HITACHI
Inspire the Next

Encryption License Key

ユーザガイド

Hitachi Virtual Storage Platform E990
Hitachi Virtual Storage Platform F350, F370, F700, F900
Hitachi Virtual Storage Platform G150, G350, G370, G700, G900

4060-1J-U05-20

Storage Navigator を使ってストレージシステムを操作する場合は、必ずこのマニュアルを読み、操作手順、および指示事項をよく理解してから操作してください。 また、このマニュアルをいつでも利用できるよう、Storage Navigator を使用するコンピュータの近くに保管してください。

免責事項
このマニュアルの内容の一部または全部を無断で複製することはできません。
このマニュアルの内容については、将来予告なしに変更することがあります。
このマニュアルに基づいてソフトウェアを操作した結果、たとえ当該ソフトウェアがインストールされているお客様所有のコンピュータに何らかの障害が発生しても、当社は一切責任を負いかねますので、あらかじめご了承ください。
このマニュアルの当該ソフトウェアご購入後のサポートサービスに関する詳細は、弊社営業担当にお問い合わせください。
この製品は OpenSSL ツールキットを利用するために OpenSSL プロジェクト(http://www.openssl.org/)によって開発されたソフトウェアを含みます。

商標類
Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
その他記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

輸出時の注意
本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。
なお、不明な場合は、弊社担当営業にお問い合わせください。

発行
2020 年 9 月（4060-1J-U05-20）

目次

はじめに

このマニュアルでは、Encryption License Key の概要と使用方法について説明しています。

- 対象ストレージシステム
- マニュアルの参照と適合ファームウェアバージョン
- 対象読者
- マニュアルで使用する記号について
- マニュアルに掲載されている画面図について
- 発行履歴

対象ストレージシステム

このマニュアルでは、次に示すストレージシステムに対応する製品（プログラムプロダクト）を対象として記述しています。

- Virtual Storage Platform G150
- Virtual Storage Platform G350
- Virtual Storage Platform G370
- Virtual Storage Platform G700
- Virtual Storage Platform G900
- Virtual Storage Platform F350
- Virtual Storage Platform F370
- Virtual Storage Platform F700
- Virtual Storage Platform F900
- Virtual Storage Platform E990

このマニュアルでは特に断りのない限り、上記モデルのストレージシステムを単に「ストレージシステム」または「本ストレージシステム」と称することがあります。

マニュアルの参照と適合ファームウェアバージョン

このマニュアルは、次の DKCMAIN ファームウェアバージョンに適合しています。

- VSP E990 の場合
  93-03-01-X0
- VSP G130, G150, G350, G370, G700, G900 および VSP F350, F370, F700, F900 の場合
  88-07-01-X0

メモ

- このマニュアルは、上記バージョンのファームウェアをご利用の場合に最も使いやすくなるよう作成されていますが、上記バージョン未満のファームウェアをご利用の場合にもお使いいただけます。
- 各バージョンによるサポート機能については、別冊の『バージョン別追加サポート項目一覧』を参照ください。
- 88-04-01-XX 未満のファームウェアをご利用の場合には、そのファームウェアに同梱されたマニュアルメディアをご使用ください。

対象読者

このマニュアルは、次の方を対象読者として記述しています。

- ストレージシステムを運用管理する方
- UNIX®コンピュータまたは Windows®コンピュータを使い慣れている方
- Web ブラウザを使い慣れている方

使用する OS および Web ブラウザの種類については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

マニュアルで使用する記号について

このマニュアルでは、注意書きや補足情報を、次のとおり記載しています。

注意
データの消失・破壊のおそれや、データの整合性がなくなるおそれがある場合などの注意を示します。

メモ
解説、補足説明、付加情報などを示します。

ヒント
より効率的にストレージシステムを利用するのに役立つ情報を示します。

マニュアルに掲載されている画面図について

このマニュアルに掲載されている画面図の色は、ご利用のディスプレイ上に表示される画面の色と異なる場合があります。

このマニュアルでは、Windows コンピュータ上の Internet Explorer での画面を掲載しています。UNIX コンピュータ上でご使用の Storage Navigator の画面は、マニュアルに掲載されている画面の表示と異なる場合があります。Storage Navigator の画面や基本操作に関する注意事項については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

発行履歴

この発行履歴では、次の略記を使用します。

- VSP G/F シリーズ：VSP G130, G150, G350, G370, G700, G900 および VSP F350, F370, F700, F900 の略記。

マニュアル資料番号	発行年月	変更内容
4060-1J-U05-20	2020 年 9 月	• 適合 DKCMAIN ファームウェアバージョン VSP G/F シリーズ：88-07-01-XX VSP E990：93-03-01-XX • 鍵管理サーバを別サーバへ移行する機能をサポートした。 ◦ 3.10.2 鍵暗号化鍵を更新する ◦ 3.11 鍵管理サーバを別サーバへ移行する ◦ 4.1 Encryption License Key 操作時のエラーと対策 ◦ A.16 鍵暗号化鍵更新ウィザード ◦ 2.2 鍵管理サーバの要件
4060-1J-U05-11	2020 年 7 月	• 適合 DKCMAIN ファームウェアバージョン VSP G/F シリーズ：88-06-02-XX VSP E990：93-02-03-XX • 証明書設定および使用についての記載を変更した。 ◦ 2.2 鍵管理サーバの要件

マニュアル資料番号	発行年月	変更内容
		• 暗号化の有効手順に注意事項を追記した。 ◦ 3.4.2 データの暗号化を有効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）
4060-1J-U05-10	2020 年 4 月	• 適合 DKCMAIN ファームウェアバージョン VSP G/F シリーズ：88-06-01-XX VSP E990：93-02-01-XX • VSP E990 で Encryption License Key をサポートした。 ◦ 1.1 Encryption License Key ◦ 1.2.1 ハードウェアの仕様 ◦ 1.2.3 格納データ暗号化で使用する鍵 ◦ 1.3 暗号化鍵の管理機能 ◦ 1.3.1 暗号化鍵の使用 ◦ 2.1 システムの要件 ◦ 3.2 暗号化鍵を作成する ◦ 3.6 暗号化鍵のリストア ◦ 3.7 暗号化鍵の強制リストア ◦ 3.11 鍵暗号化鍵を再取得する ◦ 4.1 Encryption License Key 操作時のエラーと対策 ◦ 3.2 暗号化鍵を作成する ◦ A.3.1 ［鍵生成］画面 ◦ A.14.1 ［暗号化編集］画面 ◦ A.14.2 ［設定確認］画面 • 中間証明書についての記載を追記した。 ◦ 2.2 鍵管理サーバの要件 • OpenSSL のダウンロードの記載を変更した。 ◦ 2.2.2 クライアント証明書の取得の流れ • 暗号化鍵の使用の記載を変更した。 ◦ 1.3.1 暗号化鍵の使用
4060-1J-U05-00	2020 年 1 月	初版（4046-1J-U05-40 から改訂） • 適合 DKCMAIN ファームウェアバージョン VSP G/F シリーズ：88-04-03-XX VSP E990：93-01-01-XX

1

Encryption License Key の概要

ここでは、Encryption License Key の概要について説明します。

1.1 Encryption License Key

Encryption License Key を使用すると、ストレージシステム内のボリュームに格納されたデータを暗号化できます。データを暗号化すると、ストレージシステムまたはストレージシステム内のドライブを交換するとき、あるいは、これらが盗難に遭ったときに情報の漏えいを防ぐことができます。

Encryption License Key を使用するには、Encryption License Key プログラムプロダクトのライセンスキーに加えて、次に示すハードウェアが必要です。

- VSP G150、VSP G350、VSP G370、VSP F350 および VSP F370 の場合：
  暗号化に対応したコントローラ（ECTL）
- VSP G700、VSP G900、VSP F700、および VSP F900 の場合：
  暗号化に対応したディスクボード（EDKB）
- VSP E990 の場合：
  暗号化に対応した NVMe ドライブ用のディスクボード（EDKBN）

Encryption License Key は、ボリュームに格納されたデータを暗号化できます。 データの暗号化は内部ボリュームの一部またはすべてに適用でき、データの入出力で処理時間や待ち時間に影響を与えることや、既存のアプリケーションやインフラストラクチャに損害を与えることがありません。Encryption License Key には、使用に際して簡単で安全な、鍵管理機能が備わっています。

Encryption License Key の操作は、SVP がある構成では Storage Navigator の画面、SVP がない構成では REST API で実行します。ただし、Encryption License Key に関する設定ができるのは、セキュリティ管理者（参照・編集）ロールを持ったユーザアカウントだけです。ユーザアカウントの詳細は、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

Storage Navigator および REST API でサポートしている機能を次に示します。

機能	Storage Navigator	REST API
暗号化環境設定の編集	○	○※
暗号化鍵の一覧表示/取得	○	○
暗号化環境設定編集での設定内容確認	○	○※
暗号化鍵数表示/取得	○	○
暗号化鍵生成	○	○※
パスワードポリシー編集	○	×
管理クライアント内にファイルとして暗号化鍵をバックアップ	○	○※
鍵管理サーバに接続して暗号化鍵をバックアップ	○	×
管理クライアント内のファイルから暗号化鍵をリストア	○	○※
鍵管理サーバに接続して暗号化鍵をリストア	○	×
管理クライアント内のファイルから暗号化鍵を強制リストア	○	○※
鍵管理サーバに接続して暗号化鍵を強制リストア	○	×
鍵管理サーバに接続して暗号化鍵を定期バックアップ	○	×
未使用暗号化鍵の削除および生成	○	○※
鍵管理サーバにバックアップしたバックアップデータの一覧表示	○	×
鍵管理サーバにバックアップしたバックアップデータの削除	○	×

機能	Storage Navigator	REST API
認証用鍵の更新	○	×
鍵暗号化鍵の更新	○	×
鍵暗号化鍵の再取得	○	×
暗号化有効および無効設定(パリティグループ単位)	○	×
パリティグループ作成時の暗号化有効設定	○	○

注※

ストレージシステムの暗号化環境が、鍵管理サーバと連携するよう設定されている場合、REST API では操作できません。

凡例

○：操作できる
×：操作できない

メモ

- 次のストレージシステム（バージョン）では、Encryption License Key を使用できません。
  - Virtual Storage Platform G130 （すべてのファームウェアバージョン）
  - Virtual Storage Platform E990（ファームウェアバージョン 93-02-01-XX/XX 未満）
- REST API を使用して、データを暗号化する手順や要件については『REST API リファレンスガイド』を参照してください。
- Storage Navigator を使用して、暗号化が有効なパリティグループを生成する手順については『システム構築ガイド』、REST API を使用して、暗号化が有効なパリティグループを生成する手順については『REST API リファレンスガイド』 を参照してください。

1.2 暗号化の仕様

1.2.1 ハードウェアの仕様

暗号アルゴリズム

Advanced Encryption Standard (AES) 256 bit

暗号モード

XTS モード

暗号モジュール規格

モデル	説明
VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370	FIPS 140-2 Level 1 準拠
VSP G700、VSP G900、VSP F700、および VSP F900	FIPS 140-2 Level 2 準拠
VSP E990	FIPS 140-2 Level 2 準拠

1.2.2 暗号化できるボリューム

ボリューム種別

すべてのボリュームタイプ

エミュレーションタイプ

すべてのエミュレーションタイプ

内部／外部ボリューム

内部ボリュームのみ

既存のデータの暗号化

可能

関連概念

- 1.4.1 データの暗号化

1.2.3 格納データ暗号化で使用する鍵

格納データ暗号化において使用する鍵の属性

格納データ暗号化で使用する鍵は、属性「空き」として生成し、用途に応じて各々の属性が設定されます。

- 空き：未使用鍵。格納データ暗号化において、生成され割り当て前の鍵
- DEK：データ暗号化鍵。格納したデータを暗号化するための鍵
- CEK：認証用鍵。証明書を暗号化するための鍵、かつ ECTL、EDKB または EDKBN に DEK を登録する際に DEK を暗号化するための鍵
- KEK：鍵暗号化鍵。格納データ暗号化において、ストレージシステム内に 1 つのみ存在する、属性が「KEK」以外の鍵を暗号化するための鍵

以降では、属性が「KEK」以外の鍵をまとめて暗号化鍵と呼びます。

暗号化鍵の数

作成できる暗号化鍵の数は次のとおりです。下記に加えて、KEK が常に 1 つ存在します。

モデル	DEK の最大数	CEK の最大数	ストレージシステムごとの暗号化鍵の最大数
VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370	372	4	1,024
VSP G700 および VSP F700	1,200	8	4,096
VSP G900 および VSP F900	1,440	16	4,096
VSP E990	96	16	4,096

暗号化鍵を設定する単位

DEK：ドライブ単位に 1 つ

CEK：EDKB、EDKBN または ECTL 単位に 2 つ

1.3 暗号化鍵の管理機能

格納データ暗号化で使用する鍵は、セキュリティ管理者（参照・編集）ロールを持ったユーザが SVP あり構成の場合は Storage Navigator、SVP なし構成の場合は REST API を使用して作成できます。

ストレージシステムごとに作成できる暗号化鍵の数は次のとおりです。

モデル	ストレージシステムごとに作成できる暗号化鍵の数
VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370	1,024
VSP G700 および VSP F700	4,096
VSP G900 および VSP F900	4,096
VSP E990	4,096

ただし、初めて暗号化環境を設定したときに作成される暗号化鍵の数は次のとおりです。

モデル	初めて暗号化環境を設定したときに作成される暗号化鍵数※
VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370	1,022
VSP G700 および VSP F700	4,092
VSP G900 および VSP F900	4,088
VSP E990	4,088

注※

暗号化に対応したディスクボード（EDKB）または暗号化に対応した NVMe ドライブ用のディスクボード（EDKBN）が最大数まで搭載されている場合。構成によって異なります。

暗号化環境設定が完了してから再度暗号化環境設定を実施したときは、暗号化鍵と認証用鍵（CEK）の更新、および未使用鍵の作成は行われません。前回作成した暗号化鍵がそのまま使用されます。

データの有用性を確実にするため、Encryption License Key には暗号化鍵のバックアップとリストア機能があります。

関連概念

- 1.3.1 暗号化鍵の使用
- 1.3.2 暗号化鍵のバックアップ機能
- 1.3.3 暗号化鍵のリストア機能
- 1.3.4 鍵管理サーバを使用した暗号化鍵の操作

1.3.1 暗号化鍵の使用

暗号化環境設定が完了している場合、次の操作および保守作業をしたときに暗号化鍵を使用します。

ドライブに関連する保守操作時

保守操作	使用される鍵数	備考
ドライブ増設	ドライブあたり 1 個	増設するドライブ数分必要となります。
ドライブのリプレース	ドライブあたり 1 個	リプレースするドライブ数分必要となります。
パリティグループの暗号化解除時	ドライブあたり 1 個	解除対象となるパリティグループに含まれるドライブ数分必要となります。

ディスクボード(DKB)に関連する保守操作時

保守操作	使用される鍵数		備考
	VSP G700 および VSP F700、または VSP G900 および VSP F900 [EDKB 使用]	VSP E990 [EDKBN 使用]	
ディスクボード(DKB)の増設時	DKB あたり 3 個	DKB あたり 2 個	増設する DKB（EDKB または EDKBN）数分必要となります。
ディスクボード(DKB)のリプレース時	DKB あたり 3 個	DKB あたり 2 個	リプレースする DKB（EDKB または EDKBN）数分必要となります。

暗号化に対応したコントローラに関連する保守操作時

セキュリティ運用操作	使用される鍵数	備考
	VSP G150、VSP G350 および VSP F350、または VSP G370 および VSP F370	
コントローラリプレース時	コントローラあたり 3 個	リプレースするコントローラ（ECTL）数分必要となります。

セキュリティ運用操作時

セキュリティ運用操作	使用される鍵数	備考
認証用鍵の更新時	実装されている DKB あたり 2 個	システム内に実装されている全 DKB 数分必要になります。

上記の操作および保守作業中に障害が発生した場合、回復のために上記の数以上の未使用鍵が使用される場合があります。

関連概念

- 1.3 暗号化鍵の管理機能

1.3.2 暗号化鍵のバックアップ機能

暗号化鍵のバックアップ機能について説明します。

関連概念

- 1.3 暗号化鍵の管理機能
- (1)　暗号化鍵の一次バックアップと二次バックアップ
- (2)　暗号化鍵の定期バックアップ

(1)　暗号化鍵の一次バックアップと二次バックアップ

暗号化鍵のバックアップには、一次バックアップと二次バックアップがあります。

- 暗号化鍵の一次バックアップは、ストレージシステムによって自動的に行われます。 一次バックアップでは、暗号化鍵はストレージシステム内のキャッシュフラッシュメモリにバックアップされます。
- 暗号化鍵の二次バックアップは、SVP あり構成の場合は Storage Navigator、SVP なし構成の場合は REST API を使用してユーザが実施します。このため、二次バックアップした暗号化鍵は、ユーザが責任を持って保管してください。二次バックアップは、一次バックアップが利用できなくなった場合、暗号化鍵をリストアするときに必要となります。二次バックアップを実施するには、専用の操作権限（セキュリティ管理者（参照・編集）ロール）が必要です。

注意
一次バックアップでバックアップした暗号化鍵が使用できず、かつ、二次バックアップでバックアップした暗号化鍵も使用できない場合は、データの復号化ができません。

暗号化鍵を作成したらすぐに二次バックアップを行ってください。また、データの有用性を確実にするためにも、定期的に（例えば週に一回）バックアップを行ってください。

二次バックアップには、管理クライアント内にファイルとしてバックアップする方法と、鍵管理サーバに接続してバックアップする方法があります。

暗号化鍵を管理クライアント内にファイルとしてバックアップするときはパスワードを設定します。このパスワードは暗号化鍵をリストアするときに必要です。SVP あり構成の場合、このパスワードに使用する最小文字数を［パスワードポリシー編集（暗号化鍵バックアップ）］画面で設定できます。鍵管理サーバに接続してバックアップしている場合、鍵管理サーバがバックアップできる鍵の数には上限があります。このため、鍵管理サーバ上の暗号化鍵は定期的に削除してください。

暗号化鍵のバックアップは、作成済みの暗号化鍵に対して一括して実施されます。

作成済みの暗号化鍵および認証用鍵がない状態では､暗号化鍵のバックアップはできません。また、SVP あり構成で Storage Navigator から暗号化鍵をバックアップするときは、タスクに他の処理が登録されていないことを確認してください。タスクに他の処理が登録されていると暗号化鍵のバックアップができません。

関連概念

- 1.3.2 暗号化鍵のバックアップ機能

関連タスク

- 3.3.1 管理クライアント内に暗号化鍵をファイルとしてバックアップするときに設定するパスワードの最小文字数を設定する
- 3.3.2 管理クライアント内にファイルとして暗号化鍵をバックアップする
- 3.3.3 鍵管理サーバに接続して暗号化鍵をバックアップする

(2) 暗号化鍵の定期バックアップ

［暗号化環境設定編集］画面で暗号化鍵をバックアップしたい時間を指定すると、鍵管理サーバ上に最新のバックアップが存在しない場合、毎日指定した時間に、自動的に暗号化鍵が鍵管理サーバにバックアップを試みます。これを定期バックアップと呼びます。

メモ
最新のバックアップがすでに存在する場合、定期バックアップはタスクとしてキューイングされずにスキップされます。
このとき、［タスク］画面や監査ログには出力されませんが、問題ありません。定期バックアップが必要なのに失敗した場合は、監査ログで確認できます。

定期バックアップは、ユーザが Storage Navigator にログインしていなくても実行されます。

［暗号化環境設定編集］画面で指定した時間になると、暗号化鍵のバックアップ処理がタスクとしてキューイングされ、キューイングされた順にタスクが実行されます。キューイングされたタスクは［タスク］画面で確認できます。すでに別のタスクがキューイングされている場合、定期バックアップは、そのタスクが完了するまで実行されません。このため、実際に定期バックアップが実行される時間が、［暗号化環境設定編集］画面で指定した時間と異なる場合があります。また、鍵管理サーバ上に最新のバックアップがすでに存在する場合、同じ暗号化鍵を再度バックアップする必要がないため、定期バックアップはスキップされます。

定期バックアップを実行するには、定期バックアップを実行する専用のユーザ（定期バックアップユーザと呼びます）を作成した上で、［暗号化環境設定編集］画面で定期バックアップユーザのユーザ名とパスワードを入力する必要があります。ユーザの作成については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

メモ
定期バックアップの結果は［タスク］画面および監査ログで確認できます。定期バックアップの結果を定期的に確認されることをお勧めします。監査ログは、定期バックアップユーザの名前で出力されます。

キューイングされた定期バックアップ以外のタスクが完了せず、定期バックアップのタスクが実行されない状態で、次の定期バックアップの時間になった場合、その定期バックアップのタスクはキューイングされず、定期バックアップは一回だけ実行されます。例えば、定期バックアップの時間を午前 0 時と午前 2 時に指定した状態で、午前 0 時より前に実行した定期バックアップ以外のタスクが午前 3 時に完了した場合、午前 2 時の定期バックアップのタスクはキューイングされず、定期バックアップは午前 3 時から一回だけ実行されます。

定期バックアップを停止する場合は、［暗号化環境設定編集］画面の［鍵管理サーバへ暗号化鍵定期バックアップを有効にする］に付いているチェックマークを解除して定期バックアップを無効にしてください。

定期バックアップを実行すると古い暗号化鍵は削除されます。このため、定期バックアップでバックアップした暗号化鍵は常に一つになります。手動でバックアップした暗号化鍵は削除されません。定期バックアップでバックアップした暗号化鍵は、手動でバックアップした暗号化鍵と同様に、暗号化鍵の状態を確認したり、リストアおよび削除ができます。

SVP が停止している間は、定期バックアップが実行されません。SVP の起動が完了した後、定期バックアップの時間になると、暗号化鍵のバックアップ処理がタスクとしてキューイングされます。

注意
定期バックアップは、補助的な機能です。このため、必ず自動または手動によるバックアップを併せて実行してください。特に、次の操作をしたときは必ずバックアップを実行してください。

- 暗号化鍵の作成

注意
定期バックアップユーザの編集（ユーザ削除、パスワード変更、ロール変更など）を行うと、定期バックアップが失敗する可能性があります。このため、定期バックアップユーザを編集したときは、再度［暗号化環境設定編集］画面で定期バックアップユーザを設定してください。

注意
Encryption License Key プログラムプロダクトのライセンスが期限切れになるか、または削除された場合は、定期バックアップを実行できません。定期バックアップを実行するには Encryption License Key プログラムプロダクトのライセンスを有効にしてください。

注意
保守用 PC または SVP のタイムゾーンを変更したときは、必ず［Storage Device List］画面ですべてのストレージシステムのサービスを再起動してください。サービスを再起動しない場合、設定した時刻どおりに定期バックアップが実行されません。

注意
定期バックアップの実行中は、保守員によるストレージシステムの保守作業や SVP の操作ができなくなります。 保守作業の時間と定期バックアップの時間が重なる場合は、定期バックアップを一時的に解除するか、設定を変更してください。

関連概念

- 1.3.2 暗号化鍵のバックアップ機能

関連タスク

- 3.1.2 暗号化環境を設定する

(3) 暗号化鍵の自動バックアップ

鍵管理サーバを使用している場合は、暗号化鍵を作成後、自動的にバックアップされます。これを自動バックアップといいます。

鍵管理サーバを使用していない場合は、自動バックアップは実施されません。

1.3.3 暗号化鍵のリストア機能

不具合などによって既存の暗号化鍵が利用できなくなった場合、暗号化鍵は一次バックアップまたは二次バックアップからリストアされます。

注意
最新の暗号化鍵をリストアしてください。二次バックアップ後に暗号化鍵が変更されたなどの理由によって最新でない暗号化鍵はリストアできません。

- 一次バックアップからの暗号化鍵のリストアは、ストレージシステムによって自動的に行われます。
- 二次バックアップからの暗号化鍵のリストアは、Storage Navigator を使用してユーザが実施します。二次バックアップから最新の暗号化鍵のリストアするには、専用の操作権限（セキュリティ管理者（参照・編集）ロール）が必要です。二次バックアップから最新ではない暗号化鍵のリストアするには、専用の操作権限（セキュリティ管理者（参照・編集）ロールと保守（ベンダ専用）ロール）が必要です。
  二次バックアップからの暗号化鍵のリストアには、管理クライアント内にバックアップしたファイルからリストアする方法と、鍵管理サーバに接続してリストアする方法があります。

関連概念

- 1.3 暗号化鍵の管理機能

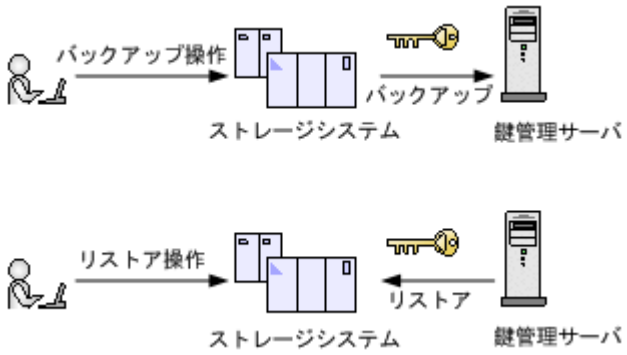
関連タスク

- 3.6.1 管理クライアント内にバックアップしたファイルから暗号化鍵をリストアする
- 3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする

1.3.4 鍵管理サーバを使用した暗号化鍵の操作

暗号化鍵を管理するための規格である KMIP（Key Management Interoperability Protocol）に準じた鍵管理サーバで作成した暗号化鍵を使用できます。また、鍵管理サーバに暗号化鍵をバックアップでき、鍵管理サーバにバックアップした暗号化鍵から暗号化鍵をリストアできます。

暗号化鍵は、鍵管理サーバにバックアップされるときに別の暗号化鍵で暗号化され、その暗号化鍵とともに鍵管理サーバに格納されます。



関連概念

- 1.3 暗号化鍵の管理機能

関連タスク

- 3.3.3 鍵管理サーバに接続して暗号化鍵をバックアップする
- 3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする
- 3.9 鍵管理サーバ上にある暗号化鍵の状態を確認する

1.4 データの暗号化機能

データの暗号化機能について説明します。

関連概念

- 1.4.1 データの暗号化
- 1.4.2 暗号化の解除
- 1.4.3 データ暗号化鍵の変更

1.4.1 データの暗号化

Encryption License Key では、パリティグループごとにデータを暗号化できます。パリティグループに対して暗号化を設定すると、そのパリティグループに属するボリュームがフォーマットされます。これを暗号化フォーマットと呼びます。暗号化フォーマットでは、ディスク領域全体に暗号化した 0 データを書き込むことで領域全体をフォーマットします。

このため、データの暗号化には注意が必要です。パリティグループ内の必要なデータは、暗号化を設定する前に責任を持ってバックアップしておいてください。あるいは、パリティグループの増設

時や LDEV フォーマット機能を利用したフォーマット時など、パリティグループ全体をフォーマットする前に、暗号化を設定してください。

暗号化を設定するには、セキュリティ管理者（参照・編集）ロールを持ったユーザである必要があります。また、フォーマットを同時にする場合は、セキュリティ管理者（参照・編集）ロールとストレージ管理者（プロビジョニング）ロールを持ったユーザである必要があります。

既存のデータを暗号化する

既存のデータを暗号化する場合は、データの移行が必要です。あらかじめ暗号化を設定したパリティグループを作成し、Volume Migration、または ShadowImage や TrueCopy などのコピー系プログラムプロダクトを使用してデータを移行します。データは LDEV 単位で移行します。

Volume Migration を使用したデータの移行については、『Volume Migration ユーザガイド』を参照してください。コピー系プログラムプロダクトを使用したデータの移行については、ご使用になるコピー系プログラムプロダクトのマニュアルを参照してください。

関連概念

- 1.4 データの暗号化機能
- 3.4 暗号化を有効にする

1.4.2 暗号化の解除

Encryption License Key では、パリティグループごとに暗号化を解除できます。パリティグループに対して暗号化を解除すると、パリティグループを構成するドライブの暗号化鍵は削除され、新しい暗号化鍵が割り当てられます。そのパリティグループに属するボリュームを利用するためには、フォーマットが必要となります。再度暗号化で使用する場合、暗号化を設定後に暗号化フォーマットを実施してください。

このため、暗号化の解除には注意が必要です。パリティグループ内の必要なデータは、暗号化を解除する前に責任を持ってバックアップしておいてください。あるいは、パリティグループの増設時や LDEV フォーマット機能を利用したフォーマット時など、パリティグループ全体をフォーマットする前に、暗号化を解除してください。

暗号化を解除するには、セキュリティ管理者（参照・編集）ロールを持ったユーザである必要があります。また、フォーマットを同時にする場合は、セキュリティ管理者（参照・編集）ロールとストレージ管理者（プロビジョニング）ロールを持ったユーザである必要があります。

関連概念

- 1.4 データの暗号化機能
- 3.5 暗号化を無効にする

1.4.3 データ暗号化鍵の変更

暗号化したデータを別の暗号化鍵で暗号化する場合は、データの移行が必要です。あらかじめ別の暗号化鍵を設定したパリティグループを作成し、Volume Migration、または ShadowImage や TrueCopy などのコピー系プログラムプロダクトを使用してデータを移行します。データは LDEV 単位で移行します。

Volume Migration を使用したデータの移行については、『Volume Migration ユーザガイド』を参照してください。コピー系プログラムプロダクトを使用したデータの移行については、ご使用になるコピー系プログラムプロダクトのマニュアルを参照してください。

データを移行後、移行元パリティグループの暗号化を解除すると、そのパリティグループを構成するドライブに割り当てられた暗号化鍵は削除され、新しい暗号化鍵が割り当てられます。また、ドライブを交換すると、そのドライブに割り当てられた暗号化鍵は削除されます。交換または増設などによって新しいドライブを実装したときに、新しい暗号化鍵が割り当てられます。

関連概念

- 1.4 データの暗号化機能

1.5 監査ログ機能

監査ログ機能を使用して、ストレージシステム上の Encryption License Key に関する操作の履歴を取得できます。監査ログファイルには、暗号化鍵の操作やデータの暗号化の操作などの Encryption License Key に関する操作の履歴が記録されます。

監査ログおよび監査ログの履歴に関する詳細については、『監査ログ リファレンスガイド』を参照してください。

2

Encryption License Key を利用するための準備

ここでは、Encryption License Key を利用するための準備について説明します。

2.1 システムの要件

格納データ暗号化機能を使用して、データを暗号化するためのシステム要件を以下に示します。

項目	必要事項
ファームウェアバージョン	• VSP G150, G350, G370, G700, G900 および VSP F350, F370, F700, F900 ◦ SVP あり構成で Encryption License Key を使用する場合 88-00-0x 以降の DKCMAIN ファームウェア ◦ SVP なし構成で Encryption License Key を使用する場合 88-03-2x-xx 以降の DKCMAIN ファームウェア • VSP E990 ◦ 93-02-01-xx 以降の DKCMAIN ファームウェア
ライセンスキー	Encryption License Key プログラムプロダクトのライセンスキーが必要です。
ロール	暗号化の設定および解除、暗号化鍵をバックアップおよびリストアするには、セキュリティ管理者（参照・編集）ロールが必要です。
SVP	Storage Navigator を用いて、Encryption License Key を使用するには SVP が必要です。また、鍵暗号化鍵を鍵管理サーバで保護する場合、SVP は常に起動している必要があります。
DNS サーバ	鍵管理サーバに、IP アドレスではなくホスト名を指定して接続する場合は、DNS サーバの設定が必要です。DNS サーバの IP アドレスを SVP に設定してください。
ホストのプラットフォーム	すべてのプラットフォームがサポートされています。
データボリューム	すべてのボリュームタイプおよびすべてのエミュレーションタイプがサポートされています。 データを暗号化できるのは、ストレージシステムの内部ボリュームだけです。外部ボリュームは暗号化できません。
暗号化に対応した NVMe ドライブ用のディスクボード（EDKBN）または暗号化に対応したディスクボード（EDKB）	暗号化に対応した NVMe ドライブ用のディスクボードまたは暗号化に対応したディスクボードが必要です。

2.2 鍵管理サーバの要件

鍵管理サーバを使用する場合、鍵管理サーバは次の要件を満たしている必要があります。最新の検証済み鍵管理サーバ、および、そのファームウェアバージョンについては、「4.2 お問い合わせ先」へお問い合わせください。

- 前提プロトコル
  Key Management Interoperability Protocol 1.0（KMIP1.0）
- 前提ソフトウェア
  - SafeNet KeySecure k460
  - Enterprise Secure Key Manager
- 証明書

KMIP サーバへ接続するには、次の証明書を SVP にアップロードする必要があります。

証明書の種別	形式	要件
鍵管理サーバのルート証明書	X.509 形式	なし
PKCS#12 形式のクライアント証明書	PKCS#12 形式	• 中間証明書が存在する場合は、中間証明書を含んだ証明書チェーンで構成された、署名付き公開鍵証明書を準備しておくこと • アップロードする証明書の証明書チェーンの階層数は、ルート CA 証明書を含めて 5 階層以下であること • アップロードする証明書の公開鍵暗号方式が RSA であること
KMIP サーバに設定されているサーバ証明書	—	• サーバ証明書の公開鍵暗号方式が RSA であること

これらの証明書については鍵管理サーバの管理者にお問い合わせください。証明書の管理については鍵管理サーバの管理者とご相談の上、適切に管理してください。
証明書には期限があります。期限が切れると鍵管理サーバと接続できなくなるため、証明書を準備するときは期限の設定にご注意ください。
X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される「基本制限（BasicConstraints）」、「キー使用法（KeyUsage）」、「サブジェクトキー識別子（SubjectKeyIdentifier）」をサポートしています。
クライアント証明書は、PKCS#12 形式に変換する必要があります。また、PKCS#12 形式に変換する前のクライアント証明書は、鍵管理サーバの CA 局（Certificate Authority）によって署名されている必要があります。
PKCS#12 形式のクライアント証明書に設定されたパスワードがわからない場合は、鍵管理サーバの管理者にお問い合わせください。

- その他
  鍵暗号化鍵を鍵管理サーバで保護する場合、鍵管理サーバはクラスタ化された 2 台のサーバによって構成されている必要があります。

2.2.1 鍵管理サーバのルート証明書の取得

鍵管理サーバのルート証明書は、鍵管理サーバのソフトウェアが Safenet KeySecure k460、Thales keyAuthority、または Enterprise Secure Key Manager 4.1 の場合、鍵管理サーバ上で作成および取得できます。詳細については、Safenet KeySecure k460、Thales keyAuthority、または Enterprise Secure Key Manager 4.1 のマニュアルを参照してください。

2.2.2 クライアント証明書の取得の流れ

クライアント証明書を取得するには、クライアント証明書を作成するためのプログラムが必要です。クライアント証明書を作成するためのプログラムは、OpenSSL のホームページ（http://www.openssl.org/）からダウンロードしてください。ここでは、OpenSSL が `C:¥openssl` フォルダにインストールされているものとします。

または SVP の OpenSSL を使用してください。SVP の OpenSSL の格納先ディレクトリは `C:¥Mapp¥OSS¥apache¥bin¥openssl` です。

クライアント証明書は、PKCS#12 形式に変換する必要があります。

以下に例として、OS に Windows を使用して秘密鍵と公開鍵を作成し、作成した公開鍵を鍵管理サーバの CA 局に署名してもらうことでクライアント証明書を取得する手順を説明します。

操作手順

1. 秘密鍵（.key ファイル）を作成します。
   秘密鍵を作成する方法については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。
2. 公開鍵（.csr ファイル）を作成します。
   公開鍵を作成する方法については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。
3. 作成した公開鍵を鍵管理サーバの CA 局に署名してもらうことで証明書を取得します。この証明書をクライアント証明書として使用します。
   詳細については、Safenet KeySecure k460、Thales keyAuthority、または Enterprise Secure Key Manager 4.1 のマニュアルを参照してください。
4. Windows のコマンドプロンプト上で、カレントディレクトリを PKCS#12 形式のクライアント証明書ファイルを出力するフォルダがあるディレクトリに移動します。
5. 秘密鍵（.key ファイル）およびクライアント証明書をこのフォルダに移動し、次に示すコマンドを実行します。なお、この例では次の条件でコマンドを実行しています。
   ・PKCS#12 形式のクライアント証明書ファイルを出力するフォルダ：c:¥key
   ・秘密鍵のファイル名：client.key
   ・クライアント証明書のファイル名：client.crt
   OpenSSL をインストールした場合：`C:¥key>c:¥openssl¥bin¥openssl pkcs12 -export -in client.crt -inkey client.key -out client.p12`
   SVP の OpenSSL を使用する場合：`C:¥key>c:¥Mapp¥OSS¥apache¥bin¥openssl pkcs12 -export -in client.crt -inkey client.key -out client.p12`

   ヒント
   `C:¥Mapp`：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。
   「`C:¥Mapp`」以外をインストールディレクトリに指定した場合は、「`C:¥Mapp`」を、指定のインストールディレクトリに置き換えてください。

6. 任意のパスワードを入力します。
   このパスワードは、PKCS#12 形式のクライアント証明書を SVP にアップロードするときに使用します。
   PKCS#12 形式のクライアント証明書を作成するときに入力するパスワードは 0 文字以上 128 文字以下で、使用できる文字は次のとおりです。
   - 数字（0 から 9）
   - 英大文字（A から Z）
   - 英小文字（a から z）
   - 半角記号 31 種：`! # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ¥ ] ^ _ ` { | } ~`

この例では、client.p12 ファイルが `c:¥key` フォルダに作成されます。この client.p12 ファイルが PKCS#12 形式に変換されたクライアント証明書です。

2.2.3 証明書のアップロード

鍵管理サーバへの接続を設定するときに、[暗号化環境設定編集] 画面で鍵管理サーバのルート証明書および PKCS#12 形式のクライアント証明書を SVP にアップロードする必要があります。

2.3 他のプログラムプロダクトとの併用

Encryption License Key と他のプログラムプロダクトとの併用について説明します。

2.3.1 Encryption License Key とコピー系プログラムプロダクトの併用

プライマリボリュームに暗号化を設定する場合は、セカンダリボリュームにも暗号化を設定してください。セカンダリボリュームに暗号化を設定しない場合、セカンダリボリュームのデータは暗号化されません。この場合、セカンダリボリュームのデータの機密性は保証できません。

2.3.2 Encryption License Key と Thin Image の併用

プライマリボリュームに暗号化を設定する場合、プールは暗号化を設定したプールボリュームだけで構成してください。暗号化を設定していないプールボリュームがある場合、プライマリボリュームの差分データは暗号化されていないデータとして格納されます。この場合、セカンダリボリュームのデータの機密性は保証できません。

プライマリボリュームの暗号化の状態とプールの暗号化の状態が異なる場合（例えば、プライマリボリュームには暗号化が設定されていないがプールは暗号化を設定したプールボリュームだけで構成されている、など）、セカンダリボリュームには暗号化されたデータと暗号化されていないデータが混在します。データの機密性を保つためにも、プライマリボリュームの暗号化の状態とプールの暗号化の状態は同じにしてください。

2.3.3 Encryption License Key と Universal Replicator の併用

プライマリボリュームに暗号化を設定する場合は、セカンダリボリュームにも暗号化を設定してください。セカンダリボリュームに暗号化を設定しない場合、セカンダリボリュームのデータは暗号化されません。この場合、セカンダリボリュームのデータの機密性は保証できません。

プライマリボリュームに暗号化を設定する場合、ジャーナルは暗号化を設定したジャーナルボリュームだけで構成してください。暗号化を設定していないジャーナルボリュームがある場合、プライマリボリュームのジャーナルは暗号化されていないデータとして格納されるため、データの機密性を保証できません。これはセカンダリボリュームについても同様です。

2.3.4 Encryption License Key と Volume Migration の併用

ソースボリュームに暗号化を設定する場合は、ターゲットボリュームにも暗号化を設定してください。ターゲットボリュームに暗号化を設定しない場合、ターゲットボリュームのデータは暗号化されません。この場合、ターゲットボリュームのデータの機密性は保証できません。

2.3.5 Encryption License Key と、Dynamic Provisioning、Dynamic Tiering、および active flash の併用

仮想ボリュームを経由してプールに書き込まれたデータを暗号化する場合は、暗号化を設定したプールボリュームだけで構成されたプールを使用してください。暗号化を設定した場合、プールボリュームと仮想ボリュームの暗号化フォーマットが必要です。

2.3.6 Encryption License Key と dedupe and compression の併用

暗号化を解除するときは、仮想ボリュームに設定した容量削減機能の設定を無効にする必要があります。

2.4 Storage Navigator の設定の流れ

システムの要件がそろったことを確認できたら、Encryption License Key を操作できるように Storage Navigator を設定します。

操作手順

1. Storage Navigator にログインします。
2. Encryption License Key プログラムプロダクトのライセンスを有効にしてください。
   Encryption License Key プログラムプロダクトのライセンスが期限切れになるか、または削除された場合は、暗号化鍵を削除できません。
3. 暗号化鍵のバックアップおよびリストアを担当するユーザにセキュリティ管理者（参照・編集）ロールを割り当てます。

各操作の詳細については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

2.5 Encryption License Key の使用を取りやめる場合

データを暗号化したあとに Encryption License Key の使用を取りやめる場合は、次の操作が必要になります。

注意
ライセンスキーを削除する前に手順 1 および手順 2 の操作が必要です。ライセンスキーを削除すると手順 1 および手順 2 の操作ができなくなります。

操作手順

1. すべてのパリティグループについて、データの暗号化を無効にしてください。
   パリティグループに属するすべてのボリュームについて、データの暗号化を無効にする必要があります。
2. ［暗号化環境設定編集］画面で、暗号化環境設定を初期化してください。
3. Encryption License Key プログラムプロダクトのライセンスキーを削除してください。

3

Encryption License Key の操作

ここでは、Encryption License Key の操作について説明します。

3.1 暗号化環境設定の編集

暗号化環境設定の編集について説明します。

関連タスク

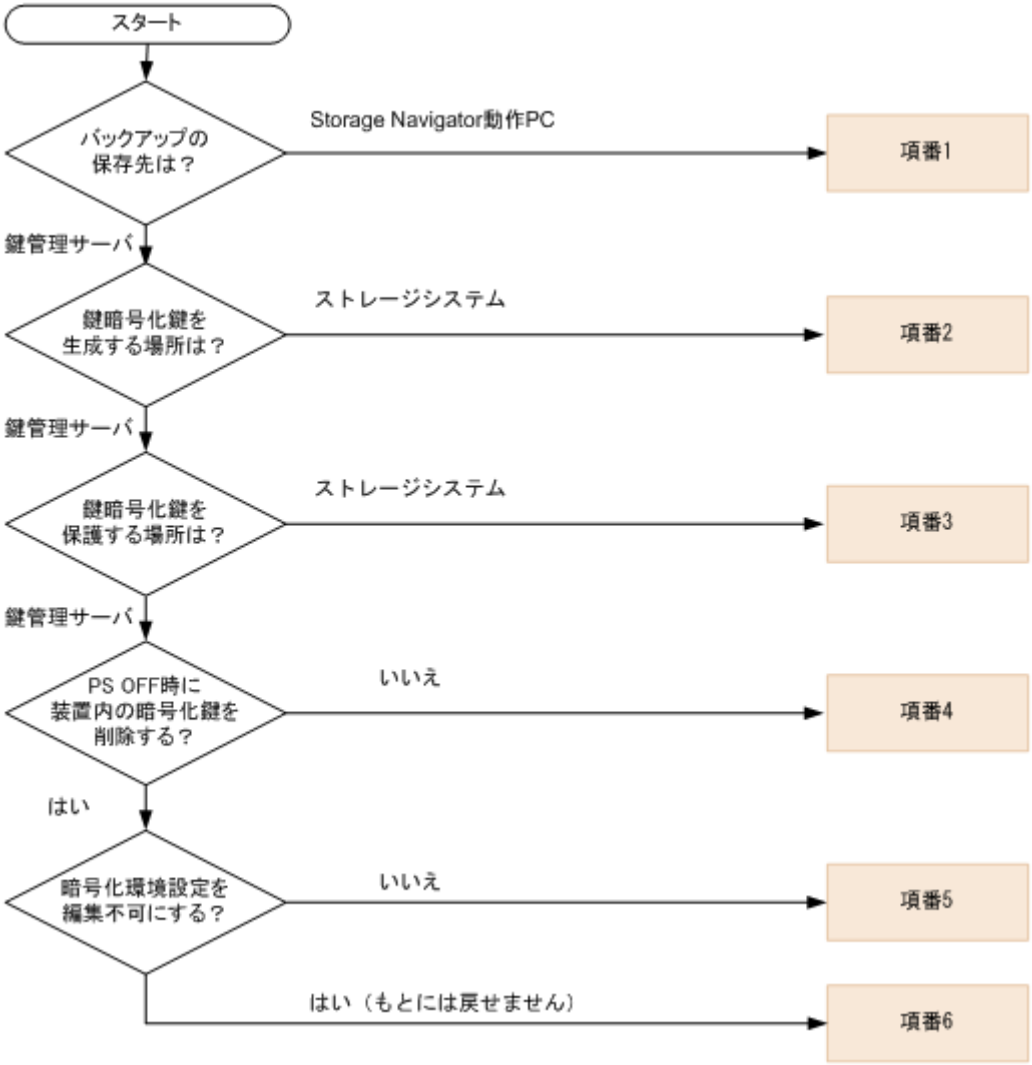
- 3.1.2 暗号化環境を設定する

関連参照

- 3.1.1 暗号化鍵の管理方法と［暗号化環境設定編集］画面の設定内容との関係

3.1.1 暗号化鍵の管理方法と［暗号化環境設定編集］画面の設定内容との関係

暗号化鍵の生成場所や保管場所など、暗号化鍵の管理方法によって［暗号化環境設定編集］画面で指定する項目が異なります。次のフローで暗号化鍵の管理方法を確認し、下の表で［暗号化環境設定編集］画面で設定する内容を確認してください。フロー中の項番は、表の項番に対応しています。



項番	［暗号化環境設定編集］画面の設定						
	［鍵管理サーバ］	［サーバ設定］		［鍵管理サーバで暗号化鍵生成］	［鍵暗号化鍵を鍵管理サーバで保護する］	［PS OFF 時に装置内の暗号化鍵を削除する］	［ローカル鍵生成を無効にする］
		［プライマリサーバ］	［セカンダリサーバ］				
1	［無効］を選択する	設定しない	設定しない	×	×	×	×
2	［有効］を選択する	設定する	使用する場合は、［有効］を選択して設定する	×	×	×	×
3	［有効］を選択する	設定する	使用する場合は、［有効］を選択して設定する	○	×	×	×
4	［有効］を選択する	設定する	［有効］を選択して設定する	○	○	×	×
5	［有効］を選択する	設定する	［有効］を選択して設定する	○	○	○	×
6	［有効］を選択する	設定する	［有効］を選択して設定する	○	○	○	○

（凡例）

○：チェックボックスを選択する

×：チェックボックスを選択しない

関連概念

- 3.1 暗号化環境設定の編集

3.1.2 暗号化環境を設定する

鍵管理サーバを使用するには、鍵管理サーバへの接続設定やネットワークの設定が必要です。ほかにもローカル鍵生成を無効にしたり、鍵暗号化鍵を DKC に保存したりするなどの暗号化環境を設定します。鍵管理サーバへの接続設定に必要な値については、各サーバの管理者にお問い合わせください。ネットワークの設定については、ネットワークの管理者にお問い合わせください。

注意
鍵管理サーバにバックアップされる暗号化鍵はクライアント証明書と関連づけられて管理されます。このため、クライアント証明書を変更した場合、クライアント証明書を変更する前にバックアップした暗号化鍵をリストアできなくなります。クライアント証明書変更後は、必ず暗号化鍵をバックアップしてください。

注意
鍵管理サーバにバックアップされる暗号化鍵はクライアント証明書と関連づけられて管理されます。このため、クライアント証明書を紛失した場合、故障などによって SVP を交換すると SVP を交換する前にバックアップした暗号化鍵をリストアできなくなります。

また、鍵管理サーバへの接続設定のバックアップにはクライアント証明書は含まれません。このため、設定完了後は必ず鍵管理サーバへの接続設定をバックアップするとともに、鍵管理サーバの管理者とご相談の上、クライアント証明書を別途保管してください。

注意
鍵暗号化鍵を鍵管理サーバで保護する場合、鍵管理サーバはクラスタ化された 2 台のサーバによって構成されている必要があります。このため、鍵暗号化鍵を鍵管理サーバで保護する場合は［セカンダリサーバ］を［有効］に設定してください。

注意
［鍵管理サーバで暗号化鍵生成］にある［鍵暗号化鍵を鍵管理サーバで保護する］および［注意事項に同意する］のチェックボックスを選択して設定を完了すると、装置の電源を ON にしたときに鍵管理サーバからバックアップした鍵暗号化鍵を取得します。このとき、鍵管理サーバとの通信が確立されている必要があります。このため、SVP と鍵管理サーバが通信できることを確認してから装置の電源を ON にしてください。

注意
［鍵管理サーバで暗号化鍵生成］にある［PS OFF 時に装置内の暗号化鍵を削除する］および［注意事項に同意する］のチェックボックスを選択して設定を完了すると、装置の電源を ON にしたときに鍵管理サーバからバックアップした暗号化鍵を取得します。このとき、鍵管理サーバとの通信が確立されている必要があります。このため、SVP と鍵管理サーバが通信できることを確認してから装置の電源を ON にしてください。

メモ
- 定期バックアップを実行するには、定期バックアップを実行する専用のユーザ（定期バックアップユーザと呼びます）を作成した上で、［暗号化環境設定編集］画面で定期バックアップユーザのユーザ名とパスワードを入力する必要があります。定期バックアップユーザには、セキュリティ管理者（参照・編集）ロールが必要です。ユーザの作成については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。
- 定期バックアップを実行する場合は、［暗号化環境設定編集］画面で次のことを確認してください。
  ・［鍵管理サーバ］で［有効］を選択していること
  ・鍵管理サーバのプライマリサーバが使用可能な状態であること。［サーバ構成テスト］の［チェック］をクリックして、接続テストが正常終了することを確認してください。
- 定期バックアップタスクの詳細を参照するには、ストレージ管理者（システムリソース管理）ロール、またはタスクを実行したユーザである必要があります。タスクの管理については、マニュアル『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール
- 鍵管理サーバに、IP アドレスではなくホスト名を指定して接続する場合は、SVP の OS のネットワーク設定に、DNS サーバが設定されていること。
- 鍵管理サーバを使用する場合は鍵管理サーバに登録されているクライアント証明書と鍵管理サーバのルート証明書を用意すること。それぞれの証明書については、鍵管理サーバの管理者にお問い合わせください。

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。

2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［暗号化環境設定編集］画面を表示します。
   - ［暗号化鍵］タブで［暗号化環境設定編集］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［暗号化環境設定編集］を選択します。
4. ［鍵管理サーバ］で［有効］または［無効］を選択します。
5. 鍵管理サーバへ接続する場合にプライマリサーバとセカンダリサーバの設定項目を入力します。
6. すでに鍵管理サーバが使用可能な場合、接続テストするときには［サーバ構成テスト］の［チェック］をクリックします。

   接続テストに失敗した場合はエラーの詳細が結果に表示されます。
7. 定期バックアップを実行する場合、［鍵管理サーバへ暗号化鍵定期バックアップを有効にする］にチェックマークを付けます。さらに［定期バックアップ時刻］で暗号化鍵をバックアップしたい時間を指定して、［定期バックアップユーザ］で定期バックアップユーザのユーザ名とパスワードを入力します。
8. 鍵管理サーバで暗号化鍵を生成する場合、［鍵管理サーバで暗号化鍵生成］にチェックマークを付けます。さらに鍵暗号化鍵を鍵管理サーバに保存する場合、［鍵暗号化鍵を鍵管理サーバで保護する］にチェックマークを付けてから、［注意事項に同意する］をチェックします。
9. 暗号化鍵を鍵管理サーバに保存し、装置電源 OFF 時に装置内の暗号化鍵を削除する場合、［PS OFF 時に装置内の暗号化鍵を削除する］にチェックマークを付けてから、［注意事項に同意する］をチェックします。
10. 暗号化鍵を鍵管理サーバ上で作成し、かつ、暗号化鍵をストレージシステム内に作成できないようにする場合は、［ローカル鍵生成を無効にする］にチェックマークを付けます。チェックマークを付けると、注意事項が表示されます。注意事項の内容をご確認の上、同意される場合は［注意事項に同意する］にチェックマークを付けてください。

注意
［鍵管理サーバで暗号化鍵生成］にある［ローカル鍵生成を無効にする］および［注意事項に同意する］のチェックボックスは、チェックマークを付けて設定を完了すると元に戻すことができません。チェックマークを付けるときには、設定をしても問題がないことをよく確認してください。

11. ［完了］をクリックします。

    ［設定確認］画面が表示されます。
12. 設定内容を確認し、［タスク名］にタスク名を入力します。
13. ［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとしてキューイングされ、順に実行されます。

ヒント
ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリックした後にタスク画面を表示］を選択して、［適用］をクリックします。

14. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したりキャンセルしたりできます。

設定したにも関わらず、鍵管理サーバが使用できない場合は、サーバへの接続設定の内容やネットワークに問題があるおそれがあります。サーバの管理者およびネットワークの管理者にお問い合わせください。

設定完了後、鍵管理サーバが使用できることを確認したら、鍵管理サーバへの接続設定をバックアップしてください。

鍵管理サーバへの接続設定をバックアップするには、SVP の設定ファイルをバックアップします。バックアップ手順については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

関連概念

- (2) 暗号化鍵の定期バックアップ

関連参照

- 3.1.1 暗号化鍵の管理方法と［暗号化環境設定編集］画面の設定内容との関係
- 付録 A.2 暗号化環境設定編集ウィザード

3.2 暗号化鍵を作成する

暗号化鍵の変更が必要になった場合に備えて暗号化鍵を作成しておくことができます。

ストレージシステムごとに作成できる暗号化鍵の数は次のとおりです。

モデル	ストレージシステムごとに作成できる暗号化鍵の数
VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370	1,024
VSP G700 および VSP F700	4,096
VSP G900 および VSP F900	4,096
VSP E990	4,096

通常、暗号化鍵はストレージシステム内に作成されます。ただし、鍵管理サーバを使用していて、かつ、暗号化環境の設定時に、［暗号化環境設定編集］画面で［鍵管理サーバで暗号化鍵を生成］のチェックボックスにチェックマークを付けている場合は、暗号化鍵は鍵管理サーバ上で生成され、ストレージシステム内で使用されます。

鍵管理サーバを使用している場合は、暗号化鍵は自動的にバックアップされます。鍵管理サーバを使用していない場合は、暗号化鍵のバックアップを行ってください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［鍵生成］画面を表示します。
   - ［暗号化鍵］タブで［鍵生成］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［鍵生成］を選択します。
4. ［鍵生成］画面で暗号化鍵の数を指定します。
   未使用鍵（属性が「空き」の暗号化鍵）が設定されます。鍵 ID は自動で割り当てられます。
5. ［完了］をクリックします。

［設定確認］画面が表示されます。

6. 設定内容を確認し、［タスク名］にタスク名を入力します。
7. ［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとしてキューイングされ、順に実行されます。

ヒント
ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

8. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連参照

- 付録 A.3 鍵生成ウィザード

3.3 暗号化鍵のバックアップ

暗号化鍵を作成後は、すぐに二次バックアップを行ってください。

鍵管理サーバを使用している場合は、暗号化鍵は自動的にバックアップされます。鍵管理サーバを使用していない場合は、［暗号化鍵］画面からファイルへ暗号化鍵のバックアップを実施できます。

また、二次バックアップした暗号化鍵は、ユーザが責任を持って保管してください。

注意
一次バックアップでバックアップした暗号化鍵が使用できず、かつ、二次バックアップでバックアップした暗号化鍵も使用できない場合は、データの復号化ができません。

二次バックアップには、管理クライアント内にファイルとしてバックアップする方法と、鍵管理サーバに接続してバックアップする方法があります。

暗号化鍵を管理クライアント内にファイルとしてバックアップするときはパスワードを設定します。このパスワードは暗号化鍵をリストアするときに必要です。このパスワードに使用する最小文字数を［パスワードポリシー編集（暗号化鍵バックアップ）］画面で設定できます。鍵管理サーバに接続してバックアップしている場合、鍵管理サーバがバックアップできる鍵の数には上限があります。このため、鍵管理サーバ上の暗号化鍵は定期的に削除してください。

暗号化鍵のバックアップは、作成済みの暗号化鍵（DEK）および認証用鍵に対して一括して実施されます。

作成済みの暗号化鍵および認証用鍵がない状態では、暗号化鍵のバックアップはできません。また、暗号化鍵をバックアップするときは、タスクに他の処理が登録されていないことを確認してください。タスクに他の処理が登録されていると暗号化鍵のバックアップができません。

関連タスク

- 3.3.1 管理クライアント内に暗号化鍵をファイルとしてバックアップするときに設定するパスワードの最小文字数を設定する
- 3.3.2 管理クライアント内にファイルとして暗号化鍵をバックアップする
- 3.3.3 鍵管理サーバに接続して暗号化鍵をバックアップする

3.3.1 管理クライアント内に暗号化鍵をファイルとしてバックアップするときに設定するパスワードの最小文字数を設定する

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、[暗号化鍵] 画面を表示します。

   Hitachi Command Suite を使用する場合：

   - [リソース] タブで [ストレージシステム] ツリーを展開します。ローカルストレージシステムの配下の [暗号化鍵] を選択します。

   Storage Navigator を使用する場合：

   - [管理] ツリーから [暗号化鍵] を選択します。
2. [設定] メニューから [セキュリティ管理] - [暗号化鍵] - [パスワードポリシー編集（暗号化鍵バックアップ）] を選択し、[パスワードポリシー編集（暗号化鍵バックアップ）] 画面を表示します。
3. 各項目について、使用する最小文字数を設定します。
4. [完了] をクリックします。

   [設定確認] 画面が表示されます。
5. 設定内容を確認し、[タスク名] にタスク名を入力します。
6. [設定確認] 画面の [適用] をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

   ヒント
   ウィザードを閉じたあとに [タスク] 画面を自動的に表示するには、ウィザードで [「適用」をクリック した後にタスク画面を表示] を選択して、[適用] をクリックします。
7. [タスク] 画面で、操作結果を確認します。実行前であれば、[タスク] 画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- (1) 暗号化鍵の一次バックアップと二次バックアップ
- 3.3 暗号化鍵のバックアップ

関連参照

- 付録 A.4 パスワードポリシー編集（暗号化鍵バックアップ）ウィザード

3.3.2 管理クライアント内にファイルとして暗号化鍵をバックアップする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、[暗号化鍵] 画面を表示します。

   Hitachi Command Suite を使用する場合：

- ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

Storage Navigator を使用する場合：

- ［管理］ツリーから［暗号化鍵］を選択します。

2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［ファイルへ鍵バックアップ］画面を表示します。
   - ［暗号化鍵］タブで［鍵バックアップ］ - ［ファイルへ］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［ファイルへ鍵バックアップ］を選択します。
4. ［パスワード］にパスワードを入力します。
   このパスワードは暗号化鍵をリストアするときに必要です。
5. ［パスワード再入力］に、確認用に再度パスワードを入力します。
6. ［完了］をクリックします。
   ［設定確認］画面が表示されます。
7. 設定内容を確認し、［タスク名］にタスク名を入力します。
8. ［設定確認］画面の［適用］をクリックします。
   準備の完了を知らせるメッセージが表示されます
9. ［OK］をクリックします。
   暗号化鍵ファイルを保存する画面が表示されます。
10. 暗号化鍵ファイルの保存場所とファイル名を指定します。
    暗号化鍵ファイルの拡張子は[.ekf]としてください。
11. ［保存］をクリックして画面を閉じます。
    キャンセルはできません。また、［設定確認］画面の［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、タスク一覧画面が表示されます。

保存した暗号化鍵ファイルとパスワードは、ユーザが責任を持って保管してください。

関連概念

- (1)　暗号化鍵の一次バックアップと二次バックアップ
- 3.3 暗号化鍵のバックアップ

関連参照

- 付録 A.5 鍵バックアップウィザード（管理クライアント内にファイルとしてバックアップする場合）

3.3.3 鍵管理サーバに接続して暗号化鍵をバックアップする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

Storage Navigator を使用する場合：

- ［管理］ツリーから［暗号化鍵］を選択します。

2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［サーバへ鍵バックアップ］画面を表示します。

［暗号化鍵］画面を使用する場合：

a. 次のどちらかの方法で、［サーバへ鍵バックアップ］画面を表示します。
［暗号化鍵］タブで［鍵バックアップ］ - ［サーバへ］をクリックします。
［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバへ鍵バックアップ］を選択します。

［サーバ内鍵バックアップ参照］画面を使用する場合：

a. 次のどちらかの方法で、［サーバ内鍵バックアップ参照］画面を表示します。
［暗号化鍵］タブで［サーバ内鍵バックアップ参照］をクリックします。
［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバ内鍵バックアップ参照］を選択します。
b. ［サーバへ鍵バックアップ］をクリックします。

4. ［説明］に暗号化鍵をバックアップする目的を入力します。入力は任意です。
5. ［完了］をクリックします。
［設定確認］画面が表示されます。
6. 設定内容を確認し、［タスク名］にタスク名を入力します。
7. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

ヒント
ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

---

8. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- (1) 暗号化鍵の一次バックアップと二次バックアップ
- 1.3.4 鍵管理サーバを使用した暗号化鍵の操作
- 3.3 暗号化鍵のバックアップ

関連参照

- 付録 A.6 鍵バックアップウィザード（鍵管理サーバに接続してバックアップする場合）

3.4 暗号化を有効にする

暗号化の設定は、パリティグループに属するボリュームがすべて閉塞状態であるか、パリティグループに属するボリュームが 0 個の場合だけできます。パリティグループ内に 1 つでも閉塞状態でないボリュームがある場合は、暗号化の設定ができません。

暗号化を設定するパリティグループの容量拡張設定が有効になっている場合は、暗号化を有効にできません。暗号化を設定するパリティグループの容量拡張設定が有効になっている場合は、『システム構築ガイド』を参照し、容量拡張設定を無効にした上で、暗号化を設定してください。

暗号化を設定するパリティグループにプールボリュームが定義されている場合は、当該プールボリュームが登録されているプールに作成されている仮想ボリュームの容量削減機能が有効になっていると、暗号化を有効にできません。

パリティグループの暗号化設定を有効化したい場合、パリティグループに属するボリュームがプールボリューム以外だけのときは「3.4.1 データの暗号化を有効にする」を、パリティグループに属するボリュームにプールボリュームが含まれるときは「3.4.2 データの暗号化を有効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）」を参照してください。

関連概念

- 1.4.1 データの暗号化

関連タスク

- 3.4.1 データの暗号化を有効にする
- 3.4.2 データの暗号化を有効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）

3.4.1 データの暗号化を有効にする

パリティグループに対して、データの暗号化を有効にする手順を次に示します。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール（フォーマットを同時にする場合は、セキュリティ管理者（参照・編集）ロールとストレージ管理者（プロビジョニング）ロール）
- パリティグループの容量拡張設定が無効であること

操作手順

1. 次のどちらかの方法で、［パリティグループ］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［パリティグループ］を右クリックし、［System GUI］選択します。

   Storage Navigator を使用する場合：
   - ［ストレージシステム］ツリーから［パリティグループ］を選択します。
2. 画面右側の［パリティグループ］タブを選択するか、ツリーから［Internal］を選択した上で画面右側の［パリティグループ］タブを選択します。
3. 画面右側の［パリティグループ］タブのテーブルの［LDEV 状態］欄で LDEV の状態を確認します。
   - ［Blocked］と表示されている場合、LDEV は閉塞状態です。
   - ［Blocked］と表示されていない場合、LDEV は閉塞状態ではありません。LDEV が 0 個であることを確認するか、LDEV が存在しない場合は、閉塞状態にしてください。
4. パリティグループのチェックボックスを選択します。
   パリティグループを選択しない場合は、すべてのパリティグループが暗号化を設定する対象となります。
5. 次のどちらかの方法で、［暗号化編集］画面を表示します。
   - ［パリティグループ］タブで［暗号化編集］をクリックします。
   - ［アクション］メニューから［パリティグループ管理］ - ［暗号化編集］を選択します。

6. 画面左側の［利用可能なパリティグループ］リストから暗号化を設定したいパリティグループのチェックボックスを選択し、［暗号化］で［有効］、［フォーマットタイプ］でフォーマット種別を選択します。

> **注意**
> パリティグループの容量拡張設定が有効になっている場合は、［暗号化］で［有効］を選択しないでください。［暗号化］で［有効］を選択した場合、タスクを実行したときにエラーとなります。パリティグループにプールボリュームが含まれている場合、ノーマルフォーマットを選択してください。クイックフォーマットを選択した場合、タスクを実行したときにエラーとなります。

7. ［追加］をクリックし ます。

   ［利用可能なパリティグループ］リストから選択されたパリティグループが、画面右側の［選択したパリティグループ］リストに表示されます。

   ［追加］をクリックすると［フォーマットタイプ］は不活性となり選択できなくなります。ほかのフォーマット種別を選択したい場合は、［選択したパリティグループ］リストに表示されたパリティグループをすべて削除してから再度フォーマット種別を選択してください。

   選択されたパリティグループにボリュームが 1 つもない場合はフォーマットが不要です。このため、［フォーマットタイプ］の指定に関わらず、［選択したパリティグループ］リストのフォーマットタイプは［ - ］となります。
8. ［完了］をクリックします。

   ［設定確認］画面が表示されます。
9. 設定内容を確認し、［タスク名］にタスク名を入力します。
10. ［設定確認］画面の［適用］をクリックします。

    変更内容をストレージシステムに適用するかどうかを尋ねるメッセージが表示されます。
11. ［OK］をクリックしてメッセージを閉じます。

    変更内容がストレージシステムに適用されます。なお、［設定確認］画面の［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、タスク一覧画面が表示されます。

関連概念

- 3.4 暗号化を有効にする

関連タスク

- 3.4.2 データの暗号化を有効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）

関連参照

- 付録 A.14 暗号化編集ウィザード

3.4.2 データの暗号化を有効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）

パリティグループに対して、データの暗号化を有効にするためには、容量削減機能を無効にする必要があります。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール（フォーマットを同時にする場合は、セキュリティ管理者（参照・編集）ロールとストレージ管理者（プロビジョニング）ロール）
- パリティグループの容量拡張設定が無効であること。

操作手順

1. ［ストレージシステム］ツリーから［プール］を選択します。
2. ［プール］タブから、暗号化を有効にするパリティグループが属しているプールを選択し、［仮想ボリューム］タブを表示します。
3. テーブルの［容量削減］欄で LDEV の容量削減機能の設定を確認します。
   - ［容量削除状態］が［Disabled］以外のすべての仮想ボリュームに対して、次の操作を実施します。
     1. 仮想ボリュームを閉塞します。
     2. 仮想ボリュームをフォーマットします。
     3. 仮想ボリュームの［容量削減］の設定を［無効］にします。
     4. 仮想ボリュームの［容量削減状態］が［Disabled］であることを確認します。
   - すべての LDEV の［容量削減状態］が［Disabled］と表示されている場合、次の手順に進みます。
4. プールのサマリで［重複排除］欄で重複排除機能の設定を確認します。
   - ［重複排除］欄が［利用可能］と表示されている場合、［プール編集］により［重複排除用システムデータボリュームを割り当てる］の設定を［いいえ］にします。
   - ［重複排除］欄が［利用可能］以外に表示されている場合、次の手順へ進みます。
5. ［仮想ボリューム］タブのテーブルの［状態］欄で LDEV の状態を確認します。
   - ［Blocked］と表示されている場合、LDEV は閉塞状態です。
   - ［Blocked］と表示されていない場合、LDEV は閉塞状態ではありません。LDEV が 0 個であることを確認するか、LDEV が存在する場合は、閉塞状態にしてください。
6. パリティグループに対してデータの暗号化を有効にします。
   「3.4.1 データの暗号化を有効にする」に示す手順を実施します。
7. 仮想ボリュームをフォーマットします。
   手順 1 で確認したプールに属している仮想ボリュームをフォーマットします。

   注意
   必ず、［LDEV フォーマット］を実行してください。［LDEV フォーマット］ではなく［LDEV 回復］を実行すると問題が発生するおそれがあります。

8. プールの重複排除機能を使用する場合は、［プール編集］により［重複排除用システムデータボリュームを割り当てる］の設定を［はい］にします。
9. 仮想ボリュームの容量削減機能を使用する場合は、［容量削減］の設定を［圧縮］または［重複排除および圧縮］にします。

関連概念

- 3.4 暗号化を有効にする

関連タスク

- 3.4.1 データの暗号化を有効にする

3.5 暗号化を無効にする

暗号化の解除は、パリティグループに属するボリュームがすべて閉塞状態であるか、パリティグループに属するボリュームが 0 個の場合だけできます。パリティグループ内に 1 つでも閉塞状態でないボリュームがある場合は、暗号化の解除ができません。

暗号化を設定するパリティグループにプールボリュームが定義されている場合は、当該プールボリュームが登録されているプールに作成されている仮想ボリュームの容量削減機能が有効になっていると、暗号化を無効にできません。

パリティグループの暗号化設定を無効化したい場合、パリティグループに属するボリュームがプールボリューム以外だけのときは「3.5.1 データの暗号化を無効にする」を、パリティグループに属するボリュームにプールボリュームが含まれるときは「3.5.2 データの暗号化を無効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）」を参照してください。

関連概念

- 1.4.2 暗号化の解除

関連タスク

- 3.5.1 データの暗号化を無効にする
- 3.5.2 データの暗号化を無効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）

3.5.1 データの暗号化を無効にする

パリティグループに対して、データの暗号化を無効にする手順を次に示します。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール（フォーマットを同時にする場合は、セキュリティ管理者（参照・編集）ロールとストレージ管理者（プロビジョニング）ロール）

操作手順

1. 次のどちらかの方法で、［パリティグループ］画面を表示します。

   Hitachi Command Suite を使用する場合：

   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［パリティグループ］を右クリックし、［Systen GUI］選択します。

   Storage Navigator を使用する場合：

   - ［ストレージシステム］ツリーから［パリティグループ］を選択します。
2. 画面右側の［パリティグループ］タブを選択するか、ツリーから［Internal］を選択した上で画面右側の［パリティグループ］タブを選択します。
3. 画面右側の［パリティグループ］タブのテーブルの［LDEV 状態］欄で LDEV の状態を確認します。

   - ［Blocked］と表示されている場合、LDEV は閉塞状態です。
   - ［Blocked］と表示されていない場合、LDEV は閉塞状態ではありません。LDEV が 0 個であることを確認するか、LDEV が存在しない場合は、閉塞状態にしてください。
4. パリティグループのチェックボックスを選択します。

5. 次のどちらかの方法で、［暗号化編集］画面を表示します。
   - ［パリティグループ］タブで［暗号化編集］をクリックします。
   - ［アクション］メニューから［パリティグループ管理］ - ［暗号化編集］を選択します。
6. 画面左側の［利用可能なパリティグループ］リストから暗号化を解除したいパリティグループのチェックボックスを選択し、［暗号化］で［無効］、［フォーマットタイプ］でフォーマット種別を選択します。

   注意
   パリティグループにプールボリュームが含まれている場合、ノーマルフォーマットを選択してください。クイックフォーマットを選択した場合、タスクを実行したときにエラーとなります。

7. ［追加］をクリックします。
   ［利用可能なパリティグループ］リストから選択されたパリティグループが、画面右側の［選択したパリティグループ］リストに表示されます。
   ［追加］をクリックすると［フォーマットタイプ］は不活性となり選択できなくなります。ほかのフォーマット種別を選択したい場合は、［選択したパリティグループ］リストに表示されたパリティグループをすべて削除してから再度フォーマット種別を選択してください。
   選択されたパリティグループにボリュームが 1 つもない場合はフォーマットが不要です。このため、［フォーマットタイプ］の指定に関わらず、［選択したパリティグループ］リストのフォーマットタイプは［ - ］となります。
8. ［完了］をクリックします。
   ［設定確認］画面が表示されます。
9. 設定内容を確認し、［タスク名］にタスク名を入力します。
10. ［設定確認］画面の［適用］をクリックします。
    変更内容をストレージシステムに適用するかどうかを尋ねるメッセージが表示されます。
11. ［OK］をクリックしてメッセージを閉じます。
    変更内容がストレージシステムに適用されます。なお、［設定確認］画面の［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、タスク一覧画面が表示されます。

関連概念

- 3.5 暗号化を無効にする

関連タスク

- 3.5.2 データの暗号化を無効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）

関連参照

- 付録 A.14 暗号化編集ウィザード

3.5.2 データの暗号化を無効にする（パリティグループに属するボリュームにプールボリュームが含まれる場合）

パリティグループに対して、データの暗号化を無効にするためには、容量削減機能を無効にする必要があります。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール（フォーマットを同時にする場合は、セキュリティ管理者（参照・編集）ロールとストレージ管理者（プロビジョニング）ロール）

操作手順

1. ［ストレージシステム］ツリーから［プール］を選択します。
2. ［プール］タブから、暗号化を有効にするパリティグループが属しているプールを選択し、［仮想ボリューム］タブを表示します。
3. テーブルの［容量削減］欄で LDEV の容量削減機能の設定を確認します。
   - ［容量削除状態］が［Disabled］以外のすべての仮想ボリュームに対して、次の操作を実施します。
     1. 仮想ボリュームを閉塞します。
     2. 仮想ボリュームをフォーマットします。
     3. 仮想ボリュームの［容量削減］の設定を［無効］にします。
     4. 仮想ボリュームの［容量削減状態］が［Disabled］であることを確認します。
   - すべての LDEV の［容量削減状態］が［Disabled］と表示されている場合、次の手順に進みます。
4. プールのサマリで［重複排除］欄で重複排除機能の設定を確認します。
   - ［重複排除］欄が［利用可能］と表示されている場合、［プール編集］により［重複排除用システムデータボリュームを割り当てる］の設定を［いいえ］にします。
   - ［重複排除］欄が［利用可能］以外と表示されている場合、次の手順へ進みます。
5. ［仮想ボリューム］タブのテーブルの［状態］欄で LDEV の状態を確認します。
   - ［Blocked］と表示されている場合、LDEV は閉塞状態です。
   - ［Blocked］と表示されていない場合、LDEV は閉塞状態ではありません。LDEV が 0 個であることを確認するか、LDEV が存在する場合は、閉塞状態にしてください。
6. パリティグループに対してデータの暗号化を無効にします。
   「3.5.1 データの暗号化を無効にする」に示す手順を実施します。
7. 仮想ボリュームをフォーマットします。
   手順 1 で確認したプールに属している仮想ボリュームをフォーマットします。
8. プールの重複排除機能を使用する場合は、［プール編集］により［重複排除用システムデータボリュームを割り当てる］の設定を［はい］にします。
9. 仮想ボリュームの容量削減機能を使用する場合は、［容量削減］の設定を［圧縮］または［重複排除および圧縮］にします。

関連概念

- 3.5 暗号化を無効にする

関連タスク

- 3.5.1 データの暗号化を無効にする

3.6 暗号化鍵のリストア

一次バックアップでバックアップした暗号化鍵を含め、ストレージシステム内の暗号化鍵が使用できなくなった場合は、二次バックアップでバックアップした暗号化鍵をリストアします。

暗号化鍵のリストアは、バックアップ済みの暗号化鍵（未使用鍵、DEK、および CEK を含む）のうち鍵情報が紛失または削除された暗号化鍵に対して一括して実施されます。バックアップ済みの暗号化鍵の最大数は次のとおりです。

モデル	バックアップ済みの暗号化鍵の最大数（未使用鍵、DEK、および CEK を含む）
VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370	1,028
VSP G700 および VSP F700	4,104
VSP G900 および VSP F900	4,112
VSP E990	4,112

注意
最新の暗号化鍵をリストアしてください。最新の暗号化鍵を含まない二次バックアップはリストアできません。

注意
暗号化鍵をリストアするには、暗号化鍵が設定されているパリティグループに属するボリュームがすべて閉塞状態である必要があります。また、暗号化鍵のリストア後は、暗号化鍵が設定されているパリティグループに属するボリュームをすべて回復する必要があります。

二次バックアップからの暗号化鍵のリストアには、管理クライアント内にバックアップしたファイルからリストアする方法と、鍵管理サーバに接続してリストアする方法があります。

関連タスク

- 3.6.1 管理クライアント内にバックアップしたファイルから暗号化鍵をリストアする
- 3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする

3.6.1 管理クライアント内にバックアップしたファイルから暗号化鍵をリストアする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［ファイルから鍵回復］画面を表示します。
   - ［暗号化鍵］タブで［鍵回復］ - ［ファイルから］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［ファイルから鍵回復］を選択します。
4. ［参照］をクリックします。
   準備の完了を知らせるメッセージが表示されます
5. ［OK］をクリックします。

暗号化鍵ファイルを選択する画面が表示されます。

6. 暗号化鍵ファイルを選択します。
7. ［開く］をクリックして画面を閉じます。
   選択した暗号化鍵ファイルの名称が［ファイルから鍵回復］画面の［ファイル名］に表示されます。
8. ［パスワード］にパスワードを入力します。
   このパスワードは、選択した暗号化鍵をバックアップしたときに入力したパスワードです。
9. ［完了］をクリックします。
   ［設定確認］画面が表示されます。
10. 設定内容を確認し、［タスク名］にタスク名を入力します。
11. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

ヒント
ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

12. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- 1.3.3 暗号化鍵のリストア機能
- 3.6 暗号化鍵のリストア

関連参照

- 付録 A.7 鍵回復ウィザード（管理クライアント内にバックアップしたファイルからリストアする場合）

3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの手順でリストアする暗号化鍵を選択します。
   ［サーバから鍵回復］画面を使用する場合：
   a. 次のどちらかの方法で、［サーバから鍵回復］画面を表示します。
      ［暗号化鍵］タブで［鍵回復］ - ［サーバから］をクリックします。
      ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバから鍵回復］を選択します。

b. リストアする暗号化鍵のラジオボタンを選択します。
c. ［完了］をクリックします。
［設定確認］画面が表示されます。

［サーバ内鍵バックアップ参照］画面を使用する場合：

a. 次のどちらかの方法で、［サーバ内鍵バックアップ参照］画面を表示します。
［暗号化鍵］タブで［サーバ内鍵バックアップ参照］をクリックします。
［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバ内鍵バックアップ参照］を選択します。
b. リストアする暗号化鍵のチェックボックスを選択します。
c. ［サーバから鍵回復］をクリックします。
［設定確認］画面が表示されます。

4. 設定内容を確認し、［タスク名］にタスク名を入力します。
5. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

ヒント
ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

6. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- 1.3.3 暗号化鍵のリストア機能
- 1.3.4 鍵管理サーバを使用した暗号化鍵の操作
- 3.6 暗号化鍵のリストア

関連参照

- 付録 A.9 鍵回復ウィザード（鍵管理サーバに接続してリストアする場合）

3.7 暗号化鍵の強制リストア

一次バックアップでバックアップした暗号化鍵を含め、ストレージシステム内の暗号化鍵が使用できなくなった場合は、二次バックアップでバックアップした暗号化鍵をリストアします。

暗号化鍵のリストアは、バックアップ済みの暗号化鍵（未使用鍵、DEK、および CEK を含む）のうち鍵情報が紛失または削除された暗号化鍵に対して一括して実施されます。バックアップ済みの暗号化鍵の最大数は次のとおりです。

モデル	バックアップ済みの暗号化鍵の最大数（未使用鍵、DEK、および CEK を含む）
VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370	1,028
VSP G700 および VSP F700	4,104
VSP G900 および VSP F900	4,112
VSP E990	4,112

注意
最新でない暗号化鍵をリストアした場合は、ドライブ、暗号化に対応した NVMe ドライブ用のディスクボード（EDKBN）、暗号化に対応したディスクボード（EDKB）や暗号化に対応したコントローラ（ECTL）が閉塞して、データを読み出せなくなる場合があります。

注意
暗号化鍵をリストアするには、暗号化鍵が設定されているパリティグループに属するボリュームがすべて閉塞状態である必要があります。また、暗号化鍵のリストア後は、暗号化鍵が設定されているパリティグループに属するボリュームをすべて回復する必要があります。

二次バックアップからの暗号化鍵のリストアには、管理クライアント内にバックアップしたファイルからリストアする方法と、鍵管理サーバに接続してリストアする方法があります。

関連タスク

- 3.7.1 管理クライアント内にバックアップしたファイルから暗号化鍵を強制リストアする
- 3.7.2 鍵管理サーバに接続して暗号化鍵を強制リストアする

3.7.1 管理クライアント内にバックアップしたファイルから暗号化鍵を強制リストアする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール、および保守（ベンダ専用）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［ファイルから強制鍵回復］画面を表示します。
   - ［暗号化鍵］タブで［鍵回復］ - ［ファイルから（強制）］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［ファイルから強制鍵回復］を選択します。
4. ［参照］をクリックします。
   準備の完了を知らせるメッセージが表示されます
5. ［OK］をクリックします。
   暗号化鍵ファイルを選択する画面が表示されます。
6. 暗号化鍵ファイルを選択します。
7. ［開く］をクリックして画面を閉じます。
   選択した暗号化鍵ファイルの名称が［ファイルから強制鍵回復］画面の［ファイル名］に表示されます。
8. ［パスワード］にパスワードを入力します。
   このパスワードは、選択した暗号化鍵をバックアップしたときに入力したパスワードです。
9. ［完了］をクリックします。

［設定確認］画面が表示されます。

10. 設定内容を確認し、［タスク名］にタスク名を入力します。
11. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

ヒント

ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

12. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- 1.3.3 暗号化鍵のリストア機能
- 3.7 暗号化鍵の強制リストア

関連参照

- 付録 A.8 強制鍵回復ウィザード（管理クライアント内にバックアップしたファイルから強制リストアする場合）

3.7.2 鍵管理サーバに接続して暗号化鍵を強制リストアする

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール、および保守（ベンダ専用）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。

   Hitachi Command Suite を使用する場合：

   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：

   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. リストアする暗号化鍵を選択します。
   a. 次のどちらかの方法で、［サーバから強制鍵回復］画面を表示します。
      ［暗号化鍵］タブで［鍵回復］ - ［サーバから（強制）］をクリックします。
      ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバから強制鍵回復］を選択します。
   b. リストアする暗号化鍵のラジオボタンを選択します。
   c. ［完了］をクリックします。
      ［設定確認］画面が表示されます。
4. 設定内容を確認し、［タスク名］にタスク名を入力します。
5. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

ヒント

ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

6. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- 1.3.3 暗号化鍵のリストア機能
- 1.3.4 鍵管理サーバを使用した暗号化鍵の操作
- 3.7 暗号化鍵の強制リストア

関連参照

- 付録 A.10 強制鍵回復ウィザード（鍵管理サーバに接続して強制リストアする場合）

3.8 暗号化鍵の削除

暗号化鍵の削除について説明します。

関連タスク

- 3.8.1 ストレージシステム内の暗号化鍵を削除する
- 3.8.2 鍵管理サーバにバックアップした暗号化鍵を削除する

3.8.1 ストレージシステム内の暗号化鍵を削除する

未使用鍵（属性が「空き」の暗号化鍵）を削除します。ほかの属性の暗号化鍵は削除できません。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。

   Hitachi Command Suite を使用する場合：

   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：

   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 暗号化鍵のチェックボックスを選択します。
4. 次のどちらかの方法で、［鍵削除］画面を表示します。

   - ［暗号化鍵］タブで［他のタスク］ - ［鍵削除］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［鍵削除］を選択します。

   引き続き、暗号化鍵を作成したい場合は、［次へ］をクリックします。
5. ［完了］をクリックします。

   ［設定確認］画面が表示されます。
6. 設定内容を確認し、［タスク名］にタスク名を入力します。

7. ［設定確認］画面の［適用］をクリックします。
   変更内容をストレージシステムに適用するかどうかを尋ねるメッセージが表示されます。
8. ［OK］をクリックします。
   タスクが登録され、［設定確認］画面の［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、タスク一覧画面が表示されます。

関連概念

- 3.8 暗号化鍵の削除

関連参照

- 付録 A.11 鍵削除ウィザード（ストレージシステム内の暗号化鍵を削除する場合）

3.8.2 鍵管理サーバにバックアップした暗号化鍵を削除する

注意
暗号化鍵のバックアップは重要です。このため、鍵管理サーバにバックアップした暗号化鍵を削除するときには、他にバックアップされた暗号化鍵があることを確認するなど、十分な確認作業を行ってから実行してください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［サーバ内鍵バックアップ参照］画面を表示します。
   - ［暗号化鍵］タブで［サーバ内鍵バックアップ参照］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバ内鍵バックアップ参照］を選択します。
4. 削除する暗号化鍵のチェックボックスを選択します。
5. ［サーバ内鍵バックアップ削除］をクリックし、［サーバ内鍵バックアップ削除］画面を表示します。
6. 設定内容を確認し、［タスク名］にタスク名を入力します。
7. ［サーバ内鍵バックアップ削除］画面の［適用］をクリックします。
   変更内容をストレージシステムに適用するかどうかを尋ねるメッセージが表示されます。
8. ［OK］をクリックします。
   タスクが登録され、［サーバ内鍵バックアップ削除］画面の［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、タスク一覧画面が表示されます。

関連概念

- 3.8 暗号化鍵の削除

関連参照

- 付録 A.12 ［サーバ内鍵バックアップ削除］画面

3.9 鍵管理サーバ上にある暗号化鍵の状態を確認する

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［サーバ内鍵バックアップ参照］画面を表示して確認します。
   - ［暗号化鍵］タブで［サーバ内鍵バックアップ参照］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバ内鍵バックアップ参照］を選択します。

関連概念

- 1.3.4 鍵管理サーバを使用した暗号化鍵の操作

関連参照

- 付録 A.13 ［サーバ内鍵バックアップ参照］画面

3.10 暗号化鍵の更新

暗号化鍵の更新について説明します。

関連タスク

- 3.10.1 認証用鍵を更新する
- 3.10.2 鍵暗号化鍵を更新する

3.10.1 認証用鍵を更新する

認証用鍵を変更する場合、［認証用鍵更新］画面で認証用鍵を更新します。認証用鍵を更新したらすぐに暗号化鍵のバックアップを行ってください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［認証用鍵更新］画面を表示します。
   - ［暗号化鍵］タブで［他のタスク］ - ［認証用鍵更新］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［認証用鍵更新］を選択します。
4. 設定内容を確認し、［タスク名］にタスク名を入力します。
5. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

   ヒント
   ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

6. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- 3.10 暗号化鍵の更新

関連参照

- 付録 A.15 ［認証用鍵更新］画面

3.10.2 鍵暗号化鍵を更新する

鍵暗号化鍵を鍵管理サーバで作成している場合、［鍵暗号化鍵更新］画面で鍵暗号化鍵を更新できます。鍵暗号化鍵を更新したらすぐに暗号化鍵のバックアップを行ってください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。
   Hitachi Command Suite を使用する場合：
   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：
   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［鍵暗号化鍵更新］画面を表示します。

- ［暗号化鍵］タブで［他のタスク］ - ［鍵暗号化鍵更新］をクリックします。
- ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［鍵暗号化鍵更新］を選択します。

4. ［完了］をクリックします。

メモ
鍵暗号化鍵を更新する場合、［鍵暗号化鍵更新］画面での［鍵管理サーバに鍵暗号化鍵を新規作成する］チェックボックスの選択は不要です。
ただし、鍵管理サーバを別サーバに移行するための暗号化環境設定の失敗により、鍵暗号化鍵を新規作成する場合、手順 4 の実施前に、［鍵管理サーバに鍵暗号化鍵を新規作成する］チェックボックスの選択が必要です。

［設定確認］画面が表示されます。

5. 設定内容を確認し、［タスク名］にタスク名を入力します。
6. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

ヒント
ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

7. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連概念

- 3.10 暗号化鍵の更新

関連参照

- 付録 A.16.1 ［鍵暗号化鍵更新］画面

3.11 鍵管理サーバを別サーバへ移行する

鍵管理サーバを別サーバへ移行する場合は、「3.1.2 暗号化環境を設定する」を参照して、プライマリサーバとセカンダリサーバの設定項目を新しい鍵管理サーバに合わせて変更してください。鍵管理サーバの接続先を変更すると、鍵暗号化鍵を鍵管理サーバで作成している場合は、変更後の鍵管理サーバに対して鍵暗号化鍵の新規作成、および暗号化鍵のバックアップが同時に行われます。

暗号化環境設定編集のタスクが失敗した場合は、「4.1 Encryption License Key 操作時のエラーと対策」を参照して、対策を実施してください。

注意
上記の設定作業の途中で、ストレージシステムの電源を OFF にしないでください。
暗号化環境を次に示すいずれか、または両方の状態に設定している場合に、上記の設定作業の途中でストレージシステムの電源を OFF にすると、電源を ON にしたときに、鍵管理サーバにバックアップした鍵暗号化鍵および暗号化鍵を取得できないため、データを復号化できなくなります。

- ［暗号化環境設定編集］画面で、［鍵管理サーバで暗号化鍵生成］にある［鍵暗号化鍵を鍵管理サーバで保護する］のチェックボックスを選択して設定している。
- ［暗号化環境設定編集］画面、［鍵管理サーバで暗号化鍵生成］にある［PS OFF 時に装置内の暗号化鍵を削除する］のチェックボックスを選択して設定している。

3.12 鍵暗号化鍵を再取得する

ストレージ装置の起動で鍵管理サーバから鍵暗号化鍵を取得する場合に、何らかの要因で鍵暗号化鍵を取得できないときに鍵暗号化鍵を再取得します。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、[暗号化鍵] 画面を表示します。

   Hitachi Command Suite を使用する場合：

   - [リソース] タブで [ストレージシステム] ツリーを展開します。ローカルストレージシステムの配下の [暗号化鍵] を選択します。

   Storage Navigator を使用する場合：

   - [管理] ツリーから [暗号化鍵] を選択します。
2. 画面右側の [暗号化鍵] タブを選択します。
3. 次のどちらかの方法で、[鍵暗号化鍵再取得] 画面を表示します。
   - [暗号化鍵] タブで [他のタスク] - [鍵暗号化鍵再取得] をクリックします。
   - [設定] メニューから [セキュリティ管理] - [暗号化鍵] - [鍵暗号化鍵再取得] を選択します。
4. 設定内容を確認し、[タスク名] にタスク名を入力します。
5. [設定確認] 画面の [適用] をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

   ヒント
   ウィザードを閉じたあとに [タスク] 画面を自動的に表示するには、ウィザードで [「適用」をクリック した後にタスク画面を表示] を選択して、[適用] をクリックします。

6. [タスク] 画面で、操作結果を確認します。実行前であれば、[タスク] 画面でタスクを一時中断したり キャンセルしたりできます。

鍵暗号化鍵を再取得したあと、暗号化に対応した NVMe ドライブ用のディスクボード（EDKBN）、暗号化に対応したディスクボード（EDKB）および閉塞したドライブやボリュームを回復させる必要があります。暗号化に対応したディスクボードおよび閉塞したドライブやボリュームの回復については、お問い合わせください。

関連参照

- 付録 A.17 [鍵暗号化鍵再取得] 画面

3.13 暗号化環境設定を初期化する

設定済みの暗号化環境設定を初期化します。暗号化環境を初期化するためには、事前にすべてのパリティグループについて、データの暗号化を無効にしてください。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. 次のどちらかの方法で、［暗号化鍵］画面を表示します。

   Hitachi Command Suite を使用する場合：

   - ［リソース］タブで［ストレージシステム］ツリーを展開します。ローカルストレージシステムの配下の［暗号化鍵］を選択します。

   Storage Navigator を使用する場合：

   - ［管理］ツリーから［暗号化鍵］を選択します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［暗号化環境設定編集］画面を表示します。
   - ［暗号化鍵］タブで［暗号化環境設定編集］をクリックします。
   - ［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［暗号化環境設定編集］を選択します。
4. ［暗号化環境設定初期化］をクリックします。
5. ［完了］をクリックします。

   ［設定確認］画面が表示されます。
6. 設定内容を確認し、［タスク名］にタスク名を入力します。
7. ［設定確認］画面の［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとして キューイングされ、順に実行されます。

   ヒント
   ウィザードを閉じたあとに［タスク］画面を自動的に表示するには、ウィザードで［「適用」をクリック した後にタスク画面を表示］を選択して、［適用］をクリックします。

   ---

8. ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタスクを一時中断したり キャンセルしたりできます。

関連参照

- 付録 A.2 暗号化環境設定編集ウィザード

4

Encryption License Key のトラブルシューティング

ここでは、トラブルシューティングについて説明します。

4.1 Encryption License Key 操作時のエラーと対策

Encryption License Key の操作中に発生したエラーの対処方法については、マニュアル『Storage Navigator メッセージガイド』を参照してください。

Storage Navigator に関する一般的なエラーと対策については、マニュアル『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

エラー	対策
暗号化鍵の操作（バックアップ／リストア）ができない。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • セキュリティ管理者（参照・編集）ロールが割り当てられているか • 鍵管理サーバに接続してバックアップ／リストアしている場合、鍵管理サーバとの接続に問題はないか • 鍵管理サーバに接続してバックアップしている場合、鍵管理サーバがバックアップできる鍵の数を超えていないか • 鍵管理サーバに接続してバックアップ／リストアしている場合、鍵管理サーバ内の鍵の数が増えたことでタイムアウトが発生していないか • 最新の暗号化鍵をリストアしているか、二次バックアップ後に暗号化鍵が変更されていないか
暗号化鍵を作成／削除できない。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • セキュリティ管理者（参照・編集）ロールが割り当てられているか • 鍵管理サーバに接続して暗号化鍵を生成／削除している場合、鍵管理サーバとの接続に問題はないか
パリティグループに暗号化を設定できない。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • パリティグループに属するボリュームがすべて閉塞状態であるか
パリティグループに設定した暗号化を無効にできない。	パリティグループに属するボリュームがすべて閉塞状態であるかを確認してください。
テスト通信が成功しない。	鍵管理サーバとの接続設定が正しいかどうか、次の項目を確認してください。 • ホスト名 • ポート番号 • クライアント証明書ファイル • ルート証明書ファイル

エラー	対策
	通信に時間が掛かっている場合は、次の項目を調整すれば通信が成功することがあります。 ・ タイムアウト ・ リトライ間隔 ・ リトライ回数
暗号化編集ウィザードの操作が失敗したが、暗号化の状態（[無効] または [有効]）は暗号化編集ウィザードで設定した内容に切り替わっている。	暗号化の切り替えは成功していますが、その後のフォーマットが失敗しています。 メッセージの内容を確認してエラーを取り除き、フォーマットを再度実行してください。
ストレージシステムを起動するときに鍵管理サーバから鍵暗号化鍵、または暗号化鍵を取得できず、すべてのボリュームが閉塞した。SIM コード 661000 または 661001 が報告された。	次の対策を実施してください。 1. SVP が起動していることを確認してください。 2. 鍵管理サーバとの接続を回復させ、[暗号化環境設定編集] 画面にて [サーバ構成テスト] の [チェック] をクリックして、接続テストが正常終了することを確認してください。 3. 問い合わせ先に連絡し、ストレージシステムの再起動を依頼してください。 4. 再起動後、閉塞していたすべてのボリュームが回復していることを確認してください。
暗号化環境設定が（00002-058578）で失敗した。	[暗号化環境設定編集] 画面で初めて暗号化環境を設定したときに（00002-058578）で失敗した場合は、次の対策を実施してください。 1. しばらくしてから [ファイル] - [すべて更新] を選択して、構成情報を再読み込みしてください。 2. 暗号化環境設定を初期化してください。 3. 再度、暗号化環境を設定してください。 暗号化環境設定が完了してから再度 [暗号化環境設定編集] 画面で設定したときに、（00002-058578）で失敗した場合は、次の対策を実施してください。 1. しばらくしてから [ファイル] - [すべて更新] を選択して、構成情報を再読み込みしてください。 2. 再度、暗号化環境を設定してください。
テスト通信は成功したが、次のエラーが表示された。 10126-105022 接続されている鍵管理サーバに、必要な機能がサポートされていません。	鍵管理サーバの設定に必要な機能が、接続している鍵管理サーバではサポートされていません。「2.2 鍵管理サーバの要件」を確認して、鍵管理サーバのソフトウェアを最新にしてください。
未使用鍵（属性が「空き」の暗号化鍵）があるのに、次のエラーが表示されて暗号化編集ウィザードの操作が失敗する。 03005-108104 空きの鍵数が不足しています。	暗号化編集ウィザードの前に実行した暗号化環境設定編集ウィザードが、暗号化に対応したディスクボードの障害により失敗している可能性があります。[タスク] 画面を確認して、暗号化環境設定編集ウィザードが失敗していないかどうかを確認してください。 暗号化環境設定編集ウィザードが失敗している場合は、メッセージの内容を確認してエラーを取り除き、暗号化環境設定を初期化した後、暗号化環境設定編集ウィザードおよび暗号化編集ウィザードを再度実行してください。
未使用鍵（属性が「空き」の暗号化鍵）を削除した後、SIM コード 660100 または 660200 が報告された。	未使用鍵（属性が「空き」の暗号化鍵）の数が保守作業に必要な閾値を下回っている可能性があります。

エラー	対策
	作成可能な最大数の暗号化鍵を作成しておくことを推奨します。
暗号化環境設定の初期化が失敗した。	次の対策を実施してください。 1. 次に示すハードウェアが閉塞状態であるか確認してください。 ・ 暗号化に対応したコントローラ（VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370 の場合） ・ 暗号化に対応したディスクボード（EDKB（VSP G700、VSP G900、VSP F700、および VSP F900 の場合） ・ 暗号化に対応した NVMe ドライブ用のディスクボード（EDKBN）（VSP E990 の場合） 2. 閉塞状態である場合： SVP あり構成の場合は Storage Navigator の［暗号化鍵］画面を開き、属性が KEK と CEK の両方、またはいずれか一方の暗号化鍵のみの状態になっているかを確認してください。 SVP なし構成の場合は REST API を使用して、暗号化鍵の個数を取得し、属性が KEK と CEK の両方、またはいずれか一方の暗号化鍵のみの状態になっているかを確認してください。 3. 属性が KEK と CEK の両方、またはいずれか一方の暗号化鍵のみの状態になっている場合： SVP あり構成の場合は Storage Navigator、SVP なし構成の場合は REST API を使用して、作成可能な最大数の未使用鍵（属性が「空き」の暗号化鍵）を作成してください。 REST API を使用して、暗号化鍵を生成した場合、KART40325 のエラーが出ることがありますが、暗号化鍵の個数を取得して必要な数が作成できていれば問題ありません。それ以外のエラーの場合は、エラーメッセージにしたがって対処したあと、再度暗号化鍵を作成してください。 4. 問い合わせ先に連絡し、次に示すハードウェアの回復を依頼してください。 ・ 暗号化に対応したコントローラ（VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370 の場合） ・ 暗号化に対応したディスクボード（EDKB（VSP G700、VSP G900、VSP F700、および VSP F900 の場合） ・ 暗号化に対応した NVMe ドライブ用のディスクボード（EDKBN）（VSP E990 の場合）
鍵管理サーバを別サーバへ移行するための暗号化環境設定が失敗した。	次の対策を実施してください。 1. ［暗号化環境設定編集］画面にて、プライマリサーバとセカンダリサーバの設定項目が変更されていることを確認してください。 2. ［鍵暗号化鍵更新］画面で、［鍵管理サーバに鍵暗号化鍵を新規作成する］チェックボックスを選択

エラー	対策
	して、新しい鍵管理サーバに鍵暗号化鍵を新規作成してください。 詳細手順は、「3.10.2 鍵暗号化鍵を更新する」を参照してください。 3. 「3.3.3 鍵管理サーバに接続して暗号化鍵をバックアップする」を参照して、新しい鍵管理サーバに暗号化鍵をバックアップしてください。

4.2 お問い合わせ先

- 保守契約をされているお客様は、以下の連絡先にお問い合わせください。
  日立サポートサービス：http://www.hitachi-support.com/
- 保守契約をされていないお客様は、担当営業窓口にお問い合わせください。

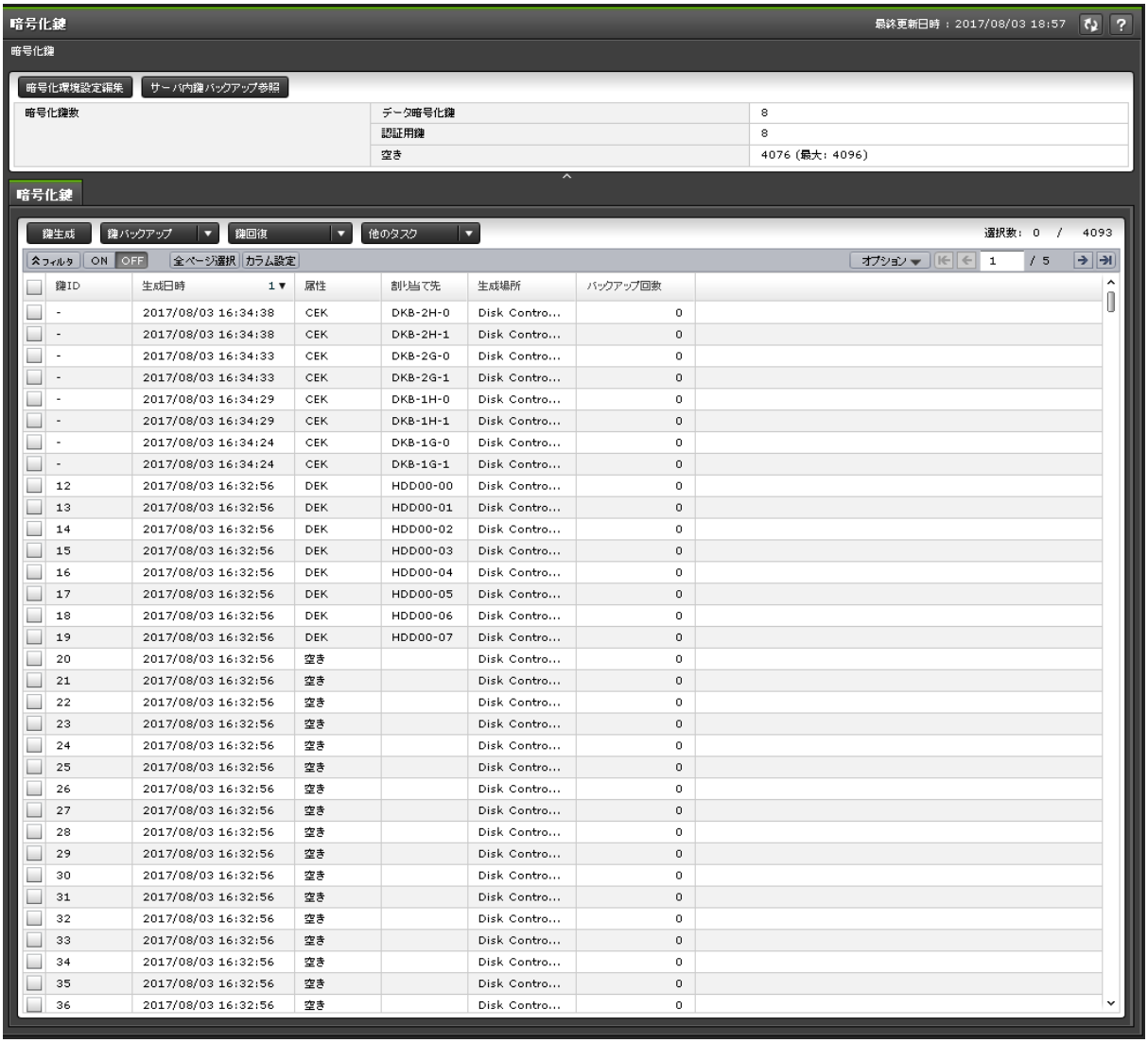
A

Encryption License Key GUI リファレンス

ここでは、Encryption License Key の操作に必要な Storage Navigator の画面とダイアログボックスについて説明します。

各画面に共通する操作（ボタンおよびタスク名入力など）については、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。

A.1 ［暗号化鍵］画面



［暗号化鍵］画面は、［管理］で［暗号化鍵］を選択して表示します。次のエリアから構成されています。

- サマリ
- ［暗号化鍵］タブ

サマリ

- ボタン

項目	説明
暗号化環境設定編集	［暗号化環境設定編集］画面が表示されます。
サーバ内鍵バックアップ参照	［サーバ内鍵バックアップ参照］画面が表示されます。

- テーブル

項目	説明
暗号化鍵数	暗号化鍵の数を表示します。鍵暗号化鍵の数は含まれません。 • データ暗号化鍵：データ暗号化鍵の数 • 認証用鍵：認証用鍵の数 • 空き：未使用鍵の数（鍵生成可能数）

［暗号化鍵］タブ

- 生成された暗号化鍵だけ表示します。
- 最終更新日付の降順に表示します。
- 初期設定されていない場合は、中央に「環境設定編集を実行してください」と表示します。
- 鍵暗号化鍵の取得に失敗した場合は、中央に「鍵暗号化鍵再取得を実行してください」と表示します。
- ボタン

項目	説明
鍵生成	［鍵生成］画面が表示されます。
鍵バックアップ	［ファイルへ］を選択すると［ファイルへ鍵バックアップ］画面が表示されます。 ［サーバへ］を選択すると［サーバへ鍵バックアップ］画面が表示されます。
鍵回復	［ファイルから］を選択すると［ファイルから鍵回復］画面が表示されます。 ［サーバから］を選択すると［サーバから鍵回復］画面が表示されます。
認証用鍵更新※	［認証用鍵更新］画面が表示されます。
鍵暗号化鍵更新※	［鍵暗号化鍵更新］画面が表示されます。
鍵削除※	［鍵削除］画面が表示されます。
鍵暗号化鍵再取得※	［鍵暗号化鍵再取得］画面が表示されます。
テーブル情報出力※	テーブル情報を出力させる画面が表示されます。

注※

［他のタスク］ボタンをクリックすると表示されます。

- テーブル

項目	説明
鍵 ID	暗号化鍵の番号を表示します。CEK および KEK の場合は、「 - 」を表示します。
生成日時	暗号化鍵を作成した年月日時を表示します。
属性	暗号化鍵の属性（CEK、DEK、KEK または空き）を表示します。鍵管理サーバの KEK を表示する場合、「KEK（UUID）」の形式で UUID を合わせて表示します。
割り当て先	暗号化鍵の割り当てリソースを表示します。KEK の場合は、「 - 」を表示します。
生成場所	暗号化鍵が生成された場所を表示します。

項目	説明
バックアップ回数	暗号化鍵をバックアップした回数を表示します。KEK の場合は、「 - 」を表示します。

A.2 暗号化環境設定編集ウィザード

関連タスク

- 3.1.2 暗号化環境を設定する
- 3.13 暗号化環境設定を初期化する

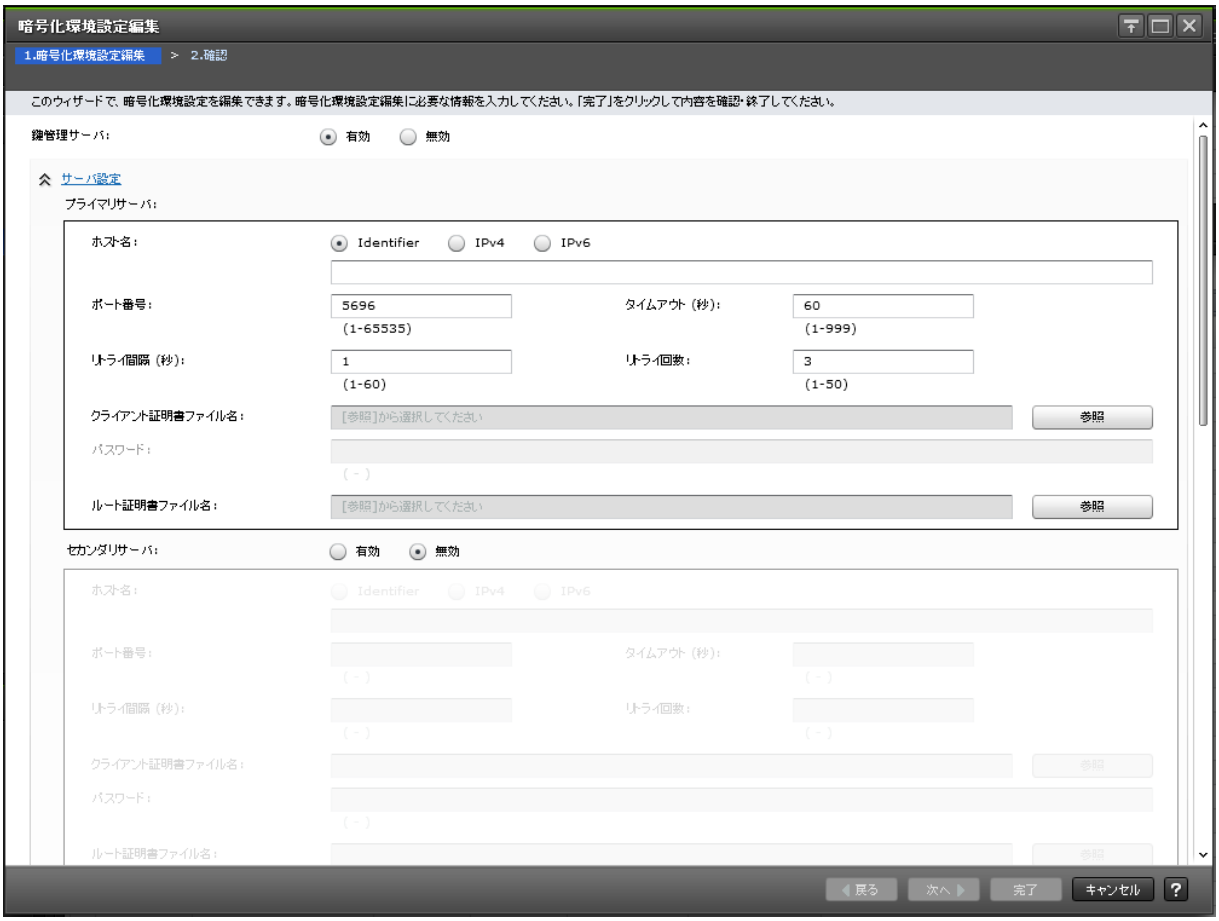
関連参照

- 付録 A.2.1 ［暗号化環境設定編集］画面
- 付録 A.2.2 ［設定確認］画面

A.2.1 ［暗号化環境設定編集］画面

次の条件によって、［暗号化環境設定編集］画面の設定項目が変わります。

- 鍵管理サーバを使用しない場合
- ローカル鍵生成を無効にする場合
- 鍵管理サーバの鍵暗号化鍵を DKC に保存する場合



情報設定エリア

項目	説明
鍵管理サーバ	鍵管理サーバを使用するかどうかを選択します。［暗号化環境設定編集］を一度も実施していない場合、［有効］または［無効］のどちらも選択されていません。 • 有効：鍵管理サーバを使用します。 • 無効：鍵管理サーバを使用しません。
サーバ設定	鍵管理サーバを使用する場合、次のサーバの項目を表示します。 • プライマリサーバ • セカンダリサーバ • サーバ構成テスト
プライマリサーバ	プライマリサーバの情報を入力します。 • ホスト名：鍵管理サーバのホスト名を入力します。 Identifier：ホストの識別子を入力します。 IPv4：ホストの IPv4 アドレスを入力します。 IPv6：ホストの IPv6 アドレスを入力します。 • ポート番号：鍵管理サーバのポート番号を入力します。設定できる値は 1 から 65535 までで、初期値は 5696 です。 • タイムアウト（秒）：鍵管理サーバへの接続がタイムアウトとなるまでの時間を入力します。設定できる値は 1 から 999 までで、初期値は 60 です。 • リトライ間隔（秒）：鍵管理サーバへの接続をリトライする間隔を入力します。設定できる値は 1 から 60 までで、初期値は 1 です。 • リトライ回数：鍵管理サーバへの接続をリトライする回数を入力します。設定できる値は 1 から 50 までで、初期値は 3 です。 • クライアント証明書ファイル名：鍵管理サーバに接続するためのクライアント証明書ファイルを選択します。［参照］から選択してください。 • 参照：クライアント証明書ファイルを選択してください。クライアント証明書の規格は PKCS#12 です。クライアント証明書ファイルがわからない場合は、サーバの管理者またはネットワークの管理者にお尋ねください。 クライアント証明書ファイルを選択すると、選択したクライアント証明書ファイルのファイル名が［クライアント証明書ファイル名］に表示されます。 • パスワード：クライアント証明書用のパスワードを入力します。パスワードは 0 文字以上 128 文字以下で、使用できる文字は次のとおりです。 数字（0 から 9） 英大文字（A から Z） 英小文字（a から z） 記号 31 種：! # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~ • ルート証明書ファイル名：鍵管理サーバに接続するためのルート証明書ファイルを選択します。［参照］から選択してください。 • 参照：ルート証明書ファイルを選択してください。ルート証明書の規格は X.509 です。ルート証明書ファイルがわからない場合は、サーバの管理者またはネットワークの管理者にお尋ねください。 ルート証明書ファイルを選択すると、選択したルート証明書ファイルのファイル名が［ルート証明書ファイル名］に表示されます。
セカンダリサーバ	［セカンダリサーバ］を［有効］に設定した場合、［プライマリサーバ］と同じ内容が設定できます。 **注意：**［セカンダリサーバ］が［無効］に設定されている場合、［鍵暗号化鍵を鍵管理サーバで保護する］、［鍵管理サーバへ暗号化鍵定期バックアップを有効にする］、および［ローカル鍵生成を無効にする］にチェックマークを付けることはできません。

項目	説明
サーバ構成テスト	設定された内容で鍵管理サーバへ接続テストします。接続テストするには［チェック］をクリックしてください。
チェック	設定された内容で鍵管理サーバへ接続テストします。
結果	鍵管理サーバへの接続テストの結果が表示されます。
鍵管理サーバへ暗号化鍵定期バックアップを有効にする	暗号化鍵の定期バックアップを実行する場合は、チェックマークを付けてください。 **注意：**［鍵管理サーバ］が［無効］に設定されている場合、チェックマークを付けることはできません。
定期バックアップ時刻	暗号化鍵をバックアップしたい時間を選択します。複数選択できます。 ［全選択］にチェックマークを付けるとすべての時間が選択され、［全選択］のチェックマークを解除するとすべての時間の選択が解除されます。
定期バックアップユーザ	定期バックアップユーザの情報を入力します。 • ユーザ名：定期バックアップユーザのユーザ名を入力します。 • パスワード：定期バックアップユーザのパスワードを入力します。
鍵管理サーバで暗号化鍵生成	暗号化鍵を鍵管理サーバ上で作成する場合は、チェックマークを付けてください。
鍵暗号化鍵を鍵管理サーバで保護する	鍵暗号化鍵を鍵管理サーバに保存したい場合に指定します。 チェックマークを付けると、［注意事項］が表示されます。注意事項の内容をご確認の上、［注意事項に同意する］にチェックマークを付けてください。 **注意：**［セカンダリサーバ］が［無効］に設定されている場合、チェックマークを付けることはできません。
PS OFF 時に装置内の暗号化鍵を削除する	暗号化鍵を鍵管理サーバに保存し、装置電源 OFF 時に装置内の暗号化鍵を削除する場合は、チェックマークを付けてください。 チェックマークを付けると、［注意事項］が表示されます。注意事項の内容をご確認の上、［注意事項に同意する］にチェックマークを付けてください。 **注意：**［セカンダリサーバ］が［無効］に設定されている場合、チェックマークを付けることはできません。
ローカル鍵生成を無効にする	暗号化鍵を鍵管理サーバ上で作成し、かつ、暗号化鍵をストレージシステム内に作成できないようにする場合は、チェックマークを付けてください。 チェックマークを付けると、［注意事項］が表示されます。注意事項の内容をご確認の上、［注意事項に同意する］にチェックマークを付けてください。 **注意：**［セカンダリサーバ］が［無効］に設定されている場合、チェックマークを付けることはできません。 **注意：**チェックマークを付けて設定を完了すると元に戻すことができません。チェックマークを付けるときには、設定をしても問題がないことをよく確認してください。
暗号化環境設定初期化	暗号化環境設定を初期化します。

関連参照

- 付録 A.2 暗号化環境設定編集ウィザード

A.2.2 ［設定確認］画面

［暗号化環境設定］テーブル

項目	説明
プライマリサーバ	プライマリサーバの情報を表示します。 • 鍵管理サーバ：鍵管理サーバを使用しているかどうかを表示します。 ◦ 有効：鍵管理サーバを使用します。 ◦ 無効：鍵管理サーバを使用しません。 ◦ 未定義：暗号化環境設定を初期化します。 • ホスト名：鍵管理サーバのホスト名を表示します。 • ポート番号：鍵管理サーバのポート番号を表示します。 • タイムアウト（秒）：鍵管理サーバへの接続がタイムアウトとなるまでの時間を表示します。 • リトライ間隔（秒）：鍵管理サーバへの接続をリトライする間隔を表示します。 • リトライ回数：鍵管理サーバへの接続をリトライする回数を表示します。 • クライアント証明書ファイル名：鍵管理サーバに接続するためのクライアント証明書ファイルを表示します。 • パスワード：クライアント証明書用のパスワードを、「******」（6 つのアスタリスク）で表示します。 • ルート証明書ファイル名：鍵管理サーバに接続するためのルート証明書ファイルを表示します。
セカンダリサーバ	セカンダリサーバがある場合、セカンダリサーバに対応した内容を表示します。
鍵管理サーバへ暗号化鍵定期バックアップ	暗号化鍵の定期バックアップを実行するかどうかを表示します。 • 該当：暗号化鍵の定期バックアップを実行します。 • 非該当：暗号化鍵の定期バックアップを実行しません。
定期バックアップ時刻	暗号化鍵をバックアップする時間を表示します。
定期バックアップユーザ名	定期バックアップユーザのユーザ名を表示します。
パスワード	定期バックアップユーザのパスワードを、「******」（6 つのアスタリスク）で表示します。
サーバで暗号化鍵生成	暗号化鍵を鍵管理サーバ上で作成するかどうかを表示します。 • 該当：暗号化鍵を鍵管理サーバ上で作成します。 • 非該当：暗号化鍵を鍵管理サーバ上で作成しません。

項目	説明
鍵暗号化鍵を鍵管理サーバで保護	鍵暗号化鍵を鍵管理サーバに保存するかどうかを表示します。 • 該当：鍵暗号化鍵を鍵管理サーバに保存します。 • 非該当：鍵暗号化鍵を鍵管理サーバに保存しません。
PS OFF 時に装置内の暗号化鍵を削除する	暗号化鍵を鍵管理サーバに保存し、装置電源 OFF 時に装置内の暗号化鍵を削除するかどうかを表示します。 • 該当：暗号化鍵を鍵管理サーバに保存し、装置電源 OFF 時に装置内の暗号化鍵を削除します。 • 非該当：装置電源 OFF 時に装置内の暗号化鍵を削除しません。
ローカル鍵生成を無効にする	暗号化鍵を鍵管理サーバ上で作成し、かつ、暗号化鍵をストレージシステム内に作成できないようにするかどうかを表示します。 • 該当：暗号化鍵を鍵管理サーバ上で作成し、かつ、ストレージシステム内で暗号化鍵を作成できないようになっています。 • 非該当：暗号化鍵を鍵管理サーバ上で作成しません。暗号化鍵はストレージシステム内で作成されます。

関連参照

- 付録 A.2 暗号化環境設定編集ウィザード

A.3 鍵生成ウィザード

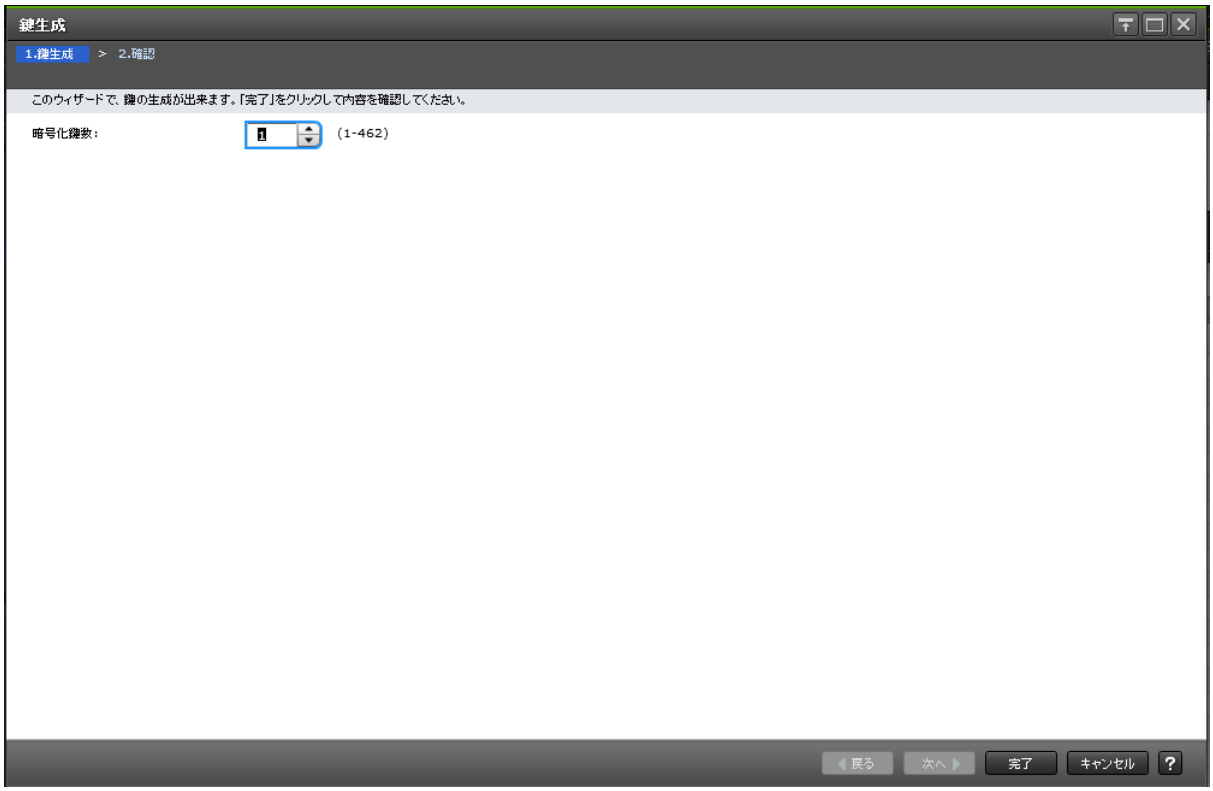
関連タスク

- 3.2 暗号化鍵を作成する

関連参照

- 付録 A.3.1 ［鍵生成］画面
- 付録 A.3.2 ［設定確認］画面

A.3.1 ［鍵生成］画面



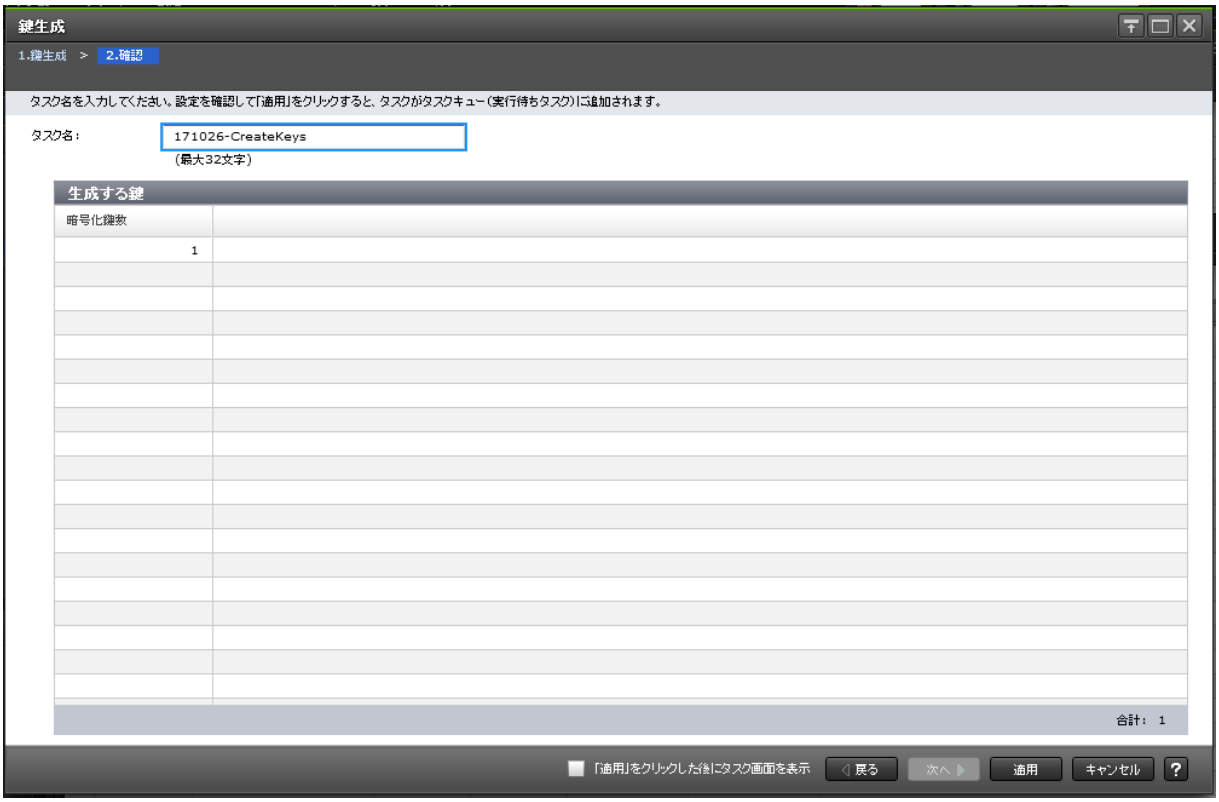
情報設定エリア

項目	説明
暗号化鍵数	暗号化する鍵の数を 1～上限値の範囲で指定します。画面には上限値から作成済みの DEK および未使用鍵の鍵数を引いた値が表示されます。 暗号化鍵数の上限値を次に示します。 • VSP G150、VSP G350、VSP G370、VSP F350、および VSP F370：1,024 • VSP G700 および VSP F700：4,096 • VSP G900 および VSP F900：4,096 • VSP E990：4,096

関連参照

- 付録 A.3 鍵生成ウィザード

A.3.2 ［設定確認］画面



［生成する鍵］テーブル

項目	説明
暗号化鍵数	暗号化する鍵の数を表示します。

関連参照

- 付録 A.3 鍵生成ウィザード

A.4 パスワードポリシー編集（暗号化鍵バックアップ）ウィザード

関連タスク

- 3.3.1 管理クライアント内に暗号化鍵をファイルとしてバックアップするときに設定するパスワードの最小文字数を設定する

関連参照

- 付録 A.4.1 ［パスワードポリシー編集（暗号化鍵バックアップ）］画面
- 付録 A.4.2 ［設定確認］画面

A.4.1 ［パスワードポリシー編集（暗号化鍵バックアップ）］画面

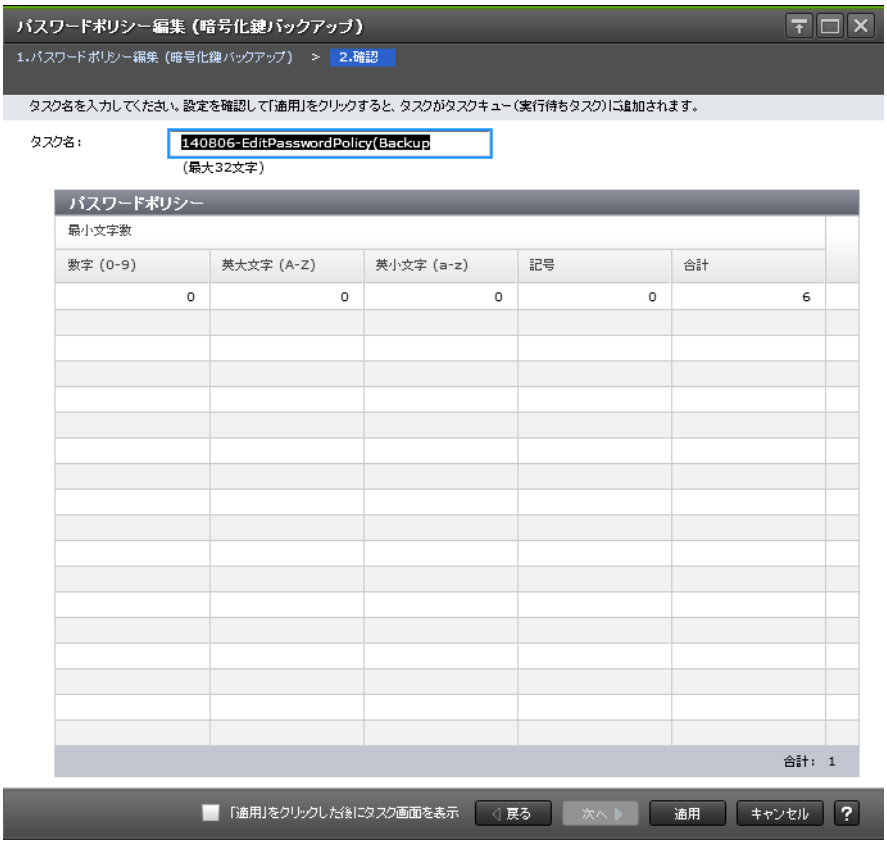
情報設定エリア

項目	説明
数字 (0-9)	パスワードに使用する数字の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
英大文字 (A-Z)	パスワードに使用する英大文字の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
英小文字 (a-z)	パスワードに使用する英小文字の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
記号	パスワードに使用する記号の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
合計	パスワードの最小文字数を入力します。設定できる値は 6 から 255 までで、初期値は 6 です。

関連参照

- 付録 A.4 パスワードポリシー編集（暗号化鍵バックアップ）ウィザード

A.4.2 ［設定確認］画面



［パスワードポリシー］テーブル

項目	説明
数字 (0-9)	パスワードに使用する数字の最小文字数を表示します。
英大文字 (A-Z)	パスワードに使用する英大文字の最小文字数を表示します。
英小文字 (a-z)	パスワードに使用する英小文字の最小文字数を表示します。
記号	パスワードに使用する記号の最小文字数を表示します。
合計	パスワードの最小文字数を表示します。

関連参照

- 付録 A.4 パスワードポリシー編集（暗号化鍵バックアップ）ウィザード

A.5 鍵バックアップウィザード（管理クライアント内にファイルとしてバックアップする場合）

関連タスク

- 3.3.2 管理クライアント内にファイルとして暗号化鍵をバックアップする

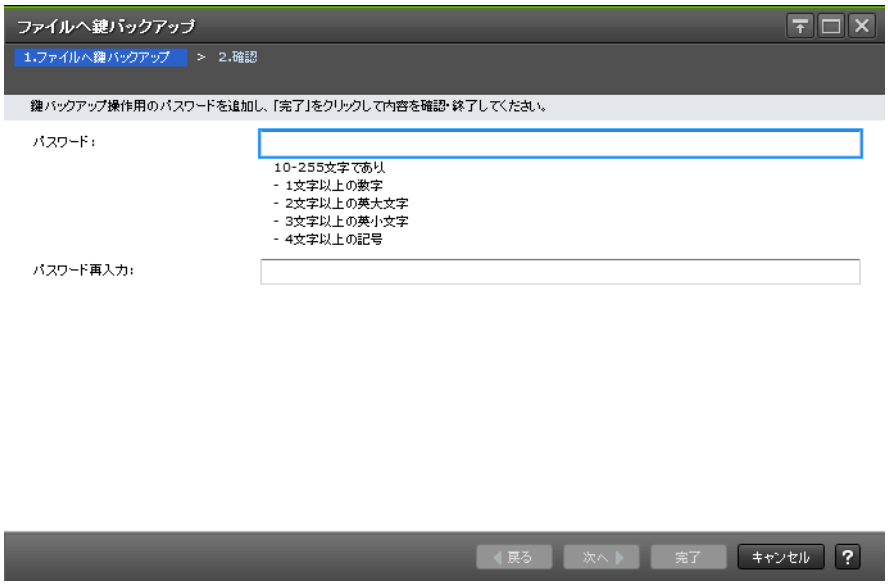
関連参照

- 付録 A.5.1 ［ファイルへ鍵バックアップ］画面

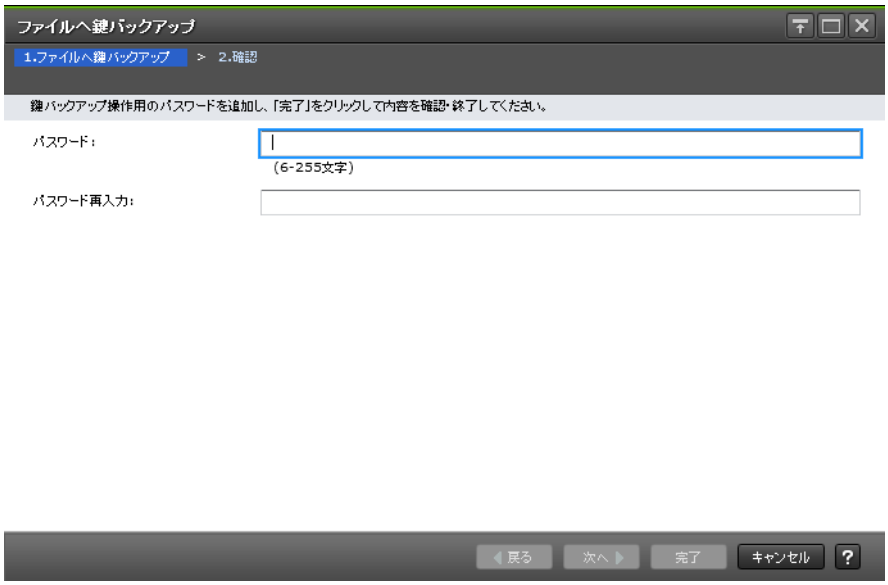
- 付録 A.5.2 ［設定確認］画面

A.5.1 ［ファイルへ鍵バックアップ］画面

- ［パスワードポリシー編集（暗号化鍵バックアップ）］画面で、パスワードに使用する最小文字数が設定されている場合



- ［パスワードポリシー編集（暗号化鍵バックアップ）］画面で、パスワードに使用する最小文字数が設定されていない場合



情報設定エリア

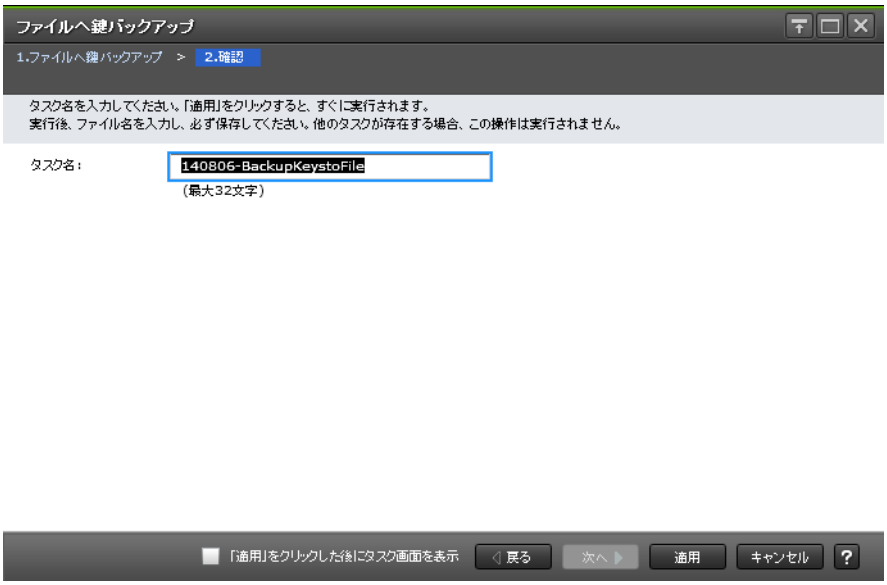
項目	説明
パスワード	暗号化鍵用のパスワードを入力します。パスワードは 6 文字以上 255 文字以下で、使用できる文字は次のとおりです。 ・ 数字（0 から 9） ・ 英大文字（A から Z） ・ 英小文字（a から z） ・ 記号 32 種：!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~

項目	説明
	［パスワードポリシー編集（暗号化鍵バックアップ）］画面で、パスワードに使用する最小文字数が設定されている場合は、使用する最小文字数が［ファイルへ鍵バックアップ］画面に表示されます。
パスワード再入力	［パスワード］で入力したパスワードを再度入力します。

関連参照

- 付録 A.5 鍵バックアップウィザード（管理クライアント内にファイルとしてバックアップする場合）

A.5.2 ［設定確認］画面



［適用］ボタンをクリックすると、準備の完了を知らせるメッセージが表示されます。［OK］ボタンをクリックすると暗号化鍵ファイルを保存する画面が表示されますので、暗号化鍵ファイルを保存してください。暗号化鍵ファイルの拡張子は[.ekf]としてください。

関連参照

- 付録 A.5 鍵バックアップウィザード（管理クライアント内にファイルとしてバックアップする場合）

A.6 鍵バックアップウィザード（鍵管理サーバに接続してバックアップする場合）

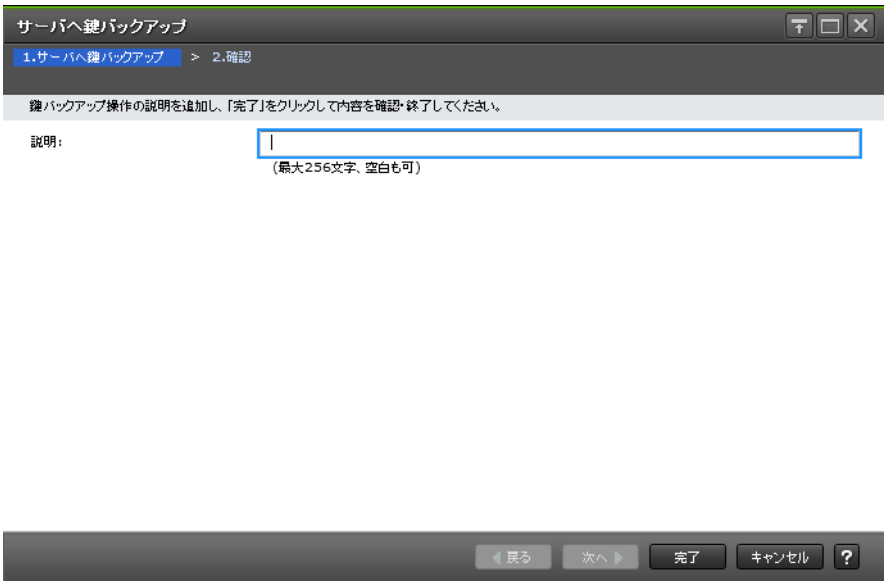
関連タスク

- 3.3.3 鍵管理サーバに接続して暗号化鍵をバックアップする

関連参照

- 付録 A.6.1 ［サーバへ鍵バックアップ］画面
- 付録 A.6.2 ［設定確認］画面

A.6.1 ［サーバへ鍵バックアップ］画面



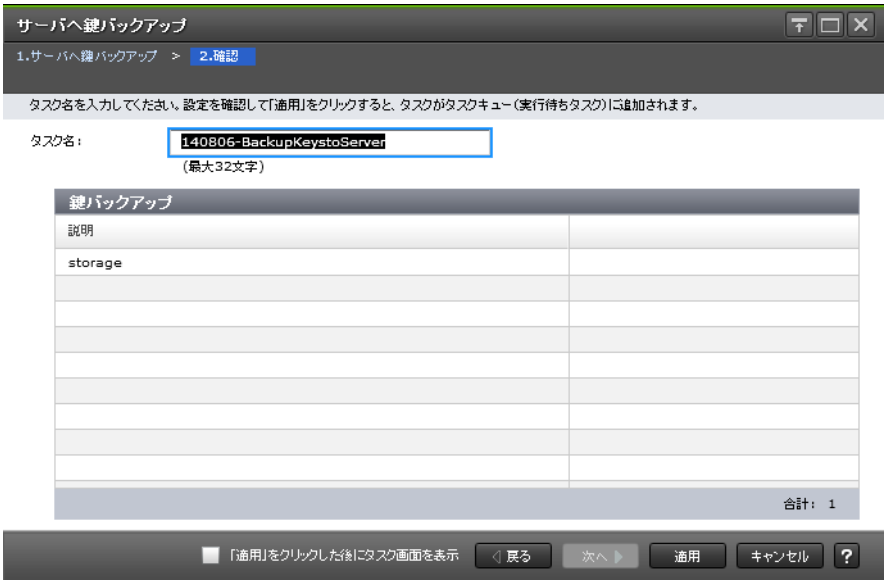
情報設定エリア

項目	説明
説明	暗号化鍵をバックアップする目的を入力します。入力は任意です。 入力できる文字は 256 文字までです。

関連参照

- 付録 A.6 鍵バックアップウィザード（鍵管理サーバに接続してバックアップする場合）

A.6.2 ［設定確認］画面



［鍵バックアップ］テーブル

項目	説明
説明	暗号化鍵をバックアップする目的を表示します。

関連参照

- 付録 A.6 鍵バックアップウィザード（鍵管理サーバに接続してバックアップする場合）

A.7 鍵回復ウィザード(管理クライアント内にバックアップしたファイルからリストアする場合)

関連タスク

- 3.6.1 管理クライアント内にバックアップしたファイルから暗号化鍵をリストアする

関連参照

- 付録 A.7.1 ［ファイルから鍵回復］画面
- 付録 A.7.2 ［設定確認］画面

A.7.1 ［ファイルから鍵回復］画面

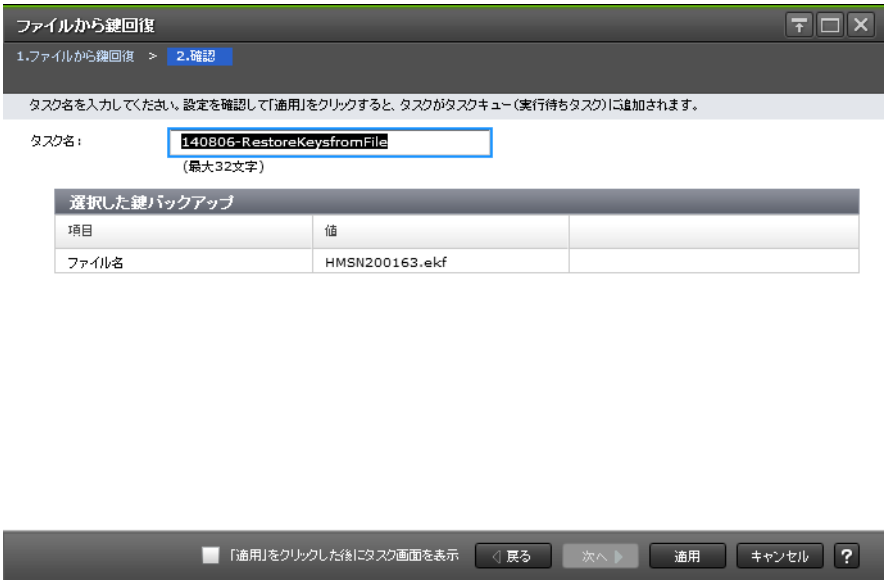
情報設定エリア

項目	説明
ファイル名	［参照］で選択した暗号化鍵ファイルのファイル名が表示されます。
参照	暗号化鍵ファイルを選択してください（ファイル拡張子.ekf)。 暗号化鍵ファイルを選択すると、選択した暗号化鍵ファイルのファイル名が［ファイル名］に表示されます。
パスワード	暗号化鍵をバックアップしたときに入力したパスワードを入力します。

関連参照

- 付録 A.7 鍵回復ウィザード（管理クライアント内にバックアップしたファイルからリストアする場合）

A.7.2 ［設定確認］画面



［選択した鍵バックアップ］テーブル

項目	説明
項目	ファイル名が表示されます。
値	回復する暗号化鍵の実際のファイル名が表示されます。

関連参照

- 付録 A.7 鍵回復ウィザード（管理クライアント内にバックアップしたファイルからリストアする場合）

A.8 強制鍵回復ウィザード（管理クライアント内にバックアップしたファイルから強制リストアする場合）

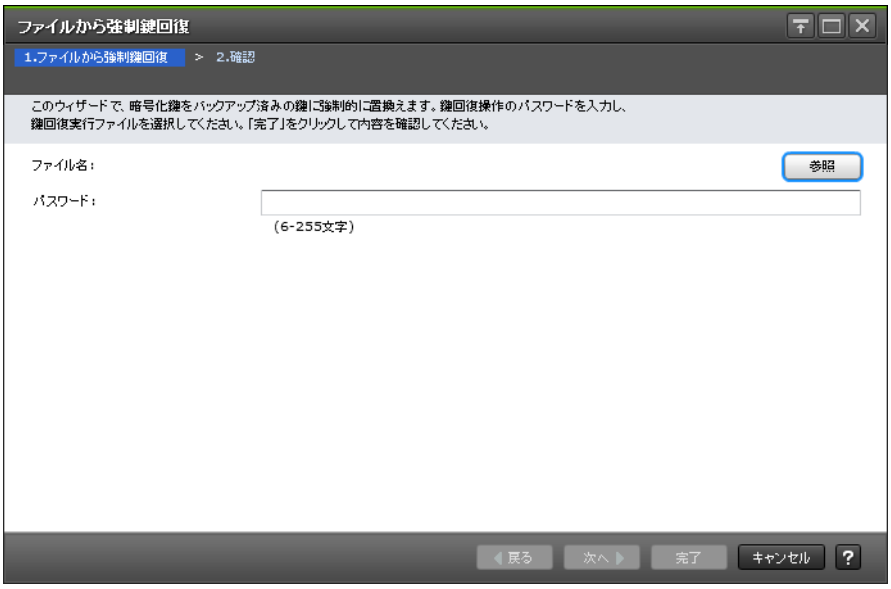
関連タスク

- 3.7.1 管理クライアント内にバックアップしたファイルから暗号化鍵を強制リストアする

関連参照

- 付録 A.8.1 ［ファイルから強制鍵回復］画面
- 付録 A.8.2 ［設定確認］画面

A.8.1 ［ファイルから強制鍵回復］画面



情報設定エリア

項目	説明
ファイル名	［参照］で選択した暗号化鍵ファイルのファイル名が表示されます。
参照	暗号化鍵ファイルを選択してください（ファイル拡張子.ekf)。 暗号化鍵ファイルを選択すると、選択した暗号化鍵ファイルのファイル名が［ファイル名］に表示されます。
パスワード	暗号化鍵をバックアップしたときに入力したパスワードを入力します。

関連参照

- 付録 A.8 強制鍵回復ウィザード（管理クライアント内にバックアップしたファイルから強制リストアする場合）

A.8.2 ［設定確認］画面

［選択した鍵バックアップ］テーブル

項目	説明
項目	ファイル名が表示されます。
値	回復する暗号化鍵の実際のファイル名が表示されます。

関連参照

- 付録 A.8 強制鍵回復ウィザード（管理クライアント内にバックアップしたファイルから強制リストアする場合）

A.9 鍵回復ウィザード（鍵管理サーバに接続してリストアする場合）

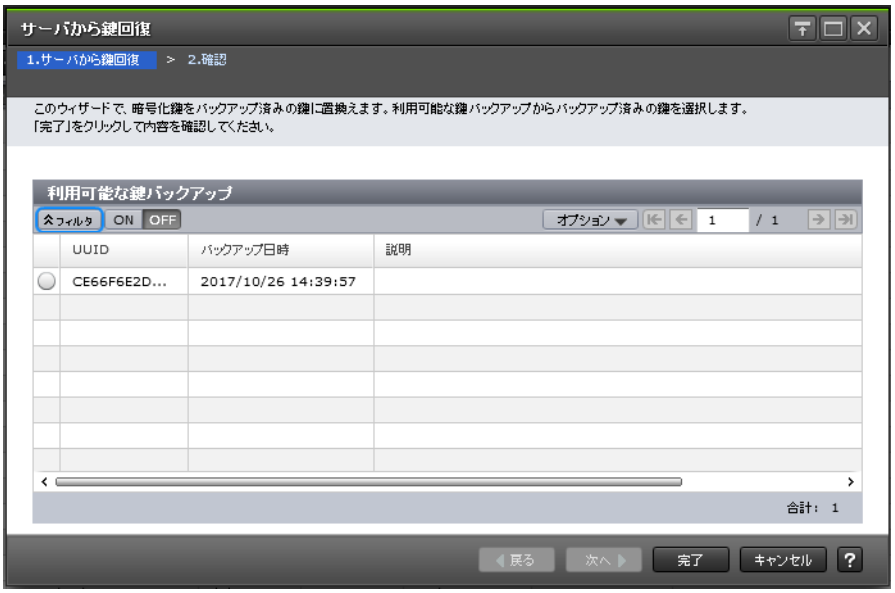
関連タスク

- 3.6.2 鍵管理サーバに接続して暗号化鍵をリストアする

関連参照

- 付録 A.9.1 ［サーバから鍵回復］画面
- 付録 A.9.2 ［設定確認］画面

A.9.1 ［サーバから鍵回復］画面



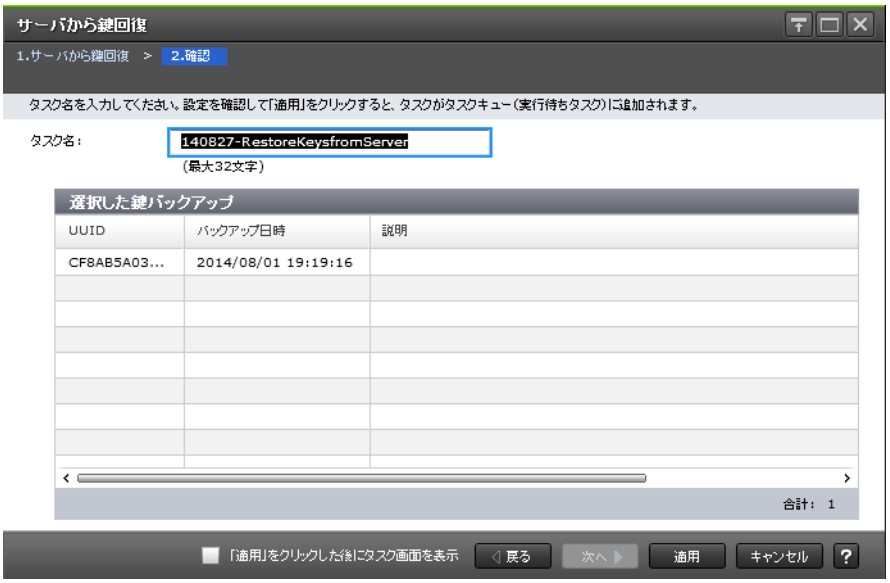
［利用可能な鍵バックアップ］テーブル

項目	説明
UUID	鍵管理サーバにバックアップされた暗号化鍵の UUID が表示されます。
バックアップ日時	暗号化鍵が鍵管理サーバにバックアップされた日時が表示されます。
説明	暗号化鍵を鍵管理サーバにバックアップしたときに入力した説明が表示されます。 定期バックアップでバックアップした暗号化鍵は、「AutoBackup_[バックアップ年月日_バックアップ時刻]」の形式で表示されます。

関連参照

- 付録 A.9 鍵回復ウィザード（鍵管理サーバに接続してリストアする場合）

A.9.2 ［設定確認］画面



［選択した鍵バックアップ］テーブル

項目	説明
UUID	鍵管理サーバにバックアップされた暗号化鍵の UUID が表示されます。
バックアップ日時	暗号化鍵が鍵管理サーバにバックアップされた日時が表示されます。
説明	暗号化鍵を鍵管理サーバにバックアップしたときに入力した説明が表示されます。 定期バックアップでバックアップした暗号化鍵は、「AutoBackup_[バックアップ年月日_バックアップ時刻]」の形式で表示されます。

関連参照

- 付録 A.9 鍵回復ウィザード（鍵管理サーバに接続してリストアする場合）

A.10 強制鍵回復ウィザード（鍵管理サーバに接続して強制リストアする場合）

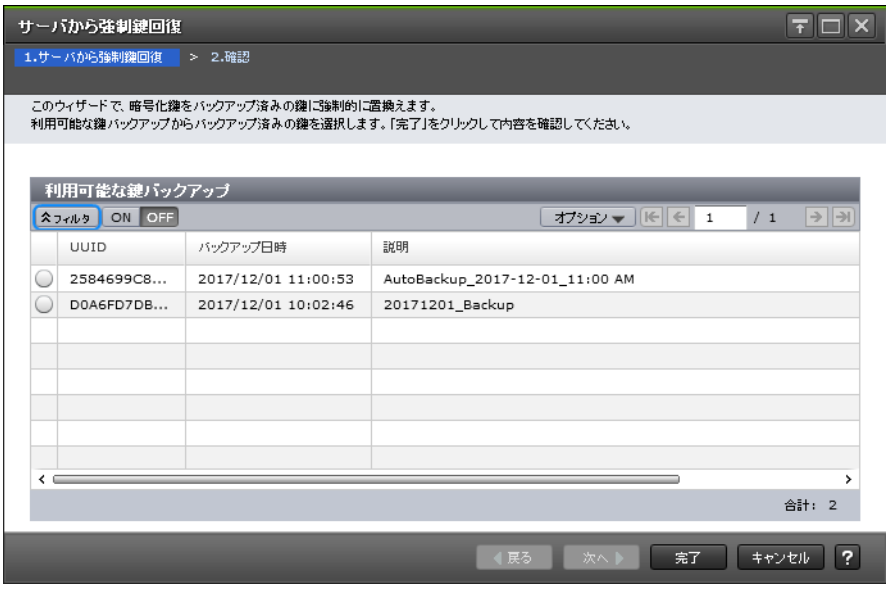
関連タスク

- 3.7.2 鍵管理サーバに接続して暗号化鍵を強制リストアする

関連参照

- 付録 A.10.1 ［サーバから強制鍵回復］画面
- 付録 A.10.2 ［設定確認］画面

A.10.1 ［サーバから強制鍵回復］画面



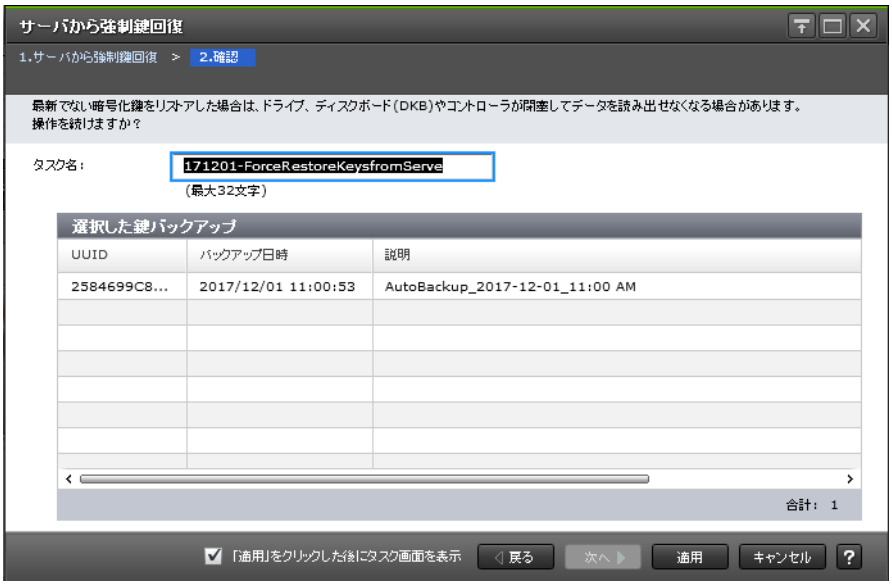
［利用可能な鍵バックアップ］テーブル

項目	説明
UUID	鍵管理サーバにバックアップされた暗号化鍵の UUID が表示されます。
バックアップ日時	暗号化鍵が鍵管理サーバにバックアップされた日時が表示されます。
説明	暗号化鍵を鍵管理サーバにバックアップしたときに入力した説明が表示されます。 定期バックアップでバックアップした暗号化鍵は、「AutoBackup_[バックアップ年月日_バックアップ時刻]」の形式で表示されます。

関連参照

- 付録 A.10 強制鍵回復ウィザード（鍵管理サーバに接続して強制リストアする場合）

A.10.2 ［設定確認］画面



［選択した鍵バックアップ］テーブル

項目	説明
UUID	鍵管理サーバにバックアップされた暗号化鍵の UUID が表示されます。
バックアップ日時	暗号化鍵が鍵管理サーバにバックアップされた日時が表示されます。
説明	暗号化鍵を鍵管理サーバにバックアップしたときに入力した説明が表示されます。 定期バックアップでバックアップした暗号化鍵は、「AutoBackup_[バックアップ年月日_バックアップ時刻]」の形式で表示されます。

関連参照

- 付録 A.10 強制鍵回復ウィザード（鍵管理サーバに接続して強制リストアする場合）

A.11 鍵削除ウィザード（ストレージシステム内の暗号化鍵を削除する場合）

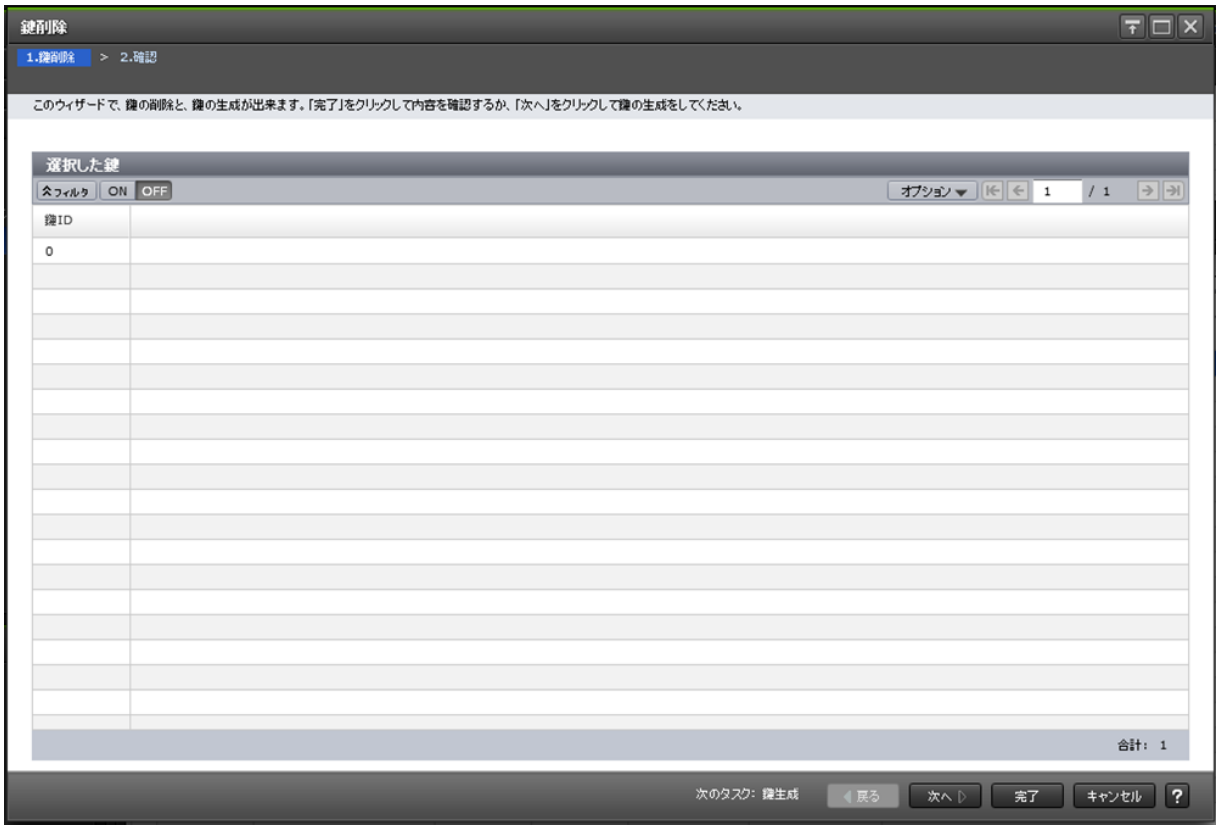
関連タスク

- 3.8.1 ストレージシステム内の暗号化鍵を削除する

関連参照

- 付録 A.11.1 ［鍵削除］画面
- 付録 A.11.2 ［設定確認］画面

A.11.1 ［鍵削除］画面



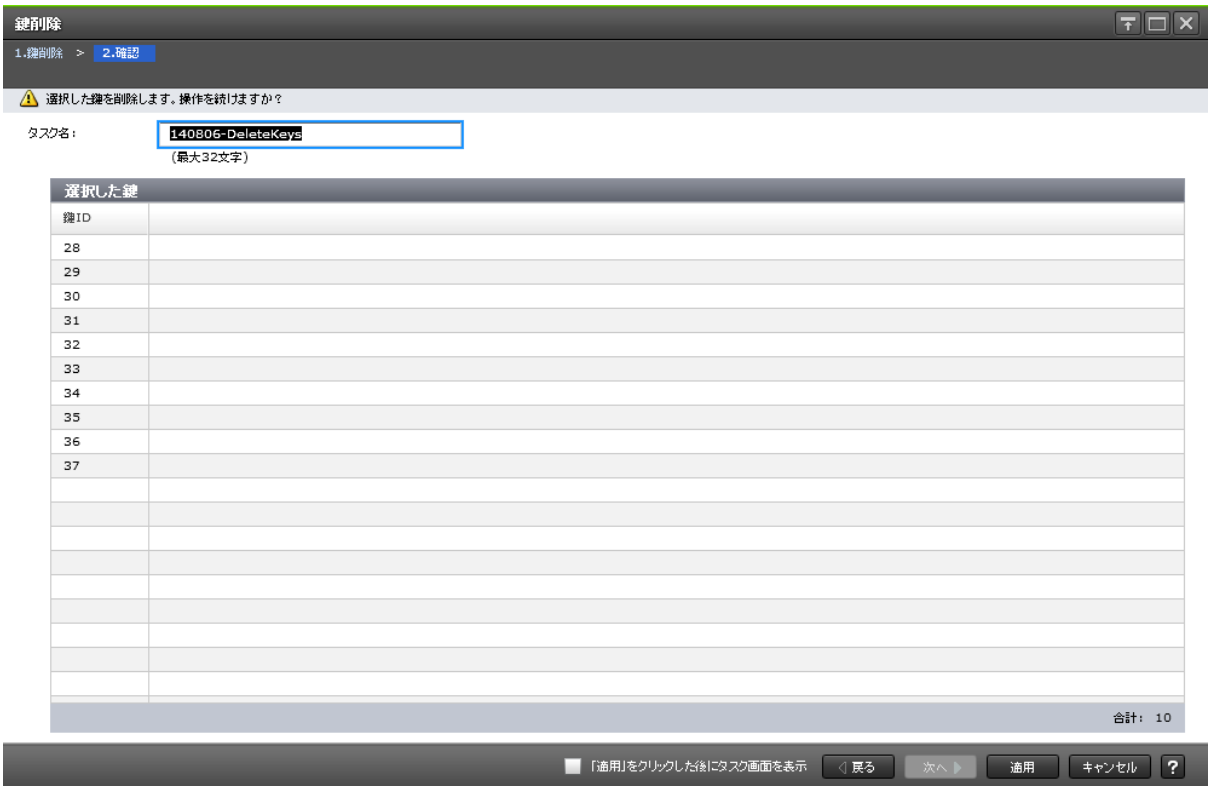
［選択した鍵］テーブル

項目	説明
鍵 ID	暗号化鍵の番号を表示します。

関連参照

- 付録 A.11 鍵削除ウィザード（ストレージシステム内の暗号化鍵を削除する場合）

A.11.2 ［設定確認］画面



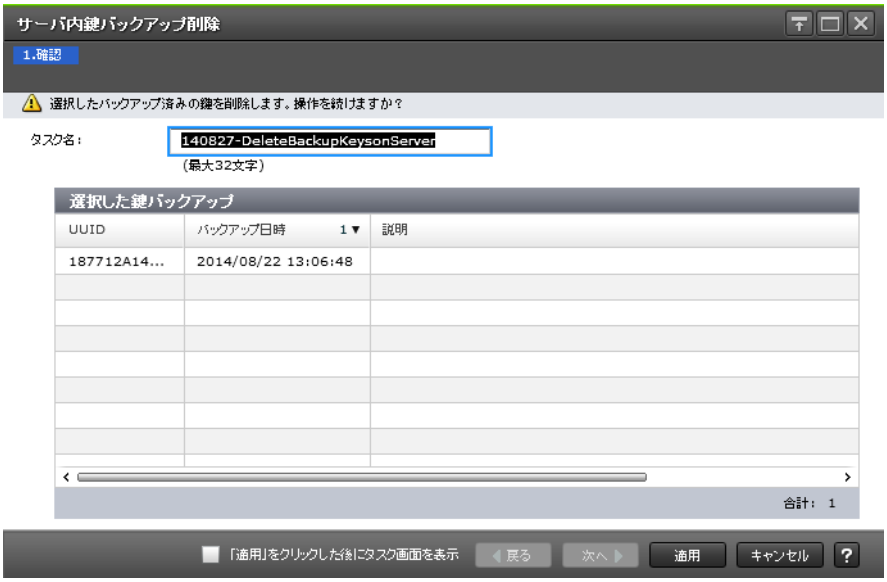
［選択した鍵］テーブル

項目	説明
鍵 ID	暗号化鍵の番号を表示します。

関連参照

- 付録 A.11 鍵削除ウィザード（ストレージシステム内の暗号化鍵を削除する場合）

A.12 ［サーバ内鍵バックアップ削除］画面



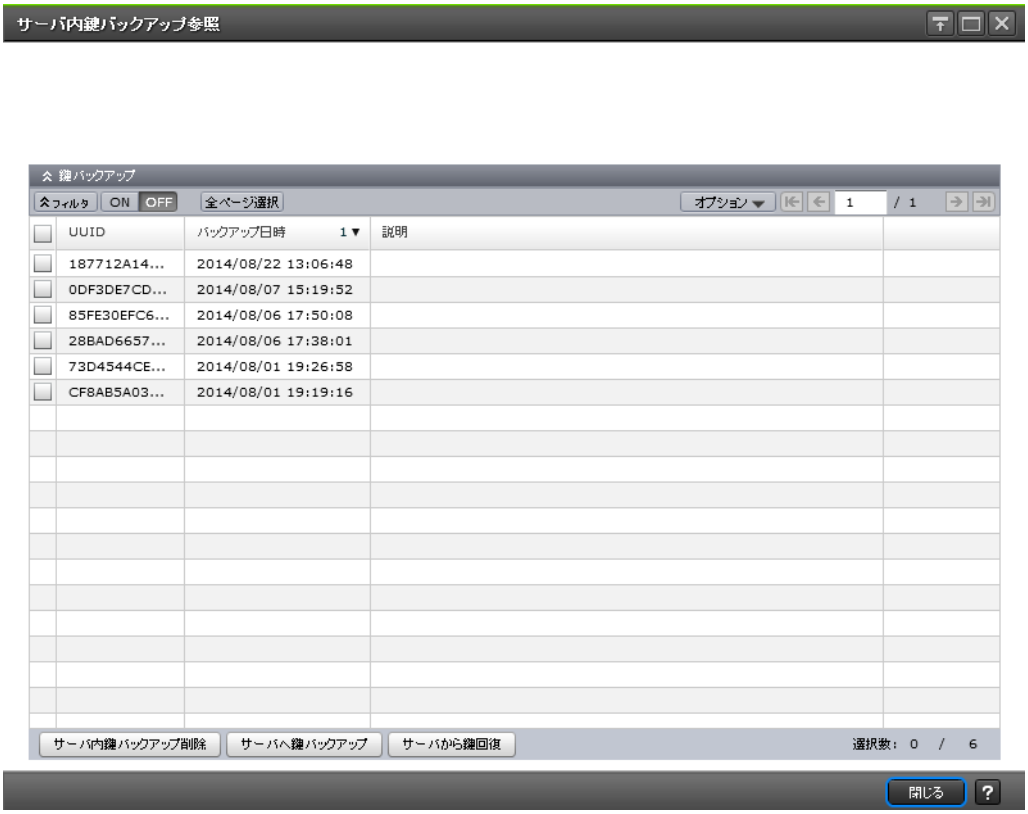
［選択した鍵バックアップ］テーブル

項目	説明
UUID	鍵管理サーバにバックアップされた暗号化鍵の UUID が表示されます。
バックアップ日時	暗号化鍵が鍵管理サーバにバックアップされた日時が表示されます。
説明	暗号化鍵を鍵管理サーバにバックアップしたときに入力した説明が表示されます。 定期バックアップでバックアップした暗号化鍵は、「AutoBackup_[バックアップ年月日_バックアップ時刻]」の形式で表示されます。

関連タスク

- 3.8.2 鍵管理サーバにバックアップした暗号化鍵を削除する

A.13 ［サーバ内鍵バックアップ参照］画面



［鍵バックアップ］テーブル

- テーブル

項目	説明
UUID	鍵管理サーバにバックアップされた暗号化鍵の UUID が表示されます。
バックアップ日時	暗号化鍵が鍵管理サーバにバックアップされた日時が表示されます。
説明	暗号化鍵を鍵管理サーバにバックアップしたときに入力した説明が表示されます。 定期バックアップでバックアップした暗号化鍵は、「AutoBackup_[バックアップ年月日_バックアップ時刻]」の形式で表示されます。

- ボタン

項目	説明
サーバ内鍵バックアップ削除	［サーバ内鍵バックアップ削除］画面が表示されます。
サーバへ鍵バックアップ	［サーバへ鍵バックアップ］画面が表示されます。
サーバから鍵回復	［サーバから鍵回復］画面が表示されます。

関連タスク

- 3.9 鍵管理サーバ上にある暗号化鍵の状態を確認する

A.14 暗号化編集ウィザード

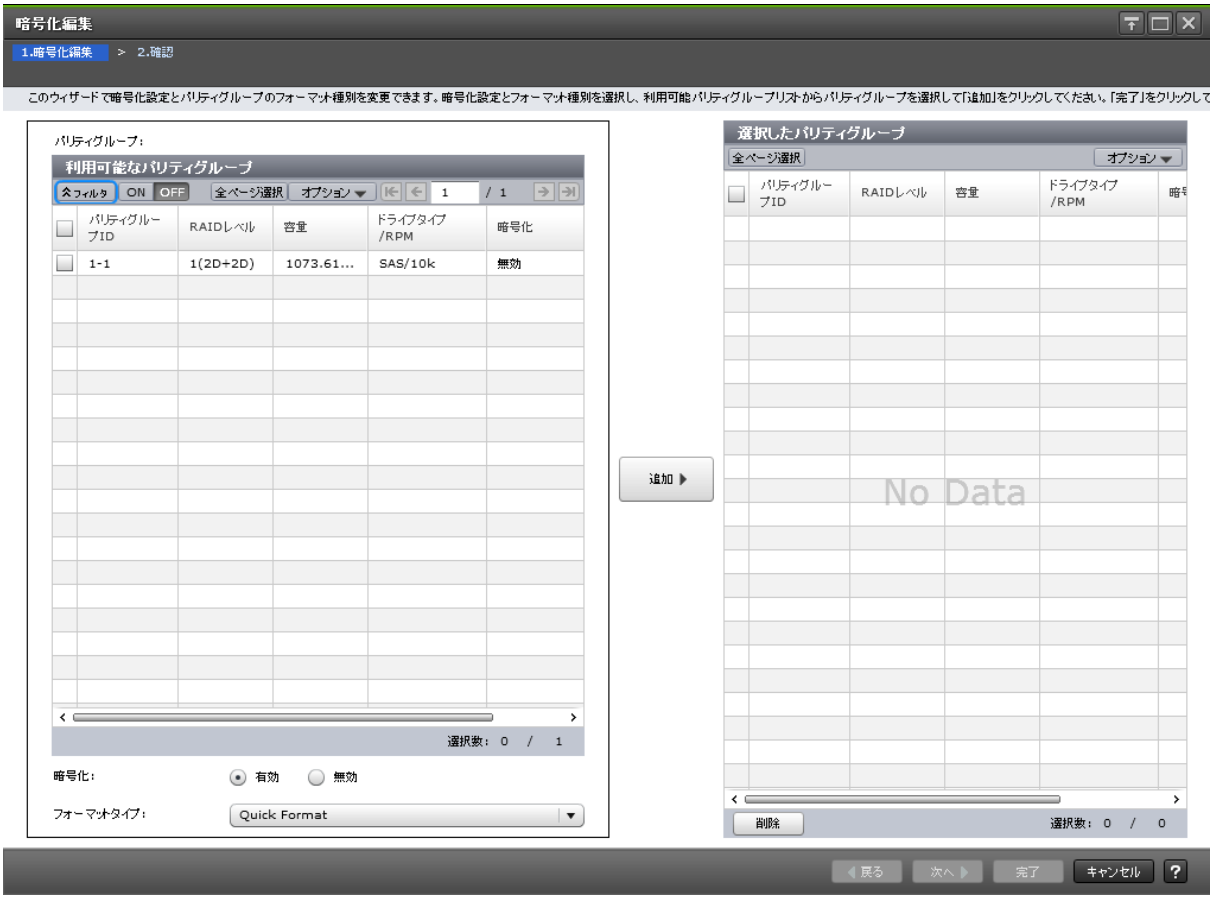
関連タスク

- 3.4.1 データの暗号化を有効にする
- 3.5.1 データの暗号化を無効にする

関連参照

- 付録 A.14.1 ［暗号化編集］画面
- 付録 A.14.2 ［設定確認］画面

A.14.1 ［暗号化編集］画面



［利用可能なパリティグループ］テーブル

項目	説明
パリティグループ ID	パリティグループ ID を表示します。
RAID レベル	パリティグループの RAID レベルを表示します。 分散パリティグループの場合は、分散数が RAID レベルの後ろに表示されます。例：1(2D+2D)*2

項目	説明
容量	パリティグループの総容量を、指定した単位で表示します。
ドライブタイプ/RPM	パリティグループ中のボリュームのドライブ種別と RPM（回転数）を表示します。 この項目は、VSP E990 の場合［ドライブタイプ/インターフェース］と表示されます。
暗号化	暗号化の設定状態が表示されます。 • 有効：暗号化が有効になっています。 • 無効：暗号化が無効になっています。

［暗号化］

暗号化を設定する場合は［有効］を選択します。暗号化を解除する場合は［無効］を選択します。

注意
パリティグループの容量拡張設定が有効になっている場合は、［暗号化］で［有効］を選択しないでください。［暗号化］で［有効］を選択した場合、タスクを実行したときにエラーとなります。

［フォーマットタイプ］

フォーマット種別を選択します。［Quick Format］、［Normal Format］、または［No Format］が選択できます。初期値は［Quick Format］です。

選択されたパリティグループにボリュームが 1 つもない場合はフォーマットが不要です。このため、［フォーマットタイプ］の指定に関わらず、［選択したパリティグループ］テーブルのフォーマットタイプは［ - ］となります。

［追加］ボタン

［利用可能なパリティグループ］テーブルで選択したパリティグループを［選択したパリティグループ］テーブルに追加します。

［選択したパリティグループ］テーブル

• テーブル

項目	説明
パリティグループ ID	パリティグループ ID を表示します。
RAID レベル	パリティグループの RAID レベルを表示します。 分散パリティグループの場合は、分散数が RAID レベルの後ろに表示されます。例：1(2D+2D)*2
容量	パリティグループの総容量を、指定した単位で表示します。
ドライブタイプ/RPM	パリティグループ中のボリュームのドライブ種別と RPM（回転数）を表示します。 この項目は、VSP E990 の場合［ドライブタイプ/インターフェース］と表示されます。
暗号化	設定した暗号化の状態が表示されます。 • 有効：暗号化が有効になっています。 • 無効：暗号化が無効になっています。

項目	説明
フォーマットタイプ	設定したフォーマット種別が表示されます。パリティグループにボリュームが 1 つもない場合はフォーマットが不要です。このため、フォーマットタイプには［ - ］が表示されます。

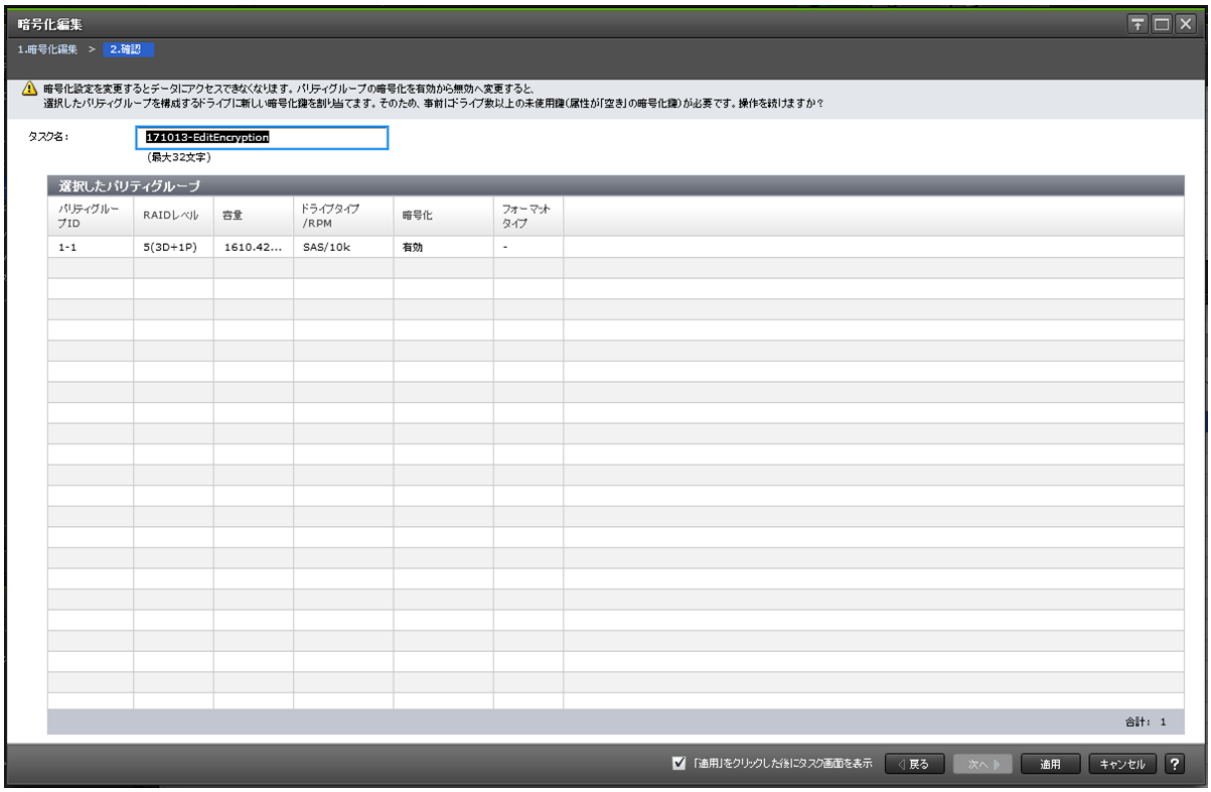
- ボタン

項目	説明
削除	選択したパリティグループを［選択したパリティグループ］テーブルから削除します。

関連参照

- 付録 A.14 暗号化編集ウィザード

A.14.2 ［設定確認］画面



［選択したパリティグループ］テーブル

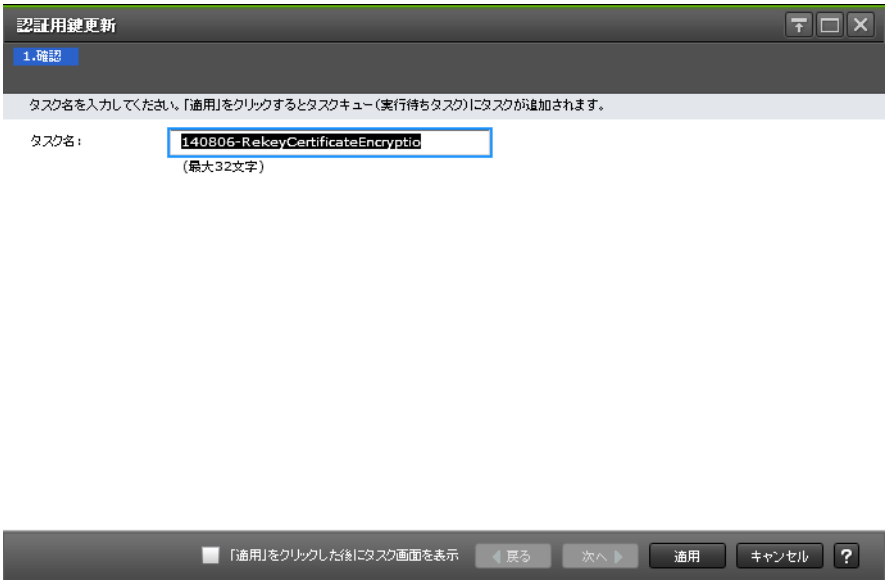
項目	説明
パリティグループ ID	パリティグループ ID を表示します。
RAID レベル	パリティグループの RAID レベルを表示します。 分散パリティグループの場合は、分散数が RAID レベルの後ろに表示されます。例：1(2D+2D)*2
容量	パリティグループの総容量を表示します。
ドライブタイプ/RPM	パリティグループ中のボリュームのを表示します。 この項目は、VSP E990 の場合［ドライブタイプ/インターフェース］と表示されます。

項目	説明
暗号化	設定した暗号化の状態が表示されます。 • 有効：暗号化が有効になっています。 • 無効：暗号化が無効になっています。
フォーマットタイプ	設定したフォーマット種別が表示されます。パリティグループにボリュームが 1 つもない場合はフォーマットが不要です。このため、フォーマットタイプには［ - ］が表示されます。

関連参照

- 付録 A.14 暗号化編集ウィザード

A.15 ［認証用鍵更新］画面



関連タスク

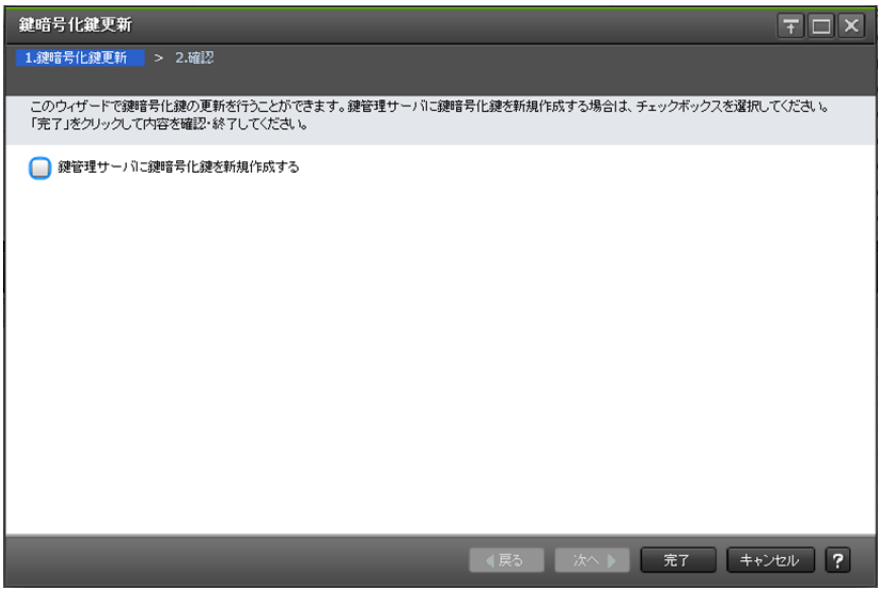
- 3.10.1 認証用鍵を更新する

A.16 鍵暗号化鍵更新ウィザード

関連参照

- 付録 A.16.1 ［鍵暗号化鍵更新］画面
- 付録 A.16.2 ［設定確認］画面

A.16.1 ［鍵暗号化鍵更新］画面



情報設定エリア

項目	説明
鍵管理サーバに鍵暗号化鍵を新規作成する	鍵管理サーバを別サーバへ移行する機能をサポートしていないファームウェアバージョンでは、この画面は表示されません。 鍵暗号化鍵を新規作成する場合のみ、チェックボックスを選択します。 **注意：**鍵管理サーバを別サーバへ移行するときに［暗号化環境設定編集］画面で鍵管理サーバの接続先を変更すると、変更後の鍵管理サーバに鍵暗号化鍵が新規作成されます。 このため、鍵管理サーバを別サーバへ移行するときには、この画面を使用しません。ただし、トラブルによって、鍵管理サーバに鍵暗号化鍵の作成が必要な場合は、このチェックボックスを使用することがあります。

関連参照

- 付録 A.16 鍵暗号化鍵更新ウィザード

A.16.2 ［設定確認］画面

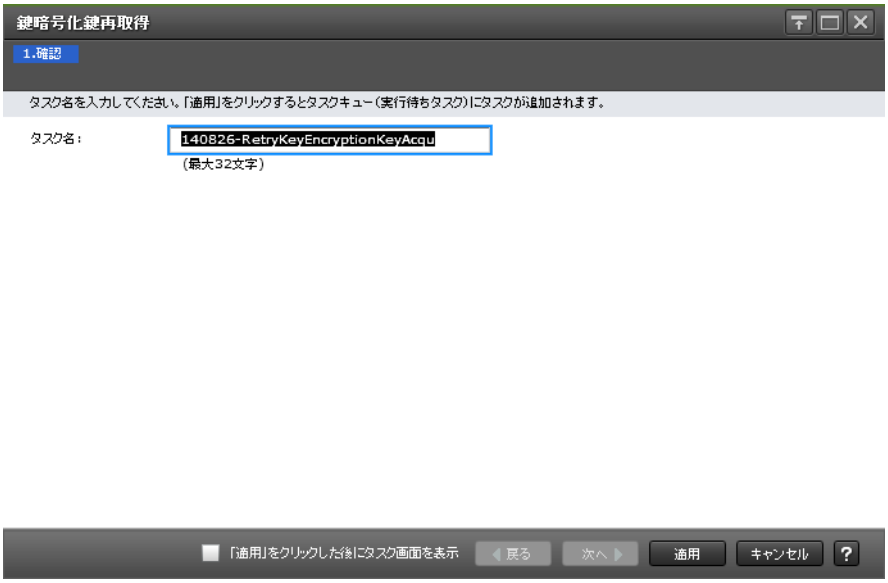
［鍵暗号化鍵更新］テーブル

項目	説明
鍵管理サーバに鍵暗号化鍵を新規作成する	鍵管理サーバを別サーバへ移行する機能をサポートしていないファームウェアバージョンでは、［鍵暗号化鍵更新］テーブルは表示されません。 ［鍵暗号化鍵更新］画面で、［鍵管理サーバに鍵暗号化鍵を新規作成する］を選択したかどうかを示します。 ・ 該当 ・ 非該当

関連参照

・ 付録 A.16 鍵暗号化鍵更新ウィザード

A.17 ［鍵暗号化鍵再取得］画面



関連タスク

- 3.12 鍵暗号化鍵を再取得する

B

このマニュアルの参考情報

このマニュアルを読むに当たっての参考情報を示します。

B.1 操作対象リソースについて

Storage Navigator のメイン画面には、ログインしているユーザ自身に割り当てられているリソースだけが表示されます。ただし、割り当てられているリソースの管理に必要とされる関連のリソースも表示される場合があります。

また、このマニュアルで説明している機能を使用するときには、各操作対象のリソースが特定の条件を満たしている必要があります。

各操作対象のリソースの条件については『システム構築ガイド』を参照してください。

B.2 このマニュアルでの表記

このマニュアルで使用している表記を次の表に示します。

表記	製品名
Storage Navigator	Hitachi Device Manager - Storage Navigator
Virtual Storage Platform F350, F370, F700, F900	次の製品を区別する必要がない場合の表記です。 • Virtual Storage Platform F350 • Virtual Storage Platform F370 • Virtual Storage Platform F700 • Virtual Storage Platform F900
Virtual Storage Platform G150, G350, G370, G700, G900	次の製品を区別する必要がない場合の表記です。 • Virtual Storage Platform G150 • Virtual Storage Platform G350 • Virtual Storage Platform G370 • Virtual Storage Platform G700 • Virtual Storage Platform G900
VSP	Hitachi Virtual Storage Platform
VSP F350	Virtual Storage Platform F350
VSP F370	Virtual Storage Platform F370
VSP F700	Virtual Storage Platform F700
VSP F900	Virtual Storage Platform F900
VSP G150	Virtual Storage Platform G150
VSP G350	Virtual Storage Platform G350
VSP G370	Virtual Storage Platform G370
VSP G700	Virtual Storage Platform G700
VSP G900	Virtual Storage Platform G900
VSP E990	Virtual Storage Platform E990

B.3 このマニュアルで使用している略語

このマニュアルで使用している略語を次の表に示します。

略語	フルスペル
CA	Certificate Authority
DNS	Domain Name System
GUI	Graphical User Interface
ID	IDentifier
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
KMIP	Key Management Interoperability Protocol
LDEV	Logical DEVice
OS	Operating System
RPM	revolution per minute
SIM	Service Information Message
SSL	Secure Sockets Layer
SVP	SuperVisor PC
UUID	User Definable LUN ID

B.4 KB（キロバイト）などの単位表記について

1KB（キロバイト）は 1,024 バイト、1MB（メガバイト）は 1,024KB、1GB（ギガバイト）は 1,024MB、1TB（テラバイト）は 1,024GB、1PB（ペタバイト）は 1,024TB です。

1block（ブロック）は 512 バイトです。1Cyl（シリンダ）を KB に換算した値は、960KB です。

用語解説

（英字）

ALU

（Administrative Logical Unit）
SCSI アーキテクチャモデルである Conglomerate LUN structure に使われる LU です。
Conglomerate LUN structure では、ホストからのアクセスはすべて ALU を介して行われ、ALU はバインドされた SLU に I/O を振り分けるゲートウェイとなります。
ホストは、ALU と ALU にバインドされた SLU を SCSI コマンドで指定して、I/O を発行します。
vSphere では、Protocol Endpoint（PE）と呼ばれます。

ALUA

（Asymmetric Logical Unit Access）
SCSI の非対称論理ユニットアクセス機能です。
ストレージ同士、またはサーバとストレージシステムを複数の交替パスで接続している構成の場合に、どのパスを優先して使用するかをストレージシステムに定義して、I/O を発行できます。優先して使用するパスに障害が発生した場合は、他のパスに切り替わります。

CHB

（Channel Board）
詳しくは「チャネルボード」を参照してください。

CLPR

（Cache Logical Partition）
キャッシュメモリを論理的に分割すると作成されるパーティション（区画）です。

CM

（Cache Memory（キャッシュメモリ））
詳しくは「キャッシュ」を参照してください。

CSV

（Comma Separate Values）
データベースソフトや表計算ソフトのデータをファイルとして保存するフォーマットの１つで、主にアプリケーション間のファイルのやり取りに使われます。それぞれの値はコンマで区切られています。

CTG

（Consistency Group）
詳しくは「コンシステンシーグループ」を参照してください。

CU

（Control Unit（コントロールユニット））
主に磁気ディスク制御装置を指します。

CV

（Customized Volume）
固定ボリューム（FV）を任意のサイズに分割した可変ボリュームです。

DKC

（Disk Controller）
ストレージシステムを制御するコントローラが備わっているシャーシ（筐体）です。

DP-VOL

詳しくは「仮想ボリューム」を参照してください。

ECC

（Error Check and Correct）
ハードウェアで発生したデータの誤りを検出し、訂正することです。

ExG

（External Group）
外部ボリュームを任意にグループ分けしたものです。詳しくは「外部ボリュームグループ」を参照してください。

External MF

詳しくは「マイグレーションボリューム」を参照してください。

FM

（Flash Memory（フラッシュメモリ））
詳しくは「フラッシュメモリ」を参照してください。

FMD

（Flash Module Drive）
ストレージシステムにオプションの記憶媒体として搭載される大容量フラッシュモジュールです。SSD よりも大容量のドライブです。FMD を利用するには専用のドライブボックスが必要になります。FMD と専用のドライブボックスをあわせて HAF（Hitachi Accelerated Flash）と呼びます。

FV

（Fixed Volume）
容量が固定されたボリュームです。

GID

（Group ID）
ホストグループを作成するときに付けられる 2 桁の 16 進数の識別番号です。

HBA

（Host Bus Adapter）
詳しくは「ホストバスアダプタ」を参照してください。

HCS

（Hitachi Command Suite）
ストレージ管理ソフトウェアです。

HDEV

（Host Device）
ホストに提供されるボリュームです。

I/O モード

global-active device ペアのプライマリボリュームとセカンダリボリュームが、それぞれに持つ I/O の動作です。

I/O レート

ドライブへの入出力アクセスが 1 秒間に何回行われたかを示す数値です。単位は IOPS（I/Os per second）です。

In-Band 方式

RAID Manager のコマンド実行方式の 1 つです。コマンドを実行すると、クライアントまたはサーバから、ストレージシステムのコマンドデバイスにコマンドが転送されます。

Initiator

属性が RCU Target のポートと接続するポートが持つ属性です。

LCU

（Logical Control Unit）
主に磁気ディスク制御装置を指します。

LDEV

（Logical Device（論理デバイス））
RAID 技術では冗長性を高めるため、複数のドライブに分散してデータを保存します。この複数のドライブにまたがったデータ保存領域を論理デバイスまたは LDEV と呼びます。ストレージ内の LDEV は、LDKC 番号、CU 番号、LDEV 番号の組み合わせで区別します。LDEV に任意の名前を付けることもできます。
このマニュアルでは、LDEV（論理デバイス）を論理ボリュームまたはボリュームと呼ぶことがあります。

LDEV 名

LDEV 作成時に、LDEV に付けるニックネームです。あとから LDEV 名の変更もできます。

LDKC

（Logical Disk Controller）
複数の CU を管理するグループです。各 CU は 256 個の LDEV を管理しています。

LUN

（Logical Unit Number）
論理ユニット番号です。オープンシステム用のボリュームに割り当てられたアドレスです。オープンシステム用のボリューム自体を指すこともあります。

LUN セキュリティ

LUN に設定するセキュリティです。LUN セキュリティを有効にすると、あらかじめ決めておいたホストだけがボリュームにアクセスできるようになります。

LUN パス、LU パス

オープンシステム用ホストとオープンシステム用ボリュームの間を結ぶデータ入出力経路です。

LUSE ボリューム

オープンシステム用のボリュームが複数連結して構成されている、1 つの大きな拡張ボリュームのことです。ボリュームを拡張することで、ポート当たりのボリューム数が制限されているホストからもアクセスできるようになります。

MP ユニット

データ入出力を処理するプロセッサを含んだユニットです。データ入出力に関連するリソース（LDEV、外部ボリューム、ジャーナル）ごとに特定の MP ユニットを割り当てると、性能をチューニングできます。特定の MP ユニットを割り当てる方法と、ストレージシステムが自動的に選択した MP ユニットを割り当てる方法があります。MP ユニットに対して自動割り当ての設定を無効にすると、その MP ユニットがストレージシステムによって自動的にリソースに割り当てられることはないため、特定のリソース専用の MP ユニットとして使用できます。

MU

（Mirror Unit）
1 つのプライマリボリュームと 1 つのセカンダリボリュームを関連づける情報です。

Out-of-Band 方式

RAID Manager のコマンド実行方式の 1 つです。コマンドを実行すると、クライアントまたはサーバから LAN 経由で SVP/GUM/RAID Manager サーバの中にある仮想コマンドデバイスにコマンドが転送されます。仮想コマンドデバイスからストレージシステムに指示を出し、ストレージシステムで処理が実行されます。

PCB

（Printed Circuit Board）
プリント基盤です。このマニュアルでは、チャネルボードやディスクボードなどのボードを指しています。

PCIe チャネルボード

VSP G800、VSP G900、VSP F800、VSP F900、および VSP E990 の DKC に搭載され、チャネルボードボックスと DKC を接続する役割を持ちます。

Quorum ディスク

パスやストレージシステムに障害が発生したときに、global-active device ペアのどちらのボリュームでサーバからの I/O を継続するのかを決めるために使われます。外部ストレージシステムに設置します。

RAID

（Redundant Array of Independent Disks）
独立したディスクを冗長的に配列して管理する技術です。

RAID Manager

コマンドインタフェースでストレージシステムを操作するためのプログラムです。

RCU Target

属性が Initiator のポートと接続するポートが持つ属性です。

Read Hit 率

ストレージシステムの性能を測る指標の 1 つです。ホストがディスクから読み出そうとしていたデータが、どのくらいの頻度でキャッシュメモリに存在していたかを示します。単位はパーセントです。Read Hit 率が高くなるほど、ディスクとキャッシュメモリ間のデータ転送の回数が少なくなるため、処理速度は高くなります。

Real Time OS

RISC プロセッサを制御する基本 OS で、主に、メインタスクや通信タスクのタスクスイッチを制御します。

SIM

（Service Information Message）
ストレージシステムのコントローラがエラーやサービス要求を検出したときに生成されるメッセージです。

SLU

（Subsidiary Logical Unit）
SCSI アーキテクチャモデルである Conglomerate LUN structure に使われる LU です。
SLU は実データを格納した LU であり、DP-VOL またはスナップショットデータ（あるいはスナップショットデータに割り当てられた仮想ボリューム）を SLU として使用できます。
ホストから SLU へのアクセスは、すべて ALU を介して行われます。
vSphere では、Virtual Volume（VVol）と呼ばれます。

SM

（Shared Memory）
詳しくは「シェアドメモリ」を参照してください。

SSL

（Secure Sockets Layer）
インターネット上でデータを安全に転送するためのプロトコルであり、Netscape Communications 社によって最初に開発されました。SSL が有効になっている 2 つのピア（装置）は、秘密鍵と公開鍵を利用して安全な通信セッションを確立します。どちらのピア（装置）も、ランダムに生成された対称キーを利用して、転送されたデータを暗号化します。

SVP

（SuperVisor PC）
ストレージシステムを管理・運用するためのコンピュータです。SVP にインストールされている Storage Navigator からストレージシステムの設定や参照ができます。

T10 PI

（T10 Protection Information）
SCSI で定義された保証コード基準の一つです。T10 PI では、512 バイトごとに 8 バイトの保護情報（PI）を追加して、データの検証に使用します。T10 PI にアプリケーションおよび OS を含めたデータ保護を実現する DIX（Data Integrity Extension）を組み合わせることで、アプリケーションからディスクドライブまでのデータ保護を実現します。

Target

ホストと接続するポートが持つ属性です。

UUID

（User Definable LUN ID）

ホストから論理ボリュームを識別するために、ストレージシステム側で設定する任意の ID です。

VDEV

（Virtual Device）
パリティグループ内にある論理ボリュームのグループです。VDEV は固定サイズのボリューム（FV）と剰余ボリューム（フリースペース）から構成されます。VDEV 内に任意のサイズのボリューム（CV）を作成することもできます。

VLAN

（Virtual LAN）
スイッチの内部で複数のネットワークに分割する機能です（IEEE802.1Q 規定）。

VOLSER

（Volume Serial Number）
個々のボリュームを識別するために割り当てられる番号です。VSN とも呼びます。LDEV 番号や LUN とは無関係です。

VSN

（Volume Serial Number）
個々のボリュームを識別するために割り当てられる番号です。VOLSER とも呼びます。

Write Hit 率

ストレージシステムの性能を測る指標の 1 つです。ホストがディスクへ書き込もうとしていたデータが、どのくらいの頻度でキャッシュメモリに存在していたかを示します。単位はパーセントです。Write Hit 率が高くなるほど、ディスクとキャッシュメモリ間のデータ転送の回数が少なくなるため、処理速度は高くなります。

WWN

（World Wide Name）
ホストバスアダプタの ID です。ストレージ装置を識別するためのもので、実体は 16 桁の 16 進数です。

（ア行）

アクセス属性

ボリュームが読み書き可能になっているか（Read/Write）、読み取り専用になっているか（Read Only）、それとも読み書き禁止になっているか（Protect）どうかを示す属性です。

アクセスパス

ストレージシステム内の、データとコマンドの転送経路です。

エミュレーション

あるハードウェアまたはソフトウェアのシステムが、ほかのハードウェアまたはソフトウェアのシステムと同じ動作をすること（または同等に見えるようにすること）です。一般的には、過去に蓄積されたソフトウェアの資産を役立てるためにエミュレーションの技術が使われます。

（カ行）

外部ストレージシステム

本ストレージシステムに接続されているストレージシステムです。

外部パス

本ストレージシステムと外部ストレージシステムを接続するパスです。外部パスは、外部ボリュームを内部ボリュームとしてマッピングしたときに設定します。複数の外部パスを設定することで、障害やオンラインの保守作業にも対応できます。

外部ボリューム

本ストレージシステムのボリュームとしてマッピングされた、外部ストレージシステム内のボリュームです。

外部ボリュームグループ

マッピングされた外部ボリュームのグループです。外部ボリュームをマッピングするときに、ユーザが外部ボリュームを任意の外部ボリュームグループに登録します。
外部ボリュームグループは、外部ボリュームを管理しやすくするためのグループで、パリティ情報は含みませんが、管理上はパリティグループと同じように取り扱います。

鍵管理サーバ

暗号化鍵を管理するサーバです。本ストレージシステムでは、暗号化鍵を管理するための規格である KMIP（Key Management Interoperability Protocol）に準じた鍵管理サーバに暗号化鍵をバックアップでき、また、鍵管理サーバにバックアップした暗号化鍵から暗号化鍵をリストアできます。

書き込み待ち率

ストレージシステムの性能を測る指標の 1 つです。キャッシュメモリに占める書き込み待ちデータの割合を示します。

鍵ペア

秘密鍵と公開鍵の組み合わせです。この 2 つの暗号鍵は、数学的関係に基づいて決められます。

仮想ボリューム

実体を持たない、仮想的なボリュームです。Dynamic Provisioning、Dynamic Tiering、または active flash で使用する仮想ボリュームを DP-VOL とも呼びます。Thin Image では、仮想ボリュームをセカンダリボリュームとして使用します。

監査ログ

ストレージシステムに対して行われた操作や、受け取ったコマンドの記録です。Syslog サーバへの転送設定をすると、監査ログは常時 Syslog サーバへ転送され、Syslog サーバから監査ログを取得・参照できます。

管理クライアント

Storage Navigator を操作するためのコンピュータです。

キャッシュ

チャネルとドライブの間にあるメモリです。中間バッファとしての役割があります。キャッシュメモリとも呼ばれます。

共用メモリ

詳しくは「シェアドメモリ」を参照してください。

形成コピー

ホスト I/O プロセスとは別に、プライマリボリュームとセカンダリボリュームを同期させるプロセスです。

更新コピー

形成コピー（または初期コピー）が完了したあとで、プライマリボリュームの更新内容をセカンダリボリュームにコピーして、プライマリボリュームとセカンダリボリュームの同期を保持するコピー処理です。

交替パス

チャネルプロセッサの故障などによって LUN パスが利用できなくなったときに、その LUN パスに代わってホスト I/O を引き継ぐ LUN パスです。

コピー系プログラムプロダクト

このストレージシステムに備わっているプログラムのうち、データをコピーするものを指します。ストレージシステム内のボリューム間でコピーするローカルコピーと、異なるストレージシステム間でコピーするリモートコピーがあります。

コマンドデバイス

ホストから RAID Manager コマンドを実行するために、ストレージシステムに設定する論理デバイスです。コマンドデバイスは、ホストから RAID Manager コマンドを受け取り、実行対象の論理デバイスに転送します。
RAID Manager 用のコマンドデバイスは Storage Navigator から設定します。

コマンドデバイスセキュリティ

コマンドデバイスに適用されるセキュリティです。

コンシステンシーグループ

コピー系プログラムプロダクトで作成したペアの集まりです。コンシステンシーグループ ID を指定すれば、コンシステンシーグループに属するすべてのペアに対して、データの整合性を保ちながら、特定の操作を同時に実行できます。

（サ行）

サーバ証明書

サーバと鍵ペアを結び付けるものです。サーバ証明書によって、サーバは自分がサーバであることをクライアントに証明します。これによってサーバとクライアントは SSL を利用して通信できるようになります。サーバ証明書には、自己署名付きの証明書と署名付きの信頼できる証明書の 2 つの種類があります。

サブ画面

Java 実行環境（JRE）で動作する画面で、メイン画面のメニューを選択して起動します。

差分テーブル

コピー系プログラムプロダクトおよび Volume Migration で共有するリソースです。Volume Migration 以外のプログラムプロダクトでは、ペアのプライマリボリュームとセカンダリボリュームのデータに差分があるかどうかを管理するために使用します。Volume Migration では、ボリュームの移動中に、ソースボリュームとターゲットボリュームの差分を管理するために使用します。

自己署名付きの証明書

自分自身で自分用の証明書を生成します。この場合、証明の対象は証明書の発行者と同じになります。ファイアウォールに守られた内部 LAN 上でクライアントとサーバ間の通信が行われている場合は、この証明書でも十分なセキュリティを確保できるかもしれません。

システムプール VOL

プールを構成するプール VOL のうち、1 つのプール VOL がシステムプール VOL として定義されます。システムプール VOL は、プールを作成したとき、またはシステムプール VOL を削除したときに、優先順位に従って自動的に設定されます。なお、システムプール VOL で使用可能な容量は、管理領域の容量を差し引いた容量になります。管理領域とは、プールを使用するプログラムプロダクトの制御情報を格納する領域です。

システムプールボリューム

プールを構成するプールボリュームのうち、1 つのプールボリュームがシステムプールボリュームとして定義されます。システムプールボリュームは、プールを作成したとき、またはシステムプールボリュームを削除したときに、優先順位に従って自動的に設定されます。なお、システムプールボリュームで使用可能な容量は、管理領域の容量を差し引いた容量になります。管理領域とは、プールを使用するプログラムプロダクトの制御情報を格納する領域です。

ジャーナルボリューム

Universal Replicator の用語で、プライマリボリュームからセカンダリボリュームにコピーするデータを一時的に格納しておくためのボリュームのことです。ジャーナルボリュームには、プライマリボリュームと関連づけられているマスタジャーナルボリューム、およびセカンダリボリュームと関連づけられているリストアジャーナルボリュームとがあります。

シュレッディング

ダミーデータを繰り返し上書きすることで、ボリューム内のデータを消去する処理です。

初期コピー

新規にコピーペアを作成すると、初期コピーが開始されます。初期コピーでは、プライマリボリュームのデータがすべて相手のセカンダリボリュームにコピーされます。初期コピー中も、ホストサーバからプライマリボリュームに対する Read／Write などの I/O 操作は続行できます。

署名付きの信頼できる証明書

証明書発行要求を生成したあとで、信頼できる CA 局に送付して署名してもらいます。CA 局の例としては VeriSign 社があります。

シリアル番号

ストレージシステムに一意に付けられたシリアル番号（装置製番）です。

スナップショットグループ

Thin Image で作成した複数のペアの集まりです。複数のペアに対して同じ操作を実行できます。

スナップショットデータ

Thin Image の用語で、更新直前のプライマリボリュームのデータを指します。Thin Image を使用すると、プライマリボリュームに格納されているデータのうち、更新される部分の更新前のデータだけが、スナップショットデータとしてプールにコピーされます。

正 VOL、正ボリューム

詳しくは「プライマリボリューム」を参照してください。

正サイト

通常時に、業務（アプリケーション）を実行するサイトを指します。

セカンダリボリューム

ペアとして設定された 2 つのボリュームのうち、コピー先のボリュームを指します。なお、プライマリボリュームとペアを組んでいるボリュームをセカンダリボリュームと呼びますが、Thin Image では、セカンダリボリューム（仮想ボリューム）ではなく、プールにデータがコピーされます。

センス情報

エラーの検出によってペアがサスペンドされた場合に、正サイトまたは副サイトのストレージシステムが、適切なホストに送信する情報です。ユニットチェックの状況が含まれ、災害復旧に使用されます。

ソースボリューム

Volume Migration の用語で、別のパリティグループへと移動するボリュームを指します。

（タ行）

ターゲットボリューム

Volume Migration の用語で、ボリュームの移動先となる領域を指します。

ダンプツール

SVP 上で使用するツール（ダンプ採取用バッチファイル）です。障害が発生した場合は、SVP に障害解析用のダンプファイルをダウンロードできます。

チャネルボード

ストレージシステムに内蔵されているアダプタの一種で、ホストコマンドを処理してデータ転送を制御します。

チャネルボードボックス

VSP G800、VSP G900、VSP F800、VSP F900、および VSP E990 の DKC に接続されるチャネルボードの搭載数を拡張する筐体です。

重複排除用システムデータボリューム（データストア）

容量削減の設定が［重複排除および圧縮］の仮想ボリュームが関連づけられているプール内で、重複データを格納するためのボリュームです。

重複排除用システムデータボリューム（フィンガープリント）

容量削減の設定が［重複排除および圧縮］の仮想ボリュームが関連づけられているプール内で、重複排除データの制御情報を格納するためのボリュームです。

ディスクボード

ストレージシステムに内蔵されているアダプタの一種で、キャッシュとドライブの間のデータ転送を制御します。

デジタル証明書

詳しくは「サーバ証明書」を参照してください。

転送レート

ストレージシステムの性能を測る指標の 1 つです。1 秒間にディスクへ転送されたデータの大きさを示します。

同期コピー

ホストからプライマリボリュームに書き込みがあった場合に、リアルタイムにセカンダリボリュームにデータを反映する方式のコピーです。ボリューム単位のリアルタイムデータバックアップができます。優先度の高いデータのバックアップ、複写、および移動業務に適しています。

トポロジ

デバイスの接続形態です。Fabric、FC-AL、および Point-to-point の 3 種類があります。

ドライブボックス

各種ドライブを搭載するためのシャーシ（筐体）です。

（ナ行）

内部ボリューム

本ストレージシステムが管理するボリュームを指します。

（ハ行）

パリティグループ

同じ容量を持ち、1 つのデータグループとして扱われる一連のドライブを指します。パリティグループには、ユーザデータとパリティ情報の両方が格納されているため、そのグループ内の 1 つまたは複数のドライブが利用できない場合にも、ユーザデータにはアクセスできます。
場合によっては、パリティグループを RAID グループ、ECC グループ、またはディスクアレイグループと呼ぶことがあります。

非対称アクセス

global-active device でのクロスパス構成など、サーバとストレージシステムを複数の交替パスで接続している場合で、ALUA が有効のときに、優先して I/O を受け付けるパスを定義する方法です。

非同期コピー

ホストから書き込み要求があった場合に、プライマリボリュームへの書き込み処理とは非同期に、セカンダリボリュームにデータを反映する方式のコピーです。複数のボリュームや複数のストレージシステムにわたる大量のデータに対して、災害リカバリを可能にします。

ピントラック

（pinned track）
物理ドライブ障害などによって読み込みや書き込みができないトラックです。固定トラックとも呼びます。

ファイバチャネル

光ケーブルまたは銅線ケーブルによるシリアル伝送です。ファイバチャネルで接続された RAID のディスクは、ホストからは SCSI のディスクとして認識されます。

ファイバチャネルアダプタ

（Fibre Channel Adapter）
ファイバチャネルを制御します。

プール

プールボリューム（プール VOL）を登録する領域です。Dynamic Provisioning、Dynamic Tiering、active flash、および Thin Image がプールを使用します。

プールボリューム、プール VOL

プールに登録されているボリュームです。Dynamic Provisioning、Dynamic Tiering、および active flash ではプールボリュームに通常のデータを格納し、Thin Image ではスナップショットデータをプールボリュームに格納します。

副 VOL、副ボリューム

詳しくは「セカンダリボリューム」を参照してください。

副サイト

主に障害時に、業務（アプリケーション）を正サイトから切り替えて実行するサイトを指します。

プライマリボリューム

ペアとして設定された 2 つのボリュームのうち、コピー元のボリュームを指します。

フラッシュメモリ

各プロセッサに搭載され、ソフトウェアを格納している不揮発性のメモリです。

分散パリティグループ

複数のパリティグループを連結させた集合体です。分散パリティグループを利用すると、ボリュームが複数のドライブにわたるようになるので、データのアクセス（特にシーケンシャルアクセス）にかかる時間が短縮されます。

ペアテーブル

ペアまたは移動プランを管理するための制御情報を格納するテーブルです。

ページ

DP の領域を管理する単位です。1 ページは 42MB です。

ホストグループ

ストレージシステムの同じポートに接続し、同じプラットフォーム上で稼働しているホストの集まりのことです。あるホストからストレージシステムに接続するには、ホストをホストグループに登録し、ホストグループを LDEV に結び付けます。この結び付ける操作のことを、LUN パスを追加するとも呼びます。

ホストグループ 0（ゼロ）

「00」という番号が付いているホストグループを指します。

ホストバスアダプタ

オープンシステム用ホストに内蔵されているアダプタで、ホストとストレージシステムを接続するポートの役割を果たします。それぞれのホストバスアダプタには、16 桁の 16 進数による ID が付いています。ホストバスアダプタに付いている ID を WWN（Worldwide Name）と呼びます。

ホストモード

オープンシステム用ホストのプラットフォーム（通常は OS）を示すモードです。

（マ行）

マイグレーションボリューム

HUS VM などの異なる機種のストレージシステムからデータを移行させる場合に使用するボリュームです。

マッピング

本ストレージシステムから外部ボリュームを操作するために必要な管理番号を、外部ボリュームに割り当てることです。

メイン画面

Storage Navigator にログイン後、最初に表示される画面です。

（ラ行）

リザーブボリューム

ShadowImage のセカンダリボリュームに使用するために確保されているボリューム、または Volume Migration の移動プランの移動先として確保されているボリュームを指します。

リソースグループ

ストレージシステムのリソースを割り当てたグループを指します。リソースグループに割り当てられるリソースは、LDEV 番号、パリティグループ、外部ボリューム、ポートおよびホストグループ番号です。

リモートコマンドデバイス

外部ストレージシステムのコマンドデバイスを、本ストレージシステムの内部ボリュームとしてマッピングしたものです。リモートコマンドデバイスに対して RAID Manager コマンドを発行すると、外部ストレージシステムのコマンドデバイスに RAID Manager コマンドを発行でき、外部ストレージシステムのペアなどを操作できます。

リモートストレージシステム

ローカルストレージシステムと接続しているストレージシステムを指します。

リモートパス

リモートコピー実行時に、遠隔地にあるストレージシステム同士を接続するパスです。

レスポンスタイム

モニタリング期間内での平均の応答時間。あるいは、エクスポートツールまたはエクスポートツール 2 で指定した期間内でのサンプリング期間ごとの平均の応答時間。単位は、各モニタリング項目によって異なります。

ローカルストレージシステム

管理クライアントを接続しているストレージシステムを指します。

索引

ひ

へ

り

る