NEC

iStorage V10e/V100/V300

Encryption License Key
ユーザガイド

iStorage

IV-UG-012-003-06

著作権

免責事項

商標類

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

2024 年 10 月（IV-UG-012）

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

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。

- iStorage V10e（iStorage V シリーズ）
- iStorage V100（iStorage V シリーズ）
- iStorage V300（iStorage V シリーズ）

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。

- iStorage V10e の場合

  88-08-14-XX 以降

- iStorage V100/V300 の場合

  93-07-24-XX 以降

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。

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
- 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、『HA 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。

Storage Navigator の画面や基本操作に関する注意事項については、『HA Device Manager - Storage Navigator ユーザガイド』を参照してください。

マニュアルに掲載されている機能、ソフトウェアについて

以下の機能、およびソフトウェアは、ストレージシステムの一部のモデルにおいてサポートしていません。サポートしていないストレージシステムを利用する場合、マニュアルに掲載されている機能、およびソフトウェアに関する記述は無効となります。

機能・ソフトウェア	サポートしていないストレージシステム
Active Mirror	iStorage V10e
Asynchronous Replication	
Dynamic Tiering	
HA Device Manager	
Realtime Tiering	
Synchronous Replication	

第 1 章
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。

- iStorage V10e の場合：

  暗号化に対応したコントローラ（ECTL）

- iStorage V100、iStorage V300 の場合：

  暗号化に対応したコントローラ（ECTL）

  暗号化に対応したディスクボード（EDKB（SAS インタフェースのドライブボックスを接続する場合に使用））

メモ

- iStorage V100、iStorage V300 に SAS インタフェースのドライブボックスを接続する場合、ドライブボックスには SSD を搭載してください。SAS の HDD は搭載できません。
- iStorage V100、iStorage V300（ファームウェアバージョン 93-07-24-XX 以降）は、NVMe インタフェースのドライブボックスを接続できます。この場合、NVMe ドライブ用のディスクボード（DKBN）を搭載する必要があります。

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 Storage Navigator の画面、もしくは 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、『HA Device Manager - Storage Navigator ユーザガイド』を参照してください。

なお、iStorage V シリーズは鍵管理サーバを用いた鍵管理機能はサポートしておりません。鍵管理は利用者自身が Storage Navigator、もしくは REST API を用いた鍵管理を行ってください。

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	○	○
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	○	○
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	○	○
未使用暗号化鍵の削除および生成	○	○
認証用鍵の更新	○	×
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	○	○

凡例

○：操作できる

×：操作できない

メモ

- 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
iStorage V10e、iStorage V100、iStorage V300	FIPS 140-2 Level 1 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

関連リンク

参照先トピック

データの暗号化（8 ページ）

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 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
iStorage V10e	372	4	1,024
iStorage V100	552	8	4,096
iStorage V300	552	12	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 単位に 2 つ

  iStorage V10e、iStorage V100 の場合は、ECTL 単位に 2 つ

  iStorage V300 の場合は、ECTL 単位に 4 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 Storage Navigator、もしくは 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
iStorage V10e	1,024
iStorage V100、iStorage V300	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
iStorage V10e	1,022
iStorage V100、iStorage V300	EDKB が搭載されていない場合：4,096 EDKB が合計で 2 つ搭載されている場合：4,094

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。

関連リンク

参照先トピック

暗号化鍵の使用（5 ページ）
暗号化鍵のバックアップ機能（6 ページ）
暗号化鍵のリストア機能（7 ページ）

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。
ドライブの保守閉塞	ドライブあたり 1 個	閉塞するドライブ数分必要となります。

ディスクボードに関連する保守操作時

保守操作	使用される鍵数	備考
ディスクボードの増設時	EDKB あたり 3 個	増設するディスクボード（EDKB）数分必要となります。
ディスクボードのリプレース時	EDKB あたり 3 個	リプレースするディスクボード（EDKB）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

保守操作	使用される鍵数			備考
	iStorage V10e	iStorage V100	iStorage V300	
コントローラリプレース時	コントローラあたり 3 個	コントローラあたり 2 個	コントローラあたり 4 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	暗号モジュール	使用される鍵数			備考
		iStorage V10e	iStorage V100	iStorage V300	
認証用鍵の更新時	コントローラあたり	2 個	2 個	4 個	システム内に実装されている全コントローラ(ECTL)/ディスクボード(EDKB)の合
	ディスクボードあたり	-	2 個	2 個	

セキュリティ運用操作	暗号モジュール	使用される鍵数			備考
		iStorage V10e	iStorage V100	iStorage V300	
					計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。

関連リンク

参照先トピック

暗号化鍵の管理機能（4 ページ）

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。

関連リンク

参照先トピック

暗号化鍵の管理機能（4 ページ）
暗号化鍵の一次バックアップと二次バックアップ（6 ページ）

1.3.2.1　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、Storage Navigator、もしくは 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。

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、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。

関連リンク

参照先トピック

暗号化鍵のバックアップ機能（6 ページ）

参照先トピック

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（18 ページ）
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（19 ページ）

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があります。

関連リンク

参照先トピック

暗号化鍵の管理機能（4 ページ）

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（29 ページ）

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。

関連リンク

参照先トピック

データの暗号化（8 ページ）
暗号化の解除（9 ページ）
データ暗号化鍵の変更（10 ページ）

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、次のロールが必要です。

- セキュリティ管理者（参照・編集）ロール
- ストレージ管理者（プロビジョニング）ロール※1
- 保守（ユーザ）ロール、または保守（ベンダ専用）ロール※2

注※1

対象の LDEV を閉塞、またはフォーマットを同時にする場合に必要なロールです。

注※2

対象の LDEV がプールボリュームで閉塞、またはフォーマットを同時にする場合に必要なロールです。

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 Local Replication や Synchronous

Replication 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。

関連リンク

参照先トピック

データの暗号化機能（8 ページ）
暗号化を有効にする（20 ページ）

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、次のロールが必要です。

- セキュリティ管理者（参照・編集）ロール
- ストレージ管理者（プロビジョニング）ロール※1
- 保守（ユーザ）ロール、または保守（ベンダ専用）ロール※2

注※1

対象の LDEV を閉塞、またはフォーマットを同時にする場合に必要なロールです。

注※2

対象の LDEV がプールボリュームで閉塞、またはフォーマットを同時にする場合に必要なロールです。

関連リンク

参照先トピック

データの暗号化機能（8 ページ）
暗号化を無効にする（25 ページ）

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 Local Replication や Synchronous Replication 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。

関連リンク

参照先トピック

データの暗号化機能（8 ページ）

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。

第 2 章
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
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。
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。
暗号化に対応したディスクボード(EDKB)および暗号化に対応したコントローラ(ECTL)	• iStorage V100、iStorage V300 に NVMe ドライブボックスを接続する場合（ファームウェアバージョン 93-07-24-XX 以降サポート） コントローラが暗号化に対応していることが必要です。 • iStorage V100、iStorage V300 に SAS ドライブボックスを接続する場合 コントローラとシステム内のすべてのディスクボードが暗号化に対応していることが必要です。

2.2　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。

2.2.1　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。

2.2.2　Encryption License Key と Snapshot 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。

2.2.3　Encryption License Key と Asynchronous Replication 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。

2.2.4　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。

2.2.5　Encryption License Key と Dynamic Provisioning、Dynamic Tiering、および Realtime Tiering 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。

2.2.6　Encryption License Key と dedupe and compression の併用

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。また、重複排除用システムデータボリュームがある場合は、重複データ初期化も必要です。

2.3　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. 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、『HA Device Manager - Storage Navigator ユーザガイド』を参照してください。

2.4　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。

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。

第 3 章
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。

関連リンク

参照先トピック
暗号化環境を設定する（14 ページ）

3.1.1　暗号化環境を設定する

⚠ 注意

鍵管理サーバは使用できません。鍵管理サーバの指定は必ず[無効]に設定してください。

⚠ 注意

次の場合は、「4.2　暗号化環境設定編集のトラブルシューティングの流れ（40 ページ）」に従って対処してください。

- 暗号化環境の設定に失敗した。
- 誤って［鍵管理サーバ］を「有効」に設定した。

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。

   HA Device Manager 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. 画面の右上に表示されている［最終更新日時］に、現在の時間が表示されていることを確認します。現在の時間が表示されていない場合は、操作手順 3. に進んでください。現在の時間が表示されている場合は、操作手順 5. に進んでください。

   メモ

   ［最終更新日時］に現在の時間が表示されていない状態で暗号化環境を設定すると、ハードウェアが閉塞する場合があります。このため、［最終更新日時］に現在の時間を反映します。

3. ［ファイル］-［すべて更新］を実行します。
4. 再度［暗号化鍵］画面を表示して、［最終更新日時］に現在の時間が表示されていることを確認します。現在の時間が表示されていない場合は、操作手順 3. から実行してください。
5. ［ストレージシステム］ツリーから［タスク］を選択します。

   暗号化環境を設定するタスクは、［タスクタイプ］に［暗号化環境設定編集］と表示されます。［暗号化環境設定編集］の［状態］が［実行中］または［実行待ち］と表示されている場合はタスクが実行中です。この場合は、タスクが完了するまで待ちます。

   メモ

   暗号化環境を設定するタスクを同時に複数実行すると、ハードウェアが閉塞する場合があります。タスクの重複を避けるため、先行しているタスクの完了を待ちます。

6. 再度［暗号化鍵］画面を表示します。
7. ［暗号化鍵］タブを選択します。
8. 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。
   - 画面上部の［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］ - ［暗号化環境設定編集］を選択します。
9. ［鍵管理サーバ］は［無効］を選択します。
10. ［完了］をクリックします。

    ［設定確認］画面が表示されます。

11. 設定内容を確認し、［タスク名］にタスク名を入力します。
12. ［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。

13. ［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。

関連リンク

参照先トピック

暗号化環境設定編集ウィザード（44 ページ）

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
iStorage V10e	1,024
iStorage V100、iStorage V300	4,096

暗号化鍵はストレージシステム内に作成されます。暗号化鍵の作成時には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。

   HA Device Manager 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］ - ［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。

メモ

［暗号化鍵数］には、作成可能な最大の暗号化鍵数を指定することを推奨します。

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. ［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。

関連リンク

参照先トピック

鍵生成ウィザード（46 ページ）

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。

［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。

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。

関連リンク

参照先トピック

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（18 ページ）

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（19 ページ）

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。

   HA Device Manager 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］ - ［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。

関連リンク

参照先トピック

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（47 ページ）
暗号化鍵の一次バックアップと二次バックアップ（6 ページ）
暗号化鍵のバックアップ（17 ページ）

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。

   HA Device Manager 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］ - ［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。

関連リンク

参照先トピック

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）（49 ページ）
暗号化鍵の一次バックアップと二次バックアップ（6 ページ）
暗号化鍵のバックアップ（17 ページ）

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（21 ページ）」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）（23 ページ）」を参照してください。

関連リンク

参照先トピック

データの暗号化（8 ページ）

データの暗号化を有効にする（21 ページ）
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）（23 ページ）

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

- 必要なロールを次に示します。
  - セキュリティ管理者（参照・編集）ロール
  - ストレージ管理者（プロビジョニング）ロール※

注※

対象の LDEV を閉塞、またはフォーマットを同時にする場合に必要なロールです。

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。

   HA Device Manager 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 が存在する場合は、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、［他のタスク］ - ［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。

   タスクの実行時にエラーが発生した場合、 パリティグループのフォーマットを実施して回復してください。パリティグループをフォーマットするには、［パリティグループ］タブで、［パリティグループフォーマット］をクリックします。手順詳細は、『システム構築ガイド』を参照してください。

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。

関連リンク

参照先トピック

暗号化編集ウィザード（57 ページ）
暗号化を有効にする（20 ページ）
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）（23 ページ）

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）

プールボリュームが含まれ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

- 必要なロールを次に示します。
  - セキュリティ管理者（参照・編集）ロール
  - ストレージ管理者（プロビジョニング）ロール※1
  - 保守（ユーザ）ロール、または保守（ベンダ専用）ロール※2

注※1

対象の LDEV を閉塞、またはフォーマットを同時にする場合に必要なロールです。

注※2

対象の LDEV がプールボリュームで閉塞、またはフォーマットを同時にする場合に必要なロールです。

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. ［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。

⚠ 注意

重複排除用システムデータボリュームを閉塞させる場合は、当該プール内の［重複排除データ］が［有効］のすべての仮想ボリュームを閉塞させてから実行してください。

この手順を守らなかった場合は、重複排除用システムデータボリュームを閉塞できません。

4. 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。

   対象プールに所属するすべてのパリティグループに対して、「3.4.1　データの暗号化を有効にする（21 ページ）」に示す手順を実施します。

5. 重複排除用システムデータボリュームが無い場合は、手順 7 へ進みます。

   重複排除用システムデータボリュームが有る場合は、次のどちらかの方法で［重複データ初期化］画面を表示します。

   - ［他のタスク］ - ［重複データ初期化］をクリックします。
   - ［アクション］メニューから［プール管理］ - ［重複データ初期化］を選択します。

6. ［適用］をクリックします。

   タスクが登録され、［「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］画面が表示されます。

7. ［仮想ボリューム］タブのテーブルの［状態］欄で、［Blocked］となっているすべての LDEV をフォーマットします。

   ⚠ 注意

   ［重複排除データ］が［有効］の仮想ボリュームをフォーマットする場合は、当該プール内の重複排除用システムデータボリューム（データストア）を LDEV フォーマットしてから実行してください。

   この手順を守らなかった場合は、［重複排除データ］が［有効］の仮想ボリュームをフォーマットできません。

関連リンク

参照先トピック

暗号化を有効にする（20 ページ）
データの暗号化を有効にする（21 ページ）

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。

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（25 ページ）」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）（27 ページ）」を参照してください。

関連リンク

参照先トピック

暗号化の解除（9 ページ）

データの暗号化を無効にする（25 ページ）

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）（27 ページ）

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

- 必要なロールを次に示します。
  - セキュリティ管理者（参照・編集）ロール
  - ストレージ管理者（プロビジョニング）ロール※

注※

対象の LDEV を閉塞、またはフォーマットを同時にする場合に必要なロールです。

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。

   HA Device Manager 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 が存在する場合は、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、［他のタスク］ - ［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。

   タスクの実行時にエラーが発生した場合、パリティグループのフォーマットを実施して回復してください。パリティグループをフォーマットするには、［パリティグループ］タブで、［パリティグループフォーマット］をクリックします。手順詳細は、『システム構築ガイド』を参照してください。

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。

関連リンク

参照先トピック

暗号化編集ウィザード（57 ページ）
暗号化を無効にする（25 ページ）
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）（27 ページ）

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）

プールボリュームが含まれ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

- 必要なロールを次に示します。
  - セキュリティ管理者（参照・編集）ロール
  - ストレージ管理者（プロビジョニング）ロール※1
  - 保守（ユーザ）ロール、または保守（ベンダ専用）ロール※2

注※1

対象の LDEV を閉塞、またはフォーマットを同時にする場合に必要なロールです。

注※2

対象の LDEV がプールボリュームで閉塞、またはフォーマットを同時にする場合に必要なロールです。

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. ［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。

   ⚠ 注意

   重複排除用システムデータボリュームを閉塞させる場合は、当該プール内の［重複排除データ］が［有効］のすべての仮想ボリュームを閉塞させてから実行してください。

   この手順を守らなかった場合は、重複排除用システムデータボリュームを閉塞できません。
4. 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。

   対象プールに所属するすべてのパリティグループに対して、「3.5.1　データの暗号化を無効にする（25 ページ）」に示す手順を実施します。
5. 重複排除用システムデータボリュームが無い場合は、手順 7 へ進みます。

   重複排除用システムデータボリュームが有る場合は、次のどちらかの方法で［重複データ初期化］画面を表示します。
   - ［他のタスク］ - ［重複データ初期化］をクリックします。
   - ［アクション］メニューから［プール管理］ - ［重複データ初期化］を選択します。
6. ［適用］をクリックします。

   タスクが登録され、［「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］画面が表示されます。
7. ［仮想ボリューム］テーブルの［状態］欄で、［Blocked］となっているすべての LDEV をフォーマットします。

   ⚠ 注意

   ［重複排除データ］が［有効］の仮想ボリュームをフォーマットする場合は、当該プール内の重複排除用システムデータボリューム（データストア）を LDEV フォーマットしてから実行してください。

   この手順を守らなかった場合は、［重複排除データ］が［有効］の仮想ボリュームをフォーマットできません。

関連リンク

参照先トピック

暗号化を無効にする（25 ページ）
データの暗号化を無効にする（25 ページ）

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、鍵情報を紛失した暗号化鍵に対して一括して実施されます。ただし、ドライブやディスクボード（DKB）の保守、パリティグループの暗号化解除、認証用鍵の更新などのときに、削除された暗号化鍵、あるいは手動操作で明示的に削除した未使用鍵はリストアされません。

⚠ 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があります。

関連リンク

参照先トピック

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（29 ページ）

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。

   HA Device Manager 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］ - ［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。

関連リンク

参照先トピック

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）（52 ページ）
暗号化鍵のリストア機能（7 ページ）
暗号化鍵のリストア（29 ページ）

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、鍵情報を紛失した暗号化鍵に対して一括して実施されます。ただし、ドライブやディスクボード（DKB）の保守、パリティグループの暗号化解除、認証用鍵の更新などのときに、削除された暗号化鍵、あるいは手動操作で明示的に削除した未使用鍵はリストアされません。

⚠ 注意

最新でない暗号化鍵をリストアした場合は、正しくデータを読み出せなくなる場合があります。その場合、ドライブ、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）が閉塞する可能性があります。

⚠ 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があります。

関連リンク

参照先トピック

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（32 ページ）

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。

   HA Device Manager 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］ - ［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。

関連リンク

参照先トピック

暗号化鍵のリストア機能（7 ページ）
暗号化鍵の強制リストア（31 ページ）
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）（53 ページ）

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。

⚠ 注意

暗号化鍵の削除後は、「3.2　暗号化鍵を作成する（16 ページ）」の手順に従い、作成可能な最大数の暗号化鍵の生成を推奨します。

関連リンク

参照先トピック

暗号化鍵を作成する（16 ページ）
ストレージシステム内の暗号化鍵を削除する（33 ページ）

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。

   HA Device Manager 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］ - ［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。

関連リンク

参照先トピック

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）（55 ページ）
暗号化鍵の削除（33 ページ）

3.9　暗号化鍵の更新

暗号化鍵の更新について説明します。

関連リンク

参照先トピック

認証用鍵を更新する（35 ページ）

3.9.1　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。

   HA Device Manager 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］ - ［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。

関連リンク

参照先トピック

［認証用鍵更新］画面（60 ページ）
暗号化鍵の更新（34 ページ）

3.10　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。

   HA Device Manager 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。
   - 画面上部の［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。

関連リンク

参照先トピック

暗号化環境設定編集ウィザード（44 ページ）

第 4 章
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 操作時のトラブルと対策

Encryption License Key の操作中に発生したトラブル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 に関する一般的なトラブルと対策については、マニュアル『HA Device Manager - Storage Navigator ユーザガイド』を参照してください。

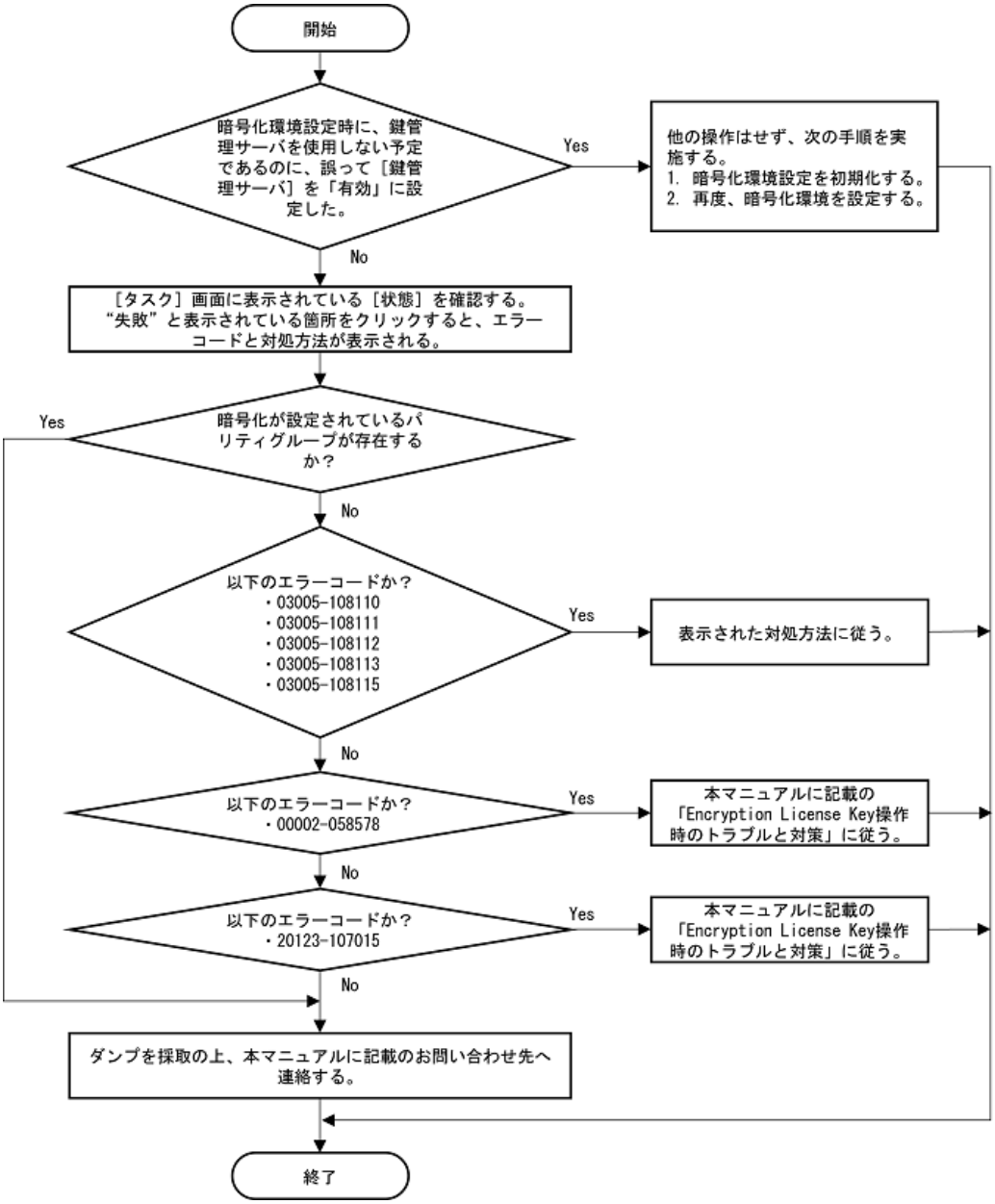
トラブル	対策
暗号化鍵の操作（バックアップ／リストア）ができない。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • セキュリティ管理者（参照・編集）ロールが割り当てられているか • 最新の暗号化鍵をリストアしているか、二次バックアップ後に暗号化鍵が変更されていないか
暗号化鍵を作成／削除できない。	次のことを確認してください。 • Encryption License Key プログラムプロダクトのライセンスが有効であるか、期限切れになっていないか • セキュリティ管理者（参照・編集）ロールが割り当てられているか
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。
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、パリティグループのフォーマットを実施して回復してください。パリティグループをフォーマットするには、[ストレージシステム] ツリーから [パリティグループ] を選択して、[パリティグループ] タブで [パリティグループフォーマット] をクリックします。手順詳細は、『システム構築ガイド』を参照してください。

トラブル	対策
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。
暗号化環境設定が（20123-107015）で失敗した。	以下の対策を実施してください。 1. Storage Navigator、ストレージ本体をつなぐユーザ LAN の通信に不具合があります。ネットワークエラーの対処をしてください。 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。
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、暗号化に対応したコントローラ、もしくは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。
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。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. コントローラ（ECTL）およびディスクボード（EDKB、DKBN）が閉塞状態であるか確認してください。 2. 閉塞状態である場合： 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。 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：

トラブル	対策
	Storage Navigator、もしくは 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、コントローラ（ECTL）およびディスクボード（EDKB、DKBN）の回復を依頼してください。
暗号化環境設定編集ウィザードで、［暗号化環境設定初期化］以外の項目が非活性になっている。	暗号化環境の設定が失敗しています。［タスク］画面からエラーを確認し、メッセージに従って対処してください。

4.2　暗号化環境設定編集のトラブルシューティングの流れ

暗号化環境の設定に失敗した場合の対策の流れを示します。



4.3　お問い合わせ先

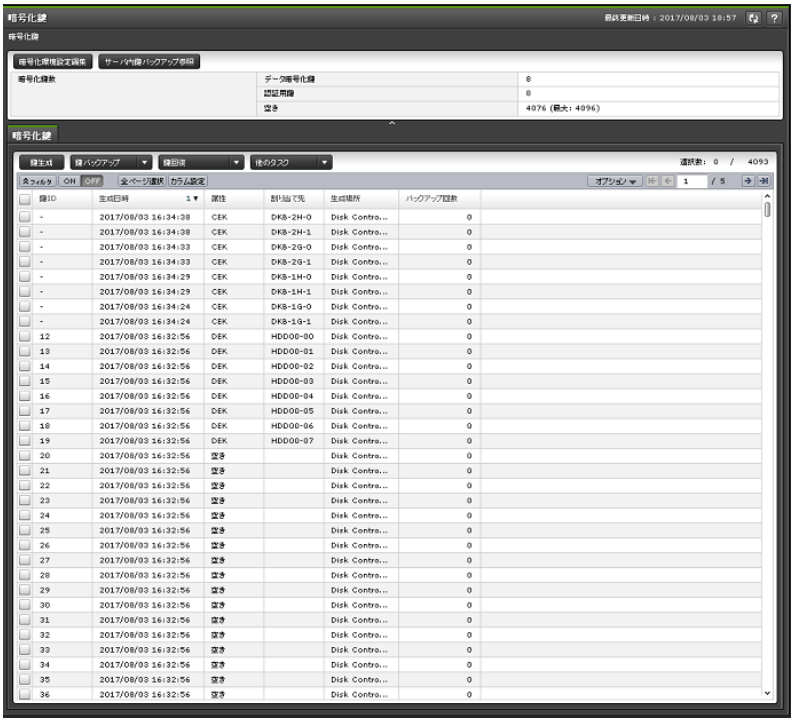
- PP サポートサービスにお問い合わせください。

付録 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、『HA 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（42 ページ）
- ［暗号化鍵］タブ（43 ページ）

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	選択できません。

- 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。
- 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。 **注意：**[サーバへ]を選択しないでください。
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。 **注意：**[サーバへ]を選択しないでください。
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※	選択しないでください。
鍵削除※	［鍵削除］画面が表示されます。
鍵暗号化鍵再取得※	選択しないでください。
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。
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。

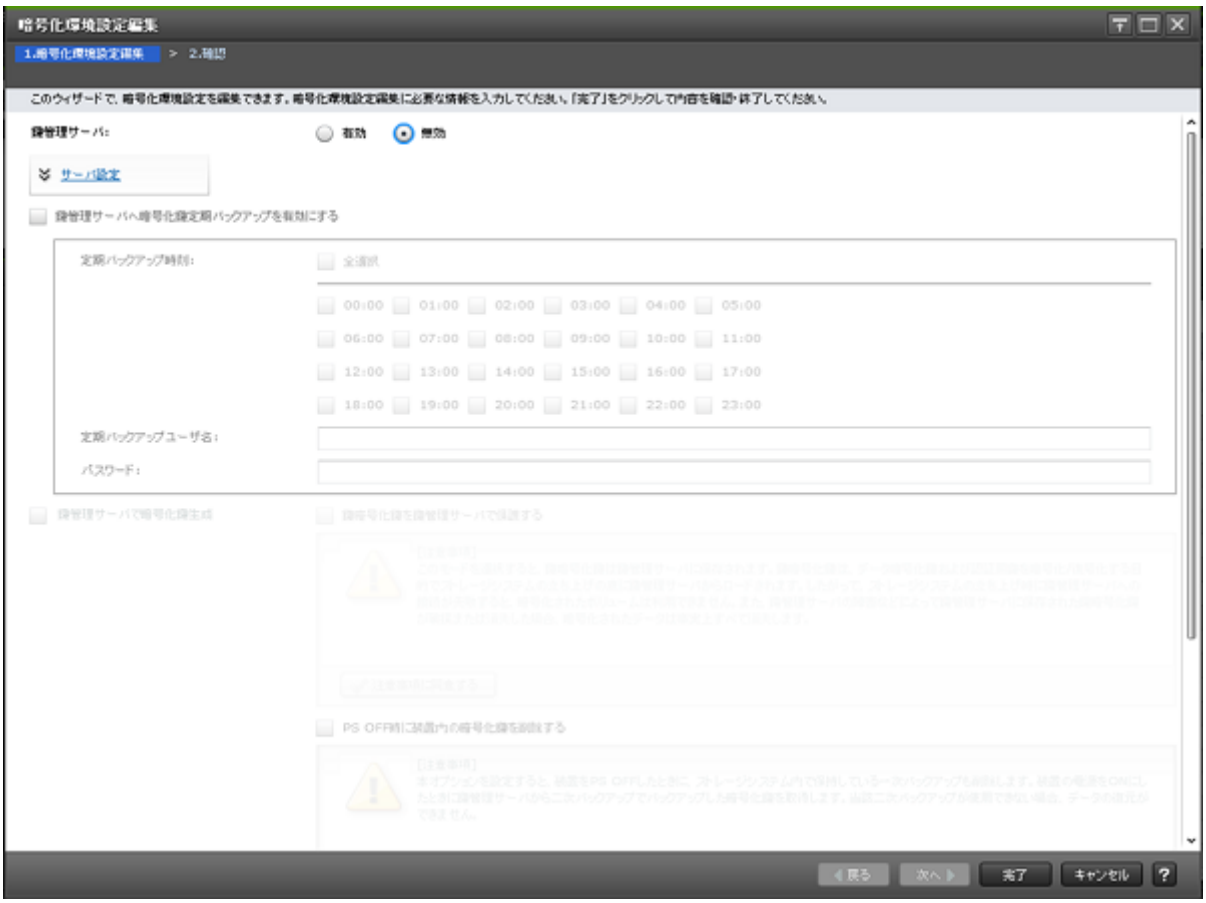
A.2 暗号化環境設定編集ウィザード

関連リンク

参照先トピック

暗号化環境を設定する（14 ページ）
暗号化環境設定を初期化する（36 ページ）
［暗号化環境設定編集］画面（44 ページ）
［設定確認］画面（45 ページ）

A.2.1 ［暗号化環境設定編集］画面



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。無効を選択してください。

項目	説明
	注意：鍵管理サーバは使用できません。鍵管理サーバの指定は必ず[無効]に設定してください。
暗号化環境設定初期化	暗号化環境設定を初期化します。

関連リンク

参照先トピック

暗号化環境設定編集ウィザード（44 ページ）

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。 - 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。 以下の項目は利用いたしません。 • ホスト名： • ポート番号： • タイムアウト（秒）： • リトライ間隔（秒）： • リトライ回数： • クライアント証明書ファイル名： • パスワード： • ルート証明書ファイル名：
セカンダリサーバ	本項目は利用いたしません。

関連リンク

参照先トピック

暗号化環境設定編集ウィザード（44 ページ）

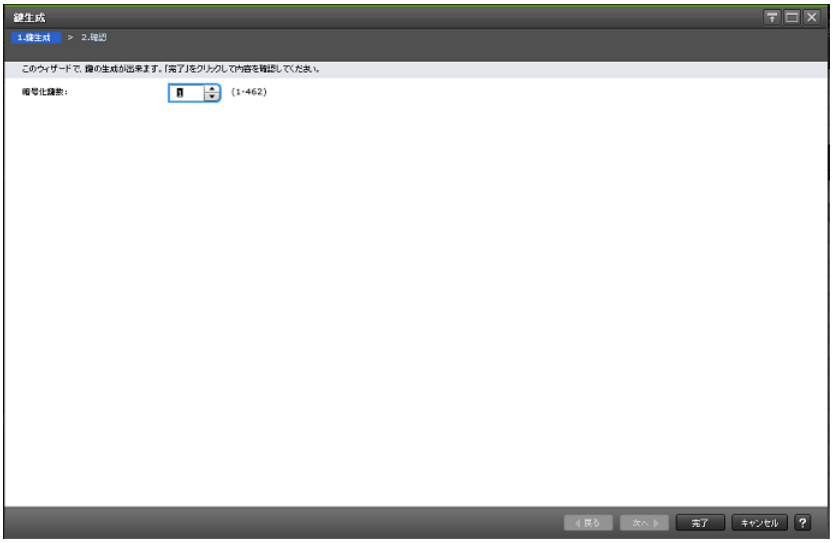
A.3 鍵生成ウィザード

関連リンク

参照先トピック

暗号化鍵を作成する（16 ページ）
［鍵生成］画面（46 ページ）
［設定確認］画面（47 ページ）

A.3.1 ［鍵生成］画面



情報設定エリア

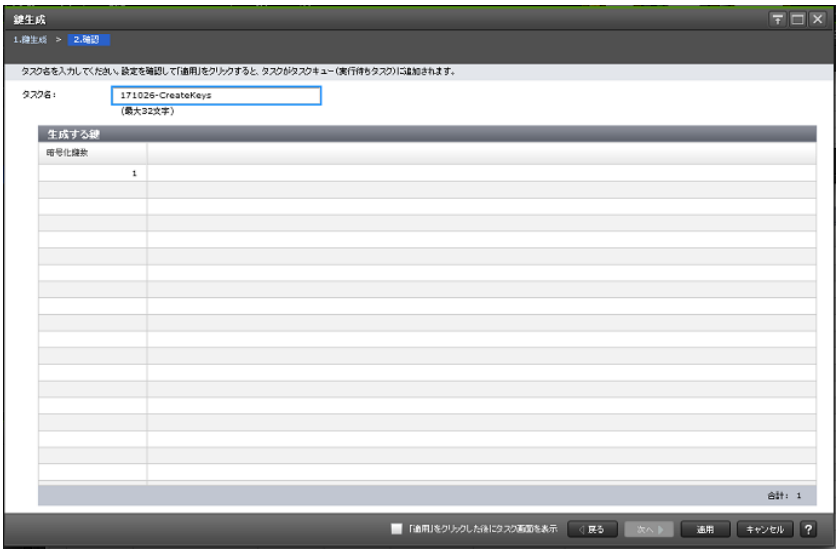
項目	説明
暗号化鍵数	生成する暗号化鍵の数を指定します。画面には(1-現在作成可能な暗号化鍵最大数(上限数－生成済の暗号化鍵数))が表示されます。

関連リンク

参照先トピック

鍵生成ウィザード（46 ページ）

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	生成する暗号化鍵の数を表示します

関連リンク

参照先トピック

鍵生成ウィザード（46 ページ）

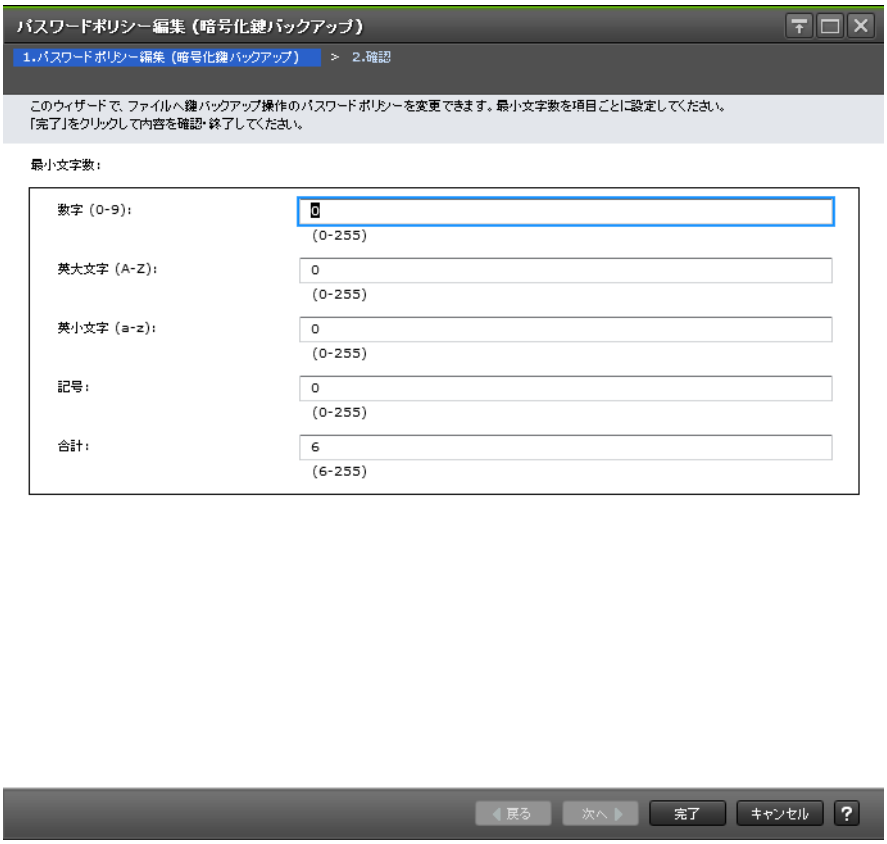
A.4 パスワードポリシー編集（暗号化鍵バックアップ）ウィザード

関連リンク

参照先トピック

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（18 ページ）
［パスワードポリシー編集（暗号化鍵バックアップ）］画面（48 ページ）
［設定確認］画面（49 ページ）

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

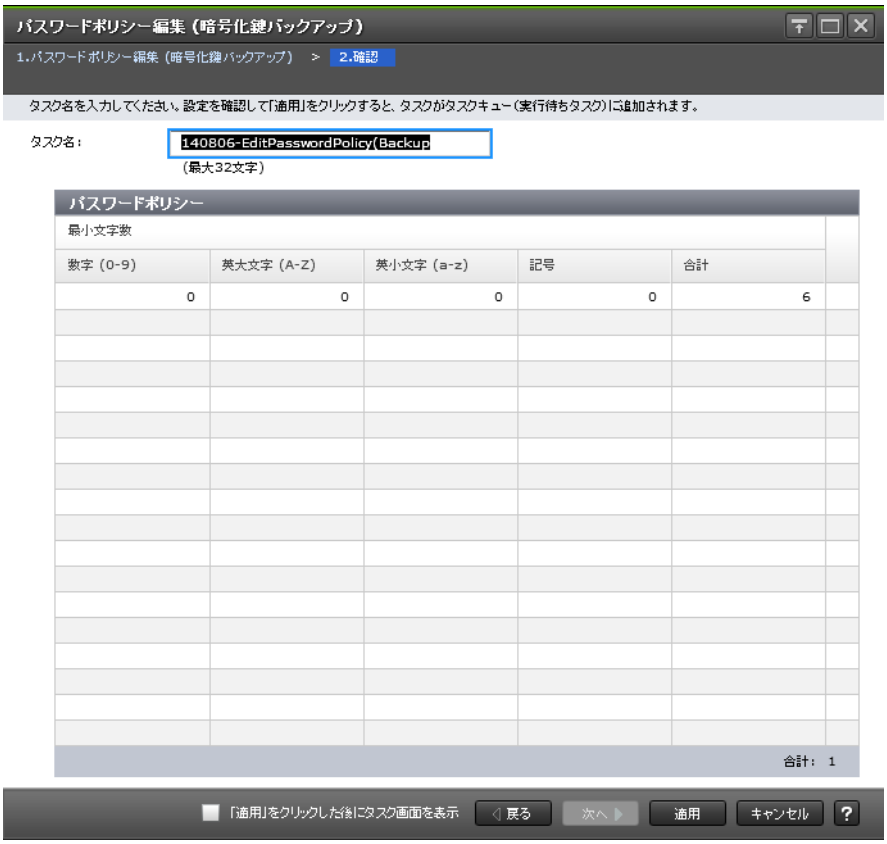
項目	説明
数字 (0-9)	パスワードに使用する数字の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
英大文字 (A-Z)	パスワードに使用する英大文字の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
英小文字 (a-z)	パスワードに使用する英小文字の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
記号	パスワードに使用する記号の最小文字数を入力します。設定できる値は 0 から 255 までで、初期値は 0 です。
合計	パスワードの最小文字数を入力します。設定できる値は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

関連リンク

参照先トピック

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（47 ページ）

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。

関連リンク

参照先トピック

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（47 ページ）

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）

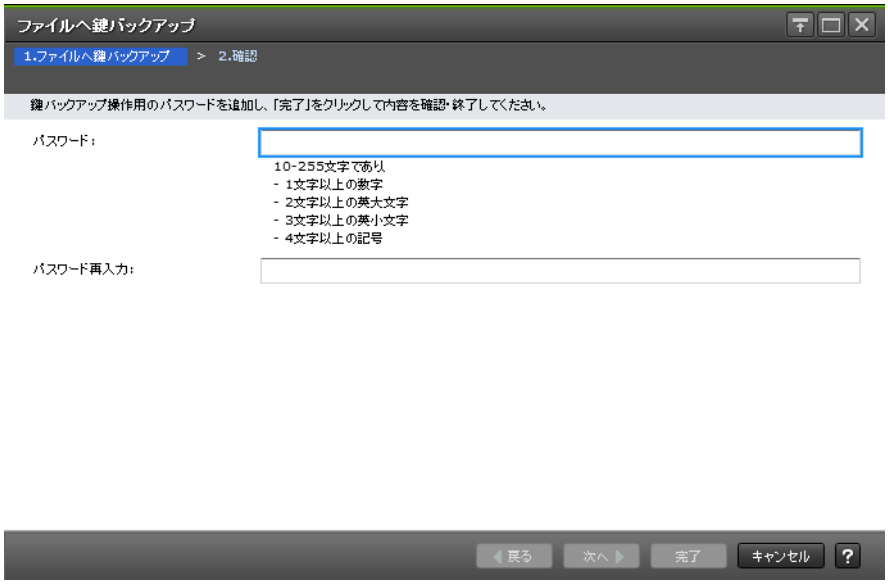
関連リンク

参照先トピック

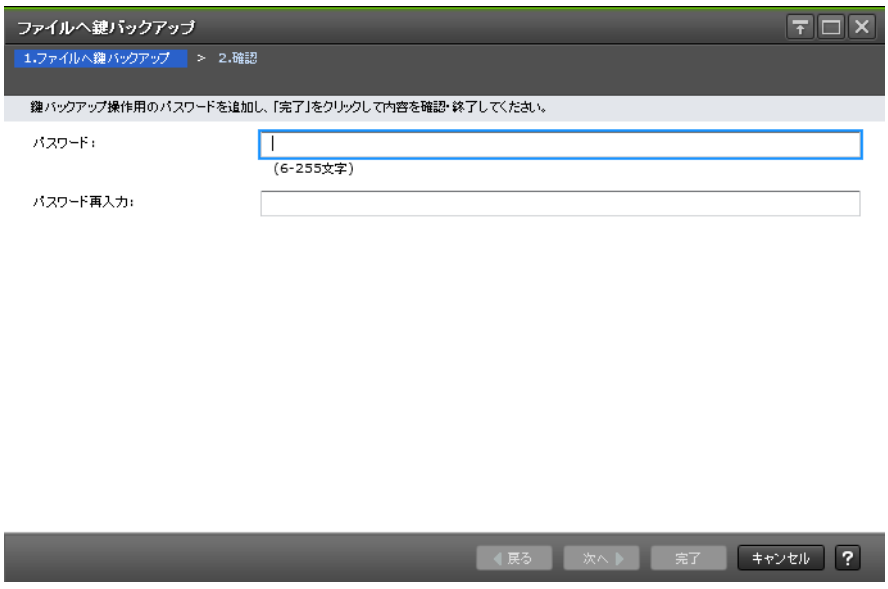
管理クライアント内にファイルとして暗号化鍵をバックアップする（19 ページ）
［ファイルへ鍵バックアップ］画面（50 ページ）
［設定確認］画面（51 ページ）

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

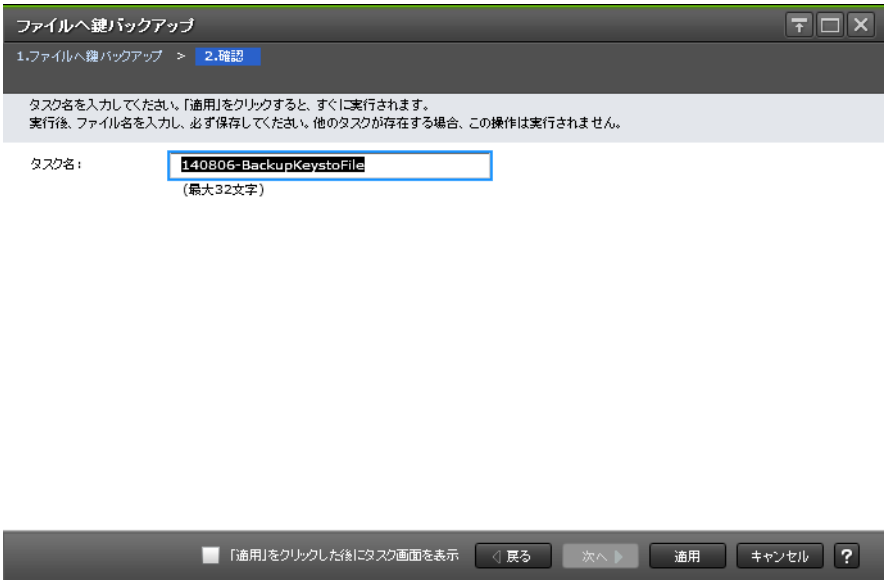
項目	説明
パスワード	暗号化鍵用のパスワードを入力します。パスワードは 6 文字以上 255 文字以下で、使用できる文字は次のとおりです。 • 数字（0 から 9） • 英大文字（A から Z） • 英小文字（a から z） • 記号 32 種：！" # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` {	} ~ ［パスワードポリシー編集（暗号化鍵バックアップ）］画面で、パスワードに使用する最小文字数が設定されている場合は、使用する最小文字数が［ファイルへ鍵バックアップ］画面に表示されます。
パスワード再入力	［パスワード］で入力したパスワードを再度入力します。

関連リンク

参照先トピック

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）（49 ページ）

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。

関連リンク

参照先トピック

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）（49 ページ）

A.6 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）

関連リンク

参照先トピック

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（29 ページ）
［ファイルから鍵回復］画面（52 ページ）
［設定確認］画面（53 ページ）

A.6.1 ［ファイルから鍵回復］画面

情報設定エリア

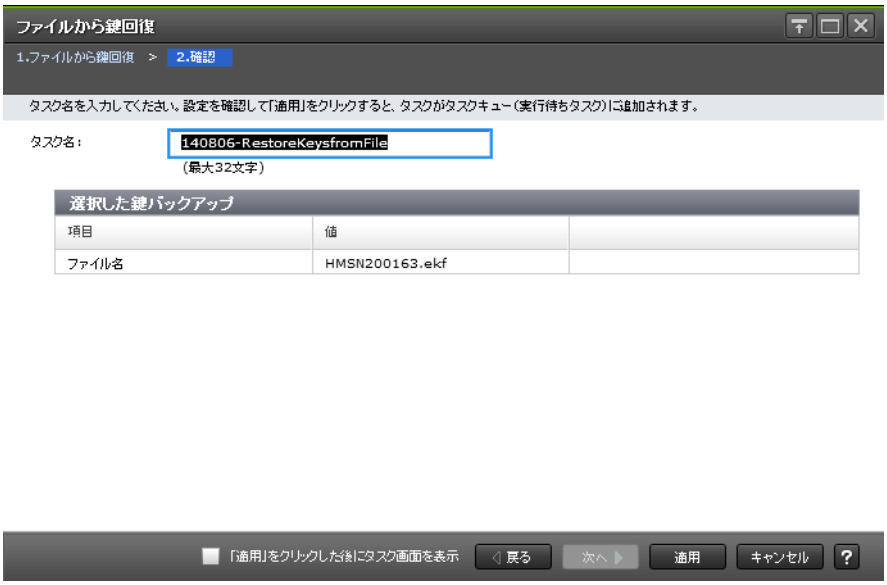
項目	説明
ファイル名	［参照］で選択した暗号化鍵ファイルのファイル名が表示されます。
参照	暗号化鍵ファイルを選択してください（ファイル拡張子.ekf）。 暗号化鍵ファイルを選択すると、選択した暗号化鍵ファイルのファイル名が［ファイル名］に表示されます。
パスワード	暗号化鍵をバックアップしたときに入力したパスワードを入力します。

関連リンク

参照先トピック

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）（52 ページ）

A.6.2 ［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。

関連リンク

参照先トピック

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）（52 ページ）

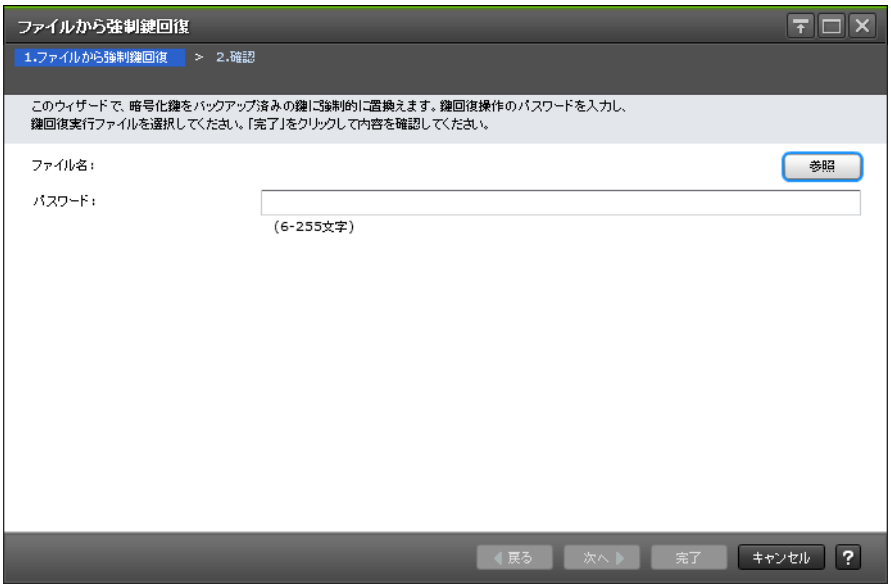
A.7 強制鍵回復ウィザード（管理クライアント内にバックアップしたファイルから強制リストアする場合）

関連リンク

参照先トピック

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（32 ページ）
［ファイルから強制鍵回復］画面（54 ページ）
［設定確認］画面（55 ページ）

A.7.1 ［ファイルから強制鍵回復］画面



情報設定エリア

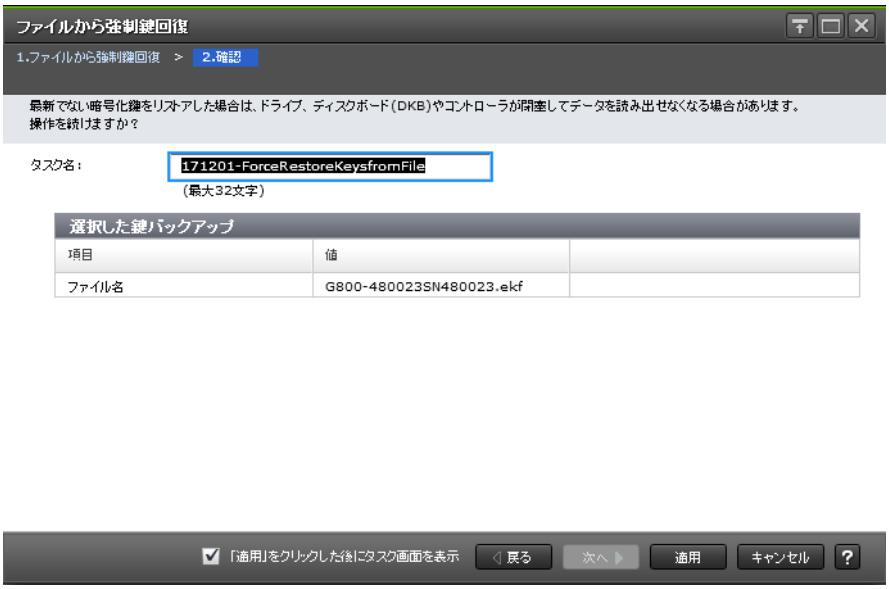
項目	説明
ファイル名	［参照］で選択した暗号化鍵ファイルのファイル名が表示されます。
参照	暗号化鍵ファイルを選択してください（ファイル拡張子.ekf)。 暗号化鍵ファイルを選択すると、選択した暗号化鍵ファイルのファイル名が［ファイル名］に表示されます。
パスワード	暗号化鍵をバックアップしたときに入力したパスワードを入力します。

関連リンク

参照先トピック

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）(53 ページ)

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。

関連リンク

参照先トピック

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）（53 ページ）

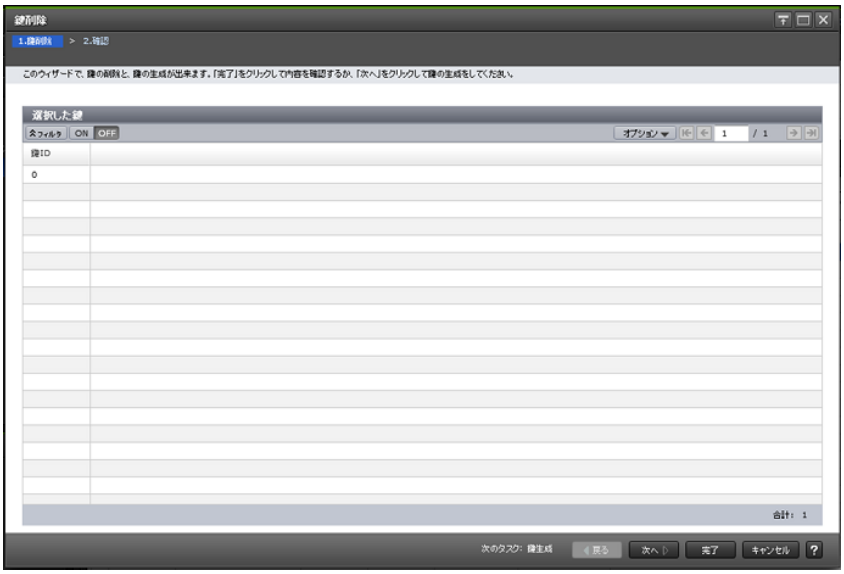
A.8 鍵削除ウィザード（ストレージシステム内の暗号化鍵を削除する場合）

関連リンク

参照先トピック

ストレージシステム内の暗号化鍵を削除する（33 ページ）
［鍵削除］画面（56 ページ）
［設定確認］画面（56 ページ）

A.8.1 ［鍵削除］画面



［選択した鍵］テーブル

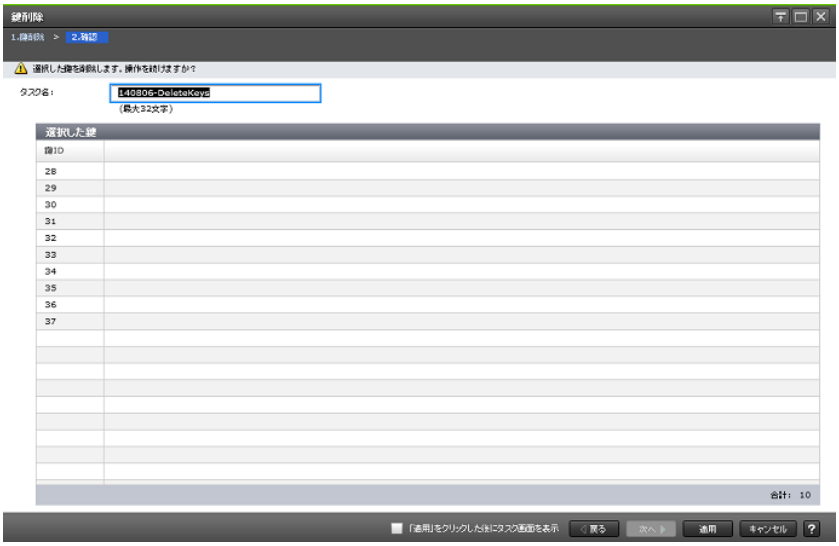
項目	説明
鍵 ID	暗号化鍵の番号を表示します。

関連リンク

参照先トピック

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）（55 ページ）

A.8.2 ［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。

関連リンク

参照先トピック

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）（55 ページ）

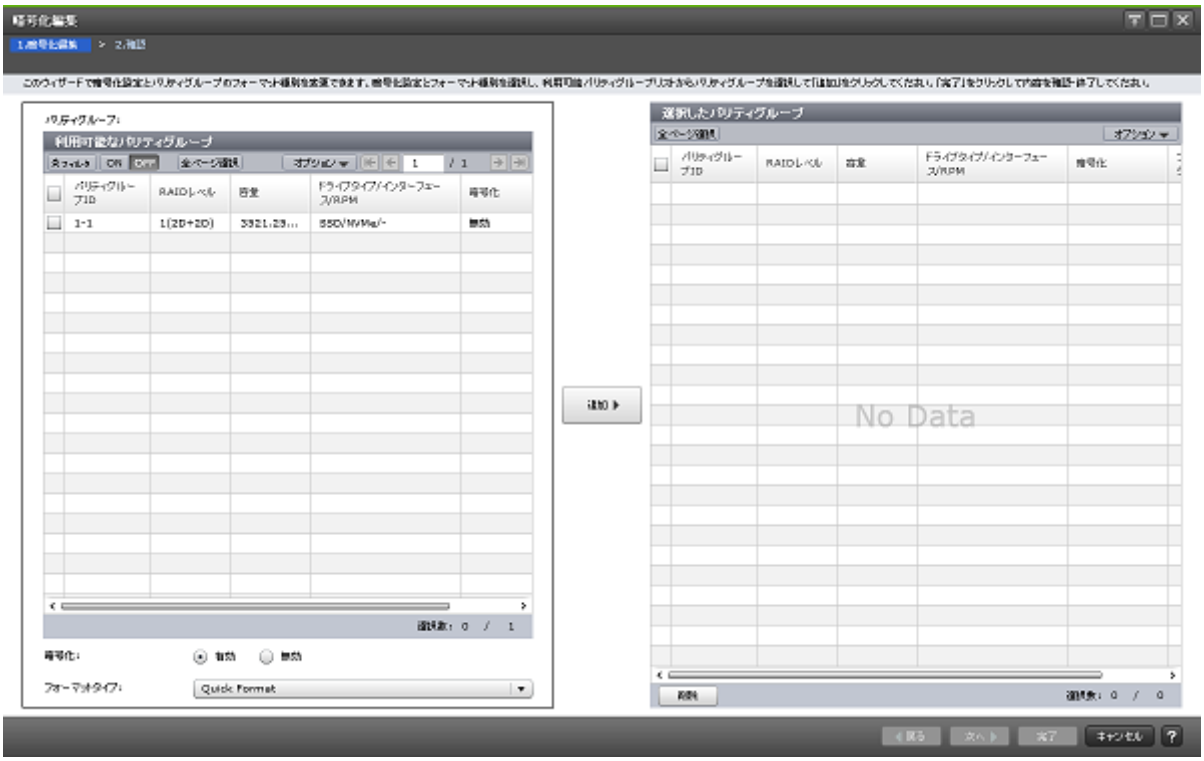
A.9 暗号化編集ウィザード

関連リンク

参照先トピック

データの暗号化を有効にする（21 ページ）
データの暗号化を無効にする（25 ページ）
［暗号化編集］画面（57 ページ）
［設定確認］画面（59 ページ）

A.9.1 ［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
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/インタフェース/RPM	ドライブ種別、インタフェース、RPM（回転数）を表示します。［−］は未設定を示します。
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。

［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/インタフェース/RPM	ドライブ種別、インタフェース、RPM（回転数）を表示します。［−］は未設定を示します。

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。

- ボタン

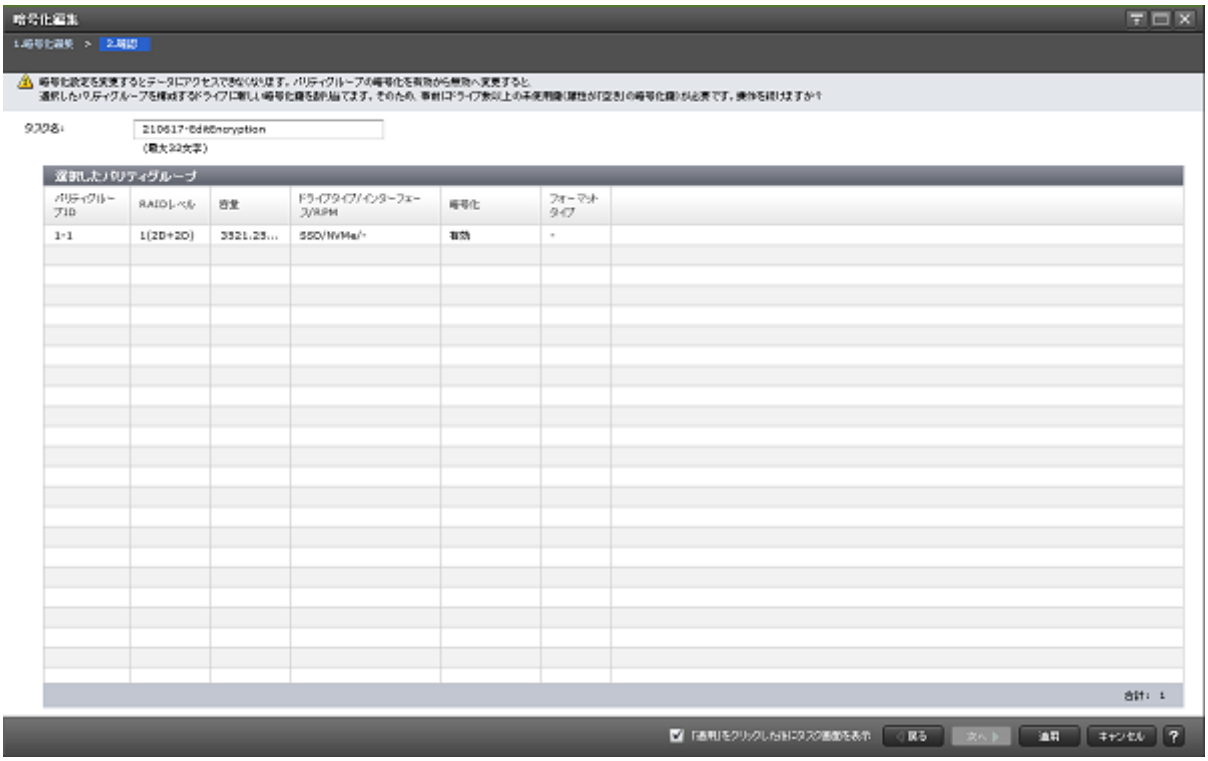
項目	説明
削除	選択したパリティグループを［選択したパリティグループ］テーブルから削除します。

関連リンク

参照先トピック

暗号化編集ウィザード（57 ページ）

A.9.2 ［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。

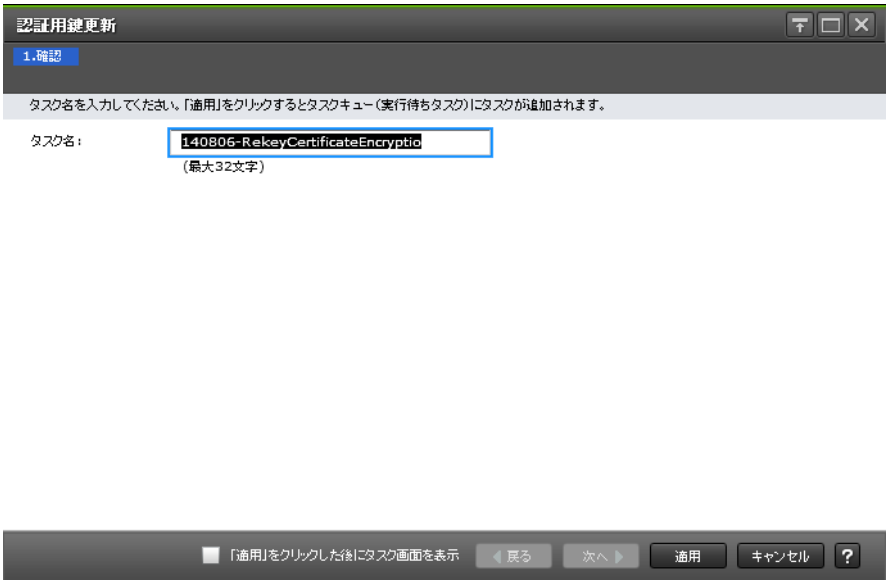
項目	説明
	分散パリティグループの場合は、分散数が RAID レベルの後ろに表示されます。例：1(2D+2D)*2
容量	パリティグループの総容量を表示します。
ドライブタイプ/インタフェース/RPM	ドライブ種別、インタフェース、RPM（回転数）を表示します。［−］は未設定を示します。
暗号化	設定した暗号化の状態が表示されます。 • 有効：暗号化が有効になっています。 • 無効：暗号化が無効になっています。
フォーマットタイプ	設定したフォーマット種別が表示されます。パリティグループにボリュームが 1 つもない場合はフォーマットが不要です。このため、フォーマットタイプには［ - ］が表示されます。

関連リンク

参照先トピック

暗号化編集ウィザード（57 ページ）

A.10 ［認証用鍵更新］画面



関連リンク

参照先トピック

認証用鍵を更新する（35 ページ）

付録 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	HA Device Manager - Storage Navigator
V10e	iStorage V10e
V100	iStorage V100
V300	iStorage V300
iStorage V シリーズ	次の製品を区別する必要がない場合の表記です。 • iStorage V10e • iStorage V100 • iStorage V300

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

略語	フルスペル
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。

索引

用語集

ALU

（Administrative Logical Unit）
Virtual Volume 機能を利用する場合のみ使用する用語です。

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）

任意のサイズが設定され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。

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

（HA 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

Active Mirror 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 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。

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。

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。

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、Active Mirror 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）
Virtual Volume 機能を利用する場合のみ使用する用語です。

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 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。

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。

鍵ペア

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

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。

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 Realtime Tiering で使用する仮想ボリュームを DP-VOL とも呼びます。Snapshot 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

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。

ローカルコピーのプログラムプロダクトには次があります。

Local Replication

Snapshot

リモートコピーのプログラムプロダクトには次があります。

Synchronous Replication（同期コピー）

Asynchronous Replication（非同期コピー）

Active Mirror（同期コピー）

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。

シェアドメモリ

キャッシュ上に論理的に存在するメモリです。共用メモリとも呼びます。ストレージシステムの共通情報や、キャッシュの管理情報（ディレクトリ）などを記憶します。これらの情報を基に、ストレージシステムは排他制御を行います。また、差分テーブルの情報もシェアドメモリで管理されており、コピーペアを作成する場合にシェアドメモリを利用します。

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

Asynchronous Replication 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。

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。

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。

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

Snapshot 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

Snapshot 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。Snapshot 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、Snapshot 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。

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。

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。

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

Active Mirror 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。

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。

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、Realtime Tiering、および Snapshot 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 Realtime Tiering ではプールボリュームに通常のデータを格納し、Snapshot 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。

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。

マイグレーションボリューム

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。

リザーブボリューム

Local Replication 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。

iStorage V10e/V100/V300
Encryption License Key
ユーザガイド

IV-UG-012-003-06

2024 年 10 月 第 6 版 発行

日本電気株式会社