデータの機密性を確保するためにホストでの暗号化が必要になることもあります。NBAC をセキュリティ構成に追加することで、NetBackup 内で管理者、オペレータ、およびユーザーを分離することができます。

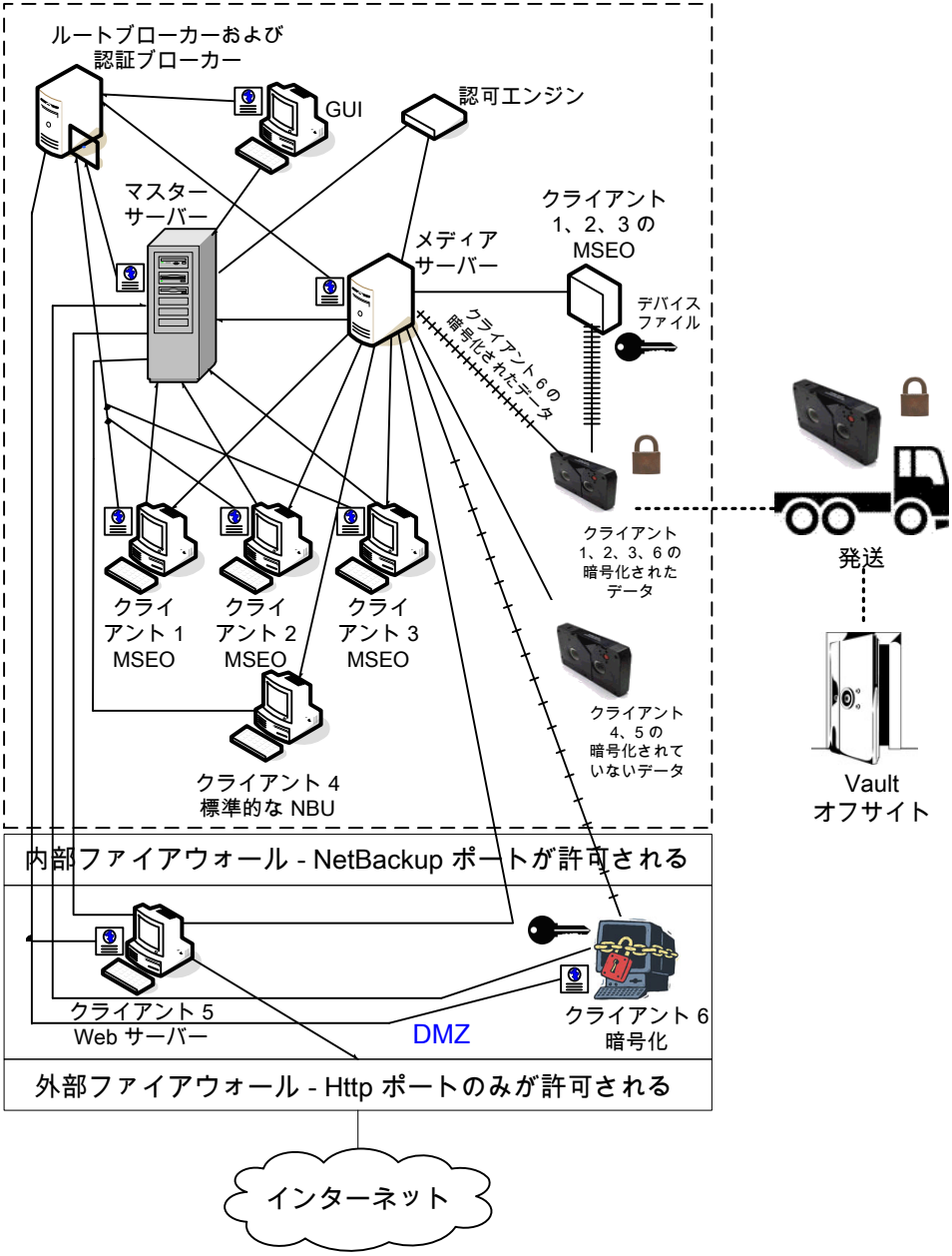
すべてのセキュリティが実装された単一のデータセンターには、次の特徴があります。

- 個々のオプションの特徴については、前述の単一のデータセンターに関する項を参照

- 最も柔軟で複雑な環境を提供する
- 類似モデルに従って綿密に設計することで、各オプションの長所を使用できる

図 2-7 に、すべてのセキュリティが実装された単一のデータセンターの例を示します。

図 2-7 すべてのセキュリティが実装された単一のデータセンター



次の表に、すべのセキュリティが実装された単一のデータセンターで使われるNetBackupの構成要素を示します。

表 2-7　すべてのセキュリティが実装された単一のデータセンターにおけるNetBackup の構成要素

構成要素	説明
マスターサーバー	メディアサーバー、ルートブローカー、認証ブローカー、認可エンジン、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) と通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。 CLI または GUI がマスターサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
メディアサーバー	マスターサーバー、クライアント 1、2、3 および DMZ 内のクライアント 5 (Web サーバー) と通信します。また、認可エンジンと通信して、認証ブローカーからクレデンシャルを受信します。メディアサーバーによって、クライアント 1、2、3、5 の暗号化されていないデータのテープへの書き込みが可能になります。 CLI または GUI がメディアサーバー上のデーモンにアクセスする場合は、ユーザーを識別するためにクレデンシャルが交換されます。デーモン機能へのアクセシビリティを判断するために認可エンジンへのアクセスが行われます。
GUI	このリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびマスターサーバーの機能へのアクセス権を取得します。
ルートブローカー	認証ブローカーを認証しますが、クライアントを認証しません。図では、ルートブローカーおよび認証ブローカーは同じコンポーネントとして示されています。
認証ブローカー	マスターサーバー、メディアサーバー、GUI、クライアントおよびユーザーに対してそれぞれクレデンシャルを設定し、認証します。
認可エンジン	マスターサーバーおよびメディアサーバーと通信して、認証済みユーザーの権限を決定します。また、認可エンジンには、ユーザーグループおよび権限が格納されます。必要となる認可エンジンは 1 つだけです。 **メモ:** 認可エンジンは、デーモンプロセスとしてマスターサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	1 つ目のテープには、MSEO によって暗号化されて書き込まれたクライアント 1、2、3 のバックアップデータと、クライアント側で暗号化されたクライアント 6 のデータが格納されます。2 つ目のテープには、クライアント 4、5 の暗号化されていないバックアップデータが格納されます。
トランスポート	トランスポートトラックにより、暗号化されたテープがセキュリティ保護されたオフサイト Vault 施設に運ばれます。輸送中にテープが失われた場合でも、データセンターの管理者は、リスクを軽減できます。データ漏洩のリスクは、暗号化により軽減されます。

構成要素	説明
オフサイト Vault	オフサイト Vault は、ディザスタリカバリ保護を支援するデータセンターとは別の場所にある安全な保管施設です。
クライアント	クライアント 1、2、3、4 は、標準的な NetBackup 形式です。クライアント 5 は、Web サーバー形式です。クライアント 6 では、クライアント側の暗号化が使用されます。認証ブローカーからクレデンシャルを受信すると、クライアント 1、2、3、5、6 は NetBackup Product Authentication Service ドメインに認証されます。標準サーバー形式と Web サーバー形式はどちらもマスターサーバーによって管理され、暗号化されていないデータがメディアサーバーを介してテープにバックアップされます。クライアント 6 には、メディアサーバーを介してテープにバックアップされる暗号化されたデータが存在します。クライアント 1、2、3 は、データセンター内に存在します。クライアント 5、6 は、DMZ 内に存在します。これらのクライアントは、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5、6 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットと通信します。
内部ファイアウォール	NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	Web サーバークライアント 5 および暗号化クライアント 6 に対して「安全な」操作領域を提供します。これらのクライアントは、内部ファイアウォールと外部ファイアウォールの間に存在します。DMZ 内の Web サーバークライアント 5 と暗号化クライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 と暗号化クライアント 6 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットに接続することができます。DMZ 内の暗号化クライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。
外部ファイアウォール	外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートはクライアント 5 に対して開かれており、内部ファイアウォールを通過して通信が行われます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。クライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。クライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

標準的な NetBackup を使用する複数のデータセンター

標準的な NetBackup を使用する複数のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、

データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

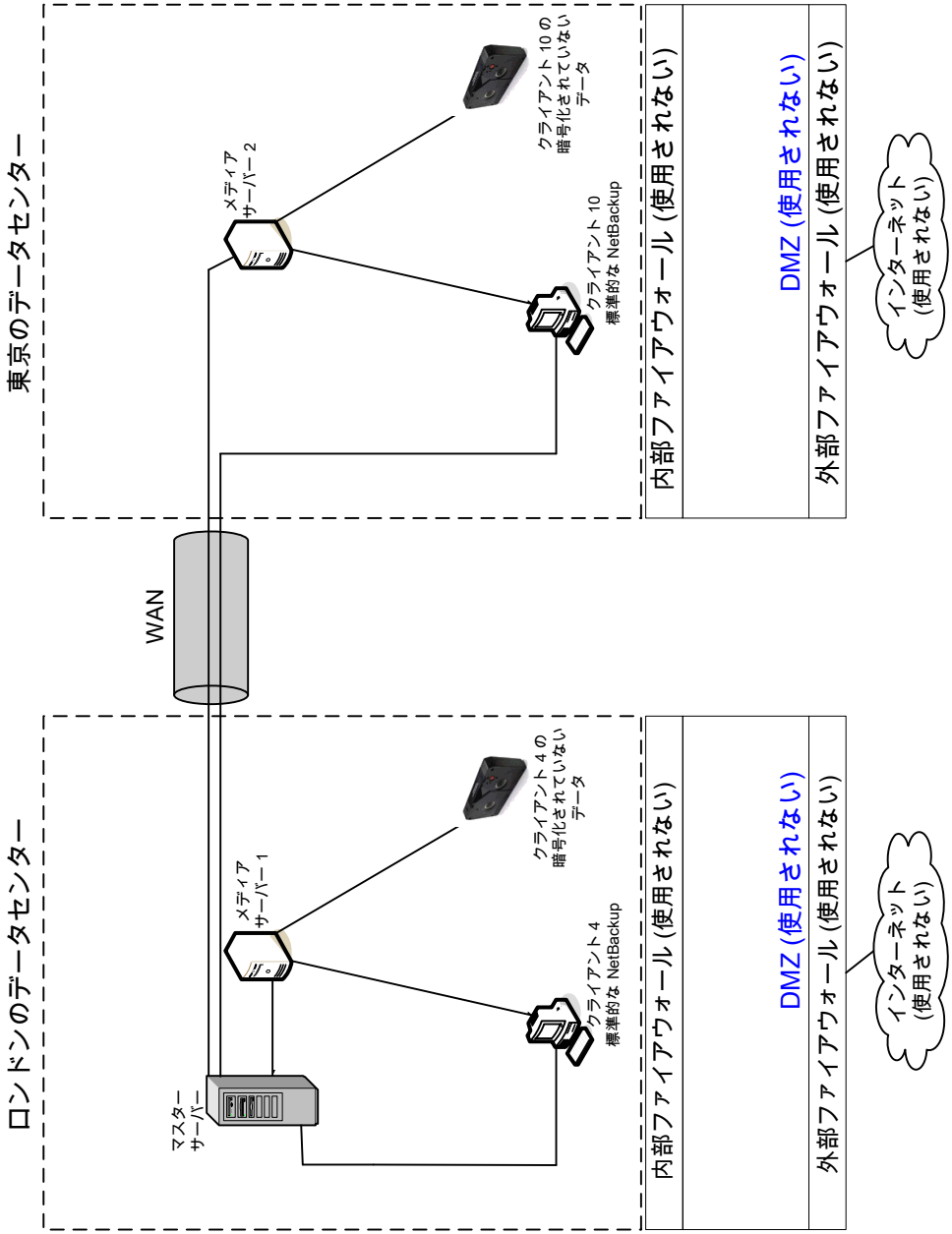
複数のデータセンターには、内部専用のホストと、DMZ を介してインターネットに展開するホストの両方が含まれます。通常、この構成には、ホスト向けの中央集中型ネーミングサービス (DNS、WINS など) が含まれます。また、ユーザー向けの中央集中型ネーミングサービス (NIS、Active Directory など) も含まれます。

標準的な NetBackup を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- 通常、中央集中型ネーミングサービスが存在する
- ホスト数が 50 を超える
- 最も単純な構成で、NetBackup の一般的な知識のみが必要である
- 複数のデータセンターには NetBackup 4.5 から 5.x ユーザー向けの一般的な構成が使用される
- バックアップ時に、回線上でデータの消極的な妨害が行われる危険性がほとんどない

図 2-8 に、標準的な NetBackup を使用する複数のデータセンターの例を示します。

図 2-8　　標準的な NetBackup を使用する複数のデータセンター



次の表に、標準的な NetBackup を実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 2-8　標準的な NetBackup が実装された複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	マスターサーバー、メディアサーバー 1、クライアント 4 の標準的な NetBackup、クライアント 4 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	メディアサーバー 2、クライアント 10 の標準的な NetBackup、クライアント 10 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN を使用することで、マスターサーバーをメディアサーバー 2 およびクライアント 10 に接続できます。
マスターサーバー	ロンドンにあり、ロンドンにあるメディアサーバー 1 と通信します。また、このマスターサーバーは、WAN を介して東京にあるメディアサーバー 2 とも通信します。さらに、ロンドンにある標準的な NetBackup クライアント 4 と通信し、WAN を介して東京にあるクライアント 10 と通信します。
メディアサーバー	複数のデータセンターには 2 つのメディアサーバーがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンのメディアサーバー 1 は、マスターサーバーと、ロンドンにある標準的な NetBackup クライアント 4 とも通信します。メディアサーバー 1 は、ロンドンにあるクライアント 4 の暗号化されていないデータのテープへの書き込みを管理します。 東京のメディアサーバー 2 は、ロンドンにあるマスターサーバーと、東京にある標準的な NetBackup クライアント 10 と通信します。メディアサーバー 2 は、東京にあるクライアント 10 の暗号化されていないデータのテープへの書き込みを管理します。
テープ	テープは、ロンドンと東京の両方のデータセンターで作成されます。ロンドンのテープには、クライアント 4 の暗号化されていないバックアップデータが格納されます。東京のテープには、クライアント 10 の暗号化されていないバックアップデータが格納されます。
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。クライアント 4 と 10 は、標準的な NetBackup 形式です。どちらのクライアントも、ロンドンにあるマスターサーバーで管理できます。これらのクライアントの暗号化されていないデータは、メディアサーバーによってテープにバックアップされます。暗号化されていないデータは、ロンドンのクライアント 4 のテープと、東京のクライアント 10 のテープの両方に書き込まれます。クライアント 10 の照合を行うすべての NetBackup 通信は、暗号化されていない状態で回線 (WAN) を介して東京からロンドンに送信されることに注意してください。
内部ファイアウォール	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、内部ファイアウォールは使用されません。

構成要素	説明
非武装地帯 (DMZ)	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、DMZ は使用されません。
外部ファイアウォール	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、外部ファイアウォールは使用されません。
インターネット	標準的な NetBackup を使用するロンドンまたは東京のデータセンターでは、インターネットは使用されません。

MSEO (Media Server Encryption Option) を使用する複数のデータセンター

MSEO (Media Server Encryption Option) を使用する複数のデータセンターは、中規模から大規模な (50 を超える) ホストのグループで、これらのホストは地理的に 2 か所以上の地域にまたがります。ホストは、WAN (ワイドエリアネットワーク) で接続されています。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

この複数のデータセンターの例には、一般的に 50 を超えるホストを含むことができます。外部に接続するすべてのホストは、MSEO (Media Server Encryption Option) を使用します。この例では、一部のクライアントには暗号化されたバックアップを使用し、その他のホストには MSEO オプションを使用しています。機密性が非常に高いためにオフサイトではアーカイブできないデータは、暗号化されていない形式でその場所に格納されたままになります。

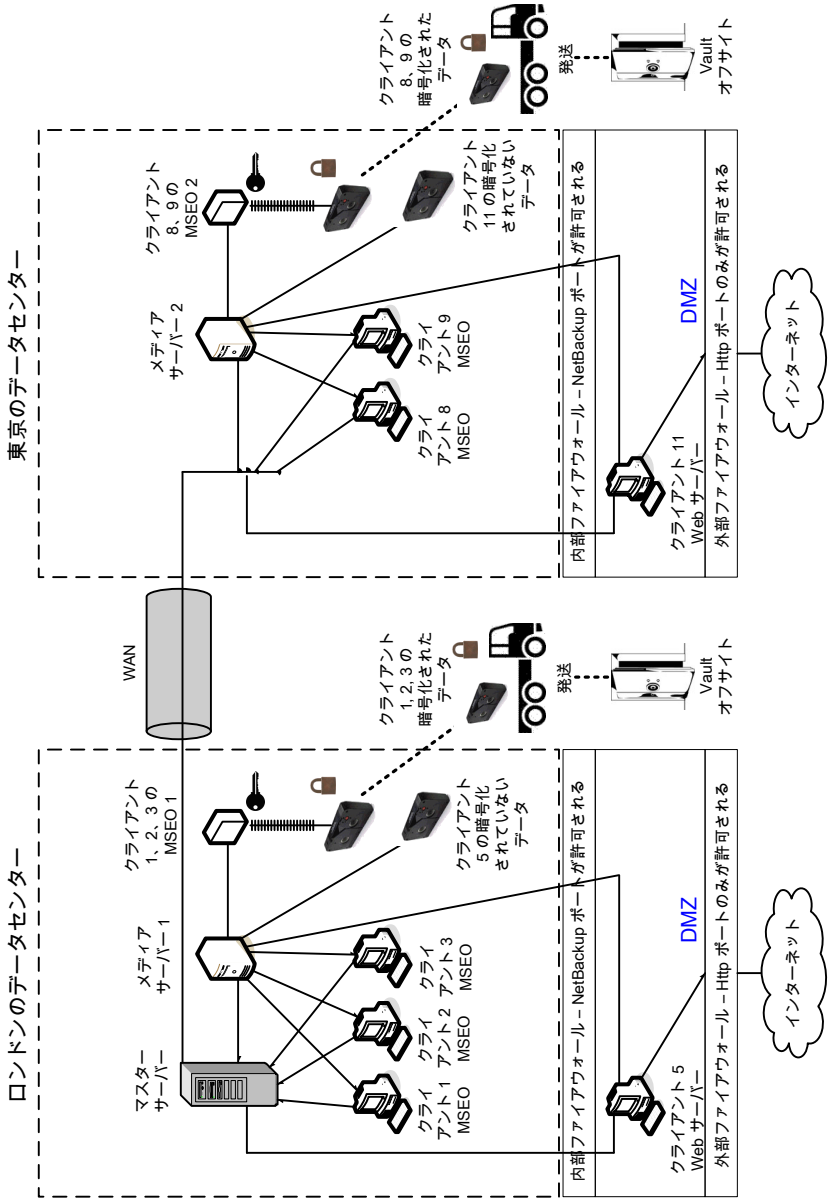
MSEO (Media Server Encryption Option) を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- NetBackup の新しいオプションである
- オフサイトデータの保護に役立つ
- 回線の消極的な妨害は許容リスクであるため、データは暗号化されずにクライアントから送信される
- 単一障害点と同様、鍵の管理と暗号化は 1 か所で管理される高可用性クラスタを使用すると便利です。
- 同時に複数のクライアントを処理するために、堅牢なメディアサーバーが必要である
- 暗号化されたテープをオフサイトに送る必要があるが、CPU に負荷がかかるクライアントの暗号化処理を軽減させる場合に有効である

- データを戻すには鍵が必要である。鍵を失うと、データも失われます。(暗号化の章の鍵の共有バックアップに関する情報を参照してください。)

図 2-9 に、MSEO (Media Server Encryption Option) を使用する複数のデータセンターの例を示します。

図 2-9　MSEO (Media Server Encryption Option) を使用する複数のデータセンター



次の表に、MSEO を実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 2-9 MSEO が実装された複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	マスターサーバー、メディアサーバー 1、MSEO 1、クライアント 1、2、3 および DMZ 内のクライアント 5 Web サーバーが含まれます。また、クライアント 1、2、3 の暗号化されたデータテープと、クライアント 5 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	メディアサーバー 2、MSEO 2、クライアント 8、9 および DMZ 内のクライアント 11 Web サーバーが含まれます。また、クライアント 8、9 用の暗号化されたデータテープと、クライアント 11 用の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN を使用することで、ロンドンのマスターサーバーを、東京のメディアサーバー 2 およびクライアント 8、9、11 に接続できます。
マスターサーバー	ロンドンのデータセンターにあるマスターサーバーは、メディアサーバー 1 およびクライアント 1、2、3、5 と通信します。また、このマスターサーバーは、WAN を使用して東京のメディアサーバー 2 およびクライアント 8、9、11 と通信します。
メディアサーバー	この複数のデータセンターは 2 つのメディアサーバーを使います。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、マスターサーバー、MSEO 1、クライアント 1、2、3、5 と通信します。メディアサーバー 1 は、クライアント 5 の暗号化されていないデータをテープに書き込みます。また、メディアサーバー 1 は、MSEO 1 を使用してクライアント 1、2、3 の暗号化されたデータもテープに書き込みます。暗号化されたテープは、ロンドンのオフサイト Vault に発送されます。 東京のメディアサーバー 2 は、WAN を介してロンドンのマスターサーバーと通信し、また、東京のクライアント 8、9、11 と通信します。メディアサーバー 2 は、クライアント 11 の暗号化されていないデータをテープに書き込みます。また、メディアサーバー 2 は、MSEO 2 を使用してクライアント 8、9 の暗号化されたデータもテープに書き込みます。暗号化されたテープは、東京のオフサイト Vault に発送されます。
MSEO	2 台の MSEO ハードウェア装置により、個々のクライアントでの暗号化処理の負荷が軽減されます。MSEO 装置を使用することで、クライアント側で暗号化を行う場合と比較して、個々のクライアントの CPU パフォーマンスが向上します。MSEO 1 はロンドンのデータセンターにあり、MSEO 2 は東京のデータセンターにあります。MSEO 1 では、クライアント 1、2、3 の暗号化されたデータテープが作成され、ロンドンのオフサイトに格納されます。MSEO 2 では、クライアント 8、9 の暗号化されたデータテープが作成され、東京のオフサイトに格納されます。

構成要素	説明
テープ	暗号化されていないデータテープおよび暗号化されたデータテープの両方が、ロンドンと東京のデータセンターで作成されます。暗号化されたテープには、MSEO によって暗号化されたバックアップデータが格納されます。ロンドンでは、クライアント 5 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。クライアント 1、2、3 用には、暗号化されたテープが書き込まれます。クライアント 1、2、3 の暗号化されたテープは、ディザスタリカバリ保護用にロンドンのオフサイト Vault に発送されます。 東京では、クライアント 11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。クライアント 8、9 用には、暗号化されたテープが書き込まれます。クライアント 8、9 の暗号化されたテープは、ディザスタリカバリ保護用に東京のオフサイト Vault に発送されます。 **メモ:** データを復号化するには、そのデータの暗号化に使用した鍵が利用可能である必要があります。
トランスポート	2 つのトランスポートがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンのトランスポートトラックにより、クライアント 1、2、3 の暗号化されたテープは、セキュリティ保護されたロンドンのオフサイト Vault 施設に運ばれます。東京のトランスポートトラックにより、クライアント 8、9 の暗号化されたテープは、セキュリティ保護された東京のオフサイト Vault 施設に運ばれます。 **メモ:** 輸送中にテープが失われた場合でも、データセンターの管理者は、データの漏洩リスクを軽減することができます。この漏洩は、データの暗号化により軽減されます。
オフサイト Vault	オフサイトに配置される Vault は 2 つあります。1 つはロンドン、もう 1 つは東京にあります。どちらの Vaultも、暗号化されたテープを格納する安全な施設であり、それぞれのデータセンターとは別の場所に存在します。 **メモ:** 優れたディザスタリカバリ保護を実現するために、暗号化されたテープはデータセンターから離れた場所に格納されます。
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンのクライアント 1、2、3 は MSEO 形式であり、クライアント 5 は DMZ 内に配置されている Web サーバー形式 (MSEO は使用しない) です。どちらの形式のサーバーも、マスターサーバーによって管理できます。また、暗号化されたデータは、MSEO ハードウェア装置が接続されたメディアサーバー 1 によってテープにバックアップされます。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。 東京のクライアント 8、9 は MSEO の形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式 (MSEO は使用しない) です。どちらの形式のサーバーも、ロンドンにあるマスターサーバーによって管理できます。また、暗号化されたデータは、MSEO ハードウェア装置が接続されたメディアサーバー 2 によってテープにバックアップされます。クライアント 11 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。

構成要素	説明
内部ファイアウォール	複数のデータセンターは 2 つの内部ファイアウォールを使うことができます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、NetBackup は、内部ファイアウォールを通過して DMZ 内のクライアント 5 (Web サーバー) にアクセスできます。東京では、NetBackup は、内部ファイアウォールを通過して DMZ 内のクライアント 11 (Web サーバー) にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。その他の HTTP ポートは外部ファイアウォールで開くことができますが、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	複数のデータセンターは 2 つの DMZ を使うことができます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 5 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京では、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 11 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。
外部ファイアウォール	MSEO を使用する複数のデータセンターは 2 つの外部ファイアウォールを使うことができます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

クライアント側の暗号化を使用する複数のデータセンター

クライアント側の暗号化オプションを使用する複数のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

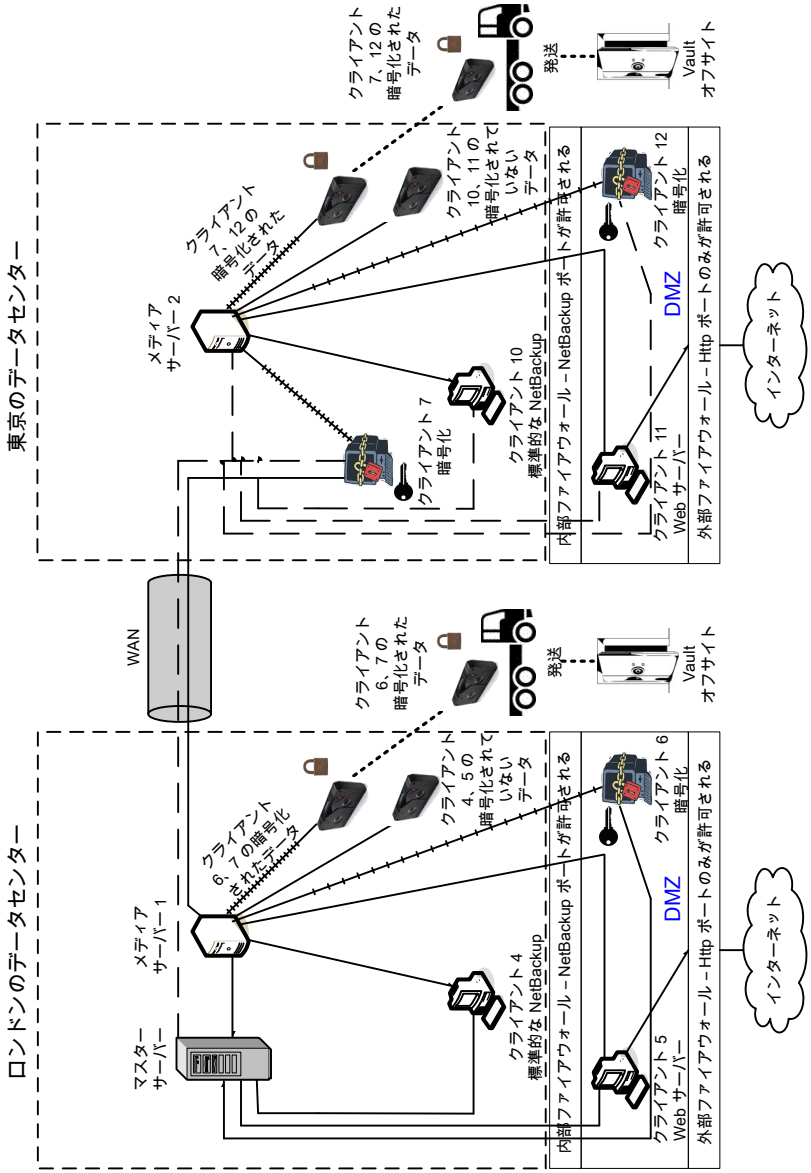
この複数のデータセンターの例では、クライアント側の暗号化を利用して、テープだけでなく回線におけるデータの機密性も確保できます。この暗号化によって、組織内での回線の消極的な盗聴の危険性を軽減できます。テープをオフサイトに移動する際のデータ流出の危険性が軽減されます。このデータセンターモデルでは、中規模から大規模 (50 を超える) の管理対象ホストに対応できます。データセンター内および DMZ 内のクライアントは、ホストおよびユーザー識別情報に中央集中型ネーミングサービスを使うことができます。

クライアント側の暗号化を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- オフサイトデータの保護に役立つ
- クライアントからのデータが暗号化されるため、回線でのデータの消極的な妨害が防止される
- 鍵の管理はクライアントに分散される
- NetBackup 独自の暗号化オプションが使用される
- 暗号化処理にはクライアントの CPU が使用される
- データを戻すには鍵が必要である。鍵を失うと、データも失われます。
- オフサイトでテープをスキャンする必要がある場合または回線上での機密性が必要な場合に有効である

図 2-10 に、クライアント側の暗号化を使用する複数のデータセンターの例を示します。

図 2-10　　クライアント側の暗号化を使用する複数のデータセンター



次の表に、クライアント側の暗号化を実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 2-10 クライアント側の暗号化を実装した複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	マスターサーバー、メディアサーバー 1、クライアント 4、5、6 が含まれます。また、クライアント 6、7 の暗号化されたデータテープと、クライアント 4、5 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	メディアサーバー 2、クライアント 7、10、11、12 が含まれます。また、クライアント 7、12 の暗号化されたデータテープと、クライアント 10、11 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN を使用することで、ロンドンのマスターサーバーを、東京のメディアサーバー 2 およびクライアント 7、10、11、12 に接続できます。また、WAN を使用して、ロンドンのメディアサーバー 1 を、東京のクライアント 7 に接続することもできます。
マスターサーバー	マスターサーバーはロンドンのデータセンターにあり、メディアサーバー 1 およびクライアント 4、5、6 と通信します。また、このマスターサーバーは、WAN を使用して東京のメディアサーバー 2 およびクライアント 7、10、11、12 と通信します。
メディアサーバー	複数のデータセンターは 2 つのメディアサーバーを使います。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、マスターサーバーおよびクライアント 4、5、6 と通信します。また、東京のクライアント 7 とも通信します。メディアサーバー 1 は、クライアント 4、5 の暗号化されていないデータをテープに書き込みます。また、クライアント 6、7 の暗号化されたデータもテープに書き込みます。クライアント 7 は東京に存在しますが、このテープバックアップはロンドンに存在することに注意してください。クライアント 6、7 の暗号化されたテープは、ロンドンのオフサイト Vault に発送されます。 東京のメディアサーバー 2 は、WAN を介してロンドンのマスターサーバーと通信し、また、東京のクライアント 7、10、11、12 と通信します。メディアサーバー 2 は、クライアント 10、11 の暗号化されていないデータをテープに書き込みます。また、クライアント 7、12 の暗号化されたデータもテープに書き込みます。クライアント 7 は東京に存在し、ロンドンでバックアップされますが、東京でもバックアップされることに注意してください。クライアント 7、12 の暗号化されたテープは、東京のオフサイト Vault に発送されます。
クライアント側の暗号化	クライアント側の暗号化 (図には示されていない) によって、テープだけでなく回線におけるデータの機密性も確保されます。

構成要素	説明
テープ	暗号化されていないデータテープおよび暗号化されたデータテープの両方が、ロンドンと東京のデータセンターで作成されます。暗号化されたテープには、クライアント側で暗号化されたバックアップデータが格納されます。ロンドンでは、クライアント 4、5 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。クライアント 6、7 用には、暗号化されたテープが書き込まれます。暗号化されたテープは、ディザスタリカバリ保護用にロンドンのオフサイト Vault に発送されます。 東京では、クライアント 10、11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。クライアント 7、12 用には、暗号化されたテープが書き込まれます。クライアント 7 は東京に存在し、東京でバックアップされますが、ロンドンでもバックアップされることに注意してください。暗号化されたテープは、ディザスタリカバリ保護用に東京のオフサイト Vault に発送されます。 **メモ:** データを復号化するには、そのデータの暗号化に使用した鍵が利用可能である必要があります。
トランスポート	複数のデータセンターは 2 つのトランスポートを使います。1 つはロンドン、もう 1 つは東京にあります。ロンドンのトランスポートトラックにより、クライアント 6、7 の暗号化されたテープは、セキュリティ保護されたロンドンのオフサイト Vault 施設に運ばれます。東京のトランスポートトラックにより、クライアント 7、12 の暗号化されたテープは、セキュリティ保護された東京のオフサイト Vault 施設に運ばれます。クライアント 7 のバックアップコピーは、ロンドンと東京の両方の Vault に格納されることに注意してください。 **メモ:** 輸送中に遠隔の場所でテープが失われた場合でも、データセンターの管理者は、データの漏洩リスクを軽減することができます。漏洩はクライアント側でのデータの暗号化の使用により軽減されます。
オフサイト Vault	複数のデータセンターは 2 つのオフサイト Vault を使います。1 つはロンドン、もう 1 つは東京にあります。どちらの Vault も、暗号化されたテープを格納する安全な施設であり、それぞれのデータセンターとは別の場所に存在します。 **メモ:** 暗号化されたテープをデータセンターから離れた場所に格納することで、ディザスタリカバリ保護が向上します。

構成要素	説明
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンの場合、クライアント 4 は標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。クライアント 6 はクライアント側で暗号化を行うクライアントで、同じく DMZ に配置されています。いずれの形式のクライアントもマスターサーバーによって管理され、クライアントのデータはメディアサーバー 1 によってテープにバックアップされます。クライアント 5 と 6 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 6 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。 東京の場合、クライアント 7 はクライアント側で暗号化を行うクライアントですが、DMZ の外に配置されています。クライアント 10 は、標準的な NetBackup 形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式です。クライアント 12 はクライアント側で暗号化を行うクライアントで、同じく DMZ に配置されています。すべての形式のクライアントは、ロンドンのマスターサーバーによって管理できます。クライアント 7 のデータは、メディアサーバー 1 および 2 によってテープにバックアップされます。クライアント 10、11、12 のデータは、メディアサーバー 2 によってテープにバックアップされます。クライアント 11、12 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。クライアント 12 は、HTTP ポートのみを使用して外部ファイアウォールを通過し、インターネットからの接続を受信します。
内部ファイアウォール	複数のデータセンターは 2 つの内部ファイアウォールを使います。1 つはロンドン、もう 1 つは東京にあります。ロンドンの場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 とクライアント側で暗号化を行うクライアント 6 にアクセスできます。東京の場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 11 とクライアント側で暗号化を行うクライアント 12 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	複数のデータセンターは 2 つの DMZ を使います。1 つはロンドン、もう 1 つは東京にあります。ロンドンの DMZ は、Web サーバークライアント 5 およびクライアント側で暗号化を行うクライアント 6 に対して「安全な」操作領域を提供します。このクライアントは、内部ファイアウォールと外部ファイアウォールとの間に存在します。DMZ 内の Web サーバークライアント 5 およびクライアント側で暗号化を行うクライアント 6 は、NetBackup と通信できます。これらのクライアントは両方とも、指定された NetBackup ポートを使って内部ファイアウォールを通過し、通信を行います。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京の DMZ は、Web サーバークライアント 11 およびクライアント側で暗号化を行うクライアント 12 に対して「安全な」操作領域を提供します。クライアント 12 は、内部ファイアウォールと外部ファイアウォールとの間に存在します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。

構成要素	説明
外部ファイアウォール	複数のデータセンターは 2 つの外部ファイアウォールを使うことができます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。クライアント側で暗号化を行うクライアント 6 には、インターネットからはアクセスできません。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは Web サーバークライアント 11 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。クライアント側で暗号化を行うクライアント 12 には、インターネットからはアクセスできません。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンター

マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンターの例は、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク)で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

このデータセンターの例では、マスターサーバーとメディアサーバー上で NetBackup アクセス制御を使用しています。データセンターでは、NetBackup へのアクセスを部分的に制限し、root 以外のユーザーが NetBackup を管理できるようなっています。この環境では、NBAC はサーバーと GUI 間で使用できるように構成されています。root 以外のユーザーは、オペレーティングシステム (UNIX のパスワードまたは Windows のローカルドメイン) を使って NetBackup にログインできます。また、グローバルユーザーリポジトリ (NIS/NIS+ または Active Directory) を使って NetBackup を管理することができます。さらに、NBAC を使用して、特定のユーザーに対して NetBackup へのアクセスレベルを

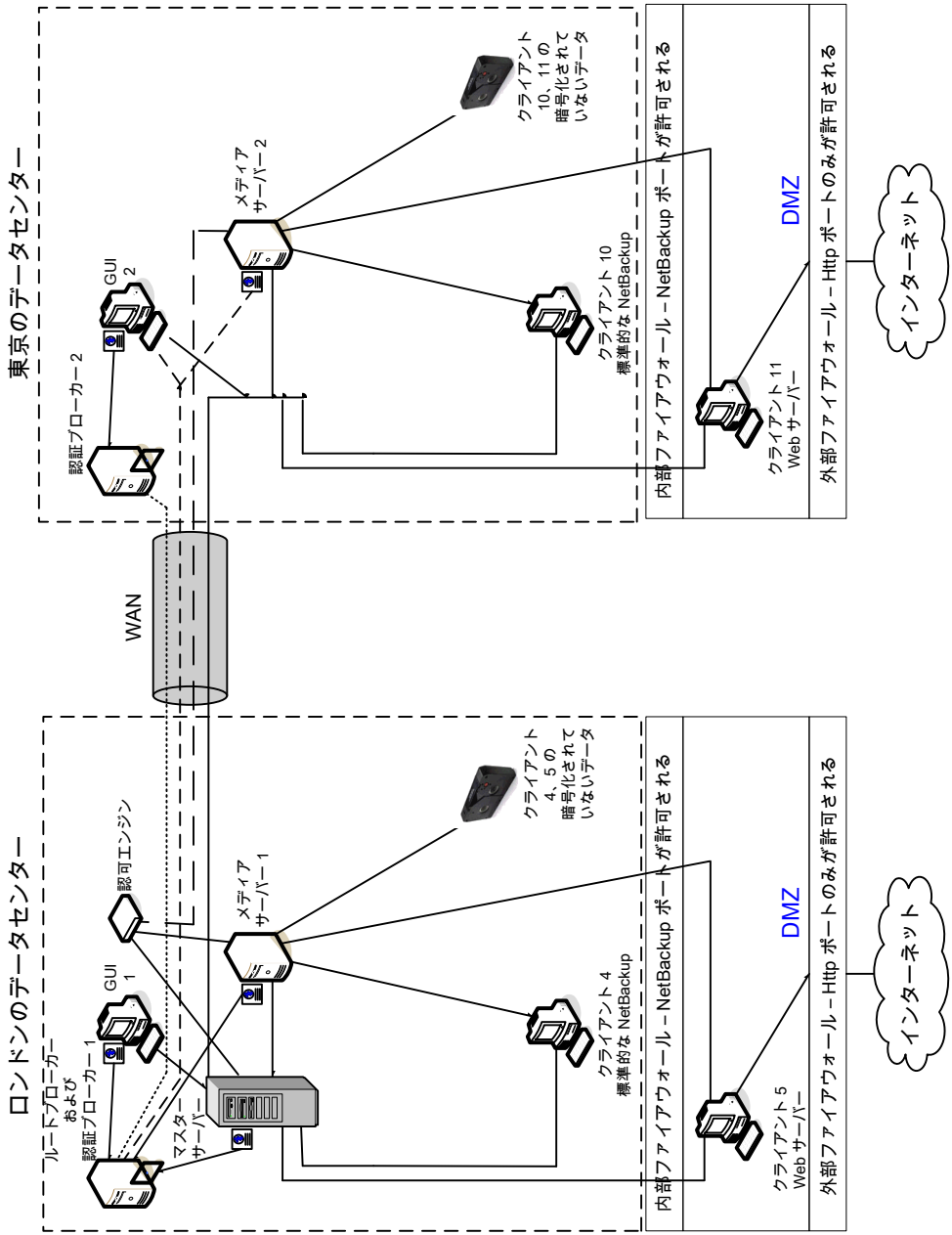
制限することもできます。たとえば、日常的な操作の制御と、新しいポリシーやロボットの追加といった環境構成を分離することもできます。

マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- root 以外のユーザーとして管理する
- Windows のユーザー ID を使用して UNIX を管理する
- UNIX アカウントを使用して Windows を管理する
- 特定のユーザーの操作を分離および制限する
- クライアントホストの root ユーザーまたは管理者はローカルクライアントのバックアップとリストアを実行できる
- 他のセキュリティ関連のオプションと組み合わせることができる
- すべてのサーバーが NetBackup バージョン 5.x 以上である必要がある

図 2-11 に、マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンターの例を示します。

図 2-11 マスターサーバーとメディアサーバーでNBACを使用する複数のデータセンター



次の表に、マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンターのために使われる NetBackup の構成要素を示します。

表 2-11　マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンターで使用される NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	ロンドンのデータセンターには、ルートブローカー、認証ブローカー 1、GUI 1、認可エンジン、マスターサーバー、メディアサーバー 1、クライアント 4、5 が含まれます。また、クライアント 4、5 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	東京のデータセンターには、認証ブローカー 2、GUI 2、メディアサーバー 2、クライアント 10、11 が含まれます。また、クライアント 10、11 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN によって、ルートブローカー/認証ブローカー 1 と認証ブローカー 2 が接続されます。さらに、ルートブローカー/認証ブローカー 1 と GUI 2/メディアサーバー 2 も接続されます。また、WAN によって、認可エンジンはメディアサーバー 2 に接続されます。マスターサーバーは GUI 2、メディアサーバー 2、クライアント 10、11 に接続されます。
マスターサーバー	マスターサーバーは、ロンドンのデータセンターにあり、ルートブローカー/認証ブローカー 1 と通信します。また、GUI 1、認可エンジン、メディアサーバー 1 とも通信します。マスターサーバーは、ロンドンのクライアント 4、5 と通信します。さらに、マスターサーバーは、東京の GUI 2、メディアサーバー 2、クライアント 10、11 とも通信します。
メディアサーバー	この複数のデータセンターの例では、2 つのメディアサーバーがあります。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、マスターサーバー、ルートブローカー/認証ブローカー 1、認可エンジン、クライアント 4、5 と通信します。メディアサーバー 1 は、クライアント 4、5 の暗号化されていないデータをテープに書き込みます。 東京のメディアサーバー 2 は、WAN を介してロンドンのマスターサーバーおよび認可エンジンと通信します。また、東京の GUI 2、クライアント 10、11 とも通信します。メディアサーバー 2 は、クライアント 10、11 の暗号化されていないデータをテープに書き込みます。
GUI	この複数のデータセンターの例では、2 つの GUI があります。GUI 1 はロンドン、GUI 2 は東京にあります。これらのリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびマスターサーバーの機能へのアクセス権を取得します。ロンドンの GUI 1 は、認証ブローカー 1 からクレデンシャルを受信します。GUI 1 には、マスターサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。東京の GUI 2 は、認証ブローカー 2 からクレデンシャルを受信します。GUI 2 には、マスターサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。

構成要素	説明
ルートブローカー	複数のデータセンターのインストールには、ルートブローカーが 1 つのみ必要です。ルートブローカーは、認証ブローカーと組み合わせて使用することもできます。この例では、ルートブローカーと認証ブローカーは同じコンポーネントとして示され、ロンドンのデータセンターに配置されています。ロンドンにあるルートブローカーは、ロンドンの認証ブローカー 1 と、東京の認証ブローカー 2 を認証します。ルートブローカーはクライアントを認証しません。
認証ブローカー	複数のデータセンターのインストールでは、複数の認証ブローカーを配置できます。認証ブローカーをルートブローカーと組み合わせて使用することもできます。このデータセンターのインストールでは、2 つの認証ブローカーが使用されています。認証ブローカーは、マスターサーバー、メディアサーバーおよび GUI に対してそれぞれクレデンシャルを設定し、認証します。認証ブローカーは、コマンドプロンプトを指定するユーザーも認証します。ロンドンの認証ブローカー 1 は、マスターサーバー、メディアサーバー 1、GUI 1 のクレデンシャルを認証します。東京とロンドンにあるすべての NetBackup サーバーとクライアントは、ロンドンの認証ブローカー 1 で認証が行われます。GUI 1 はロンドンの認証ブローカー 1 で認証が行われます。GUI 2 は東京の認証ブローカー 2 で認証が行われます。
認可エンジン	複数のデータセンターのインストールには、認可エンジンが 1 つのみ必要です。認可エンジンは、マスターサーバーおよびメディアサーバーと通信して、認証されたユーザーの権限を決定します。これらの権限によって、ユーザーが利用できる機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。認可エンジンはロンドンに存在し、マスターサーバー、メディアサーバー 1 と通信します。また、認可エンジンは、WAN を介して通信を行い、東京のメディアサーバー 2 へのアクセス権を認可します。 **メモ:** 認可エンジンは、デーモンプロセスとしてマスターサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	暗号化されていないデータテープは、ロンドンのデータセンターと東京のデータセンターで生成されます。ロンドンでは、クライアント 4、5 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。東京では、クライアント 10、11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンの場合、クライアント 4 は標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもマスターサーバーによって管理され、クライアントのデータはメディアサーバー 1 によってテープにバックアップされます。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。 東京の場合、クライアント 10 は標準的な NetBackup 形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもマスターサーバーによって管理され、クライアントのデータはメディアサーバー 2 によってテープにバックアップされます。クライアント 11 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 11 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。

構成要素	説明
内部ファイアウォール	この複数のデータセンターの例では、2 つの内部ファイアウォールがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンの場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 にアクセスできます。東京の場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 11 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、内部ファイアウォールを通過して DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	この複数のデータセンターの例では、2 つの DMZ があります。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 5 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 とクライアント側で暗号化を行うクライアント 6 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京では、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 11 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。
外部ファイアウォール	この複数のデータセンターの例では、2 つの外部ファイアウォールがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは Web サーバークライアント 11 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

すべてに NBAC を使用する複数のデータセンター

すべてに NBAC を使用する複数のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

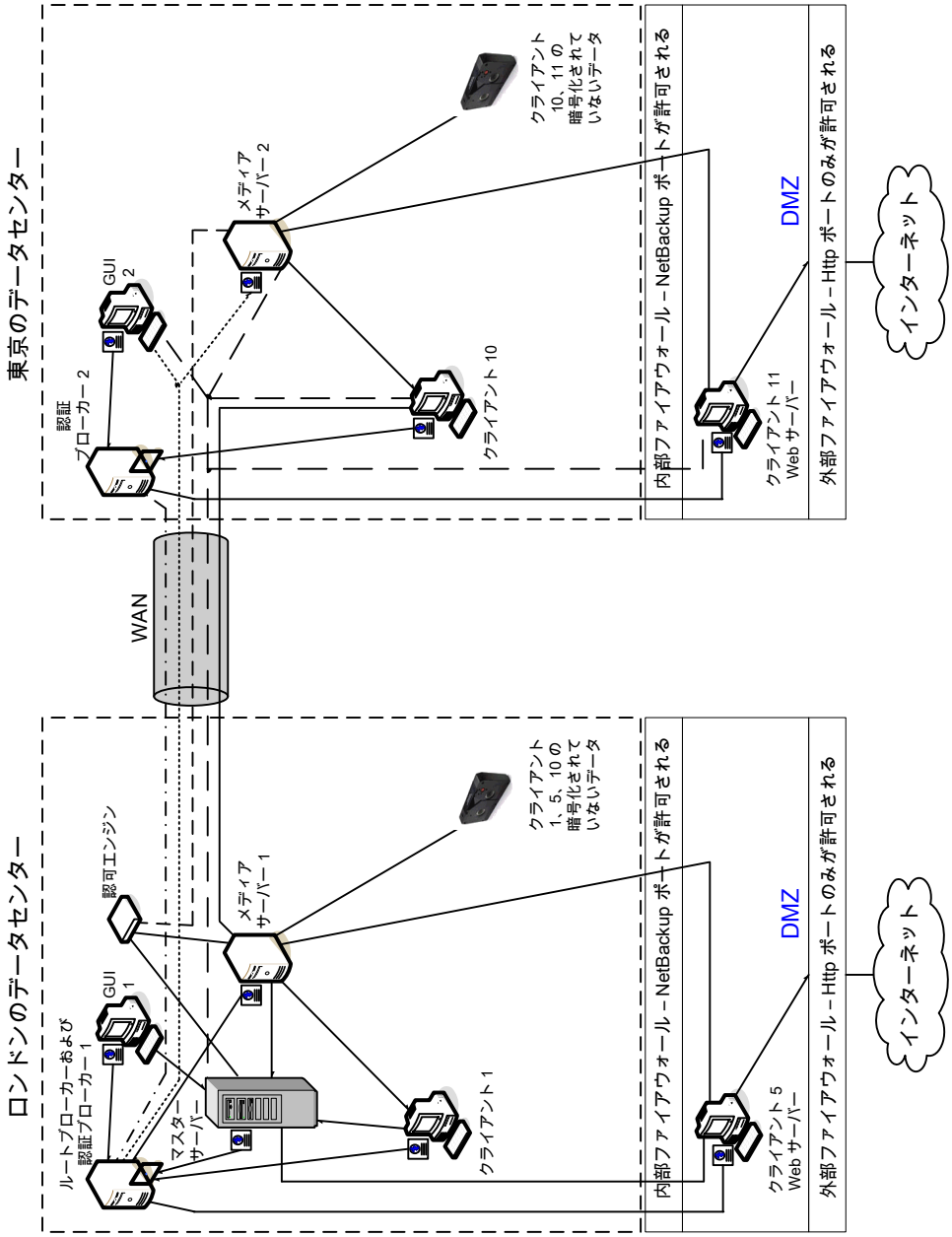
この環境は、マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンターに非常に類似しています。主な違いは、NetBackup 環境に参加するすべてのホストがクレデンシャルを使って確実に識別され、root 以外の管理者が構成可能なアクセスレベルに基づいて NetBackup クライアントを管理できることです。ユーザー識別情報は、Windows の Active Directory または UNIX の NIS などのグローバルリポジトリに存在する場合があります。また、識別情報は、認証ブローカーをサポートするホスト上のローカルのリポジトリ (UNIX のパスワード、Windows のローカルドメイン) に存在する場合もあります。

すべてに NBAC を使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる
- マスターサーバーとメディアサーバーで NBAC を使用する複数のデータセンターの場合の特徴と類似している (クライアントの root ユーザーまたは管理者についての項目は除く)。この構成では、クライアントとサーバーの root 以外の管理者による管理が許可されています。
- クライアントシステムでは、ローカルバックアップとリストアを行うために root 以外または管理者以外のユーザーが設定される場合がある (デフォルト設定)
- この環境では、NetBackup に含まれるすべてのホストの信頼できる識別が容易である
- すべてのホストは NetBackup バージョン 5.0 以上である必要がある

図 2-12 に、すべてに NBAC を使用する複数のデータセンターの例を示します。

図 2-12　　すべてに NBAC を使用する複数のデータセンター



次の表に、すべてに NBAC を実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 2-12 すべてに NBAC を実装した複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	ロンドンのデータセンターには、ルートブローカー、認証ブローカー 1、GUI 1、認可エンジン、マスターサーバー、メディアサーバー 1、クライアント 1、5 が含まれます。また、クライアント 1、5、10 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	東京のデータセンターには、認証ブローカー 2、GUI 2、メディアサーバー 2、クライアント 10、11 が含まれます。また、クライアント 10、11 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN によって、ルートブローカー/認証ブローカー 1 と認証ブローカー 2 が接続されます。さらに、ルートブローカー/認証ブローカー 1 と GUI 2/メディアサーバー 2 も接続されます。また、WAN によって、認可エンジンはメディアサーバー 2 に接続されます。マスターサーバーは GUI 2、メディアサーバー 2、クライアント 10、11 に接続されます。メディアサーバー 1 はクライアント 10 に接続されます。
マスターサーバー	マスターサーバーは、ロンドンのデータセンターにあり、ルートブローカー/認証ブローカー 1 と通信します。また、GUI 1、認可エンジン、メディアサーバー 1 とも通信します。マスターサーバーは、東京の GUI 2、メディアサーバー 2、クライアント 10、11 と通信します。
メディアサーバー	この複数のデータセンターの例では、2 つのメディアサーバーがあります。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、マスターサーバー、ルートブローカー/認証ブローカー 1、認可エンジン、クライアント 1、5、10 と通信します。メディアサーバー 1 は、クライアント 1、5、10 の暗号化されていないデータをテープに書き込みます。 東京のメディアサーバー 2 は、WAN を介してロンドンのマスターサーバー、ルートブローカー/認証ブローカー 1 および認可エンジンと通信します。また、東京の GUI 2、クライアント 10、11 とも通信します。メディアサーバー 2 は、クライアント 10、11 の暗号化されていないデータをテープに書き込みます。
GUI	この複数のデータセンターの例では、2 つの GUI があります。GUI 1 はロンドン、GUI 2 は東京にあります。これらのリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびマスターサーバーの機能へのアクセス権を取得します。ロンドンの GUI 1 は、認証ブローカー 1 からクレデンシャルを受信します。GUI 1 には、マスターサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。東京の GUI 2 は、認証ブローカー 2 からクレデンシャルを受信します。GUI 2 には、マスターサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。

構成要素	説明
ルートブローカー	複数のデータセンターのインストールには、ルートブローカーが 1 つのみ必要です。ルートブローカーは、認証ブローカーと組み合わせて使用することもできます。この例では、ルートブローカーと認証ブローカーは同じコンポーネントとして示され、ロンドンのデータセンターに配置されています。ロンドンにあるルートブローカーは、ロンドンの認証ブローカー 1 と、東京の認証ブローカー 2 を認証します。ルートブローカーはクライアントを認証しません。
認証ブローカー	データセンターのインストールでは、複数の認証ブローカーを配置できます。認証ブローカーをルートブローカーと組み合わせて使用することもできます。このデータセンターのインストールでは、2 つの認証ブローカーがあります。認証ブローカーは、マスターサーバー、メディアサーバー、GUI およびクライアントに対してそれぞれクレデンシャルを設定し、認証します。認証ブローカーは、コマンドプロンプトを使用するユーザーも認証します。ロンドンの認証ブローカー 1 は、マスターサーバー、メディアサーバー 1、GUI 1、クライアント 1、5 のクレデンシャルを認証します。東京とロンドンにあるすべての NetBackup サーバーとクライアントは、ロンドンの認証ブローカー 1 で認証が行われます。GUI 1 はロンドンの認証ブローカー 1 で認証が行われます。GUI 2 は東京の認証ブローカー 2 で認証が行われます。
認可エンジン	データセンターのインストールには、認可エンジンが 1 つのみ必要です。認可エンジンは、マスターサーバーおよびメディアサーバーと通信して、認証されたユーザーの権限を決定します。これらの権限によって、ユーザーが利用できる機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。認可エンジンはロンドンに存在し、マスターサーバー、メディアサーバー 1 と通信します。また、認可エンジンは、WAN を介して通信を行い、東京のメディアサーバー 2 へのアクセス権を認可します。 **メモ:** 認可エンジンは、デーモンプロセスとしてマスターサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	暗号化されていないデータテープは、ロンドンと東京の両方のデータセンターで作成されます。ロンドンでは、クライアント 1、5、10 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。東京では、クライアント 10、11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。クライアント 10 は東京に存在し、東京でバックアップされますが、ロンドンでもバックアップされることに注意してください。

構成要素	説明
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンの場合、クライアント 1 は標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもマスターサーバーによって管理され、クライアントのデータはメディアサーバー 1 によってテープにバックアップされます。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。 東京の場合、クライアント 10 は標準的な NetBackup 形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式です。いずれの形式のクライアントもマスターサーバーによって管理され、クライアントのデータはメディアサーバー 2 によってテープにバックアップされます。クライアント 11 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 11 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。
内部ファイアウォール	この複数のデータセンターの例では、2 つの内部ファイアウォールを設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンの場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 にアクセスできます。東京の場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 11 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、内部ファイアウォールを通過して DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。
非武装地帯 (DMZ)	この複数のデータセンターの例では、2 つの DMZ を設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 5 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京では、DMZ は、内部ファイアウォールと外部ファイアウォールとの間に存在する Web サーバークライアント 11 に対して、「安全な」操作領域を提供します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。

構成要素	説明
外部ファイアウォール	この複数のデータセンターの例では、2 つの外部ファイアウォールを設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは Web サーバークライアント 11 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

すべての NetBackup セキュリティを使用する複数のデータセンター

すべての NetBackup セキュリティを使用する複数のデータセンターは、中規模から大規模な (50 を超える) ホストのグループとして定義されます。これらのホストは、地理的に 2 か所以上の地域にまたがり、WAN (ワイドエリアネットワーク) で接続することができます。この例では、データセンターの 1 つはロンドンにあり、もう 1 つは東京にあります。両方のデータセンターは、専用の WAN 接続を介して接続されています。

この例では、前述のすべての例が組み合わされています。これは、非常に高度な環境であり、様々なクライアントに対して要件が異なる場合があります。クライアントの要件によっては、ホスト以外での暗号化が必要になることもあります (ホストのリソースが不足している場合やデータベースのバックアップ時など)。また、クライアントの要件によっては、ホスト上のデータの機密性を確保するためにホストでの暗号化が必要になることもあります。NBAC をセキュリティ構成に追加することで、NetBackup 内で管理者、オペレータ、およびユーザーを分離することができます。

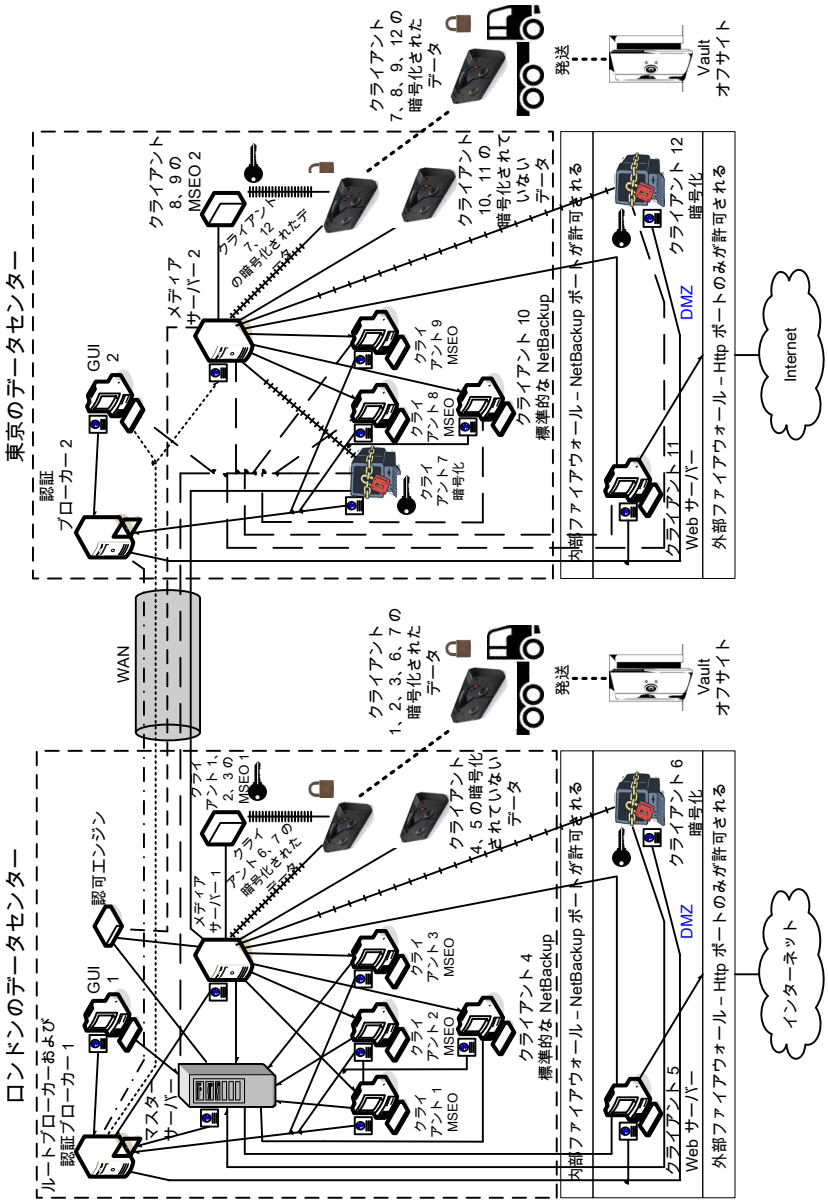
すべての NetBackup セキュリティを使用する複数のデータセンターには、次の特徴があります。

- NetBackup は WAN を介して地理的に 2 か所以上の地域にまたがる

- 個々のオプションの特徴については、前述の複数のデータセンターに関する項を参照
- 最も柔軟性のある複雑な環境である
- 類似モデルに従って綿密に設計することで、各オプションの長所を使用できる

図 2-13 に、すべての NetBackup セキュリティを使用する複数のデータセンターの例を示します。

図 2-13　すべての NetBackup セキュリティを使用する複数のデータセンター



次の表に、すべての NetBackup セキュリティを実装した複数のデータセンターで使われる NetBackup の構成要素を示します。

表 2-13 すべての NetBackup セキュリティを実装した複数のデータセンターにおける NetBackup の構成要素

構成要素	説明
ロンドンのデータセンター	ルートブローカー、認証ブローカー 1、GUI 1 が含まれます。また、認可エンジン、マスターサーバー、メディアサーバー 1、MSEO 1、クライアント 1 から 6、トランスポート、オフサイト Vault も含まれます。また、クライアント 1、2、3、6、7 の暗号化されたデータテープと、クライアント 4、5 の暗号化されていないデータテープが含まれます。ロンドンのデータセンターは、専用の WAN 接続を介して東京のデータセンターに接続されます。
東京のデータセンター	認証ブローカー 2、GUI 2、メディアサーバー 2、MSEO 2、クライアント 7 から 12、トランスポート、オフサイト Vault が含まれます。また、クライアント 7、8、9、12 の暗号化されたデータテープと、クライアント 10、11 の暗号化されていないデータテープが含まれます。東京のデータセンターは、専用の WAN 接続を介してロンドンのデータセンターに接続されます。
WAN (ワイドエリアネットワーク)	東京のデータセンターにロンドンのデータセンターを接続する専用の WAN リンクです。WAN によって、ルートブローカー/認証ブローカー 1 と認証ブローカー 2 が接続されます。さらに、ルートブローカー/認証ブローカー 1 と GUI 2/メディアサーバー 2 も接続されます。また、WAN によって、認可エンジンはメディアサーバー 2 に接続されます。マスターサーバーは GUI 2、メディアサーバー 2、クライアント 7 から 12 に接続されます。メディアサーバー 1 はクライアント 7 に接続されます。
マスターサーバー	マスターサーバーは、ロンドンのデータセンターにあり、ルートブローカー/認証ブローカー 1、GUI 1、認可エンジン、メディアサーバー 1、クライアント 1 から 6 と通信します。また、東京の GUI 2、メディアサーバー 2、クライアント 7 から 12 とも通信します。
メディアサーバー	この複数のデータセンターの例では、2 つのメディアサーバーを設定できます。メディアサーバー 1 はロンドンのデータセンターにあり、メディアサーバー 2 は東京のデータセンターにあります。ロンドンのメディアサーバー 1 は、マスターサーバー、ルートブローカー/認証ブローカー 1 と通信します。また、認可エンジン、MSEO 1、クライアント 1 から 6、7 とも通信します。メディアサーバー 1 は、クライアント 4、5 用に暗号化されないデータをテープに書き込み、クライアント 1 から 6 用に暗号化されたデータをテープに書き込みます。 東京のメディアサーバー 2 は、WAN を介してロンドンのマスターサーバー、ルートブローカー/認証ブローカー 1 および認可エンジンと通信します。また、東京の MSEO 2、GUI 2、クライアント 7 から 12 とも通信します。メディアサーバー 2 は、クライアント 10、11 の暗号化されていないデータをテープに書き込み、クライアント 7、8、9、12 の暗号化されたデータをテープに書き込みます。
GUI	この複数のデータセンターの例では、2 つの GUI を設定できます。GUI 1 はロンドン、GUI 2 は東京にあります。これらのリモート管理コンソール GUI は、認証ブローカーからクレデンシャルを受信します。GUI は受け取ったクレデンシャルを使用して、メディアサーバーおよびマスターサーバーの機能へのアクセス権を取得します。ロンドンの GUI 1 は、認証ブローカー 1 からクレデンシャルを受信します。GUI 1 には、マスターサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。東京の GUI 2 は、認証ブローカー 2 からクレデンシャルを受信します。GUI 2 には、マスターサーバーおよびメディアサーバー 1、2 の機能へのアクセス権が付与されます。

構成要素	説明
ルートブローカー	複数のデータセンターのインストールには、ルートブローカーが 1 つ必要です。ルートブローカーは、認証ブローカーと組み合わせて使用することもできます。この例では、ルートブローカーと認証ブローカーは同じコンポーネントとして示され、ロンドンのデータセンターに配置されています。ロンドンにあるルートブローカーは、ロンドンの認証ブローカー 1 と、東京の認証ブローカー 2 を認証します。ルートブローカーはクライアントを認証しません。
認証ブローカー	データセンターのインストールでは、複数の認証ブローカーを配置できます。認証ブローカーをルートブローカーと組み合わせて使用することもできます。このデータセンターのインストールでは、2 つの認証ブローカーが使用されています。認証ブローカーは、マスターサーバー、メディアサーバー、GUI およびクライアントに対してそれぞれクレデンシャルを設定し、認証します。認証ブローカーは、コマンドプロンプトを使用するユーザーも認証します。ロンドンの認証ブローカー 1 は、マスターサーバー、メディアサーバー 1、GUI 1、クライアント 1 から 6 のクレデンシャルを認証します。東京とロンドンにあるすべての NetBackup サーバーとクライアントは、ロンドンの認証ブローカー 1 で認証が行われます。GUI 1 はロンドンの認証ブローカー 1 で認証が行われます。GUI 2 は東京の認証ブローカー 2 で認証が行われます。
認可エンジン	複数のデータセンターのインストールには、認可エンジンが 1 つのみ必要です。認可エンジンは、マスターサーバーおよびメディアサーバーと通信して、認証されたユーザーの権限を決定します。これらの権限によって、ユーザーが利用できる機能が決まります。また、認可エンジンには、ユーザーグループおよび権限が格納されます。認可エンジンはロンドンに存在し、マスターサーバー、メディアサーバー 1 と通信します。また、認可エンジンは、WAN を介して通信を行い、東京のメディアサーバー 2 へのアクセス権を認可します。 **メモ:** 認可エンジンは、デーモンプロセスとしてマスターサーバーに存在します。この図では、例に示すために個別のイメージとして示しています。
テープ	暗号化されていないデータテープおよび暗号化されたデータテープが、ロンドンと東京のデータセンターで作成されます。ロンドンでは、クライアント 4、5 用に、暗号化されていないテープが書き込まれ、ロンドンのデータセンターのオンサイトに格納されます。クライアント 1、2、3、6、7 用には、暗号化されたテープが書き込まれます。暗号化されたテープは、ディザスタリカバリに備えてロンドンのオフサイト Vault に発送されます。東京では、クライアント 10、11 用に、暗号化されていないテープが書き込まれ、東京のデータセンターのオンサイトに格納されます。クライアント 7、8、9、12 用には、暗号化されたテープが書き込まれます。暗号化されたテープは、ディザスタリカバリ保護用に東京のオフサイト Vault に発送されます。クライアント 7 は東京に存在し、東京でバックアップされますが、さらにセキュリティとバックアップの冗長性を高めるためにロンドンでもバックアップされます。 **メモ:** データを復号化するには、そのデータの暗号化に使用した鍵が利用可能である必要があります。

構成要素	説明
トランスポート	トランスポートを 2 つ設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンのトランスポートトラックにより、クライアント 1、2、3、6、7 の暗号化されたテープは、セキュリティ保護されたロンドンのオフサイト Vault 施設に運ばれます。東京のトランスポートトラックにより、クライアント 7、8、9、12 の暗号化されたテープは、セキュリティ保護された東京のオフサイト Vault 施設に運ばれます。クライアント 7 のバックアップコピーは、ロンドンと東京の両方の Vault に格納されることに注意してください。 **メモ:** 輸送中にテープが失われた場合でも、データセンターの管理者は、データをクライアント側で暗号化することでデータの漏洩リスクを軽減することができます。
オフサイト Vault	オフサイト Vault を 2 つ配置できます。1 つはロンドン、もう 1 つは東京にあります。どちらの Vault も、暗号化されたテープを格納する安全な施設であり、それぞれのデータセンターとは別の場所に存在します。 **メモ:** 暗号化されたテープをデータセンターから離れた場所に格納することで、ディザスタリカバリ保護が向上します。
クライアント	クライアントは、ロンドンと東京の両方のデータセンターに配置されています。ロンドンの場合、クライアント 1 から 3 は、MSEO による暗号化形式です。クライアント 4 は、標準的な NetBackup 形式です。クライアント 5 は、DMZ に配置されている Web サーバー形式です。クライアント 6 は、クライアント側で暗号化を行う形式のクライアントで、同じく DMZ に配置されています。いずれの形式のクライアントもマスターサーバーによって管理され、クライアントのデータはメディアサーバー 1 によってテープにバックアップされます。クライアント 5 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 5 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。 東京の場合、クライアント 7 から 9 は、MSEO による暗号化形式です。クライアント 10 は、標準的な NetBackup 形式です。クライアント 11 は、DMZ に配置されている Web サーバー形式です。クライアント 12 は、クライアント側で暗号化を行う形式のクライアントで、同じく DMZ に配置されています。すべての形式のクライアントはマスターサーバーによって管理でき、クライアントのデータはメディアサーバー 2 を介してテープにバックアップされます。クライアント 7 は、メディアサーバー 1 と 2 の両方から管理できることに注意してください。クライアント 11 は、NetBackup ポートのみを使用して内部ファイアウォールを通過し、NetBackup と通信します。また、クライアント 11 は HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットからの接続を受信します。
内部ファイアウォール	この複数のデータセンターの例では、2 つの内部ファイアウォールがあります。1 つはロンドン、もう 1 つは東京にあります。ロンドンの場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 5 と暗号化クライアント 6 にアクセスできます。東京の場合、NetBackup は、内部ファイアウォールを通過して DMZ 内の Web サーバークライアント 11 と暗号化クライアント 12 にアクセスできます。選択された NetBackup ポートおよび他のアプリケーションポート (可能な場合) のみが、内部ファイアウォールを通過して DMZ とのデータ通信を行うことができます。外部ファイアウォールで開かれている HTTP ポートは、内部ファイアウォールを通過できません。

構成要素	説明
非武装地帯 (DMZ)	この複数のデータセンターの例では、2 つの DMZ を設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンの DMZ は、Web サーバークライアント 5 および暗号化クライアント 6 に対して「安全な」操作領域を提供します。これらのクライアントは、内部ファイアウォールと外部ファイアウォールの間に存在します。DMZ 内の Web サーバークライアント 5 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 5 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。 東京の DMZ は、Web サーバークライアント 11 および暗号化クライアント 12 に対して「安全な」操作領域を提供します。これらのクライアントは、内部ファイアウォールと外部ファイアウォールの間に存在します。DMZ 内の Web サーバークライアント 11 は、指定の NetBackup ポートを使用して内部ファイアウォールを通過し、NetBackup と通信できます。また、Web サーバークライアント 11 は、HTTP ポートのみを使用して外部ファイアウォールも通過し、インターネットに接続することができます。
外部ファイアウォール	この複数のデータセンターの例では、2 つの外部ファイアウォールを設定できます。1 つはロンドン、もう 1 つは東京にあります。ロンドンでは、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 5 にアクセスできます。NetBackup ポートは Web サーバークライアント 5 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 5 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。 東京では、外部ユーザーは、HTTP ポートを経由して外部ファイアウォールを通過し、インターネットから DMZ 内の Web サーバークライアント 11 にアクセスできます。NetBackup ポートは Web サーバークライアント 11 に対して開かれており、内部ファイアウォールを通過して NetBackup と通信できます。NetBackup ポートは、外部ファイアウォールを通過してインターネットに接続することはできません。Web サーバークライアント 11 の HTTP ポートのみが外部ファイアウォールを通過してインターネットに接続できます。
インターネット	インターネットは 1 つしかありませんが、この複数のデータセンターの例では 2 つのインターネット接続があります。1 つはロンドン、もう 1 つは東京にあります。インターネットは、相互に接続されたコンピュータネットワークの集まりで、銅線、ファイバー光ケーブル、および無線接続によってリンクされています。ロンドンでは、Web サーバークライアント 5 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。東京では、Web サーバークライアント 11 は、HTTP ポートを使用して外部ファイアウォールを通過し、インターネットでの通信を行うことができます。

3

ポートセキュリティ

この章では以下の項目について説明しています。

- NetBackup TCP/IP ポートについて
- NetBackup のデーモン、ポート、通信について
- ポートの構成について
- NDMP バックアップのポート要件
- サードパーティの製品とともに NetBackup を使う場合の既知のファイアウォールの問題

NetBackup TCP/IP ポートについて

他のアプリケーションソフトウェアのように、NetBackup はネットワークにデータパケットを送り、ネットワークからデータパケットを受信します。オペレーティングシステムは、TCP/IP 用語でポートとして知られているキューで、これらのデータパケットを編成します。NetBackup のすべてのデータ通信は、TCP/IP プロトコルを使用します。

NetBackup では、2 種類のポートが使用されます。これらのポートは、予約済みポートおよび予約されていないポートと呼ばれます。これらのポートは、次のとおりです。

- 予約済みポートは 1024 番以下のポートで、通常、オペレーティングシステムのコンポーネントにのみアクセスできます。

  NetBackup マスターサーバーは予約済みポートを使用して、ネットワーク上のクライアント、メディアサーバーおよび NetBackup の他のコンポーネントに存在する NetBackup ソフトウェアのより古いリビジョンと通信します。これらは、back-rev 接続と呼ばれることがあります。コールバックは back-rev 接続にのみ使われます。

- 予約済みでないポートは 1024 以上の番号が付いています。ユーザーアプリケーションはこれらのポートにアクセスできます。

一部の NetBackup ポートは Internet Assigned Numbers Authority (IANA) に登録され、他の NetBackup ポートは動的に割り当てられます。表 3-1 はこれらのポートを説明します。

表 3-1 TCP/IP 接続を有効にするために NetBackup が使うポート

ポート	説明
登録ポート	NetBackup サービスとして割り当てられ、Internet Assigned Numbers Authority (IANA) へ恒久的に登録されているポートを示します。たとえば、NetBackup Client デーモン bpcd のポートは 13782 です。デフォルトポート番号を上書きする必要がある場合、次のファイルでエントリを指定できます。 ■ UNIX システムでは、/etc/services ファイルでポートを指定できます。 ■ Windows システムでは、%systemroot%¥System32¥drivers¥etc¥services ファイルでポートを指定できます。
動的割り当てポート	NetBackup クライアントおよびサーバー上で指定可能な範囲から割り当てられているポートを示します。 範囲内のポート番号をランダムに選択するように NetBackup を構成できます。あるいは、範囲の先頭で開始し、利用可能な最初のポートを使うように NetBackup を構成できます。

注意: NetBackup サービスおよびインターネットサービスのポートには、デフォルトのポート番号の設定を使用することをお勧めします。

デーモンのポート番号を修正したら、互いに通信するすべての NetBackup マスターサーバー、メディアサーバーおよびクライアントシステムで、デーモンのポート番号が同一であることを確認してください。シマンテック社のテクニカルサポートに連絡する必要がある場合は、NetBackup 環境のすべての標準以外のポートを技術サポート担当者に知らせてください。

次の他のガイドには、NetBackup ポートについての情報が記載されています。

- 『NetBackup 管理者ガイド Vol. 1』
- 『NetBackup 管理者ガイド Vol 2』

次のトピックには、NetBackup ポートについての情報が記載されています。

- p.96 の「NetBackup のデーモン、ポート、通信について」を参照してください。
- p.107 の「ポートの構成について」を参照してください。
- p.118 の「NDMP バックアップのポート要件」を参照してください。
- p.118 の「サードパーティの製品とともに NetBackup を使う場合の既知のファイアウォールの問題」を参照してください。

NetBackup のデーモン、ポート、通信について

次の項では、NetBackup デーモンが使うポートについて説明します。

- p.96 の「NetBackup の標準ポート」を参照してください。
- p.97 の「NetBackup マスターサーバーの外部接続ポート」を参照してください。
- p.98 の「NetBackup メディアサーバーの外部接続ポート」を参照してください。
- p.99 の「NetBackup 企業メディア管理 (EMM)サーバーの送信ポート」を参照してください。
- p.100 の「クライアントの外部接続ポート」を参照してください。
- p.100 の「Windows 管理コンソールおよび Java サーバーの外部接続ポート」を参照してください。
- p.101 の「Java コンソールの外部接続ポート」を参照してください。
- p.102 の「NetBackup と相互運用する製品のためのポートの追加情報」を参照してください。

NetBackup の標準ポート

表 3-2 に、NetBackup 環境の標準ポートを示します。一部のデーモンはアドオン製品にのみ関連付けられます。［注意事項 (Notes)］列はデーモンを使う製品を示します。

表 3-2 NetBackup の標準環境で使われるデーモンおよびポート

ソース	ポート名およびポート番号	宛先	注意事項
NetBackup マスターサーバー	13724	NetBackup マスターサーバー、メディアサーバー、またはクライアント	ネットワークデーモン、VNETD。
NetBackup メディアサーバー	13724	NetBackup マスターサーバー、メディアサーバー、またはクライアント	ネットワークデーモン、VNETD。
クライアント	13724	NetBackup マスターサーバー	ネットワークデーモン、VNETD。
NetBackup マスターサーバー	veritas_pbx 1556	NetBackup マスターサーバー、メディアサーバー、またはクライアント	Symantec Private Branch Exchange サービス、VxPBX。
NetBackup メディアサーバー	veritas_pbx 1556	NetBackup マスターサーバー、メディアサーバー、またはクライアント	Symantec Private Branch Exchange サービス、VxPBX。

ソース	ポート名および ポート番号	宛先	注意事項
クライアント	`veritas_pbx` 1556	NetBackup マスターサーバー	Symantec Private Branch Exchange サービス、VxPBX。
NetBackup マスターサーバー、メディアサーバー、またはクライアント	`vrts-at-port` 13783	master	NetBackup Authentication Service、VxAT。 `nbatd` プロセスは旧バージョンのメディアサーバーとクライアントの場合は 13783 番のポートで待機します。NetBackup のメディアサーバーとクライアントは PBX ポートを使って接続します。
NetBackup マスターサーバーまたはメディアサーバー	`vrts-auth-port` 13722	NetBackup マスターサーバー	NetBackup Authorization Service、VxAZ。 `nbazd` プロセスは旧バージョンのメディアサーバーとクライアントの場合は 13722 番のポートで待機します。NetBackup のメディアサーバーとクライアントは PBX ポートを使って接続します。

NetBackup 環境では、ポート番号はソースコンポーネントのクライアントポートウィンドウまたはクライアント予約済みポートウィンドウから常に取得されます。一般的な NetBackup 環境は、次のトピックで説明されている追加デーモンおよびポートを使います。

NetBackup マスターサーバーの外部接続ポート

表 3-3 はマスターサーバーがデータパケットを送信するために使用するポートを示します。

表 3-3 NetBackup マスターサーバー送信ポートおよび宛先

ポート名および ポート番号	宛先	注意事項
veritas_pbx 1556	メディアサーバー	ジョブ情報を取得するために接続を再確立します。 リソース情報を取得するために接続を再確立します。 メディアサーバーで NetBackup ソフトウェアリリースレベルを判断します。 バックアップとリストアのために bpbrm を開始します。 テープストレージユニットを管理するために、bptm を開始します。 ディスクストレージユニットを管理するために、bpstsinfo を開始します。 メディアサーバーのホストプロパティにアクセスまたは更新します。
veritas_pbx 1556	企業メディア管理 (EMM) サーバー	クライアントで NetBackup ソフトウェアリリースレベルを判断します。 デバイス、メディアおよびストレージのデータベースについての情報にアクセスします。 マルチストリームバックアップのマウントポイントのリストを取得します。 クライアントのホストプロパティにアクセスまたは更新します。
veritas_pbx 1556	管理コンソールまたは Java サーバー	アクティビティモニターを取得するために接続を再確立します。
veritas_pbx 1556	Java コンソール	ジョブモニターを取得するために接続を再確立します。
vrts-at-port 13783	認証サーバー	ユーザーおよびコンピュータを認証します。 次のいずれも該当する場合にのみ使用されます。 ■ NetBackup のアクセス制御 (NBAC) が有効である。 ■ NetBackup 環境のメディアサーバーおよびクライアントが、マスターサーバーのリリースレベルより低い NetBackup ソフトウェアリリースレベルをホストしている。
vrts-auth-port 13722	認可サーバー	システム管理ユーザーを承認します。 NBAC が有効な場合にのみ使用されます。

NetBackup メディアサーバーの外部接続ポート

表 3-4 はメディアサーバーがデータパケットを送信するために使用するポートを示します。表は、ポート名、ポート番号、宛先および追加情報を示したものです。

表 3-4 NetBackup メディアサーバー送信ポートおよび宛先

ポート名および ポート番号	宛先	注意事項
veritas_pbx 1556	マスターサーバー	bpdbm からレガシーポリシー情報にアクセスします。 bpjobd からレガシージョブ情報にアクセスします。 bpdbm へイメージのカタログ情報を更新します。 bprd にその他の要求を送信します。 ジョブ情報にアクセスします。 リソース情報にアクセスします。
veritas_pbx 1556	メディアサーバー	複製、ディスクのステージングおよび合成のために、他のメディアサーバーへのソケットを確立します。
veritas_pbx 1556	企業メディア管理 (EMM) サーバー	デバイス、メディアおよびストレージのデータベースについての情報にアクセスします。
veritas_pbx 1556	クライアント	クライアントで NetBackup ソフトウェアリリースレベルを判断します。
vrts-at-port 13783	認証サーバー	ユーザーおよびコンピュータを認証します。 NetBackup アクセス制御 (NBAC) が有効な場合にのみ使用されます。
vrts-auth-port 13722	認可サーバー	システム管理ユーザーを認証します。 NBAC が有効な場合にのみ使用されます。

NetBackup 企業メディア管理 (EMM)サーバーの送信ポート

表 3-5 は EMM サーバーがデータパケットを送信するために使用するポートを示します。

表 3-5 NetBackup EMM サーバー送信ポートおよび宛先

ポート名および ポート番号	宛先	注意事項
veritas_pbx 1556	マスターサーバー	デバイス、メディアおよびストレージのデータベースについての情報を取得するために接続を再確立します。
veritas_pbx 1556	メディアサーバー	デバイス、メディアおよびストレージのデータベースについての情報を取得するために接続を再確立します。

ポート名および ポート番号	宛先	注意事項
veritas_pbx 1556	管理コンソールまたは Java サーバー	デバイス、メディアおよびストレージのデータベースについての情報を取得するために接続を再確立します。
vrts-at-port 13783	認証サーバー	ユーザーおよびコンピュータを認証します。 次のいずれも該当する場合にのみ使用されます。 ■ NetBackup のアクセス制御 (NBAC) が有効である。 ■ NetBackup 環境のメディアサーバーおよびクライアントが、マスターサーバーのリリースレベルより低い NetBackup ソフトウェアリリースレベルをホストしている。
vrts-auth-port 13722	認可サーバー	システム管理ユーザーを承認します。

クライアントの外部接続ポート

表 3-6 はクライアントがデータパケットを送信するために使用するポートを示します。

表 3-6 NetBackup クライアント送信ポートおよび宛先

ポート名および ポート番号	宛先	注意事項
veritas_pbx 1556	マスターサーバー	bprd にバックアップ、リストア、および他の要求を送信します。
vrts-at-port 13783	認証サーバー	ユーザーまたはコンピュータを認証します。

Windows 管理コンソールおよび Java サーバーの外部接続ポート

表 3-7 は Windows 管理コンソールと Java サーバーがデータパケットを送信するために使用するポートを示します。

また、Windows 管理コンソールまたは Java サーバーでは、NetBackup Product Authentication and Authorization Service (vxss サーバーと表示) への外部接続ポートも使用されます。

表 3-7 Windows 管理コンソールおよび Java サーバーの外部接続ポートおよび宛先

ポート名およびポート番号	宛先	注意事項
veritas_pbx 1556	マスターサーバー	Job Manager nbjm にアクセスします。 ポリシーを管理します。 ホストのプロパティを管理します。 手動バックアップとリストアを開始します。
veritas_pbx 1556	メディアサーバー	デバイスにアクセスします。
veritas_pbx 1556	企業メディア管理 (EMM) サーバー	デバイス、メディアおよびストレージユニットのデータベースにアクセスします。
vrts-at-port 13783	認証サーバー	管理のためのユーザークレデンシャルを確立します。

Java コンソールの外部接続ポート

表 3-8 は Java コンソールがデータパケットを送信するために使用するポートを示します。

表 3-8 Java コンソール送信ポートおよび宛先

ポート名およびポート番号	宛先	注意事項
veritas_pbx 1556	マスターサーバー	Job Manager nbjm とのソケットを確立します。
vnetd 13724	マスターサーバー	レガシー Job Manager bpjobd とのソケットを確立します。 Java コンソールの NetBackup ソフトウェアのレベルが NetBackup 7.6 未満の場合にのみ使用されます。
vnetd 13724	Java サーバー	レガシー Java サーバー bpjava とのソケットを確立します。 Java コンソールの NetBackup ソフトウェアのレベルが NetBackup 7.6 未満の場合にのみ使用されます。

MSDP ポートの使用について

次の表は NetBackup の重複排除に使われるポートを示したものです。ファイアウォールが各種の重複排除ホストの間にある場合は、その重複排除ホストで指定されているポートを開きます。重複排除ホストは、自身のデータを重複排除する重複排除ストレージサーバー、負荷分散サーバー、およびクライアントです。

ストレージサーバーが 1 つのみで、自身のデータを重複排除する負荷分散サーバーまたはクライアントがない場合、ファイアウォールポートを開く必要はありません。

表 3-9　　重複排除ポート

ポート	使用方法
10082	NetBackup Deduplication Engine (`spoold`)。データを重複排除するホスト間でこのポートを開いてください。ホストには、負荷分散サーバーと、自身のデータを重複排除するクライアントが含まれます。
10102	NetBackup Deduplication Manager (`spad`)。データを重複排除するホスト間でこのポートを開いてください。ホストには、負荷分散サーバーと、自身のデータを重複排除するクライアントが含まれます。
443	PureDisk Storage Pool Authority。自身のデータを重複排除する NetBackup クライアントと PureDisk ストレージプールの間でこのポートを開きます。

Cloud ポートの使用について

NetBackup Cloud は、nbcssc サービスのデフォルトポート番号として 5637 を使用します。

NetBackup と相互運用する製品のためのポートの追加情報

次の項では、NetBackup を OpsCenter、Backup Exec、NetBackup と相互運用するほかの製品とともに使う場合に重要なポート情報を説明します。

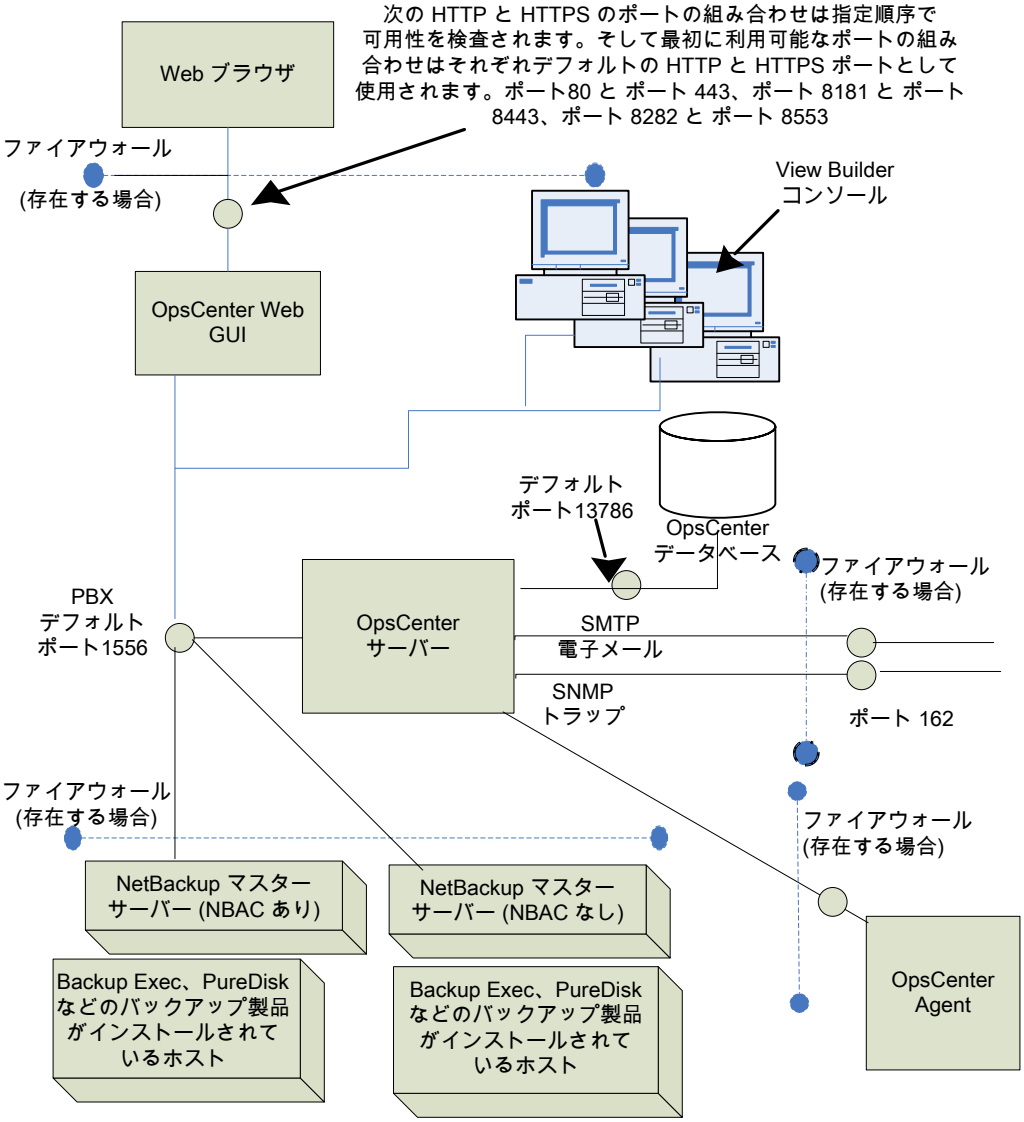
-
- p.104 の「バックアップ製品との通信に必要なポート」を参照してください。
-
- p.106 の「NetBackup Web GUI から NetBackup サーバーソフトウェアへの通信について」を参照してください。
- p.106 の「NetBackup サーバーから NetBackup マスターサーバー (NBSL) への通信について」を参照してください。
- p.107 の「SNMP トラップについて」を参照してください。

- p.107 の「NetBackup Web GUI または NetBackup サーバーから Sybase データベースへの通信について」を参照してください。
- p.107 の「NetBackup Web GUI からNetBackup サーバー電子メールへの通信について」を参照してください。

通信およびファイアウォールについての注意事項

次の図は、NetBackup の主要なコンポーネントと、使用される COM ポートを示します。

図 3-1 NetBackup の主要なコンポーネントと通信方法



バックアップ製品との通信に必要なポート

この項では、NetBackup Agent が 、Backup Exec、PureDisk などのバックアップ製品と通信するために使用するポートについて説明します。

表 3-10 に、各種のバックアップ製品からデータを収集するために NetBackup Agent で開く必要があるポートを示します。

表 3-10 他のバックアップ製品と通信するために必要なポート

バックアップ製品	通信	ポート番号
Backup Exec	NetBackup (Backup Exec データコレクタ) は、Backup Exec API を使って Backup Exec サーバーと通信します。	6106
PureDisk	NetBackup (PureDisk データコレクタ) は `atssl` を使って PureDisk SPA と通信します。	443 (HTTPS) 2821 (AT)

Web ブラウザから NetBackup Web GUI への接続

Web ブラウザでは、セキュリティ保護されていないハイパーテキスト転送プロトコル (HTTP) およびセキュリティ保護されたハイパーテキスト転送プロトコル (HTTPS) を使用して、NetBackup Web GUI と通信します。これらのプロトコルでは、TCP/IP が使用されます。

HTTP では、指定した順序で指定したポートの可用性が確認され、最初に利用可能なポートがデフォルトで使われます。

表 3-11 に、デフォルトの HTTP および HTTPS ポートがどのように選択されるかを示します。

表 3-11 デフォルトの HTTP および HTTPS ポート

選択される順序	HTTP ポート番号	HTTPS ポート番号	説明
1.	80	443	ポート 80 とポート 443 の可用性が確認されます。 ■ ポート 80 とポート 443 が利用可能であれば、ポート 80 がデフォルトの HTTP ポートとして使用され、ポート 443 がデフォルトの HTTPS ポートとして使用されます。 ■ Web サーバーなどの他のアプリケーションによって一方または両方のポートが使用されている場合は、次のポートの組み合わせについて可用性が確認されます。

選択される順序	HTTP ポート番号	HTTPS ポート番号	説明
2.	8181	8443	ポート 8181 とポート 8443 の可用性が確認されます。 ■ ポート 8181 とポート 8443 が利用可能であれば、ポート 8181 がデフォルトの HTTP ポートとして使用され、ポート 8443 がデフォルトの HTTPS ポートとして使用されます。 ■ VCS などの製品と共にインストールされた VRTSWeb など、他のアプリケーションによって一方または両方のポートが使用されている場合は、次のポートの組み合わせについて可用性が確認されます。
3.	8282	8553	ポート 8282 とポート 8553 の可用性が確認されます。

これらの HTTP ポートと HTTPS ポートは入力のためにのみ開かれ、コマンドラインを使って構成可能です。

NetBackup Web GUI から NetBackup サーバーソフトウェアへの通信について

NetBackup Web GUI は、Symantec Private Branch Exchange (PBX) を使用して NetBackup サーバーソフトウェアと通信します。デフォルトのポートは 1556 です。PBX ポートは、入出力の通信用に開かれたポートです。

NetBackup サーバーから NetBackup マスターサーバー (NBSL) への通信について

NetBackup では、NetBackup Service Layer (NBSL) がすべての管理対象のマスターサーバーにある必要があります。

NetBackup サーバーソフトウェアでは、次の方法を使用して NBSL からデータを収集します。

- 初回のデータロード
- 変更の通知またはイベントの待機

NetBackup サーバーソフトウェアが起動されたときや、マスターサーバーのデータ収集が有効にされたとき、またはマスターサーバーが NetBackup に追加されたときに、OpsCenter サーバーは、NBSL を使って NetBackup マスターサーバーから OpsCenter データベースへすべての利用可能なデータの収集を開始します。初回のデータロードは

各データタイプに対して連続的に行われます。初回のデータロードが完了すると、NetBackup サーバーソフトウェアは、NetBackup データの変更に関する通知が NBSL から送信されるまで待機します。それから NetBackup は NetBackup データベースを更新します。

Symantec Private Branch Exchange (PBX) は通信に使われ、入出力のために OpsCenter サーバーと NetBackup マスターサーバーでポートが開いている必要があります。使われるデフォルト PBX ポートは 1556 です。PBX ポートを構成することは OpsCenter 7.5 ではサポートされません。

SNMP トラップについて

SNMP トラッププロトコルは、アウトバウンド UDP トラフィックで使用され、出力用に開かれたポートを必要とします。ポート番号は 162 です。

NetBackup Web GUI または NetBackup サーバーから Sybase データベースへの通信について

NetBackup Web GUI では、デフォルトポート 13786 を使用して、NetBackup Sybase SQL Anywhere データベースサーバーと通信します。

Sybase データベースサーバーポートは、すべてのインバウンド接続に対して閉じられています。NetBackup サーバー上に存在する NetBackup コンポーネントでのみデータベースを使用できます。

NetBackup Web GUI からNetBackup サーバー電子メールへの通信について

SMTP 電子メールサーバープロトコルは、メールの送信に使用されます。ポート番号は、ユーザーが SMTP サーバーポートを指定した際に定義されます (このポートを指定するには、NetBackup コンソールの［設定 (Settings)］>［構成 (Configuration)］>［SMTP サーバー (SMTP Server)］にアクセスします)。このポートは、出力用にのみ開かれたポートです。

ポートの構成について

NetBackup インターフェースでは、ファイアウォールおよび他のネットワーク機能をサポートするために、環境のさまざまなデフォルト以外のポートを構成できます。

次のトピックはポートの構成オプションを設定する方法を説明します。

- p.108 の「ランダムなポートの割り当ての有効化または無効化」を参照してください。
- p.109 の「NetBackup サーバーまたはクライアントのファイアウォール接続オプションの指定」を参照してください。

- p.112 の「接続元コンピュータから接続先コンピュータのファイアウォール接続オプションを指定する」を参照してください。
- p.114 の「構成ファイルのポート情報の編集」を参照してください。
- p.115 の「クライアント接続オプションの更新」を参照してください。
- p.115 の「vm.conf ファイルの Media Manager ポート設定の更新」を参照してください。

ランダムなポートの割り当ての有効化または無効化

[ランダムポート割り当てを使用する (Use random port assignments)] プロパティは他のコンピュータの NetBackup と通信するときに、選択したコンピュータがポートをどのように選択するかを指定します。

- 有効な場合、NetBackup によって、許容範囲内の空きポートからポート番号がランダムに選択されます。たとえば、範囲が 1023 から 5000 である場合、この範囲内の番号から選択されます。これはデフォルトの動作です。
- 無効な場合、NetBackup によって、許容範囲内の利用可能な番号のうち最も大きい番号から順に選択されます。たとえば、範囲が 1023 から 5000 である場合、NetBackup によって 5000 が選択されます (この番号が空きである場合)。5000 が使用される場合、NetBackup は 4999 番ポート選択します。

ポート選択方式はマスターサーバーとすべてのメディアサーバーと同じである必要があります。デフォルトでは、NetBackup はポートをランダムに割り当てます。順次ポート割り当てを使うために、コンピュータのいずれかを変更した場合、順次ポートの割り当てを使用するには、環境のコンピュータすべてを変更してください。

次の手順はポートの割り当てを指定する方法を説明します。

Java または Windows インターフェースからポート割り当てを指定する方法

1. NetBackup 管理コンソール で次のいずれかを展開します。
   - マスターサーバーポートの割り当てを指定するためには、[NetBackup の管理 (NetBackup Management)]>[ホストプロパティ (Host Properties)]>[マスターサーバー (Master Servers)] を展開します。
   - メディアサーバーポートの割り当てを指定するためには、[NetBackup の管理 (NetBackup Management)]>[ホストプロパティ (Host Properties)]>[メディアサーバー (Media Servers)] を展開します。
2. 設定するホストをダブルクリックします。

3 ［ポートの範囲 (Port Ranges)］をクリックします。

4 ［ランダムポート割り当てを使用する (Use random port assignments)］のチェックマークを付くか外します。

環境のマスターサーバーおよびメディアサーバーが同一に設定されることを確かめてください。すなわち、［ランダムポート割り当てを使用する (Use random port assignments)］が両方のシステムで消去されるか、または［ランダムポート割り当てを使用する (Use random port assignments)］が両方のシステムで選択されていることを確かめてください。

NetBackup サーバーまたはクライアントのファイアウォール接続オプションの指定

NetBackup 環境では、接続 (ソースコンピュータ) を開始するコンピュータおよび情報を受信するコンピュータ (宛先コンピュータ) の間の接続オプションを定義できます。

さらに、ソースコンピュータからの他の宛先コンピュータすべてのデフォルト接続オプションを設定できます。たとえば、マスターサーバーとメディアサーバー間にファイアウォールがある場合、NetBackup マスターサーバーからのすべての接続オプションを指定できます。

宛先コンピュータが NetBackup マスターサーバーよりも前の NetBackup バージョンを実行すれば、ソースコンピュータからの接続オプションを指定する機能は、宛先コンピュータの NetBackup リリースレベルによって決まります。詳しくは、宛先コンピュータと一致する NetBackup リリースレベルのマニュアルを参照してください。

ソースコンピュータからファイアウォール接続オプションを指定する方法

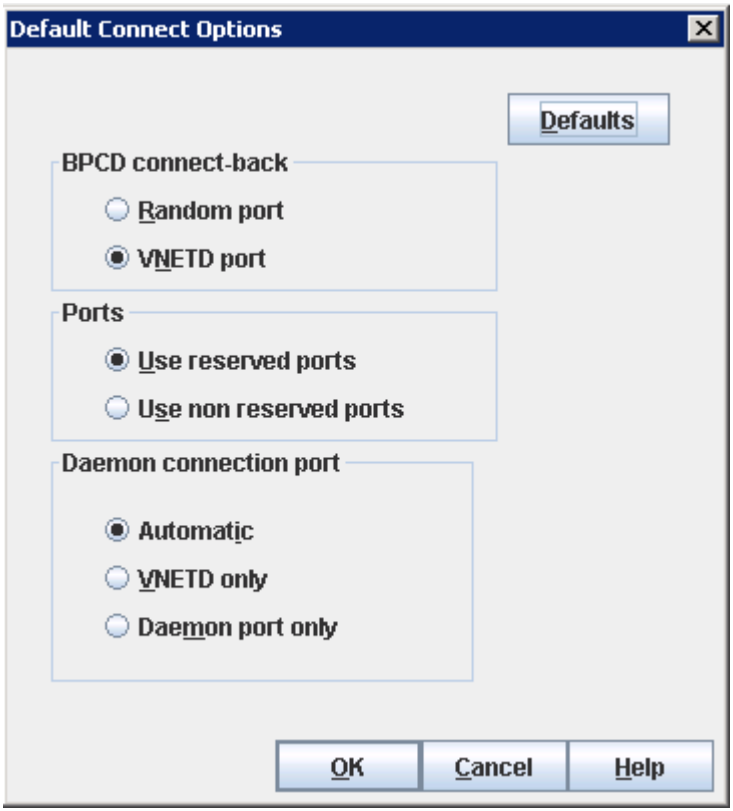
1 NetBackup 管理コンソールで、［NetBackup の管理 (NetBackup Management)］>［ホストプロパティ (Host Properties)］>［マスターサーバー (Master Servers)］を展開します。

2 設定するホストをダブルクリックします。

3 ［ファイアウォール (Firewall)］をクリックします。

4 ［デフォルト接続オプション (Default Connect Options)］ペインで［変更 (Change)］をクリックします。

次のように表示されます。



次の情報は[デフォルト接続オプション (Default Connect Options)]表示に適用されます。

- ソースコンピュータが NetBackup クライアントである場合、[デーモン接続ポート (Daemon connection port)]設定のみが表示されます。
- ソースおよび宛先コンピュータが両方 NetBackup 6.5 リリースレベル以降であれば、[BPCD コネクトバック (BPCD connect-back)]および[ポート (Ports)]の設定は一般に効果をもたらしません。デフォルトでは、NetBackup は予約済みでないポートを使い、コールバックを使いません。

この手順の残りのステップでは、接続オプションを設定する方法を説明します。

5 (オプション) [BPCD コネクトバック (BPCD connect-back)]設定を変更します。

次のいずれかを選択します。

- ランダムポート (Random port)NetBackup 5.1 以前の場合はデフォルト。
ホストコンピュータがレガシー bpcd ランダムポートコールバックメソッドを使用して、他のコンピュータに接続することを指定します。

- VNETD ポート. NetBackup 5.1 より後のリリースのデフォルトです。
  ホストコンピュータが vnetd デーモンを使用して、他のコンピュータに接続することを指定します。

6 (オプション) [ポート (Ports)]設定を変更します。

次のいずれかを選択します。

- [予約済みポートを使用する (Use reserved ports)]これはデフォルトです。
  有効な場合、接続元コンピュータが予約済みのポート番号を使用する宛先コンピュータの bpcd に接続します。
- [予約済みではないポートを使用する (Use nonreserved ports)]
  有効な場合、接続元コンピュータが予約済みではないポート番号を使用する宛先コンピュータの bpcd に接続します。
  この手順のステップ8を実行し、NetBackup 環境の他のコンピュータが予約済みでないポートで構成されること確認してください。

7 (オプション) [デーモン接続ポート (Daemon connection port)]設定を変更します。

次のいずれかを選択します。

- 自動. NetBackup 5.0 以降の場合はデフォルト。
  vnetd デーモンを使用して、他のコンピュータがこのホストに接続することを指定します。vnetd 経由の接続が使用できない場合、デーモンのレガシーポート番号が使用されます。
- [VNETD のみ (VNETD only)]。
  vnetd デーモンのみを使用して、他のコンピュータがこのホストに接続することを指定します。サイトのファイアウォールの規則によって、レガシーポート番号を使用したホストへの接続が禁止されている場合は、必ず、この設定を有効にしてください。
- デーモンポートのみ (Daemon port only)NetBackup 5.0 より前のリリースのデフォルト。
  他のコンピュータがこのホストに接続するのにレガシーのポート番号を使うことを指定します。
  NetBackup 5.0 より前のリリースでは、bpcd への接続には常に bpcd ポート番号が使用されます。
  NetBackup リリース 5.0 以降の場合、接続元および宛先コンピュータが両方とも NetBackup 5.0 以上である場合、bpcd への接続に vnetd ポート番号を使用できます。
  vnetd ポート番号を使用して bpcd 接続が行われる場合、[ポート (Ports)]および[BPCD コネクトバック (BPCD connect-back)]のオプションは無視されます。この場合、NetBackup は予約されていない接続元ポート番号、vnetd 宛先ポート番号が使用され、コールバックは行われません。

この設定は veritas_pbx、veritas-at-port、およびveritas-auth-port への接続に影響しません。これらの接続には、常にレガシーまたは IANA で定義されたポート番号が使用されます。

8 (該当する場合のみ) 予約済みでないポートを使うためには、NetBackup 環境の他のコンピュータを構成してください。

[予約済みではないポートを使用する (Use nonreserved ports)]を選択したら、このステップを実行します。

環境のホストが NetBackup 6.5 以前を実行する場合、デフォルトである予約済みではないポートの接続をホストが許可することを確認してください。[NetBackup 管理コンソール (NetBackup Administration Console)]>[ホストプロパティ (Host Properties)]>[ユニバーサル設定 (Universal Settings)]をクリックし、必ず[予約されていないポートでの接続を許可する (Accept connections on nonreserved ports)]を選択します。このプロパティについて詳しくは、NetBackup 6.5 のマニュアルを参照してください。

予約済みでないポートを使うようにクライアントを構成します。[クライアント属性 (Client Attributes)]ダイアログボックスの[接続オプション (Connect Options)]タブの NetBackup 管理コンソールからこのタスクを実行できます。このタブのオプションを使う方法について詳しくは、『Symantec NetBackup 管理者ガイド』を参照してください。

接続元コンピュータから接続先コンピュータのファイアウォール接続オプションを指定する

次の手順は、特定の接続先コンピュータに適用されるファイアウォール接続オプションを接続元コンピュータで指定する方法です。たとえば、マスターサーバーからのこの手順を実行し、クライアントの接続オプションを指定できます。

接続先コンピュータに適用されるファイアウォール接続オプションを接続元コンピュータで指定する方法

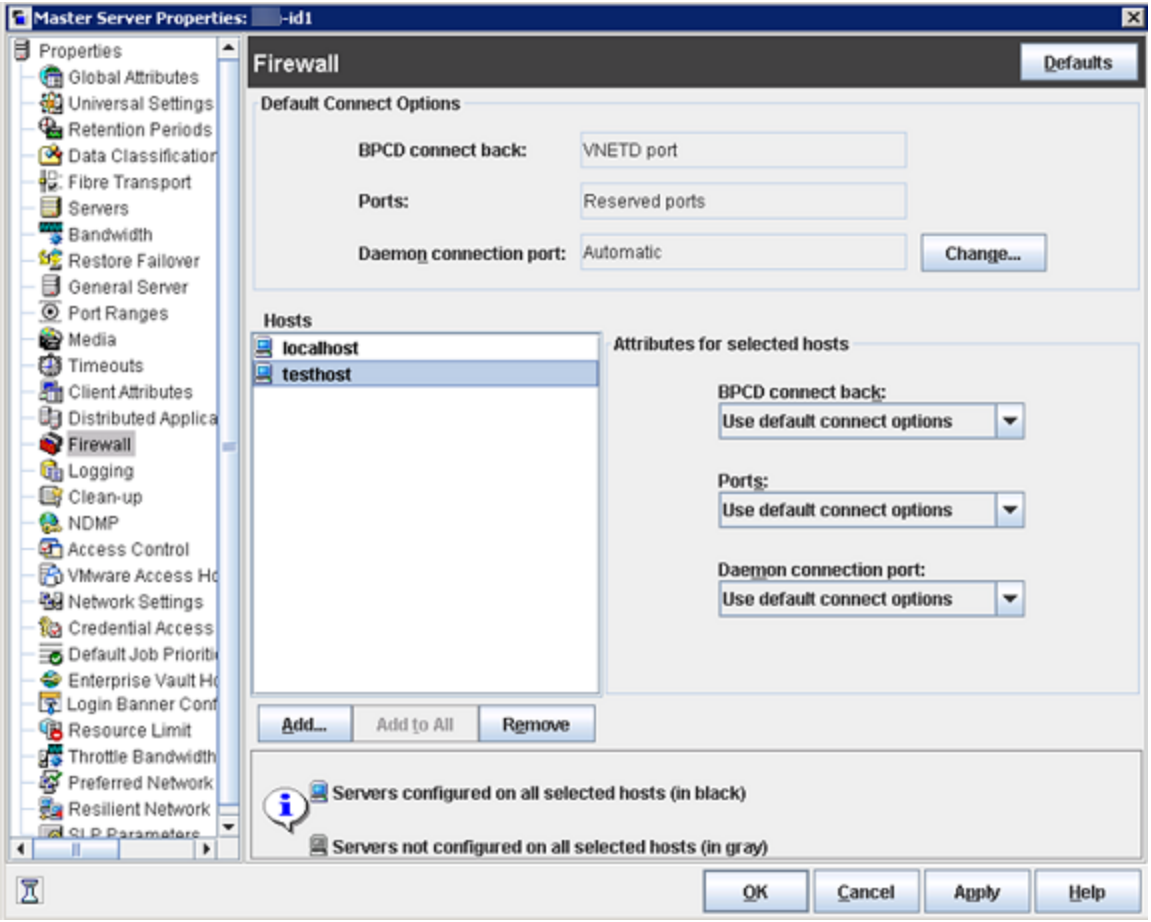
1 NetBackup 管理コンソールで、[NetBackup の管理 (NetBackup Management)]>[ホストプロパティ (Host Properties)]>[マスターサーバー (Master Servers)]を展開します。

2 設定するホストをダブルクリックします。

3 [ファイアウォール (Firewall)]をクリックします。

4 ［ホスト (Hosts)］ペインで［追加 (Add)］をクリックします。ホストの一覧に接続先ホスト (通常は別の NetBackup サーバー) を追加します。

ホストの一覧については、次の図を参照してください。



5 (任意) [選択されたホストの属性 (Attributes for selected hosts)] で適切なオプションを選択します。

[BPCD コネクトバック (BPCD connect-back)]、[ポート (Ports)]、[デーモン接続ポート (Daemon connection port)] 属性について詳しくは、次を参照してください。

p.109 の「NetBackup サーバーまたはクライアントのファイアウォール接続オプションの指定」を参照してください。

[デフォルト接続オプションを使用 (Use default connect options)] を選択した場合、NetBackup では [デフォルト接続オプション (Default Connect Options)] リストに表示される値が使われます。

構成ファイルのポート情報の編集

NetBackup では、必要なすべてのポート変更用の GUI を提供しません。設定によっては、bp.conf ファイルを編集する必要があります。次に、変更する可能性がある bp.conf 設定を示します。

- ALLOW_NON_RESERVED_PORTS
- CLIENT_PORT_WINDOW
- CLIENT_RESERVED_PORT_WINDOW
- CONNECT_OPTIONS
- DEFAULT_CONNECT_OPTIONS
- RANDOM_PORTS
- SERVER_RESERVED_PORT_WINDOW
- SERVER_PORT_WINDOW

上記の設定について詳しくは、『NetBackup 管理者ガイド Vol 1』を参照してください。

シマンテック社は bp.conf ファイルを直接変更しないことを推奨します。次の手順では、一般的な用語を使用して、bpgetconfig および bpsetconfig コマンドを使用して、bp.conf ファイルのポート情報を変更する方法について説明します。

bp.conf ファイルのポート設定を変更する方法

1. NetBackup マスターサーバー、NetBackup メディアサーバー、またはクライアントで bpgetconfig コマンドを入力します。

   ```
   bpgetconfig options > outputfile
   ```

   options の場合、bpgetconfig マニュアルページからのオプションを指定します。

   outputfile に、テキストファイルの名前を指定します。

2. ポート情報を更新するために、作成した出力ファイルを編集します。

   たとえば、UNIX または Linux プラットフォームでは、vi(1) を使用してファイルを編集できます。Windows システムでは、テキストエディタを使用して、ファイルを編集できます。

3. NetBackup にファイルを書き込むには、bpsetconfig コマンドを入力します。

構成設定とポートについて詳しくは、次を参照してください。

- 『NetBackup 管理者ガイド Vol. 1』
- 『NetBackup コマンドリファレンスガイド』

クライアント接続オプションの更新

NetBackup はクライアント接続オプションを指定する次の方法を提供します。

- NetBackup 管理コンソールを起動します。[ホストプロパティ (Host Properties)]>[マスターサーバー (Master Servers)]>[クライアント属性 (Client Attributes)]>[接続オプション (Connect Options)]を展開します。
- コマンドラインで、次のコマンドを実行します。各種クライアント属性を更新する bpclient コマンドを使うことができます。
  例えば、クライアントポートの接続オプションを指定する bpclient コマンドに -connect_options 引数を使うことができます。
  コマンドについて詳しくは、『NetBackup コマンド』マニュアルを参照してください。

vm.conf ファイルの Media Manager ポート設定の更新

vm.conf ファイルは Media Manager の接続オプションを指定します。デフォルト接続オプションを上書きする場合、vm.conf ファイルを編集する必要があります。NetBackup 管理コンソールはこれらの設定を変更する方法を提供しません。vm.conf へのパスは次のとおりです。

- UNIX または Linux の場合、パスは次のとおりです。
  /usr/openv/volmgr/vm.conf
- Windows の場合、パスは次のとおりです。

install_path¥volmgr¥vm.conf

NetBackup 5.1 以前のリリースを実行するホストの場合、vm.conf ファイルを検査します。これらの以前のリリースを実行するホストでは、Media Manager の接続オプションを手動で指定する必要があります。

表 3-12 はポートに影響する vm.conf ファイル設定を示します。

表 3-12　ポートの使用に関連する Media Manager 構成の設定

設定	説明
CLIENT_PORT_WINDOW	Media Manager の外部接続に使用される接続元ポートの範囲を指定します。形式は次のとおりです。 CLIENT_PORT_WINDOW = *min max* *min* 引数は最小の送信元ポートポート番号を定義します。 *max* 引数は最大の送信元ポート番号を定義します。 *min* および *max* には、0 (ゼロ) を指定するか、1024 ～ 65535 の整数を指定してください。*min* が 0 であるか、*max* が *min* よりより小さい場合、オペレーティングシステムは送信元ポートポート番号を判断します。 デフォルトでは、CLIENT_PORT_WINDOW = 0 0 です。 たとえば、次の設定では 3000 から 8000 の範囲の接続元ポートが定義されます。 CLIENT_PORT_WINDOW = 3000 8000

設定	説明
CONNECT_OPTIONS	**メモ:** CONNECT_OPTIONS 設定は NetBackup 7.0 以前を実行するホストへの接続にのみ影響します。NetBackup が NetBackup 7.0.1 以降を実行するホストに接続するとき、NetBackup は veritas_pbx ポートを使います。 Media Manager サービスに接続するために使うことができる接続先ポート番号を指定します。形式は次のとおりです。 CONNECT_OPTIONS = *host* 0 0 0|1|2 この設定には 4 つのスペースで区切られた引数を指定できます。引数は次のとおりです。 *host* には、他のコンピュータが接続する必要があるメディアサーバーの名前を指定します。 *host* の名前の後ろで、0 0 と入力します。これらの位置の引数は使われません。 0 0 の後に、0、1、または 2 を入力し、対象コンピュータ上の Media Manager サービスへの接続方法を指定します。接続方法の仕様は次のとおりです。 ■ 0 の場合、ホストは vnetd ポートを使います。試行が失敗する場合、ホストはレガシーのポート番号を使います。 ■ 1 の場合、ホストは vnetd ポートのみを使用して、サーバーに接続します。 ■ 2 の場合、ホストはレガシーの Media Manager のポートを使います。 5.1 以前のサーバーの場合はデフォルト。 vm.conf ファイルには、複数の CONNECT_OPTIONS の設定を指定することができます。 NetBackup では、vm.conf ファイルが CONNECT_OPTIONS エントリを含まない場合、Media Manager は DEFAULT_CONNECT_OPTIONS と CONNECT_OPTIONS の bp.conf ファイル設定に基づいてポートを選択します。 たとえば、次の設定では、Media Manager の server3 への接続において、宛先ポートとして vnetd を指定します。 CONNECT_OPTIONS = server3 0 0 1
RANDOM_PORTS	他の NetBackup サーバーと通信するときに、NetBackup がポートか順次選択するか、ランダムに選択するかどうかを指定します。形式は次のとおりです。 RANDOM_PORTS = YES | NO RANDOM_PORTS = YES の場合、または RANDOM_PORT エントリがない場合、NetBackup は vm.conf ファイルの CLIENT_PORT_WINDOW 設定によって指定された範囲からランダムなポートを選択します。 RANDOM_PORTS = NO の場合、NetBackup は範囲内の最大接続元ポート番号を使用して接続しようとします。その接続元ポートが機能しない場合、NetBackup は、次に大きい接続元ポート番号を使用しようとします。ポート番号は、機能する接続元ポート番号を検出するまでリストから選択されます。

NDMP バックアップのポート要件

ネットワークデータ管理プロトコル (NDMP) ストレージユニットバックアップでは、特定のポートがファイアウォール環境で開いている必要があります。ファイアウォールで開く必要のあるポートは、バックアップ形式によって決定されます。

次の表に NDMP バックアップのポート要件を示します。

表 3-13 NDMP **バックアップのポート要件**

バックアップ形式	説明
ローカル	ローカル操作では、データ管理アプリケーション (DMA) は NDMP サーバーのポート 10000 にアクセスする必要があります。この場合、NDMP サーバーは NDMP テープサーバーであり、NDMP データサーバーでもあります。
3-Way およびリモート NDMP	3-Way およびリモート NDMP では、DMA は NDMP テープサーバーおよび NDMP データサーバーのポート 10000 にアクセスする必要があります。NDMP テープサーバーと NDMP データサーバー間にはファイアウォールは使用できません。データの移動に使用される TCP/IP ポートを制御する必要はないため、ファイアウォールは必要ありません。
リモート NDMP (5.0/5.1)	リモート NDMP (5.0/5.1) では、DMA を NDMP テープサーバーと同じコンピュータに配置できるため、DMA と NDMP ホスト間のファイアウォールは特に必要ありません。NDMP テープサーバーと NDMP データサーバー間でデータ移動を実行するには、無制限の数のポートを利用できる必要があります。

UNIX システムでは、NetBackup `avrd` プロセスは、ネットワーク接続を確認するために NDMP ホストに ping を実行する際、Internet Control Message Protocol (ICMP) を使用します。ping が失敗した場合、NetBackup によって特定のデバイスがスキップされ、ドライブの状態は起動のままになります。

Windows システムでは、NetBackup による NDMP デバイスへの ping は実行されません。NetBackup によって接続が試行されます。ネットワーク接続に問題がある場合、NetBackup はタイムアウトを待機するため、この処理には時間がかかる可能性があります。

サードパーティの製品とともに NetBackup を使う場合の既知のファイアウォールの問題

他社製品と NetBackup 間の通信は未定義ポート経由で発生します。NetBackup はこの通信を制御しません。このため、NetBackup メディアサーバーと次のサードパーティサーバーの間でファイアウォールポートを開く方法がありません。

- 自動カートリッジシステム (ACS)サーバー。リモートプロシージャコールはこの通信を有効にします。共通ポートがありません。
- 冨士通ライブラリー管理プログラム機能 (LMF)サーバー。
- テープライブラリの半インチ (TLH) IBM ライブラリマネージャサーバー。
- テープライブラリのマルチメディア (TLM) ADIC DAS/SDLC サーバー。

4

NetBackup 操作の監査

この章では以下の項目について説明しています。

- NetBackup の監査について
- 現在の監査設定の表示
- NetBackup マスターサーバーでの監査の構成
- 監査レポートでのユーザーの識別情報
- 拡張監査について
- 拡張監査の有効化
- 拡張監査の設定
- 拡張監査の無効化
- ホストプロパティの変更の監査
- 監査記録の保持とバックアップ
- 監査レポートの表示
- -reason または -r option コマンドラインの使用
- nbaudit ログの動作
- 監査エラーの監査アラート通知

NetBackup の監査について

監査記録は、NetBackup 環境でユーザーが開始した操作の記録です。基本的に、監査はだれが何をいつ変更したか答えるのに役立つ情報を集めます。

NetBackup 操作の監査は次の領域の情報の提供に役立ちます。

概要の追跡	お客様は NetBackup 環境の予想外の変更を調査するときに、監査記録から推測することができます。たとえば、クライアントまたはバックアップパスの付加によりバックアップ時間が大幅に増加したことが分かる場合があります。監査レポートは、ポリシーの変更に対応するためにスケジュールまたはストレージユニットの構成への調節が必要な可能性があることを示すことがあります。
規制コンプライアンス	監査はだれが何をいつ変更したかのレコードを作成します。レコードはサーベンスオクスリー法 (SOX) で必要とされるようなガイドラインに従います。
企業の変更管理	内部変更の管理ポリシーを固守する必要があるお客様のために NetBackup の監査はそのようなポリシーを固守するための方式を提供します。
トラブルシューティング	NetBackup の監査からの情報は NetBackup サポートがお客様のために問題をトラブルシューティングするのに役立ちます。

NetBackup Audit Manager (`nbaudit`) はマスターサーバー上で動作し、監査レコードは Enterprise Media Manager (EMM) データベースに保持されます。

Audit Manager は監査情報に対する問い合わせおよびレポートのための機構を提供します。たとえば、管理者は、処理が実行された日時、特定のユーザーが実行した処理、特定のコンテンツの領域で実行された処理、または監査の構成への変更に基づいて、特定の情報を検索できます。

監査を構成するとき (デフォルトでは監査は有効になります)、次の NetBackup のユーザーが開始する処理が記録され、`nbauditreport` コマンドまたは Symantec NetBackup OpsCenter を使うことによって表示できます。

- NetBackup の次のエンティティが監査されます。
  - ポリシー
    ポリシーの属性、クライアント、スケジュール、バックアップ対象リストの追加、削除、更新。
  - アクティビティモニター
    任意の形式のジョブを取り消すか、中断するか、再開するか、再起動するか、または削除すると、監査レコードが作成されます。
  - ストレージユニット
    ストレージユニットの追加、削除、または更新。

    メモ: [ストレージライフサイクルポリシー (Storage Lifecycle Policies)] と関連している処理は監査されません。

  - ストレージサーバー
    ストレージサーバーの追加、削除、または更新。
  - ディスクプールとボリュームプール
    ディスクプールまたはボリュームプールの追加、削除、または更新。

- ホストプロパティ
  ホストプロパティの更新。(NetBackup のアクセス制御 (NBAC) は、ホストプロパティの監査を実行するために有効にする必要があります。)

- リストアジョブの開始。
  リストアジョブは開始が監査される唯一のジョブ形式です。たとえば、バックアップジョブが始まるとき、監査レコードは作成されません。
- NetBackup の監査の有効化または無効化。
- NetBackup Audit Manager (`nbaudit`) の開始と停止。

メモ: 監査が無効になっていても、監査設定の有効化と無効化、`nbaudit` の開始と停止はすべて監査されます。

- `bp.conf` ファイル (UNIX の場合) またはレジストリ (Windows の場合) への変更。
  NetBackup の場合、`bp.conf` ファイルまたはレジストリへの変更に対する監査を実行するために、NetBackup のアクセス制御 (NBAC) を有効にする必要があります。これらの変更を行うには、NetBackup 管理コンソールの `bpsetconfig`、`nbsetconfig`、ホストプロパティユーティリティのいずれかを使う必要があります。
  `bp.conf` ファイルまたはレジストリの手動変更は監査されません。
  p.131 の「ホストプロパティの変更の監査」を参照してください。
  NetBackup の[アクセス制御 (Access Control)]の設定について詳しくは、次のトピックを参照してください。p.152 の「NetBackup アクセス制御 (NBAC) の構成」を参照してください。

次の処理は監査されないため、監査レポートに表示されません。

任意の失敗した処理。	失敗した処理は NetBackup のエラーログに記録されます。失敗した試行で NetBackup のシステム状態が変更されることはないので、失敗した処理は監査レポートに表示されません。
設定変更の影響。	NetBackup の構成への変更の結果は監査されません。たとえば、ポリシーの作成は監査されますが、その作成から生じるジョブは監査されません。
手動で開始されたリストアジョブの完了状態。	リストアジョブの開始は監査されますが、ジョブの完了状態は監査されません。手動で開始されたかどうかにかかわらず、他のどのジョブ形式の完了状態も監査されません。完了はアクティビティモニターに表示されます。
内部的に開始された処理。	NetBackup によって開始された内部処理は監査されません。たとえば、期限切れのイメージのスケジュールされた削除、定時バックアップ、または定期的なイメージデータベースのクリーンアップは監査されません。

現在の監査設定の表示

現在の監査の構成を表示するためには、NetBackup マスターサーバーの nbemmcmd コマンドを使うか、Symantec NetBackup OpsCenter を使って設定を表示してください。

OpsCenter を使って監査を構成する方法については、『Symantec NetBackup OpsCenter 管理者ガイド』を参照してください。

現在の監査の設定を表示する方法

1. コマンドプロンプトで、マスターサーバー上の次のディレクトリの nbemmcmd コマンドを見つけます。
   - Windows の場合:
     Install_path¥Veritas¥NetBackup¥bin¥admincmd
   - UNIX の場合:
     /usr/openv/netbackup/bin/admincmd
2. 次の構文を使って nbemmcmd コマンドを入力します。

   ```
   nbemmcmd -listsettings -machinename masterserver
   ```

   ここでは、*masterserver* が対象のマスターサーバーです。

   メモ: オプションでは、大文字と小文字が区別されます。

3. 出力は多くの設定をリストします。次が含まれます。
   - AUDIT="ENABLED"
     監査がオンであることを示します。
   - AUDIT="DISABLED"
     監査がオフであることを示します。
   - AUDIT_RETENTION_PERIOD="90"
     監査が有効になっている場合に、レコードがこの期間 (日数) 保持されてから削除されることを示します。デフォルトの監査保持期間は 90 日です。0 (ゼロ) という値はレコードが削除されないことを示します。

NetBackup マスターサーバーでの監査の構成

新規インストールでは監査がデフォルトで有効になります。ただし、デフォルトはアップグレードの前の設定によってアップグレード後、有効と無効を切り替えられることがあります。

NetBackup の監査は NetBackup マスターサーバー上または Symantec NetBackup OpsCenter の使用によって直接構成できます。

監査ログの有効化または無効化のマスターサーバー設定、および保持期間の設定は、OpsCenter の[管理 (Manage)]>[ホスト (Hosts)]セクションで構成されます。OpsCenter では、監査ログの有効期限の設定は[設定 (Settings)]>[パージ (Purge)]で構成されます。

詳細については、『Symantec NetBackup OpsCenter 管理者ガイド』を参照してください。

マスターサーバーで監査を構成するには、-changesetting オプションを指定して nbemmcmd コマンドを使います。

マスターサーバーで NetBackup の監査を構成する方法

1. コマンドプロンプトで、マスターサーバー上の次のディレクトリの nbemmcmd コマンドを見つけます。
   - Windows の場合:
     Install_path¥Veritas¥NetBackup¥bin¥admincmd
   - UNIX の場合:
     /usr/openv/netbackup/bin/admincmd
2. 次の構文を使って nbemmcmd コマンドを入力します。

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename masterserver
   ```

   ここでは、-AUDIT DISABLED は示されているマスターサーバーの監査をオフにします。

   メモ: オプションでは、大文字と小文字が区別されます。

   次の例では server1 に対して監査がオフになります。

   例:

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename server1
   ```

3 次の構文を使って監査の保持期間を構成します。

```
nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD
number_of_days -machinename masterserver
```

ここで、*number_of_days* は、監査レポートで監査レコードがどの位保持されるべきであるかを (日数で) 示します。保持期間が示されていない場合、デフォルトの監査保持期間は 90 日です。

メモ: 監査保持期間の値が 0 (ゼロ) の場合は、レコードが削除されないことを示します。

OpsCenter は監査レコードを定期的にダウンロードし、OpsCenter で構成可能な一定期間保持します。マスターサーバーでの監査レコードの保持は、マスターサーバーでコマンドラインを使って監査レポートを表示する場合にのみ必要です。

詳しくは、次の項を参照してください。

p.132 の「監査記録の保持とバックアップ」を参照してください。

次の例では、ユーザー操作のレコードは 30 日間保持されてから、削除されます。

```
nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD 30
-machinename server1
```

2 つのオプションは次の例のように 1 つのコマンドラインで組み合わせることができます。

```
nbemmcmd -changesetting -AUDIT ENABLED -machinename server1
-AUDIT_RETENTION_PERIOD 30
```

4 監査情報のレポートを表示するために nbauditreport を実行します。

p.132 の「監査レポートの表示」を参照してください。

監査レポートでのユーザーの識別情報

監査レポートは特定の処理を実行したユーザーの識別情報をリストします。識別情報は認証されたユーザーのユーザー名、ドメイン、ドメイン形式を含んでいます。

監査レポートに取り込まれるユーザー名は次のように決まります。

- デフォルトでは、ルートまたは管理者ユーザーのみが CLI と NetBackup 管理コンソールを使って NetBackup 操作を行うことができます。したがって、ルートまたは管理者はルートまたは管理者のユーザー名で監査されます。

- 拡張監査または NBAC のいずれかが有効になっている場合、CLI または NetBackup 管理コンソールを使って NetBackup 操作を行ったユーザーの実際のユーザー名が監査レポートに記録されます。
- デフォルトでは、ルートまたは管理者ユーザーのみが CLI と NetBackup 管理コンソールを使って NetBackup 操作を行うことができるので、ルートまたは管理者のユーザー名で監査されます。
- 拡張監査も NBAC も有効になっていないとき、すべてのタスクが root または管理者として監査されます。

p.149 の「NetBackup アクセス制御 (NBAC) の使用について」を参照してください。

p.126 の「拡張監査について」を参照してください。

拡張監査について

拡張監査を使うと、NetBackup 管理者は他の指定ユーザーに NetBackup 管理者権限を委託できます。したがって、この機能を使うと root ユーザー以外でも NetBackup を管理できます。監査ログには、NetBackup 環境の変更を実行した実際のユーザー情報が記録されます。拡張監査を使えば、監査コンプライアンスの必要条件に重要なユーザーアクティビティに関する主要な情報を組織が追跡しやすくなります。特に、高度に制御された企業のユーザーに役立つ機能です。

デフォルトでは、root ユーザーまたは管理者のみがコマンドラインを使って NetBackup 操作を実行できます。ただし、拡張監査を設定した NetBackup と正しい NetBackup 管理者権限で、コマンドラインを使って NetBackup 操作を実行できます。拡張監査はユーザーが管理者でも管理者でなくても適切なアクセス制御は提供しません。

メモ: NBAC と拡張監査は相互に排他的な機能です。

メモ: 現時点では、拡張監査サポートは NetBackup ポリシー、ジョブ、ストレージユニットなどのユーザー操作に利用可能です。

次の表に、ユーザー操作を拡張監査で監査する場合のコマンドを示します。

表 4-1　拡張監査をサポートするコマンドとカテゴリ

コマンド	カテゴリ
bpplcatdrinfo	ポリシー
bpplclients	ポリシー
bppldelete	ポリシー

コマンド	カテゴリ
bpplinclude	ポリシー
bpplinfo	ポリシー
bppllist	ポリシー
bpplsched	ポリシー
bpplschedrep	ポリシー
bpplschedwin	ポリシー
bpplvalid	ポリシー
bppolicynew	ポリシー
bpdbjobs	ジョブ
bpstuadd	ストレージユニット
bpstuddel	ストレージユニット
bpsturep	ストレージユニット
bpstulist	ストレージユニット

拡張監査の有効化

NetBackup では、拡張監査を有効にするのに bpnbaz -SetupExAudit コマンドを使用する必要があります。次の手順に従います。

拡張監査用に NetBackup を設定する方法

1 マスターサーバー上で bpnbaz -SetupExAudit コマンドを実行します。

メモ: このコマンドは、クラスタセットアップ時に、アクティブノードとパッシブノードの両方で実行する必要があります。

---

2 NetBackup サービスを再起動します。

p.128 の「拡張監査の設定」を参照してください。

拡張監査の設定

拡張監査の一部のシナリオでは、いくつかの設定手順を追加で実行する必要があります。これらの手順はサーバーの変更操作を実行するときに適用できます。

- NetBackup 管理コンソールからメディアサーバーに接続する場合は、セキュリティ証明書が必須になります。
  p.128 の「拡張監査でのメディアサーバーへの接続」を参照してください。
- マスターサーバーから別のマスターサーバーにサーバーを変更するときに、マスターサーバーで追加手順を実行する必要があります。
  p.128 の「NetBackup ドメイン間でのサーバー変更」を参照してください。

拡張監査でのメディアサーバーへの接続

拡張監査の場合に、NetBackup 管理コンソールを使ってメディアサーバーに接続するには、セキュリティ証明書が必須です。各メディアサーバーの証明書を取得するには、マスターサーバー上で追加の手順を実行する必要があります。詳しくは、次の手順を参照してください。

サーバーのセキュリティ証明書を生成するには

1. マスターサーバー上で `bpnbaz -ProvisionCert target.server.com` コマンドを実行します。ここで、`target.server.com` はメディアサーバー名です。

   使用例: `acme.domain.mycompany.com` は、サーバー変更を実行する対象となるメディアサーバーです

   マスターサーバー上で `bpnbaz -ProvisionCert acme.domain.mycompany.com` コマンドを実行します。

   出力は次のとおりです。

   ```
   bpnbaz -ProvisionCert acme.domain.mycompany.com

   Setting up security on target host: acme.domain.mycompany.com

   Certificate deployed successfully

   Operation completed successfully.
   ```

2. 証明書を生成した後は、必ずメディアサーバー上でサービスを再起動します。

メモ: セキュリティ証明書は 1 回だけ生成します。

NetBackup ドメイン間でのサーバー変更

拡張監査の場合に、1 つの NetBackup ドメインのマスターサーバーまたはメディアサーバーから別の NetBackup ドメインのホスト (マスターまたはメディアのサーバーまたはク

ライアント) へのサーバー変更操作を実行するときには、各 NetBackup サーバー上で追加手順を実行する必要があります。また、両方のマスターサーバー上で信頼を設定する必要もあります。

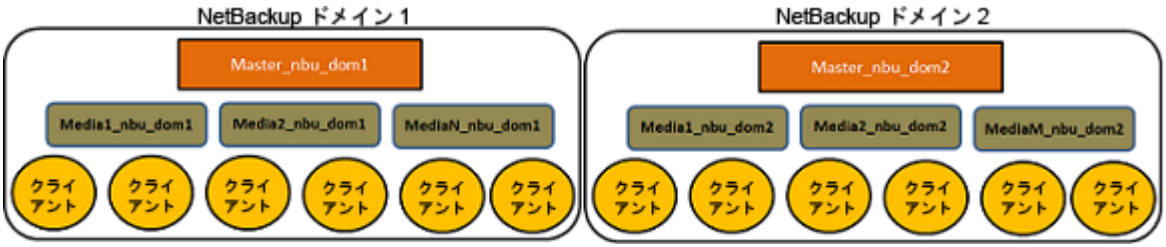
メモ: これらの手順は、1 回だけ実行します。

次の手順では、サーバーを変更し、両方のマスターサーバー上で信頼を設定できます。

マスターからマスターにサーバーを変更するには

1 NetBackup Domain 1 と NetBackup Domain 2 という、2 つの NetBackup ドメインがあります。

Master_nbu_dom1 と Master_nbu_dom2 という、2 つのマスターサーバーがあります。Master_nbu_dom1 には、Media1_nbu_dom1、Media2_nbu_dom1、MediaN_nbu_dom1 の各メディアサーバーと、クライアントのセットがあります。同様に、Master_nbu_dom2 には、Media1_nbu_dom2、Media2_nbu_dom2、MediaM_nbu_dom2 の各メディアサーバーと、クライアントのセットがあります (イメージを参照)。



ユーザーは、NetBackup Domain 1 のサーバー (マスターまたはメディア) のいずれか (Master_server_nbu_dom1 など) に接続されており、NetBackup Domain 2 のホストのいずれか (Host_nbu_dom2 など) にサーバーを変更する必要があります。両方のマスターサーバー (ここでは Master_nbu_dom1 と Master_nbu_dom2) で信頼が確立されていることが必要です。Host_nbu_dom2 は、Master_server_nbu_dom1 との信頼を設定する必要があります。

2 信頼を設定するには、UNIX と Windows 上でコマンドのセットを呼び出す必要があります。

UNIX および Linux の場合:

```
/usr/openv/netbackup/sec/at/bin/vssat setuptrust -b
```

```
Master_server_nbu_dom1:1556:nbatd -s high on Host_nbu_dom2
```

Windows の場合:

```
InstallPath¥Veritas¥NetBackup¥sec¥at¥bin¥vssat.bat
```

3 bp.conf ファイルで、Master_server_nbu_dom1 用に Host_nbu_dom2 にサーバーエントリを追加する必要があります。次のコマンドを実行します。

```
SERVER = Master_server_nbu_dom1 /*this should __not__ be the first
SERVER entry*/
```

NetBackup 管理コンソールを使って対象のマスターサーバーに接続することで、サーバーエントリを追加することもできます。

4 NetBackup 管理コンソールまたはリモート Java 管理コンソールを備えたホストは、`Master_server_nbu_dom2` の X.509 NBATD 証明書を信頼する必要もあります。

信頼は、GUI を使って `Master_server_nbu_dom2` マスターサーバーに直接接続することで設定できます。

また、`/usr/openv/java/sec/at/bin/vssat setuptrust -b` を呼び出すこともできます。

NetBackup 管理コンソールのホスト上で、`Master_server_nbu_dom2:1556:nbatd -s high` を実行します。

サーバーの変更を NBAC または拡張監査と一緒に使った場合の設定要件

NetBackup アクセス制御または拡張監査が使われる場合にサーバーの変更を実行するには、追加の設定が必要になります。

次の手順では、NBAC または拡張監査がすでに設定されていることを想定しています。

サーバーの変更操作をサポートするための設定: *fromServer -> toServer*

- *toServer* のホストプロパティの追加サーバーリストに、*fromServer* を追加します。
- *fromServer* と *toServer* が異なる NetBackup ドメイン (異なるマスターサーバーのメディアサーバー) にある場合:
  - *fromServer* と *toServer* のマスターサーバーの間で信頼を設定するために `vssat` コマンドを使います。(p.128 の「NetBackup ドメイン間でのサーバー変更」を参照してください。 手順 2 を参照してください。)
  - *fromServer* のマスターサーバーを、*toServer* のホストプロパティの追加サーバーリストに追加します。
- *fromServer* または *toServer* がメディアサーバーの場合:
  - 必要に応じて、`bpnbaz -ProvisionCert` コマンドを使って、セキュリティ (マシン) 証明書を配備します (p.128 の「拡張監査でのメディアサーバーへの接続」を参照してください。)。

追加の設定手順

auth.conf ファイルを使う場合:

- 各サーバーの auth.conf ファイルに USER エントリを追加します。
- NBAC が有効な場合は、各サーバーで nbsetconfig を実行して、エントリ USE_AUTH_CONF_NBAC = YES を追加します。

リモート管理コンソールを使う場合:

- vssat コマンドを使うか、少なくとも 1 度各サーバーに明示的にログオンして、各マスターサーバーに信頼を設定します。(p.128 の「NetBackup ドメイン間でのサーバー変更」を参照してください。 手順 2 を参照してください。)

設定後にトラブルシューティングを行う場合は、サーバー通信を検査するために nslookup と bptestnetconn -a -s を使います。

拡張監査の無効化

NetBackup の拡張監査を無効にすることができます。拡張監査を有効にすると USE_AUTHENTICATON オプションが ON になります。拡張監査を無効にするには、このオプションを OFF にする必要があります。次の手順が役立ちます。

拡張監査を無効にするには

1. マスターサーバー上で bpsetconfig コマンドを実行します。
2. bpsetconfig> USE_AUTHENTICATON=OFF を設定します。
3. NetBackup サービスを再起動します。

ホストプロパティの変更の監査

管理者が、bpsetconfig コマンド、nbsetconfig コマンド、[ホストプロパティ (Host Properties)]ユーティリティの同等のプロパティのいずれかを使用すると、NetBackup はホストプロパティの変更を監査します。

監査を実行するには、次の条件を満たす必要があります。

- 環境を NetBackup アクセス制御 (NBAC) 用に構成する必要があります。
- bp.conf ファイルまたはレジストリが変更されるホストは、NetBackup 7.1 以降であること。
- 監査を実行するために、管理者は、bpsetconfig コマンド、nbsetconfig コマンド、[ホストプロパティ (Host Properties)]ユーティリティの同等のプロパティのいずれかを使用する必要があります。bp.conf ファイルまたはレジストリを直接変更した場合、

その変更は監査されません。すなわち、bpsetconfig または nbsetconfig なしで行なわれた変更です。

たとえば、bpsetconfig コマンドまたは nbsetconfig コマンドを使ってクライアントをオフラインにすることはできないため、クライアントをオフラインにする操作は監査ログには表示されません。

監査記録の保持とバックアップ

デフォルトでは、監査レコードは 90 日間保持されます。デフォルトを変更するには、-AUDIT_RETENTION_PERIOD オプションを指定して nbemmcmd -changesetting コマンドを使用します。

p.123 の「NetBackup マスターサーバーでの監査の構成」を参照してください。

構成された保持設定に基づいて、NetBackup の監査サービス (nbaudit) は 12:00 AM (ローカルタイム) に期限切れの監査レコードを 24 時間ごとに一度削除します。

監査レコードは NetBackup のデータベースの一部分である監査表に保存されます。表は -AUDIT_RETENTION_PERIOD に示される期間中保持され、NetBackup カタログバックアップの一部としてバックアップされます。

監査レコードがカタログバックアップから欠けていないようにするには、カタログバックアップの間隔を -AUDIT_RETENTION_PERIOD と同じかそれより大きくなるように構成します。

Symantec NetBackup OpsCenter は EMM データベースから監査レコードを定期的にダウンロードします。OpsCenter は、OpsCenter 内で構成されている期間、レコードを保持します。従って、NetBackup マスターサーバーの監査レコードの保持は、マスターサーバーのコマンドラインを使って監査レポートを表示したい場合にのみ必要です。また、監査レコードを OpsCenter からエクスポートすることもできます。

監査レポートの表示

監査レポートを表示するためには、NetBackup マスターサーバーの nbauditreport コマンドを使うか、Symantec NetBackup OpsCenter を使って設定を表示してください。

OpsCenter では、[監視 (Monitor)]>[監査記録 (Audit Trail)]セクションで監査ログの詳細が提供され、その情報を Excel にエクスポートしたり、pdf ファイルとして保存したりできます。

詳細については、『Symantec NetBackup OpsCenter 管理者ガイド』を参照してください。

監査が有効な場合、ユーザー操作が監査レコードの作成に失敗すると、監査エラーが nbaudit ログでキャプチャされます。

NetBackup 管理コンソール の監査アラート通知ボタンにより、監査エラーが起きたとき管理者に通知できます。

p.138 の「監査エラーの監査アラート通知」を参照してください。

監査レコードを作成するエラーは実行されたユーザー操作に影響がありません。

ユーザー操作が成功すれば、正常な処理を反映する終了コードが戻ります。処理の監査が失敗した場合、NetBackupの状態コード 108 は戻されます (**処理に成功しましたが監査に失敗しました** (`Action succeeded but auditing failed`))。

メモ: NetBackup 管理コンソール (Windows と UNIX (`jnbSA`)) は監査が失敗したとき、終了状態コード 108 を戻しません。

NetBackup の監査レポートを表示する方法

1. コマンドプロンプトで、マスターサーバー上の次のディレクトリの `nbauditreport` コマンドを見つけます。
   - Windows の場合:
     Install_path¥Veritas¥NetBackup¥bin¥admincmd
   - UNIX の場合:
     /usr/openv/netbackup/bin/admincmd
2. 最も簡単な形式では、次の構文を使って `nbauditreport` コマンドを入力します。

   ```
   nbauditreport
   ```

   `nbauditreport` は多くのオプションを指定して使うこともできます。

   メモ: オプションでは、大文字と小文字が区別されます。

`-help`	コマンドプロンプトでコマンドの補足情報を表示するために使用します。
`-sdate <"MM/DD/YY [HH:[MM[:SS]]]">`	表示するレポートデータの開始日時を示すために使用します。
`-edate <"MM/DD/YY [HH:[MM[:SS]]]">`	表示するレポートデータの終了日時を示すために使用します。
`-ctgy POLICY`	ポリシーの変更と関連している情報を表示するために `-ctgy POLICY` を使います。
`-ctgy JOB`	ジョブと関連している情報を表示するために `-ctgy JOB` を使います。

-ctgy STU	ストレージユニットに関連する情報を表示するために -ctgy STU を使用します。
-ctgy STORAGESRV	ストレージサーバーに関連する情報を表示するために -ctgy STORAGESRV を使用します。
-ctgy POOL	ストレージプールに関連する情報を表示するために -ctgy POOL を使用します。
-ctgy AUDITCFG	監査の設定変更に関連する情報を表示するために -ctgy AUDITCFG を使います。
-ctgy AUDITSVC	NetBackup の監査サービス (nbaudit) の開始と停止に関する情報を表示するために -ctgy AUDITSVC を使います。
-ctgy BPCONF	bp.conf ファイルの変更に関連する情報を表示するために -ctgy BPCONF を使用します。
-ctgy USER	拡張監査モードのユーザーの追加と削除に関する情報を表示するには - ctgy USER を使用します。
-user <username[:domainname]>	監査情報を表示するユーザーの名前を指定するために使います。
-fmt SUMMARY	レポート出力形式のオプション (-fmt) が指定されていない場合は、SUMMARY オプションがデフォルトで使われます。
-fmt DETAIL	-fmt DETAIL オプションは監査情報の総合的なリストを表示します。たとえば、ポリシーが変更されると、属性の名前、古い値と新しい値が一覧表示されます。
-fmt PARSABLE	-fmt PARSABLE オプションは DETAIL レポートと同じセットの情報を解析可能な形式で表示します。レポートは監査レポートデータ間の解析トークンとしてパイプ文字 (|) を使います。
[-notruncate]	レポートの詳細セクションの別々の行に、変更された属性の古い値と新しい値を表示するには、-notruncate オプションを使います。 **メモ:** -notruncate は -fmt DETAIL オプションと組み合わせた場合にのみ有効です。

[-pagewidth <NNN>]	レポートの詳細セクションのページ幅を設定するために -pagewidth オプションを使います。 **メモ:** -pagewidth は -fmt DETAIL オプションと組み合わせた場合にのみ有効です。
[-order <DTU|DUT|TDU|TUD|UDT|UTD>]	-order オプションは -fmt PARSABLE でのみ有効です。情報が表示される順序を示すために使います。 次のパラメータを使います。 ■ D (説明) ■ T (タイムスタンプ) ■ U (ユーザー)

3 監査レポートは次の詳細を含んでいます。

DESCRIPTION	実行された処理の詳細。詳細には、修正されたオブジェクトに指定された新しい値、および新しく作成されたオブジェクトのすべての属性の新しい値が含まれています。詳細は、削除されたすべてのオブジェクトの ID も含んでいます。
USER	処理を実行したユーザーの識別情報。識別情報は認証されたユーザーのユーザー名、ドメイン、ドメイン形式を含んでいます。 p.125 の「監査レポートでのユーザーの識別情報」を参照してください。
TIMESTAMP	処理が実行された時間。時間は協定世界時 (UTC) で示され、秒で示されます。(たとえば、12/06/11 10:32:48。)
CATEGORY	実行されたユーザー操作のカテゴリ。CATEGORY は、-fmt DETAIL|PARSABLE オプションを指定したときのみ表示されます。 例は次のとおりです。 ■ AUDITSVC START、AUDITSVC STOP ■ POLICY CREATE、POLICY MODIFY、POLICY DELETE
ACTION	実行された処理。ACTION は、-fmt DETAIL|PARSABLE オプションを指定したときのみ表示されます。 例は次のとおりです。 ■ START、STOP ■ CREATE、MODIFY、DELETE

REASON	処理が実行された理由。変更を作成したコマンドで理由が指定済みの場合に理由が表示されます。bpsetconfigコマンドとnbsetconfigコマンドは -r オプションを受け入れます。 p.136 の「-reason または -r option コマンドラインの使用」を参照してください。 理由は、-fmt DETAIL|PARSABLE オプションを指定したときのみ表示されます。
DETAILS	すべての変更の詳細。古い値と新しい値をリストします。-fmt DETAIL|PARSABLE オプションを指定したときのみ表示されます。

終了状態が出力に表示されたら、NetBackup 管理コンソール (トラブルシュータ)、オンラインヘルプ、または『状態コードリファレンスガイド』を参照してコードを調べます。

図 4-1 は server1 で実行された監査レポートのデフォルトの内容を示します。

図 4-1　概略監査レポートの例

```
[root@server1 admincmd]# ./nbauditreport
TIMESTAMP                USER            DESCRIPTION
09/23/2010 14:40:54      root@server1    Policy 'test_pol_1' was created
09/23/2010 14:40:54      root@server1    Schedule 'full' was added to
Policy'test_pol_1'
09/22/2010 17:10:23      root@server1    Audit setting(s) of master server
'server1'were modified

Audit records fetched: 3
```

-reason または -r option コマンドラインの使用

多くのコマンドは、処理がなぜ実行されたか示すために管理者が使用できる -reason オプションを提供します。監査レポートに理由が表示されます。

-reason の文字列は 512 文字以下である必要があります。文字列が 512 文字を超えると -reason オプションを受け入れるコマンドラインはエラーを表示します。

監査の理由がダッシュ文字 (-) で始まることができないことに留意してください。また、理由は単一引用符 (') を含むことができません。

次のコマンドは、-reason オプション (または bpsetconfig と nbsetconfig の場合には -r オプション) を受け入れます。

- bpdbjobs
- bpplcatdrinfo
- bpplclients

- bppldelete
- bpplinclude
- bpplinfo
- bpplsched
- bpplschedrep
- bppolicynew
- bpsetconfig

メモ: bpsetconfig と nbsetconfig コマンドは、-reason オプションの代わりに -r オプションを受け入れます。

- bpstuadd
- bpstudel
- bpsturep
- nbdecommission
- nbdevconfig
- nbsetconfig
- vmpool

コマンドの使用方法について詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

nbaudit ログの動作

nbaudit ログは、次の場所で確認できます。

- Windows の場合:
  Install_path¥Veritas¥NetBackup¥logs¥nbaudit
- UNIX の場合:
  /usr/openv/logs/nbaudit

監査が有効な場合、ユーザー操作が監査レコードの作成に失敗すると、監査エラーが nbaudit ログでキャプチャされます。

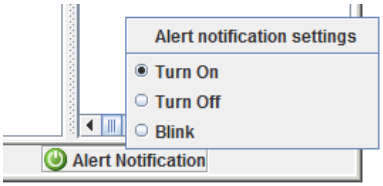
NetBackup 管理コンソール の監査アラート通知ボタンにより、監査エラーが起きたとき管理者に通知できます。

nbaudit サービスは、監査レコードを作成するときに次の方法で動作します。

- 監査レコードは、エントリの詳細を最大 4096 文字に制限します。(たとえば、ポリシー名。) 残りの文字は監査データベースに格納されるときに切り捨てられます。
- 監査レコードは、リストアイメージ ID を最大 1024 文字に制限します。残りの文字は監査データベースに格納されるときに切り捨てられます。
- ロールバック操作は監査されません。
  一部の操作は、複数の手順として実行されます。たとえば、MSDP ベースのストレージサーバーの作成は、複数の手順で構成されています。成功したすべての手順が監査されます。いずれかの手順が失敗するとロールバックという結果になります。または、成功した手順を取り消す必要がある場合もあります。監査レコードはロールバック操作についての詳細を含んでいません。

監査エラーの監査アラート通知

監査アラート通知オプションは NetBackup 管理コンソールの下部にあるステータスバーにあります。この設定を行った場合には、このオプションにより、監査処理による監査レコードの作成に失敗したことが示されます。たとえば、ポリシー属性が変更されても、NetBackup Audit Manager (`nbaudit`) は動作していません。



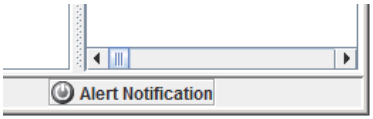
監査アラート通知を設定するには、ステータスバーの監査アラートオプションを右クリックします。

表 4-2　監査のアラート通知の設定

オンにする (Turn on)	[オンにする (Turn on)] に設定されている場合には、次の状況でポップアップメッセージが表示されます。 監査は有効ですが、監査処理は NetBackup 管理コンソールで実行され、監査レコードの作成に失敗しました。 エラーを管理者に通知するポップアップメッセージが表示されます。
点滅 (Blink)	[点滅 (Blink)] に設定されているとき、オプションは監査エラーが発生した場合に点滅します。オプションをクリックして、エラーメッセージを表示します。

オフにする (Turn off)

［オフにする (Turn off)］に設定されているとき、監査エラーの通知は表示されません。オプションは網掛けして表示されます。



メモ: ［オフにする (Turn off)］に設定しても、監査が無効になっているわけではありません。監査は続行されますが、NetBackup 管理コンソールの監査エラーメッセージは無効になります。

5

アクセス制御のセキュリティ

この章では以下の項目について説明しています。

- NetBackup のアクセス制御について
- ユーザー管理
- ユーザー認証
- Java インターフェース認証でのアクセス制御と拡張監査の影響

NetBackup のアクセス制御について

NetBackup は、Java ベースのアクセス制御、NetBackup アクセス制御 (NBAC)、拡張監査という、3 つのタイプのアクセス制御に対応しています。

- デフォルトでは Java ベースのアクセス制御が使われます。これは表示ベースのアクセス制御で、NetBackup の Java 管理コンソールインターフェースに限定されます。CLI ユーザーが NetBackup 操作を実行するには root または管理者である必要がありますが、NetBackup 管理コンソールには root や管理者でないユーザーでもアクセスできます。ユーザーは、auth.conf ファイルで定義されている権限に従って、これらのノードを表示だけできます。

  Java ベースのアクセス制御について詳しくは、『NetBackup 管理者ガイド Vol. 1』の「NetBackup 管理コンソールの使用」の章を参照してください。

- NetBackup アクセス制御 (NBAC) は、次の場合に、マスターサーバー、メディアサーバー、クライアント用に使うことができる役割ベースのアクセス制御です。
  - 1 つのアプリケーションに対して複数レベルの管理者権限を使う場合。バックアップアプリケーションは、オペレータ (ジョブの監視)、または管理者 (NetBackup 認可オブジェクトに対するアクセス、設定、使用を実行するための完全権限を有する) を持つことができます。また、アクセス制御のみ設定できるセキュリティ管理者を持つこともできます。

- システム管理に root 権限が必須とならないように管理者を分離する場合。システムに対する管理者と、アプリケーションに対する管理者を分離できます。
  p.149 の「NetBackup アクセス制御 (NBAC) の使用について」を参照してください。

- 拡張監査では、root 以外のユーザーや管理者以外のユーザーが、コマンドラインインターフェースまたは NetBackup 管理コンソールを使ってすべての NetBackup 操作を実行できます。ユーザーは、すべて操作を実行できるか、まったくできないかのいずれかになります。NBAC とは異なり、この機能では、役割ベースのアクセス制御は提供されません。
  p.126 の「拡張監査について」を参照してください。

これらアクセス制御の重要な違いを次の表にまとめます。

表 5-1

重要なパラメータ	Java GUI - auth.conf ベースのアクセス制御 (デフォルトモード)	NBAC	拡張監査
アクセス可能なユーザー	root ユーザーまたは管理者ユーザーが、CLI を使ってアクセス可能。root 以外のユーザーと管理者以外のユーザーが、Java GUI を使ってアクセス可能。	root 以外のユーザーまたは管理者以外のユーザーが、CLI または Java GUI を使ってアクセス可能。	root 以外のユーザーまたは管理者以外のユーザーが、CLI または Java GUI を使ってアクセス可能。
アクセス可能な対象	CLI ユーザーはアクセス制御なし、Java GUI ユーザーは auth.conf ファイルによるアクセス制御あり。	詳細なアクセス制御。	バイナリ (おおまかな) アクセス制御。
ユーザーの監査方法	ユーザーは root または管理者として監査される。	ユーザーは実際のユーザー名で監査される。	ユーザーは実際のユーザー名で監査される。
連携対象	拡張監査と連携可能。アクセス制御は auth.conf ファイルのエントリに従う。	NBAC は独立して機能できる。	Java GUI 認証と連携可能。アクセス制御は auth.conf ファイルのエントリに従う。

ユーザー管理

拡張監査用に NetBackup を設定すると、管理者は以下のことが行えるようになります。

- ユーザーに NetBackup 管理者権限を付与したり、取り消したりできます。

- NetBackup 管理者権限を持つユーザーを検出できます。
- NetBackup 管理者権限を持つユーザーを一覧表示できます。

メモ: NetBackup 管理者権限を持つユーザーのみユーザー管理タスクを実行できます。

ユーザー管理タスクを実行するには bpnbaz コマンドを使用します。ユーザーの追加、削除、ルックアップ、リストのコマンドは、次のオプションで実行する必要があります。

```
bpnbaz -[AddUser | DelUser] Domain_Type:Domain_Name:User_Name [-M
server] [-credfile][-reason]
```

```
bpnbaz -LookupUser Domain_Type:Domain_Name:User_Name [-M server]
[-credfile] bpnbaz -ListUsers [-M server] [-credfile]
```

```
bpnbaz -ListUsers Domain_Type:Domain_Name:User_Name [-M server]
[-credfile] bpnbaz -ListUsers [-M server] [-credfile]
```

次の表で、各コマンドについて説明します。

表 5-2

コマンド	説明	使用例
-AddUser	ユーザーが NetBackup 管理者権限を付与できるようにします。	`bpnbaz -AddUser unixpwd:v-123790b.punin.sen.symantec.com:Debbie`
-DelUser	ユーザーが NetBackup 管理者権限を取れ消せるようにします。	`bpnbaz -DelUser unixpwd:v-123790b.punin.sen.symantec.com:Debbie`
-LookupUser	ユーザーが、ユーザーを検索したり、管理者権限を持つユーザーを検出できるようにします。	`bpnbaz -LookupUser unixpwd:v-123790b.punin.sen.symantec.com:Debbie`
-ListUsers	ユーザーが、NetBackup 管理者権限を持つユーザーを一覧表示できるようにします。	`bpnbaz -ListUsers`

bpnbaz コマンドについて詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

ユーザー認証

デフォルトでは、NetBackup はユーザー認証を委任しません。ただし、NetBackup を拡張監査用に設定する場合、マスターサーバーからのユーザー認証が必須になります。

ユーザー認証の実行には `bpnbat -login` コマンドを使う必要があります。

UNIX ユーザーと Windows ユーザーのログオンプロセスは異なります。以下の情報を参照してください。

UNIX の場合

- root ユーザーの場合は、`bpnbat -login` は必須ではありません。
- ただし、root 以外のユーザーは、`bpnbat -login` を実行する必要があります。

Windows の場合

- 管理者はシングルサインオン (SSO) オプションを介して自動的にログオンします。
- 標準ユーザーも SSO オプションを介してログオンします。しかし SSO が失敗した場合、ユーザーが `bpnbat -login` を実行する必要があります。また、`bpnbat -GetBrokerCert` コマンドを実行して、サーバーとの信頼を構築することもできます。

Java インターフェース認証でのアクセス制御と拡張監査の影響

拡張監査モードを構成すると、コマンドラインと Java インターフェースアクセスは異なる働きをします。auth.conf ファイルのエントリは NetBackup 管理コンソールのアクセス制御に優先します。

p.141 の「ユーザー管理」を参照してください。

管理者権限が割り当てられたユーザーは、コマンドラインを使ってすべての監査可能な NetBackup 操作を実行できます。ユーザーアクセスについて詳しくは、次の表を参照してください。

表 5-3　ユーザーアクセス

auth.conf エントリ	CLI アクセス	Java インターフェースアクセス
auth.conf ファイルにエントリが存在する	アクセス不可	auth.conf ファイルに指定されたとおりにアクセスする
NetBackup 管理者権限を所有しているが、auth.conf ファイルにエントリが存在しない	完全なアクセス	完全なアクセス

auth.conf エントリ	CLI アクセス	Java インターフェースアクセス
NetBackup 管理者権限を所有し、auth.conf ファイルにエントリも存在する	完全なアクセス	auth.conf ファイルに指定されたとおりにアクセスする
auth.conf ファイルにエントリが存在せず、NetBackup 管理者権限も所有していない	アクセス不可	アクセス不可

6

NetBackup アクセス制御セキュリティ (NBAC)

この章では以下の項目について説明しています。

- NetBackup アクセス制御 (NBAC) の使用について
- NetBackup のアクセス管理
- NBAC (NetBackup アクセス制御) 構成について
- NetBackup アクセス制御 (NBAC) の構成
- NBAC の構成の概要
- スタンドアロンのマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成
- クラスタでの高可用性の NetBackup マスターサーバーのインストール
- クラスタ化されたマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成
- メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成
- クライアントでのアクセス制御のインストールおよび構成
- ブローカーと Windows リモートコンソール間の信頼関係の確立
- NBAC の構成コマンドの概略
- NetBackup アクセス制御 (NBAC) のアップグレード
- NetBackup ホットカタログバックアップへの認証データベースおよび認可データベースの追加について
- NetBackup の古いバージョンがリモートコンピュータにインストールされているルートブローカーを使っている場合の NetBackup のアップグレード

- NetBackup 7.0 より前のメディアサーバーおよびクライアントコンピュータの NetBackup アクセス制御 (NBAC) の構成
- [アクセス制御 (Access Control)]ホストプロパティの手動構成
- NetBackup 管理インフラストラクチャと setuptrust コマンドの統合
- setuptrust コマンドの使用
- マスターサーバーおよびメディアサーバーのホストプロパティへのアクセス
- [アクセス制御 (Access Control)]ホストプロパティ
- [ネットワーク設定 (Network Settings)]タブ
- [認証ドメイン (Authentication Domain)]タブ
- [認可サービス (Authorization Service)]タブ
- クライアントのホストプロパティへのアクセス
- クライアントの[アクセス制御 (Access Control)]ホストプロパティダイアログボックス
- クライアントの[認証ドメイン (Authentication Domain)]タブ
- クライアントの[ネットワーク設定 (Network Settings)]タブ
- アクセス管理のトラブルシューティングのガイドライン
- NetBackup Authentication and Authorization の構成とトラブルシューティング
- NBAC の問題のトラブルシューティング
- UNIX の検証手順について
- UNIX マスターサーバーの検証
- UNIX メディアサーバーの検証
- UNIX クライアントの検証
- UNIX マスターサーバーが存在する複合環境での検証項目
- 複合環境の UNIX マスターサーバーのマスターサーバーでの検証項目
- 複合環境の UNIX マスターサーバーのメディアサーバーでの検証項目
- 複合環境の UNIX マスターサーバーのクライアントでの検証項目
- Windows マスターサーバーが存在する複合環境での検証項目
- 複合環境の Windows マスターサーバーのマスターサーバーでの検証項目

- 複合環境の Windows マスターサーバーのメディアサーバーでの検証項目
- 複合環境の Windows マスターサーバーのクライアントでの検証項目
- Windows での検証項目
- Windows マスターサーバーでの検証項目
- Windows メディアサーバーでの検証項目
- Windows クライアントでの検証項目
- アクセス管理ユーティリティの使用
- nbac_cron ユーティリティについて
- nbac_cron ユーティリティの使用
- NetBackup へアクセス可能なユーザーの決定について
- 個々のユーザー
- ユーザーグループ
- NetBackup のデフォルトユーザーグループ
- ユーザーグループの構成
- 新しいユーザーグループの作成
- 既存のユーザーグループのコピーによる新しいユーザーグループの作成
- ユーザーグループの名前の変更
- [一般 (General)]タブ
- [ユーザー (Users)]タブ
- [ユーザー (Users)]タブの[定義されているユーザー (Defined Users)]ペイン
- [ユーザー (Users)]タブの[割り当て済みのユーザー (Assigned Users)]ペイン
- ユーザーグループへの新しいユーザーの追加
- ユーザーグループおよびユーザーの定義について
- 新しいユーザーとしてのログオン
- ユーザーグループへのユーザーの割り当て
- [アクセス権 (Permissions)]タブ
- 認可オブジェクトおよび権限について

- 権限の付与
- NetBackup ユーザーグループの特定のユーザー権限の表示
- 認可オブジェクト
- メディアの認可オブジェクトの権限
- ポリシーの認可オブジェクトの権限
- ドライブの認可オブジェクトの権限
- レポートの認可オブジェクトの権限
- NBU_Catalog の認可オブジェクトの権限
- ロボットの認可オブジェクトの権限
- ストレージユニットの認可オブジェクトの権限
- ディスクプールの認可オブジェクトの権限
- バックアップおよびリストアの認可オブジェクトの権限
- ジョブの認可オブジェクトの権限
- サービスの認可オブジェクトの権限
- ホストプロパティの認可オブジェクトの権限
- ライセンスの認可オブジェクトの権限
- ボリュームグループの認可オブジェクトの権限
- ボリュームプールの認可オブジェクトの権限
- デバイスホストの認可オブジェクトの権限
- セキュリティの認可オブジェクトの権限
- ファットサーバーの認可オブジェクトの権限
- ファットクライアントの認可オブジェクトの権限
- Vault の認可オブジェクトの権限
- サーバーグループの認可オブジェクトの権限
- キー管理システム (kms) グループの認可オブジェクトの権限

NetBackup アクセス制御 (NBAC) の使用について

NetBackup アクセス制御 (NBAC) は、マスターサーバー、メディアサーバー、クライアントに対して使われる、役割に基づくアクセス制御です。NBAC は、次のことが必要な場合に使うことができます。

- 1 つのアプリケーションに対して複数レベルの管理者権限を使う場合。たとえば、1 つのバックアッププリケーションに対して、オペレータ (テープのロードとアンロード)、ローカルの管理者 (1 つの施設内でのアプリケーションの管理)、統括的な管理者 (複数のサイトを担当し、バックアップポリシーを決定) を割り当てることができます。この機能はユーザーエラーの防止にもきわめて有効です。経験の浅い管理者に対して特定の操作を制限することにより、不慮の操作ミスが防止されます。
- システム管理にシステムの root 権限が必須とならないように管理者を分離する場合。システムの管理者とアプリケーションの管理者を分離することができます。

次の表は NBAC の注意事項をリストしたものです。

表 6-1 NBAC の注意事項

注意事項または問題	説明または解決
NBAC を構成する前の前提条件	ここでは、NBAC の構成を開始する前に準備しておくと役立つ前提条件を示します。これらの項目によりインストールが簡単になります。このインストールで使う情報は次のリストのとおりです。 ■ マスターサーバーのユーザー名またはパスワード (root 権限または管理者権限) ■ マスターサーバーの名前 ■ マスターサーバーに接続されるすべてのメディアサーバーの名前 ■ バックアップされるすべてのクライアントの名前 ■ ホスト名または IP アドレス **メモ:** ホスト名は有効な IP アドレスに解決可能であることが必要です。 ■ `ping` または `traceroute` コマンド (ホストに接続可能であることを確認するためのツールの 1 つとして使用)。これらのコマンドを使うことで、ファイアウォールやアクセスを遮断するための他の防御手段を構成していないことが確認できます。

注意事項または問題	説明または解決
マスターサーバー、メディアサーバー、クライアントのアップグレードが必要かどうかについての判断	マスターサーバー、メディアサーバー、クライアントのアップグレードが必要かどうかについては、次に基づいて判断します。 ■ マスターサーバー、メディアサーバー、クライアントのアップグレードによって提供される機能がそれぞれあります。 ■ NetBackup は、上位リビジョンのマスターサーバーおよび下位リビジョンのクライアントとメディアサーバーと連携して動作します。 ■ 機能の内容により配置される内容が決定されます。 ■ 配置は必要に応じて段階的に実行できます。
役割に関する情報	構成において役割を次のように決定します。 ■ ホストの管理者 (マスターサーバーの root 権限は主席管理者と同等)。 ■ 開始時の役割を決定した後、必要に応じて役割を追加します。
NBAC のライセンスキーの要件	アクセス制御を有効にする際にライセンスは必要ありません。
NBAC と KMS の権限	通常 NBAC を使って `Setupmaster` コマンドを実行するとき、NetBackup 関連グループの権限 (たとえば、NBU_Admin と KMS_Admin) が作成されます。デフォルトの root と管理者ユーザーもそれらのグループに追加されます。場合によっては NetBackup が 7.0 から 7.0.1 にアップグレードされるときに、root と管理者レベルのユーザーが KMS グループに追加されないことがあります。解決するには、root と管理者レベルのユーザーに NBU_Admin と KMS_Admin の権限を手動で付与します。
PBX からの共有セキュリティサービスを解除する間に表示される Windows Server Failover Clustering（WSFC）のエラーメッセージ	WSFC 環境で `bpnbaz -UnhookSharedSecSvcsWithPBX <virtualhostname>`コマンドを実行することにより、エラーメッセージをトリガできます。ただし共有の認証と認可サービスは、PBX から正常に解除され、エラーは無視できます。
表示される可能性のあるクラスタノードエラー	クラスタ環境で`bpnbaz -setupmaster` コマンドをローカル管理者として実行するとき、`AUTHENTICATION_DOMAIN`エントリには他のクラスタノードエントリが含まれない場合があります。そのような場合、これらのエントリはホストプロパティから`bp.conf` ファイルに手動で追加される必要があります。
カタログリカバリは、NBAC が REQUIRED モードに設定されているとき失敗します	NBAC がREQUIRED モードで実行され、カタログリカバリが実行された場合には、NBAC はPROHIBTED モードから REQUIRED モードにリセットされる必要があります。

注意事項または問題	説明または解決
ポリシーの検証は NBAC モードでは失敗します (つまり USE_VXSS = REQUIRED の場合)	次のいずれかが実行された場合、NBAC 有効化モードでのスナップショットポリシーのバックアップ、リストア、検証は失敗する場合があります。 ■ 認証済みの原理は NBAC グループから削除されます。NBU_Users グループ ■ NBU_User グループのバックアップとリストアの権限は削除されました
bpnbaz -setupmaster コマンドはエラー「認可サーバーに接続できません。」で失敗します	管理者以外のユーザーが NetBackup のセキュリティを変更しようとした場合には bpnbaz –setupmaster が失敗します。 管理者グループの一員である「管理者」ユーザーのみに NetBackup のセキュリティを修正したり NBAC を有効にする権限があります。
インストール中の認証ブローカー構成の失敗	システムの無効なドメイン名構成により認証ブローカーの構成中に失敗します。 この問題を修正するには、`bpnbaz -configureauth` コマンドを使って認証ブローカーを構成します。 `bpnbaz -configureauth` コマンドについて詳しくは、次を参照してください。『NetBackup コマンドリファレンスガイド』

NetBackup のアクセス管理

NetBackup へのアクセス権は、ユーザーグループを定義して、そのグループに権限を明示的に付与することによって制御できます。ユーザーグループを構成し、権限を割り当てることができます。NetBackup 管理コンソールの［アクセス管理 (Access Management)］を選択します。

メモ: NetBackup-Java 管理コンソールが機能するには、ユーザーがシステムにリモートでログオンする権限を所有している必要があります。

メモ: アクセス制御が構成されていないメディアサーバーは、root または管理者以外のユーザーが管理することはできません。

NBAC (NetBackup アクセス制御) 構成について

メモ: NBAC は NetBackup のインストールの一部としてすでにインストールされています。NBAC の構成のみこのリリースに必要になります。

NBAC の構成手順は、非 HA 環境の NBAC 構成向けです。NetBackup は、AIX、HP-UX、Linux、Solaris、Windows の環境における広範な HA 環境をサポートします。NBAC の構成は次のとおりです。

- 必要に応じて、マスターサーバーのクラスタを構築します。HA 情報については、レプリケーションとディザスタリカバリに関する『NetBackup 高可用性の環境管理者ガイド』を参照してください。クラスタに関する情報は、『NetBackup マスターサーバーのクラスタ化管理者ガイド』を参照してください。
- 提供される手順を使用して操作に関する NBAC を構成します。
  p.152 の「NetBackup アクセス制御 (NBAC) の構成」を参照してください。

NetBackup アクセス制御 (NBAC) の構成

メモ: 認証クライアントおよび認可クライアントの手動インストールは、古いメディアサーバーとクライアントホスト (NetBackup バージョン 7.5 未満) の場合に実行する必要があります。NetBackup バージョン 7.5 には、認証クライアントと認可クライアントが組み込まれています。認証サーバーと認可サーバーはメディアサーバーとクライアントに必要ありません。

NBAC の構成手順については、次の手順を参照してください。

NetBackup アクセス制御 (NBAC) の構成

1 マスターサーバーで NetBackup アクセス制御 (NBAC) を構成します。

p.154 の「スタンドアロンのマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成」を参照してください。

メモ: マスターサーバーは、スタンドアロンモードまたはクラスタでの高可用性構成としてインストールできます。

---

2 メディアサーバーで NBAC を構成します。

p.156 の「メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成」を参照してください。

3 クライアントで NBAC を構成します。

p.158 の「クライアントでのアクセス制御のインストールおよび構成」を参照してください。

NBAC の構成の概要

この項では、bpnbaz コマンドを使って NetBackup アクセス制御 (NBAC) を構成する場合の推奨事項について説明します。このコマンドは、NETBACKUP_INSTALL_PATH/bin/admincmd ディレクトリから使用できます。

bpnbaz ユーティリティは、マスターサーバー、メディアサーバーおよびクライアントで NBAC を構成するために必要になります。このツールは、すべての下位リビジョンのメディアサーバーやクライアントのホストの NBAC も構成します。bpnbaz コマンドの概略は、次の項を参照してください。p.160 の「NBAC の構成コマンドの概略」を参照してください。この項では、これらのコマンドの使用方法の例を、推奨される使用法の詳細とともに示します。サービスを構成した後は、サーバーとクライアントのそれぞれにおいてサービスを再起動する必要があります。

構成はマスターサーバーから実行されるため、マスターサーバー、メディアサーバー、およびクライアントの間で通信リンクが確実に動作することが必要です。前提条件リストを確認する方法: p.149 の「NetBackup アクセス制御 (NBAC) の使用について」を参照してください。その一覧を確認し、関連するメディアサーバー、クライアント、それらと通信するためのアドレスのすべてをメモしておいてください。

トラブルシューティングの情報については、次の項を参照してください。p.183 の「NetBackup Authentication and Authorization の構成とトラブルシューティング」を参照してください。トラブルシューティングの初期段階において便利な OS コマンドと NetBackup コマンドがあります。OS コマンドは ping、traceroute、および telnet です。NetBackup コマンドは bpclntcmd です。これらのコマンドは、ホストが相互に通信可能であることを確認するために使用します。

スタンドアロンのマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成

次の手順では、単一のコンピュータにインストールされているマスターサーバーで NetBackup アクセス制御 (NBAC) を構成する方法について記述します。マスターサーバーには、認証サーバーおよび認可サーバーが必要です。

次の表に、NBAC 構成例のホスト名を示します。

表 6-2　ホスト名の例

ホスト名	Windows	UNIX
マスターサーバー	win_master	unix_master
メディアサーバー	win_media	unix_media
クライアント	win_client	unix_client

次の手順では、スタンドアロンのマスターサーバーでの NBAC の構成方法について説明します。

メモ: マスターサーバーで `-setupmaster` を使用して `USE_VXSS = AUTOMATIC` を設定してください。`USE_VXSS = REQUIRED` がマスターサーバーで設定されている場合にメディアサーバーで NBAC を構成しようとすると、NetBackup マスターサーバーが `REQUIRED` モードで構成されていることを示すエラーが発生することがあります。モードを `AUTOMATIC` に変更してメディアサーバーの構成を完了してください。

スタンドアロンのマスターサーバーでの NBAC の構成

1. すべての NetBackup マスターサーバーのインストールまたはアップグレードを実行します。
2. `bpnbaz -setupmaster` コマンドを実行します。

   「y」を入力します。システムは構成情報を集め始めます。それから、システムは認可情報を設定し始めます。
3. `bpnbaz -setupmaster` コマンドが正常に終了したら、このコンピュータの NetBackup サービスを再起動します。
4. メディアサーバーの設定に進みます。p.156 の「メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成」を参照してください。

クラスタでの高可用性の NetBackup マスターサーバーのインストール

クラスタで高可用性の NetBackup マスターサーバーをインストールするには次の手順を使うことができます。

NetBackup のインストールとクラスタ化

1. NetBackup マスターサーバーをインストールするクラスタシステムを構成します。
2. クラスタのすべてのノードに NetBackup マスターサーバーをインストールします。
3. NetBackup マスターサーバーをクラスタ化します。HA 情報については、レプリケーションとディザスタリカバリに関する『NetBackup 高可用性の環境管理者ガイド』を参照してください。クラスタに関する情報は、『NetBackup マスターサーバーのクラスタ化管理者ガイド』を参照してください。
4. NBAC を有効化せずに NetBackup ドメイン内で動作することを確認するために、テストバックアップを実行します。

クラスタ化されたマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成

メモ: Windows のクラスタ化環境では、-setupmaster の実行後に、パッシブノードの `AUTHENTICATION_DOMAIN` エントリがアクティブノードの名前と同じである場合があります。これは許容されません。パッシブノードでのフェールオーバー後、`MFC UI` が (<[local machine name] > ¥[Administrator user] を使って) 起動されると、認証関連のポップアップエラーメッセージが表示されます。この問題の回避策は setupmaster の実行後 (フェールオーバーの前) に、パッシブノードの `AUTHENTICATION_DOMAIN` にローカルノード名を認証ドメインとして追加することです。`AUTHENTICATION_DOMAIN` の値を更新する前に、`C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd¥bpgetconfig` コマンドを使って現在の値を取得します。それから `C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd¥bpsetconfig` コマンドを使って既存のドメインリストに認証ドメインとしてローカルノード名を追加します。`bpsetconfig` コマンドプロンプトを終了して保存するには、`Ctrl + Z` を押し、`Enter` キーを押します。

メモ: クラスタのアクティブノードで NBAC モードを REQUIRED から PROHIBITED に戻すと、クラスタがエラー状態になることがあります。この問題の回避策は次の操作を実行することです。アクティブノードで bpclusterutil -disableSvc nbatd コマンドを実行し、次に bpclusterutil -disableSvc nbazd コマンドを実行します。bpsetconfig コマンドを使って bp.conf USE_VXSS=AUTOMATIC または REQUIRED の値を PROHIBITED に変更します。アクティブノードで bpclusterutil -enableSvc nbazd コマンド、その次に bpclusterutil -enableSvc nbatd コマンドを実行して、セキュリティサービスを監視するために NBAC を REQUIRED モードに変更します。

クラスタ化されたマスターサーバーで NetBackup アクセス制御 (NBAC) を構成するには、次の手順を実行します。

クラスタ化されたマスターサーバーでの NetBackup アクセス制御 (NBAC) の構成

1. プライマリクラスタノードにログオンします。
2. Windows を使用している場合は、コマンドコンソールを開きます。
3. UNIX の場合は、ディレクトリを /usr/openv/netbackup/bin/admincmd に変更します。Windows の場合は、ディレクトリを C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd に変更します。
4. アクティブノードで bpnbaz -setupmaster を実行します。
5. マスターサーバーのコンソール GUI にログオンします。
6. NBAC の設定を確実に有効にするために、NetBackup サービスを再起動してください。

メディアサーバーでの NetBackup アクセス制御 (NBAC) の構成

次の手順では、NetBackup 構成内のメディアサーバーで NetBackup アクセス制御 (NBAC) を構成する方法について記述します。これらの手順は、マスターサーバーと同じ場所に配置されていないメディアサーバーに必要です。

メモ: マスターサーバーで -setupmedia を使用して USE_VXSS = AUTOMATIC を設定してください。USE_VXSS = REQUIRED がマスターサーバーで設定されている場合にメディアサーバーで NBAC を構成しようとすると、NetBackup マスターサーバーが REQUIRED モードで構成されていることを示すエラーが発生することがあります。モードを AUTOMATIC に変更してメディアサーバーの構成を完了してください。

メディアサーバーでのアクセス制御の構成

1. マスターサーバーコンピュータにログオンします。
2. bpnbat -login コマンドを実行します。

   コマンドのエラーを防ぐため、必ず bpnbat -login コマンドを実行してから bpnbaz -setupmedia コマンドを実行してください。

   bpnbaz -setupmedia コマンドには、いくつかのオプションがあります。

   このコマンドは、個別のホストまたは -all オプションのいずれかの拡張が指定されていないと動作しません。

   p.160 の「NBAC の構成コマンドの概略」を参照してください。

   最初に -dryrun オプションを使用して、構成のドライランを実行をすることをお勧めします。このオプションは、-all および単一のサーバー構成の両方に使用できます。デフォルトでは、検出されたホストのリストは SetupMedia.nbac ファイルに書き込まれます。また、-out <output file> オプションを使用して、ユーザー独自の出力ファイル名を指定することもできます。ユーザー独自の出力ファイルを使う場合、-file オプションを使って、このファイルを以降の実行に渡す必要があります。ドライランコマンドは、次のように指定します。

   bpnbaz -SetupMedia -all -dryrun [-out <outfile>] または

   bpnbaz -SetupMedia <media.server.com> -dryrun [-out <outfile>]

   更新するメディアサーバーがすべてログファイルにある場合、-dryrun オプションを使用します。-all コマンドを使うことにより、それらすべてを一度に実行することができます。たとえば、次のように使用できます。

   bpnbaz -SetupMedia -all または

   bpnbaz -SetupMedia -file <progress file>

   -all オプションを使う場合、検出されたすべてのメディアサーバーがコマンドを実行するたびに更新される点に注意してください。選択したメディアサーバーのセットに対してコマンドを実行することもできます。構成するメディアサーバーのホスト名のみをファイルに保持し、-file オプションを使用してそのファイルを渡します。この入力ファイルは、SetupMedia.nbac、または前述のドライランの際に -out オプションで与えたカスタムファイル名になります。たとえば、次のように指定できます。- bpnbaz -SetupMedia -file SetupMedia.nbac。

   単一のメディアサーバーを構成する場合には、メディアサーバーのホスト名をオプションとして指定します。たとえば、以下を使用します。

   bpnbaz -SetupMedia <media.server.com>

3 コマンドが正常に終了したら、ターゲットのメディアサーバーの NetBackup サービスを再起動します。

これより、ターゲットホストで NBAC が設定されます。特定のターゲットホストの構成が完了しなかった場合には、出力ファイルを確認してください。

この手順の後、クライアントホストのアクセス制御の構成に進みます。

p.158 の「クライアントでのアクセス制御のインストールおよび構成」を参照してください。

クライアントでのアクセス制御のインストールおよび構成

次の手順では、NetBackup 構成内でクライアントに NetBackup アクセス制御をインストールおよび構成する方法について説明します。ターゲットのクライアントは、バージョン 7.1 以上の NetBackup クライアントソフトウェアを実行していることが必要です。

クライアントでのアクセス制御のインストールおよび構成

1 クライアントマシンのバックアップが現在実行されていないことを確認します。

2 UNIX の root ユーザーまたは Windows 管理者としてマスターサーバーマシンにログインします。

3 認証デーモン (`nbatd`) が動作していることを確認します。そうでない場合は、認証デーモンを起動します。

4 `NBU_INSTALL_PATH/bin` ディレクトリに移動します。

5 次のコマンドを使用して、NetBackup セキュリティ管理者としてログオンします。

メモ: マスターサーバーの UNIX の root ユーザーおよび Windows の管理者がデフォルトの NetBackup セキュリティ管理者です。

```
bpnbat -Login
```

次の情報が表示されます。

```
Authentication Broker [master.server.com is default]:
Authentication port [0 is default]:
Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd)
[unixpwd is default]:
Domain [master.server.com is default]:
Login Name [root is default]:
Password:
Operation completed successfully.
```

6 前述のオプションを使用して、bpnbaz -SetupClient を実行します。

このコマンドは、個別のホストまたは -all オプションのいずれかの拡張が指定されていないと動作しない点に注意してください。

p.160 の「NBAC の構成コマンドの概略」を参照してください。

最初にドライランを実行して、すべてのクライアントがマスターサーバーで確認できることを確認します。この処理は、クライアントが多数 (250 超) 存在する場合に使用します。-dryrun オプションは、-all および単一のサーバー構成の両方に使用できます。デフォルトでは、検出されたホストのリストは同じディレクトリの SetupClient.nbac ファイルに書き込まれます。また、-out <output file> オプションを使用して、ユーザー独自の出力ファイル名を指定することもできます。ユーザー独自の出力ファイルを使う場合、-file オプションを使って、このファイルを以降の実行に渡す必要があります。たとえば、次のように使用できます。

bpnbaz -SetupClient -all -dryrun [-out <outfile>] または

bpnbaz -SetupClient <client.host.com> -dryrun [-out <outfile>]

ドライランの後、クライアントのホスト名を確認し、-dryrun オプションを使用せずに同じコマンドを実行します。たとえば、次のように使用します。

bpnbaz -SetupClient -all または

bpnbaz -SetupClient -file SetupClient.nbac or bpnbaz -SetupClient <client.host.com>

-all オプションは、マスターサーバーに既知のクライアントで実行されます。大規模な環境 (クライアントが 250 超) では、すべてのクライアントに対応するのに時間を要することがあります。

-all でクライアントを列挙することにより、すべてのクライアントのクレデンシャルが更新されます。その場合、時間とリソースを要することがあります。クライアントのサブセットを更新する場合には、代わりに -file オプションを使用します。進捗ファイルのすべてのクライアントが正常に構成されるまで、同じコマンドを複数回実行できます。各クライアントの状態は、入力ファイルで更新されます。それぞれの実行で正常に終了したクライアントは、以降の実行ではコメントアウトされます。小さいサブセットが連続した実行ごとに残ります。このオプションは、多数のクライアント (250 超) を追加した場合に使用します。実行時に更新するクライアントを対象にします。

-images オプションに -all を使うと、イメージカタログでクライアントのホスト名が検索されます。そのため、さらに大規模な環境の廃止されたホストを返すことができます。更新する必要があるホストを判別するには、-images オプションを付けて -all -dryrun オプションを実行します。

7 インストールが終了したら、目的のクライアントのクライアントサービスを再起動します。

ブローカーとWindowsリモートコンソール間の信頼関係の確立

次の手順によって、マスターサーバー (ブローカー) と管理クライアント間の信頼関係を確立します。

ブローカーと Windows リモートコンソール間の信頼関係の確立

1. マスターサーバーから、次のコマンドを実行します。

   ```
   Install_path¥Veritas¥NetBackup¥bin¥
   admincmd>bpgetconfig USE_VXSS AUTHENTICATION_DOMAIN
   >VXSS_SETTINGS.txt
   ```

   VXSS_SETTINGS.txt の出力例は次のとおりです。

   ```
   USE_VXSS = AUTOMATIC
   AUTHENTICATION_DOMAIN = <domain_name> "" WINDOWS <broker_host> 0
   ```

2. VXSS_SETTINGS.txt を管理クライアントにコピーします。
3. 管理クライアントから、次のコマンドを実行します。

   ```
   C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd>bpsetconfig
   "<absolute_path>¥VXSS_SETTINGS.txt"
   ```

   このコマンドを実行すると、管理クライアントの設定とブローカーの設定が一致します。また、管理クライアントがブローカーに自動的にログオンするように設定されます。
4. 管理クライアントから NetBackup 管理コンソールを起動し、ブローカーとの信頼関係の確立を要求する必要があります。一度信頼関係が確立されると、NetBackup 管理コンソールが利用可能になります。

NBAC の構成コマンドの概略

次の表に、NBAC のクイック構成手順で使用されるコマンドの概略を示します。

コマンドの使用方法の説明では、次の表記規則を使用します。

角カッコ [ ] の中のコマンドラインの要素は、必要に応じて指定します。

垂直バーまたはパイプ (|) は、選択可能な引数の区切りを示します。たとえば、コマンドの形式が command arg1|arg2 の場合、変数 arg1 または arg2 を選択できます。

表 6-3　NBAC の構成コマンドの概略

コマンド	説明
bpnbaz -GetConfiguredHosts [target.server.com [-out file] | -all [-outfile] | -file progress.file]	bpnbaz -GetConfiguredHosts コマンドは、ホストの NBAC 状態を取得するために使われます。このコマンドには、-all または target.server.com オプションが必要です。 構文は次のとおりです。 ■ *target.server.com* は、1 台のターゲットホストの名前です。たとえば、1 台のホストの NBAC 状態を確認する場合にこのオプションを使用します。 ■ -out オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は SetupMedia.nbac ファイルに書き込まれます。このオプションは、-all および単一のホスト構成オプションに使用できます。 ■ -all オプションを指定すると、すべてのポリシーが調べられ、一意のホスト名がすべて収集されます。これらのホスト名は、ポリシー内で調べられます。さらに、構成済みのメディアサーバーがすべて収集され、各ホストの NBAC 状態が ConfiguredHosts.nbac ファイルに取得されます。 ■ -file progress.file は、progress_file から読み取るホスト名を指定する場合に使われるオプションです。このオプションは、progress_file の 1 行ごとにホスト名が 1 つ記述されていることを想定しています。この CLI により、progress_file の NBAC の状態が更新されます。hostname の後に # が付加され、その後に NBAC の状態が続きます。 ■ target.server.com または -all オプションとともに使う場合、ホストの状態は ConfiguredHosts.nbac ファイルに取得されます。

コマンド	説明
bpnbaz -SetupMaster [-fsa [<domain type>:<domain name>:]<user name>]	bpnbaz -SetupMaster コマンドは、NBAC を使用するためのマスターサーバーを設定するために実行します。認可サーバーと認証ブローカーは、マスターサーバーにインストールして実行するように想定されています。 NBU 管理者として特定の OS ユーザーをプロビジョニングするには、最初のセキュリティ管理者オプションを指定して bpnbaz -SetupMaster -fsa コマンドを使います。 構文は次のとおりです。 ■ -fsa オプションは、NBU 管理者として特定の OS ユーザーをプロビジョニングするために使われます。このオプションを使用するときに、現在の OS のユーザー識別情報に対するパスワードの入力が求められます。 ■ *domain type* は、使用しているネットワークドメインの種類です。たとえば、bpnbaz -SetupMaster -fsa nt:ENTERPRISE:jdoe コマンドは、NBU 管理者として Windows のエンタープライズドメインユーザー jdoe をプロビジョニングします。 ■ *domain name* は、使用している特定のドメインの名前です。たとえば、bpnbaz -SetupMaster -fsa jdoe コマンドは、現在のログオンユーザーのドメイン形式 (Windows/UNIXPWD)、ドメイン名を取得し、そのドメインの jdoe ユーザーをプロビジョニングします。 ■ *user name* は NBU 管理者として指定している特定の OS ユーザー名です。 **メモ:** ユーザーは、指定済みのドメインに存在するか検証されます。ログオンしている管理者または root を NBU 管理者としてプロビジョニングする既存の動作は保持されます。

コマンド	説明
`bpnbaz -SetupMedia [ media.server.com [-out file] | -all [-out file] | -file progress.file ] [-dryrun] [-disable]`	`bpnbaz -SetupMedia` コマンドは、NBU_Administrator グループのメンバーがマスターサーバー上で実行します。このコマンドは、`bpnbaz -SetupMaster` が正常に終了するまで実行しないでください。マスターサーバーとターゲットメディアサーバーシステム間の接続を想定します。このコマンドには、`-all` または `target.server.com` オプションが必要です。 構文は次のとおりです。 ■ *media.server.com* は単一のターゲットホストの名前です。NBAC で使用する単一の追加ホストを追加するにはこのオプションを使用します。 ■ `-out` オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は `SetupMedia.nbac` ファイルに書き込まれます。このオプションは、`-all` および単一のホスト構成オプションに使用できます。 ■ `-all` を指定すると、すべてのストレージユニットが調べられ、ストレージユニットで見つかった一意のホスト名がすべて収集されます。これらは、ソートした順序で試行できます。結果は進捗ファイルに書き込まれます。 ■ `-file` *`progress_file`* オプションは、一連のメディアサーバーホスト名を持つ入力ファイルを指定する場合に使用します。実行後、各メディアサーバーの状態は進捗ファイルで更新されます。正常に完了したホストは、以降の実行ではコメントアウトされます。このコマンドは、入力ファイルのすべてのメディアサーバーが正常に構成されるまで繰り返すことができます。 ■ `-dryrun` はメディアサーバー名のリストを生成し、ログに書き込むことができます。このオプションは media.server.com で機能しますが、`-all` オプションとともに使用することを目的にしています。 ■ `-disable` オプションは、ターゲットホストの NBAC を無効化 (USE_VXSS = PROHIBITED) できます。

コマンド	説明
bpnbaz -SetupClient [client.server.com [-out file] | -all [-images] [-out file] | -file progress.file] [-dryrun] [-disable]	bpnbaz -SetupClient コマンドは、クライアントの NBAC を設定するために使われます。このコマンドは、bpnbaz -SetupMaster コマンドが正常に終了するまで実行しないでください。bpnbaz -SetupClient は、マスターサーバーから実行する必要があります。このコマンドは、マスターサーバーとターゲットクライアントシステムが接続されていることを想定しています。このコマンドには、-all または target.server.com オプションが必要です。 構文は次のとおりです。 ■ *client.server.com* は、1 台のターゲットホストの名前です。たとえば、NBAC で使用するホストを 1 台追加する場合に、この名前が選択肢となります。 ■ -out オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は SetupClient.nbac ファイルに書き込まれます。このオプションは、-all および単一のホスト構成オプションに使用できます。-out オプションは、カスタム出力ファイル名を指定するために使われます。デフォルトでは、出力は SetupClient.nbac ファイルに書き込まれます。このオプションは、-all および単一のホスト構成オプションに使用できます。 ■ -all オプションを指定すると、すべてのポリシーが調べられ、ポリシー内で見つかった一意のホスト名がすべて収集されます。ポリシーは、ソートした順序で試行されます。結果は進捗ファイルに書き込まれます。 ■ -images オプションを指定すると、一意のホスト名のイメージがすべて検索されます。大規模なカタログが存在する場合には、-dryrun オプションを追加しないかぎり、このオプションは推奨できません。このオプションは、イメージカタログ内に含まれるすべての一意のクライアントに対応します。古いカタログには、膨大な数の廃止されたホストや、新しいマスターに移動されたホスト、名前が変更されたホストが含まれる可能性があります。到達不能なホストへの接続が試行される場合、コマンドの実行時間が長くなる可能性があります。 ■ -dryrun は、クライアント名のリストを生成し、それらをログに書き込むオプションです。この場合、ターゲットシステムの実際の構成は実行されません。 ■ -disable は、ターゲットホストの NBAC を無効化 (USE_VXSS = PROHIBITED) するオプションです。 ■ -file progress.file は、進捗ログに異なるファイル名を指定する場合に使われるオプションです。この CLI により、progress_file からホスト名が読み取られます。状態は、各ホスト名の横に [# separated value] とともに追加されます。正常に完了したホストは、コメントアウトされます。このコマンドは、progress_file のすべてのクライアントが正常に構成されるまで複数回実行することができます。

NetBackup アクセス制御 (NBAC) のアップグレード

メモ: NBAC が有効になっている場合、NBAC は NetBackup アップグレードの一部としてアップグレードされます。NetBackup のアップグレード方法の手順については、『NetBackup アップグレードガイド』を参照してください。アップグレードが実行されるときに現在のAT および AZ サービスが動作していることを確認してください。NetBackup がクラスタサーバーで動作している場合は、NetBackup が動作してアップグレードが実行されているアクティブノードで両方のサービスが動作していることを確認してください。

次の手順では、NetBackup アクセス制御 (NBAC) のアップグレード方法について説明します。

NetBackup アクセス制御 (NBAC) のアップグレード

1. マスターサーバーで NetBackup を停止します。
2. NetBackup をアップグレードします。

   メディアサーバーおよびクライアントコンピュータで、NetBackup を停止した後、NetBackup をアップグレードします。共有の認証と認可のパッケージは、メディアサーバーおよびクライアントコンピュータで使われなくなります。これらの製品が他のシマンテック製品で使用されていない場合には、これらを削除できます。

NetBackup ホットカタログバックアップへの認証データベースおよび認可データベースの追加について

オンラインホットカタログバックアップ方式を使用する NetBackup 環境の場合、NetBackup の認証データベースおよび認可データベースをカタログバックアップに含めるために追加の構成を行う必要はありません。

NetBackup の古いバージョンがリモートコンピュータにインストールされているルートブローカーを使っている場合の NetBackup のアップグレード

NetBackup の古いバージョンがリモートコンピュータにインストールされているルートブローカーを使っている場合の NetBackup のアップグレードには次の手順を使うことができます。

NetBackup の古いバージョンがリモートコンピュータにインストールされているルートブローカーを使っている場合の NetBackup のアップグレード

1. NetBackup にアップグレードする前に、NetBackup サービスを停止し、USE_VXSS=PROHIBITED を設定することによって NBAC を無効にします。USE_VXSS の新しい値を設定するには、次のコマンドを実行します。それから NetBackup のアップグレードを開始します。

   UNIX プラットフォームでは、次のコマンドを使います。

   ```
   /usr/openv/netbackup/bin/admincmd/bpsetconfig
   bpsetconfig> USE_VXSS=PROHIBITED
   bpsetconfig>Crtl + D (to save and quit).
   ```

   Windows では、次のコマンドを使います。

   ```
   C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd¥bpsetconfig
   bpsetconfig> USE_VXSS=PROHIBITED
   bpsetconfig> Crtl + Z + Enter (to save and quit).
   ```

2. NetBackup のアップグレードが完了したら、NetBackup に付属の atutil ツールを使って、リモートルートブローカー（RB）とローカル共有の認証ブローカー（AB）を NetBackup に移行します。

3. NetBackup コンピュータからルートブローカーコンピュータに atutil ユーティリティをコピーします。

   UNIX プラットフォームでは、NetBackup コンピュータからルートブローカーコンピュータに /usr/openv/netbackup/sec/at/bin/atutil ファイルをコピーします。

   Windows では、NetBackup コンピュータからルートブローカーコンピュータに C:¥Program Files¥Veritas¥NetBackup¥sec¥at¥bin¥atutil.exe ファイルをコピーします。

4. atutil コマンドがコピーされたディレクトリに移動します。次に、atutil export -r -f <RB output xml file> -p <password> コマンドを実行してルートブローカーをエクスポートします。

5. エクスポートされたファイルを NetBackup コンピュータにコピーします。

6 次のコマンドを実行して NetBackup コンピュータにルートブローカーをインポートします。

UNIX プラットフォームでは、 `/usr/openv/netbackup/sec/at/bin/atutil import -z /usr/openv/var/global/vxss/eab/data/ -f <RB output xml file> -p <password>` を実行します。

Windows では、`C:¥Program Files¥Veritas¥NetBackup¥sec¥at¥bin¥atutil import -z C:¥Program Files¥Veritas¥NetBackup¥var¥global¥vxss¥eab¥data -f <RB output xml file> -p <password>` を実行します。

クラスタコンピュータでは、***-z*** オプションは共有ドライブを指す必要があります。

7 次のコマンドを実行して `R+AB` モードで NetBackup Authentication Service を構成します。

UNIX プラットフォームでは、`/usr/openv/netbackup/sec/at/bin/vssregctl -s -f /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf -b "Security¥Authentication¥Authentication Broker" -k Mode -t int -v 3` を実行します。

Windows では、`C:¥Program Files¥Veritas¥NetBackup¥sec¥at¥bin¥vssregctl -s -f C:¥Program Files¥VERITAS¥NetBackup¥var¥global¥vxss¥eab¥data¥systemprofile¥VRTSatlocal.conf -b "Security¥Authentication¥Authentication Broker" -k Mode -t int -v 3` を実行します。

クラスタコンピュータでは、共有ドライブを指すように ***-f*** オプションを設定します。

8 認証サービスを開始するために `USE_VXSS` の値を AUTOMATIC に設定します。`USE_VXSS` の新しい値を設定するには、次のコマンドを実行します。

UNIX プラットフォームの場合、

```
/usr/openv/netbackup/bin/admincmd/bpsetconfig
bpsetconfig> USE_VXSS=AUTOMATIC
bpsetconfig> Crtl + D (to save and quit).
```

Windows の場合、

```
C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd¥bpsetconfig
bpsetconfig> USE_VXSS=AUTOMATIC
bpsetconfig> Crtl + Z + Enter (to save and quit).
```

9 次のコマンドを実行して NetBackup Authentication Service を開始します。

UNIX プラットフォームでは、/usr/openv/netbackup/bin/nbatd を実行します。

Windows では、net start nbatd を実行します。

10 USE_VXSS の値を PROHIBITED にリセットします。

UNIX プラットフォームでは、手動で /usr/openv/netbackup/bp.conf ファイルを編集し、USE_VXSS を PROHIBITED に設定します。

Windows では、HKEY_LOCAL_MACHINE¥SOFTWARE¥Veritas¥NetBackup¥CurrentVersion¥Config のレジストリエントリを開き、USE_VXSS の値を PROHIBITED に設定します。

11 共有 AB ドメインをエクスポートし、NetBackup に次のコマンドを実行することによってインポートします。

UNIX プラットフォームでは、次のコマンドを順次実行します。

```
/usr/openv/netbackup/sec/at/bin/atutil export -t ab -f
 <AB output xml file> -p <password>
/usr/openv/netbackup/sec/at/bin/atutil import -z
/usr/openv/var/global/vxss/eab/data/ -f <AB output xml file> -p
 <password>.
```

Windows で、次のコマンドを順次実行します。

```
C:¥Program Files¥Veritas¥NetBackup¥sec¥at¥bin¥atutil export -t
 ab -d broker -f <AB output xml file> -p <password>
C:¥Program Files¥Veritas¥NetBackup¥sec¥at¥bin¥atutil import -z
 C:¥Program Files¥Veritas¥NetBackup¥var¥global¥vxss¥eab¥data -f
<AB output xml file> -p <password>
```

クラスタコンピュータでは、*-z* オプションは共有ドライブを指す必要があります。

12 次のコマンドを実行して NetBackup Authentication Service を開始します。

UNIX プラットフォームでは、/usr/openv/netbackup/bin/nbazd -f を実行します。

Windows では、net start nbazd を実行します。

13 共有 AZ サービスにログオンします。

UNIX プラットフォームでは、`/opt/VRTSaz/bin/vssaz login --domain localhost` を実行します。

Windows X86 プラットフォームでは、 `C:¥Program Files¥VERITAS¥Security¥Authorization¥bin¥ vssaz login --domain localhost` を実行します。

Windows X64 プラットフォームでは、`C:¥Program Files (x86)¥VERITAS¥Security¥Authorization¥bin¥ vssaz login --domain localhost` を実行します。

14 次のコマンドを使って共有 AZ から NetBackup APS の名前を検索します。

UNIX プラットフォームでは、`/opt/VRTSaz/bin/vssaz listaps` を実行します。

Windows X86 プラットフォームでは、`C:¥Program Files¥VERITAS¥Security¥Authorization¥bin¥ vssaz listaps` を実行します。

Windows X64 プラットフォームでは、`C:¥Program Files (x86)¥VERITAS¥Security¥Authorization¥bin¥ vssaz listaps` を実行します。

15 次のコマンドを実行して共有 AZ から NetBackup リソースの集合をエクスポートします。

UNIX プラットフォームでは、`/opt/VRTSaz/bin/vssaz rcexport --toplevelrcname <NBU APS name>` を実行します。

Windows X86 プラットフォームでは、`C:¥Program Files¥VERITAS¥Security¥Authorization¥bin¥vssaz rcexport --toplevelrcname <NBU APS name>` を実行します。

Windows X64 プラットフォームでは、`C:¥Program Files (x86)¥VERITAS¥Security¥Authorization¥bin¥vssaz rcexport --toplevelrcname <NBU APS name>` を実行します。

16 次のコマンドを使って共有 AZ からログアウトします。

UNIX プラットフォームでは、`/opt/VRTSaz/bin/vssaz logout` を実行します。

Windows X86 プラットフォームでは、`C:¥Program Files¥VERITAS¥Security¥Authorization¥bin¥ vssaz logout` を実行します。

Windows X64 プラットフォームでは、`C:¥Program Files (x86)¥VERITAS¥Security¥Authorization¥bin¥ vssaz logout` を実行します。

17 次のコマンドを使って NetBackup の AZ にログオンします。

UNIX プラットフォームでは、`/usr/openv/netbackup/sec/az/bin/vssaz login --domain localhost` を実行します。

Windows では、`C:¥Program Files¥Veritas¥NetBackup¥sec¥az¥bin¥ vssaz login --domain localhost` を実行します。

18 次のコマンドを使って共有 AZ から NetBackup に NetBackup リソースの集合をインポートします。

UNIX プラットフォームでは、`/usr/openv/netbackup/sec/az/bin/vssaz rcimport --location /var/VRTSaz/objdb/export/<OID>/rc_<OID>.xml` を実行します。

Windows X86 プラットフォームでは、`C:¥Program Files¥Veritas¥NetBackup¥sec¥az¥bin¥ vssaz rcimport --location C:¥Program Files¥VERITAS¥Security¥Authorization¥data¥objdb¥export¥<OID>¥rc_<OID>.xml` を実行します。

Windows X64 プラットフォームでは、`C:¥Program Files¥Veritas¥NetBackup¥sec¥az¥bin¥ vssaz rcimport --location C:¥Program Files (x86)¥VERITAS¥Security¥Authorization¥data¥objdb¥export¥<OID>¥rc_<OID>.xml` を実行します。

19 `USE_VXSS = PROHIBITED` モードで NetBackup サービスを再起動します。

20 `setupmaster` コマンドを実行します。

21 NetBackup サービスを再起動します。

NetBackup 7.0 より前のメディアサーバーおよびクライアントコンピュータの NetBackup アクセス制御 (NBAC) の構成

メモ: この手順は NetBackup 7.0 より前のメディアサーバーおよびクライアントコンピュータにのみ適用可能です。NetBackup リリース 7.0 以降では組み込みのクライアントを使用します。

NetBackup 7.0 より前のメディアサーバーおよびクライアントコンピュータの NetBackup アクセス制御 (NBAC) を構成するために次の手順を使うことができます。

NetBackup 7.0 より前のメディアサーバーおよびクライアントコンピュータの NetBackup アクセス制御 (NBAC) の構成

1 認証および認可のクライアントパッケージをターゲットコンピュータにインストールします。

ターゲットコンピュータが NetBackup クライアントの場合は、認証クライアントのみをインストールします。ターゲットコンピュータが NetBackup メディアサーバーの場合は、認証クライアントと認可クライアントの両方をインストールします。

クライアントバイナリとサーバーバイナリの両方をターゲットコンピュータにインストールすることを選択できますが、サーバーを構成する必要はありません。以前の NetBackup メディアに付属のインフラストラクチャ共通サービス (ICS) DVD に収録された認証パッケージと認可パッケージをインストールする必要があります。NetBackup 7.6 に付属の認証バイナリと認可バイナリは、以前の NetBackup メディアサーバーやクライアントと互換性がない場合があります。

UNIX プラットフォームでは、`installics` ユーティリティを使って、認証パッケージと認可パッケージをインストールします。

Windows では、`VxSSVRTSatSetup.exe` および `VRTSazSetup.exe` を使います。

認証と認可のクライアントのインストール方法について詳しくは、以前の NetBackup のマニュアルを参照してください。

2 マスターサーバーから `bpnbaz -setupmedia` を実行し、7.0 より前のメディアサーバーのパスワードを入力します。

3 ターゲットメディアサーバーまたはクライアントホストの[アクセス制御 (Access Control)]ホストプロパティを適切に設定します。

メディアサーバーの場合: p.174 の「マスターサーバーおよびメディアサーバーのホストプロパティへのアクセス」を参照してください。

クライアントの場合: p.179 の「クライアントのホストプロパティへのアクセス」を参照してください。

4 ターゲットのメディアサーバーまたはクライアントコンピュータの NetBackup プロセスを再起動します。

[アクセス制御 (Access Control)]ホストプロパティの手動構成

メモ: この構成を自動で実行するには、`bpnbaz -setupClient` コマンド、`bpnbaz -setupMedia` コマンドおよび `bpnbaz -setupMaster` コマンドを実行します。この構成が必要になるのは、デフォルトを変更する場合やブローカーを追加する場合のみです。また、下位リビジョンのメディアサーバーやクライアントホストの場合にも実行します。

以降の項は、[アクセス制御 (Access Control)]ホストプロパティを手動で構成する場合に参照してください。

メモ: クライアントでアクセス制御が構成されるまでは、マスターサーバーの[NetBackup Product Authentication and Authorization]プロパティを[自動 (Automatic)]に設定する必要があります。クライアントの構成後、マスターサーバーの[NetBackup Product Authentication and Authorization]プロパティを[必須 (Required)]に変更してください。

NetBackup 管理インフラストラクチャと setuptrust コマンドの統合

メモ: これは OpsCenter サーバー名がインストール時に入力されると自動的に実行されます。そうでなければ、NBU マスターに OpsCenter サーバー名を追加する CLI があります。これは NBU 側から信頼確立部分を処理します。

シマンテック製品管理サーバーは、1 つの製品の管理者が別の製品を管理するための権限を持つように通信する必要があります。この通信により、1 つの管理サーバーのアプリケーション処理が別のサーバーと連携して動作することが保証されます。通信を保証するための 1 つの方法は、ルートブローカーと呼ばれる共通の独立したセキュリティサーバーを使うことです。すべての管理サーバーが共通のルートブローカーを指す場合、各サーバーの権限は共通の証明書に基づきます。通信を保証するためのもう 1 つの方法は、`setuptrust` コマンドを使うことです。このコマンドは、2 つの管理サーバー間で信頼を確立するために使われます。このコマンドは、別の管理サーバーを信頼する必要がある管理サーバーから発行されます。セキュリティ情報は、そのホストから、信頼の確立を要求しているホストに転送されます。一方向の信頼が確立されます。双方向 (相互) の信頼の設定は、これら 2 つのサーバーのそれぞれが `setuptrust` コマンドを発行することにより実行されます。たとえば、Symantec の構成に Symantec OpsCenter Server (OPS) と 3 つのマスターサーバー (A、B、C) が含まれるとします。それぞれのマスターサーバーは、クライアントおよびメディアサーバーの NBAC ポリシーと管理に接続されています。

最初のステップは、それぞれのマスターサーバー (A、B、C) との信頼を Symantec OpsCenter Server (OPS) に設定することです。この信頼は、Symantec OpsCenter Server が、それぞれのマスターサーバー、およびそれぞれのマスターサーバーに接続されたクライアントおよびメディアサーバーから、セキュリティ保護された通信を受け取ることを保証するものです。これらのイベントの順序は次のとおりです。

- OPS がマスターサーバー A との信頼を設定します。
- OPS がマスターサーバー B との信頼を設定します。
- OPS がマスターサーバー C との信頼を設定します。

Symantec OpsCenter が個々のマスターサーバーでアクションを実行するように設定される場合には、それぞれのマスターサーバーから Symantec OpsCenter Server (OPS) に対して信頼関係が設定される必要があります。これらのイベントの順序は次のとおりです。この場合、setuptrust コマンドが 6 回実行されます。

- マスターサーバー A が Symantec OpsCenter Server (OPS) との信頼を設定します。
- マスターサーバー B が Symantec OpsCenter Server (OPS) との信頼を設定します。
- マスターサーバー C が Symantec OpsCenter Server (OPS) との信頼を設定します。
- Symantec OpsCenter Server (OPS) がマスターサーバー A との信頼を設定します。
- Symantec OpsCenter Server (OPS) がマスターサーバー B との信頼を設定します。
- Symantec OpsCenter Server (OPS) がマスターサーバー C との信頼を設定します。

メモ: NetBackup 7.6 と OpsCenter 7.6 は、自動的に信頼を確立します。以前の NetBackup マスターサーバーの場合には、これらの setuptrust 操作を手動で実行することが必要になる場合があります。NetBackup マスターサーバー 7.6 のインストールの最後に、OpsCenter のホスト名に関する質問があります。それを使って、マスターサーバーは双方向の信頼の設定を開始できます。

---

setuptrust コマンドの詳細については、『NetBackup コマンドリファレンスガイド』を参照してください。p.173 の「setuptrust コマンドの使用」を参照してください。

setuptrust コマンドの使用

setuptrust コマンドは、信頼するブローカーに連絡し、その証明書や詳細を回線を介して取得して、提供された詳細が信頼できる場合に信頼のリポジトリに追加するために使用できます。セキュリティ管理者は、ルート証明書を配布するための次のセキュリティレベルの 1 つを構成できます。

- 高セキュリティ(2): 以前に信頼できないルートがピアから取得されている (つまり、同じシグネチャの証明書がこちらのトラストストアに存在しない) 場合、ユーザーはハッシュを検証するように求められます。
- 中セキュリティ(1): 確認を求めずに、最初の認証ブローカーが信頼されます。以降の認証ブローカーを信頼しようとすると、ユーザーは、証明書が信頼済みストアに追加される前に、ハッシュを検証するように求められます。

- 低セキュリティ(0):確認を求めずに、認証ブローカーの証明書は常に信頼されます。vssat CLI が認証サービスの 'bin' ディレクトリにあります。

setuptrust コマンドでは、次の構文を使います。

```
vssat setuptrust --broker <host[:port]> --securitylevel high
```

setuptrust コマンドでは、次の引数を使います。

重要な引数は、broker、host、port です。信頼するブローカーのホストとポートを指定します。認証の登録ポートは 2821 です。ブローカーが別のポート番号で構成されている場合には、セキュリティ管理者に情報を問い合わせてください。

マスターサーバーおよびメディアサーバーのホストプロパティへのアクセス

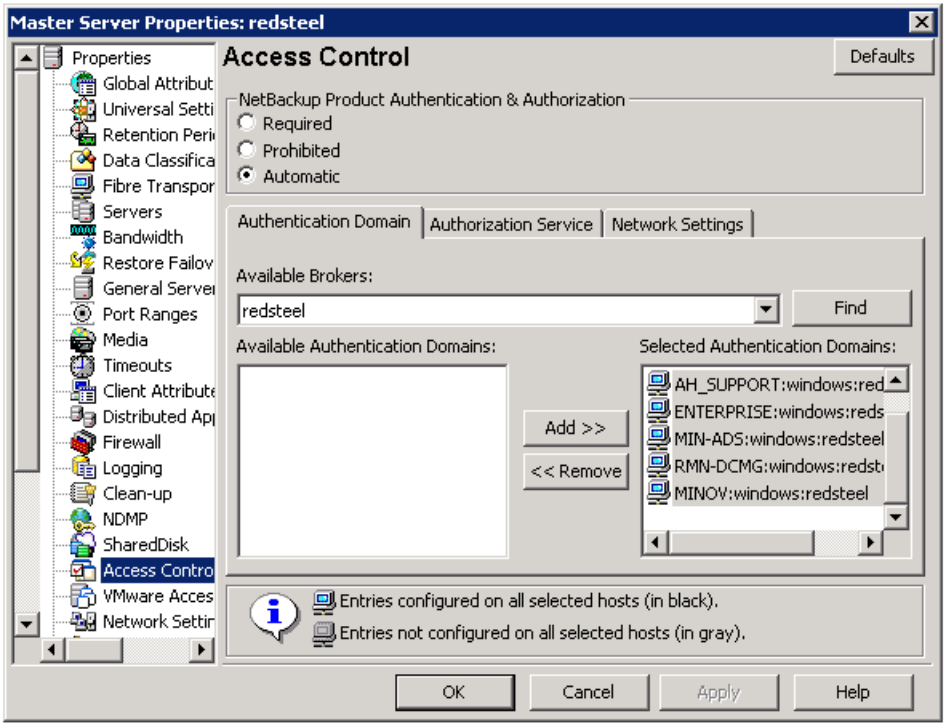
NetBackup 管理コンソールのマスターサーバーとメディアサーバーのホストプロパティにアクセスするには、[NetBackup の管理 (NetBackup Management)] > [ホストプロパティ (Host Properties)]*を展開し、マスターサーバーまたはメディアサーバーを選択して*[アクセス制御 (Access Control)]を選択します。

[アクセス制御 (Access Control)]ホストプロパティ

[必須 (Required)]か[自動 (Automatic)]に[NetBackup Product Authentication and Authorization]を設定します。[自動 (Automatic)]は、NBAC がまだ構成されていないホストが構成内に存在する場合を考慮した設定です。他の NetBackup システムとの通信時に、使用可能な接続のうちで最もセキュリティ保護された接続の使用が、サーバーによって試行されます。[自動 (Automatic)]設定は、すべてのクライアントおよびサーバーで NBAC が構成されるまで使用する必要があります。

図 6-1 に、[アクセス制御 (Access Control)]ホストプロパティダイアログボックスを示します。

図 6-1　［アクセス制御 (Access Control)］ホストプロパティダイアログボックス



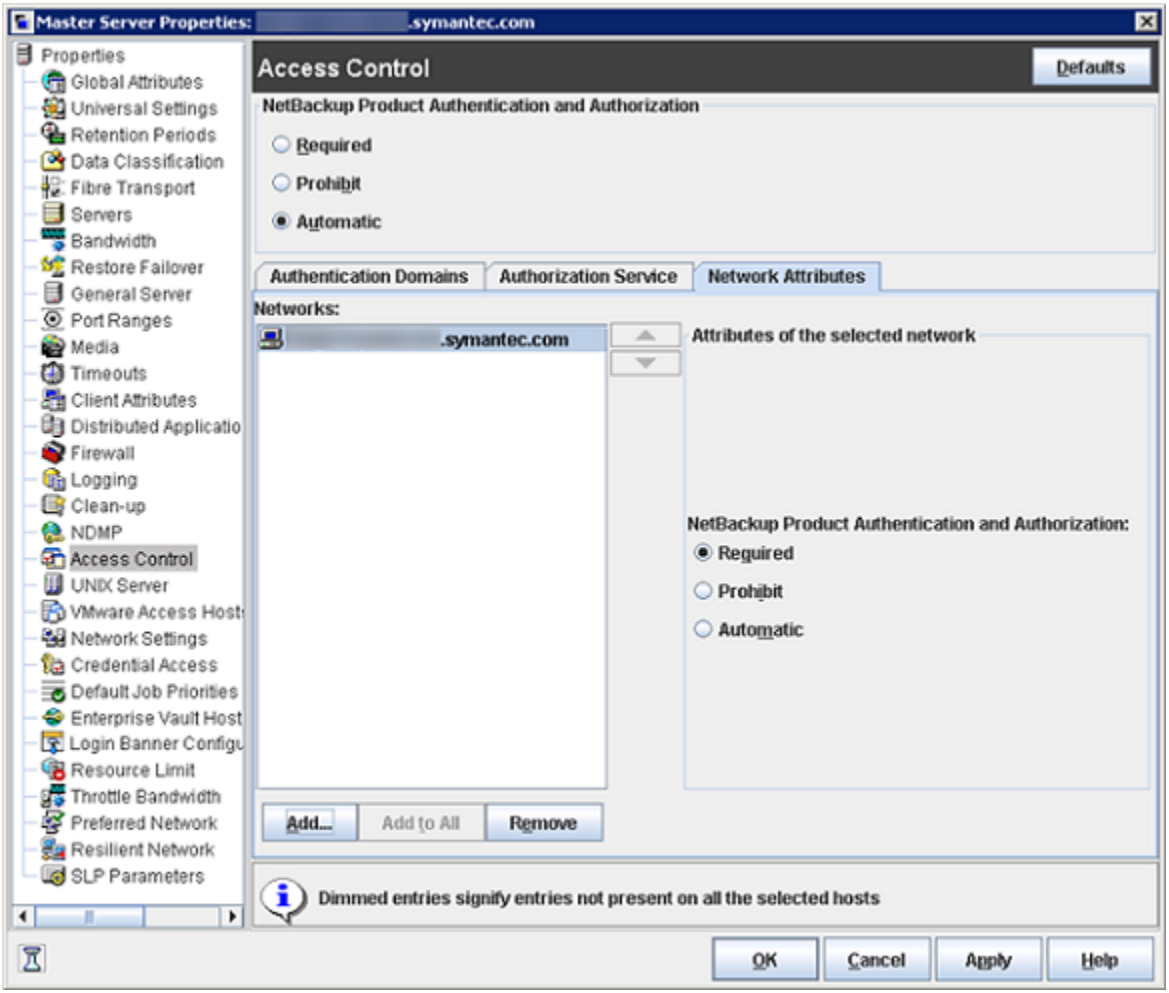
［自動 (Automatic)］を選択した場合、NetBackup Product Authentication and Authorization を使うために必要なコンピュータかドメインを指定できます。そうしない場合は、NetBackup Product Authentication and Authorization の使用が禁止されているコンピュータを指定できます。

［ネットワーク設定 (Network Settings)］タブ

［ネットワーク設定 (Network Settings)］タブで［アクセス制御 (Access Control)］ホストプロパティを表示します。［ネットワーク (Networks)］リストにマスターサーバーを追加します。それから、［NetBackup Product Authentication and Authorization］を［必須 (Required)］に設定します。

図 6-2 に［ネットワーク設定 (Network Settings)］タブを示します。

図 6-2　［ネットワーク設定 (Network Settings)］タブ



NetBackup マスターサーバーに追加した新しい NetBackup クライアントまたはメディアサーバー (バージョン 5.0 以上) ごとに、［アクセス制御 (Access Control)］プロパティを構成する必要があります。このプロパティは、各マシンとマスターサーバーの両方で構成します。この構成は、マスターサーバーのホストプロパティで行うことができます。

［認証ドメイン (Authentication Domain)］タブ

［認証ドメイン (Authentication Domain)］タブは、次の構成を行うために使用します。

- どの認証サーバーでどの認証機構がサポートされているか

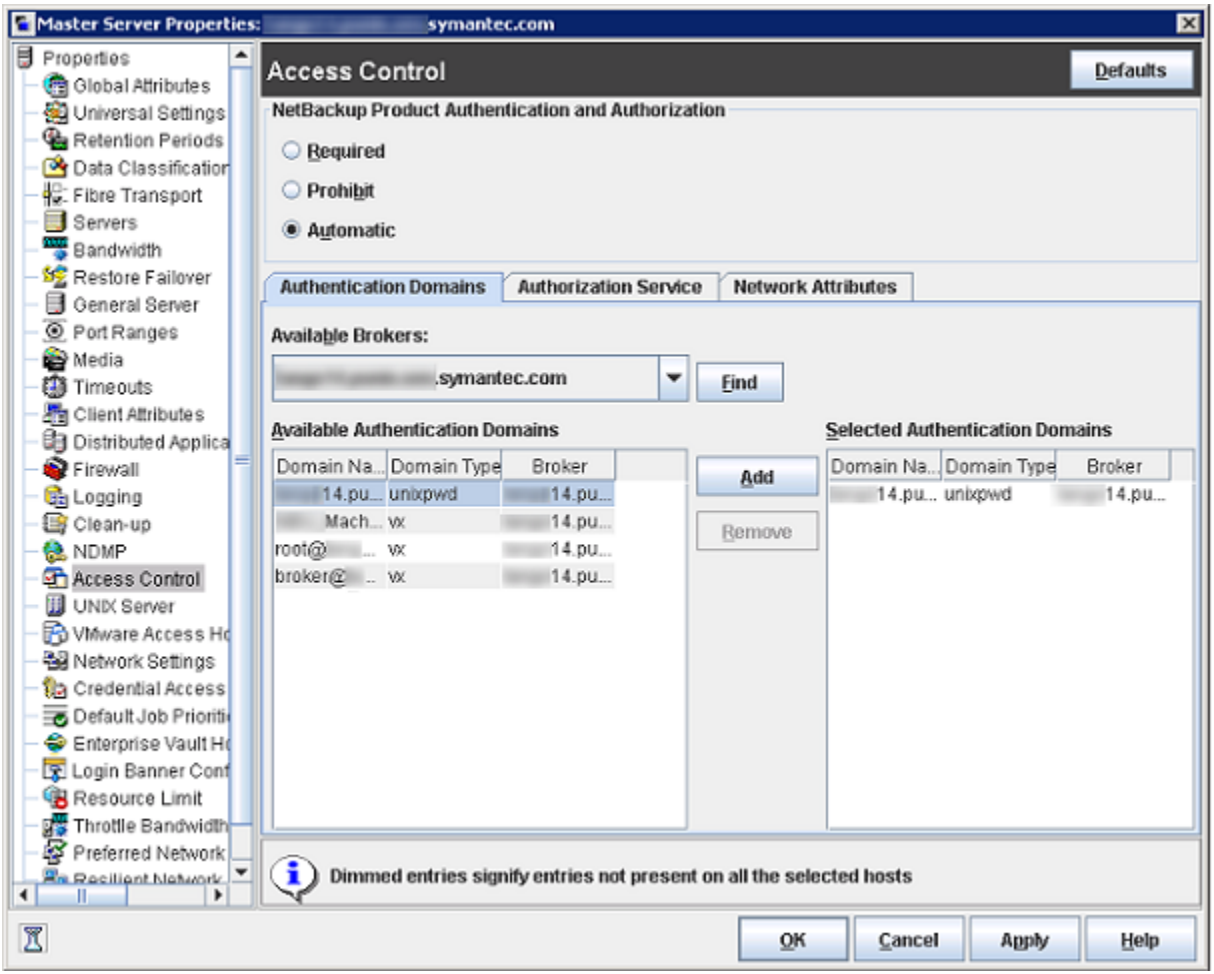
- 各ドメインで何をサポートしているか

認証するユーザーのドメインを追加します。

次の例は 6 つの認証ドメインを含んでいます。

図 6-3 に、［認証ドメイン (Authentication Domain)］タブを示します。

図 6-3　　［認証ドメイン (Authentication Domain)］タブ



メモ: UNIX の認証ドメインを使用する場合は、認証を行ったホストの完全修飾ドメイン名を入力します。

メモ: サポートされる認証形式は、NIS、NISPLUS、WINDOWS、vx、unixpwd です (デフォルトは unixpwd です)。

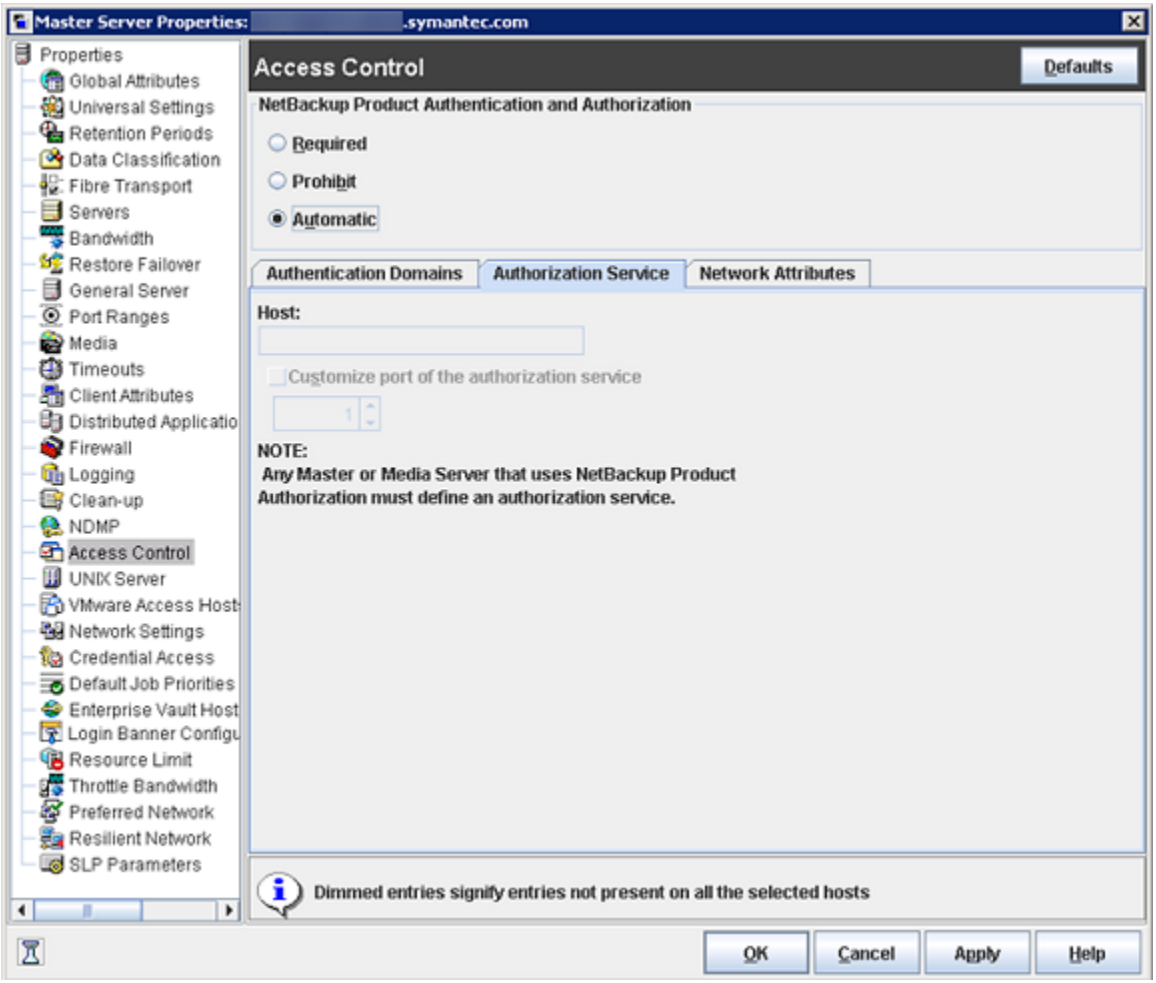
［認可サービス (Authorization Service)］タブ

メモ: このタブからは変更できません。このタブは読み取り専用です。

［アクセス制御 (Access Control)］ホストプロパティの［認可サービス (Authorization Service)］タブで、ホスト名を参照できます。この情報はすべて読み取り専用であるためグレー表示です。この画面への変更を行うことはできません。

図 6-4 に、［認可サービス (Authorization Service)］タブを示します。

図 6-4 ［認可サービス (Authorization Service)］タブ



クライアントのホストプロパティへのアクセス

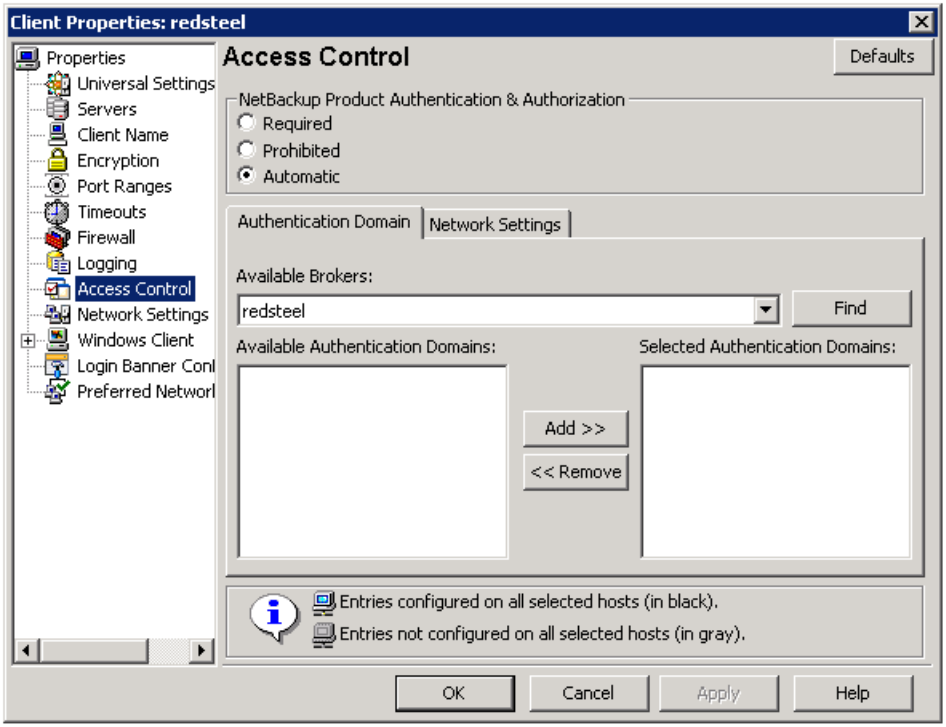
NetBackup 管理コンソールのクライアントのホストプロパティにアクセスするには、［NetBackup の管理 (NetBackup Management)］>［ホストプロパティ (Host Properties)］>［クライアント (Clients)］を展開し、クライアントを選択して［アクセス制御 (Access Control)］を選択します。

クライアントの［アクセス制御 (Access Control)］ホストプロパティダイアログボックス

ホストプロパティで NetBackup クライアントを選択します。(マスターサーバーの NetBackup 管理コンソールで、［NetBackup の管理 (NetBackup Management)］>［ホストプロパティ (Host Properties)］>［クライアント (Clients)］を展開してクライアントを選択し、［アクセス制御 (Access Control)］を選択します。)

次の図に、クライアントの［アクセス制御 (Access Control)］ホストプロパティを示します。

図 6-5　クライアントの［アクセス制御 (Access Control)］ホストプロパティ



［必須 (Required)］か［自動 (Automatic)］に［NetBackup Product Authentication and Authorization］を設定します。この例では、［自動 (Automatic)］が選択されています。

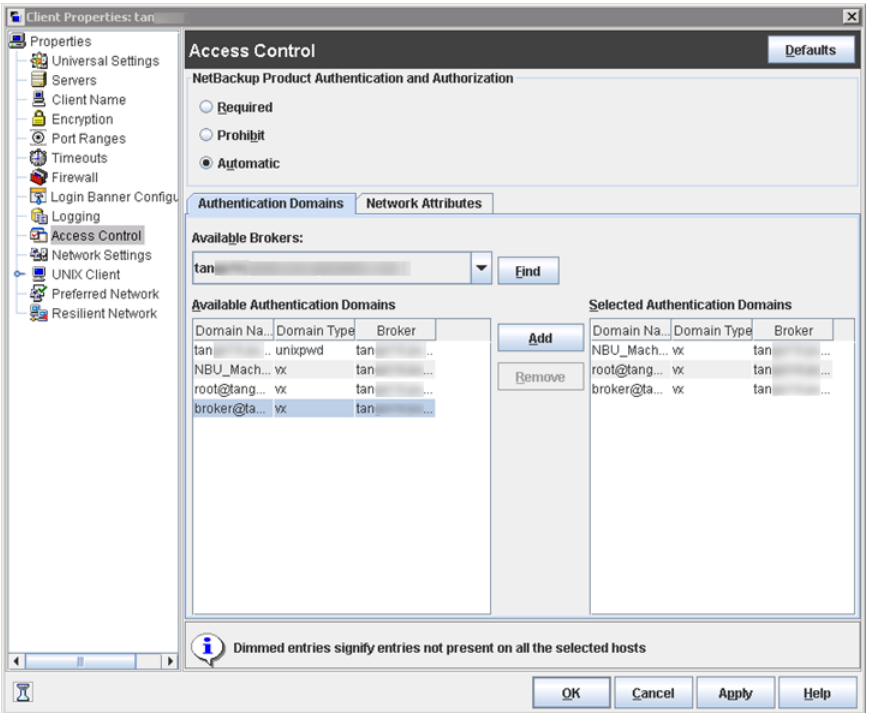
クライアントの［認証ドメイン (Authentication Domain)］タブ

ホストプロパティで NetBackup クライアントを選択します。このタブを使用して、コンピュータごとに NetBackup Product Authentication and Authorization の使用を要求または禁止することができます。通信を行う両方のシステムで、設定が一致している必要があります。

［アクセス制御 (Access Control)］ホストプロパティの［認証ドメイン (Authentication Domain)］タブで、クライアントで認証に使用できるドメインのリストを追加します。［検索 (Find)］をクリックすると、利用可能な認証ドメインのリストを取得できます。それから、選択した認証ドメインのリストを作成するために［追加 (Add)］をクリックします。

図 6-6 に［認証ドメイン (Authentication Domain)］タブと、選択した認証ドメインを示します。

図 6-6　クライアントの［認証ドメイン (Authentication Domain)］タブ

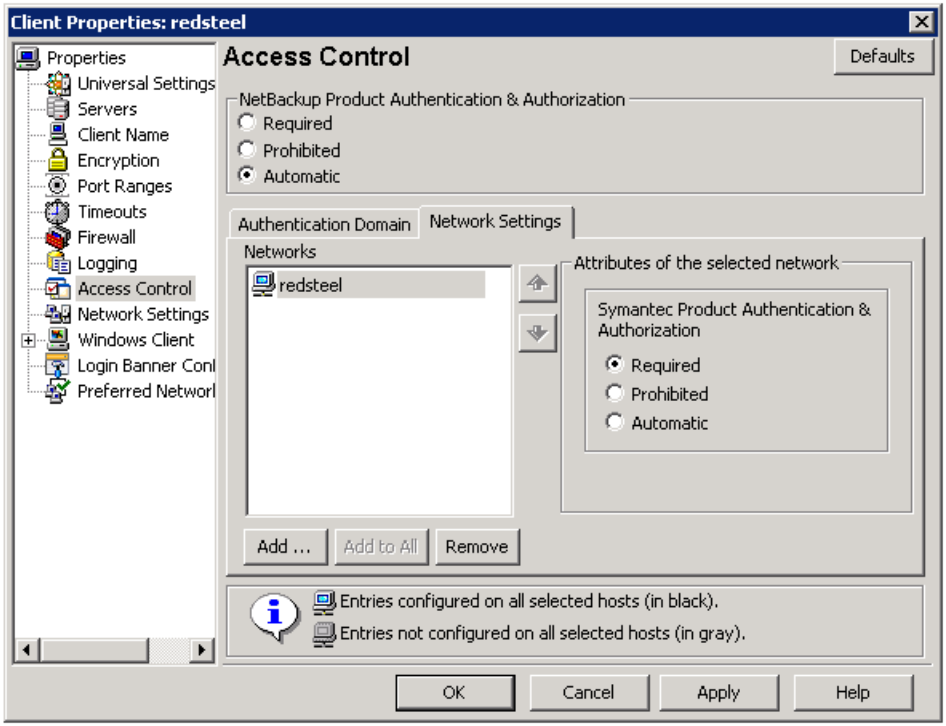


クライアントの［ネットワーク設定 (Network Settings)］タブ

［アクセス制御 (Access Control)］ホストプロパティの［ネットワーク設定 (Network Settings)］タブで、クライアントで認証に使用できるドメインのリストを追加します。

図 6-7 にクライアントの［ネットワーク設定 (Network Settings)］タブを示します。

図 6-7　クライアントの［ネットワーク設定 (Network Settings)］タブ



アクセス管理のトラブルシューティングのガイドライン

アクセス管理のトラブルシューティングし、特定の処理および機能が正しく行われているかどうかを判断する方法

p.183 の「NetBackup Authentication and Authorization の構成とトラブルシューティング」を参照してください。

検証項目には次のものが含まれます。

- Windows での検証項目

p.209 の「Windows での検証項目」を参照してください。

- UNIX での検証項目
  p.190 の「UNIX の検証手順について」を参照してください。
- UNIX マスターサーバーが存在する複合環境での検証項目
  p.198 の「UNIX マスターサーバーが存在する複合環境での検証項目」を参照してください。
- Windows マスターサーバーが存在する複合環境での検証項目
  p.203 の「Windows マスターサーバーが存在する複合環境での検証項目」を参照してください。

NetBackup Authentication and Authorization の構成とトラブルシューティング

次の表に、NetBackup Authentication and Authorization の構成とトラブルシューティングのトピックとヒントを示します。この表示には、いくつかの既知の問題についての情報とそれを解決するためのヒントも含んでいます。

表 6-4 NetBackup Authentication and Authorization の構成とトラブルシューティングのトピックとヒント

トピック	構成のヒント
マスターサーバー設定の検証	bpnbat -whoami を実行し、コンピュータのクレデンシャルを指定すると、ホストが登録されているドメイン、および証明書に示されているコンピュータの名前が表示されます。 `bpnbat -whoami -cf "c:¥program Files¥veritas¥netbackup¥var¥vxss¥credentials¥ master.company.com "Name: master.company.com Domain: NBU_Machines@master.company.com Issued by: /CN=broker/OU=root@master.company.com/O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Symantec Private Security Operation completed successfully.` 表示されたドメインが NBU_Machines@master.company.com でない場合、対象の名前 (master) に対して bpnbat -addmachine を実行することを検討してください。NBU_Machines ドメインとして機能するコンピュータ (master) でこのコマンドを実行します。 次に、クレデンシャルを配置するマシン上で、bpnbat -loginmachine コマンドを実行します。

トピック	構成のヒント

ルートクレデンシャルの設定	認証サーバーまたは認可サーバーのいずれかの設定で問題が発生し、アプリケーションでユーザーのクレデンシャルが root であるとエラー表示された場合は、root に対して $HOME 環境変数が正しく設定されていることを確認します。
	次のコマンドを実行して、現在の値を検出します。
	`echo $HOME`
	この値は root のホームディレクトリと一致する必要があります。このディレクトリは、通常、/etc/passwd ファイルに存在します。
	root に切り替える場合は、次のコマンドを実行します。
	`su -`
	この場合、su とだけ入力するのではなく、root 環境変数を正しく調整する必要があります。

期限切れのクレデンシャルメッセージ	クレデンシャルが期限切れであるか、または不正である場合、bpnbaz または bpnbat コマンドの実行時に、次のメッセージが表示されます。 `Supplied credential is expired or incorrect. Please reauthenticate and try again.` bpnbat -Login を実行して、期限切れのクレデンシャルを更新します。
有効なデバッグログ	次のログは、NetBackup アクセス制御のデバッグを行う場合に役立ちます。 マスター上: admin、bpcd、bprd、bpdbm、bpjobd、bpsched クライアント上: admin、bpcd アクセス制御: nbatd、nbazd. 適切なログ記録の手順については、『NetBackup トラブルシューティングガイド』を参照してください。
NetBackup の認証と認可の共有サービスのアンインストール	UNIX の場合: installics を使用して、認証および認可をアンインストールするオプションを選択します。アンインストール後に、次のディレクトリが空になります。 /opt/VRTSat および /opt/VRTSaz /etc/vx/vss /var/VRTSat and /var/VRTSaz Windows の場合: Windows の[コントロールパネル]から[アプリケーションの追加と削除]を使用して、認証および認可をアンインストールします。アンインストール後に、¥Veritas¥Security ディレクトリが空になります。

トピック	構成のヒント
PBX からの共有 AT の解除	NetBackup 7.5 がアップグレードされ、NBAC が以前の設定ですでに有効になっている場合は、古い共有 AT を PBX から解除する必要があります。 共有 AT を解除するには、次のコマンドを実行します。 UNIX プラットフォームでは、`/opt/VRTSat/bin/vssat setispbxexchflag --disable` を実行します。 Windows X86 では、`C:¥Program Files¥VERITAS¥Security¥Authentication¥bin¥vssat setispbxexchflag--disable` を実行します。 Windows X64 では、`C:¥Program Files(x86)¥VERITAS¥Security¥Authentication¥bin¥vssat setispbxexchflag--disable` を実行します。
クレデンシャルの格納場所	NetBackup Authentication and Authorization のクレデンシャルは次のディレクトリに格納されます。 UNIX の場合: ユーザーのクレデンシャル: `$HOME/.vxss` コンピュータのクレデンシャル: `/usr/openv/var/vxss/credentials/` Windows の場合: <user_home_dir>¥Application Data¥VERITAS¥VSS
システム時間がアクセス制御に与える影響	クレデンシャルには、作成時間と終了時間が含まれます。コンピュータ間でシステム時間が大きく異なっていると、クレデンシャルが未来に作成されたものと見なされたり、実際よりも早く期限切れと見なされます。システム間の通信で問題が発生した場合は、システム時間の同期化を検討してください。

トピック	構成のヒント

NetBackup Authentication and Authorization のポート	NetBackup Authentication and Authorization デーモンサービスは旧バージョンのメディアサーバーとクライアントにポート 13783 番と 13722 番を使います。7.5 以降のバージョンには PBX 接続を使います。
	次のコマンドで、プロセスが待機していることを確認できます。
	認証:
	UNIX の場合
	`netstat -an | grep 13783`
	Windows の場合
	`netstat -a -n | find "13783"`
	認可:
	UNIX の場合
	`netstat -an | grep 13722`
	Windows の場合
	`netstat -a -n | find "13722"`

共有サービスの NetBackup の認証および認可デーモンの停止	NetBackup Authentication and Authorization Service を停止する場合は、認可を最初に停止し、その後認証を停止します。
	UNIX の場合、次のコマンドを使用します。
	認可を停止する場合、次の例に示すように、TERM シグナルを送信します。
	`# ps -fed |grep nbazd`
	`root 17018 1 4 08:47:35 ? 0:01 ./nbazd`
	`root 17019 16011 0 08:47:39 pts/2 0:00 grep nbazd`
	`# kill 17018`
	認証を停止する場合、次の例に示すように、TERM シグナルを送信します。
	`# ps -fed |grep nbatd`
	`root 16018 1 4 08:47:35 ? 0:01 ./nbatd`
	`root 16019 16011 0 08:47:39 pts/2 0:00 grep nbatd`
	`# kill 16018`
	Windows の場合
	これらのサービスは NetBackup アクティビティモニターに表示されないため、Windows の[サービス]ユーティリティを使用します。

トピック	構成のヒント
NetBackup にアクセスできない場合	アクセス制御が正しく構成されていないと、NetBackup 管理コンソールにアクセスできない場合があります。 アクセスできない場合は、vi を使って bp.conf エントリを参照するか（UNIX）、または regedit を使って次の場所の Windows レジストリを参照します（Windows）。 HKEY_LOCAL_MACHINE¥Software¥Veritas¥NetBackup¥CurrentVersion¥config AUTHORIZATION_SERVICE、AUTHENTICATION_DOMAIN および USE_VXSS エントリが正しく設定されているかどうかを確認します。 管理者は、NetBackup アクセス制御の使用を好まない場合や認可ライブラリをインストールしていないことがあります。USE_VXSS エントリが[**禁止** (Prohibited)]に設定されているか完全に削除されていることを確認します。
メディアサーバーのストレージユニットのバックアップが NBAC 環境で実行されない	NetBackup ドメインのシステム (マスターサーバー、メディアサーバー、またはクライアント) のホスト名と bp.conf ファイルで指定するホスト名は、同じである必要があります。
nbac_cron ユーティリティの使用	nbac_cron.exe ユーティリティを使用して、cron または at ジョブを実行する際の識別情報を作成します。 nbac_cron ユーティリティについての詳細 p.220 の「nbac_cron ユーティリティについて」を参照してください。 nbac_cron.exe は、次の場所に存在します。 UNIX の場合、/opt/openv/netbackup/bin/goodies/nbac_cron Windows の場合、*Install_path*¥Veritas¥netbackup¥bin¥goodies¥nbac_cron.exe nbac_cron ユーティリティの使用についての詳細 p.220 の「nbac_cron ユーティリティの使用」を参照してください。
Windows でのリカバリ後の NBAC の有効化	Windows でリカバリ後に手動で NBAC を有効にするには次の手順を使います。 ■ AUTHENTICATION_DOMAIN、AUTHORIZATION_SERVICE、USE_VXSS エントリをレジストリに追加します。 ■ NetBackup Authentication and Authorization サービスのサービスの種類を AUTOMATIC に変更します。 ■ NetBackup サービスを再起動します。 ■ nbatd および nbazd サービスが実行されていることを検証します。 **メモ:** クラスタで bpclusterutil -enableSvc nbatd および bpclusterutil -enable nbazd コマンドを実行します。

トピック	構成のヒント
クラスタインストールで setupmaster が失敗する	構成ファイルが共有ディスクにあるクラスタインストールの場合には setupmaster が失敗することがある既知の問題があります。
共有セキュリティサービス (vxatd または vxazd) がマスターサーバーとともにクラスタ化されている場合のクラスタの既知の問題	共有セキュリティサービス(vxatd または vxazd)がマスターサーバーとともにクラスタ化されている場合にクラスタに既知の問題があります。bpnbaz -SetupMaster コマンドを実行し、セキュリティ (NBAC) を設定するときに、該当する場合は共有セキュリティサービスのサービスグループを永続的にフリーズするか、サービスをオフラインにします (ただし、共有ディスクはオンラインであることを確認します)。その後、setupmaster コマンドを実行します。
bp.conf ファイルのすべての AUTHENTICATION_DOMAIN エントリが認証ブローカーとしてマスターサーバー仮想名で更新される、NBAC に関するクラスタ化されたマスターサーバーアップグレードの既知の問題	bp.confNファイルのすべての AUTHENTICATION_DOMAI エントリが認証ブローカーとしてマスターサーバー仮想名で更新される、NBAC に関するクラスタ化されたマスターサーバーアップグレードの既知の問題があります。マスターサーバー以外の異なる認証ブローカーを示す任意のドメインエントリがある (また、マスターサーバーはそのドメインをサービスしない) 場合は、そのエントリは手動で bp.conf ファイルから削除される必要があります。
nbazd が Solaris x64 でエラーを表示して失敗する既知の問題	nbazd が Solaris x64 で次のエラーを表示して失敗する既知の問題があります。 ld.so.1: nbazd: fatal: relocation error: R_AMD64_PC32: file /usr/lib/64/libCrun.so.1: symbol __1cH__CimplMex_terminate6F_v_: value 0x28001a4b2ba does not fit 問題を解決するにはパッチ 119964-* をインストールします。
Windows 2003 のデュアルスタックコンピュータの既知の問題	Windows 2003 のデュアルスタックコンピュータの既知の問題があります。http://support.microsoft.com/ からの Microsoft 社のパッチ kb/928646 が必要です。
アクセス制御エラーと短いホスト名および長いホスト名に関する既知の問題	アクセス制御に関するエラーを含む既知の問題があります。短いホスト名と長いホスト名を解決することができ、同じ IP アドレスに解決されるかを調べてください。
ブローカーのプロファイルで ClusterName が AT の仮想名に設定されている場合の NBAC に関するクラスタアップグレードの既知の問題	ブローカーのプロファイルで ClusterName が AT の仮想名に設定されている場合の NBAC に関するクラスタアップグレードの既知の問題があります。これは組み込みのブローカーにそのまま移行されます。組み込みのブローカーはプロファイルで UseClusterNameAsBrokerName が 1 に設定されています。ブローカーのドメインマップに要求が送られると、共有 AT の仮想名をブローカー名として使用します。bpnbaz -GetDomainInfosFromAuthBroker は何も戻しません。アップグレードでは、bp.conf ファイルが NetBackup 仮想名を持つように更新されます。

トピック	構成のヒント
エラーが発生する可能性のある bpcd の複数インスタンスの既知の問題	bpnbaz -SetupMedia コマンドで、bprd が AT_LOGINMACHINE_RQST プロトコルを使用して宛先フィールドの bpcd と通信する既知の問題があります。bpcd の新しいインスタンスが起動されます。コマンドは、完了後に char アレイを通常のポインタとして解放することを試行し、bpcd によってクライアント側にコアダンプを発生させる場合があります。この bpcd インスタンスは一時的に作成されて正常に終了するため、機能は損なわれないはずです。親 bpcd には影響しません。
共有ドライブの構成ファイルと共有 AT を使用するクラスタに関する既知の問題	共有ドライブの構成ファイルと共有 AT を使用するクラスタに関する既知の問題があります。共有サービスの解除は、この共有ドライブがアクセス可能であるノードでのみ有効になります。解除は残りのノードでは失敗します。つまり、管理を行う bpnbaz -SetupMaster を実行している間は、リモートブローカーの個々の操作が失敗します。手動でパッシブノードを構成する必要があります。各パッシブノードで bpnbaz -SetupMedia を実行します。
NBAZDB をサポートするデータベースユーティリティに関する既知の問題	あるデータベースユーティリティが NBAZDB をサポートし、他のデータベースユーティリティはサポートしない既知の問題があります。 データベースユーティリティ nbdb_backup、nbdb_move、nbdb_ping、nbdb_restore、nbdb_admin は NBAZDB をサポートします。 ユーティリティ nbdb_unload と dbadm は NBAZDB をサポートしません。

NBAC の問題のトラブルシューティング

次の表は NBAC に関連する問題とソリューションをリストしたものです。

表 6-5 NBAC の問題

問題と原因	解決方法
ユーザー主導のバックアップまたはリストアに失敗します ユーザー主導のバックアップまたはリストアに自動モードの NBAC で失敗します。バックアップ、アーカイブおよびリストアインターフェースは、NBAC が構成されている場合、Windows インターフェースに一部のエラーを表示します。 NBAC で UNIXマスターサーバーの NetBackup の設定し、最初にインターフェースを設定せずに Windows インターフェースでこのような設定を行う場合は、バックアップまたはリストアに失敗することがあります。その他の原因として、ホームディレクトリに期限切れの証明書があることが考えられます。	設定をサポートするために Windows インターフェースを構成してください。 Active Directory のドメインからユーザーを認証するには、認証ブローカーとして機能する Microsoft Windows システムが 1 つ以上存在する必要があります。 Windows インターフェースを構成し、Active Directory の既存ユーザーを活用して、主に UNIX/Linux プラットフォーム上の NetBackup 環境を管理、操作、または使用するための手順については、TECH199281 を参照してください。 設定を正しく構成した後、bpnbat -logout コマンドを実行し、インターフェースを再起動する前に設定からログアウトしてください。

問題と原因	解決方法
認証エラーが 116 で発生しました (Authentication failure with error 116) ターゲットホストで NBAC を設定する際に、**エラー** `116-VxSS` **認証** `(error 116-VxSS authentication)` で認証が失敗します。	NBAC 認証が正しく構成され、ターゲットホストの有効で使用可能なクレデンシャルがあることを確認してください。
NBU_Operator グループの非管理ユーザーがアクセス管理の使用を試みた際にエラーが発生しました (Error when a non-admin user from the NBU_Operator group tries to use Access Management) 非管理ユーザーが NBU_Operator グループに追加されました。読み込み、表示、構成権限は、ホストプロパティの構成権限と共に割り当てられます。ただし、ユーザーがアクセス管理ユーティリティを開こうとすると、エラーが表示されます。	NBU_Operator グループのユーザーの権限は制限されています。 ユーザーがアクセス管理ユーティリティを使用するには、異なる権限が必要です。必要な権限を取得するには、NBU_Security_Admin グループにユーザーを追加してください。 ユーザーグループのについての詳細 p.225 の「NetBackup のデフォルトユーザーグループ」を参照してください。
認可ファイル (auth.conf) 機能は、NBAC 対応の環境では役に立ちません。デフォルトでは、auth.confファイルは非 NBAC 環境の Java インターフェースのみでサポートされます。	NBAC 対応環境で auth.conf ファイルを機能させるには、`nbgetconfig` コマンドと `nbsetconfig` コマンドを使用して `USE_AUTH_CONF_NBAC` エントリを Windows レジストリに追加するか、または bp.conf ファイルを UNIX に追加します。エントリは次のように `YES` に設定する必要があります。 `USE_AUTH_CONF_NBAC = YES` auth.conf ファイルについて詳しくは、『NetBackup 管理者ガイド Vol. 1』を参照してください。

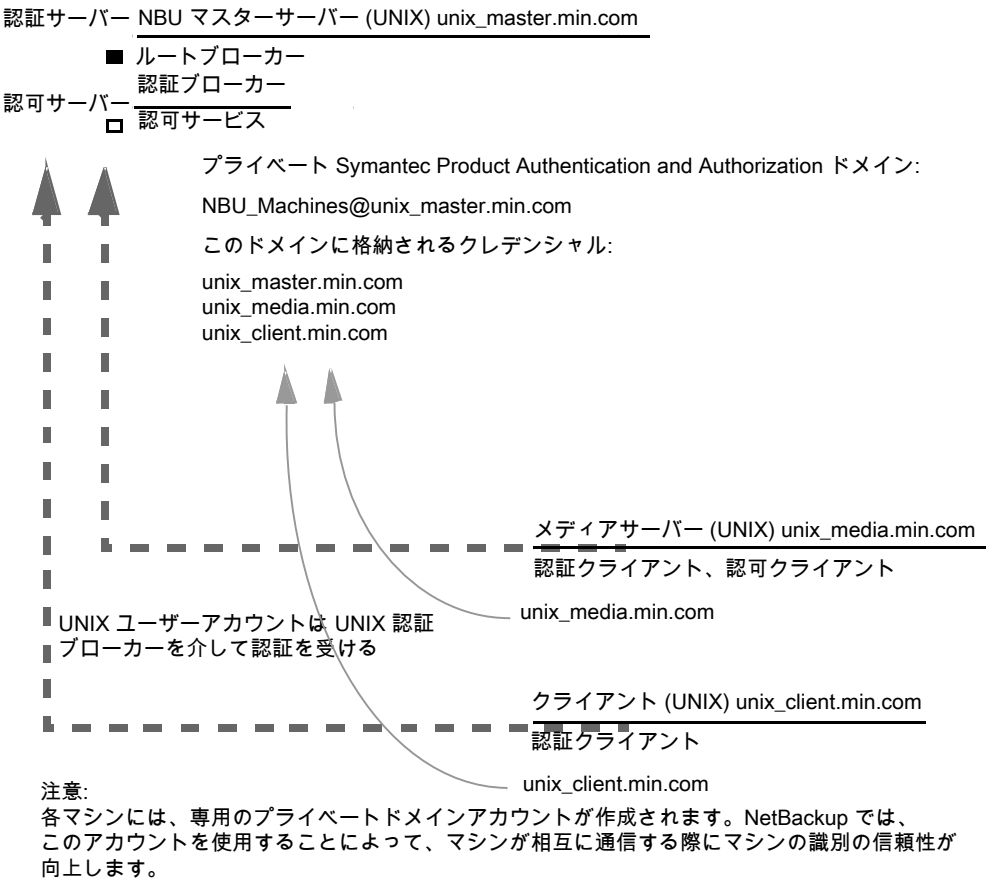
UNIX の検証手順について

次の手順 (および 次の図) を使用して、UNIX マスターサーバー、メディアサーバーおよびクライアントでアクセス制御が正しく構成されていることを確認します。

- UNIX マスターサーバーの検証
  p.191 の「UNIX マスターサーバーの検証」を参照してください。
- UNIX メディアサーバーの検証
  p.194 の「UNIX メディアサーバーの検証」を参照してください。
- UNIX クライアントの検証
  p.196 の「UNIX クライアントの検証」を参照してください。

次の例は UNIX システムのみを含む構成例を示したものです。

図 6-8　UNIX システムだけが存在する構成の例



UNIX マスターサーバーの検証

UNIX マスターサーバーを検証するには次の手順を使います。

- UNIX マスターサーバー設定を検証します。
- 認可の照合が許可されているコンピュータを検証します。
- データベースが正しく構成されていることを検証します。
- `nbatd` および `nbazd` プロセスが実行されていることを検証します。
- ホストプロパティが正しく構成されていることを検証します。

次の表に、UNIX マスターサーバーの検証プロセスを示します。

表 6-6 UNIX マスターサーバーの検証プロセス

プロセス	説明
UNIX マスターサーバー設定の検証	ホストが登録されているドメイン (プライマリ認証ブローカーが存在する場所)、および証明書に示されているコンピュータの名前を判断します。bpnbat に -whoami およびマスターサーバーのクレデンシャルファイルを指定する -cf を指定して実行します。サーバークレデンシャルは /usr/openv/var/vxss/credentials/ ディレクトリに存在します。 例: bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_master.company.com Name: unix_master.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@unix_master/O=vx Expiry Date: Oct 31 15:44:30 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@unix_master.company.com でない場合、またはファイルが存在しない場合、対象の名前 (unix_master) に対して bpnbat -addmachine を実行することを検討してください。NBU_Machines ドメインとして機能するコンピュータ (unix_master) でこのコマンドを実行します。 次に、証明書を配置するコンピュータ (unix_master) 上で、コマンド bpnbat -loginmachine を実行します。 **メモ:** クレデンシャルの期限が切れているかどうかを判断する場合、有効期限がローカル時間ではなく GMT で表示されることに注意してください。 **メモ:** この検証の残りの手順では、コンソールウィンドウからコマンドを実行することを想定しています。このコンソールウィンドウから、対象のユーザー識別情報で NBU_Security Admin のメンバーである識別情報を使用して bpnbat -login が実行されています。この識別情報は、通常、セキュリティが設定された最初の識別情報です。
認証ブローカーに存在するコンピュータの検証	認証ブローカーに存在するコンピュータを検証するには、管理者グループのメンバーでログオンし、次のコマンドを実行します。 bpnbat -ShowMachines 実行されているコンピュータが次のコマンドで表示されます。 bpnbat -AddMachine

プロセス	説明

認可の照合が許可されているコンピュータの検証	認可の照合を実行可能なコンピュータを検証するには、認可ブローカーで root ユーザーとしてログオンし、次のコマンドを実行します。
	
	`bpnbaz -ShowAuthorizers`
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_master.company.com`
	`Name: unix_master.company.com`
	
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_master.company.com`
	`Name: unix_media.company.com`
	
	`Operation completed successfully.`
	
	このコマンドを実行すると、unix_master および unix_media が認可を照合する権限を所有していることが示されます。両方のサーバーが、同じ vx (Veritas プライベートドメイン) ドメイン NBU_Machines@unix_master.company.com に対して認証されていることに注意してください。
	
	認可済みコンピュータのリストにマスターサーバーまたはメディアサーバーが表示されない場合、`bpnbaz -allowauthorization <server_name>` を実行して、表示されていないコンピュータを追加します。

データベースが正しく構成されていることの検証	データベースが正しく構成されていることを検証するには、`bpnbaz -listgroups` を実行します。
	
	`bpnbaz -listgroups`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	グループが表示されない場合または `bpnbaz -listmainobjects` を実行してもデータが戻されない場合は、`bpnbaz -SetupSecurity` を実行します。

プロセス	説明

nbatd および nbazd プロセスが実行されていることの検証	ps コマンドを実行して、指定したホスト上で nbatd および nbazd プロセスが実行されていることを確認します。必要に応じて、これらのプロセスを起動します。
	例:
	`ps -fed |grep vx`
	`root 10716 1 0 Dec 14 ? 0:02 /usr/openv/netbackup/bin/private/nbatd`
	`root 10721 1 0 Dec 14 ? 4:17 /usr/openv/netbackup/bin/private/nbazd`

ホストプロパティが正しく構成されていることの検証	[アクセス制御 (Access Control)]ホストプロパティで、[NetBackup Product Authentication and Authorization]プロパティが正しく設定されていることを検証します。この設定は、すべてのコンピュータが NetBackup Authentication and Authorization を使うかどうかによって[自動 (Automatic)]または[必須 (Required)]のいずれかにする必要があります。すべてのコンピュータで NetBackup Authentication and Authorization が使用されているわけではない場合は、[自動 (Automatic)]に設定します。
	[アクセス制御 (Access Control)]ホストプロパティで、リスト内の認証ドメインの綴りが正しいことを確認します。また、ドメインが適切なサーバー (有効な認証ブローカー) を示していることを確認します。すべてのドメインが UNIX ベースである場合、ドメインは、認証ブローカーを実行している UNIX マシンを示している必要があります。
	また、このプロセスは、cat を使用して bp.conf で確認することもできます。
	`cat bp.conf`
	`SERVER = unix_master`
	`SERVER = unix_media`
	`CLIENT_NAME = unix_master`
	`AUTHENTICATION_DOMAIN = company.com "default company NIS namespace"`
	`NIS unix_master 0`
	`AUTHENTICATION_DOMAIN = unix_master "unix_master password file"`
	`PASSWD unix_master 0`
	`AUTHORIZATION_SERVICE = unix_master.company.com 0`
	`USE_VXSS = AUTOMATIC`
	`#`

UNIX メディアサーバーの検証

UNIX メディアサーバーを検証するには次を実行します。

- メディアサーバーを検証します。
- サーバーが認可データベースにアクセスできることを検証します。
- ライブラリメッセージをロードできないことを理解します。

次の表に、UNIX メディアサーバーの検証手順を示します。

表 6-7 UNIX メディアサーバーの検証プロセス

プロセス	説明
メディアサーバーの検証	bpnbat -whoami にメディアサーバーのクレデンシャルファイルを指定する -cf を指定して実行し、メディアサーバーを認証する認証ブローカーを判断します。サーバークレデンシャルは /usr/openv/var/vxss/credentials/ ディレクトリに存在します。 例: bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_media.company.com Name: unix_media.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@unix_master.company.com/ O=vx Expiry Date: Oct 31 14:48:08 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@unix_master.company.com でない場合、対象の名前 (unix_media) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (unix_master) で実行します。 次に、証明書を配置するコンピュータ (unix_master) 上で、bpnbat -loginmachine を実行します。
サーバーが認可データベースにアクセスできることの検証	bpnbaz -ListGroups "machine_credential_file" を実行して、メディアサーバーが必要に応じて認可データベースにアクセスできることを確認します。 "machine_credential_file" 例: bpnbaz -ListGroups -CredFile /usr/openv/var/vxss/credentials/unix_media.company.com NBU_User NBU_Operator NBU_Admin NBU_Security Admin Vault_Operator Operation completed successfully. このコマンドが失敗した場合、認可ブローカーであるマスターサーバー (unix_master) 上で bpnbaz -AllowAuthorization を実行します。root または管理者で実行する必要があることに注意してください。

プロセス	説明
ライブラリメッセージをロードできない場合	メディアサーバーを検証します。また、メディアサーバーが適切なデータベースにアクセスできることを検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを間接的に確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合、認証および認可クライアントライブラリがインストールされていることを確認します。 また、認証ドメインが正しいことを検証することもできます。これを検証するには、このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示するか、`bp.conf` ファイルの内容を `cat` コマンドで確認します。

UNIX クライアントの検証

次の手順が UNIX クライアントを検証するために使われます。

- UNIX クライアントのクレデンシャルを検証します。
- 認証クライアントライブラリがインストールされているを検証します。
- 正しい認証ドメインを検証します。

次の表に、UNIX クライアントの検証手順を示します。

表 6-8 UNIX クライアントの検証手順

手順	説明

UNIX クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。
	例:
	`bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_client.company.com`
	`Name: unix_client.company.com`
	`Domain: NBU_Machines@unix_master.company.com`
	`Issued by: /CN=broker/OU=root@unix_master.company.com/O=vx`
	`Expiry Date: Oct 31 14:49:00 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	表示されたドメインが NBU_Machines@unix_master.company.com でない場合、対象の名前 (unix_client) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (unix_master) で実行します。
	次に、証明書を配置するコンピュータ(unix_client) 上で、コマンド bpnbat -loginmachine を実行します。

認証クライアントライブラリがインストールされていることの検証	クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。
	`bpnbat -login`
	`Authentication Broker: unix_master.company.com`
	`Authentication port [Enter = default]:`
	`Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd): NIS`
	`Domain: min.com`
	`Name: Smith`
	`Password:`
	`Operation completed successfully.`

手順	説明

正しい認証ドメインの検証	[アクセス制御 (Access Control)]ホストプロパティで、または cat (1) を使用して、クライアントのすべての定義済み認証ドメインが正しいことを確認します。ドメインの綴りが正しいことを確認します。また、各ドメインに一覧表示された認証ブローカーがそのドメイン形式に対して有効であることを確認します。
	また、このプロセスは、cat (1) を使用して bp.conf で確認することもできます。
	`cat bp.conf`
	`SERVER = unix_master`
	`SERVER = unix_media`
	`CLIENT_NAME = unix_master`
	`AUTHENTICATION_DOMAIN = min.com "default company NIS namespace"`
	`NIS unix_master 0`
	`AUTHENTICATION_DOMAIN = unix_master.company.com "unix_master password file" PASSWD unix_master 0`
	`AUTHORIZATION_SERVICE = unix_master.company.com 0`
	`USE_VXSS = AUTOMATIC`

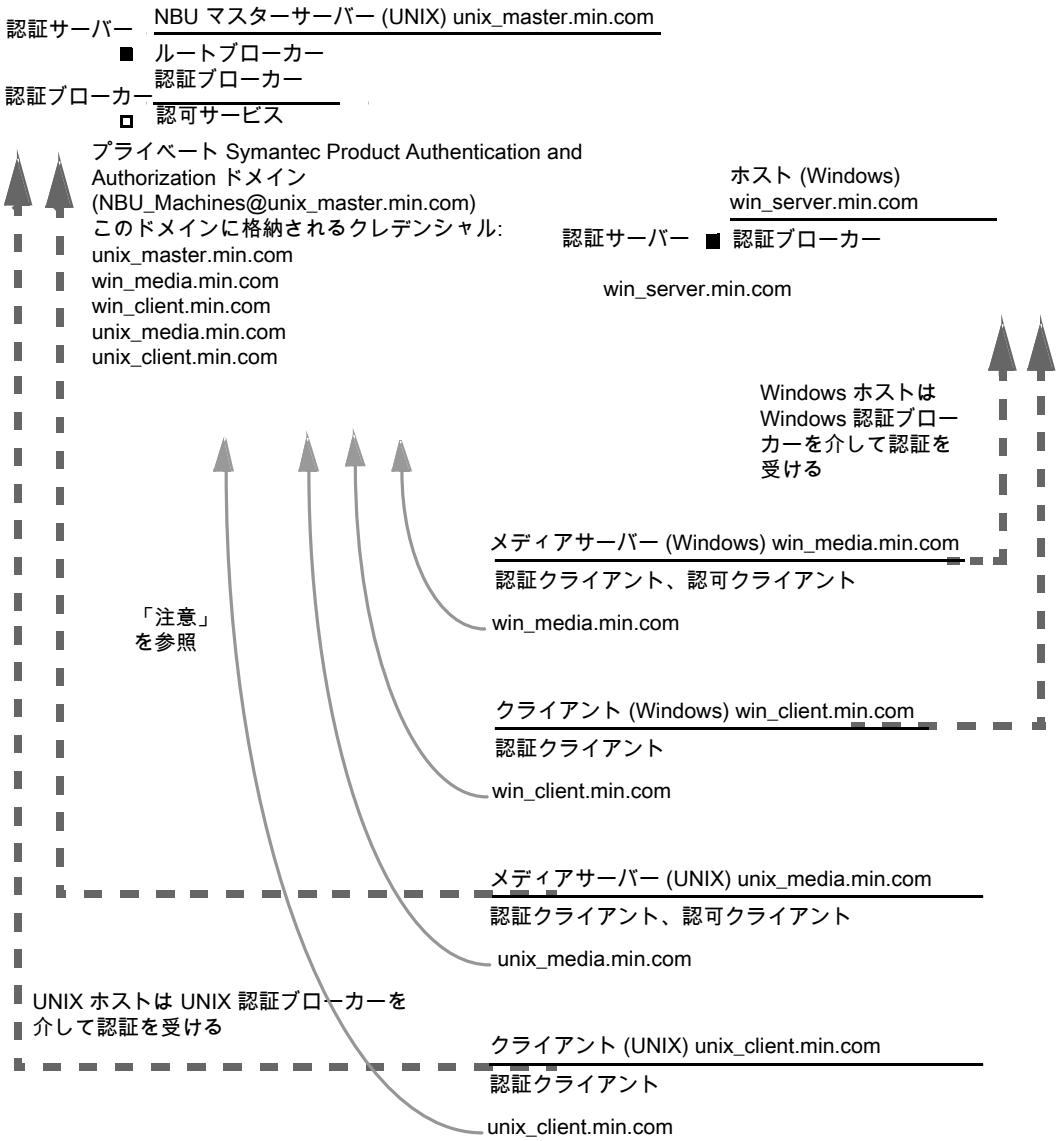
UNIX マスターサーバーが存在する複合環境での検証項目

次の手順は、マスターサーバー、メディアサーバーおよびクライアントが正しく構成されていることを確認するのに役立ちます。これらのマシンは、異機種間で NetBackup アクセス制御を使用する環境用に構成されている必要があります。マスターサーバーは UNIX マシンです。

- 複合環境の UNIX マスターサーバーのマスターサーバーでの検証項目
- 複合環境の UNIX マスターサーバーのメディアサーバーでの検証項目
- 複合環境の UNIX マスターサーバーのクライアントでの検証項目

図 6-9に、UNIX マスターサーバーが存在する複合構成の例を示します。

図 6-9　UNIX マスターサーバーが存在する複合構成の例



注意:
各マシンには、プライベートドメインアカウントがあります。NetBackup では、このアカウントを使用することによって、マシンが相互に通信する際にマシンの識別の信頼性が向上します。

複合環境の UNIX マスターサーバーのマスターサーバーでの検証項目

UNIX マスターサーバーの検証手順については、次の項を参照してください。

p.191 の「UNIX マスターサーバーの検証」を参照してください。

複合環境の UNIX マスターサーバーのメディアサーバーでの検証項目

次の表に、複合環境の UNIX マスターサーバーのメディアサーバーでの検証手順を示します。

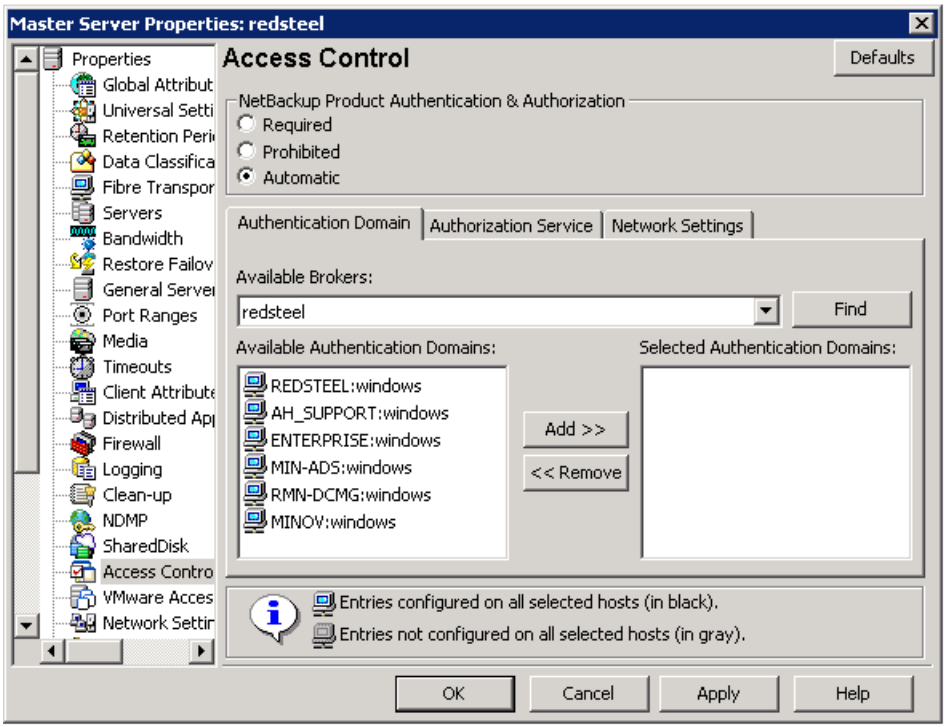
表 6-9　複合環境の UNIX マスターサーバーの検証手順

手順	説明
UNIX メディアサーバーの検証	UNIX メディアサーバーの検証手順については、次の項を参照してください。 p.194 の「UNIX メディアサーバーの検証」を参照してください。

Windows メディアサーバーの検証	コンピュータの証明書が、UNIX マスターサーバー (unix_master) に存在するルート認証ブローカーから取得されていることを確認します。
	表示されない証明書がある場合、次のコマンドを実行して問題を解決します。
	■ `bpnbat -addmachine` ルート認証ブローカー上で実行します。(この例では、unix_master です。)
	■ `bpnbat -loginmachine` (この例では、win_media です。)
	例:
	`bpnbat -whoami -cf "C:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_media.company.com"`
	`Name: win_media.company.com`
	`Domain: NBU_Machines@unix_master.company.com`
	`Issued by: /CN=broker/OU=root@ unix_master.company.com/O=vx`
	`Expiry Date: Oct 31 20:11:04 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

手順	説明
認可の照合が許可されているメディアサーバーの検証	bpnbaz -listgroups -CredFile を実行して、メディアサーバーが認可の確認を実行できることを確認します。 例: bpnbaz -listgroups -CredFile "C:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_media.company.com" NBU_User NBU_Operator NBU_Admin NBU_Security Admin Vault_Operator Operation completed successfully. メディアサーバーの認可の確認が許可されていない場合、マスターサーバー上で、対象のメディアサーバー名に対して bpnbaz -allowauthorization を実行します。
ライブラリメッセージをロードできない場合	Windows メディアサーバーを検証します。また、Windows メディアサーバーで認可の確認が行えることを間接的に検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合、認証クライアントライブラリおよび認可クライアントライブラリがインストールされていることを確認します。
認証ドメインの検証	このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示することによって、認証ドメインが正しいことを検証します。 また、regedit (または regedit32) をメディアサーバー上で使用して次の場所で直接確認できます。 HKEY_LOCAL_MACHINE¥Software¥Veritas¥NetBackup¥ CurrentVersion¥config¥AUTHENTICATION_DOMAIN
クロスプラットフォームの認証ドメイン	複合環境では、適切なドメイン形式が正しい認証ブローカーを指していることを特に注意して確認してください。 [認証ドメイン (Authentication Domain)]タブの例は、Windows ブローカーに追加できる利用可能な Windows の認証ドメインを示します。この場合、システムが両方とも Windows ベースであるため、複合環境ではありません。Windows ドメインと UNIX ドメインの組み合わせがある場合は、ブローカーを最も有用な認証ドメインに合わせることが重要です。 プラットフォームを最も有用な認証ドメインに一致させる方法の表示については、図 6-10

図 6-10　クロスプラットフォームの認証ドメイン



複合環境の UNIX マスターサーバーのクライアントでの検証項目

UNIX クライアントコンピュータを検証する手順については、次の項を参照してください。

p.196 の「UNIX クライアントの検証」を参照してください。

次の表に、Windows クライアントを検証する手順を示します。

表 6-10 Windows クライアントを検証する手順

手順	説明
Windows クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。 例: bpnbat -whoami -cf "c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_client.company.com Name: win_client.company.com Domain: NBU_Machines@unix_master.company.com Issued by: /CN=broker/OU=root@unix_master.company.com/ O=vx Expiry Date: Oct 31 19:50:50 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.
認証クライアントライブラリがインストールされていることの検証	クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。 例: bpnbat -login Authentication Broker: unix_master.company.com Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : NIS Domain: min.com Name: Smith Password: Operation completed successfully.
Windows 認証ブローカーの検証	Windows 認証ブローカーが UNIX のメイン認証ブローカーとの相互信頼関係を確立していることを確認します。また、このブローカーが UNIX ブローカーをルートブローカーとして使用していることを確認します。

Windows マスターサーバーが存在する複合環境での検証項目

次の手順は、マスターサーバー、メディアサーバーおよびクライアントが正しく構成されていることを確認するのに役立ちます。これらのマシンは、異機種間で NetBackup アクセ

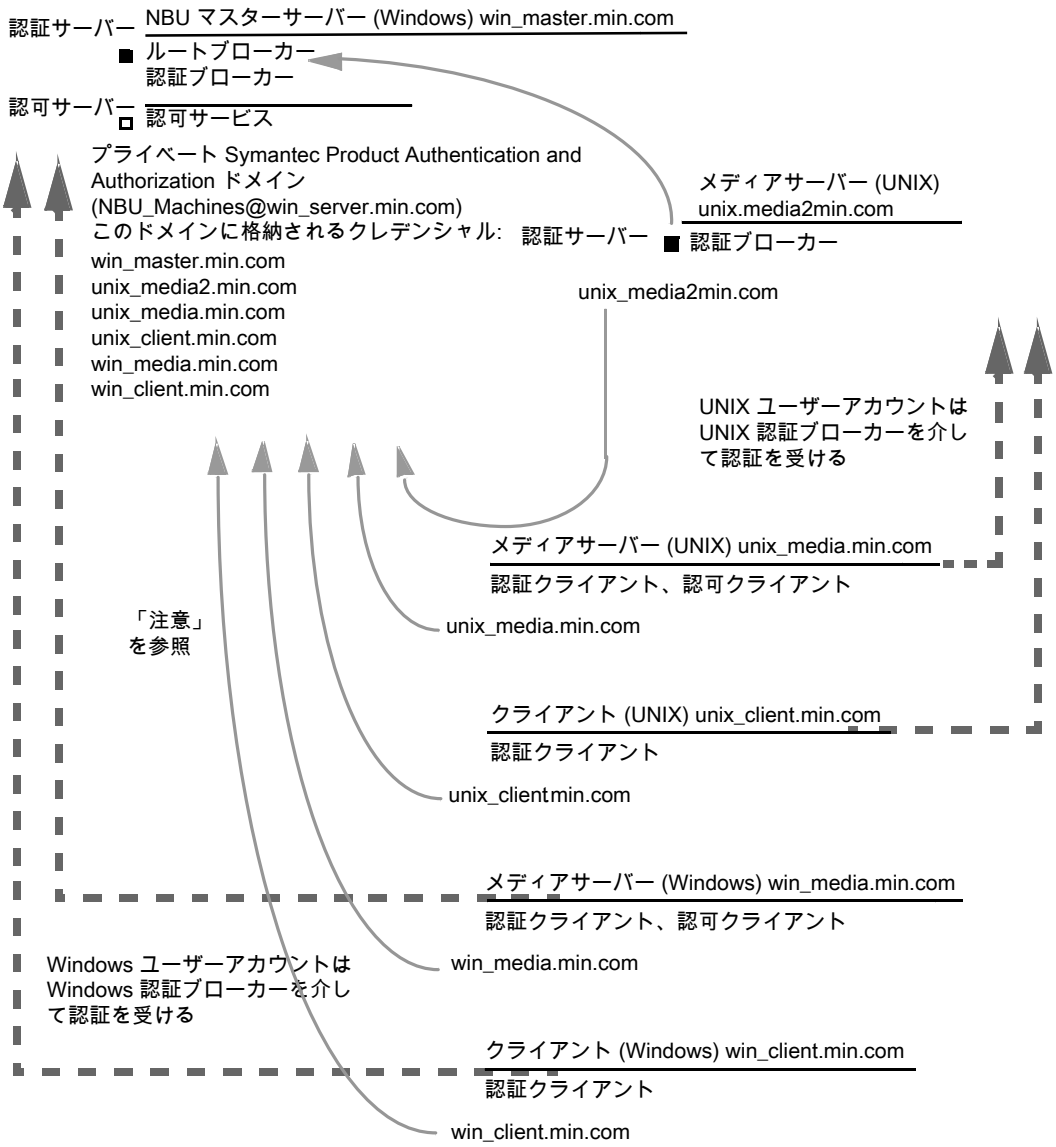
ス制御を使用する環境用に構成する必要があります。マスターサーバーは Windows コンピュータです。

- 複合環境の Windows マスターサーバーのマスターサーバーでの検証項目
  p.206 の「複合環境の Windows マスターサーバーのマスターサーバーでの検証項目」を参照してください。
- 複合環境の Windows マスターサーバーのメディアサーバーでの検証項目
  p.206 の「複合環境の Windows マスターサーバーのメディアサーバーでの検証項目」を参照してください。
- 複合環境の Windows マスターサーバーのクライアントでの検証項目

p.208 の「複合環境の Windows マスターサーバーのクライアントでの検証項目」を参照してください。

図 6-11に、Windows マスターサーバーを含む構成の例を示します。

図 6-11　Windows マスターサーバーが存在する複合構成の例



注意:
各マシンには、プライベートドメインアカウントがあります。NetBackup では、このアカウントを使用することによって、マシンが相互に通信する際にマシンの識別の信頼性が向上します。

複合環境の Windows マスターサーバーのマスターサーバーでの検証項目

複合環境の Windows マスターの検証手順については、次の項を参照してください。

p.211 の「Windows マスターサーバーでの検証項目」を参照してください。

複合環境の Windows マスターサーバーのメディアサーバーでの検証項目

次の表に、複合環境の Windows マスターサーバーのメディアサーバーでの検証手順を示します。

表 6-11　複合環境の Windows マスターサーバーのメディアサーバーでの検証手順

手順	説明
複合環境の Windows マスターサーバーの Windows メディアサーバーでの検証	Windows メディアサーバーの検証手順については、次の項を参照してください。 p.215 の「Windows メディアサーバーでの検証項目」を参照してください。

UNIX メディアサーバーの検証	コンピュータの証明書が、Windows マスターサーバー (win_master) に存在するルート認証ブローカーから発行されていることを確認します。bpnbat -whoami にメディアサーバーのクレデンシャルファイルを指定する -cf を指定して実行し、メディアサーバーを認証する認証ブローカーを判断します。
	例:
	`bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_media.company.com`
	`Name: unix_media.company.comDomain: NBU_Machines@ win_master.company.com`
	`Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx`
	`Expiry Date: Oct 31 14:48:08 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

手順	説明
サーバーが認可データベースにアクセスできることの検証	メディアサーバーが認可データベースにアクセスできることを確認するには、認可の確認を行う必要があります。bpnbaz -ListGroups -CredFile "*/usr/openv/var/vxss/credentials/<hostname>*"を実行します。 例: bpnbaz -ListGroups -CredFile¥ /usr/openv/var/vxss/credentials/unix_media.company.com NBU_Operator NBU_AdminNBU_SAN Admin NBU_UserNBU_Security Admin Vault_Operator Operation completed successfully. メディアサーバーの認可の確認が許可されていない場合、マスターサーバー上で、対象のメディアサーバー名に対して bpnbaz -allowauthorization を実行します。
ライブラリメッセージをロードできない場合	メディアサーバーを検証します。また、メディアサーバーが適切なデータベースにアクセスできることを間接的に検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合は、認証クライアントライブラリおよび認可クライアントライブラリがインストールされていることを確認します。

手順	説明

クロスプラットフォームの認証ドメイン	また、このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示することによって、認証ドメインが正しいことを検証することもできます。または、bp.conf ファイルの内容を cat(1) コマンドで確認して検証することもできます。
	複合環境では、適切なドメイン形式が正しい認証ブローカーを指していることを特に注意して確認してください。
	次の例では、PASSWD ドメインおよび NIS ドメインが unix_media2.company.com (この例における UNIX 認証ブローカー) を指しています。
	`cat bp.conf`
	`SERVER = win_master.company.com`
	`MEDIA_SERVER = unix_media.company.com`
	`MEDIA_SERVER = unix_media2.company.com`
	`CLIENT_NAME = unix_media`
	`AUTHENTICATION_DOMAIN = win_master "win_master domain" WINDOWS win_master.company.com 0`
	`AUTHENTICATION_DOMAIN = enterprise "enterprise domain" WINDOWS win_master.company.com 0`
	`AUTHENTICATION_DOMAIN = unix_media2.company.com "local unix_media2 domain" PASSWD unix_media2.company.com 0`
	`AUTHENTICATION_DOMAIN = min.com "NIS domain" NIS unix_media.company.com 0`
	`AUTHORIZATION_SERVICE = win_master.company.com 0`
	`USE_VXSS = AUTOMATIC`

複合環境の Windows マスターサーバーのクライアントでの検証項目

次の表に、複合環境の Windows マスターサーバーのクライアントでの検証手順を示します。

表 6-12　複合環境の Windows マスターサーバーの検証手順

手順	説明
Windows クライアントのクレデンシャルの検証	Windows クライアントの検証手順については、次の項を参照してください。 p.217 の「Windows クライアントでの検証項目」を参照してください。

手順	説明

UNIX クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。
	例:
	`bpnbat -whoami -cf ¥`
	`"/usr/openv/var/vxss/credentials/`
	`unix_client.company.com"`
	`Name: unix_client.company.com`
	`Domain: NBU_Machines@win_master.company.com`
	`Issued by: /CN=broker/OU=root@`
	`win_master.company.com/O=vx`
	`Expiry Date: Oct 31 21:16:01 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

認証クライアントライブラリがインストールされていることの検証	クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。
	`bpnbat -login`
	`Authentication Broker: unix_media2.company.com`
	`Authentication port [Enter = default]:`
	`Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd)`
	`: NIS`
	`Domain: min.com`
	`Name: Smith`
	`Password:`
	`You do not currently trust the server:`
	`unix_media.company.com, do`
	`you wish to tr`
	`ust it? (y/n):`
	`y`
	`Operation completed successfully.`

UNIX 認証ブローカーの検証	UNIX の認証ブローカーが、メイン Windows 認証ブローカーとの相互信頼関係を確立していること、またはルートブローカーとして Windows ブローカーを使用していることを確認します。

Windows での検証項目

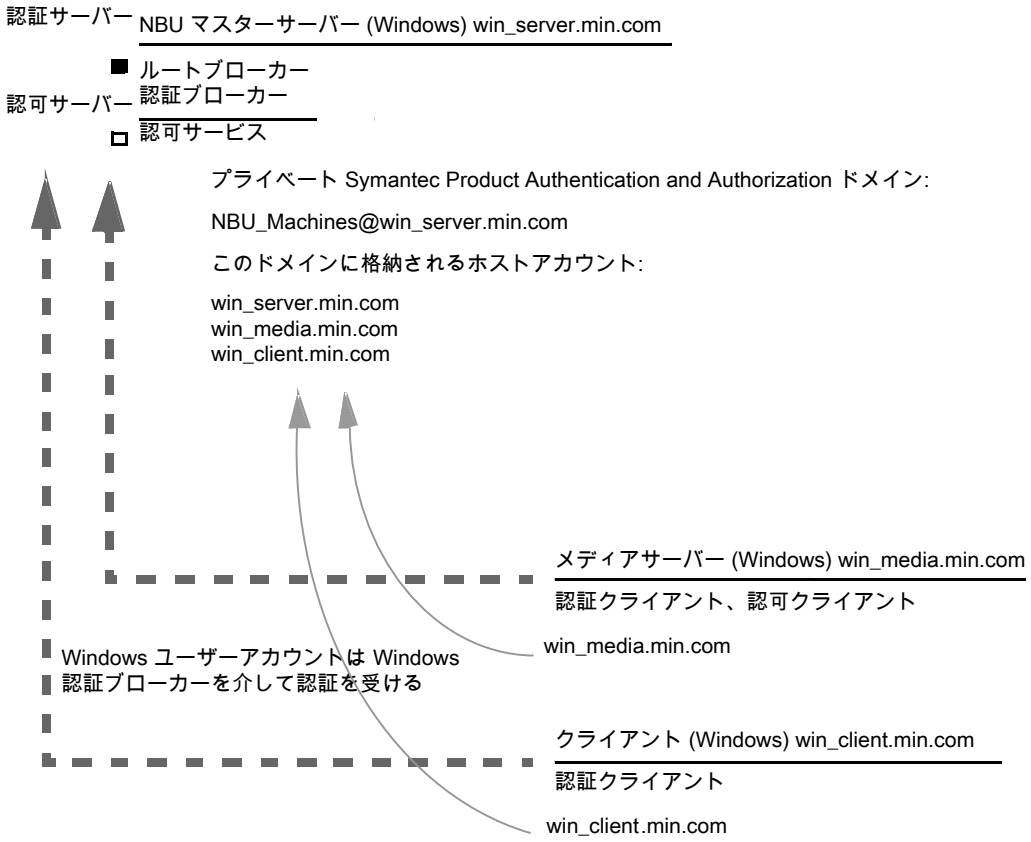
次の構成手順は、マスターサーバー、メディアサーバーおよびクライアントでアクセス制御が正しく構成されていることを確認するのに役立ちます。

Windows での検証項目には次のものが含まれます。

- p.211 の「Windows マスターサーバーでの検証項目」を参照してください。
- p.215 の「Windows メディアサーバーでの検証項目」を参照してください。
- p.217 の「Windows クライアントでの検証項目」を参照してください。

図 6-12 に、Windows システムだけが存在する構成の例を示します。

図 6-12 Windows システムだけが存在する構成の例



注意:
各マシンには、専用のプライベートドメインアカウントが作成されます。NetBackup では、このアカウントを使用することによって、マシンが相互に通信する際にマシンの識別の信頼性が向上します。

Windows マスターサーバーでの検証項目

この項では、次の手順について説明します。

- Windows マスターサーバー設定を検証します。
- 認可の照合が許可されているコンピュータを検証します。
- データベースが正しく構成されていることを検証します。
- nbatd および nbazd プロセスが実行されていることを検証します。
- ホストプロパティが正しく構成されていることを検証します。

次の表に、Windows マスターサーバーでの検証手順を示します。

表 6-13 Windows マスターサーバーでの検証手順

手順	説明
Windows マスターサーバー設定の検証	ホストが登録されているドメイン (プライマリ認証ブローカーが存在する場所) を判断できます。または、証明書に示されているコンピュータの名前を判別することもできます。bpnbat に -whoami を指定して実行し、ホストのクレデンシャルファイルを指定します。サーバークレデンシャルは、c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥... ディレクトリに存在します。 例: bpnbat -whoami -cf "c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_master" Name: win_master.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@win_master.company.com でない場合、対象の名前 (win_master) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (win_master) で実行します。 次に、証明書を配置するコンピュータ (win_master) 上で、次のコマンドを実行します。 bpnbat -loginmachine **メモ:** ユーザーのクレデンシャルの期限を判断する場合、有効期限がローカル時間ではなく GMT で表示されることに注意してください。 **メモ:** この検証の残りの手順では、コンソールウィンドウからコマンドを実行することを想定しています。また、そのウィンドウから、対象のユーザー識別情報で bpnbat -login が実行されていることを想定しています。このユーザーは、NBU_Security Admin のメンバーであると識別されます。この識別情報は、通常、セキュリティが設定された最初の識別情報です。

手順	説明
認証ブローカーに存在するコンピュータの検証	認証ブローカーに存在するコンピュータを検証するには、管理者グループのメンバーでログオンし、次のコマンドを実行します。 `bpnbat -ShowMachines` このコマンドを実行すると、`bpnbat -AddMachine` を実行したコンピュータが示されます。 **メモ:** ホストがリストに表示されない場合、マスターから `bpnbat -AddMachine` を実行します。その後、対象のホストから `bpnbat -loginMachine` を実行します。

認可の照合が許可されているコンピュータの検証	認可の照合が許可されているコンピュータを検証するには、管理者グループのメンバーでログオンし、次のコマンドを実行します。
	
	`bpnbaz -ShowAuthorizers`
	
	このコマンドを実行すると、win_master および win_media (マスターサーバーおよびメディアサーバー) が認可を照合する権限を所有していることが示されます。両方のサーバーが、同じプライベートドメイン (ドメイン形式 vx)、NBU_Machines@win_master.company.com に対して認証されていることに注意してください。
	
	メモ: このコマンドは、ローカル管理者または `root` ユーザーで実行します。ローカル管理者は、NBU_Security Admin ユーザーグループのメンバーである必要があります。
	
	`bpnbaz -ShowAuthorizers`
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@win_master.company.com`
	`Name: win_master.company.com`
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@win_master.company.com`
	`Name: win_media.company.com`
	`Operation completed successfully.`
	
	認可済みコンピュータのリストにマスターサーバーまたはメディアサーバーが表示されない場合、`bpnbaz -allowauthorization server_name` を実行して、表示されていないコンピュータを追加します。

手順	説明
データベースが正しく構成されていることの検証	データベースが正しく構成されていることを検証するには、bpnbaz -listgroups を実行します。 bpnbaz -listgroups NBU_Operator NBU_Admin NBU_SAN Admin NBU_User NBU_Security Admin Vault_Operator Operation completed successfully. グループが表示されない場合または bpnbaz -listmainobjects を実行してもデータが戻されない場合は、bpnbaz -SetupSecurity の実行が必要になる場合があります。
nbatd および nbazd プロセスが実行されていることの検証	Windows のタスクマネージャを使用して、指定したホスト上で nbatd.exe および nbazd.exe が実行されていることを確認します。必要に応じて、これらのプロセスを起動します。
ホストプロパティが正しく構成されていることの検証	[アクセス制御 (Access Control)]ホストプロパティで、[NetBackup Product Authentication and Authorization]プロパティが正しく設定されていることを検証します。この設定は、すべてのコンピュータが NetBackup Authentication and Authorization を使うかどうかによって[自動 (Automatic)]または[必須 (Required)]のいずれかにする必要があります。すべてのコンピュータで NetBackup Authentication and Authorization が使用されているわけではない場合は、[自動 (Automatic)]に設定します。 また、ホストプロパティは、次のレジストリで USE_VXSS を参照して確認することもできます。 HKEY_LOCAL_MACHINE¥Software¥Veritas¥NetBackup¥CurrentVersion¥config. 図 6-13に、[認証 (Authentication)]ドメインタブのホストプロパティの設定例を示します。 [アクセス制御 (Access Control)]ホストプロパティで、表示された認証ドメインの綴りが正しいこと、およびドメインが適切なサーバー (有効な認証ブローカー) を示していることを確認します。すべてのドメインが Windows ベースである場合、ドメインは、認証ブローカーを実行している Windows コンピュータを示している必要があります。

次の図に、[認証 (Authentication)]ドメインタブのホストプロパティの設定を示します。

図 6-13　　ホストプロパティの設定

Name	Type	Data
(Default)	REG_SZ	(value not set)
AUTHORIZATION_SERVICE	REG_SZ	redsteel 0
Browser	REG_SZ	redsteel
Client_Name	REG_SZ	redsteel
EMMPORT	REG_DWORD	0x00000614 (1556)
EMMSERVER	REG_SZ	redsteel
Exclude	REG_MULTI_SZ	C:\Program Files\Veritas\NetBackup\bin*.lock C:\Prog...
HOST_CACHE_TTL	REG_DWORD	0x00000e10 (3600)
IP_ADDRESS_FAMILY	REG_SZ	AF_UNSPEC
Port_BPCD	REG_DWORD	0x000035d6 (13782)
Port_BPRD	REG_DWORD	0x00003598 (13720)
Server	REG_MULTI_SZ	redsteel
USE_VXSS	REG_SZ	AUTOMATIC
VXDBMS_NB_CONF	REG_SZ	C:\Program Files\Veritas\NetbackupDB\conf
VXDBMS_NB_DATA	REG_SZ	C:\Program Files\Veritas\NetBackupDB\data
VXSS_NETWORK	REG_MULTI_SZ	redsteel REQUIRED
VXSS_SERVICE_TYPE	REG_SZ	INTEGRITYANDCONFIDENTIALITY

Windows メディアサーバーでの検証項目

この項では、次の Windows メディアサーバーでの検証手順について説明します。

- メディアサーバーを検証します。
- サーバーが認可データベースにアクセスできることを検証します。
- ライブラリメッセージをロードできない場合

次の表に、Windows メディアサーバーでの検証手順を示します。

表 6-14 Windows メディアサーバーでの検証手順

手順	説明
メディアサーバーの検証	bpnbat -whoami にメディアサーバーのクレデンシャルファイルを指定する -cf を指定して実行し、メディアサーバーを認証する認証ブローカーを判断します。サーバークレデンシャルは、c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥... ディレクトリに存在します。 例: bpnbat -whoami -cf "c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_media.company.com" Name: win_media.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx Expiry Date: Oct 31 20:11:40 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@win_master.company.com でない場合、対象の名前 (win_media) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (win_master) で実行します。 次に、証明書を配置するコンピュータ (win_media) 上で、次のコマンドを実行します。 bpnbat -loginmachine

手順	説明

サーバーが認可データベースにアクセスできることの検証	`bpnbaz -ListGroups -CredFile "machine_credential_file"` を実行して、メディアサーバーが必要に応じて認可データベースにアクセスできることを確認します。
	例:
	`bpnbaz -ListGroups -CredFile "C:¥Program Files¥Veritas¥NetBackup¥var¥vxss¥credentials¥ win_media.company.com"`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	このコマンドが失敗した場合、認可ブローカーであるマスターサーバー (win_master.company.com) 上で `bpnbaz -AllowAuthorization` を実行します。

ライブラリメッセージをロードできない場合	メディアサーバーを検証します。また、メディアサーバーが適切なデータベースにアクセスできることを検証します。この検証によって、認証および認可の両方の NetBackup Authentication and Authorization のクライアントライブラリが正しくインストールされていることを間接的に確認できます。ライブラリをロードできないことを示すメッセージが表示され、前述のいずれかの手順が失敗した場合は、認証クライアントライブラリおよび認可クライアントライブラリがインストールされていることを確認します。 また、このメディアサーバーの[アクセス制御 (Access Control)]ホストプロパティを表示することによって、認証ドメインが正しいことを検証することもできます。

Windows クライアントでの検証項目

この項では、次の Windows クライアントでの検証手順を説明します。

- クライアントのクレデンシャルを検証します。
- 認証クライアントライブラリがインストールされているを検証します。
- 正しい認証ドメインを検証します。

次の表に、Windows クライアントでの検証手順を示します。

表 6-15 Windows クライアントでの検証手順

手順	説明
クライアントのクレデンシャルの検証	クライアントのクレデンシャルが、正しいクライアント用であること、および正しいドメインから取得されていることを確認します。bpnbat -whoami にクライアントのクレデンシャルファイルを指定する -cf を指定して実行します。 例: bpnbat -whoami -cf "c:¥Program Files¥Veritas¥Netbackup¥var¥vxss¥credentials¥ win_client.company.com " Name: win_client.company.com Domain: NBU_Machines@win_master.company.com Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx Expiry Date: Oct 31 20:11:45 2007 GMT Authentication method: Veritas Private Security Operation completed successfully. 表示されたドメインが NBU_Machines@win_master.company.com でない場合、対象の名前 (win_client) に対して bpnbat -addmachine を実行することを検討してください。このコマンドは、NBU_Machines ドメインとして機能する認証ブローカーのコンピュータ (win_master) で実行します。 次に、証明書を配置するコンピュータ (win_client) 上で、コマンド bpnbat -loginmachine を実行します。
認証クライアントライブラリがインストールされていることの検証	**メモ:** クライアントで bpnbat -login を実行して、認証クライアントライブラリがインストールされていることを確認します。 bpnbat -login Authentication Broker: win_master Authentication port [Enter = default]: Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : WINDOWS Domain: ENTERPRISE Name: Smith Password:Operation completed successfully. ライブラリがインストールされていない場合は、NetBackup Authentication and Authorization のライブラリがインストールされていないことを示すメッセージが表示されます。この検証は Windows の[プログラムの追加と削除]を参照して行うこともできます。

手順	説明
正しい認証ドメインの検証	[アクセス制御 (Access Control)]ホストプロパティで、または regedit を使用して、クライアントのすべての定義済み認証ドメインが正しいことを確認します。ドメインの綴りが正しいことを確認します。各ドメインに一覧表示された認証ブローカーがそのドメイン形式に対して有効であることを確認します。

アクセス管理ユーティリティの使用

NetBackup のセキュリティ管理者ユーザーグループに割り当てられているユーザーは、NetBackup 管理コンソールの[アクセス管理 (Access Management)]ノードにアクセスできます。他のユーザーグループに割り当てられているユーザーおよび NetBackup 管理者の場合、[アクセス管理 (Access Management)]ノードを参照できます。このノードは NetBackup 管理コンソールに表示されますが、展開できません。

セキュリティ管理者以外のユーザーが[アクセス管理 (Access Management)]を選択しようとすると、エラーメッセージが表示されます。[アクセス管理 (Access Management)]固有のツールバーオプションおよびメニュー項目は、表示されません。

前の手順が正常に完了すると、デフォルトの NetBackup ユーザーグループが、NetBackup 管理コンソールの[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]ウィンドウに表示されます。

コマンドラインでグループを表示するには、認可サーバーソフトウェアがインストールされているコンピュータで、bpnbaz -ListGroups を実行します。

UNIX

bpnbaz は、/usr/openv/netbackup/bin/admincmd ディレクトリに存在します。

Windows

bpnbaz は、*Install_path*¥Veritas¥NetBackup¥bin¥admincmd ディレクトリに存在します。

(bpnbat -login を使用して、セキュリティ管理者としてログオンしておく必要があります。)

```
bpnbaz -ListGroups
 NBU_User
 NBU_Operator
 NBU_Admin
 NBU_Security Admin
 Vault_Operator
 NBU_SAN Admin
 NBU_KMS Admin
 Operation completed successfully.
```

NetBackup のユーザーグループが表示されます。この処理によって、セキュリティ管理者がユーザーグループにアクセスできることを確認します。

nbac_cron ユーティリティについて

cron ユーティリティを使うと、NetBackup 操作をスケジュールされたジョブとして実行できます。NBAC が有効になると、これらのジョブは、必要なコマンドを実行する権限がある OS ユーザーというコンテキストで実行できます。nbac_cron.exe ユーティリティを使って、cron ジョブまたは AT ジョブの実行に必要な資格情報を作成できます。これらの資格情報は、bpnbat ログオンを実行して取得される資格情報と比べて、より長期間有効になります。ここでは、1 年間有効になります。

このユーティリティは次の場所にあります。

```
-/opt/openv/netbackup/bin/goodies/nbac_cron
```

nbac_cron ユーティリティを設定して cron ジョブを実行する手順について詳しくは、次のトピックを参照してください。

p.220 の「nbac_cron ユーティリティの使用」を参照してください。

nbac_cron ユーティリティの使用

次の手順により、cron ジョブを実行するためのクレデンシャルを作成できます。

nbac_cron ユーティリティを使用した cron ジョブの実行

1 マスターサーバー上で root または管理者として nbac_cron-addCron コマンドを実行します。

```
root@amp# /usr/openv/netbackup/bin/goodies/nbac_cron -AddCron

# nbac_cron -AddCron

This application will generate a Symantec private domain identity
that can be used in order to run unattended cron and/or at jobs.

User name to create account for (e.g. root, JSmith etc.): Dan

Password:*****

Password:*****

Access control group to add this account to [NBU_Admin]:

Do you with to register this account locally for root(Y/N) ? N

In order to use the account created please login as the OS
identity that will run the at or cron jobs. Then run nbac_cron
-setupcron or nbac_cron -setupat. When nbac_cron -setupcron or
```

```
nbac_cron -setupat is run the user name, password and
authentication broker will need to be supplied. Please make note
of the user name, password, and authentication broker. You may
rerun this command at a later date to change the password for an
account.

Operation completed successfully.
```

明示的に、ユーザーを追加するアクセス制御グループ (NBU_Operator、Vault_Operator など) を指定しない場合、cron ユーザー (ここでは Dan) が NBU_Admin グループに追加されます。

「Yes」を選択して、ローカルにアカウントを root として登録すると、`nbac_cron -SetupCron` コマンドは自動的に root として cron_user ユーザーに対して実行されます。root 以外の OS ユーザーとして cron ジョブを実行する場合は、「No」を選択して、手動で `nbac_cron -SetupCron` コマンドを root 以外の OS ユーザーとして実行する必要があります。

ID は Symantec プライベートドメイン内で生成されます。この ID を cron ジョブの実行に使用できます。

2 次に、cron ジョブを実行する必要がある OS ユーザーとして `nbac_cron-SetupCron` コマンドを実行して、この ID のクレデンシャルを取得します。

```
[dan@amp ~]$ /usr/openv/netbackup/bin/goodies/nbac_cron -SetupCron

This application will now create your cron and/or at identity.

Authentication Broker: amp.sec.punin.sen.symantec.com

Name: Dan

Password:*****

You do not currently trust the server:
amp.sec.punin.sen.symantec.com, do you wish to trust it? (Y/N):
Y

Created cron and/or at account information. To use this account
in your own cron or at jobs make sure that the environment
variable VXSS_CREDENTIAL_PATH is set to
"/home/dan/.vxss/credentials.crat"

Operation completed successfully.
```

「You do not currently trust the server」メッセージは、そのブローカーをまだ信頼できていない場合、1 回だけ表示されます。

クレデンシャルは、ユーザーのホームディレクトリ `user/.vxss/credentials.crat` に作成されます。クレデンシャルは、生成から 1 年間有効になります。

必要に応じて、次のコマンドによりクレデンシャル情報を確認できます。

```
dan@amp~]$ /usr/openv/netbackup/bin/bpnbat -whoami -cf
~dan/.vxss/credentials.crat

Name: CronAt_dan

Domain: CronAtUsers@amp.sec.punin.sen.symantec.com

Issued by: /CN=broker/OU=amp.sec.punin.sen.symantec.com

Expiry Date: Feb 4 13:36:08 2016 GMT

Authentication method: Symantec Private Domain

Operation completed successfully.
```

期限切れになる前にクレデンシャルを更新するには、SetupCron の操作 (手順 2) を再実行する必要があります。

3 これで、独自の cron ジョブを作成できるようになりました。新しいジョブをスケジュールする前に、VXSS_CREDENTIAL_PATH パスが、作成したクレデンシャルを指していることを確認してください。

NetBackup へアクセス可能なユーザーの決定について

アクセス管理ユーティリティでは、1 つのユーザーグループのみが許可されます。デフォルトでは、NBU_Security Admin ユーザーグループが NetBackup のアクセス管理に関する次の事項を定義します。

- 個々のユーザーの権限。
  p.223 の「個々のユーザー」を参照してください。
- ユーザーグループの作成。
  p.224 の「ユーザーグループ」を参照してください。

まず、ユーザーがアクセスする必要のある NetBackup リソースを決定します。リソースと関連する権限の場合

p.237 の「NetBackup ユーザーグループの特定のユーザー権限の表示」を参照してください。

セキュリティ管理者は、まず複数のユーザー間の共通点を検討し、次にそれらのユーザーが必要とする権限を付与されたユーザーグループを作成できます。一般に、ユーザーグループは、その役割 (管理者、オペレータ、エンドユーザーなど) に対応します。

次に示す 1 つ以上の条件に基づいたユーザーグループを検討してください。

- 組織内の機能に基づいた単位 (UNIX 管理など)
- NetBackup リソース (ドライブ、ポリシーなど)

- 場所 (西部、東部など)
- 個人の職務 (テープオペレータなど)

権限は、ホストごとの各ユーザーではなく、ユーザーグループ内の各ユーザーに付与されます。ユーザーは付与された権限の範囲内でのみ処理を実行できます。コンピュータ名に基づく制限はありません。

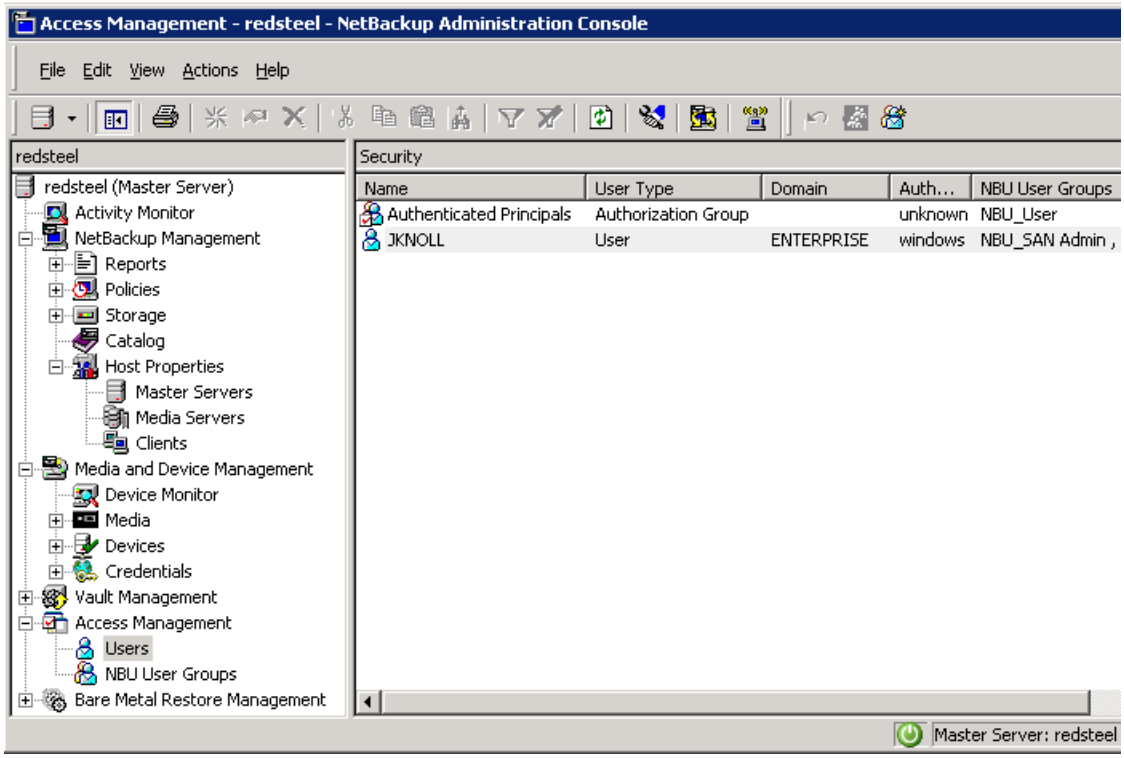
個々のユーザー

NetBackup のアクセス管理ユーティリティでは、OS で定義されている既存のユーザー、グループおよびドメインが使用されます。アクセス管理ユーティリティでは、ユーザーおよびパスワードのリストが保持されません。セキュリティ管理者がグループのメンバーを定義する場合は、OS の既存のユーザーをユーザーグループのメンバーとして指定します。

認証されたすべてのユーザーは、1 つ以上の認可ユーザーグループに属します。デフォルトでは、すべてのユーザーは、NBU_Users ユーザーグループに属します。このユーザーグループには、認証済みのすべてのユーザーが含まれています。

図 6-14に、個々の認証済みユーザーを示します。

図 6-14　　個々のユーザー



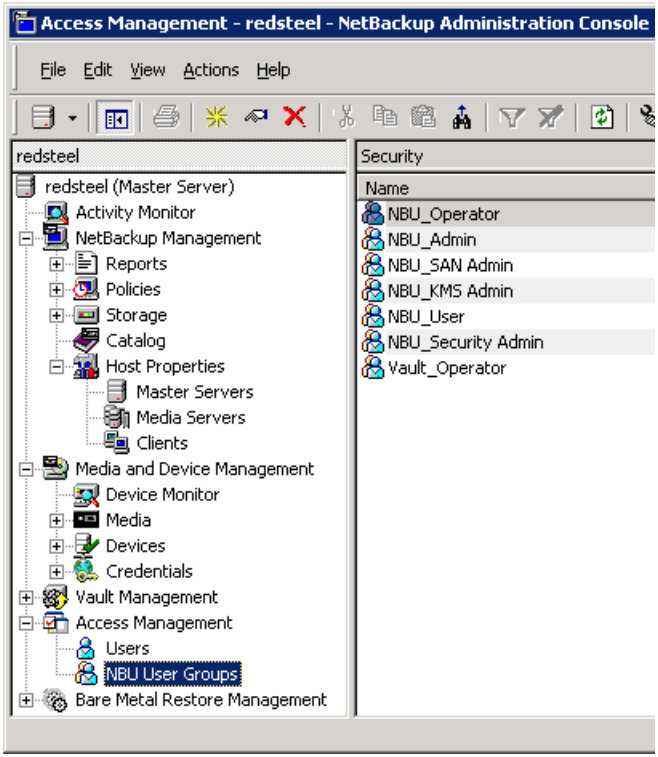
すべての認証済みユーザーは、NBU_Users ユーザーグループの暗黙的なメンバーです。他のすべてのグループには、メンバーを明示的に定義する必要があります。NetBackup セキュリティ管理者は、他のグループに手動で追加されたメンバーを削除することができます。ただし、NBU_Security Admin グループの事前定義された暗黙的なメンバーを削除することはできません。OS グループおよび OS ユーザーを認可グループに追加することもできます。

ユーザーグループ

NetBackup のアクセス管理を構成する場合、ユーザーグループに権限を割り当て、次にユーザーをユーザーグループに割り当てます。個々のユーザーに権限を直接割り当てるのではなく、グループに権限を割り当てます。

図 6-15に、ユーザーグループのリストを示します。

図 6-15　　ユーザーグループ



インストールが正常に行われると、多くのサイトにおける NetBackup 運用の作業管理を支援するデフォルトユーザーグループが作成されます。これらのユーザーグループは、[**アクセス管理** (Access Management)]>[NBU **ユーザーグループ** (NBU User Groups)] に表示されます。[アクセス管理 (Access Management)]の内容は NBU_Security Admin グループのメンバーだけが参照できます。

セキュリティ管理者は、デフォルトの NetBackup ユーザーグループを使うか、またはカスタムユーザーグループを作成できます。

NetBackup のデフォルトユーザーグループ

デフォルトユーザーグループで権限が付与されているユーザーは、ユーザーグループ名と直接関連しています。原則として、認可オブジェクトは、NetBackup 管理コンソールのツリーに表示されるノードと関連しています。

次の表では、NetBackup の各デフォルトユーザーグループについて説明します。

表 6-16 NetBackup のデフォルトユーザーグループ

デフォルトユーザーグループ	説明
オペレータ (NBU_Operator)	NBU_Operator ユーザーグループの主な作業は、ジョブの監視です。たとえば、NBU_Operator ユーザーグループのメンバーがジョブを監視し、問題が発生した場合は、NetBackup 管理者に通知する場合があります。その後、管理者によってその問題が解決されます。多くの場合、デフォルトでは、NBU_Operator ユーザーグループのメンバーは、より大きな問題を解決するために必要な権限を持っていません。 NBU_Operator ユーザーグループのメンバーは、テープの移動、ドライブの操作、ロボットのインベントリなどの作業を実行する権限を持ちます。
管理者 (NBU_Admin)	NBU_Admin ユーザーグループのメンバーは、任意の NetBackup 認可オブジェクトに対してアクセス、構成および操作を行うための完全な権限を持ちます。SAN 管理者の場合には、一部例外があります。つまり、メンバーは、[アクセス管理 (Access Management)] 以外に管理者が利用可能なすべての権限を持ちます。ただし、このグループのメンバーは、OS に root または管理者としてログオンする必要はありません。 **メモ:** NBU_Admin ユーザーグループのメンバーは [アクセス管理 (Access Management)] の内容を参照できないため、他のユーザーグループに権限を割り当てることはできません。
SAN 管理者 (NBU_SAN Admin)	デフォルトでは、NBU_SAN Admin ユーザーグループのメンバーは、ディスクプールおよびホストプロパティの表示、読み込み、操作および構成を行うための完全な権限を持ちます。これらの権限によって、SAN 環境および NetBackup との関係を構成できます。
ユーザー (NBU_User)	NBU_User ユーザーグループは、付与された権限が最も少ない、NetBackup のデフォルトユーザーグループです。NBU_User ユーザーグループのメンバーは、ローカルホストでファイルのバックアップ、リストアおよびアーカイブだけを実行できます。NBU_User ユーザーグループのメンバーは、NetBackup のクライアントインターフェース (BAR) の機能にアクセスする権限を持ちます。
セキュリティ管理者 (NBU_Security Admin)	通常、NBU_Security Admin ユーザーグループに属するメンバーは非常に少数です。 デフォルトでは、セキュリティ管理者が所有する権限は、[アクセス管理 (Access Management)] でアクセス制御を構成する権限だけです。アクセス制御を構成する権限には、次の権限が含まれます。 ■ NetBackup 管理コンソールで [アクセス管理 (Access Management)] の内容を参照する ■ ユーザーとユーザーグループを作成、変更および削除する ■ ユーザーグループにユーザーを割り当てる ■ ユーザーグループに権限を割り当てる

デフォルトユーザーグループ	説明
Vault オペレータ (Vault_Operator)	Vault_Operator ユーザーグループは、Vault 処理で必要なオペレータ操作を実行する権限を付与されたデフォルトユーザーグループです。
KMS 管理者 (NBU_KMS Admin)	デフォルトでは、NBU_KMS Admin ユーザーグループのメンバーは、暗号化キーマネージメントプロパティの表示、読み込み、操作および構成を行うための完全な権限を持ちます。これらの権限によって、KMS 環境および NetBackup との関係を構成することができます。
追加ユーザーグループ	セキュリティ管理者 (NBU_Security Admin または同等のグループのメンバー) は、必要に応じてユーザーグループを作成できます。デフォルトユーザーグループは、選択して変更および保存することができます。今後の参照用にデフォルト設定を残しておくために、デフォルトユーザーグループをコピーして、名前を変更してから保存することをお勧めします。

ユーザーグループの構成

セキュリティ管理者は、新しいユーザーグループを作成できます。[アクセス管理 (Access Management)]>[処理 (Actions)]>[新しいグループ (New Group)]を展開するか、または既存のユーザーグループを選択して[アクセス管理 (Access Management)]>[処理 (Actions)]>[新しいグループにコピー (Copy to New Group)]を展開します。

新しいユーザーグループの作成

次の手順に従って、新しいユーザーグループを作成することができます。

新しいユーザーグループを作成する方法

1. NBU_Security Admin ユーザーグループ (または同等のユーザーグループ) のメンバーで、[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]を展開します。
2. [処理 (Actions)]>[新しいユーザーグループにコピー (New User Group)]を選択します。[新しいユーザーグループの追加 (Add New User Group)]ダイアログボックスが表示され、[一般 (General)]タブが開きます。
3. 新しいグループの名前を[名前 (Name)]フィールドに入力し、次に[ユーザー (Users)]タブをクリックします。

   p.229 の「[ユーザー (Users)]タブ」を参照してください。
4. 作成した新しいユーザーグループに割り当てる定義済みユーザーを選択します。次に[割り当て (Assign)]をクリックします。または、グループにすべての定義済みユーザーを割り当てる場合は、[すべて割り当て (Assign All)]をクリックします。[割り当て済みのユーザー (Assigned Users)]リストからユーザーを削除するには、ユーザー名を選択して[削除 (Remove)]をクリックします。

5 ［アクセス権 (Permissions)］タブをクリックします。p.234 の「［アクセス権 (Permissions)］タブ」を参照してください。

6 ［リソース (Resources)］リストおよび認可オブジェクトからリソースを選択します。次にそのオブジェクトに対する権限を選択します。

7 ［OK］をクリックし、ユーザーグループおよびグループ権限を保存します。

既存のユーザーグループのコピーによる新しいユーザーグループの作成

次の手順に従って、既存のユーザーグループのコピーから新しいユーザーグループを作成することができます。

既存のユーザーグループをコピーして新しいユーザーグループを作成する方法

1 NBU_Security Admin ユーザーグループ (または同等のユーザーグループ) のメンバーで、［アクセス管理 (Access Management)］>［NBU ユーザーグループ (NBU User Groups)］を展開します。

2 ［詳細 (Details)］ペインで、既存のユーザーグループを選択します。(NetBackup 管理コンソールの左側のペイン。)

3 ［処理 (Actions)］>［新しいユーザーグループにコピー (Copy to New User Group)］を選択します。選択したユーザーグループに基づいたダイアログボックスが表示され、［一般 (General)］タブが開きます。

4 新しいグループの名前を［名前 (Name)］フィールドに入力し、次に［ユーザー (Users)］タブをクリックします。

5 作成した新しいユーザーグループに割り当てる定義済みユーザーを選択します。次に［割り当て (Assign)］をクリックします。または、グループにすべての定義済みユーザーを割り当てる場合は、［すべて割り当て (Assign All)］をクリックします。［割り当て済みのユーザー (Assigned Users)］リストからユーザーを削除するには、ユーザー名を選択して［削除 (Remove)］をクリックします。

6 ［アクセス権 (Permissions)］タブをクリックします。

7 ［リソース (Resources)］リストのリソースおよび認可オブジェクトを選択し、次にそのオブジェクトに対する権限を選択します。

8 ［OK］をクリックし、ユーザーグループおよびグループ権限を保存します。ユーザーグループの新しい名前が詳細ペインに表示されます。

ユーザーグループの名前の変更

一度 NetBackup ユーザーグループを作成すると、ユーザーグループの名前は変更できません。ユーザーグループの名前を直接変更する代わりに、ユーザーグループをコ

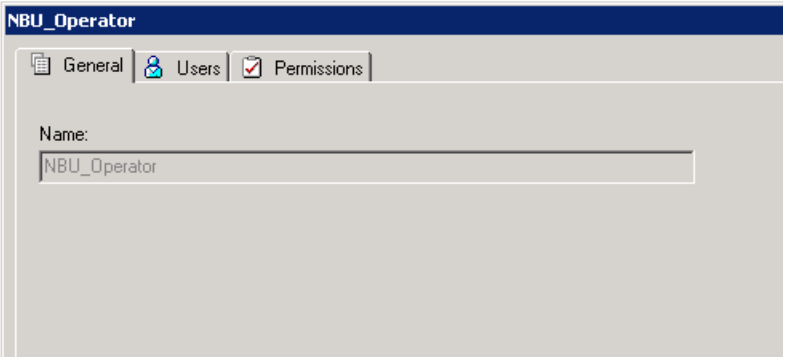
ピーして新しい名前を付け、元のグループとメンバーシップが同じであることを確認してから、元の NetBackup ユーザーグループを削除します。

[一般 (General)]タブ

[一般 (General)]タブにはユーザーグループの名前が表示されます。新しいユーザーグループを作成する場合、[名前 (Name)]テキストボックスを編集できます。

次の図に[一般 (General)]タブを示します。

図 6-16 [一般 (General)]タブ

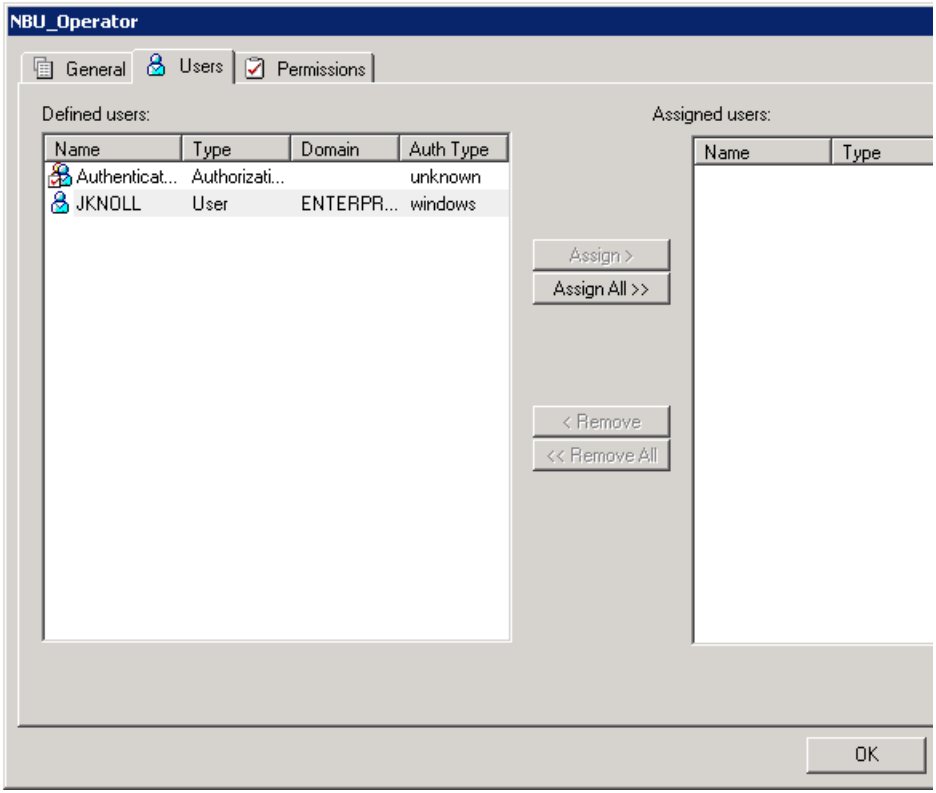


[ユーザー (Users)]タブ

[ユーザー (Users)]タブでは、ユーザーグループに対してユーザーの割り当ておよび削除を行うことができます。

次の図に[ユーザー (Users)]タブを示します。

図 6-17　［ユーザー (Users)］タブ



［ユーザー (Users)］タブの［定義されているユーザー (Defined Users)］ペイン

［定義されているユーザー (Defined Users)］ペインは他のグループ内で定義済みのユーザー全員のリストを表示します。

- ［割り当て (Assign)］オプション。
  ［定義されているユーザー (Defined Users)］ペインからユーザーを選択し、［割り当て (Assign)］をクリックすると、そのユーザーがユーザーグループに割り当てられます。
- ［すべて割り当て (Assign All)］オプション。
  ［すべて割り当て (Assign All)］をクリックすると、すべての定義済みユーザーがユーザーグループに追加されます。

［ユーザー (Users)］タブの［割り当て済みのユーザー (Assigned Users)］ペイン

［割り当て済みのユーザー (Assigned Users)］ペインには、ユーザーグループに追加されている定義済みユーザーが表示されます。

- ［削除 (Remove)］オプション。
  ［割り当て済みのユーザー (Assigned Users)］ペインからユーザーを選択し、［削除 (Remove)］をクリックすると、そのユーザーがユーザーグループから削除されます。
- ［すべて削除 (Remove All)］オプション。
  ［すべて削除 (Remove All)］をクリックすると、すべての割り当て済みユーザーが［割り当て済みのユーザー (Assigned Users)］リストから削除されます。

ユーザーグループへの新しいユーザーの追加

［新しいユーザー (New User)］をクリックして［定義されているユーザー (Defined Users)］リストにユーザーを追加します。 追加したユーザーの名前が［定義されているユーザー (Defined Users)］リストに表示されます。セキュリティ管理者は、このユーザーをユーザーグループに割り当てることができます。

p.233 の「ユーザーグループへのユーザーの割り当て」を参照してください。

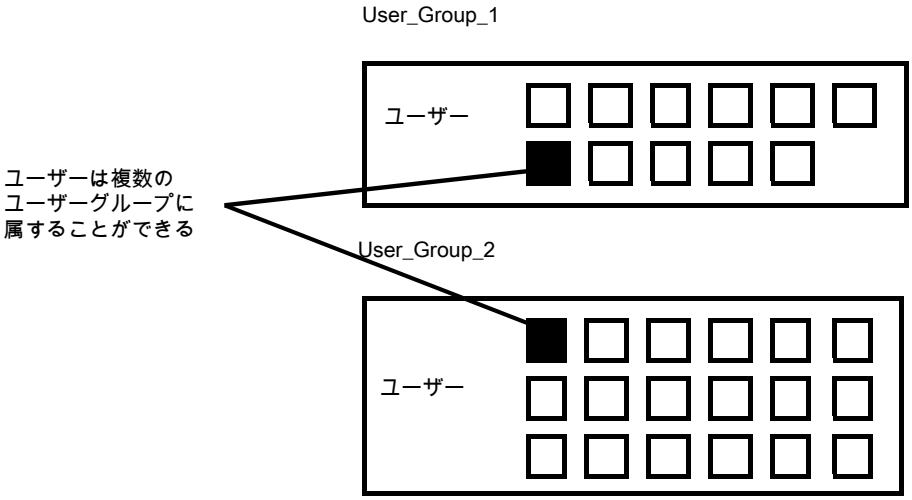
ユーザーグループおよびユーザーの定義について

NetBackup では、オペレーティングシステムの既存のユーザーが認証されます。NetBackup のパスワードとプロファイルを使用して NetBackup ユーザーを作成する必要はありません。

ユーザーは複数のユーザーグループに属することができ、属するグループのアクセス権を組み合わせた権限を持ちます。

図 6-18 に、ユーザーグループの定義を示します。

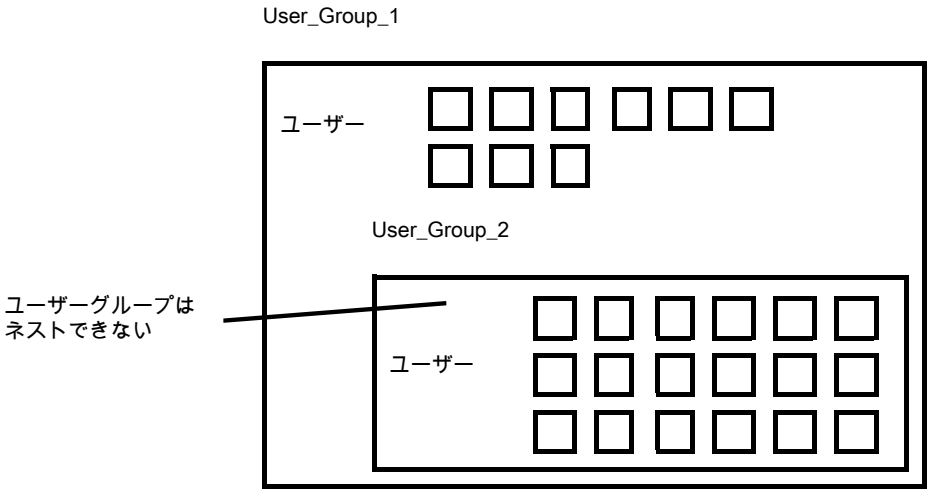
図 6-18　　ユーザーグループの定義



ユーザーは同時に複数のユーザーグループのメンバーになることができますが、NetBackup では、ユーザーグループをネストできません。たとえば、ユーザーグループのメンバーは複数のユーザーグループに属することができますが、ユーザーグループは他のユーザーグループに属することはできません。

次の図に、ユーザーグループはネストできないことを示します。

図 6-19　　ユーザーグループはネストできない



新しいユーザーとしてのログオン

新しいユーザーとしてログオンするには次の手順を使うことができます。

新しいユーザーとしてログオンする方法

◆ ［ファイル (File)］>［新しいユーザーとしてログオン (Login as New User)］を展開します (Windows)。このオプションはアクセス制御が構成されるコンピュータでのみ利用可能です。これは、最小限の権限で操作を行うという考え方を取り入れる場合に有効です。各ユーザーは、より高度な権限を持つアカウントを使用するように設定を切り替える必要があります。

ユーザーグループへのユーザーの割り当て

次の手順に従って、ユーザーをユーザーグループに割り当てることができます。ユーザーは、既存のネームスペース (NIS、Windows など) から NBU のユーザーグループに割り当てられます。この手順においては、新しいユーザーアカウントは作成されていません。

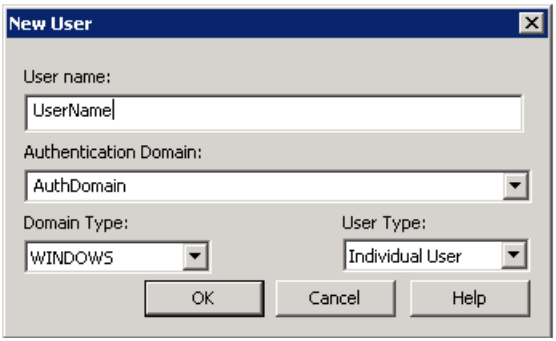
ユーザーをユーザーグループに追加する方法

1 NBU_Security Admin ユーザーグループ (または同等のユーザーグループ) のメンバーで、［アクセス管理 (Access Management)］>［NBU ユーザーグループ (NBU User Groups)］を展開します。

2 ユーザーを追加するユーザーグループをダブルクリックします。

3 ［ユーザー (Users)］タブを選択し、［ユーザーの追加 (Add User)］をクリックします。

次のように表示されます。



4 ユーザー名と認証ドメインを入力します。ユーザーのドメイン形式を、［NIS］、［NIS+］、［PASSWD］、［Windows］または［Vx］から選択します。ドメイン形式について詳しくは、『Symantec Product Authentication and Authorization Administrator's Guide』を参照してください。

5 ユーザーのドメイン形式を、次のいずれかから選択します。

- NIS
  ネットワーク情報サービス
- NIS+
  ネットワーク情報サービスプラス
- PASSWD
  認証サーバー上の UNIX パスワードファイル
- Windows
  プライマリドメインコントローラまたは Active Directory
- Vx
  Veritas プライベートデータベース

6 ［ユーザー形式 (User Type)］で、ユーザーが個々のユーザーか OS グループかを選択します。

7 ［OK］をクリックします。名前が［割り当て済みのユーザー (Assigned Users)］リストに追加されます。

［アクセス権 (Permissions)］タブ

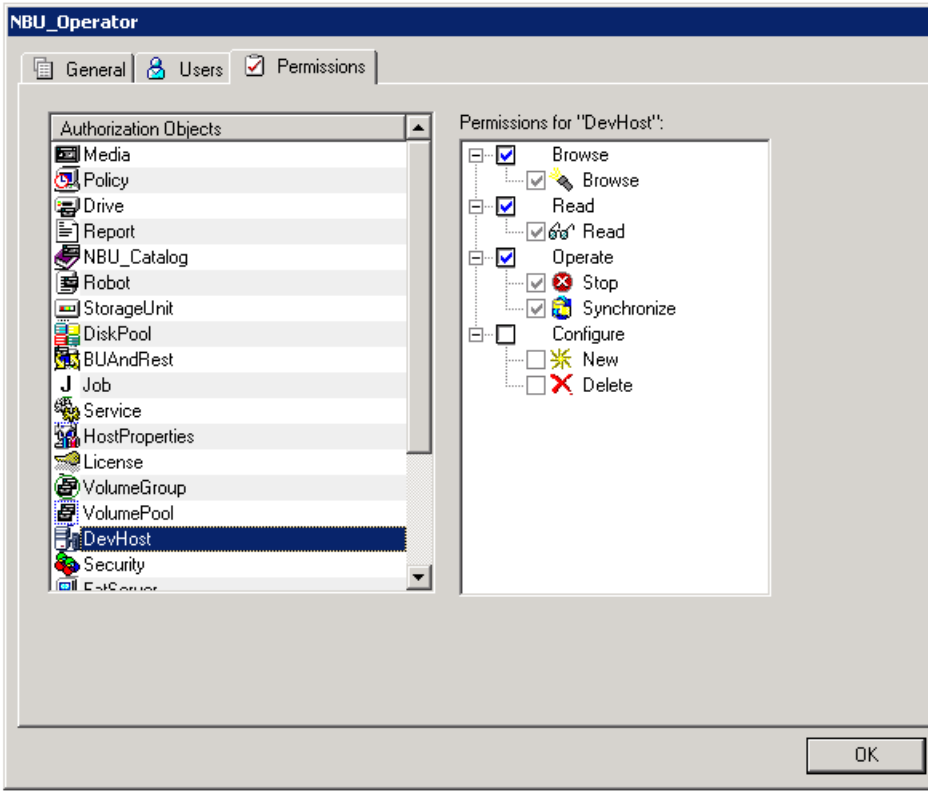
［アクセス権 (Permissions)］タブには、NetBackup の認可オブジェクトおよび各オブジェクトに関連付けられている構成可能な権限が表示されます。

認可オブジェクトおよび権限について

通常、認可オブジェクトは、NetBackup 管理コンソールのツリーに表示されるノードと関連しています。

次の図に認可オブジェクトを示します。

図 6-20　　認可オブジェクト



[認可オブジェクト (Authorization Objects)] ペインには、権限を付与することが可能な NetBackup オブジェクトが表示されます。

[「DevHost」の権限 (Permissions for "DevHost")] ペインには、選択したユーザーグループに構成されている権限のセットが表示されます。

認可オブジェクトには、次の権限セットのいずれかを付与できます。

- 参照および読み込み
- 操作
- 構成

[「DevHost」の権限 (Permissions for "DevHost")] 列に小文字が表示されている場合は、権限セットのすべての権限ではなく、一部の権限を示します。権限はオブジェクトに対して付与されています。

権限の付与

ユーザーグループのメンバーに権限を付与するために次の手順を使うことができます。

権限をユーザーグループのメンバーに付与する方法

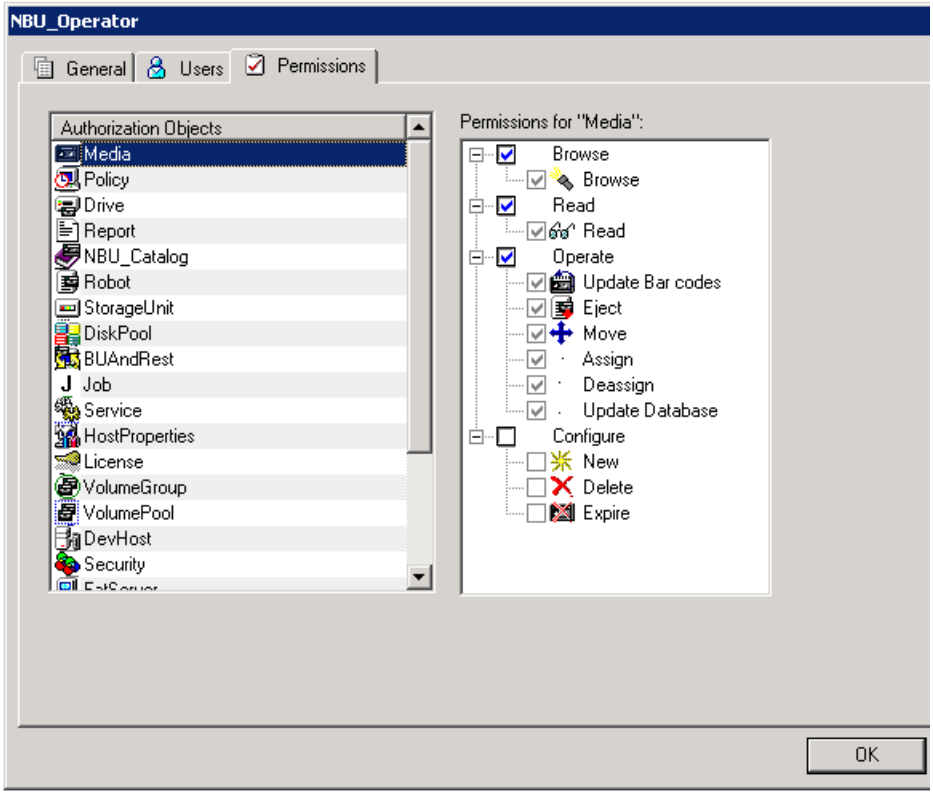
1 認可オブジェクトを選択します。

2 次に、現在選択しているユーザーグループのメンバーに付与する権限のチェックボックスにチェックマークを付けます。

新しいユーザーグループを作成するためにユーザーグループをコピーすると、権限の設定もコピーされます。

次の図に、権限リストの例を示します。

図 6-21 権限リスト



NetBackup ユーザーグループの特定のユーザー権限の表示

各 NBU ユーザーグループに付与される権限は、認可オブジェクトの名前と関連しています。デフォルトの NBU ユーザーグループには、NBU_Operator、NBU_Admin、NBU_SAN Admin、NBU_User、NBU_Security Admin および Vault_Operator が含まれます。

リソース間の相互依存の複雑さのために、場所によってはリソースへのアクセスや単一の権限へのアクセスをマッピングすることは不可能です。アクセス確認の決定をするために評価される必要のある複数の基礎的な権限がリソース間に存在することがあります。このような権限の混在により、リソース権限とリソースアクセス間で何らかの不一致が生じる可能性があります。この潜在的な不一致は、ほとんどの場合読み込み権限に限定されます。たとえば、Security_Admin には、ポリシーの参照や表示の権限がないことがあります。ポリシーはクライアントのセキュリティの構成に必要なクライアント情報を含んでいるため、管理者はポリシーへのアクセス権が必要です。

メモ: 権限の例外がある場合があります。NBU_User、NBU_KMS_Admin、NBU_SAN Admin、Vault_Operator ユーザーは、Java GUI からホストプロパティにアクセスできません。ホストプロパティのデータをフェッチするには、ポリシーオブジェクトにも参照を作ります。この例外は、ホストプロパティにアクセスするためには、ユーザーはポリシーオブジェクトの読み込みまたは参照アクセス権が必要であることを意味します。ポリシーオブジェクトに手動で読み込みアクセス権を与えることで問題を解決します。

メモ: この件に関して詳しくは、http://entsupport.symantec.com/docs/336967 を参照してください。

特定のユーザー権限を表示する方法

1. NetBackup 管理コンソールで、[アクセス管理 (Access Management)]>[NBU ユーザーグループ (NBU User Groups)]を展開します。
2. [セキュリティ (Security)]ウィンドウで、NBU_Operator、NBU_Admin、NBU_SAN Admin、NBU_User、NBU_Security Admin または Vault_Operator のいずれか適切なものをダブルクリックします。
3. [NBU_Operator]ウィンドウで、[アクセス権 (Permissions)]タブを選択します。
4. [認可オブジェクト (Authorization Objects)]ペインで、必要な認可オブジェクトを選択します。[アクセス権 (Permissions)]ペインはその認可オブジェクトの権限を表示します。

認可オブジェクト

次の表に、NetBackup 管理コンソールの［NBU_Operator］ウィンドウに表示されている順序で認可オブジェクトを示します。

また、これらの表は、次のように、NBU ユーザーグループごとに認可オブジェクトとデフォルトの権限の関係も示します。

- X は、ユーザーグループが対象の動作を実行する権限を所有していることを示します。
- 「---」は、ユーザーグループが対象の動作を実行する権限を所有していないことを示します。
- p.239 の「メディアの認可オブジェクトの権限」を参照してください。
- p.239 の「ポリシーの認可オブジェクトの権限」を参照してください。
- p.240 の「ドライブの認可オブジェクトの権限」を参照してください。
- p.240 の「レポートの認可オブジェクトの権限」を参照してください。
- p.241 の「NBU_Catalog の認可オブジェクトの権限」を参照してください。
- p.241 の「ロボットの認可オブジェクトの権限」を参照してください。
- p.242 の「ストレージユニットの認可オブジェクトの権限」を参照してください。
- p.242 の「ディスクプールの認可オブジェクトの権限」を参照してください。
- p.243 の「バックアップおよびリストアの認可オブジェクトの権限」を参照してください。
- p.244 の「ジョブの認可オブジェクトの権限」を参照してください。
- p.244 の「サービスの認可オブジェクトの権限」を参照してください。
- p.245 の「ホストプロパティの認可オブジェクトの権限」を参照してください。
- p.245 の「ライセンスの認可オブジェクトの権限」を参照してください。
- p.246 の「ボリュームグループの認可オブジェクトの権限」を参照してください。
- p.246 の「ボリュームプールの認可オブジェクトの権限」を参照してください。
- p.247 の「デバイスホストの認可オブジェクトの権限」を参照してください。
- p.247 の「セキュリティの認可オブジェクトの権限」を参照してください。
- p.248 の「ファットサーバーの認可オブジェクトの権限」を参照してください。
- p.248 の「ファットクライアントの認可オブジェクトの権限」を参照してください。
- p.249 の「Vault の認可オブジェクトの権限」を参照してください。
- p.249 の「サーバーグループの認可オブジェクトの権限」を参照してください。

- p.249 の「キー管理システム (kms) グループの認可オブジェクトの権限」を参照してください。

メディアの認可オブジェクトの権限

次の表に、メディアの認可オブジェクトに関連する権限を示します。

表 6-17　メディアの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
操作	バーコードの更新	X	X	---	---	---	X	---
	取り出し	X	X	---	---	---	X	---
	移動	X	X	---	---	---	X	---
	割り当て	X	X	---	---	---	X	---
	割り当て解除	X	X	---	---	---	X	---
	データベースの更新	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	X	---
	削除	---	X	---	---	---	X	---
	期限切れ	---	X	---	---	---	X	---

ポリシーの認可オブジェクトの権限

次の表に、ポリシーの認可オブジェクトに関連する権限を示します。

表 6-18　ポリシーの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	---	---	---	---	---
読み込み	読み込み	X	X	---	---	---	---	---

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
操作	バックアップ (Back up)	X	X	---	---	---	---	---
構成	有効化	---	X	---	---	---	---	---
	無効化	---	X	---	---	---	---	---
	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

ドライブの認可オブジェクトの権限

次の表に、ドライブの認可オブジェクトに関連する権限を示します。

表 6-19　ドライブの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	X	X	X	---	---	X	---
読み込み	読み込み	X	X	X	---	---	X	---
操作	起動	X	X	---	---	---	---	---
	停止	X	X	---	---	---	---	---
	リセット	X	X	---	---	---	---	---
	割り当て	X	---	---	---	---	---	---
	割り当て解除	X	---	---	---	---	---	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

レポートの認可オブジェクトの権限

次の表に、レポートの認可オブジェクトに関連する権限を示します。レポートには、アクセス権限セットだけを指定できます。構成権限セットまたは操作権限セットは指定できません。

表 6-20　レポートの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
参照	参照	---	X	---	---	---	X	---
読み込み	読み込み	---	X	---	---	---	X	---

NBU_Catalog の認可オブジェクトの権限

次の表に、NetBackup カタログの認可オブジェクトに関連する権限を示します。

表 6-21　NBU_Catalog の認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	---	X	---	---	---	X	---
読み込み	読み込み	---	X	---	---	---	X	---
操作	バックアップ (Back up)	---	X	---	---	---	---	---
	リストア	---	X	---	---	---	---	---
	検証	---	X	---	---	---	---	---
	複製	---	X	---	---	---	---	---
	インポート	---	X	---	---	---	---	---
	期限切れ	---	X	---	---	---	---	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---
	構成の読み込み	---	X	---	---	---	---	---
	構成の設定	---	X	---	---	---	---	---

ロボットの認可オブジェクトの権限

次の表に、ロボットの認可オブジェクトに関連する権限を示します。

表 6-22　ロボットの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	X	---	---	X	---
読み込み	読み込み	X	X	X	---	---	X	---
操作	インベントリ	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	X	---
	削除	---	X	---	---	---	X	--

ストレージユニットの認可オブジェクトの権限

次の表に、ストレージユニットの認可オブジェクトに関連する権限を示します。

表 6-23　ストレージユニットの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	---	---	---	---	---
読み込み	読み込み	X	X	---	---	---	---	---
構成	割り当て	---	X	---	---	---	---	---
	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

ディスクプールの認可オブジェクトの権限

次の表に、ディスクプールの認可オブジェクトに関連する権限を示します。

表 6-24　ディスクプールの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	X	---	---	---	---

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
読み込み	読み込み	X	X	X	---	---	---	---
操作	新規	---	X	X	---	---	---	---
	削除	---	X	X	---	---	---	---
	変更	---	X	X	---	---	---	---
	マウント	---	X	X	---	---	---	---
	マウント解除	---	X	X	---	---	---	---
構成	構成の読み込み	---	X	X	---	---	---	---
	構成の設定	---	---	X	---	---	---	---

バックアップおよびリストアの認可オブジェクトの権限

次の表に、バックアップおよびリストアの認可オブジェクトに関連する権限を示します。

表 6-25　バックアップおよびリストアの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照 (Browse)	参照	X	X	X	X	---	---	X
読み込み	読み込み	X	X	X	X	---	---	X
操作	バックアップ (Back up)	X	X	X	X	---	---	X
	リストア	X	X	X	X	---	---	X
	代替クライアント	X	X	---	---	---	---	---
	代替サーバー	X	X	---	---	---	---	---
	管理者アクセス	X	X	---	---	---	---	---
	データベースエージェント	---	---	---	---	---	---	---
	一覧表示	---	---	X	X	---	---	X

ジョブの認可オブジェクトの権限

次の表に、ジョブの認可オブジェクトに関連する権限を示します。

表 6-26　ジョブの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
操作	一時停止	X	X	---	---	---	X	---
	再開	X	X	---	---	---	X	---
	キャンセル	X	X	---	---	---	X	---
	削除	X	X	---	---	---	X	---
	再起動	X	X	---	---	---	X	---
	新規	X	X	---	---	---	X	---

サービスの認可オブジェクトの権限

次の表に、サービスの認可オブジェクトに関連する権限を示します。

表 6-27　サービスの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
操作	停止	X	X	---	---	---	---	---

読み込み権限および表示権限は、[サービス (Services)]タブまたは[デーモン (Daemons)]タブには影響を与えません。この情報はサーバーからユーザーレベルの呼び出しを使用して取得されます。呼び出しは、プロセスタスクリストにアクセスし、すべてのユーザーに対してこの情報が表示するために使用されます。

NBU_Admin ユーザーグループのメンバーではないユーザーが、OS 管理者 (管理者または root) としてログオンしている場合:

- ユーザーは、NetBackup 管理コンソールまたはコマンドラインからサービスを再起動できます。
- ユーザーは、NetBackup 管理コンソールからサービスを停止できます。コマンドラインから停止することはできません。

NBU_Admin ユーザーグループのメンバーでないユーザーが、OS 管理者 (`root`) としてログオンする場合:ユーザーは、次のコマンドラインからのみデーモンを再起動できます。

```
/etc/init.d/netbackup start
```

NBU_Admin ユーザーグループのメンバーであるユーザーが、OS 管理者 (管理者) としてログオンしていない場合:

- ユーザーは、NetBackup 管理コンソールまたはコマンドラインからサービスを再起動できません。
- ユーザーは、NetBackup 管理コンソールからサービスを停止できません。ただし、コマンドラインを使用してサービスを停止できます。

  (`bprdreq -terminate`、`bpdbm -terminate`、`stopltid` など)

NBU_Admin ユーザーグループのメンバーであるユーザーが、OS 管理者 (`root`) としてログオンしていない場合:この場合、ユーザーは NetBackup 管理コンソールまたはコマンドラインからデーモンを再起動できません。

ホストプロパティの認可オブジェクトの権限

次の表に、ホストプロパティの認可オブジェクトに関連する権限を示します。

表 6-28　ホストプロパティの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	X	X	X	X	X
読み込み	読み込み	X	X	X	X	X	X	X
構成	新規 削除	--- ---	X X	--- ---	--- ---	--- ---	--- ---	--- --

ライセンスの認可オブジェクトの権限

次の表に、ライセンスの認可オブジェクトに関連する権限を示します。

表 6-29　ライセンスの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	X	X	X	X	X
読み込み	読み込み	X	X	X	X	X	X	X
構成	割り当て	---	X	---	---	---	---	---
	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

ボリュームグループの認可オブジェクトの権限

次の表に、ボリュームグループの認可オブジェクトに関連する権限を示します。

表 6-30　ボリュームグループの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

ボリュームプールの認可オブジェクトの権限

次の表に、ボリュームプールの認可オブジェクトに関連する権限を示します。

表 6-31　ボリュームプールの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
構成	割り当て	---	X	---	---	---	---	---
	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

デバイスホストの認可オブジェクトの権限

次の表に、デバイスホストの認可オブジェクトに関連する権限を示します。

メモ: DevHost オブジェクトは、[メディアおよびデバイスの管理 (Media and Device Management)]>[クレデンシャル (Credentials)]ノードへのアクセスを制御します。

表 6-32　デバイスホストの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照 (Browse)	参照	X	X	X	---	---	X	---
読み込み	読み込み	X	X	X	---	---	X	---
操作	停止	X	X	---	---	---	---	---
	同期化	X	X	---	---	---	---	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---

セキュリティの認可オブジェクトの権限

次の表に、セキュリティの認可オブジェクトに関連する権限を示します。

表 6-33　セキュリティの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	---	---	---	---	X	---	---

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
読み込み	読み込み	---	---	---	---	X	---	---
構成	セキュリティ	---	---	---	---	X	---	---

ファットサーバーの認可オブジェクトの権限

次の表に、ファットサーバーの認可オブジェクトに関連する権限を示します。

表 6-34　ファットサーバーの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	X	---	---	---	---
読み込み	読み込み	X	X	X	---	---	---	---
構成	変更	---	X	X	---	---	---	---
	SAN 構成の変更	---	---	X	---	---	---	---

ファットクライアントの認可オブジェクトの権限

次の表に、ファットクライアントの認可オブジェクトに関連する権限を示します。

表 6-35　ファットクライアントの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	X	---	---	---	---
読み込み	読み込み	X	X	X	---	---	---	--
操作	検出	---	X	X	---	---	---	---
構成	変更	---	X	X	---	---	---	---

Vault の認可オブジェクトの権限

次の表に、Vault の認可オブジェクトに関連する権限を示します。

表 6-36　Vault の認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	---	X	---	---	---	X	---
読み込み	読み込み	---	X	---	---	---	X	---
操作	コンテナの管理	---	X	---	---	---	X	---
	レポートの実行	---	X	---	---	---	X	---
構成	変更	---	X	---	---	---	---	---
	セッションの実行	---	X	---	---	---	---	---

サーバーグループの認可オブジェクトの権限

次の表に、サーバーグループの認可オブジェクトに関連する権限を示します。

表 6-37　サーバーグループの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照	参照	X	X	---	---	---	X	---
読み込み	読み込み	X	X	---	---	---	X	---
構成	新規	---	X	---	---	---	---	---
	削除	---	X	---	---	---	---	---
	変更	---	X	---	---	---	---	---

キー管理システム (kms) グループの認可オブジェクトの権限

次の表では、キー管理システムグループの認可オブジェクトに関連する権限を示します。

表 6-38　キー管理システムグループの認可オブジェクトの権限

セット	動作	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
参照 (Browse)	参照 (Browse)	---	X	---	---	---	---	X
読み込み	読み込み	---	X	---	---	---	---	X
構成	新規	---	---	---	---	---	---	X
	削除 (Delete)	---	---	---	---	---	---	X
	変更	---	---	---	---	---	---	X

7

格納データの暗号化セキュリティ

この章では以下の項目について説明しています。

- 格納データの暗号化に関する用語
- 格納データの暗号化に関する制限事項
- 暗号化セキュリティについて考慮する際の質問
- NetBackup 格納データの暗号化オプション
- 暗号化オプションの比較
- オプション 1 - NetBackup クライアントの暗号化
- 暗号化を使用したバックアップの実行について
- バックアップの暗号化の選択について
- 標準暗号化を使用したバックアップ処理
- レガシー暗号化を使用したバックアップ処理
- NetBackup 標準暗号化を使用したリストア処理
- NetBackup レガシー暗号化を使用したリストア処理
- 暗号化セキュリティのインストール前提条件
- UNIX 版 NetBackup サーバーへの暗号化のインストール
- Windows 版 NetBackup サーバーへの暗号化のインストール
- UNIX 版 NetBackup クライアントへの暗号化のローカルインストールについて

- Windows 版 NetBackup クライアントへの暗号化のローカルインストールについて
- クライアントでの標準暗号化の構成について
- 標準暗号化の構成オプションの管理
- NetBackup 暗号化鍵ファイルの管理
- サーバーからの標準暗号化の構成について
- クライアントノードでの暗号化鍵ファイルの作成について
- 鍵ファイルの作成
- 鍵ファイルのリストアの推奨する実施例
- 鍵ファイルのパスフレーズを保護するための手作業による保存
- 鍵ファイルの自動バックアップ
- 暗号化されたバックアップファイルの、異なるクライアントへのリストア
- クライアントでの標準暗号化の直接的な構成について
- ポリシーでの標準暗号化属性の設定
- NetBackup サーバーからのクライアントの暗号化設定の変更
- レガシー暗号化の構成について
- サーバーからのレガシー暗号化の構成について
- レガシー暗号化構成オプション
- クライアントへのレガシー暗号化構成のプッシュインストールについて
- クライアントへのレガシー暗号化パスフレーズのプッシュインストールについて
- レガシー暗号化鍵ファイルの管理
- 別のクライアントで作成されたレガシー暗号化が使用されたバックアップのリストア
- ポリシーでのレガシー暗号化属性の設定について
- サーバーからのクライアントのレガシー暗号化設定の変更
- UNIX 版クライアントのレガシー鍵ファイルの追加によるセキュリティの向上
- bpcd -keyfile コマンドの実行
- UNIX クライアントでの bpcd の終了
- オプション 2 - メディアサーバーの暗号化

- メディアサーバー暗号化オプション管理

格納データの暗号化に関する用語

次の表では、格納データの暗号化に関する用語について説明します。

表 7-1　格納データの暗号化に関する用語

用語	説明
非同期暗号化	公開鍵と秘密鍵の両方を使用する暗号化アルゴリズムが含まれます。
同期暗号化	暗号化と復号化の両方に同じ鍵を使用する暗号化アルゴリズムが含まれます。鍵のサイズが同じ場合、同期暗号化は非同期暗号化よりも高速で安全です。
初期化ベクター	暗号化アルゴリズムの事前準備に使われるシード値を指定します。この事前準備は、複数のデータファイルの暗号化に同じ鍵を使用する場合に現れるパターンを、分かりにくくするために行われます。これらのファイルは同じパターンで始まります。
AES (Advanced Encryption Standard)	DES に代わる同期暗号化アルゴリズムを指定します。
DES (Data Encryption Standard)	1970 年代から 1998 年までのデータ同期暗号化の一般的な規格を指定します。
公開鍵暗号化	非同期暗号化を使います。

格納データの暗号化に関する制限事項

次の表では、格納データの暗号化に関する制限事項について説明します。

表 7-2　格納データの暗号化に関する制限事項

制限事項	説明
データの暗号化によるコンピュータのパフォーマンスへの影響	データ圧縮アルゴリズムと同様、暗号化アルゴリズムでは CPU に高い負荷がかかります。コンピュータのハードウェア (専用または共有のいずれか) を追加せずにデータを圧縮すると、コンピュータと NetBackup のパフォーマンスに影響します。
データの圧縮はデータの暗号化より先に実行する必要がある	データの圧縮アルゴリズムでは、データを圧縮するためにデータのパターンが検索されます。暗号化アルゴリズムでは、データにスクランブルがかけられ、パターンが削除されます。このため、データの圧縮を行う場合はデータの暗号化手順の前に行う必要があります。

制限事項	説明
暗号化アルゴリズムの選択	多くの暗号化アルゴリズムおよび関連する鍵のサイズがあります。データの暗号化には、どれを使用すればよいでしょうか。AES (Advanced Encryption Standard) はデータの暗号化規格であり、128、192 または 256 ビットの暗号化鍵がサポートされます。
AES の標準化	AES は、1998 年頃までは安全な規格であった、以前の規格である DES に代わるものです。コンピュータの処理速度の向上と並列処理技術によって、DES は数十時間の攻撃に対して脆弱であることが明らかになりました。このとき、米国政府は DES に代わる暗号化規格を公募しました。Rijndael (ラインダール) と呼ばれるアルゴリズムが最有力候補となりました。約 5 年間の専門家による評価と米国政府による評価の結果、Rijndael の特定の構成が AES となりました。 2003 年 6 月、米国政府は AES を機密情報に使用することができると発表しました。 「AES アルゴリズムのすべての鍵長の設計と強度は、128、192 および 256 である。これらは、極秘 (SECRET) レベルまでの機密情報を十分保護できる。最高機密 (TOP SECRET) 情報には、192 または 256 のいずれかの鍵長を使用する必要がある。製品への AES の実装は、国家のセキュリティシステムを保護することを目的とする。AES の取得および使用に先立ち、情報は NSA によって評価および認定される。」 詳しくは Web サイト http://www.cnss.gov/Assets/pdf/cnssp_15_fs.pdf を参照してください。
推奨される鍵のサイズ	有効な最大の鍵サイズを選択してください。通常、鍵のサイズが大きいと、鍵サイズが小さい場合よりもデータをより安全に、長期間保護できます。AES は最良の選択の 1 つです。3 つの鍵長 (128、192、256 ビット) がすべてサポートされているため、安全であると考えられています。
NIST FIPS 140	NIST (国立標準技術研究所) の FIPS (連邦情報処理標準) 140 は米国連邦政府の規格です。この規格では、連邦政府向けのデータ暗号化ソリューションが認定されます。この規格は、使用の観点とセキュリティインターフェースの観点の両方から暗号化ソリューションプロバイダが製品を文書化することを必要とします。その後、評価を受けるために、製品を公認のサードパーティのレビューアに提出します。評価に合格した場合は、製品に対して評価認定が発行されます。

制限事項	説明
暗号化ソリューションの FIPS 認定	米国政府による使用には FIPS 認定が必要です。この認定は、信頼性の目安として使用できますが、FIPS 認定を暗号化ソリューションを評価する唯一の条件にしないでください。 次に示す他の事項も考慮して決定する必要があります。 ■ FIPS 認定は、名前の付いた製品にのみ適用されます。さらに、製品の使用が、製品の評価時に提示される「FIPS Security Policy」文書に適合する場合にのみ適用されます。製品の将来のバージョンおよび標準外の使用については、検証の認定が適用されない可能性があります。 ■ AES のようなアルゴリズムのセキュリティ保護は、その動作の難解さによるものではありません。セキュリティ保護は、不明な暗号化鍵の推測の困難さによって行われます。何年もの精密な調査と専門家による評価によって、AES の実装は十分なものになりました。実際に、AES に対して、特定の鍵とデータセットを入力するテストが行われ、予測される出力が検証されています。 ■ データの暗号化は自動車のセキュリティによく似ています。問題の多くは鍵の消失または置き間違いに関連するもので、ロックの異常に関連する問題ではありません。 ■ 誤用によって問題が発生する可能性が高いため、暗号化製品の操作性も考慮の対象にする必要があります。 操作性の考慮事項には次のものがあります。 ■ 暗号化の製品との統合 ■ 暗号化のビジネスプロセスとの統合 ■ 暗号化鍵の適切な粒度 ■ リカバリの可能性
暗号化鍵の適切な粒度	暗号化鍵の適切な粒度は、家のセキュリティを例に使用すると最も分かりやすくなります。家の鍵が 1 つだけの場合は便利です。車庫、玄関口、裏口すべてに同じ鍵を使用して入ることができます。このセキュリティは、鍵の安全性が低下する (すなわち、鍵が犯罪者に盗まれる) までは効果的です。鍵の安全性が低下した場合は、この鍵を使用するすべてのロックを取り替える必要があります。極端な例では、家の引き出しと戸棚に対してそれぞれの鍵を持っている人もいます。この場合、鍵を紛失しても 1 つのロックを取り替えるだけで済みます。 適切な解決方法は、これらの 2 つの例の中間にあります。ビジネスプロセスの観点から、安全性の低下した鍵または消失した鍵に対する耐性を理解する必要があります。鍵を消失した場合は、その鍵で暗号化されたすべてのデータが失われます。鍵の安全性が低下した場合は、その鍵で暗号化されたすべてのデータを復号化し、再び暗号化してセキュリティ保護する必要があります。

暗号化セキュリティについて考慮する際の質問

暗号化のセキュリティについて考慮する前に、次の質問について考えておく必要があります。

答えは、ユーザー固有の暗号化の要件によって次のように異なります。

- どのようにして最適な暗号化を選択するか。
- なぜ暗号化セキュリティを使用するのか。
- 可能性のある内部の攻撃に対してどのような保護が必要なのか。
- 可能性のある外部の攻撃に対してどのような保護が必要なのか。
- どの領域の NetBackup を暗号化セキュリティで保護するのか。
- 暗号化セキュリティの動作を示す NetBackup アーキテクチャの図を作成する必要があるか。
- どのような暗号化セキュリティの配置ユースケースを採用するか。

NetBackup 格納データの暗号化オプション

次の項では、NetBackup 格納データの暗号化の次の 3 つのオプションの比較を示します。

p.256 の 表 7-3 を参照してください。

- オプション 1 - NetBackup クライアントの暗号化
  p.257 の「オプション 1 - NetBackup クライアントの暗号化」を参照してください。
- オプション 2 - メディアサーバーの暗号化
  p.282 の「オプション 2 - メディアサーバーの暗号化」を参照してください。
- オプション 3 - サードパーティの暗号化装置とハードウェアデバイス

暗号化オプションの比較

次の表は 3 つの暗号化オプションとそれぞれの長所と短所を示します。

表 7-3　暗号化オプションの比較

暗号化オプション	長所	短所
p.257 の「オプション 1 - NetBackup クライアントの暗号化」を参照してください。	■ 暗号化鍵はクライアントコンピュータに存在し、NetBackup 管理者によって制御されない。 ■ NetBackup マスターサーバーおよびメディアサーバーに影響を与えずに配置することができる。 ■ クライアントごとに配置することができる。	■ クライアントの暗号化鍵は、各クライアントが一意の暗号化鍵と個別の暗号化鍵を持つ必要のある環境には適さない。 ■ クライアント上で実行される暗号化および圧縮は、クライアントのパフォーマンスに影響を与える可能性がある。

暗号化オプション	長所	短所
p.282 の「オプション 2 - メディアサーバーの暗号化」を参照してください。	■ クライアントコンピュータのパフォーマンスに影響を与えない。 ■ マスターサーバーまたはメディアサーバーに鍵が集中される。	■ マスターサーバーまたはメディアサーバーに鍵が集中される。 ■ 鍵の粒度の詳細についてオプションが制限される。 ■ NetBackup 構成と操作が密接に統合されていない。 ■ メディアサーバー上で実行される暗号化および圧縮は、メディアサーバーのパフォーマンスに影響を与える可能性がある。
オプション 3 - サードパーティの暗号化装置とハードウェアデバイス	■ ハードウェアが追加されるため、通常、パフォーマンスへの影響がほとんど (またはまったく) ない ■ 通常、NIST FIPS 140 で認定されている。	■ シマンテック社では、これらのソリューションの一部がテストされている。保証または廃棄に対するテストは行われていない。また、特定のソリューションに対するテストも行われていない。このテストでは、基本的な機能が、特定のバージョンの NetBackup での使用に対して検証されている。 ■ NetBackup 構成、操作または診断が密接に統合されていない。 ■ 装置またはデバイスごとディザスタリカバリの例が提供されている。

オプション 1 - NetBackup クライアントの暗号化

NetBackup クライアントの暗号化オプションは次の場合に最適です。

- クライアントが圧縮と暗号化の際の CPU 負荷を処理できる場合
- クライアントでデータの暗号化鍵の制御を保持する場合
- NetBackup と暗号化をできるだけ密接に統合する必要がある場合
- ユーザーごとに暗号化が必要な場合

暗号化を使用したバックアップの実行について

次のようにして、暗号化を使用したバックアップを実行できます。

- バックアップの暗号化の選択
  p.258 の「バックアップの暗号化の選択について」を参照してください。
- 標準暗号化を使用したバックアップ処理

p.258 の「標準暗号化を使用したバックアップ処理」を参照してください。

- レガシー暗号化を使用したバックアップ処理
  p.259 の「レガシー暗号化を使用したバックアップ処理」を参照してください。

バックアップの暗号化の選択について

バックアップを開始すると、サーバーは、バックアップを暗号化する必要があるかどうかをポリシー属性によって判別します。その後、サーバーは、クライアント上で bpcd に接続してバックアップを開始し、バックアップ要求で暗号化ポリシー属性を渡します。

クライアントは、次のようにして、暗号化ポリシー属性をクライアントの構成の CRYPT_OPTION と比較します。

- ポリシー属性が yes で、CRYPT_OPTION が REQUIRED または ALLOWED である場合、クライアントは暗号化されたバックアップを実行します。
- ポリシー属性が yes で、CRYPT_OPTION が DENIED である場合、クライアントはバックアップを実行しません。
- ポリシー属性が no で、CRYPT_OPTION が ALLOWED または DENIED である場合、クライアントは暗号化されていないバックアップを実行します。
- ポリシー属性が no で、CRYPT_OPTION が REQUIRED である場合、クライアントはバックアップを実行しません。

次の表に、それぞれの状況で実行されるバックアップ形式を示します。

表 7-4　実行されるバックアップ形式

CRYPT_OPTION	暗号化ポリシー属性あり	暗号化ポリシー属性なし
REQUIRED	暗号化する	なし
ALLOWED	暗号化する	暗号化しない
DENIED	なし	暗号化しない

p.258 の「標準暗号化を使用したバックアップ処理」を参照してください。

p.260 の「NetBackup 標準暗号化を使用したリストア処理」を参照してください。

p.259 の「レガシー暗号化を使用したバックアップ処理」を参照してください。

p.261 の「NetBackup レガシー暗号化を使用したリストア処理」を参照してください。

標準暗号化を使用したバックアップ処理

標準バックアップを暗号化する場合の前提条件は、次のとおりです。

- **メモ:** NetBackup 7.5 以降のバージョンでは、暗号化ソフトウェアは、NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

  鍵ファイルが存在している必要があります。サーバーまたはクライアントから bpkeyutil コマンドを実行すると、鍵ファイルが作成されます。

- クライアントが含まれる NetBackup ポリシーで、暗号化属性が選択されている必要があります。

前提条件が満たされると、次のようにバックアップが実行されます。

- クライアントは、鍵ファイルから最新の鍵を取得します。

  バックアップされる各ファイルについて、次の処理が実行されます。

  - クライアントは、暗号化 tar ヘッダーを作成します。tar ヘッダーには、NetBackup によって暗号化に使用された鍵および暗号のチェックサムが含まれます。
  - クライアントは、CRYPT_CIPHER 構成エントリで定義された暗号を使用して、鍵で暗号化されたファイルデータを書き込みます。(デフォルトの暗号は AES-128-CFB です。)

  メモ: ファイルデータだけが暗号化されます。ファイル名および属性は暗号化されません。

- サーバー上のバックアップイメージには、バックアップが暗号化されているかどうかを示すフラグが含まれます。

レガシー暗号化を使用したバックアップ処理

レガシーバックアップを暗号化する場合の前提条件は、次のとおりです。

- 暗号化ソフトウェアには、次のように適切な DES ライブラリが含まれる必要があります。
  - 40 ビット DES 暗号化の場合、DES ライブラリは、libvdes40.suffix です。suffix は so、sl または dll で、クライアントプラットフォームによって異なります。
  - 56 ビット DES 暗号化の場合、DES ライブラリは、libvdes56.suffix です。suffix は so、sl または dll で、クライアントプラットフォームによって異なります。

  メモ: NetBackup 7.5 以降のバージョンでは、暗号化ソフトウェアは NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

- 鍵ファイルは、CRYPT_KEYFILE 構成オプションで指定したとおりに存在する必要があります。サーバーの場合は bpinst コマンド、クライアントの場合は bpkeyfile コマンドを実行して NetBackup パスフレーズを指定した場合に、鍵ファイルが作成されます。
- クライアントが含まれる NetBackup ポリシーで、暗号化属性を選択する必要があります。

前提条件が満たされ、バックアップが暗号化される場合に、次の操作が行われます。

- クライアントは、鍵ファイルから最新のデータを取得し、現在の時間 (バックアップ時間) と結合して DES 鍵を生成します。40 ビット DES の場合、鍵の 16 ビットは常に 0 (ゼロ) に設定されます。

  各バックアップファイルについて、次の処理が実行されます。

  - クライアントは、暗号化 tar ヘッダーを作成します。tar ヘッダーには、NetBackup によって暗号化に使用された DES のチェックサムが含まれます。
  - クライアントは、DES 鍵で暗号化されたファイルデータを書き込みます。ファイルデータのみが暗号化されます。ファイル名および属性は暗号化されません。
- サーバーは、クライアントからファイル名、属性およびデータを読み込んで、サーバー上のバックアップイメージにそれらを書き込みます。サーバーは、データの暗号化または復号化を行いません。サーバー上のバックアップイメージには、バックアップ時間およびバックアップが暗号化されているかどうかを示すフラグが含まれます。

NetBackup 標準暗号化を使用したリストア処理

標準暗号化が使用されたバックアップをリストアする場合の前提条件は、次のとおりです。

- 暗号化ソフトウェアは、クライアント上にコピーする必要があります。

  メモ: NetBackup 7.5 以降のバージョンでは、暗号化ソフトウェアは、NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

- 鍵ファイルが存在している必要があります。サーバーまたはクライアントから bpkeyutil コマンドを実行すると、鍵ファイルが作成されます。

リストアが実行されると、サーバーはバックアップが暗号化されているかどうかをバックアップイメージによって判別します。その後、サーバーは、クライアント上の bpcd に接続してリストアを開始します。サーバーは、リストア要求の暗号化フラグをクライアントに送信します。

バックアップが正しく実行された場合、リストアは次のように行われます。

- サーバーは、リストアされるクライアントにファイル名、属性および暗号化されたファイルデータを送信します。

- クライアントは、暗号化 tar ヘッダーを読み込むと、ヘッダーのチェックサムと鍵ファイル内の鍵のチェックサムを比較します。1 つの鍵のチェックサムがヘッダーのチェックサムと一致する場合、NetBackup では鍵を使用してファイルデータが復号化されます。ヘッダーに定義されている暗号が使用されます。
- 鍵および暗号が利用可能な場合、ファイルは復号化され、リストアされます。鍵または暗号が利用できない場合、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。

NetBackup レガシー暗号化を使用したリストア処理

レガシー暗号化が使用されたバックアップをリストアする場合の前提条件は、次のとおりです。

- レガシー暗号化ソフトウェアは、クライアント上にコピーする必要があります。

メモ: NetBackup 7.5 以降のバージョンでは、暗号化ソフトウェアは、NetBackup UNIX サーバーおよびクライアントのインストール時に自動的にインストールされます。

- 暗号化ソフトウェアには、40 ビット DES ライブラリが含まれる必要があります。40 ビット DES ライブラリの名前は、`libvdes40.suffix` です。suffix は `so`、`sl` または `dll` で、クライアントプラットフォームによって異なります。
- CRYPT_STRENGTH 構成オプションが DES_56 に設定されている場合、暗号化ソフトウェアには 56 ビット DES ライブラリが含まれている必要があります。56 ビット DES ライブラリの名前は、`libvdes56.suffix` です。suffix は `so`、`sl` または `dll` で、クライアントプラットフォームによって異なります。
- 鍵ファイルは、CRYPT_KEYFILE 構成オプションで指定したとおりに存在する必要があります。サーバーの場合は `bpinst` コマンド、クライアントの場合は `bpkeyfile` コマンドを実行して NetBackup パスフレーズを指定した場合に、鍵ファイルが作成されます。

サーバーは、バックアップが暗号化されているかどうかをバックアップイメージによって判別します。その後、サーバーは、クライアント上の `bpcd` に接続してリストアを開始します。サーバーは、リストア要求のバックアップイメージから暗号化フラグおよびバックアップ時間をクライアントに送信します。

前提条件が満たされると、次の操作が行われます。

- サーバーは、リストアされるクライアントにファイル名、属性および暗号化されたファイルデータを送信します。
- クライアントは、鍵ファイルのデータを取得し、バックアップ時間と結合して、1 つ以上の 40 ビット DES 鍵を生成します。56 ビット DES ライブラリが利用可能な場合、クライアントは、1 つ以上の 56 ビット DES 鍵も生成します。

- クライアントは、暗号化 tar ヘッダーを読み込むと、ヘッダーのチェックサムと DES 鍵のチェックサムを比較します。DES 鍵のチェックサムがヘッダーのチェックサムと一致する場合、NetBackup では DES 鍵を使用してファイルデータが復号化されます。

DES 鍵が利用可能な場合、ファイルは復号化され、リストアされます。DES 鍵が利用できない場合、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。

暗号化セキュリティのインストール前提条件

暗号化されたバックアップを構成および実行するには、NetBackup クライアント上で NetBackup Encryption ソフトウェアが利用可能である必要があります。NetBackup Encryption ソフトウェアは、NetBackup のサーバーおよびクライアントのインストールによってインストールされます。

クライアントが暗号化されたバックアップを必要とする場合、接続するサーバーが NetBackup 7.6 サーバーソフトウェアを実行している必要があります。NetBackup Encryption の構成が可能なプラットフォームのリストについては、『Symantec NetBackup リリースノート UNIX、Windows および Linux』を参照してください。

UNIX 版 NetBackup サーバーへの暗号化のインストール

UNIX 版 NetBackup サーバーとクライアントのインストールによって、暗号化ソフトウェアもインストールされます。NetBackup Encryption 用のライセンスキーが、NetBackup マスターサーバーに登録されていることを確認するには、次の手順を実行します。

NetBackup の暗号化が UNIX 版 NetBackup マスターサーバーに登録済みであることを確認する方法

◆ NetBackup Encryption 用のライセンスキーが、NetBackup マスターサーバーに登録されていることを確認します。

UNIX 版 NetBackup マスターサーバーの場合、root ユーザーとしてログオンし、次のコマンドを入力してライセンスキーを一覧表示および追加します。

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

既存の NetBackup Encryption (40 ビットまたは 56 ビット) 用のライセンスキーをアップグレードに使用できます。

Windows 版 NetBackup サーバーへの暗号化のインストール

Windows 版 NetBackup サーバーとクライアントのインストールによって、暗号化ソフトウェアもインストールされます。NetBackup Encryption 用のライセンスキーが、NetBackup マスターサーバーに登録されていることを確認するには、次の手順を実行します。

NetBackup の暗号化が Windows 版 NetBackup マスターサーバーに登録済みであることを確認する方法

◆ 管理者として Windows 版マスターサーバーにログオンします。NetBackup 管理コンソールで[ヘルプ (Help)]>[ライセンスキー (License Keys)]メニューを使用して、ライセンスキーを一覧表示および追加します。

既存の NetBackup Encryption (40 ビットまたは 56 ビット) 用のライセンスキーをアップグレードに使用できます。

UNIX 版 NetBackup クライアントへの暗号化のローカルインストールについて

UNIX 版 NetBackup クライアントにローカルインストールを実行する必要はありません。暗号化ソフトウェアは、UNIX 版 NetBackup クライアントのインストールによって自動的にインストールされます。次にクライアントの暗号化の設定を構成できます。p.263 の「クライアントでの標準暗号化の構成について」を参照してください。

Windows 版 NetBackup クライアントへの暗号化のローカルインストールについて

Windows 版 NetBackup クライアントにローカルインストールを実行する必要はありません。暗号化ソフトウェアは、Windows 版 NetBackup クライアントのインストールによって自動的にインストールされます。p.263 の「クライアントでの標準暗号化の構成について」を参照してください。

クライアントでの標準暗号化の構成について

このトピックでは NetBackup 標準暗号化を構成する方法について説明します。

次の構成オプションは、UNIX クライアント上の `bp.conf` ファイル、または Windows クライアント上のレジストリ内に存在します。

構成オプションは次のとおりです。

- CRYPT_OPTION

- CRYPT_KIND
- CRYPT_CIPHER

また、NetBackup 管理コンソールを使用して、サーバーからオプションを構成することもできます。これらのオプションは、[クライアントプロパティ (Client Properties)]ダイアログボックスの[暗号化 (Encryption)]タブに表示されます。

次を参照してください。『NetBackup 管理者ガイド Vol. 1』を参照してください。

標準暗号化の構成オプションの管理

次の表に、NetBackup クライアントの標準暗号化に関連する 3 つの構成オプションを示します。

これらのオプションが、クライアントに適切な値に設定されていることを確認します。

表 7-5　暗号化に関連する 3 つの構成オプション

オプション	値	説明
CRYPT_OPTION = *option*		NetBackup クライアントに、暗号化オプションを定義します。*option* に指定可能な値は、次のとおりです。
	denied|DENIED	クライアントが暗号化されたバックアップを許可しないように設定します。サーバーが暗号化されたバックアップを要求すると、エラーであると判断されます。
	allowed|ALLOWED	(デフォルト値) クライアントが暗号化されたバックアップまたは暗号化されないバックアップを許可するように指定します。
	required|REQUIRED	クライアントが暗号化されたバックアップを要求するように設定します。サーバーが暗号化されないバックアップを要求すると、エラーであると判断されます。
CRYPT_KIND = *kind*		NetBackup クライアントに、暗号化の種類を定義します。*kind* には、次のオプション値いずれかを設定できます。
	NONE	標準暗号化またはレガシー暗号化のどちらも、クライアント上では構成されません。
	STANDARD	標準の暗号に基づき、128 ビット暗号化または 256 ビット暗号化を使用するように指定します。このオプションは、標準暗号化をクライアント上で構成する場合のデフォルト値です。

オプション	値	説明
	LEGACY	40 ビット DES または 56 ビット DES 暗号化のレガシー暗号化を使用するように指定します。
CRYPT_CIPHER = *cipher*		使用する暗号の形式を定義します。これは、次のオプション値のいずれかに設定できます。
	AES-128-CFB	128 ビット AES。これはデフォルト値です。
	BF-CFB	128 ビット Blowfish
	DES-EDE-CFB	2 つの鍵の Triple DES
	AES-256-CFB	256 ビット AES

NetBackup 暗号化鍵ファイルの管理

このトピックは NetBackup 暗号化鍵ファイルを管理する方法を記述します。

メモ: クラスタ内のすべてのノードで同じ鍵ファイルを使用する必要があります。

bpkeyutil コマンドを実行すると、NetBackup Encryption クライアント上に暗号を使用した暗号化鍵ファイルおよびパスフレーズが設定されます。

- Windows クライアントの場合、コマンドのフルパスは次のとおりです。

  install_path¥NetBackup¥bin¥bpkeyutil

- UNIX クライアントの場合、コマンドのフルパスは次のとおりです。

  /usr/openv/netbackup/bin/bpkeyutil

クライアントのパスフレーズを追加するためのプロンプトが表示されます。

NetBackup では、指定したパスフレーズを使用して、鍵ファイルが次のように作成されます。

- 次の 2 つのアルゴリズムを組み合わせて、パスフレーズから 256 ビット鍵が作成されます。
  - セキュアハッシュアルゴリズム (SHA1)
  - メッセージダイジェストアルゴリズム (MD5)
- NetBackup の秘密鍵と 128 ビット AES アルゴリズムを使用して、鍵が暗号化されます。

- この鍵は、クライアント上の鍵ファイルに格納されます。
- 実行時、鍵およびランダム初期化ベクターを使用して、クライアントデータが暗号化されます。初期化ベクターは、バックアップイメージのヘッダーに格納されます。

以前のパスフレーズは、これらのパスフレーズを使用して暗号化されたバックアップのリストアを許可する鍵ファイルでは利用可能な状態のままです。

注意: 古いパスフレーズも含め、パスフレーズを控えておく必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

クライアントマシンの管理者に対してだけ、鍵ファイルのアクセスを可能にする必要があります。

UNIX クライアントの場合、次のことを確認する必要があります。

- 所有者が root ユーザーである。
- アクセス権モード設定が 600 である。
- ファイルは NFS マウントが可能なファイルシステムには存在しない。

サーバーからの標準暗号化の構成について

サーバーから `bpkeyutil` コマンドを実行して、多くの NetBackup クライアントを暗号化用に構成できます。

前提条件は次のとおりです。

- NetBackup のクライアントソフトウェアは NetBackup の暗号化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(『Symantec NetBackup リリースノート UNIX、Windows および Linux』を参照してください)。
- NetBackup クライアントは、リリース 7.0 以上の NetBackup を実行している必要があります。

クライアントノードでの暗号化鍵ファイルの作成について

クライアントノードで暗号化キーファイルを作成するには、次の通りガイドラインを使います。

- サーバーがクラスタ内にあり、暗号化クライアントでもある場合、クラスタ内のすべてのノードは同じ鍵ファイルを持つ必要があります。
- `bpkeyutil` コマンドを実行すると、各 NetBackup Encryption クライアント上に暗号を使用した暗号化鍵ファイルおよびパスフレーズが設定されます。

- Windows サーバーの場合、コマンドのフルパスは次のとおりです。

  install_path¥NetBackup¥bin¥bpkeyutil

- UNIX サーバーの場合、コマンドのフルパスは次のとおりです。

  /usr/openv/netbackup/bin/bpkeyutil

鍵ファイルの作成

各暗号化クライアントに対して、次のコマンドを実行します。

```
bpkeyutil -clients client_name
```

クライアントの鍵ファイルに追加する新しいパスフレーズを入力するプロンプトが表示されます。

複数のクライアントで同じパスフレーズを使用するよう設定するには、次のようにカンマで区切られたクライアント名のリストを指定します。

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

鍵ファイルの作成には、指定したパスフレーズが使用されます。

NetBackup では、指定したパスフレーズを使用して、鍵ファイルが次のように作成されます。

- 次の 2 つのアルゴリズムを組み合わせて、パスフレーズから 256 ビット鍵が作成されます。
  - セキュアハッシュアルゴリズム (SHA1)
  - メッセージダイジェストアルゴリズム (MD5)
- NetBackup の秘密鍵と 128 ビット AES アルゴリズムを使用して、鍵が暗号化されます。
- この鍵は、クライアント上の鍵ファイルに格納されます。
- 実行時、鍵およびランダム初期化ベクターを使用して、クライアントデータが暗号化されます。初期化ベクターは、バックアップイメージのヘッダーに格納されます。

以前のパスフレーズは、これらのパスフレーズで暗号化されたバックアップのリストア用のファイルでは利用可能な状態のままです。

注意: 新しいパスフレーズか以前に使用されたパスフレーズかどうかにかかわらず、パスフレーズが安全で取得可能であることを確認する必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

クライアントマシンの管理者に対してだけ、鍵ファイルのアクセスを可能にする必要があります。UNIX クライアントの場合、次のことを確認する必要があります。

- 所有者が root ユーザーである。
- アクセス権モード設定が 600 である。
- ファイルは NFS マウントが可能なファイルシステムには存在しない。

鍵ファイルのリストアの推奨する実施例

暗号化されたバックアップに利用可能な鍵ファイルがない場合でも、鍵ファイルをリストアできることがあります。

鍵ファイルのパスフレーズを保護するための手作業による保存

手作業による保存は、鍵ファイルのパスフレーズを保護する最も安全な方法です。

`bpkeyutil` コマンドを使用してフレーズを追加する際に、次のように手作業による保存を実行します。

- フレーズを紙に書きます。
- 紙を封筒に入れて封印します。
- 安全な場所に封筒を保管します。

鍵ファイルを消失した場合、後で暗号化されたバックアップからリストアするには、次の手順を実行します。

- NetBackup を再インストールします。
- `bpkeyutil` コマンドを実行し、安全な場所からパスフレーズを取り出して新しい鍵ファイルを作成します。

鍵ファイルの自動バックアップ

自動バックアップはセキュリティが低い方法ですが、鍵ファイルのバックアップコピーを確実に保存できます。

この方法では、暗号化されていないポリシーを作成して、鍵ファイルをバックアップする必要があります。鍵ファイルが消失した場合、暗号化されていないバックアップから鍵ファイルをリストアできます。

この方法の問題点は、クライアントの鍵ファイルが、異なるクライアントによってリストアされることです。

鍵ファイルのクライアントへのバックアップを行わない場合、鍵ファイルのパス名をクライアントのエクスクルードリストに追加します。

リダイレクトリストアでは、リストアを実行するために特別な構成の変更が必要です。

暗号化されたバックアップファイルの、異なるクライアントへのリストア

次に、リダイレクトリストアの手順について説明します。

暗号化されたバックアップを異なるクライアントにリストアする方法

1. サーバーは、リダイレクトリストアを実行できる必要があります。また、ユーザーはリダイレクトリストアを実行するために認証されている必要があります。

   リダイレクトリストアについて詳しくは、『NetBackup 管理者ガイド Vol 1』を参照してください。

2. 暗号化されたバックアップが作成されたときに、他のクライアントで使用されたパスフレーズを取得します。このパスフレーズがないと、ファイルをリストアすることはできません。

   両方のクライアントで同じパスフレーズが使用されている場合は、手順 5 に進んでください。

3. 現在の鍵ファイルを保存するために、鍵ファイルを移動するか、ファイル名を変更します。

4. `bpkeyutil` コマンドを実行して他のクライアントに一致する鍵ファイルを作成します。`bpkeyutil` プロセスでパスフレーズを入力するように求められたら、他のクライアントのパスフレーズを指定します。

5. 他のクライアントにファイルをリストアします。

   暗号化されたファイルをクライアントからリストアしたら、手順 4 で作成した鍵ファイルの名前を変更するか、ファイルを削除します。

   次に、元の鍵ファイルを元の場所または元の名前に戻します。鍵ファイルを元の場所および元の名前に戻さないと、暗号化されたバックアップをリストアできない場合があります。

クライアントでの標準暗号化の直接的な構成について

次の項で説明するとおり、クライアントで直接 NetBackup Encryption を構成することもできます。

- ポリシーでの標準暗号化属性の設定
  p.270 の「ポリシーでの標準暗号化属性の設定」を参照してください。
- サーバーからのクライアントの暗号化設定の変更
  p.270 の「NetBackup サーバーからのクライアントの暗号化設定の変更」を参照してください。

ポリシーでの標準暗号化属性の設定

次のように、NetBackup ポリシーに暗号化属性を設定する必要があります。

- この属性を設定した場合、NetBackup サーバーは、ポリシーで定義された NetBackup クライアントに暗号化されたバックアップの実行を要求します。
- この属性を設定していない場合、NetBackup サーバーは、そのポリシー内で定義されている NetBackup クライアントに暗号化されたバックアップの実行を要求しません。

NetBackup 管理コンソールでポリシーの［属性 (Attributes)］タブを使用して、ポリシーの暗号化属性を設定または設定解除することができます。

ポリシーの構成方法について詳しくは、『Symantec NetBackup 管理者ガイド Vol. 1』を参照してください。

NetBackup サーバーからのクライアントの暗号化設定の変更

NetBackup サーバー上の［クライアントプロパティ (Client Properties)］ダイアログボックスから、NetBackup クライアントの暗号化設定を変更することができます。

NetBackup サーバーからクライアントの暗号化設定を変更する方法

1. サーバー上で NetBackup 管理コンソールを開きます。
2. ［ホストプロパティ (Host Properties)］>［クライアント (Clients)］を展開します。

3 ［クライアント (Clients)］リストで、変更するクライアントの名前をダブルクリックします。［クライアントプロパティ (Client Properties)］ウィンドウが表示されます。

4 ［プロパティ (Properties)］>［暗号化 (Encryption)］を展開してそのクライアントの暗号化設定を表示します。

［暗号化 (Encryption)］ペインの設定に対応する構成オプションについては、次の項を参照してください。

p.264 の「標準暗号化の構成オプションの管理」を参照してください。

設定について詳しくは、ウィンドウの［ヘルプ (Help)］ボタンをクリックするか、または『NetBackup 管理者ガイド Vol 1』を参照してください。

レガシー暗号化の構成について

このトピックは NetBackup レガシー暗号化の構成を説明します。

構成オプションは、UNIX クライアント上の `bp.conf` ファイル、または Windows クライアント上のレジストリ内に存在します。

オプションは次のとおりです。

- CRYPT_OPTION
- CRYPT_STRENGTH
- CRYPT_LIBPATH
- CRYPT_KEYFILE

また、NetBackup 管理コンソールを使用して、サーバーからオプションを構成することもできます。これらのオプションは、［クライアントプロパティ (Client Properties)］ダイアログボックスの［暗号化 (Encryption)］タブに表示されます。

詳しくは、『Symantec NetBackup 管理者ガイド Vol. 1』を参照してください。

`bpinst -LEGACY_CRYPT` コマンドに CRYPT_OPTION および CRYPT_STRENGTH オプションを設定することができます。それぞれの構成オプションと同等のオプションは、-crypt_option および -crypt_strength です。

サーバーからのレガシー暗号化の構成について

サーバーから `bpinst` コマンドを実行して、多くの NetBackup クライアントを暗号化用に構成できます。

この方法の前提条件は次のとおりです。

- NetBackup クライアントソフトウェアは、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。

サポートされるプラットフォームについて詳しくは、『Symantec NetBackup リリースノート UNIX、Windows および Linux』を参照してください。

- NetBackup クライアントは、リリース 7.0 以上の NetBackup を実行している必要があります。
- クラスタサーバーが NetBackup Encryption のクライアントである場合、クラスタ内のすべてのノードが同じ鍵ファイルを持っていることを確認します。

bpinst コマンドは、サーバー上の NetBackup の bin ディレクトリに次のようにロードされます。

- Windows サーバーの場合、bin ディレクトリは次のとおりです。

  install_path¥NetBackup¥bin

- UNIX サーバーの場合、bin ディレクトリは次のとおりです。

  /usr/openv/netbackup/bin

bpinst コマンドで利用で可能なオプションについて詳しくは、『NetBackup コマンドリファレンスガイド』で bpinst コマンドの説明を参照してください。

bpinst の使用法の例

p.274 の「クライアントへのレガシー暗号化構成のプッシュインストールについて」を参照してください。

p.275 の「クライアントへのレガシー暗号化パスフレーズのプッシュインストールについて」を参照してください。

通常、bpinst コマンドでクライアント名を指定します。ただし、-policy_names オプションを指定した場合、代わりにポリシー名を指定する必要があります。このオプションは、指定したポリシーのすべてのクライアントに影響します。

レガシー暗号化構成オプション

次の表は NetBackup クライアントのレガシー暗号化関連の構成オプションを含んでいます。これらのオプションが、クライアントに適切な値に設定されていることを確認します。これらのオプションは、サーバーからクライアント名に対して bpinst -LEGACY_CRYPT コマンドを実行して設定します。

表 7-6　レガシー暗号化構成オプション

オプション	値	説明
CRYPT_OPTION = *option*		NetBackup クライアントに、暗号化オプションを定義します。*option* に指定可能な値は、次のとおりです。

オプション	値	説明
	denied|DENIED	クライアントが暗号化されたバックアップを許可しないように設定します。サーバーが暗号化されたバックアップを要求すると、エラーであると判断されます。
	allowed|ALLOWED	(デフォルト値) クライアントが暗号化されたバックアップまたは暗号化されないバックアップを許可するように指定します。
	required|REQUIRED	クライアントが暗号化されたバックアップを要求するように設定します。サーバーが暗号化されないバックアップを要求すると、エラーであると判断されます。
CRYPT_KIND = *kind*		NetBackup クライアントに、暗号化の種類を定義します。*kind* に指定可能な値は、次のとおりです。
	NONE	標準暗号化またはレガシー暗号化のどちらも、クライアント上では構成されません。
	LEGACY	レガシーの 40 ビット DES または 56 ビット DES 暗号化形式を指定します。このオプションは、レガシー暗号化形式がクライアント上で構成されている場合および標準暗号化形式が構成されていない場合のデフォルトです。
	STANDARD	128 ビット暗号化または 256 ビット暗号化のいずれかの暗号化形式を指定します。
CRYPT_STRENGTH = *strength*		NetBackup クライアントに、暗号化の強度を定義します。*strength* に指定可能な値は、次のとおりです。
	des_40|DES_40	(デフォルト値) 40 ビット DES 暗号化を指定します。
	des_56|DES_56	56 ビット DES 暗号化を指定します。
CRYPT_LIBPATH = *directory_path*		NetBackup クライアントに、暗号化ライブラリを含むディレクトリを定義します。 *install_path* は NetBackup がインストールされるディレクトリで、デフォルトでは C:¥VERITAS です。
	/usr/openv/lib/	UNIX システムでのデフォルト値。
	install_path¥NetBackup¥bin¥	Windows システムのデフォルト値
CRYPT_KEYFILE = *file_path*		NetBackup クライアントに、暗号化鍵を含むファイルを定義します。

オプション	値	説明
	/usr/openv/netbackup/keyfile	UNIX システムでのデフォルト値。
	install_path¥NetBackup¥bin¥keyfile.dat	Windows システムのデフォルト値。

クライアントへのレガシー暗号化構成のプッシュインストールについて

NetBackup クライアントで暗号化に関連する構成を設定するには、次に示すように bpinst コマンドで -crypt_option および -crypt_strength オプションを使用します。

- -crypt_option オプションは、クライアントが暗号化されたバックアップを拒否する (denied) か、暗号化されたバックアップを許可する (allowed) か、または暗号化されたバックアップを要求する (required) かを指定します。
- -crypt_strength オプションは、クライアントが暗号化されたバックアップに使用する DES 鍵の長さ (40 または 56) を指定します。

暗号化クライアントソフトウェアをインストールし、56 ビットの DES 鍵で暗号化されたバックアップを要求するには、サーバーから次のコマンドを実行します。

```
bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56 ¥
-policy_names policy1 policy2
```

例では、コマンドが長いため UNIX の継続文字 (¥) を使用しています。40 ビットの DES 鍵で暗号化されたバックアップまたは暗号化されていないバックアップのいずれかを許可するには、次のコマンドを実行します。

```
bpinst -LEGACY_CRYPT -crypt_option allowed -crypt_strength des_40 ¥
client1 client2
```

クラスタ環境では、次の操作を実行できます。

- アクティブノードから、クライアントに構成をプッシュインストールします。
- クライアントのリストには、仮想名ではなく各ノードのホスト名を指定します。

メモ: bp.conf 内でのマスターサーバーの USE_VXSS 設定は、AUTOMATIC に設定する必要があります。この設定は、NBAC が有効化されたマスターから、NetBackup が前にインストールされていないホストにプッシュする場合に使用します。この設定は、NBAC で bp.conf 内のマスターサーバー設定 USE_VXSS が有効化されていない場合にも使用します。

クライアントへのレガシー暗号化パスフレーズのプッシュインストールについて

NetBackup クライアントへパスフレーズを送信するには、bpinst コマンドの -passphrase_prompt オプションまたは -passphrase_stdin オプションを使用します。NetBackup クライアントは、パスフレーズを使用して、鍵ファイルのデータを作成または更新します。

鍵ファイルには、次に示すように、クライアントがバックアップを暗号化するための DES 鍵の生成に使用するデータが含まれます。

- -passphrase_prompt オプションを使用すると、0 文字から 62 文字のパスフレーズを入力するプロンプトが表示されます。パスフレーズを入力しても、文字は表示されません。確認のために、パスフレーズを再入力するためのプロンプトがもう一度表示されます。
- -passphrase_stdin オプションを使用すると、標準入力 (STDIN) に、0 文字から 62 文字のパスフレーズを 2 回入力する必要があります。通常、-passphrase_prompt オプションは -passphrase_stdin オプションよりセキュリティが高いのですが、シェルスクリプトで bpinst を使用する場合には -passphrase_stdin の方が便利です。

NetBackup サーバーから標準入力で、client1 という名前のクライアントへのパスフレーズを入力するには、次のようにコマンドを入力します。

```
bpinst -LEGACY_CRYPT -passphrase_stdin client1 <<EOF
This pass phase is not very secure
This pass phase is not very secure
EOF
```

NetBackup サーバーから、client2 という名前のクライアントへのパスフレーズを入力するには、次のようにコマンドを入力します。

```
bpinst -LEGACY_CRYPT -passphrase_prompt client2
Enter new NetBackup pass phrase: ********************
Re-enter new NetBackup pass phrase: ********************
```

新しいパスフレーズは頻繁に入力する必要があります。NetBackup クライアントは、鍵ファイルに古いパスフレーズの情報を保存します。古いパスフレーズから生成された DES 鍵で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: 新しいパスフレーズか以前に使用されたパスフレーズかどうかにかかわらず、パスフレーズが安全で取得可能であることを確認する必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

多くのクライアントに対して、同じパスフレーズを使用するかどうかを決定する必要があります。1 回の bpinst コマンドで、各クライアントにパスフレーズを指定できるため、同じパスフレーズを使用することをお勧めします。同じパスフレーズを使用する場合、クライアント間でリダイレクトリストアを行うこともできます。

メモ: リダイレクトリストアを回避する場合、クライアントごとに別の bpinst コマンドを入力して異なるパスフレーズを指定する必要があります。

クラスタ環境の場合、次の操作を実行できます。

- アクティブノードから、クライアントに構成をプッシュインストールします。
- クライアントのリストには、仮想名ではなく各ノードのホスト名を指定します。

メモ: bp.conf 内でのマスターサーバーの USE_VXSS 設定は、AUTOMATIC に設定する必要があります。この設定は、NBAC が有効化されたマスターから、NetBackup が前にインストールされていないホストにプッシュする場合に使用します。この設定は、NBAC で bp.conf 内のマスターサーバー設定 USE_VXSS が有効化されていない場合にも使用します。

レガシー暗号化鍵ファイルの管理

このトピックでは、レガシー暗号化鍵ファイルの管理について説明します。

メモ: クラスタ内のすべてのノードで同じ鍵ファイルを使用する必要があります。

暗号化バックアップおよびリストアを実行する NetBackup クライアントごとに鍵ファイルが必要です。鍵ファイルには、クライアントがバックアップを暗号化するための DES 鍵の生成に使用するデータが含まれます。

鍵ファイルを管理するには、クライアントで bpkeyfile コマンドを実行します。詳しくは、『NetBackup 子アンドリファレンスガイド』で bpkeyfile コマンドの説明を確認してください。

鍵ファイルが存在しない場合、最初に、鍵ファイルを作成する必要があります。鍵ファイルを作成するには、サーバーからクライアント名に対して bpinst -LEGACY_CRYPT コマンドを実行して、パスフレーズを設定します。

ファイル名は、次に示すように、CRYPT_KEYFILE 構成オプションで指定したファイル名と同じであることが必要です。

- Windows クライアントの場合、デフォルトの鍵ファイル名は次のとおりです。

  install_path¥NetBackup¥bin¥keyfile.dat

- UNIX クライアントの場合、デフォルトの鍵ファイル名は次のとおりです。

  ```
  /usr/openv/netbackup/keyfile
  ```

NetBackup では、鍵ファイルのパスフレーズを使用して DES 鍵が生成され、DES 鍵を使用して鍵ファイルが暗号化されます。

通常、NetBackup アプリケーションにハードコードされている鍵ファイルのパスフレーズを使います。ただし、セキュリティを高めるため、ユーザー独自の鍵ファイルパスフレーズを使用することも可能です。

p.280 の「UNIX 版クライアントのレガシー鍵ファイルの追加によるセキュリティの向上」を参照してください。

メモ: 独自の鍵ファイルパスフレーズを使用しない場合には、新しい鍵ファイルパスフレーズを入力しないでください。代わりに、鍵ファイルの標準パスフレーズを使用して、新しい NetBackup パスフレーズを入力します。

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、鍵ファイルに格納するデータを生成するために使用します。そのデータは、バックアップを暗号化するための DES 鍵の生成に使用します。

鍵ファイルの標準パスフレーズで暗号化された UNIX クライアントでデフォルトの鍵ファイルを作成するには、次のようなコマンドを入力します。

```
bpkeyfile /usr/openv/netbackup/keyfile
Enter new keyfile pass phrase: (standard keyfile pass phrase)
Re-enter new keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: ************************
Re-enter new NetBackup pass phrase: ************************
```

新しい NetBackup パスフレーズは頻繁に入力する必要があります。古いパスフレーズに関する情報は鍵ファイルに保存されています。この方法では、古いパスフレーズから生成された DES 鍵で暗号化された任意の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` コマンドに -change_netbackup_pass_phrase (または -cnpp) オプションを使用します。

Windows クライアントで、新しい NetBackup パスフレーズを入力する場合は、次の例のようなコマンドを入力します。

```
bpkeyfile.exe -cnpp install_path¥NetBackup¥bin¥keyfile.dat
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: **********
Re-enter new NetBackup pass phrase: **********
```

注意: 新しいパスフレーズか以前に使用されたパスフレーズかどうかにかかわらず、パスフレーズが安全で取得可能であることを確認する必要があります。クライアントの鍵ファイルが破損または消失した場合、鍵ファイルを再作成するために以前のすべてのパスフレーズが必要になります。鍵ファイルがないと、パスフレーズによって暗号化されたファイルをリストアすることはできません。

クライアントマシンの管理者に対してだけ、鍵ファイルのアクセスを可能にする必要があります。

UNIX クライアントの場合、次のことを確認する必要があります。

- 所有者が root ユーザーである。
- アクセス権モード設定が 600 である。
- ファイルは NFS マウントが可能なファイルシステムには存在しない。

ご使用の鍵ファイルをバックアップするかどうかを検討する必要があります。暗号化されたバックアップの場合、鍵ファイルがクライアント上にすでに存在すると、鍵ファイルのリストアだけが実行されるため、このようなバックアップは効果的ではありません。代わりに、クライアントの鍵ファイルに対して、暗号化しないバックアップを行う NetBackup ポリシーを設定することができます。このポリシーは鍵ファイルの緊急リストアが必要な場合に有効です。ただし、この方法では、クライアントの鍵ファイルが異なるクライアント上にリストアされます。

鍵ファイルのバックアップを行わない場合、鍵ファイルのパス名をクライアントのエクスクルードリストに追加します。

別のクライアントで作成されたレガシー暗号化が使用されたバックアップのリストア

サーバーでリダイレクトリストアを実行できる場合、ユーザーはリダイレクトリストアを実行するために認証されている必要があります。

リダイレクトリストアについて詳しくは、『NetBackup 管理者ガイド Vol 1』を参照してください。

異なるクライアントで作成された、暗号化されたバックアップをリストアする方法

1. 暗号化されたバックアップが作成されたときに、他のクライアントで使用されたパスフレーズを取得します。このパスフレーズがないと、ファイルをリストアすることはできません。

   両方のクライアントで同じパスフレーズが使用されている場合は、手順 4 に進んでください。

2. 現在の鍵ファイルを保存するために、鍵ファイルを移動するか、ファイル名を変更します。

3 bpkeyfile コマンドを実行して他のクライアントに一致する鍵ファイルを作成します。bpkeyfile プロセスでパスフレーズを入力するように求められたら、他のクライアントのパスフレーズを指定します。

```
bpkeyfile -change_key_file_pass_phrase key_file_path
```

key_file_path は、クライアント上の新しい鍵ファイルのパスです。この鍵ファイルは他のクライアントの鍵ファイルと一致します。

コマンドを入力した後、bpkeyfile ではクライアントのパスフレーズ (手順 1 で取得) を入力するプロンプトが表示されます。

bpkeyfile について詳しくは、『NetBackup コマンドリファレンスガイド』を参照してください。

4 他のクライアントにファイルをリストアします。

暗号化されたファイルをクライアントからリストアしたら、手順 3 で作成した鍵ファイルの名前を変更するか、ファイルを削除します。

次に、元の鍵ファイルを元の場所または元の名前に戻します。鍵ファイルを元の場所および元の名前に戻さないと、暗号化されたバックアップをリストアできない場合があります。

ポリシーでのレガシー暗号化属性の設定について

次に示す動作に基づいて、NetBackup ポリシーに暗号化属性を設定する必要があります。

- この属性を設定した場合、NetBackup サーバーは、ポリシーで定義された NetBackup クライアントに暗号化されたバックアップの実行を要求します。
- この属性を設定していない場合、NetBackup サーバーは、そのポリシー内で定義されている NetBackup クライアントに暗号化されたバックアップの実行を要求しません。

NetBackup 管理コンソールでポリシーの［属性 (Attributes)］タブを使用して、ポリシーの暗号化属性を設定または設定解除することができます。

ポリシーの構成方法について詳しくは、『Symantec NetBackup 管理者ガイド Vol. 1』を参照してください。

また、bpinst コマンドを実行して、NetBackup ポリシーの暗号化属性を設定または設定解除することもできます。この方法は、複数のポリシーに対して属性を設定または設定解除する場合に便利です。

たとえば、NetBackup サーバーから、policy1 および policy2 に対して暗号化属性を設定するには、次のようにコマンドを入力します。

```
bpinst -LEGACY_CRYPT -policy_encrypt 1 -policy_names policy1 policy2
```

パラメータ 1 は暗号化属性を設定します (0 は設定を解除します)。

サーバーからのクライアントのレガシー暗号化設定の変更

NetBackup サーバー上の[クライアントプロパティ (Client Properties)]ダイアログボックスから、NetBackup クライアントの暗号化設定を変更することができます。

NetBackup サーバーからクライアントの暗号化設定を変更する方法

1. サーバーの NetBackup 管理コンソールで、[ホストプロパティ (Host Properties)] >[クライアント (Clients)]を展開します。
2. [クライアント (Clients)]リストで、変更するクライアントの名前をダブルクリックします。[クライアントプロパティ (Client Properties)]ダイアログボックスが表示されます。
3. [プロパティ (Properties)]ペインで、[暗号化 (Encryption)]をクリックして、クライアントの暗号化設定を表示します。

   設定の詳細な説明については、ダイアログボックスの[ヘルプ (Help)]オプションをクリックするか、または次を参照してください。『Symantec NetBackup 管理者ガイド Vol. 1』。

UNIX 版クライアントのレガシー鍵ファイルの追加によるセキュリティの向上

この項は、UNIX 版 NetBackup クライアントだけに適用されます。セキュリティを強化する機能は、Windows クライアントでは利用できません。

メモ: 鍵ファイルのセキュリティを強化する機能は、クラスタ内で使用しないことをお勧めします。

暗号化クライアントの鍵ファイルは、鍵ファイルのパスフレーズから生成された DES 鍵を使用して暗号化されます。デフォルトでは、鍵ファイルは、NetBackup にハードコードされている鍵ファイルの標準パスフレーズから生成された DES 鍵を使って暗号化されます。

鍵ファイルの標準パスフレーズを使用すると、暗号化されていないバックアップおよびリストアを実行するのとほぼ同じ方法で暗号化バックアップおよびリストアの自動実行が可能になります。

ただし、認証されていないユーザーがクライアントの鍵ファイルへのアクセス権を取得した場合、この方法では問題が発生する可能性があります。認証されていないユーザーはバックアップに使用する暗号化鍵を解読できるようになり、鍵ファイルを使用して、クライア

ントの暗号化されたバックアップをリストアできる場合があります。このような理由から、クライアントの管理者だけが鍵ファイルにアクセスできるようにする必要があります。

特別な保護用に、鍵ファイルを暗号化するための DES 鍵の生成に鍵ファイルの独自のパスフレーズを使用できます。認証されていないユーザーがこの鍵ファイルへのアクセス権を取得しても、リストアすることはより困難になります。

鍵ファイルの独自のパスフレーズを使用すると、バックアップおよびリストアは自動化されなくなります。鍵ファイルの独自のパスフレーズを使用した場合、UNIX 版 NetBackup クライアントでは、次のことが行われます。

クライアント上でバックアップまたはリストアを開始するために、NetBackup サーバーはクライアント上の bpcd デーモンに接続して、要求を作成します。

暗号化されたバックアップまたはリストアを実行するには、bpcd は鍵ファイルを復号化して読み込む必要があります。

鍵ファイルの標準パスフレーズが使用されている場合、bpcd は鍵ファイルを自動的に復号化できます。

ユーザー独自の鍵ファイルパスフレーズが使用されている場合、bpcd では自動的に鍵ファイルは復号化されません。また、デフォルトの bpcd は使用できません。特別なパラメータを使用して bpcd を開始してください。p.281 の「bpcd -keyfile コマンドの実行」を参照してください。

メモ: クラスタ環境では、1 つのノードの鍵ファイルを変更した場合、すべてのノードの鍵ファイルを同じように変更する必要があります。

---

bpcd -keyfile コマンドの実行

この項では、bpcd コマンドをスタンドアロンプログラムとして実行する方法について説明します。

bpcd をスタンドアロンプログラムとして実行する方法

1 次の例のように bpkeyfile コマンドで -change_key_file_pass_phrase (または -ckfpp) オプションを使用し、鍵ファイルのパスフレーズを変更します。

```
bpkeyfile -ckfpp /usr/openv/netbackup/keyfile
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new keyfile pass phrase: (standard keyfile pass phrase)
******
Re-enter new keyfile pass phrase: (standard keyfile pass
phrase) ******
```

Enter キーを押すと、NetBackup で鍵ファイルの標準パスフレーズが使用されます。

2 bpcd -terminate コマンドを実行して、既存の bpcd を停止します。

3 -keyfile オプションを指定して bpcd コマンドを起動します。プロンプトが表示されたら、鍵ファイルの新しいパスフレーズを入力します。

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

bpcd はバックグラウンドで実行され、NetBackup サーバーからの要求を待ちます。

bpkeyfile コマンドに -ckfpp オプションを指定すると、鍵ファイルのパスフレーズをいつでも変更できます。新しい鍵ファイルのパスフレーズは、次に bpcd を起動したときに有効になります。

バックアップを暗号化するための DES 鍵の生成に使用する NetBackup パスフレーズを変更することもできます。bpkeyfile コマンドに -cnpp オプションを指定して、このパスフレーズをいつでも変更できます。ただし、新しい NetBackup パスフレーズは、現行の bpcd プロセスを終了して、bpcd を再起動したときに有効になることに注意してください。

UNIX クライアントでの bpcd の終了

UNIX クライアントで bpcd を終了するには、bpcd -terminate コマンドを使用します。

オプション 2 - メディアサーバーの暗号化

NetBackup メディアサーバーの暗号化は次の場合に最適です。

- メディアサーバーで圧縮と暗号化の負荷を処理できる場合
- NetBackup 管理者が大まかな鍵管理を集中的に行う場合
- NetBackup 操作の密接な統合が必要でない場合

メディアサーバー暗号化オプション管理

この項では、メディアサーバーの暗号化管理について説明します。

メディアサーバー暗号化オプションの管理についての情報は、他のサポートドキュメントにあります。『NetBackup Media Server Encryption Option 管理者ガイド』と『NetBackup Media Server Encryption Option リリースノート』はシマンテック社のサポート Web サイトの次の場所で見つけることができる個別のドキュメントです。

www.symantec.com/business/support/index?page=content&id=DOC4879

8

格納するデータのキーマネージメントサービス

この章では以下の項目について説明しています。

- FIPS (連邦情報処理標準)
- FIPS 対応 KMS について
- キーマネージメントサービス (Key Management Service: KMS) の概要
- KMS の注意事項
- KMS の操作原理
- 暗号化テープへの書き込みの概要
- 暗号化テープの読み取りの概要
- KMS の用語
- KMS のインストール
- KMS の NBAC との使用
- HA クラスタに使用する KMS のインストールについて
- クラスタでの KMS サービスの有効化
- KMS サービスの監視の有効化
- KMS サービスの監視の無効化
- 監視対象リストからの KMS サービスの削除
- KMS の構成

- キーデータベースの作成
- キーグループとキーレコードについて
- キーグループの作成について
- キーレコードの作成について
- キーレコードの状態の概要
- キーレコードの状態に関する注意事項
- キーレコードの prelive 状態
- キーレコードの active 状態
- キーレコードの inactive 状態
- キーレコードの deprecated 状態
- キーレコードの terminated 状態
- KMS データベースファイルのバックアップについて
- すべてのデータファイルのリストアによる KMS のリカバリについて
- KMS データファイルのみのリストアによる KMS のリカバリ
- データ暗号化キーの再生成による KMS のリカバリ
- KMS データファイルのバックアップに関する問題
- KMS データベースファイルのバックアップソリューション
- キーレコードの作成
- 主要グループからのキーのリスト
- KMS と連携するための NetBackup の構成
- NetBackup および KMS のキーレコード
- テープ暗号化を使用するための Netbackup の設定例
- 暗号化への KMS の使用について
- 暗号化テープバックアップの実行例
- 暗号化バックアップの確認例
- KMS 暗号化イメージのインポートについて
- KMS データベースの要素

- 空の KMS データベースの作成
- KPK ID および HMK ID の重要性
- HMK および KPK の定期的な更新について
- KMS キーストアおよび管理者キーのバックアップ
- コマンドラインインターフェース (CLI) コマンド
- CLI の使用方法のヘルプ
- 新しいキーグループの作成
- 新しいキーの作成
- キーグループの属性の変更
- キーの属性の変更
- キーグループの詳細の取得
- キーの詳細の取得
- キーグループの削除
- キーの削除
- キーのリカバリ
- KMS データベースからのキーのエクスポートと KMS データベースへのキーのインポートについて
- ホストマスターキー (HMK) の変更
- ホストマスターキー (HMK) ID の取得
- キーの保護キー (KPK) ID の取得
- キーの保護キー (KPK) の変更
- キーストアの統計の取得
- KMS データベースの静止
- KMS データベースの静止解除
- キーの作成オプション
- KMS のトラブルシューティング
- バックアップが暗号化されていない問題の解決方法

- リストアが復号化されない問題の解決方法
- トラブルシューティングの例 - active キーレコードが存在しない場合のバックアップ
- トラブルシューティングの例 - 不適切なキーレコード状態でのリストア

FIPS (連邦情報処理標準)

FIPS (連邦情報処理標準) には米国連邦政府とカナダ政府のコンピュータシステムに対するセキュリティと相互運用性の必要条件が定義されています。FIPS 140-2 標準には暗号化モジュールのセキュリティ必要条件が明記されています。対称キー暗号化と非対称キー暗号化、メッセージ認証、ハッシュの承認済みセキュリティ機能について説明しています。

FIPS 140-2 標準とその検証プログラムについて詳しくは、http://csrc.nist.gov/groups/STM/cmvp で、米国標準技術研究所 (NIST) とカナダの通信セキュリティ機構 (CSEC) の暗号化モジュール検証プログラム Web サイトを参照してください。

NetBackup 暗号化モジュールが FIPS* で検証されるようになりました。NetBackup KMS は NetBackup 暗号化モジュールを使うので FIPS モードで操作できるようになりました。p.287 の「FIPS 対応 KMS について」を参照してください。

* FIPS 証明書についてはまだ導入されていません。

FIPS 対応 KMS について

NetBackup KMS は FIPS モードに対応できるようになりました。このモードでは、作成する暗号化キーが常に FIPS 承認になります。FIPS 設定はデフォルトでは有効です。

メモ: FIPS 暗号化は NetBackup 7.7 以降のバージョンでサポートされています。

7.7 以降のバージョンで作成されたキーはすべて FIPS 承認済みとなります。アップグレード時、旧バージョンの NetBackup を使用して作成されていたキーは FIPS 承認になりません。NetBackup 7.7 以降のバージョンを使用して作成されたキーグループに移動した場合でも、キーは FIPS 承認キーに変換されません。

7.7 以降のバージョンを使って新しいキーを作成すると、常に新しいキーとともに Salt が生成されます。キーのリカバリには Salt 値の指定が必須です。

たとえば、次の例を考えてみます。`hrs09to12hrs` は、NetBackup の旧バージョンを使用して作成されたキーです。

```
Key Group Name : ENCR_Monday

Supported Cipher : AES_256
```

```
Number of Keys : 8

Has Active Key : Yes

Creation Time : Wed Feb 25 22:46:32 2015

Last Modification Time: Wed Feb 25 22:46:32 2015

Description : -

Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Wed Feb 25 23:14:18 2015

Description : active
```

NetBackup 7.7 へのアップグレード後、キー hrs09to12hrs がキーグループ ENCR_Monday から新しいキーグループ ENCR_77 に移動します。

```
C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd>nbkmsutil -modifykey
-keyname hrs09to12hrs -kgname ENCR_Monday -move_to_kgname ENCR_77

Key details are updated successfully
```

ここで、ENCR_77 キーグループのすべてのキーのリストを表示してください。新しいキー Fips77 は FIPS 承認済みになりますが、旧バージョンの NetBackup を使って作成された hrs09to12hrs は FIPS 承認済みにはなっていません。

```
C:¥Program Files¥Veritas¥NetBackup¥bin¥admincmd>nbkmsutil -listkeys
-kgname NCR_77

Key Group Name : ENCR_77 Supported

Cipher : AES_256

Number of Keys : 2

Has Active Key : Yes

Creation Time : Thu Feb 26 04:44:12 2015

Last Modification Time: Thu Feb 26 04:44:12 2015

Description : -

Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9
```

```
Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : No

Key Tag :
4590e304aa53da036a961cd198de97f24be43b212b2a1091f896e2ce3f4269a6

Key Name : Fips77

Current State : INACTIVE

Creation Time : Thu Feb 26 04:44:58 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : Yes

Salt : 53025d5710ab36ac1099194fb97bad318da596e27fdfe1f2

Number of Keys: 2
```

新しいキー `Fips77` は FIPS 承認済みになり、Salt 値も有します。

FIPS コンプライアンス付き KMS は次のプラットフォームでサポートされます。

- MS Windows Server 2012
- Linux.2.6.16 x86-64 Suse-10
- Linux.2.6.18 x86-64 RHEL-5
- HP-UX IA-64 11.31
- AIX 5.3 TL12 SP2
- AIX 5.3 TL12 SP2

キーマネージメントサービス (Key Management Service: KMS) の概要

NetBackup キーマネジメントサービス (KMS) 機能は NetBackup Enterprise Server と NetBackup サーバーソフトウェアの一部として含まれています。この機能を使うために追加のライセンスは必要ありません。KMS は NetBackup で実行される、マスターサー

バーベースの対称キー管理サービスです。KMS は、T10 規格に準拠するテープドライブの対称暗号化キーを管理します。KMS は、ボリュームプールベースのテープ暗号化を使用するように設計されています。KMS は、組み込みのハードウェア暗号化機能を持つテープハードウェアで使用されます。組み込みの暗号化機能を持つテープドライブの例は、IBM ULTRIUM TD4 カートリッジドライブです。KMS は NetBackup AdvancedDisk ストレージソリューションと関連付けられるディスクボリュームでも使われます。KMS はクラウドストレージプロバイダと一緒に実行します。KMS は、Windows および UNIX 上で実行されます。KMS では、パスコードからキーが生成されるか、または自動的にキーが生成されます。KMS 操作は KMS コマンドラインインターフェース (CLI) またはクラウドストレージサーバーの構成ウィザード (KMS をクラウドストレージプロバイダと一緒に使用する場合) によって実行します。CLI オプションは、`nbms` および `nbmkmsutil` の両方で利用可能です。

KMS は、既存の NetBackup 操作システム管理に与える影響を最小限に留めながら、将来キーマネージメントサービスを拡張するための基盤を提供します。

KMS の注意事項

次の表に、KMS の機能および使用に関する注意事項を示します。

表 8-1 KMS の機能および使用に関する注意事項

注意事項	説明
新しい NBKMS サービス	`nbkms` サービスはメディアサーバーの BPTM プロセスに暗号化キーを提供する、マスターサーバーベースのサービスです。
新しい `nbkmsutil` KMS 構成ユーティリティ	セキュリティ上の理由のため、KMS 構成ユーティリティは、root または管理者としてマスターサーバーからのみ実行可能です。
NetBackup の大幅な変更	次の処理を可能にするために、NetBackup の変更が必要でした。 ■ ボリュームプール名で `ENCR_` 接頭辞を使用できるようにするため。 ■ キーマネージメントサービスと通信するため。 ■ 暗号化が埋め込まれた T10 / SCSI 規格のテープドライブをサポートするため。 ■ NetBackup イメージ情報への暗号化キータグの追加を通知するように NetBackup GUI および CLI を変更 `bpimmedia` および `bpimagelist` が変更されました。 ■ この NetBackup リリースのリカバリ能力および使用しやすさを強化 すべての暗号化キーをパスフレーズを使って生成することをお勧めします。パスフレーズを入力すると、キーマネージメントシステムによって、そのパスフレーズから再作成可能な暗号化キーが作成されます。

注意事項	説明
KMS のインストールおよび配置の決定	次に KMS の配置について決定する必要のある事項を示します。 ■ KMS のランダムに生成されたキーまたはパスフレーズで生成されたキーのどちらを選択するか ■ NBAC の配置を含めるかどうか
KMS のセキュリティ	既存の NetBackup サービスに追加されるセキュリティ上の問題はありません。
暗号形式	KMS では、次の暗号形式がサポートされています。 ■ AES_128 ■ AES_192 ■ AES_256 (デフォルトの暗号)
KMS のリカバリ能力	KMS を使って、すべての暗号化キーをパスフレーズから生成できます。これらのパスフレーズを記録して、NetBackup の KMS 全体を再作成するために後で使うことができます。
KMS ファイル	次のような KMS に関連する KMS ファイルがあり、キーに関する情報が維持されます。 ■ キーファイルまたはキーデータベース データ暗号化キーが含まれます。キーファイルは、/opt/openv/kms/db/KMS_DATA.dat にあります。 ■ ホストマスターキー AES 256 を使用して KMS_DATA.dat キーファイルを暗号化および保護する暗号化キーが含まれます。ホストマスターキーは、/opt/openv/kms/key/KMS_HMKF.dat にあります。 ■ キーの保護キー AES 256 を使用して KMS_DATA.dat キーファイルの個々のレコードを暗号化および保護する暗号化キーです。キーの保護キーは、/opt/openv/kms/key/KMS_KPKF.dat にあります。現在は、すべてのレコードを暗号化するために同じキーの保護キーが使用されます。 ■ KMS ファイルのバックアップ KMS ファイルをバックアップする場合には、推奨される方法に従ってください。KMS データベースファイルを置くテープは、HMK ファイルおよび KPK ファイルを置くテープと別にします。すると、暗号化のテープにアクセスするためには、両方のテープが必要となります。 また、KMS のデータファイルのバックアップを、NetBackup の通常の処理とは別に行うという方法もあります。これらのファイルを、別々の CD、DVD、または USB ドライブにコピーできます。 パスフレーズで生成された暗号化キーを使って手動で KMS を再構築することもできます。暗号化キーはすべてパスフレーズで生成できます。暗号化キーのパスフレーズのすべてを記録している場合には、書き留めた情報から KMS を手動で再作成することができます。生成した暗号化キーが数個しかない場合は、この処理には時間はかかりません。

注意事項	説明
キーレコード	キーレコードには多数のフィールドが含まれますが、主要なレコードは、暗号化キー、暗号化キータグおよびレコードの状態です。また、キーレコードにはいくつかのメタデータも含まれます。 これらのキーレコードは次のように定義されます。 ■ 暗号化キー このキーは、テープドライブに指定されます。 ■ 暗号化キータグ このタグは、暗号化キーの識別子です。 ■ レコードの状態 各キーレコードには状態があります。状態は、prelive、active、inactive、deprecated および terminated です。 ■ メタデータ メタデータには、論理名、作成日、変更日および説明が含まれます。
キーグループ	キーグループはキーレコードの論理名および論理グループです。作成されるすべてのキーレコードはグループに属する必要があります。キーグループには、常に active 状態のキーレコードを 1 つだけ含めることができます。NetBackup 7.5 は 100 のキーグループをサポートします。NetBackup 7.0 は 20 のキーグループをサポートします。キーグループごとに 10 個の暗号化キーのみが許可されます。
テープドライブおよびメディアの機能	ドライブ、テープおよび NetBackup の機能は、ドライブの暗号化が正常に行われるようにすべて適合している必要があります。多数のドライブが T10 規格に準拠しています。対応しているテープドライブ (T10 規格に準拠) のうちよく知られているものには、LT0-4、LT0-5、LT0-6、IBM TS1120/30/40、Oracle T10000B/C などがあります。 読み取りおよび書き込みのために旧バージョンの LTO ドライブを実行することはできますが、データを暗号化することはできません。たとえば、LTO2 メディアを使用している場合、LTO4 ドライブでデータを読み取ることはできますが、暗号化されていない形式でも暗号化されている形式でも書き込みはできません。 暗号化を設定する際は、これらのドライブおよびメディアの問題を常に把握しておくことが必要です。暗号化が可能なドライブが必要なだけでなく、メディアをグループ化して暗号化を実行できるようにする必要があります。後で復号化するために、テープは復号化が可能なドライブに配置する必要があります。 メディアとテープドライブの相互操作性の概要については、表 8-2を参照してください。詳細については、ベンダー固有のユーザーガイドを参照されることをお勧めします。 詳しくは、HOWTO56305 を参照してください。
KMS と NBAC	KMS を NBAC とともに使用する場合については、このマニュアルのさまざまな項で、必要に応じて説明されています。詳しくは、NetBackup の NBAC のマニュアルを参照してください。

注意事項	説明
KMS と HA クラスタ	KMS を HA クラスタとともに使用する場合については、このマニュアルのさまざまな項で、必要に応じて説明されています。詳しくは、NetBackup の HA のマニュアルを参照してください。
KMS ログ	サービスでは新しく統合ログが使用され、サービスに OID 286 が割り当てられています。`nbkmsutil` コマンドでは従来のログが使用され、そのログはファイル `/usr/openv/netbackup/logs/admin/*.log` にあります。
クラウドと KMS	KMS をクラウドプロバイダとともに使用することについては、このマニュアルのさまざまな項で、必要に応じて説明されています。詳しくは、『NetBackup Cloud 管理者ガイド』を参照してください。
AdvancedDisk と KMS	KMS を AdvancedDisk ストレージとともに使用することについては、このマニュアルのさまざまな項で、必要に応じて説明されています。詳しくは、『NetBackup AdvancedDisk ストレージソリューションガイド』を参照してください。
NBAC と KMS の権限	通常 NBAC を使って `Setupmaster` コマンドを実行するとき、NetBackup 関連グループの権限 (たとえば、NBU_Admin と KMS_Admin) が作成されます。デフォルトの root と管理者ユーザーもそれらのグループに追加されます。場合によっては NetBackup が .x から に、または 7.0 から 7.0.1 にアップグレードされるとき、root と管理者レベルのユーザーは KMS グループに追加されません。解決するには、root と管理者レベルのユーザーに NBU_Admin と KMS_Admin の権限を手動で付与します。

表 8-2　暗号化のメディアサポート

メディア (Media)	LT04 テープドライブ	LT05 テープドライブ	LT06 テープドライブ
LTO-2 メディア	読み取り専用暗号化サポート無し	サポートされない	サポートされない
LTO-3 メディア	読み書き暗号化サポートなし	読み取り専用暗号化サポート無し	サポートされない
LTO-4 メディア	読み書き暗号化有効	読み書き暗号化有効	読み取り専用暗号化有効
LTO-5 メディア	サポートされない	読み書き暗号化有効	読み書き暗号化有効
LTO-6 メディア	サポートされない	サポートされない	読み書き暗号化有効

KMS の操作原理

KMS は、暗号化可能なテープドライブと連携して動作します。KMS は、システム管理の観点から NetBackup の使用が複雑にならないような方法で、NetBackup に統合されています。KMS は、組み込みの暗号化機能を使用して、テープドライブに暗号化キーマネージメントを提供します。これらのテープドライブは、SCSI 規格に準拠します。SCSI コマンドによって、テープドライブでの暗号化が可能になります。NetBackup は、ボリュームプール名を使用してこの機能へアクセスします。

暗号化テープへの書き込みの概要

BPTM は、名前に ENCR_ の接頭辞が付いたボリュームプールからのテープへの書き込み要求およびテープの使用要求を受け取ります。ENCR_ 接頭辞は、テープに書き込まれる情報が暗号化されることを BPTM に通知するシグナルです。

BPTM は KMS と通信し、ボリュームプール名に一致する名前のキーグループの暗号化キーを要求します。

KMS は、BPTM に暗号化キーおよびキー識別子 (暗号化キータグとも呼ばれる) を戻します。

BPTM は、ドライブを暗号化モードにして、キータグおよび識別子タグをドライブに登録します。この処理はすべて、SCSI 仕様に追加されている SCSI セキュリティプロトコルの in/out コマンドを使用して行われます。

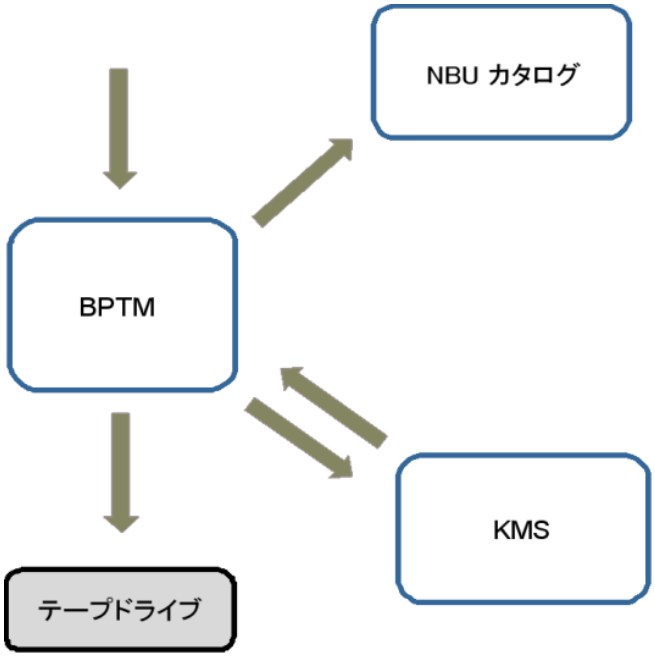
バックアップは通常どおりに処理されます。

バックアップが完了すると、BPTM はキーおよびタグをドライブから登録解除し、ドライブを通常モードに設定し直します。

この後、BPTM は NetBackup イメージレコードカタログにタグを記録します。

図 8-1 に、処理の流れを示します。

図 8-1 暗号化テープへの書き込み処理の流れ



暗号化テープの読み取りの概要

テープの読み取りが行われ、イメージが暗号化されているテープの領域が検出されると、BPTM は使用されているタグを特定し、KMS はそのレコードおよびキーを BPTM にロードします。それから BPTM はドライブにキーを提供し、テープの読み取りが通常どおりに行われます。

KMS の用語

表 8-3 に KMS に関連する用語の定義を示します。

表 8-3　一般的な KMS の用語の定義

用語	定義
コマンドラインインターフェース (Command line interface: CLI)	CLI では、指定されたコマンドラインから nbkmsutil コマンドを使用して、KMS の機能を操作できます。 CLI を使用して、新しいキーグループの作成、新しいキーの作成、キーグループ属性の変更、キー属性の変更、キーグループの詳細の取得を実行できます。キーの詳細の取得、キーグループの削除、キーの削除、キーのリカバリ、ホストマスターキーの変更、ホストマスターキー ID の取得を実行することもできます。さらに、キーの保護キーの変更、キーの保護キー ID の取得、キーストアの統計の取得、KMS データベースの静止、KMS データベースの静止解除を実行できます。
ホストマスターキー (Host Master Key: HMK)	ホストマスターキーには、AES 256 を使用して KMS_DATA.dat キーファイルを暗号化および保護する暗号化キーが含まれます。ホストマスターキーは、/opt/openv/kms/key/KMS_HMKF.dat にあります。
キー (Key)	キーとは、データの暗号化および復号化に使用される暗号化キーです。
キーグループレコード (Key group record: KGR)	キーグループレコードには、キーグループの詳細が含まれます。
キーマネージメントサービス (Key Management Service: KMS)	キーマネージメントサービス (KMS) は、マスターサーバーベースの対称キー管理サービスであり、対称暗号化キーを管理します。T10 規格 (LTO4) に準拠しているテープドライブのキーが管理されます。KMS は /usr/openv/netbackup/bin/nbkms にあります。
キーレコード (Key record: KR)	キーレコードには、暗号化キーの詳細が含まれます。
KMS データベース (KMS database)	KMS データベースには、データ暗号化キーが含まれます。
キーの保護キー (Key Protection Key: KPK)	キーの保護キーとは、AES 256 を使用して KMS_DATA.dat キーファイルの個々のレコードを暗号化および保護する暗号化キーです。キーの保護キーは kms/key/KMS_KPKF.dat にあります。現在は、すべてのレコードを暗号化するために同じキーの保護キーが使用されます。
キーファイル (キーデータベース) (Key file (key database))	キーファイルまたはキーデータベースには、データ暗号化キーが含まれます。キーファイルは、/opt/openv/kms/db/KMS_DATA.dat にあります。
キーグループ (Key group)	キーグループとはキーレコードの論理名および論理グループです。キーグループには、常に active 状態のキーレコードを 1 つだけ含めることができます。 100 のキーグループがサポートされます。

用語	定義
キーレコード (Key record)	キーレコードには、暗号化キー、暗号化キータグおよびレコードの状態が含まれます。その他の有効なメタデータ (論理名、作成日、変更日、説明など) も含まれます。
キーレコードの状態 (Key record states)	キーレコードの状態を次に示します。 ■ prelive。キーレコードは作成されていますが、使用されていません。 ■ active。キーレコードは、バックアップおよびリストアの両方で暗号化および復号化に使用できます。 ■ inactive。キーレコードは暗号化には使用できませんが、リストア中に復号化のみに使用できます。 ■ deprecated。キーレコードは暗号化または復号化には使用できません。 ■ terminated。キーレコードは使用できませんが、削除できます。 ■ キーストア (Keystore)。キーストアとはデータ暗号化キーを保持するファイルです。 ■ パスフレーズ。パスフレーズとはユーザー指定のランダムな文字列です。暗号化キーを作成するためのシードです。パスフレーズを使って、またはパスフレーズを使わずに、HMK、KPK および暗号化キーを作成することを選択できます。 **メモ:** 将来的な使用に備え、すべてのパスフレーズを記録し、安全な場所に保管しておいてください。 パスフレーズを使うと、明らかな利点があります。キーのセキュリティ強度が向上します。また、キーを紛失した場合も、元のキーの作成時に使ったパスフレーズを提供することにより、キーを再生成できます。
静止 (Quiesce)	静止とは、KMS データベースを読み取り専用管理者モードに設定することです。静止は、KMS データベースファイルの一貫性のあるコピーのバックアップを作成するために必要です。
タグ (Tag)	タグとは、キーストア内の個々のキーまたはキーグループを特定するために使用される一意の識別子 (UUID) です。

KMS のインストール

次の手順では、KMS のインストール方法について説明します。

メモ: Cloud ストレージ環境で KMS を構成する方法について詳しくは、次を参照してください。『NetBackup Cloud 管理者ガイド』

KMS サービスは `nbkms` と呼ばれます。

サービスは、データファイルが設定されるまで実行されないため、KMS を使用しない環境への影響は最小限に留められます。

KMS をインストールする方法

1. `nbkms -createemptydb` コマンドを実行します。
2. ホストマスターキー（HMK）のパスフレーズを入力します。また、Enter キーを押して、ランダムに生成されるキーを作成することもできます。
3. HMK の ID を入力します。この ID には、HMK を特定するのに使用する、わかりやすい任意の ID を指定できます。
4. キーの保護キー（KPK）のパスフレーズを入力します。
5. KPK の ID を入力します。この ID には、KPK を特定するのに使用する、わかりやすい任意の ID を指定できます。

   ID を入力して Enter キーを押すと、KMS サービスが起動します。
6. 次のコマンドを実行してサービスを起動します。

   ```
   nbkms
   ```
7. 次のように `grep` コマンドを使用してサービスが起動していることを確認します。

   ```
   ps -ef | grep nbkms
   ```
8. キーグループを作成します。キーグループ名はボリュームプール名に一意に一致する必要があります。すべてのキーグループ名には接頭辞 `ENCR_` が付いている必要があります。

   メモ: クラウドストレージでキーマネージメントを使用する場合、キーグループ名に `ENCR_` 接頭辞は必要ありません。

   (クラウド以外のストレージ) キーグループを作成するには、次のコマンド構文を使用します。

   ```
   nbkmsutil -creatkg -kgname ENCR_volumepoolname
   ```

   `ENCR_` 接頭辞は重要です。BPTM は `ENCR_` 接頭辞を含むボリュームプール要求を受け取る場合に、そのボリュームプール名を KMS に渡します。KMS はそれがボリュームプールと完全に一致するかを判別し、そのグループからバックアップ用に active キーレコードを取得します。

   クラウドストレージキーグループを作成するには、次のコマンド構文を使用します。

   ```
   nbkmsutil -creatkg -kgname cloud_provider_URL:volume_name
   ```

9 -createkey オプションを使用してキーレコードを作成します。

```
nbkmsutil -createkey -kgname ENCR_volumepool -keyname keyname -activate -desc "message"
```

キー名およびキーメッセージは任意です。これらは、キーを表示するときにこのキーを特定するのに役立ちます。

-activate オプションは、prelive 状態をスキップしてこのキーを active として作成します。

10 スクリプトでパスフレーズを求められたら、パスフレーズを再入力します。

次の例では、キーグループは ENCR_pool1 と呼ばれ、キー名は Q1_2008_key です。説明部分はこのキーが 1 月、2 月、3 月用のキーであることを示します。

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q1_2008_key -activate -desc "key for
Jan, Feb, & Mar"
```

11 同じコマンドを使用して別のキーレコードを作成できます。別のキー名および説明にすると、キーレコードの区別に役立ちます。

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q2_2008_key -activate -desc "key for
Apr, May, & Jun"
```

メモ: コマンド `nbkmsutil -kgname name -activate` を使用して複数のキーレコードを作成すると、最後のキーのみが active に保たれます。

12 あるキーグループ名に属するすべてのキーを表示するには、次のコマンドを使用します。

```
nbkmsutil -listkeys -kgname keyname
```

メモ: `nbkmsutil` -listkeys コマンドの出力の記録を保管しておくことをお勧めします。キーをリカバリする必要がある場合、出力に表示されるキータグが必要です。

次のコマンドと出力では、この手順の例が使用されています。

```
# nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name        : ENCR_pool1
Supported Cipher      : AES_256
Number of Keys        : 2
Has Active Key        : Yes
Creation Time         : Thu Aug  8 16:23:06 2013
Last Modification Time: Thu Aug  8 16:23:06 2013
Description           : -
 Key Tag    : 825784185f87145c368c54e919908905a45f79927cb733337a53e9b174bbe046
 Key Name              : Q2_2013_key
 Current State         : ACTIVE
 Creation Time         : Thu Aug  8 16:25:19 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Apr, May, & Jun
 FIPS Approved Key     : No

 Key Tag    : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
 Key Name              : Q1_2013_key
 Current State         : INACTIVE
 Creation Time         : Thu Aug  8 16:25:03 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description           : key for Jan, Feb, & March
 FIPS Approved Key     : No
Number of Keys: 2
```

p.301 の「HA クラスタに使用する KMS のインストールについて」を参照してください。

p.301 の「KMS の NBAC との使用」を参照してください。

KMS の NBAC との使用

KMS の導入をサポートするために、次の変更が NBAC に加えられました。

- 新しい認可オブジェクト KMS の追加
- 新しい NetBackup ユーザーグループ NBU_KMS Admin の追加

KMS オブジェクトに対してユーザーが所有する権限によって、KMS 関連の実行可能なタスクが異なります。

表 8-4 に、各 NetBackup ユーザーグループのデフォルトの KMS 権限を示します。

表 8-4 NetBackup ユーザーグループのデフォルトの KMS 権限

セット	動作	NBU_ User	NBU_ Operator	NBU_ Admin	NBU_ Security Admin	Vault_ Operator	NBU_SAN Admin	NBU_ KMS Admin
参照 (Browse)	参照 (Browse)	---	---	X	---	---	---	X
読み込み	読み込み	---	---	X	---	---	---	X
構成	新規	---	---	---	---	---	---	X
構成	削除	---	---	---	---	---	---	X
構成	変更	---	---	---	---	---	---	X

前述の KMS 権限に加えて、NBU_KMS 管理グループはその他の認可オブジェクトに関する次の権限も所有しています。

- BUAndRest は参照、読み取り、バックアップ、リストア、表示権限を所有
- HostProperties は参照、読み取り権限を所有
- License は参照、読み取り権限を所有

HA クラスタに使用する KMS のインストールについて

通常の NetBackup 環境では、一部のオプションパッケージのみがインストール、ライセンス付与または構成されていることがあります。このような状況では、これらのオプション製品に付随するサービスが常に有効でない場合があります。このため、これらのサービスはデフォルトでは監視されず、サービスに障害が発生しても NetBackup はフェールオーバーされません。 将来、オプション製品のインストール、ライセンス取得および構成が行われると、そのサービスに障害が発生した場合に NetBackup をフェールオーバーするようにサービスを手動で構成できます。この項では、クラスタを監視するよう手動で KMS を設定する手順を説明します。

クラスタでの KMS サービスの有効化

監視可能なサービスのリストに KMS サービスを追加し、クラスタで KMS サービスを有効にできます。

クラスタで KMS サービスを有効にする方法

1. クラスタのアクティブノードで、コマンドプロンプトを開きます。
2. 次の場所にディレクトリを変更します。

   Windows の場合:`<NetBackup_install_path>¥NetBackup¥bin`

   UNIX の場合:`/usr/openv/netbackup/bin`
3. 次のコマンドを実行します。

   Windows の場合:`bpclusterutil -addSvc "NetBackup Key Management Service"`

   UNIX の場合:`bpclusterutil -addSvc nbkms`
4. オプション製品固有の手順に従って、製品を有効にします。NetBackup キーマネージメントサービスの場合、コマンドを実行してデータベースを作成し、サービスを起動します。

KMS サービスの監視の有効化

KMS サービスの監視を有効にし、サービスに障害が発生したときに NetBackup をフェールオーバーすることができます。

KMS サービスの監視を有効にし、サービスに障害が発生したときに NetBackup をフェールオーバーする方法

1. クラスタのアクティブノードで、コマンドプロンプトを開きます。
2. 次の場所にディレクトリを変更します。

   Windows の場合: `<NetBackup_install_path>¥NetBackup¥bin`

   UNIX の場合: `/usr/openv/netbackup/bin`
3. 次のコマンドを実行します。

   Windows の場合:`bpclusterutil -enableSvc "NetBackup Key Management Service"`

   UNIX の場合: `bpclusterutil -enableSvc nbkms`

KMS サービスの監視の無効化

KMS サービスの監視を無効にすることができます。

KMS サービスの監視を無効にする方法

1. クラスタのアクティブノードで、コマンドプロンプトを開きます。
2. 次の場所にディレクトリを変更します。

   Windows の場合: `<NetBackup_install_path>¥NetBackup¥bin`

   UNIX の場合: `/usr/openv/netbackup/bin`
3. 次のコマンドを実行します。

   Windows の場合: `bpclusterutil -disableSvc "NetBackup Key Management Service"`

   UNIX の場合: `bpclusterutil -disableSvc nbkms`

監視対象リストからの KMS サービスの削除

KMS サービスを、監視可能なサービスのリストから削除できます。

監視対象サービスのリストから KMS サービスを削除する方法

1. 前述の手順を使用して、オプション製品のサービスの監視を無効にします。
2. オプション製品固有の手順に従って、製品を削除します。
3. クラスタのアクティブノードで、コマンドプロンプトを開きます。
4. 次の場所にディレクトリを変更します。

   Windows の場合: `<NetBackup_install_path>¥NetBackup¥bin`

   UNIX の場合: `/usr/openv/netbackup/bin`
5. 次のコマンドを実行します。

   Windows の場合: `bpclusterutil -deleteSvc "NetBackup Key Management Service"`

   UNIX の場合: `bpclusterutil -deleteSvc nbkms`

KMS の構成

KMS の構成は、キーデータベース、キーグループおよびキーレコードの作成によって行います。その後、KMS と連携するように NetBackup を構成します。

KMS を構成して初期化する方法

1. キーデータベース、ホストマスターキー (HMK) およびキーの保護キー (KPK) を作成します。
2. ボリュームプールと一致するキーグループを作成します。
3. active キーレコードを作成します。

キーデータベースの作成

空のキーデータベースを作成するには、次の手順を使用します。キーデータベースは、`-createemptydb` オプションを指定してサービス名を起動すると作成されます。この処理は、既存のキーデータベースの有無をチェックし、存在しないことを確認してから作成を開始します。KMS の初期化時に、2 つの保護キーを作成する必要があります。ホストマスターキー (HMK) とキーの保護キー (KPK) です。

すべての KMS キーの作成操作と同様に、これらのキーの作成に関しても次のオプションが用意されています。

- パスフレーズによって生成されたキー
- ランダムに生成されたパスフレーズ

各キーに関連付けられる論理 ID の入力を求められます。この操作が終了すると、キーデータベースおよび保護キーが作成されます。

Windows システムの場合は、これらを次のファイルで確認できます。

```
¥Program Files¥Veritas¥kms¥db¥KMS_DATA.dat
¥Program Files¥Veritas¥kms¥key¥KMS_HMKF.dat
¥Program Files¥Veritas¥kms¥key¥KMS_HKPKF.dat
```

UNIX システムの場合は、これらを次のファイルで確認できます。

```
/opt/openv/kms/db/KMS_DATA.dat
/opt/openv/kms/key/KMS_HMKF.dat
/opt/openv/kms/key/KMS_HKPKF.dat
```

メモ: Windows では、次の `nbkms` コマンドは `C:¥Program Files¥Veritas¥NetBackkup¥bin` ディレクトリから実行されます。

キーデータベースを作成する方法

1. 次のコマンドを実行します。

   ```
   nbkms -createemptydb.
   ```

2. ホストマスターキーのパスフレーズを入力するか、または Enter キーを押してランダムに生成されたキーを使います。次のプロンプトでパスフレーズを再入力します。
3. HMK ID を入力します。この ID は HMK に関連付けられ、後でこの特定のキーの確認に使用できます。
4. キーの保護キーのパスフレーズを入力するか、または Enter キーを押してランダムに生成されたキーを使います。次のプロンプトでパスフレーズを再入力します。
5. KPK ID を入力します。この ID は KPK に関連付けられ、後でこの特定のキーの確認に使用できます。
6. KPK ID に 10 と入力します。

キーグループとキーレコードについて

キーグループはキーレコードの論理コレクションで、1 つのレコードだけが active 状態になります。

キーグループの定義は、次の情報で構成されています。

- 名前
  キーグループに付ける名前。キーストア内で一意である必要があります。キーグループの名前の変更は、新しい名前がキーストア内で一意であれば可能です。
- タグ
  一意のキーグループ識別子 (変更不可)。
- 暗号
  サポートされている暗号。このキーグループに属するキーは、すべてこの暗号に基づいて作成されます (変更不可)。
- 説明
  任意の説明 (変更可能)。
- 作成時刻 (Creation Time)
  このキーグループの作成日時 (変更不可)。
- 最終変更日時
  変更可能な属性を最後に変更した日時 (変更不可)。

キーグループの作成について

暗号化を設定する最初の手順は、キーグループを作成することです。

次の例では、キーグループ ENCR_mygroup を作成しています。

```
nbkmsutil -createkg -kgname ENCR_mygroup
```

メモ: このバージョンの KMS では、作成するグループの名前 (たとえば、mygroup) に接頭辞 ENCR_ を付けることが重要です。

キーレコードの作成について

次の手順は、active キーレコードの作成です。キーレコードは prelive 状態で作成してから、active 状態に移すことができます。または、キーレコードは active 状態で直接作成することもできます。

キーレコードは、次の重要な情報で構成されています。

- 名前
  キーに付ける名前。キーグループ内で一意である必要があります。キーの名前の変更は、新しい名前がキーグループ内で一意であれば可能です。
- キータグ
  一意のキー識別子 (変更不可)。
- キーグループタグ
  このキーが属している一意のキーグループ識別子 (変更不可)。
- 状態 (State)
  キーの現在の状態 (変更可能)。
- 暗号化キー
  バックアップまたはリストアデータの暗号化または復号化に使用されるキー (変更不可)。
- 説明
  任意の説明 (変更可能)。
- 作成時刻 (Creation Time)
  キーの作成日時 (変更不可)。
- 最終変更日時
  変更可能な属性を最後に変更した日時 (変更不可)。

キーレコードには次の状態があります。

- prelive。レコードは作成されていますが、使用されていないことを示します。

- active。レコードおよびキーが暗号化と復号化に使用されることを示します。
- inactive。レコードおよびキーを暗号化に使用できないことを示します。ただし、復号化には使用できます。
- deprecated。レコードは暗号化または復号化には使用できないことを示します。
- terminated。レコードを削除できることを示します。

キーレコードの状態の概要

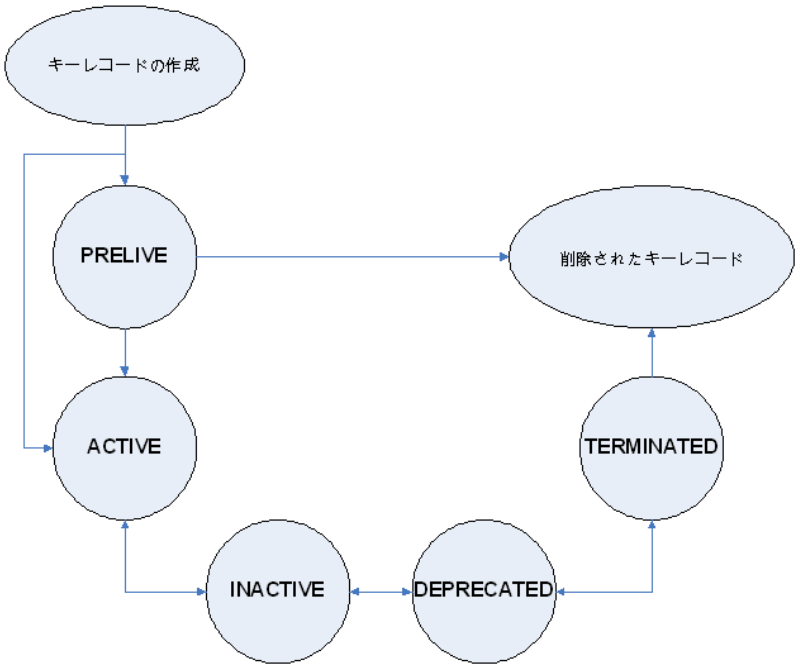
キーレコードの状態には、prelive、active、inactive、deprecated および terminated があります。キーレコードの状態は、キーレコードのライフサイクルに準拠しています。いったんキーが active 状態になると (すなわち、暗号化に使用するように設定されると)、キーはライフサイクルを通じて、適切な順序で遷移する必要があります。適切な順序とは、ある状態からその隣接した状態に移ることです。キーは、いずれかの状態を省略して遷移することはできません。

active 状態と terminated 状態の間では、前後いずれかの方向に一度に 1 つの状態だけ遷移できます。この範囲以外の状態の場合、移行の方向は一方向のみです。削除されたキーレコードはリカバリできません（パスフレーズを使って作成されていない場合）。また、active 状態のキーを prelive 状態に戻すことはできません。

メモ: キーは、prelive 状態または active 状態のいずれかで作成できます。active キーレコードは、バックアップとリストアの両方の操作で使用できます。inactive キーは、リストア操作でのみ使用できます。deprecated キーは、使用できません。キーレコードが deprecated 状態のときに、そのキーレコードを使用してバックアップまたはリストアを実行しようとすると失敗する可能性があります。terminated 状態にあるキーレコードは、システムから削除できます。

次の図に、prelive 状態または active 状態のキーを作成する処理の流れを示します。

図 8-2 キーの作成の状態



キーレコードの状態に関する注意事項

キーレコードの状態に関して次の注意事項に従ってください。

- キーレコードの状態の遷移は明確に定義されているため、キーレコードを削除するにはこれらの状態をすべて経由する必要があります。
- キーレコードを active に設定すると、active 状態のキーレコードはそのグループに対して inactive 状態になります。1 つのグループに存在可能な active レコードは 1 つだけです。
- deprecated 状態は、キーを保存し、キーの使用を制限する場合に便利です。管理者としてキーのセキュリティが低下したと判断した場合は、そのキーをシステムから削除せずに手動でユーザーによるそのキーの使用を一時停止できます。そのキーレコードを deprecated 状態に設定すると、この deprecated キーを使用してバックアップまたはリストアを試みたユーザーにはエラーが表示されるようになります。
- キーレコードの削除は、キーを誤って削除する可能性を減らすために 2 つの手順で構成されています。まず、deprecated キーを terminated に設定する必要があります。その後、そのキーレコードを削除できます。terminated キーレコードのみを削除できます (prelive 状態のキーを除く)。

- 使用前にキーレコードを作成しておく場合には、prelive 状態を使用できます。

キーレコードの prelive 状態

prelive 状態で作成したキーは、active にすることも、削除することもできます。

prelive 状態は、次の場合に使用できます。

- KMS 管理者が、システムに影響を与えずにキーレコードの作成をテストする場合。レコードが正しく作成されたら、そのレコードを active 状態にできます。正しく作成されていなかった場合、そのレコードを削除できます。
- KMS 管理者がキーレコードを作成しておいて、そのレコードを将来のある時点で active 状態にする場合。これは、レコードを active に設定する操作を、KMS キーストアのバックアップ後（またはパスフレーズの記録後）まで延期する場合などです。または、レコードを active に設定する操作を、将来のある時点に延期する場合もあります。
  prelive 状態のキーレコードは、active にすることも、システムから削除することもできます。

キーレコードの active 状態

active キーレコードは、データの暗号化および復号化に使用できます。必要に応じて、active キーレコードを inactive にすることもできます。active 状態は、最も重要な 3 つのデータ管理状態のうちの 1 つです。他の 2 つの重要なデータ管理状態は、inactive 状態および deprecated 状態です。

キーレコードは、prelive 状態を省略して直接 active 状態で作成できます。active 状態のキーレコードは、active のままにするか、inactive に変更できます。active レコードを prelive 状態に戻すことはできません。

キーレコードの inactive 状態

inactive キーレコードは、データの復号化に使用できます。必要に応じて、inactive キーレコードを再度 active にすることも、deprecated 状態に移行させることも可能です。inactive 状態は、最も重要な 3 つのデータ管理状態のうちの 1 つです。他の 2 つの重要なデータ管理状態は、active 状態および deprecated 状態です。

inactive 状態のキーレコードは、inactive のままにするか、active または deprecated に変更できます。

キーレコードの deprecated 状態

deprecated キーレコードは、データの暗号化または復号化に使用できません。必要に応じて、deprecated 状態のキーレコードを inactive または terminated にすることが可能です。deprecated 状態は、最も重要な 3 つのデータ管理状態のうちの 1 つです。他の 2 つの重要なデータ管理状態は、active 状態および inactive 状態です。

deprecated 状態は、次の場合に使用できます。

- キーの使用を追跡または規制する必要がある場合。deprecated キーが適切な状態に変更されないかぎり、このキーの使用を試みても失敗する可能性があります。
- 今後キーが必要になることはないが、念のために terminated 状態に設定しない場合。
  deprecated 状態のキーレコードは、deprecated のままにするか、inactive または terminated に変更できます。

キーレコードの terminated 状態

terminated 状態は、deprecated 状態のキーレコードを削除する場合の 2 番目の手順、つまり安全のための手順となります。terminated キーレコードは、必要に応じて deprecated 状態に移すか、最終的に再度 active 状態まで戻すことができます。terminated キーレコードは、KMS から削除することもできます。

注意: キーを削除する前に、このキーで暗号化された有効なイメージが存在しないことを確認してください。

---

terminated 状態のキーレコードは、terminated のままにするか、deprecated に変更するかまたは物理的に削除することができます。

KMS データベースファイルのバックアップについて

KMS データベースのバックアップでは、KMS ファイルもバックアップされます。

KMS ユーティリティには、データベースファイルの静止オプション、つまり任意のユーザーによるデータファイルの変更を一時的に禁止するオプションがあります。バックアップを目的として `KMS_DATA.dat`、`KMS_HMKF.dat` および `KMS_KPKF.dat` ファイルを別の場所にコピーする計画の場合は、静止オプションを実行することが重要です。

静止中は、NetBackup によってこれらのファイルに対する書き込みアクセスは排除され、読み込みアクセスのみが許可されます。

`nbkmsutil -quiescedb` を実行すると、静止成功に関するメッセージと、未処理のコール数を示すメッセージが戻されます。この未処理のコール数は、カウントされます。ファイルの未処理の要求数に対して、ファイルにカウントが設定されます。

静止後、そのファイルを別のディレクトリの場所にコピーすることでバックアップを実行できます。

ファイルをコピーした後、nbkmsutil -unquiescedb を使用して KMS データベースファイルの静止を解除できます。

未処理の静止要求カウントが 0 になると、KMS は KMS_DATA.dat、KMS_HMKF.dat、KMS_KPKF.dat ファイルの変更が可能なコマンドを実行できるようになります。これらのファイルに対する書き込みアクセスが再び可能になります。

すべてのデータファイルのリストアによる KMS のリカバリについて

KMS_DATA.dat、KMS_HMKF.dat および KMS_KPKF.dat ファイルのバックアップコピーを作成済みである場合は、これら 3 つのファイルをリストアするだけです。その後 nbkms サービスを起動すると、KMS システムが起動し、再び動作します。

KMS データファイルのみのリストアによる KMS のリカバリ

KMS データファイル kms/db/KMS_DATA.dat のバックアップコピーは、パスフレーズを使って KMS_HMKF.dat と KMS_KPKF.dat ファイルを再生成することで、リストアできます。したがって、ホストマスターキーおよびキーの保護キーのパスフレーズを書き留めてある場合は、これらのファイルを再生成するコマンドを実行できます。システムからパスフレーズの入力を求められ、ここで入力したパスフレーズが元々入力してあったものと一致すると、ファイルをリセットできます。

KMS データファイルのみのリストアによって KMS をリカバリする方法

1. nbkms -resetkpk コマンドを実行します。
2. nbkms -resethmk コマンドを実行します。
3. nbkms サービスを起動します。

データ暗号化キーの再生成による KMS のリカバリ

データ暗号化キーの再生成を行うことで、完全な KMS データベースを再生成できます。目的は、新しい空の KMS データベースを作成し、個々のすべてのキーレコードを再度登録することです。

データ暗号化キーの再生成によって KMS をリカバリする方法

1 次のコマンドを実行して、空の KMS データベースを作成します。

```
nbkms -createemptydb
```

同じホストマスターキーおよびキーの保護キーを使用する必要はありません。新しいキーを選択できます。

2 `nbkmsutil -recoverkey` コマンドを実行し、キーグループ、キー名およびタグを指定します。

```
nbkmsutil -recoverkey -kgname ENCR_pool1 -keyname Q1_2008_key
  -tag
d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
```

キーの作成時に `nbkmsutil -listkey` コマンドの出力の電子コピーを保持しなかった場合は、64 文字すべてを手動で入力する必要があります。

3 プロンプトでパスフレーズを入力します。以前に入力した元のパスフレーズと、正確に一致する必要があります。

メモ: 入力したタグがすでに KMS データベースに存在する場合は、そのキーを再作成することはできません。

---

4 リカバリしたキーがバックアップに使用するキーである場合、次のコマンドを実行してキーを active にします。

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
 -state active
```

`-recoverkey` オプションによってキーレコードは inactive 状態になり、inactive 状態で KMS データベースに登録されます。

5 このキーレコードが今後使用されない予定のものである場合は、次のコマンドを実行します。

```
nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
-state deprecated
```

KMS データファイルのバックアップに関する問題

通常の NetBackup テープまたはカタログバックアップで KMS データファイルをバックアップする場合、問題が生じる可能性があります。

注意: KMS データファイルは、NetBackup カタログバックアップに含まれていません。

KPK、HMK およびキーファイルがカタログバックアップに含まれている場合、そのカタログバックアップテープを紛失すると、キーにアクセスするために必要なデータがすべてそのテープに含まれているため、キーストアのセキュリティが低下します。

たとえば、同じトランスポートトラックで運ばれるカタログバックアップテープとデータテープを両方一緒に紛失した場合は、重大な問題が生じる可能性があります。両方のテープを一緒に紛失した場合は、最初からこのテープを暗号化していなかったのと大差ありません。

カタログの暗号化も良いソリューションとはいえません。KPK、HMK およびキーファイルをカタログバックアップに含めて、そのカタログバックアップ自体を暗号化することは、車内に鍵を残したままロックするのと同じです。このような問題を防止するために、KMS は NetBackup の別のサービスとして確立されており、KMS ファイルは NetBackup ディレクトリとは別のディレクトリに保存されます。ただし、KMS データファイルをバックアップするためのソリューションは存在します。

KMS データベースファイルのバックアップソリューション

KMS データファイルをバックアップする最良のソリューションは、通常の NetBackup プロセス以外でバックアップするか、パスフレーズで生成された暗号化キーを使って手動で KMS を再構築することです。暗号化キーはすべてパスフレーズで生成できます。したがって、パスフレーズをすべて記録してある場合は、書き留めてある情報から KMS を手動で再作成することができます。KMS をバックアップする方法の 1 つは、別の CD、DVD または USB ドライブに KMS の情報を配置することです。

キーレコードの作成

次の手順は、パスフレーズを使って、prelive 状態を省略して active 状態のキーを作成してキーレコードを作成する方法を示します。

メモ: すでに active キーが存在するグループにキーを追加しようとすると、既存のキーは自動的に inactive 状態になります。

キーレコードと active 状態のキーを作成する方法

1. キーレコードを作成するには、次のコマンドを入力します。

```
nbkmsutil -createkey -usepphrase -kgname ENCR_mygroup -keyname
my_latest_key -activate -desc "key for Jan, Feb, March data"
```

2. パスフレーズを入力します。

主要グループからのキーのリスト

次の手順を使用して、特定のキーグループで作成したすべてのキーまたは選択したキーをリストします。

キーグループのキーのリストを作成する方法

◆ キーグループのキーのリストを作成するには、次のコマンドを入力します。

```
nbkmsutil -listkeys -kgname ENCR_mygroup
```

デフォルトでは、nbkmsutil によって詳細形式のリストが出力されます。次に、詳細形式ではないリストの出力を示します。

```
KGR ENCR_mygroup AES_256 1 Yes 134220503860000000

134220503860000000 -
KR my_latest_key Active 134220507320000000 134220507320000000
key for Jan, Feb, March data
Number of keys: 1
```

次のオプションで特定のキーグループのすべてのキーまたは特定のキーグループの特定のキーをリストできます。

```
# nbkmsutil -listkeys -all | -kgname <key_group_name> [ -keyname
<key_name> | -activekey ]

[ -noverbose | -export ]
```

-all オプションですべてのキーグループのすべてのキーをリストします。キーは詳細な形式でリストに登録済みです。

-kgname オプションは指定されたキーグループからのキーをリストします。

-keyname オプションは指定されたキーグループから特定のキーをリストします。ただし、-kgname オプションと一緒に使用する必要があります。

-activekey オプションは、指定されたキーグループ名からアクティブなキーをリストします。ただし、-kgname オプションと一緒に使用する必要があります。

メモ: -activekey オプションと -keyname オプションは互いに排他的です。

-noverbose オプションは、フォーマットされた形式 (非可読形式) でキーとキーグループの詳細をリストします。デフォルトは、詳細 (verbose) リストです。

-export オプションは、key_file が必要とする出力を生成します。（key_file は、nbkmsutil -export -path <key_container_path > -key_file ファイルで使用されます。別の key_file の出力を使用できます。

次のコマンドを実行して、特定のキーグループからすべてのキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name>
```

次のコマンドを実行して、特定のキーグループから特定のキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name> -keyname <key_name>
```

次のコマンドを実行して、すべてのグループからすべてのキーをリストします。

```
nbkmsutil -listkeys -all
```

次のコマンドを実行して、特定のキーグループからすべてのキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name>
```

次のコマンドを実行して、特定のキーグループからアクティブなキーをリストします。

```
nbkmsutil -listkeys -kgname <key_group_name> -activekey
```

KMS と連携するための NetBackup の構成

KMS と連携するための NetBackup の構成について、次のトピックで説明します。

- NetBackup が KMS からキーレコードを取得する
  p.315 の「NetBackup および KMS のキーレコード」を参照してください。
- NetBackup で暗号化を使用するように設定する
  p.316 の「テープ暗号化を使用するための Netbackup の設定例」を参照してください。

NetBackup および KMS のキーレコード

KMS と連携するための NetBackup の構成の最初の手順は、NetBackup でサポートされる暗号化可能なテープドライブと、必要なテープメディアをセットアップすることです。

2 番目の手順は、通常どおり NetBackup を構成することです。ただし、暗号化可能なメディアを、KMS を構成したときに作成したキーグループと同じ名前のボリュームプール内に配置する必要がある点が異なります。

メモ: キーマネージメント機能では、キーグループ名と NetBackup ボリュームプール名が同一で、両方の名前に接頭辞 ENCR_ が付いている必要があります。この構成方法により、NetBackup のシステム管理インフラストラクチャに大幅な変更を行わなくても、暗号化サポートが利用可能になっています。

テープ暗号化を使用するための Netbackup の設定例

次の例では、暗号化用に作成した 2 つの NetBackup ボリュームプールを設定します (接頭辞 ENCR_ が付いています)。

次の図に示す NetBackup 管理コンソールには、KMS を使用するための適切な命名規則が適用された 2 つのボリュームプールが表示されています。

図 8-3 KMS を使用するための 2 つのボリュームプールの設定が表示された NetBackup 管理コンソール

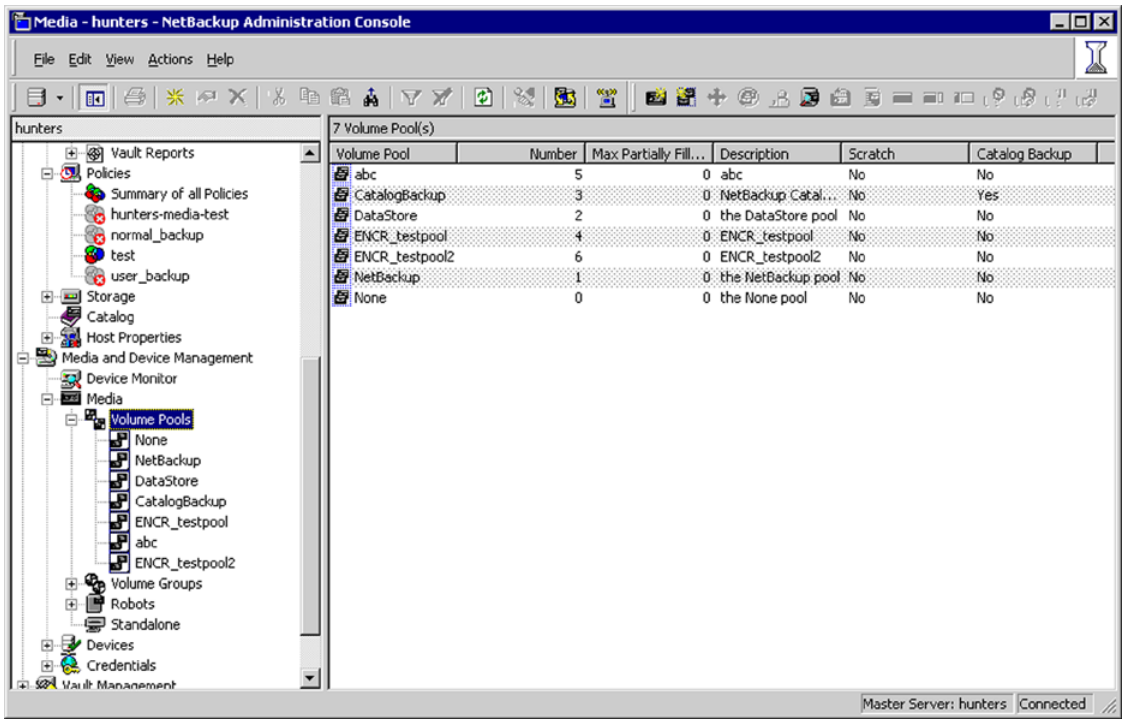
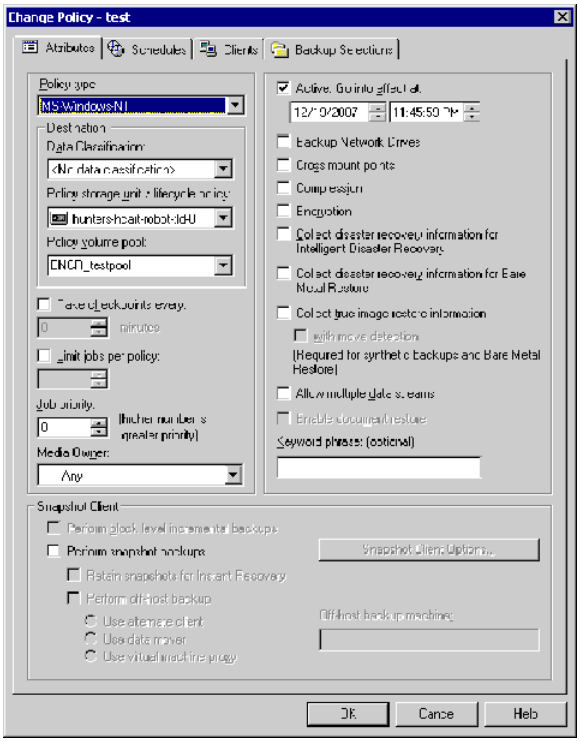


図 8-4 に、ボリュームプール ENCR_testpool を使用するように設定された NetBackup ポリシーを示します。これは、以前に設定したキーグループと同じ名前です。

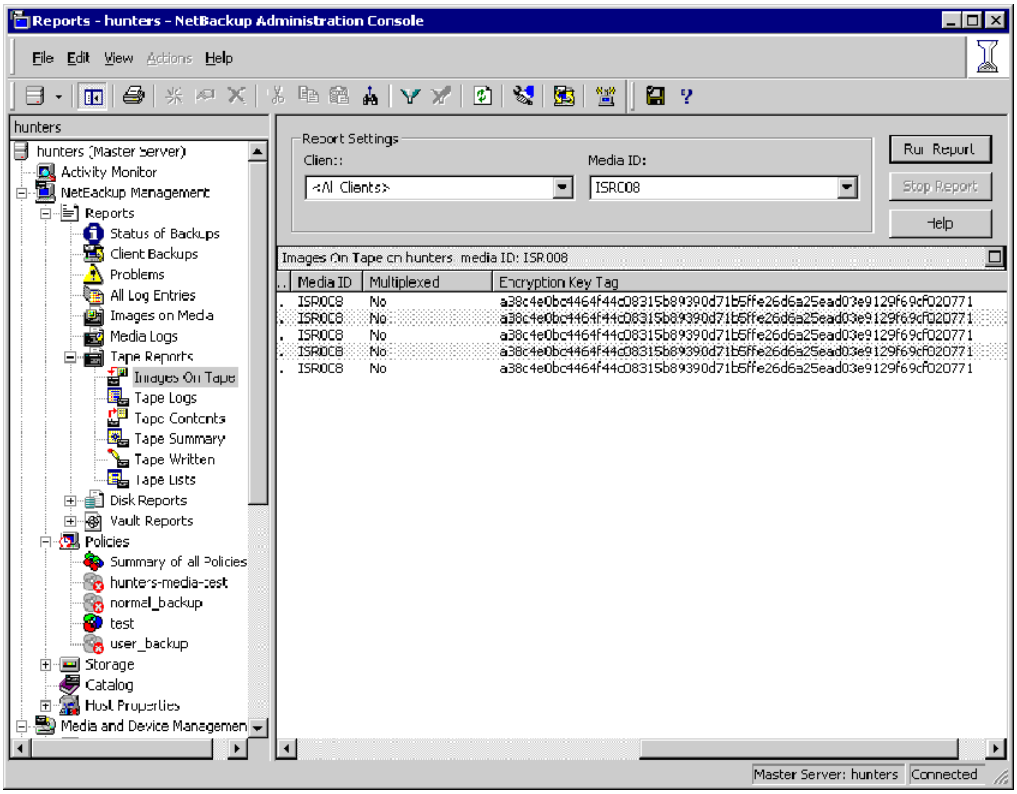
図 8-4 KMS のボリュームプールが表示された NetBackup の［ポリシーの変更 (Change Policy)］ダイアログボックス



NetBackup イメージが暗号化されると、キータグが記録され、イメージと関連付けられます。この情報は、NetBackup 管理コンソールのレポートで確認するか、または `bpimmedia` および `bpimagelist` コマンドの出力で確認できます。

次の図は暗号化キータグが表示されている［テープ上のイメージ (Images on Tape)］レポートを示します。

図 8-5　テープの暗号化キーが表示されている[テープ上のイメージ(Images on Tape)]



暗号化への KMS の使用について

KMS は、暗号化テープバックアップの実行、暗号化テープバックアップの確認、およびキーの管理に使用できます。以降の項では、これらの各シナリオの例を示します。

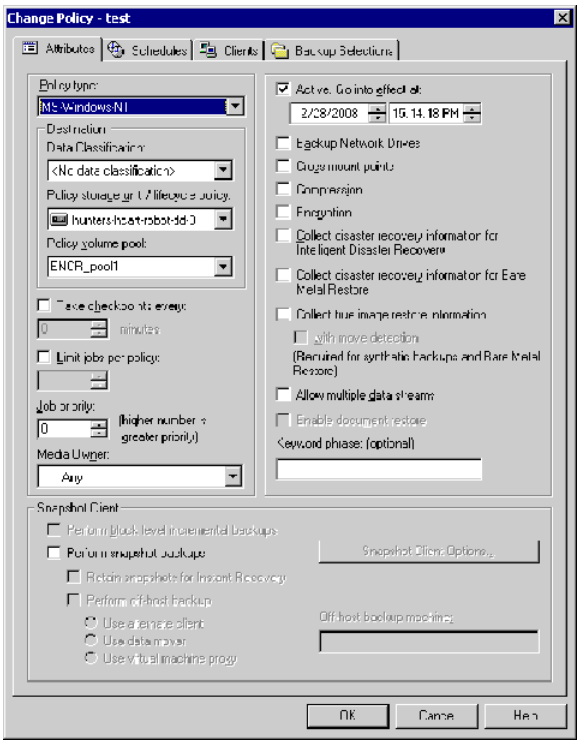
- 暗号化テープバックアップの実行例
  p.319 の「暗号化テープバックアップの実行例」を参照してください。
- 暗号化バックアップの確認例
  p.319 の「暗号化バックアップの確認例」を参照してください。
- KMS 暗号化イメージのインポートについて
  p.320 の「KMS 暗号化イメージのインポートについて」を参照してください。

暗号化テープバックアップの実行例

暗号化テープバックアップを実行するには、キーグループと同じ名前のボリュームプールから取得するように設定されたポリシーが必要です。

図 8-6 に、ボリュームプール ENCR_pool1 を使用するように設定した NetBackup ポリシーを示します。

図 8-6 KMS のボリュームプール ENCR_pool1 が表示された NetBackup の [ポリシーの変更 (Change Policy)] ダイアログボックス

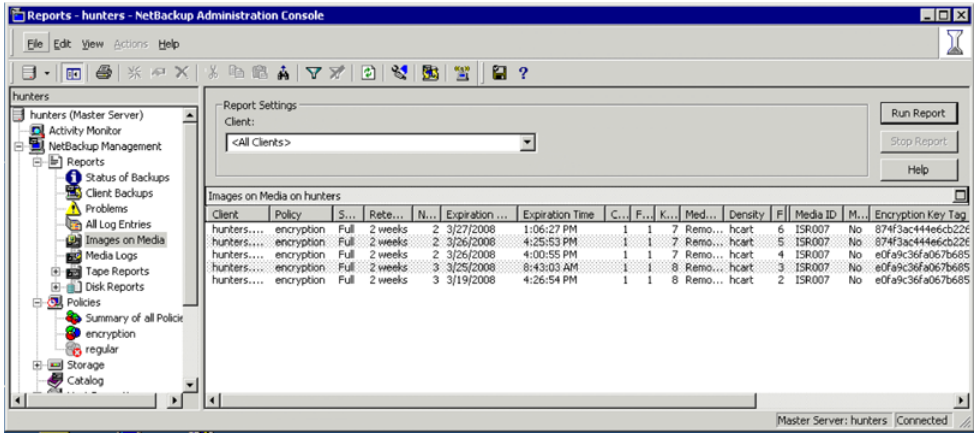


暗号化バックアップの確認例

NetBackup による暗号化テープバックアップの実行時に [メディア上のイメージ (Images on Media)] を表示すると、レコードとともに登録される暗号化キータグが表示されます。このキータグによって、テープに書き込まれた内容が暗号化されたことがわかります。この暗号化キータグは、データの暗号化に使用されたキーを一意に識別するものです。レポートを実行してポリシー列を下まで読むと、特定のテープ上のすべての内容が暗号化されているかどうかを確認できます。

図 8-7 に、暗号化キータグが表示されている[メディア上のイメージ (Images on Media)] レポートを示します。

図 8-7 テープの暗号化キーが表示されている[メディア上のイメージ (Images on Media)]



KMS 暗号化イメージのインポートについて

KMS 暗号化イメージのインポートは、2 フェーズの操作です。フェーズ 1 では、メディアヘッダーと各フラグメントのバックアップヘッダーが読み込まれます。このデータは暗号化されていません。ただし、バックアップヘッダーには、フラグメントファイルデータが KMS で暗号化されているかどうかが示されています。要するに、フェーズ 1 ではキーは必要ありません。

フェーズ 2 では、カタログ `.f` ファイルが再構築され、このファイルに暗号化データを読み込むように要求されます。`key-tag` (`SCSI` 用語では `KAD`) は、ハードウェアによってテープに保存されます。`NBU`/`BPTM` は、`key-tag` をドライブから読み込み、キーの照合用にこれを KMS に送信します。KMS にキーがある場合は、フェーズ 2 の処理で引き続き暗号化データが読み込まれます。KMS にキーがない場合には、KMS がキーを再作成するまでデータは読み込み可能になりません。このときにパスフレーズが重要になります。

キーを破壊していない場合、これまでに使用されたすべてのキーが KMS に含まれており、任意の暗号化されたテープをインポートできます。キーストアを DR サイトに移動すれば、再作成する必要はありません。

KMS データベースの要素

KMS データベースは、次の 3 つのファイルで構成されています。

- キーストアファイル (KMS_DATA.dat)。すべてのキーグループおよびキーレコードと、一部のメタデータが含まれています。
- KPK ファイル (KMS_KPKF.dat)。キーストアファイルに格納されるキーレコードの暗号テキスト部分の暗号化に使用される KPK が含まれています。
- HMK ファイル (KMS_HMKF.dat)。キーストアファイルの内容全体の暗号化に使用される HMK が含まれています。キーストアファイルのヘッダーは例外です。キーストアファイルのヘッダーには、暗号化されない KPK ID および HMK ID のような一部のメタデータが含まれています。

空の KMS データベースの作成

空の KMS データベースは、コマンド nbkms -createemptydb を実行して作成できます。

このコマンドでは、次の情報の入力が求められます。

- HMK パスフレーズ(ランダムな HMK の場合は何も指定しません)
- HMK ID
- KPK パスフレーズ(ランダムな KPK の場合は何も指定しません)
- KPK ID

KMS データベースのバックアップとディザスタリカバリの手順は、次に示すように、KPK および HMK がランダムに生成された場合とパスフレーズで生成された場合で異なります。

HMK と KPK をランダムに生成した場合のリカバリ方法

1. バックアップからキーストアファイルをリストアします。
2. コマンド nbkms -info を実行して、このキーストアファイルの復号化に必要な KPK および HMK の KPK ID および HMK ID を確認します。この出力では、このキーストアファイルの HMK および KPK がランダムに生成されたことも示されているはずです。
3. セキュリティ保護されたバックアップから、この HMK ID に対応する HMK ファイルをリストアします。
4. セキュリティ保護されたバックアップから、この KPK ID に対応する KPK ファイルをリストアします。

KPK ID および HMK ID の重要性

キーストアファイルの内容を解読するには、そのジョブを実行する正しい KPK と HMK を識別することが重要です。識別は、KPK ID および HMK ID で行うことができます。これ

らの ID はキーストアファイルのヘッダーに暗号化されずに格納されているため、キーストアファイルにアクセスしかできない場合でも特定することができます。ディザスタリカバリの実行を可能にするために、一意の ID を選択し、ID とパスフレーズおよびファイルの関連付けを記憶しておくことが重要です。

HMK および KPK の定期的な更新について

HMK と KPK は、KMS CLI の `modifyhmk` と `modifykpk` オプションを使って定期的に更新できます。この操作では、新しいパスフレーズと ID の入力を求められ、その後 KPK/HMK が更新されます。更新のたびに、ランダムベースの KPK/HKM にするか、パスフレーズベースの KPK/HKM にするかを選択できます。

メモ: HMK および KPK の変更時には `-usepphrase` オプションを使って、今後のリカバリ時に既知のパスフレーズの使用が求められるようにすることが推奨されます。-nopphrase オプションを使った場合は、KMS で未知のランダムパスフレーズが生成され、今後の必要なリカバリが実行できなくなる可能性があります。

KMS キーストアおよび管理者キーのバックアップ

重要な KMS データファイルは、キーデータベース KMS_DATA.dat、ホストマスターキー KMS_HMKF.dat およびキーの保護キー KMS_HKPKF.dat のコピーを作成することでバックアップできます。

Windows の場合、これらのファイルは次の場所にあります。

```
¥Program Files¥Veritas¥kms¥db¥KMS_DATA.dat
¥Program Files¥Veritas¥kms¥key¥KMS_HMKF.dat
¥Program Files¥Veritas¥kms¥key¥KMS_KPKF.dat
```

UNIX の場合、これらのファイルは次の場所にあります。

```
/opt/openv/kms/db/KMS_DATA.dat
/opt/openv/kms/key/KMS_HMKF.dat
/opt/openv/kms/key/KMS_KPKF.dat
```

コマンドラインインターフェース (CLI) コマンド

以下の項では、次のコマンドラインインターフェース (CLI) について説明します。

- CLI の使用方法のヘルプ
  p.324 の「CLI の使用方法のヘルプ」を参照してください。
- 新しいキーグループの作成

p.324 の「新しいキーグループの作成」を参照してください。

- 新しいキーの作成
  p.325 の「新しいキーの作成」を参照してください。
- キーグループの属性の変更
  p.325 の「キーグループの属性の変更」を参照してください。
- キーの属性の変更
  p.326 の「キーの属性の変更」を参照してください。
- キーグループの詳細の取得
  p.326 の「キーグループの詳細の取得」を参照してください。
- キーの詳細の取得
  p.327 の「キーの詳細の取得」を参照してください。
- キーグループの削除
  p.328 の「キーグループの削除」を参照してください。
- キーの削除
  p.328 の「キーの削除」を参照してください。
- キーのリカバリ
  p.329 の「キーのリカバリ」を参照してください。
- ホストマスターキー (HMK) の変更
  p.333 の「ホストマスターキー (HMK) の変更」を参照してください。
- ホストマスターキー (HMK) ID の取得
  p.333 の「ホストマスターキー (HMK) ID の取得」を参照してください。
- キーの保護キー (KPK) の変更
  p.334 の「キーの保護キー (KPK) の変更」を参照してください。
- キーの保護キー (KPK) ID の取得
  p.334 の「キーの保護キー (KPK) ID の取得」を参照してください。
- キーストアの統計の取得
  p.334 の「キーストアの統計の取得」を参照してください。
- KMS データベースの静止
  p.334 の「KMS データベースの静止」を参照してください。
- KMS データベースの静止解除
  p.335 の「KMS データベースの静止解除」を参照してください。

CLI の使用方法のヘルプ

CLI の使用方法のヘルプを取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

個別のオプションに関するヘルプを表示するには、nbkmsutil -help -*option* を使用します。

```
# nbkmsutil -help
nbkmsutil [ -createkg ] [ -createkey ]
[ -modifykg ] [ -modifykey ]
[ -listkgs ] [ -listkeys ]
[ -deletekg ] [ -deletekey ]
[ -modifyhmk ] [ -modifykpk ]
[ -gethmkid ] [ -getkpkid ]
[ -quiescedb ] [ -unquiescedb ]
[ -recoverkey]
[ -ksstats ]
[ -help ]
```

新しいキーグループの作成

新しいキーグループを作成するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -createkg
nbkmsutil -createkg -kgname <key_group_name>
[ -cipher <type> ]
[ -desc <description> ]
```

メモ: デフォルトの暗号は AES_256 です。

-kgname	新しいキーグループの名前を指定します (キーストア内で一意である必要があります)。
-cipher	このキーグループでサポートされる暗号形式を指定します。

新しいキーの作成

新しいキーを作成するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -createkey
nbkmsutil -createkey [ -nopphrase ]
-keyname <key_name>
-kgname <key_group_name>
[ -activate ]
[ -desc <description> ]
```

メモ: デフォルトのキーの状態は prelive です。

-nopphrase	パスフレーズを使わずにキーを作成します。このオプションを指定しない場合は、ユーザーはパスフレーズの入力を求められます
-keyname	新しいキーの名前を指定します (このキーが属するキーグループ内で一意である必要があります)。
-kgname	新しいキーが追加される、既存のキーグループの名前を指定します。
-activate	キーの状態を active に設定します (デフォルトのキーの状態は prelive です)。

メモ: このリリースからパスフレーズを使用して新しいキーを作成するときに salt が生成されます。キーを回復する場合は、システムから salt とパスフレーズおよびキータグを入力するように求めるメッセージが表示されます。

キーグループの属性の変更

キーグループの属性を変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -modifykg
nbkmsutil -modifykg -kgname key_group_name
[ -name <new_name_for_the_key_group> ]
[ -desc <new_description> ]
```

-kgname	変更するキーグループの名前を指定します。

-name	キーグループの新しい名前を指定します (キーストア内で一意である必要があります)。

キーの属性の変更

キーの属性を変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -modifykey
nbkmsutil -modifykey -keyname <key_name>
-kgname <key_group_name>
[ -state <new_state> | -activate ]
[ -name <new_name_for_the_key> ]
[ -desc <new_description> ]
[ -move_to_kgname <key_group_name> ]
```

メモ: -state オプションと -activate オプションは互いに排他的です。

-keyname	変更するキーの名前を指定します。
-kgname	このキーが属するキーグループの名前を指定します。
-name	キーの新しい名前を指定します (キーグループ内で一意である必要があります)。
-state	キーの新しい状態を指定します (有効なキーの状態の遷移順序を参照してください)。
-activate	キーの状態を active に設定します。
-desc	キーに新しい説明を追加します。
move_to_kgname	キーの移動先のキーグループの名前を指定します。

キーグループの詳細の取得

キーグループの詳細を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -listkgs
nbkmsutil -listkgs [ -kgname <key_group_name> |
-cipher <type> |
```

```
-emptykgs |
-noactive ]
[ -noverbose ]
```

メモ: デフォルトでは、すべてのキーグループがリストに表示されます。オプションを指定しない場合、すべてのキーグループの詳細が戻されます。

-kgname	キーグループの名前を指定します。
-cipher	特定の暗号形式をサポートするすべてのキーグループの詳細を取得します。
-emptykgs	キーのないすべてのキーグループの詳細を取得します。
-noactive	active キーが存在しないすべてのキーグループの詳細を取得します。
-noverbose	フォーマットされたフォーム形式 (読みやすい形式ではない) で詳細を出力します。デフォルトは、詳細 (verbose) 形式です。出力は読みやすい形式で表示されます。

-export オプションは、key_file が必要とする出力を生成します。key_file は、nbkmsutil -export -path <key_container_path > -key_file ファイルで使用されます。出力は別の key_file に使用できます。

```
# nbkmsutil -listkeys -all | -kgname <key_group_name>
[ -keyname <key_name> | -activekey ]
[ -noverbose | -export ]
```

キーの詳細の取得

キーの詳細を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
#nbkmsutil -help -listkeys
nbkmsutil -listkeys -kgname <key_group_name>
[ -keyname <key_name> | -activekey ]
[ -noverbose ]
```

-kgname	キーグループ名を指定します。キーグループに属するすべてのキーの詳細が戻されます。
-keyname	特定のキーグループに属する特定のキーの詳細を取得します。
-activekey	特定のキーグループの有効なキーの詳細を取得します。

-noverbose　フォーマットされたフォーム形式 (読みやすい形式ではない) で詳細を出力します。デフォルトは、詳細 (verbose) 形式です。出力は読みやすい形式で表示されます。

キーグループの削除

キーグループを削除するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

メモ: 空のキーグループのみを削除できます。

```
# nbkmsutil -help -deletekg
nbkmsutil -deletekg -kgname <key_group_name>
```

-kgname　削除するキーグループの名前を指定します。空のキーグループのみを削除できます。

空のキーグループのみを-deletekgオプションで削除できます。しかし、キーグループを空でなくても強制的に削除することもできます。強制的にキーグループを削除するには、次のコマンドを実行します。

```
# nbkmsutil -deletekg -kgname <key_group_name> -force
```

キーの削除

キーを削除するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -deletekey
nbkmsutil -deletekey -keyname <key_name>
-kgname <key_group_name>
```

メモ: prelive または terminated のいずれかの状態のキーを削除できます。

-keyname　削除するキーの名前を指定します (削除するには、キーの状態が prelive または terminated のいずれかである必要があります)。

-kgname　このキーが属するキーグループの名前を指定します。

キーのリカバリ

キーをリカバリするには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

```
# nbkmsutil -help -recoverkey
nbkmsutil -recoverkey -keyname <key_name>
-kgname <key_group_name>
-tag <key_tag>
[ -desc <description> ]
```

メモ: キーの状態は inactive に設定されます。

バックアップデータの暗号化に使用したキーが失われ、そのコピーも入手できない場合、リストアが失敗することがあります。このようなキーは、元のキーの属性(タグおよびパスフレーズ)がわかれば、リカバリ(再作成)できます。

-keyname	リカバリ (再作成) するキーの名前を指定します。
-kgname	このキーが属するキーグループの名前を指定します。
-tag	元のキーを識別するタグを指定します (同じタグを使用する必要があります)。

メモ: ユーザーは、正しいキーを取得するために正しいパスフレーズの入力を求められます(システムは入力されたパスフレーズの有効性を検証しません)。

メモ: このリリースから、キーを回復するときは必ずシステムから salt を入力するように求めるメッセージが表示されます。salt はこのバージョンの KMS でパスフレーズ派生キー用に生成されます。旧バージョンの KMS で生成されたキーを回復するには、salt フィールドを空白のままにしてください。

KMS データベースからのキーのエクスポートと KMS データベースへのキーのインポートについて

キーのエクスポートおよびインポートにより、同じキーセットを使用する複数の NetBackup ドメインを迅速に同期化したり、キーセットをドメイン間で迅速に移動したりできます。この機能は、ディザスタリカバリにより発生する別の NetBackup ドメインでのリストアに特に役立ちます。

キーのエクスポート

-export コマンドにより、キーおよびキーグループをドメイン間でエクスポートできます。キーおよびキーグループのエクスポートについて重要な情報を次の一覧に示します。

- キーは必ず、所属するキーグループに基づいてエクスポートされます。
- キーとキーグループは、キーマネージメントサービス(KMS)ユーティリティ(nbkmsutil)が実行されるホスト上の暗号化キーコンテナ (ファイル) でエクスポートされます。キーコンテナはパスフレーズで保護されます。

  メモ: キーおよびキーグループをインポートするとき、同じパスフレーズを使用する必要があります。

- エクスポート内容の指定には、特定のキーグループを選択する方法、またはキーを選択してエクスポートする方法があります。

次のように -export コマンドを使用します。

```
nbkmsutil -export -path <secure_key_container>
```

```
[ -key_groups <key_group_name_1 ...> | -key_file <key_file_name> ]
```

デフォルトでは、キーストア全体がエクスポートされます。

-path コマンドは、安全なキーコンテナが格納される完全修飾パスを指定します。

-key_groups コマンドは、キーグループ名をスペースで区切って指定します。

-key_file コマンドは、特定形式でエクスポートするキーをリストで示すファイルパスです。

<key_group_name>/<key_name> コマンドでは、キーを選択してエクスポートできます。特定のグループのすべてのキーをエクスポートする場合は、「*」を使用できます。

```
<key_group_name>/*
```

nbkmsutil -listkeys -export コマンドを使って、このオプションに必要とされる形式で出力を生成できます。詳しくは、nbkmsutil -listkeys -export を参照してください。

キーのリスト作成の詳細:

p.314 の「主要グループからのキーのリスト」を参照してください。

メモ: -key_groups コマンドと -key_file コマンドは相互に排他的です。

次のコマンドを実行すると、キーストア全体がエクスポートされます。

```
nbkmsutil -export -path <secure_key_container>
```

次のコマンドを実行すると、選択したキーグループがエクスポートされます。

```
nbkmsutil -export -path
<secure_key_container> -key_groups
<key_group_name_1 key_group_name_2 ...>
```

次のコマンドを実行すると、選択したキーがエクスポートされます。

```
nbkmsutil -export -path
<secure_key_container> -key_file
<key_file_name>
```

エクスポート時における一般的なエラーのトラブルシューティング

キーおよびキーグループをエクスポートする場合に発生する一連のエラー。この項は、このようなエラーをトラブルシューティングするのに役立ちます。

- 指定したキーコンテナがホスト上にすでに存在していた場合、エクスポートは失敗します。
  別のキーコンテナファイルを指定してから、エクスポート操作を再度実行してください。
- 正しくないキーまたはキーグループ名を指定した場合も、エクスポートは失敗します。
  キーまたはキーグループ名を訂正し、再度エクスポートを実行してください。

キーのインポート

-import コマンドにより、キーおよびキーグループをドメイン間でインポートできます。キーおよびキーグループのインポートについて重要な情報を次の一覧に示します。

- キーおよびキーグループをインポートする場合、エクスポート中に作成されたキーコンテナファイルが必要です。また、エクスポート中に使われた同じパスフレーズも必要です。
- キーのインポートはアトミック操作です。操作中にエラーが発生した場合、すべての更新が元に戻されます。
- 部分的なインポートはサポートされません。
- インポート出力のプレビューが利用可能です。-previewコマンドを実行すると、インポート結果がプレビューされます。
- インポート操作には 2 つのモードがあります。-preserve_kgnameコマンドを含んでいるモード、-preserve_kgnameコマンドを含まないモードがあります。
  デフォルトでは、キーグループは次の名前形式でインポートされます。
  < Original_Kgname_<timestamp> >

明示的に <-preserve_kgname> オプションを指定することにより、キーグループ名を保持することができます。

- 同じキータグのキーまたは同じキーのある重複キーはインポートされません。
- インポートでは、キーグループのマージをサポートしません。

ただし、<-preserve_kgname> コマンドを使用しなければ、キーをマージして、キーグループとしてインポートできます。nbkmsutil -modifykey -keyname <key_name> -kgname <key_group_name> コマンドを実行すると、現在のグループから目的のグループにキーを移動できます。

キーの移動についての詳細:

p.326 の「キーの属性の変更」を参照してください。

キーグループに同じキーまたは同じキータグを持つキーが含まれている場合、これらはインポート中無視されます。キーおよびキーグループをインポートするには、次のコマンドを実行します。

```
# nbkmsutil -import -path <secure_key_container>

[-preserve_kgname]

[ -desc <description> ]

[ -preview ]
```

-preserve_kgname コマンドは、インポート中、キーグループ名を保持します。

-desc <description> コマンドは、インポート中、キーグループと関連付けられる説明になります。

-preview コマンドは、インポート結果のプレビューを表示します。

-preserve_kgname を使用するインポート操作は次のように実行します。

```
nbkmsutil -import -path

<secure_key_container>

[-preserve_kgname]
```

-preserve_kgname とともに -import コマンドを実行すると、キーコンテナから元のキーグループ名を使ったインポートが試みられます。同じ名前のキーグループが存在すれば、インポート操作は失敗します。

-preserve_kgname なしのインポート操作は次のように実行します。

```
nbkmsutil -import -path

<secure_key_container>
```

-preserve_kgname なしで -import コマンドを実行すると、キーグループはインポートされますが、キーグループ名は、タイムスタンプなどが接尾語として使用されることにより変更されます。名前が変更されるキーグループは、必ず一意の名前になります。

インポート時における一般的なエラーのトラブルシューティング

キーおよびキーグループをインポートする場合に発生する一連のエラー。この項は、このようなエラーをトラブルシューティングするのに役立ちます。

- [-preserve_kgname] オプションでキーグループをインポートしようとしていて、そのグループが KMS にすでに存在していた場合、インポート操作全体が失敗します。
  既存のキーグループを削除するか、名前を変更して、または [-preserve_kgname] オプションを除外してから、インポート操作を再度実行してください。
- NetBackup KMS には、100 キーグループという制限が存在します。各グループには、30 キーという制限が存在します。100 を超えるキーグループをインポートすると、操作が失敗します。
  不要な既存のキーグループを削除して、インポート操作を再実行する必要があります。

ホストマスターキー (HMK) の変更

ホストマスターキーを変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

HMK は、キーストアの暗号化に使用します。現在の HMK を変更するには、オプションのシードまたはパスフレーズを指定する必要があります。また、その指定されたパスフレーズを連想できるような ID (HMK ID) を指定する必要もあります。パスフレーズと HMK ID は、どちらも対話形式で読み込まれます。

```
# nbkmsutil -help -modifyhmk
nbkmsutil -modifyhmk [ -nopphrase ]
```

ホストマスターキー (HMK) ID の取得

HMK ID を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。これにより、HMK ID が戻されます。

```
# nbkmsutil -help -gethmkid
nbkmsutil -gethmkid
```

キーの保護キー (KPK) ID の取得

KPK ID を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。このコマンドにより、現在の KPK ID が戻されます。

```
# nbkmsutil -help -getkpkid
nbkmsutil -getkpkid
```

キーの保護キー (KPK) の変更

キーの保護キーを変更するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

KPK は、KMS キーの暗号化に使用します。現在、KPK はキーストアごとに存在します。現在の KPK を変更するには、オプションのシードまたはパスフレーズを指定する必要があります。また、その指定されたパスフレーズを連想できるような ID（KPK ID）を指定する必要もあります。パスフレーズと KPK ID は、どちらも対話形式で読み込まれます。

```
# nbkmsutil -help -modifykpk
nbkmsutil -modifykpk [ -nopphrase ]
```

キーストアの統計の取得

キーストアの統計を取得するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

このコマンドでは、次のキーストアの統計が戻されます。

- キーグループの総数
- キーの総数
- 未処理の静止要求

```
# nbkmsutil -help -ksstats
nbkmsutil -ksstats [ -noverbose ]
```

KMS データベースの静止

KMS データベースを静止するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (nbkmsutil コマンド) を、組み込みの引数を指定して使用します。

このコマンドは、KMS に静止要求を送信します。コマンドが正常に実行されると、現在の未処理の静止カウントが戻されます (複数のバックアップジョブが KMS データベースを静止させる場合があるため)。

```
# nbkmsutil -help -quiescedb
nbkmsutil -quiescedb
```

KMS データベースの静止解除

KMS データベースを静止解除するには、NetBackup キーマネージメントサービス (KMS) ユーティリティのコマンド (`nbkmsutil` コマンド) を、組み込みの引数を指定して使用します。

このコマンドは、KMS に静止解除要求を送信します。コマンドが正常に実行されると、現在の未処理の静止数が返されます。カウントが 0 (ゼロ) の場合は、KMS データベースが完全に静止解除されていることを意味します。

```
# nbkmsutil -help -unquiescedb
nbkmsutil -unquiescedb
```

キーの作成オプション

NetBackup KMS 機能を使用する場合は、必ず `kms/db` および `kms/key` ディレクトリのバックアップが作成されます。保護キーおよびキーデータベースは 2 つの別個のサブディレクトリに存在しており、バックアップコピーの作成時にこれらを容易に分けられるようになっています。

メモ: これらのファイルは、サイズが小さい点、変更頻度が低い点、およびそれ自体が暗号化される NetBackup テープには含めてはならないという点から、バックアップメディアに手動でコピーする必要があります。

メモ: このバージョンの KMS で推奨されるキーの作成方法は、常にパスフレーズからキーを作成することです。このようなキーには、保護キー (ホストマスターキーおよびキーの保護キー) と、キーレコードに関連付けられているデータ暗号化キーの両方が含まれます。キーの作成に使うパスフレーズは、リカバリで使うことができるように、記録し、保管しておくことをお勧めします。

KMS システムでランダムな暗号化キーの生成を許可するとより強力なソリューションが得られますが、この使用方法ではキーストアおよび保護キーのすべてのコピーが失われた場合または破損した場合にリカバリできなくなるため、お勧めしません。

KMS のトラブルシューティング

KMS のトラブルシューティングを開始するには、次の手順を使用します。

KMS のトラブルシューティングを開始する方法

1. 発生したエラーコードおよび説明を特定します。
2. KMS が実行されているかどうかを判別し、次の KMS データファイルが存在することを確認します。

   ```
   kms/db/KMS_DATA.dat
   kms/key/KMS_HMKF.dat
   kms/key/KMS_KPKF.dat
   ```

   このファイルが存在しない場合は、KMS は構成されていないか、または構成が削除されています。ファイルが存在しない場合は、ファイルに何が発生したかを特定します。KMS が構成されていない場合、`nbkms` サービスは実行されません。KMS が実行されていないか、または構成されていない場合は、NetBackup 操作には影響を及ぼしません。これまでボリュームプール名に `ENCR_` の接頭辞を使用していた場合は、この名前を変更する必要があります。`ENCR_` は現在 NetBackup で特別な意味を持ちます。
3. KMS 構成情報を取得します。

   コマンド `nbkmsutil -listkgs` を実行して、キーグループのリストを取得します。
   コマンド `nbkmsutil -listkeys -kgname` *`key_group_name`* を実行して、キーグループのすべてのキーのリストを取得します。
4. VxUL OID 286 および BPTM ログを介して、KMS ログなどの操作ログ情報を取得します。
5. ログ情報を評価します。KMS エラーは BPTM に戻されます。
6. KMS ログに記録されている KMS エラーを評価します。

バックアップが暗号化されていない問題の解決方法

テープバックアップが暗号化されていない場合、次の解決方法を検討します。

- 暗号化キータグフィールドがイメージレコードに設定されていないことを確認し、バックアップが暗号化されていないことを確認します。
- キーグループ名とボリュームプール名が完全に一致することを確認します。
- キーグループに active 状態のキーレコードがあることを確認します。

その他の KMS 以外の構成オプションでは、次の点に注目してください。

- 従来のメディア管理に関するすべての項目が適切に構成されていることを確認します。
- NetBackup ポリシーが適切なボリュームプールからテープを取得していることを確認します。
- 暗号化が可能なテープドライブで、暗号化が可能なメディアが利用可能であることを確認します。たとえば、LTO4 メディアが LTO4 テープドライブにインストールされていることを確認します。

リストアが復号化されない問題の解決方法

暗号化されたテープのリストアが復号化されていない場合は、次の解決方法を検討します。

- イメージレコードの暗号化キータグフィールドを参照して、元のバックアップイメージが最初から暗号化されていたことを確認します。
- 同じ暗号化キータグフィールドを持つキーレコードが、リストアをサポートするレコードの状態であることを確認します。これらの状態には、active 状態または inactive 状態があります。
- キーレコードが適切な状態でない場合は、キーを inactive 状態に戻します。

その他の KMS 以外の構成ソリューションのオプションを次のように検討します。

- ドライブおよびメディアが暗号化をサポートしていることを確認します。
- 読み取り中の暗号化されたメディアが、暗号化が可能なテープドライブにあることを確認します。

トラブルシューティングの例 - active キーレコードが存在しない場合のバックアップ

次の例は、active キーレコードが存在しない場合にバックアップを試行したときの結果を示します。

図 8-8 に、キーレコードのリストを示します。キーグループ `ENCR_mygroup` および同一のボリュームプール名を持つ 3 つのキーレコードがあります。`Q2_2008_key` という名前のキーグループは active でした。コマンドの終わりには、`Q2_2008_key` キーグループの状態は inactive に設定されます。

図 8-8 キーレコードのリスト

```
fel (root) [385]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name        : ENCR_mygroup
Supported Cipher      : AES_256
Number of Keys        : 3
Has Active Key        : Yes
Creation Time         : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description           : -
  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name              : Q2_2008_key
  Current State         : Active
  Creation Time         : Sat Mar 15 11:02:46 2008
  Last Modification Time: Sat Mar 15 11:02:46 2008
  Description           : key for Apr, May, & Jun
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name              : Q1_2008_key
  Current State         : Inactive
  Creation Time         : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description           : Key for Jan, Feb, & March
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name              : test
  Current State         : Inactive
  Creation Time         : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description           : -
Number of Keys: 3
fel (root) [383]: nbkmsutil -modifykey -keyname Q2_2008_key -kgname ENCR_mygroup -state
Inactive
Key details are updated successfully
```

図 8-9 に、再作成されたキーレコードのリストを示します。`Q2_2008_key` の状態が inactive と表示されるのがわかります。

図 8-9　active キーグループが変更された状態のキーレコードのリスト

```
fel (root) [384]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name         : ENCR_mygroup
Supported Cipher       : AES_256
Number of Keys         : 3
Has Active Key         : No
Creation Time          : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description            : -
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name               : Q1_2008_key
  Current State          : Inactive
  Creation Time          : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description            : Key for Jan, Feb, & March
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name               : test
  Current State          : Inactive
  Creation Time          : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description            : -
  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name               : Q2_2008_key
  Current State          : Inactive
  Creation Time          : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 13:53:33 2008
  Description            : key for Apr, May, & Jun

Number of Keys: 3
```

active キーがない場合のバックアップへの影響を考えてみます。

図 8-10 に BPTM ログの出力を示します。BPTM ログのエラーコード 1227 内にメッセージが記録されます。

図 8-10　bptm コマンドの出力

```
14:29:16.381 [19978] <2> manage_drive_attributes: MediaPool [ENCR_mygroup], MediaLabel [MEDIA=JR0111;]
14:29:16.384 [19978] <2> manage_drive_attributes: encryption status: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decryp mode 0x0, algorithm index 0, key instance
0
14:29:16.384 [19978] <2> KMSCLIB::kmsGetKeyAndKad: Entering function....(KMSClib.cpp:583)
14:29:16.384 [19978] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:29:16.384 [19978] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:29:16.385 [19978] <2> Orb::init: Created anon service name: NB_19978_1536015948517350(Orb.cpp:600)
14:29:16.385 [19978] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_19978_1536015948517350(Orb.cpp:618)
14:29:16.385 [19978] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory ''" -ORBSvcConfDirective "static
EndpointSelectorFactory ''" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_19978_1536015948517350 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:29:16.406 [19978] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:29:16.406 [19978] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:29:16.460 [19978] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:29:16.461 [19978] <16> get_encryption_key: NBKMS failed with error status: Key group does not have an active key
(1227)
14:29:16.462 [19978] <2> send_MDS_msg: MEDIADB 1 42 JR0111 4000007 *NULL* 6 1205781805 1205782033 1206991633 0 64 2
2 1 4 0 8193 1024 0 8 0
```

このエラーがアクティビティモニターでどのように表示されるかを次に示します。

図 8-11 は、状態コード 83 のメディアのオープンエラーメッセージが戻されていることを示します。

図 8-11　　状態コード 83 を表示するアクティビティモニター

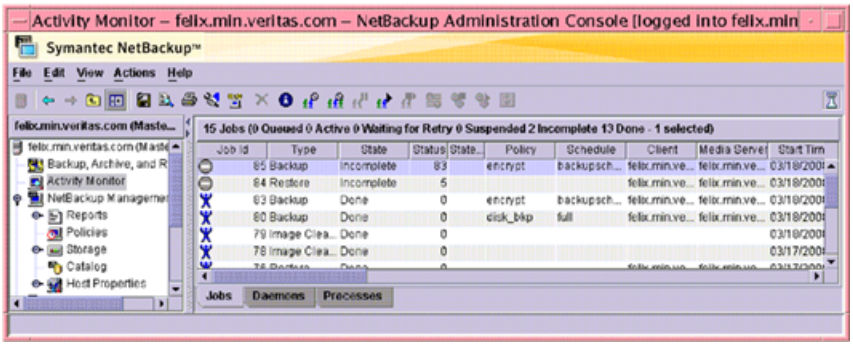


図 8-12 に、状態の詳細を示します。[NBKMS がエラー状態で失敗しました: キーグループに有効なキーがありません (1227) (NBKMS failed with error status: Key group does not have an active key (1227))]というメッセージが表示されます。以前の診断の情報と合わせて、特定の問題を判別することや、発生した問題が何に関連しているかを特定することができます。

図 8-12　　[ジョブの詳細 (Job Details)]ダイアログボックス

トラブルシューティングの例 - 不適切なキーレコード状態でのリストア

次の例は、不適切な状態のキーレコードを使用したリストアを示します。

図 8-13 は、必要なレコードが deprecated に設定されていることを示します。次にリストを示します。同じコマンドを使用して、状態が inactive から deprecated に変更されています。

図 8-13 deprecated キーグループを含むキーレコードのリスト

```
fel (root) [426]: !385
nbkmsutil -listkeys -kgname ENCR_mygroup

Key Group Name        : ENCR_mygroup
Supported Cipher      : AES_256
Number of Keys        : 3
Has Active Key        : No
Creation Time         : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description           : -

  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name              : Q1_2008_key
  Current State         : Inactive
  Creation Time         : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description           : Key for Jan, Feb, & March

  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name              : test
  Current State         : Inactive
  Creation Time         : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description           : -

  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name              : Q2_2008_key
  Current State         : Deprecated
  Creation Time         : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 14:52:59 2008
  Description           : key for Apr, May, & Jun

Number of Keys: 3
```

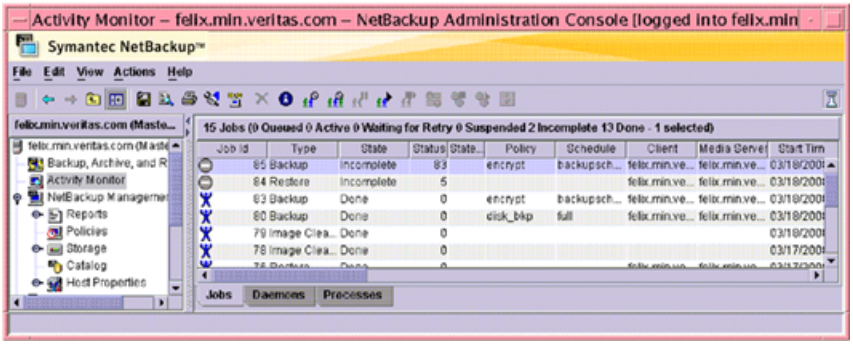
図 8-14 は、bptm ログの出力に 1242 エラーが戻されていることを示します。

図 8-14 1242 エラーを含む bptm ログ

```
14:53:48.782 [21109] <2> io_read_back_header: drive index 0, reading backup header
14:53:48.791 [21109] <2> io_position_for_read: successfully positioned JR0111 to file number 3
14:53:48.796 [21109] <2> io_position_for_read: next block encryption status: LON 0x0000000000000009, algorithm
index 1, encryption status 0x6
14:53:48.796 [21109] <2> io_position_for_read: Kad type 0x0, kad length 32 Kad
[cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d]
14:53:48.796 [21109] <2> KMSCLIB::kmsGetKeyAndKadByKeyTag: Entering function....(KMSClib.cpp:655)
14:53:48.796 [21109] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:53:48.796 [21109] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:53:48.797 [21109] <2> Orb::init: Created anon service name: NB_21109_1537488329610200(Orb.cpp:600)
14:53:48.798 [21109] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_21109_1537488329610200(Orb.cpp:618)
14:53:48.798 [21109] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory '" -ORBSvcConfDirective "static
EndpointSelectorFactory '" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_21109_1537488329610200 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:53:48.818 [21109] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:53:48.818 [21109] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:53:48.842 [21109] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:53:48.844 [21109] <16> get_encryption_key: NBKMS failed with error status: Operation not allowed for key record
in this state (1242)
```

図 8-15 に、状態コード 5 の[リストアは、要求されたファイルのリカバリに失敗しました (the restore failed to recover the requested files)]を示します。

図 8-15 状態コード 5 を含むアクティビティモニター



索引

記号

40 ビット DES 鍵
　ライブラリ 259
40 ビット DES 鍵
　ライブラリ 261
56 ビット DES 鍵
　ライブラリ 261
アクセス制御 (Access Control)。「NetBackup アクセス制御 (NBAC)」を参照
　ホストプロパティ 174
アクセス管理
　トラブルシューティング 182
アップグレード
　NetBackup アクセス制御（NBAC） 165
インストール
　KMS 297、301
オプション
　BPCD コネクトバック (BPCD connect-back) 109
　デーモン接続ポート 109
　ポート 109
　格納データの暗号化 256
オペレータアクセス制御ユーザーグループ 226
キー
　作成 325
キーの作成
　オプション 335
キーの保護キー (Key Protection Key: KPK) 296、298、304、321～322、334
キーの属性
　変更 326
キーグループ
　作成 324
　削除 328
　定義 305
　詳細 326
キーグループの属性
　変更 325
キーストアの統計 334
キーデータベース、作成 304
キーマネージメントサービス (Key Management Service: KMS)
　NBAC の使用 301
　NetBackup とキーレコード 315
　データベースの要素 320
　操作原理 294
　暗号化への使用 318
　概要 289
キーマネージメントサービス（KMS）
　インストール 297、301
　トラブルシューティング 336
　リカバリ 311
　構成 303、315
　注意事項 290
　用語 295
キーレコード
　作成 313
キーレコードの状態
　active 309
　deprecated 310
　inactive 309
　prelive 309
　terminated 310
　注意事項 308
クライアントの暗号化設定
　変更 270
クライアント属性の設定によるポートの使用の構成
　bpclient コマンド 115
クラスタ環境
　鍵ファイルのセキュリティの強化 (レガシー) 281
　鍵ファイルの管理 (レガシー) 276
コマンドラインインターフェース (CLI)
　使用 322
　使用方法のヘルプ 324
サーバーからのレガシー暗号化
　構成 271
サーバーからの標準暗号化
　構成 266
サーバーの変更 (Change Server) 130
セキュリティ
　Media Server Encryption Option (MSEO) 27
　実装レベル 13

セキュリティ管理者アクセス制御ユーザーグループ 226
セキュリティ証明書 128、130
テープ暗号化、NetBackup の設定 316
デフォルトユーザーアクセス制御ユーザーグループ 226
デフォルトユーザーグループ 225
データベースの要素
KMS 320
デーモン接続ポート (Daemon connection port)
オプション 109
トラブルシューティング
active キーレコードが存在しない場合のバックアップ 337
Authentication and Authorization 183
KMS 336
アクセス管理 182
不適切なキーレコード状態でのリストア 341
ネットワーク設定 (Network Settings)タブ 175、182
バックアップ
暗号化されていない、解決方法 336
暗号化の選択 258
パスフレーズ
リダイレクトリストア (レガシー) 278
リダイレクトリストア (標準) 269
鍵ファイルの暗号化 (レガシー) 277、281
ファイアウォール接続オプション
Media Manager 115
NetBackup サーバーまたはクライアント上。 109
特定の接続先コンピュータに適用する接続元コンピュータへの指定 112
ホストプロパティ
アクセス制御 (Access Control) 174、180
ホストプロパティへのアクセス 179
［ネットワーク設定 (Network Settings)］タブ 175
［認証サービス (Authorization Service)］タブ 178
［認証ドメイン (Authentication Domain)］タブ 176
ホストマスターキー (HMK)
変更 333
ホストマスターキー (Host Master Key: HMK) 298、304、321～322、333～334
ポート
NetBackup 94
オプション 109
概要 94
認可 186
認証 186
ポートの使用に関連する Media Manager 構成の設定
vm.conf 115
ポートの使用法の設定
bp.conf 114
ポート番号
バックアップ製品とアーカイブ製品 104
上書きまたは変更について 94
マスターサーバー設定
検証 183
ユーザーの割り当てユーザーグループ 233
ユーザーグループ 224
KMS 管理者 227
SAN 管理者 226
Vault オペレータ 227
オペレータ 226
セキュリティ管理者 226
デフォルトユーザー 226
ユーザーの割り当て 233
作成 227
既存のユーザーグループのコピー 228
名前の変更 228
定義 231
新しいユーザーの追加 231
特定のユーザー権限の表示 237
管理者 226
ユーザーグループへの新しいユーザーの追加 231
リカバリ
KMS 311
キー 329
リストア
別のクライアントで作成されたレガシー暗号化が使用されたバックアップ 278
リストア処理
NetBackup 標準暗号化 260
リダイレクトリストア
レガシー暗号化が使用されたバックアップ 278
他のクライアントのバックアップ (レガシー) 278
他のクライアントのバックアップ (標準) 269
暗号化されたバックアップファイル 269
レガシー暗号化
バックアップ処理 259
管理 276
レガシー暗号化用の tar ヘッダー 260
レガシー鍵ファイルのセキュリティ
UNIX クライアントの場合 280
ログオン新しいユーザー 233
上書きまたは変更
ポート番号 94
代替クライアントへのリストア (「リダイレクトリストア」を参照) 269、278
作成
キーデータベース 304
キーレコード 313

新しいキー 325
新しいキーグループ 324
新しいユーザーグループ 227～228
空の KMS データベース 321
例
NetBackup でテープ暗号化を使用するように設定する 316
暗号化テープバックアップの実行 319
暗号化バックアップの確認 319
別のクライアントで作成されたレガシー暗号化が使用されたバックアップ
リストア 278
制限事項
格納データの暗号化 253
削除
キー 328
キーグループ 328
変更
サーバーからのクライアントの暗号化設定 270
復号化
概要 (標準) 260
鍵ファイル (レガシー) 281
拡張監査
(アクセス制御の 1 タイプ) 140
サーバーの変更を使うための設定 130
サーバー間の信頼の設定 129
メディアサーバーへの接続 128
ユーザー管理 141
ユーザー認証 143
有効化 127
構成 128
無効化 131
指定
bpclient コマンド 115
暗号化
KMS の使用 318
tar ヘッダー
レガシー 260
ポリシー属性 258
レガシー
前提条件 259
属性 260
概要 (標準) 260
標準
tar ヘッダー 261
鍵ファイル (レガシー) 281
暗号化されたバックアップ
リストア (レガシー) 278
リストア (標準) 269
暗号化されたバックアップファイル
異なるクライアントへのリストア 269
暗号化のインストール
UNIX 版 NetBackup クライアントへローカルに 263
Windows 版 NetBackup クライアントへローカルに 263
暗号化テープ
書き込み 294
読み取り 295
暗号化テープの読み取り 295
暗号化テープへの書き込み 294
暗号化バックアップの確認 319
暗号形式 291
更新
HMK と KPK 322
格納データの暗号化
オプション 256
制限事項 253
検証手順
UNIX 190～191、194、196、198、200
Windows 203、206、208～209、211、215、217
構成
クラスタ (レガシー) 272
サーバーからのレガシー暗号化 271
サーバーからの標準暗号化 266
暗号化用のクライアント
サーバーから (標準) 266
標準暗号化用の tar ヘッダー 261
権限
付与 236
管理
レガシー暗号化鍵ファイル 276
管理者アクセス制御ユーザーグループ 226
複合化されないリストア、解決方法 337
認可ポート 186
認証オブジェクトと権限 234
認証ポート 186
鍵
キーグループのリスト 314
リカバリ 329
削除 328
詳細 327
鍵ファイル 260
クラスタ内 (レガシー) 276、280～281
バックアップ (レガシー) 278
リダイレクトリストア (標準) 269、279
レガシー 260
作成 (レガシー) 276
暗号化 (レガシー) 276

管理パスフレーズによる暗号化 (レガシー) 281
鍵ファイルの管理 (レガシー) 276
［アクセス管理 (Access Management)］
ユーティリティ 219
［割り当て済みのユーザー (Assigned Users)］ペイン 231
［定義されているユーザー (Defined Users)］ペイン 230
［認可サービス (Authorization Service)］タブ 178
［認証ドメイン (Authentication Domain)］タブ 176、181

A

ALLOWED (暗号化オプション) 264、272
Audit Manager 121、132
auth.conf 131、140、143、190
Authentication and Authorization
トラブルシューティング 183

B

bp.conf ファイル
ポートの使用法の設定 114
bp.conf ファイル
変更の監査 122、131
bpcd 260～261
終了 282
BPCD コネクトバック (BPCD connect-back)
オプション 109
bpclient コマンド
指定 115
bpinst コマンド 260
bpinst コマンド 261
暗号化属性の設定 (レガシー) 279
クライアントへの構成のプッシュインストール (レガシー) 274
bpkeyfile コマンド
change_netbackup_pass_phrase オプション 277
概要 (標準) 260
鍵ファイルの管理 (レガシー) 276
bpkeyfile コマンド
概要 (標準) 261
鍵ファイルのパスフレーズの変更 282
bpkeyutil コマンド
リダイレクトリストア 269、279
標準リストアの概要 260
bpkeyutil コマンド
概要 259
鍵ファイルの管理 265
鍵ファイルの作成 267
パスフレーズの追加 265

C

cnpp オプション 277
CRYPT_KEYFILE オプション 260、276
CRYPT_OPTION 258
CRYPT_CIPHER オプション 265
CRYPT_KEYFILE オプション 261、273
CRYPT_KIND オプション 264、273
CRYPT_LIBPATH オプション 273
CRYPT_OPTION 264、272、274
CRYPT_STRENGTH オプション 261、273～274
CRYPT オプション 279

D

DENIED (暗号化オプション) 264、272
DES
鍵のチェックサム 262
標準暗号化用の鍵のチェックサム 259
鍵のチェックサム 260～261
DES 鍵のチェックサム
説明
レガシー暗号化 260
標準リストア 261
DES 鍵のチェックサム
説明
標準暗号化 259
レガシーのリストア 262
DevHost の認可オブジェクト
権限 247

E

EMM サーバー
外部接続ポート 99
EMM データベース
監査レコードの格納 125、132
Enterprise Media Manager (EMM)
データベース 121

F

FIPS (連邦情報処理標準) 287

I

ICMP
NDMP の ping 118

J

Java コンソール
外部接続ポート 101

K

KMS からのキーのエクスポート 329
KMS のリカバリ 311
KMS へのキーのインポート 329
KMS サービス
　監視 302～303
　監視対象リスト 303
KMS サービスの監視 302～303
KMS データファイル
　バックアップの問題 312
　バックアップソリューション 313
KMS データベース (KMS database)
　空のデータベースの作成 321
　静止 334
　静止解除 335
KMS データベースファイル
　バックアップ 310
KMS データベースファイルのバックアップ 310
KMS 管理者アクセス制御ユーザーグループ 227
KMS 暗号化イメージ
　インポート 320
KMS キーストアと管理者キー
　バックアップ 322
kms グループの認可オブジェクト
　権限 249
KMS サービス
　クラスタでの有効化 302

M

Media Manager
　ファイアウォール接続オプション 115
Media Server Encryption Option (MSEO)
　セキュリティ 27
Media Manager 構成
　ランダムポートの割り当て 108
Media Server Encryption Option (MSEO)
　単一のデータセンター 44
　複数のデータセンターの使用 65

N

NBAC
　マスターサーバー、メディアサーバーおよび GUI でのセキュリティ 30
nbac_cron ユーティリティ 187
nbac_cron.exe 187
nbaudit (NetBackup の監査サービス) 121～122、132、134
nbauditreport 125、133
nbaudit ログ 137
NBU_Admin アクセス制御ユーザーグループ 226
NBU_KMS Admin アクセス制御ユーザーグループ 227
NBU_Operator アクセス制御ユーザーグループ 226
NBU_Security Admin アクセス制御ユーザーグループ 226
NBU_User アクセス制御ユーザーグループ 226
NBU_Catalog の認可オブジェクト
　権限 241
NBU のセキュリティ
　ワークグループ 37
NDMP
　ファイアウォール環境における 118
NDMP の ping
　ICMP 118
NetBackup
　セキュリティ
　　all 33
　セキュリティの実装形式 23
　セキュリティの脆弱性 25
　アクセスの決定 222
　コンポーネント
　　セキュリティで使用 17
　セキュリティ
　　実装レベル 13
　ポート 94
NetBackup とキーレコード
　KMS 315
NetBackup の構成
　KMS との連携 315
NetBackup アクセス制御 (NBAC)
　(アクセス制御の 1 タイプ) 140
　nbac_cron ユーティリティ 187
　nbac_cron.exe 187
　コンポーネント 17
　サーバーの変更を使うための設定 130
　ユーザーグループ 224
　　KMS 管理者 227
　　SAN 管理者 226
　　Vault オペレータ 227
　　オペレータ 226
　　セキュリティ管理者 226
　　デフォルトユーザー 226
　　ユーザーグループの名前の変更 228
　　構成 227
　　管理者 226
　個々のユーザー 223
NetBackup アクセス制御（NBAC）
　デフォルトユーザーグループ 225

構成 152～156、160、165、170～171、174
NetBackup 標準暗号化
リストア処理 260
NetBackup Audit Manager 121、132
NetBackup Service Layer (NBSL) 106
NetBackup アクセス制御 (NBAC) 122、131。「NetBackup アクセス制御 (NBAC)」を参照
使用 149
NetBackup クライアントの暗号化
オプション 1 257
NetBackup セキュリティ
標準 26
NetBackup のアクセス管理
管理 151
NetBackup レガシー暗号化
リストア処理 261

O

OpsCenter 121、123、125、132

P

passphrase_prompt オプション 275
passphrase_stdin オプション 275

R

REQUIRED (暗号化オプション) 264、272

S

setuptrust コマンド 172～173
SNMP ポート 107

U

UNIX クライアント
レガシー鍵ファイルのセキュリティ 280
UNIX 版 NetBackup クライアント
暗号化のインストール 263
UNIX 版 NetBackup サーバー
暗号化のインストール 262
USE_AUTH_CONF_NBAC 190

V

Vault オペレータアクセス制御ユーザーグループ 227
Vault_Operator アクセス制御ユーザーグループ 227
Vault の認可オブジェクト
権限 249
vm.conf
ポートの使用に関連する Media Manager 構成の設定 115
VxSS 認可ポート 186
VxSS 認証ポート 186

W

Windows
クライアントでの検証項目 217
マスターサーバーでの検証項目 211
メディアサーバーでの検証項目 215
検証項目 209
Windows 版 NetBackup クライアント
暗号化のインストール 263
Windows 管理コンソールおよび Java サーバーの外部接続ポート 100
Windows 版 NetBackup サーバー
暗号化のインストール 263

あ

[アクセス権 (Permissions)]タブ 234
アクセス制御のインストール
クライアント 158
アクセス制御の構成
クライアント 158
アップグレードと監査の構成 123
暗号化
tar ヘッダー
標準 259
暗号化の有無 (標準) 259
概要 (レガシー) 261
鍵を含むファイル (レガシー) 273
強度
定義 (レガシー) 273
許可
拒否。「必要」を参照
クライアントでの管理 (標準) 264
クライアントでの構成 (標準) 270
構成オプション (レガシー) 272
種類
定義 (標準) 264
定義 (レガシー) 273
セキュリティの質問 255
属性
設定 270
ポリシー属性
設定方法 270、279

ライブラリ
定義 (レガシー) 273
レガシー
tar ヘッダー 262
リストアの前提条件 261
[暗号化 (Encryption)]属性
ポリシー 279
暗号化オプション
比較 256
暗号化セキュリティ
インストールの前提条件 262
暗号化属性 270、279
暗号化属性の設定
ポリシー 270
暗号化のインストール
UNIX 版 NetBackup サーバーの場合 262
Windows 版 NetBackup サーバーの場合 263
暗号化バックアップ
実行 257
[一般 (General)]タブ 229
インストール
クライアントへの構成のプッシュインストール (レガシー) 274
クライアントへのパスフレーズのプッシュインストール (レガシー) 275
クライアントへのプッシュインストールのためのサーバーへのインストール 262
インストールの前提条件
暗号化セキュリティ向け 262
インポート
KMS 暗号化イメージ 320
大文字と小文字の区別
コマンド構文で 123～124、133
オプション 1
NetBackup クライアントの暗号化 257
オプション 2
メディアサーバーの暗号化 282
オフライン
クライアントの設定 132
オペレーティングシステム
セキュリティ 25

か

外部接続ポート
EMM サーバー 99
Java コンソール 101
Windows 管理コンソールおよび Java サーバー 100
クライアント 100
マスターサーバー 97
メディアサーバー 98
概要
標準暗号化を使用したバックアップ 258
レガシーのリストア 261
鍵ファイル 259、261
bpkeyutil コマンド 265
管理パスフレーズによる暗号化 (標準) 265
管理 (標準) 265
クラスタ内 (標準) 265
作成
クライアントノード上 266
作成 (標準) 267
自動バックアップ 268
説明 (レガシー) 275
定義 (レガシー) 273
パスフレーズ (レガシー) 282
鍵ファイルのパスフレーズの保護
手作業による保存 268
鍵ファイルのリストア
推奨する実施例 268
拡張監査
概要 126
格納データの暗号化
用語 253
カタログバックアップ
監査レコードの保持 132
監査
アップグレード後の構成 123
概要 121
監査のアラート通知 132、137～138
現在の設定の表示 123
有効化 124
レポート 133、135
監査アラート通知ボタン 132、137～138
監査サービス (nbaudit) 121～122、132
監査レポートのユーザーの ID 125
管理
NetBackup 暗号化鍵ファイル 265
NetBackup のアクセス管理 151
暗号化用のクライアント
クライアントから (標準) 264
鍵ファイル (標準) 265
標準暗号化の構成オプション 264
メディアサーバーの暗号化 283
レガシー暗号化構成オプション 272
企業レベル
セキュリティ 15

キーグループ
作成 306
キーレコード
作成 306
キーレコードの状態
概要 307
クライアント
オフラインの設定 132
外部接続ポート 100
標準暗号化の構成 263
クライアント側の暗号化
セキュリティ 28
単一のデータセンター 47
複数のデータセンター 71
クライアントのレガシー暗号化設定
変更 280
クラス
「ポリシー」を参照 270、279
クラスタ環境
鍵ファイルの管理 (標準) 265
構成のプッシュインストール (レガシー) 274
ソフトウェアのプッシュインストール (標準) 276
クラスタでの有効化
KMS サービス 302
権限
DevHost の認可オブジェクト 247
kms グループの認可オブジェクト 249
NBU_Catalog の認可オブジェクト 241
Vault の認可オブジェクト 249
サーバーグループの認可オブジェクト 249
サービスの認可オブジェクト 244
ジョブの認可オブジェクト 244
ストレージユニットの認可オブジェクト 242
セキュリティの認可オブジェクト 247
ディスクプールの認可オブジェクト 242
ドライブの認可オブジェクト 240
バックアップおよびリストアの認可オブジェクト 243
ファットクライアントの認可オブジェクト 248
ファットサーバーの認可オブジェクト 248
ホストプロパティの認可オブジェクト 245
ポリシーの認可オブジェクト 239
ボリュームグループの認可オブジェクト 246
ボリュームプールの認可オブジェクト 246
メディアの認可オブジェクト 239
ライセンスの認可オブジェクト 245
レポートの認可オブジェクト 240
ロボットの認可オブジェクト 241
構成
暗号化用のクライアント
クライアントから (標準) 270
サーバーから (レガシー) 274
オプション (レガシー) 272
クライアントへのプッシュインストール (レガシー) 274
クラスタ (標準) 266
標準暗号化
クライアント 263
ポート 107
レガシー暗号化 271

さ

作成
暗号化鍵ファイル
クライアントノード上 266
鍵ファイル 267
キーグループ 306
キーレコード 306
サーバーグループの認可オブジェクト
権限 249
サービスの認可オブジェクト
権限 244
サーベンスオクスリー法 (SOX) 121
実行
bpkeyfile コマンド 281
暗号化バックアップ 257
実装されるすべてのセキュリティ
単一のデータセンター 57
自動バックアップ
鍵ファイル 268
ジョブの認可オブジェクト
権限 244
推奨する実施例
鍵ファイルのリストア 268
ストレージユニットの認可オブジェクト
権限 242
すべてに NBAC を使用
セキュリティ 32
単一のデータセンター 53
複数のデータセンター 82
すべての NetBackup セキュリティ
複数のデータセンター 87
世界レベル
セキュリティ 14
世界レベル、企業レベルおよびデータセンターレベルの統合 22

セキュリティ
NetBackup
all 33
オペレーティングシステム 25
企業レベル 15
クライアント側の暗号化 28
すべてに NBAC を使用 32
世界レベル 14
データセンターレベル 17
セキュリティの実装形式
NetBackup 23
セキュリティの脆弱性
NetBackup 25
セキュリティの認可オブジェクト
権限 247

た

単一のデータセンター
Media Server Encryption Option (MSEO) の使用 44
クライアント側の暗号化の使用 47
すべてのセキュリティが実装された状態 57
すべてへの NBAC の使用 53
標準の NetBackup の使用 41
マスターサーバーおよびメディアサーバーでの NBAC の使用 49
重複排除ホスト
ファイアウォール 102
重複排除ポートの使用
概要 102
ディスクプールの認可オブジェクト
権限 242
データセンター
単一 37
複数 37
データセンターレベル
セキュリティ 17
デフォルト
ポート番号
NetBackup 96
ドライブの認可オブジェクト
権限 240

な

認可オブジェクト 238
認可オブジェクトおよび権限 234

は

パスフレーズ
クライアントへのプッシュインストール (レガシー) 275
バックアップ
KMS キーストアと管理者キー 322
バックアップおよびリストアの認可オブジェクト
権限 243
比較
暗号化オプション 256
標準
NetBackup セキュリティ 26
標準暗号化
バックアップ処理 258
標準暗号化用の tar ヘッダー 259
標準的な NetBackup
複数のデータセンターの使用 61
ファイアウォール環境
NDMP 118
ファイアウォールと重複排除ホスト 102
ファイアウォールについての注意事項 103
ファイアウォールの問題
他の製品とともに NetBackup を使用した場合 118
ファットクライアントの認可オブジェクト
権限 248
ファットサーバーの認可オブジェクト
権限 248
復号化
概要 (レガシー) 261
複数のデータセンター 37
Media Server Encryption Option (MSEO) の使用 65
クライアント側の暗号化の使用 71
すべての NetBackup セキュリティの使用 87
すべてへの NBAC の使用 82
標準の NetBackup の使用 61
マスターサーバーおよびメディアサーバーでの NBAC の使用 76
プッシュインストール
クライアントの構成 (レガシー) 274
クライアントのパスフレーズ (レガシー) 275
クライアントへのレガシー暗号化パスフレーズ 275
変更
クライアントのレガシー暗号化設定 280
ホストプロパティの認可オブジェクト
権限 245
ポート
構成 107
ポートの使用法
重複排除 102

ポート番号
HTTP 105
HTTPS 105
NetBackup のデフォルト 96
OpsCenter の主要コンポーネント 103
ポリシーの認可オブジェクト
権限 239
ボリュームグループの認可オブジェクト
権限 246
ボリュームプールの認可オブジェクト
権限 246

ま

マスターサーバー
外部接続ポート 97
マスターサーバーおよびメディアサーバー上の NBAC
単一のデータセンター 49
複数のデータセンター 76
マスターサーバー、メディアサーバーおよび GUI でのセキュリティ
NBAC 30
無効化
ランダムポートの割り当て 108
メディアサーバー
外部接続ポート 98
メディアサーバーの暗号化
オプション 2 282
管理 283
メディアの認可オブジェクト
権限 239

や

[ユーザー (Users)]タブ 229
用語
格納データの暗号化 253

ら

ライセンスの認可オブジェクト
権限 245
ライブラリ
暗号化の定義 (レガシー) 273
ランダムポートの割り当て
Media Manager 構成における 108
無効化 108
リストア
概要 (レガシー) 261
リストア処理
NetBackup レガシー暗号化 261
リダイレクトリストア
回避 (レガシー) 276
レガシー暗号化
構成 271
レガシー暗号化構成
クライアントへのプッシュインストール 274
レガシー暗号化構成オプション
管理 272
レガシー暗号化構成のプッシュインストール
クライアント 274
レガシー暗号化属性
ポリシーでの設定 279
レガシー暗号化パスフレーズ
クライアントへのプッシュインストール 275
レガシー暗号化用の tar ヘッダー 262
レジストリ (registry)
変更の監査 131
レポート
nbauditreport 132
監査イベントの場合 132
レポートの認可オブジェクト
権限 240
ロボットの認可オブジェクト
権限 241

わ

ワークグループ
NBU のセキュリティ 37
NetBackup の使用 38