NEC

iStorage V51/V110/V310/V310F

Encryption License Key
ユーザガイド



著作権

© NEC Corporation 2024-2026

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

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。

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。

Python は，Python Software Foundation の登録商標です。

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

2026 年 10 月

目次

第 1 章 Encryption License Key の概要 1

1.1 Encryption License Key 1

1.2 暗号化の仕様 2

1.2.1 ハードウェアの仕様 2

1.2.2 暗号化できるボリューム 2

1.2.3 格納データ暗号化で使用する鍵 3

1.3 暗号化鍵の管理機能 3

1.3.1 暗号化鍵の使用 4

1.3.2 暗号化鍵のバックアップ機能 5

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 5

1.3.3 暗号化鍵のリストア機能 6

1.4 データの暗号化機能 6

1.4.1 データの暗号化 6

1.4.2 暗号化の解除 7

1.4.3 データ暗号化鍵の変更 7

1.5 監査ログ機能 8

第 2 章 Encryption License Key を利用するための準備 9

2.1 システムの要件 9

2.2 他のプログラムプロダクトとの併用 9

2.2.1 Encryption License Key とコピー系プログラムプロダクトの併用 9

2.2.2 Encryption License Key と Snapshot Advanced の併用 9

2.2.3 Encryption License Key と Asynchronous Replication の併用 10

2.2.4 Encryption License Key と Volume Migration の併用 10

2.2.5 Encryption License Key と Dynamic Provisioning の併用 10

2.3 Encryption License Key の使用を取りやめる場合 10

第 3 章 Encryption License Key の操作 12

3.1 暗号化環境を設定する 12

3.2 暗号化鍵を作成する 12

3.3 暗号化鍵のバックアップ 13

3.3.1 管理ツールの操作端末内にファイルとして暗号化鍵をバックアップする 13

3.4 暗号化を有効にする 14

3.5 暗号化を無効にする 15

3.6 暗号化鍵のリストア 15
3.6.1 管理ツールの操作端末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 16
3.7 暗号化鍵の削除 16
3.7.1 ストレージシステム内の暗号化鍵を削除する 16
3.8 暗号化環境設定を初期化する 17
第 4 章 Encryption License Key のトラブルシューティング 18
4.1 Encryption License Key 操作時のトラブルと対策 18
4.2 お問い合わせ先 19
付録 A. このマニュアルの参考情報 20
A.1 操作対象リソースについて 20
A.2 このマニュアルでの表記 20
A.3 このマニュアルで使用している略語 20
A.4 KB（キロバイト）などの単位表記について 20
用語集 22
索引 43

はじめに

このマニュアルでは、 Encryption License Key の機能概要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 V51
- iStorage V110
- iStorage V310
- iStorage V310F

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。

A3-05-21-XX 以降

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

このマニュアルの位置付け

このマニュアルでは、主に Encryption License Key の機能、操作の準備、およびトラブルシューティングについて説明します。

詳細な操作方法や、操作上の注意事項などについては、次の管理ソフトウェアのマニュアルを参照してください。

管理ソフトウェア	参照マニュアル
HA Storage Manager Embedded	『HA Storage Manager Embedded ユーザガイド』

管理ソフトウェア	参照マニュアル
HA Storage Manager Embedded の API	『REST API リファレンスガイド』
詳細 API	
RAID Manager	『RAID Manager コマンドリファレンス』

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
Synchronous Replication	iStorage V51
Asynchronous Replication	
Active Mirror	

「容量削減機能が有効なボリューム」について

このマニュアルで「容量削減機能が有効なボリューム」と記載されている場合、特に断りのない限り、データ削減共有ボリュームおよび dedupe and compression により容量削減機能を有効に設定した仮想ボリュームのことを示します。

ユーザの操作権限（ロール）について

このマニュアルに記載されている、RAID Manager および内蔵 CLI を操作する際に、前提条件として必要となるロールの詳細は、『RAID Manager ユーザガイド』※を参照してください。

注※

詳細は、「ユーザ認証機能」の Storage Navigator または Maintenance Utility で設定したユーザの操作権限に従って実行されるコマンドに関する記載を参照してください。

REST API の管理ツールについて

iStorage V51,V110,V310,V310F が提供する REST API の管理ツールには、次の 2 種類があります。それぞれの特徴や使い分けなどの詳細は、『REST API リファレンスガイド』を参照してください。

「REST API」と記載している箇所は、次の両方の REST API を示します。

REST API 管理ツール	DKCMAIN バージョン A3-04-22-XX 以前のマニュアル上の表記	説明
HA Storage Manager Embedded の API	『HA Storage Manager Embedded の API』	リクエストラインに simple を含む REST API です。 基本的なプロビジョニングのために設計されており、高速な実行を確保するためのアーキテクチャーを取り入れています。 設定項目は最小限に抑えられ、複雑さを軽減し、効率的な手順で迅速にシステムのプロビジョニングができます。
詳細 API	『REST API』	リクエストラインに simple を含まない REST API です。 プロビジョニングのための詳細な設定項目を提供しており、ストレージシステムが混在した環境での高度な設定に対応した、幅広い選択肢が用意されています。 設定には HA Storage Manager Embedded の API よりも多くの手順を伴いますが、より柔軟な制御を実現できます。

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が必要です。

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、詳細 API で実行します。一部機能は、HA Storage Manager Embedded でも実行できます。HA Storage Manager Embedded の操作は、『HA Storage Manager Embedded ユーザガイド』を参照してください。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、『システム管理者ガイド』を参照してください。

各管理ツールでの、機能ごとの操作可否を次に示します。

機能	HA Storage Manager Embedded	RAID Manager	REST API	
			HA Storage Manager Embedded の API	詳細 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	×	×	×	○
管理ツールの操作端末内にファイルとして暗号化鍵をバックアップ	○	×	×	○
管理ツールの操作端末内のファイルから暗号化鍵をリストア	○	×	×	○
未使用暗号化鍵の削除および生成	×	×	×	○

機能	HA Storage Manager Embedded	RAID Manager	REST API	
			HA Storage Manager Embedded の API	詳細 API
パリティグループ作成時の暗号化有効設定	×	○	×	×
プール作成時の暗号化有効設定	○	×	○	×

凡例

○：操作できる

×：操作できない

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 V51 • iStorage V110 • iStorage V310 • iStorage V310F	FIPS 140-3 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（6 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」（鍵種別が FREE）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
- 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、「DEK」を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	ストレージシステムごとの暗号化鍵の最大数
• iStorage V51 • iStorage V110 • iStorage V310 • iStorage V310F	984	4,096

暗号化鍵を設定する単位

- DEK：ドライブ単位に 1 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詳細 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 V51 • iStorage V110 • iStorage V310 • iStorage V310F	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 V51 • iStorage V110 • iStorage V310 • iStorage V310F	4,096

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（4 ページ）
暗号化鍵のバックアップ機能（5 ページ）
暗号化鍵のリストア機能（6 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。
ドライブ交換	ドライブあたり 1 個	交換するドライブ数分必要となります。
暗号化が有効なパリティグループの削除時	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。

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（3 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（3 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（5 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、詳細 API または HA Storage Manager Embedded 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。

二次バックアップは、管理クライアント内にファイルとしてバックアップします。

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。

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がない状態では、暗号化鍵のバックアップはできません。

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（5 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、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の暗号化鍵のリストアは、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します。

関連リンク

参照先トピック

暗号化鍵の管理機能（3 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（6 ページ）
暗号化の解除（7 ページ）
データ暗号化鍵の変更（7 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。パリティグループ作成時に、暗号化設定を有効にします。そのパリティグループにボリュームを作成すると、そのボリュームに格納するデータが暗号化されます。

暗号化が無効なパリティグループの暗号化設定を有効に変更できません。パリティグループを一度削除して、暗号化を有効にしたパリティグループを新規作成してください。既存のパリティグループ内にボリュームが存在して、そのデータを暗号化する場合は、「既存のデータを暗号化する（7 ページ）」を参照してください。

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。データは仮想ボリューム単位で移行します。

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（6 ページ）

1.4.2　暗号化の解除

Encryption License Key でパリティグループの暗号化を解除するには、暗号化が有効なパリティグループを削除します。暗号化が有効なパリティグループを削除すると、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。

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。

関連リンク

参照先トピック

データの暗号化機能（6 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。データは仮想ボリューム単位で移行します。

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を削除すると、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（6 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。
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。

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 Advanced 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 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。

2.3　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. 暗号化が有効なパリティグループをすべて削除してください。

   削除するパリティグループ内に必要なデータが含まれている場合は、削除前に必ずデータのバックアップまたはデータ移行を実施してください。

2. 暗号化環境設定を初期化してください。
3. 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。

第 3 章
Encryption License Key の操作

ここでは、詳細 API を使った、Encryption License Key（暗号化）の設定操作、前提条件、および注意事項について説明します。

詳細 API の詳細な操作方法については、『REST API リファレンスガイド』を参照してください。

3.1　暗号化環境を設定する

操作手順

1. 暗号化環境設定を有効にすることで、暗号化の運用を開始できます。有効に設定すると、ストレージシステム内に暗号化鍵が作成されます。

   リクエストライン：

   ```
   PATCH ＜ベース URL＞/v1/objects/encryption-settings/instance
   ```

3.2　暗号化鍵を作成する

暗号化鍵は、暗号化環境の設定が有効に設定された際に、自動で作成されます。ただし、次のような場合は、手動で暗号化鍵の作成が必要になります。

- 暗号化鍵の変更が必要になった場合
- ドライブ交換によって、未割り当ての鍵が不足した場合

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 V51,V110,V310,V310F	4,096

暗号化鍵はストレージシステム内に作成されます。

注意事項

- 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。
- 作成可能な最大の暗号化鍵数は、ストレージシステムごとに作成できる暗号化鍵の数（4,096）から、現在の暗号化鍵の数を引いた数が、その時点で作成可能な暗号化鍵の最大数になります。

現在の暗号化鍵の数は、下記リクエストラインで確認できます。

```
GET ＜ベース URL＞/v1/objects/encryption-key-counts/instance
```

操作手順

1. 暗号化鍵を作成します。

   リクエストライン：

   ```
   POST ＜ベース URL＞/v1/objects/encryption-keys
   ```

3.3　暗号化鍵のバックアップ

暗号化鍵の一次バックアップは自動で取得されますが、二次バックアップは手動での取得操作が必要です。暗号化環境設定を有効化した後、または暗号化鍵を作成後は、暗号鍵を管理ツールの操作端末内にファイルとしてバックアップしてください。

個別にバックアップを取り直したい場合や手動でバックアップを取得するようにガイドされた場合は、暗号鍵を管理ツールの操作端末内にファイルとしてバックアップしてください。

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、管理ツールの操作端末内にファイルとしてバックアップします。

暗号化鍵を管理ツールの操作端末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。

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

作成済みの暗号化鍵がない状態では、暗号化鍵のバックアップはできません。

関連リンク

参照先トピック

管理ツールの操作端末内にファイルとして暗号化鍵をバックアップする（13 ページ）

3.3.1　管理ツールの操作端末内にファイルとして暗号化鍵をバックアップする

暗号化鍵を管理ツールの操作端末内にファイルとしてバックアップできます。

注意事項

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。

操作手順

1. 暗号化鍵をファイルとしてバックアップします。

   リクエストライン：

   ```
   POST ＜ベース URL＞/v1/objects/encryption-keys/file/actions/backup/invoke
   ```

3.4　暗号化を有効にする

Encryption License Key では、パリティグループごとに暗号化の設定をします。暗号化を有効に設定できるのは、パリティグループ作成時のみです。

暗号化が無効なパリティグループに対して、後から暗号化を有効に設定できません。暗号化が無効なパリティグループに対して暗号化を設定したい場合は、その暗号化が無効なパリティグループを一度削除します。その後、暗号化が有効なパリティグループを作成します。ただし、前述の方法は、暗号化が無効なパリティグループにボリュームが作成されていない場合に限ります。

この手順は、RAID Manager で操作します。各コマンドの使用方法は『RAID Manager コマンドリファレンス』を参照してください。

操作手順

1. 暗号化が無効なパリティグループを削除します。

   コマンド：

   ```
   raidcom delete parity_grp
   ```

2. 暗号化が有効なパリティグループを作成します。

   コマンド：

   ```
   raidcom add parity_grp
   ```

   ヒント

   暗号化を有効にしたパリティグループを作成するには、`-encryption` オプションで `enable` を指定します。

3.5　暗号化を無効にする

暗号化を有効にしたパリティグループの暗号化設定を無効に変更できません。代わりに、暗号化が有効なパリティグループを一度削除した後に、暗号化が無効なパリティグループを作成することで、暗号化を無効にします。

ただし、前述の方法は、パリティグループにボリュームが存在しない場合に限ります。

この手順は、RAID Manager で操作します。各コマンドの使用方法は『RAID Manager コマンドリファレンス』を参照してください。

操作手順

1. 暗号化が有効なパリティグループを削除します。

   コマンド：

   ```
   raidcom delete parity_grp
   ```

2. 暗号化が無効なパリティグループを作成します。

   コマンド：

   ```
   raidcom add parity_grp
   ```

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 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、ドライブの保守などのときに、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プール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プール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は、管理ツールの操作端末内にバックアップしたファイルからリストアします。

関連リンク

参照先トピック

管理ツールの操作端末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（16 ページ）

3.6.1　管理ツールの操作端末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

操作手順

1. 管理ツールの操作端末にバックアップしたファイルから、 暗号化鍵をリストアします。

   リクエストライン：

   ```
   POST ＜ベース URL＞/v1/objects/encryption-keys/file/actions/restore/invoke
   ```

関連リンク

参照先トピック

暗号化鍵のリストア機能（6 ページ）
暗号化鍵のリストア（15 ページ）

3.7　暗号化鍵の削除

⚠ 注意

暗号化鍵の削除後は、「3.2　暗号化鍵を作成する（12 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

暗号化環境を設定する（12 ページ）
暗号化鍵を作成する（12 ページ）
ストレージシステム内の暗号化鍵を削除する（16 ページ）

3.7.1　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」（鍵種別が FREE）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。

操作手順

1. ストレージシステム内の暗号化鍵を削除します。
   - リクエストの body で指定した暗号化鍵を削除する場合

     リクエストライン：

     ```
     POST ＜ベース URL＞/v1/services/encryption-key-service/actions/delete/invoke
     ```

   - 鍵の ID を指定して削除する場合

     リクエストライン：

     ```
     DELETE ＜ベース URL＞/v1/objects/encryption-keys/＜オブジェクト ID＞
     ```

関連リンク

参照先トピック

暗号化鍵の削除（16 ページ）

3.8　暗号化環境設定を初期化する

前提条件

暗号化が有効なパリティグループが存在しないこと。

操作手順

1. 設定済みの暗号化環境設定を初期化します。

   リクエストライン：

   ```
   PATCH ＜ベース URL＞/v1/objects/encryption-settings/instance
   ```

   ヒント

   暗号化環境設定を初期化するには、属性 `isEnabled` に `false` を指定します。

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と対処方法について次に示します。

トラブル	対策
暗号化鍵の操作（バックアップ／リストア）が失敗した。	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 上記を確認後、再度暗号化鍵の操作（バックアップ／リストア）を実施してください。
暗号化鍵の作成操作が失敗した。	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 上記を確認後、暗号化鍵の一覧を参照し、暗号化鍵が作成されているかどうか確認してください。 暗号化鍵の一覧参照手順は、『REST API リファレンスガイド』の暗号化鍵の一覧を取得するを参照してください。 • 暗号化鍵が作成されていた場合 暗号化鍵の作成は成功しています。暗号化鍵の外部バックアップを実施してください。 • 暗号化鍵が作成されていない場合 再度暗号化鍵の作成を実施してください。暗号化鍵の作成が成功した後、手動で管理ツールの操作端末内に、ファイルとしてバックアップしてください。
暗号化鍵の削除に失敗した。	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

トラブル	対策
	上記を確認後、暗号化鍵の一覧を参照して、暗号化鍵が削除されているかどうか確認してください。 暗号化鍵の一覧参照手順は、『REST API リファレンスガイド』の暗号化鍵の一覧を取得するを参照してください。 • 暗号化鍵が削除されていた場合 対処不要です。 • 暗号化鍵が削除されていない場合 再度暗号化鍵の削除を実施してください。
暗号化環境設定に失敗した（暗号化の無効から有効への設定）。	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 上記を確認後、暗号化環境設定の初期化を実行してください。暗号化環境設定の初期化が正常に終了したことを確認してから、再度暗号化環境設定を実施してください。
暗号化鍵の操作が、次のどれかのエラーコードで失敗した。 • 36162-00204208 • 36162-00204209 • 36162-00204224	次の対策を実施してください。 1. ストレージシステムの状態を確認し、ボリュームの閉塞部位があれば回復してください。 2. ボリュームの閉塞部位を回復後、失敗した暗号化鍵の操作を再度実施してください。
SIM コード 660100 または 660200 が報告された。	未使用鍵（属性が「空き」（鍵種別が FREE）の暗号化鍵）の数が保守作業に必要なしきい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。

4.2　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.　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。

A.1　操作対象リソースについて

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。

A.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
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 V51 • iStorage V110 • iStorage V310 • iStorage V310F
V51	iStorage V51
V110	iStorage V110
V310	iStorage V310
V310F	iStorage V310F

A.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
LDEV	Logical DEVice
SIM	Service Information Message

A.4　KB（キロバイト）などの単位表記について

1KB（キロバイト）、1MB（メガバイト）、1GB（ギガバイト）、1TB（テラバイト）、1PB（ペタバイト）は、それぞれ 1KiB（キビバイト）、1MiB（メビバイト）、1GiB（ギビバイト）、1TiB（テビバイト）、1PiB（ペビバイト）と読み替えてください。

1KiB、1MiB、1GiB、1TiB、1PiB は、それぞれ 1,024 バイト、1,024KiB、1,024MiB、1,024GiB、1,024TiB です。

1block（ブロック）は 512 バイトです。

用語集

ADP

（Advanced Dynamic Provisioning）

パリティグループを構成する各ドライブの領域を複数の領域に分割して、各ドライブ内の分割された領域の 1 つを、スペア用の領域として使用します。これにより、リビルド I/O、または Correction I/O を分散できるため、リビルド時間が短縮できます。

ADP 用のパリティグループ

ADP 機能が有効なパリティグループのことです。

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冗長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。

bps

（bits per second）

データ転送速度の標準規格です。

CHAP

（Challenge Handshake Authentication Protocol）

認証方式のひとつ。ネットワーク上でやり取りされる認証情報はハッシュ関数により暗号化されるため、安全性が高いです。

CHB

（Channel Board）

詳しくは「チャネルボード」を参照してください。

Child

Snapshot Advanced の用語で、Parent のメタデータを共有する先のペアまたはボリュームを指します。

Family 内に vClone 属性のボリュームが存在しない場合、ルートボリュームと同じスナップショットツリーに属するペアまたはボリュームが該当します。

Family 内に vClone 属性のボリュームが存在する場合、vClone Parent 属性のボリュームと同じスナップショットツリーに属するペアまたはボリューム、同一 Family 内の vClone 属性のボリューム、同一 Family 内の vClone 属性のボリュームと同じスナップショットツリーに属するペアまたはボリュームが該当します。

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。

CNA

（Converged Network Adapter）

HBA と NIC を統合したネットワークアダプタ。

CRC

（Cyclic Redundancy Check）

巡回冗長検査。コンピュータデータに対し、偶発的変化を検出するために設計された誤り訂正符号。

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。

DKB

（Disk Board SAS）

SAS ドライブとキャッシュメモリ間のデータ転送を制御するモジュールです。

DKBN

（Disk Board NVMe）

NVMe ドライブとキャッシュメモリ間のデータ転送を制御するモジュールです。

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。

DKU

各種ドライブを搭載するためのシャーシ（筐体）です。

DB(Drive Box)と同義語となります。

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。

ENC

ドライブボックスに搭載され、コントローラシャーシまたは他のドライブボックスとのインターフェース機能を有します。

ESM

（Embedded Storage Manager）

iStorage V51,V110,V310,V310F における管理系ソフトウェアです。

ESMOS

（Embedded Storage Manager Operating System）

ESM を動作させるための OS や OSS を含んだファームウェアです。

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。

Failover

故障しているものと機能的に同等のシステムコンポーネントへの自動的置換。

この Failover という用語は、ほとんどの場合、同じストレージデバイスおよびホストコンピュータに接続されているインテリジェントコントローラに適用されます。

コントローラのうちの 1 つが故障している場合、Failover が発生し、残っているコントローラがその I/O 負荷を引き継ぎます。

Family

Snapshot Advanced の用語で、メタデータを共有する Parent（メタデータ共有元となるボリューム）と Child（Parent のメタデータ共有するペアまたはボリューム）の群れを指します。

FC

（Fibre Channel）

ストレージシステム間のデータ転送速度を高速にするため、光ケーブルなどで接続できるようにするインターフェースの規格のことです。

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。

GUI

（Graphical User Interface）

コンピュータやソフトウェアの表示画面をウィンドウや枠で分け、情報や操作の対象をグラフィック要素を利用して構成するユーザインターフェース。マウスなどのポインティングデバイスで操作することを前提に設計されます。

HA Storage Manager Embedded

ストレージシステムの構成やリソースを操作するシンプルな GUI の管理ツールです。

HA Storage Manager Embedded の API

リクエストラインに simple を含む REST API です。

ストレージシステムの情報取得や構成変更することができます。

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。

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、管理ツールの操作端末またはサーバから、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。

iSNS

（Internet Storage Naming Service）

iSCSI デバイスで使われる、自動検出、管理および構成ツールです。

iSNS によって、イニシエータおよびターゲット IP アドレスの特定リストで個々のストレージシステムを手動で構成する必要がなくなります。代わりに、iSNS は、環境内のすべての iSCSI デバイスを自動的に検出、管理および構成します。

LACP

（Link Aggregation Control Protocol）

複数回線を 1 つの論理的な回線として扱うための制御プロトコル。

LAN ボード

コントローラシャーシに搭載され、ストレージシステムの管理とのインターフェース機能を有するモジュールです。

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。

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。

NVM

（Non-Volatile Memory）

不揮発性メモリです。

NVMe

（Non-Volatile Memory Express）

PCI Express を利用した SSD の接続インタフェース、通信プロトコルです。

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 ESM/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。

Parent

Snapshot Advanced の用語で、メタデータの共有元となるボリュームを指します。

Family 内に vClone 属性のボリュームが存在しない場合、ルートボリュームが該当します。Family 内に vClone 属性のボリュームが存在する場合、vClone Parent 属性のボリュームが該当します。

PCB

（Printed Circuit Board）

プリント基盤です。このマニュアルでは、コントローラボードやチャネルボード、ディスクボードなどのボードを指しています。

Point to Point

2 点を接続して通信するトポロジです。

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。

SAN

（Storage-Area Network）

ストレージシステムとサーバ間を直接接続する専用の高速ネットワークです。

SAS ケーブル

コントローラシャーシとドライブボックス間、ドライブボックスとドライブボックス間を接続するためのケーブルです。

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。

SM

（Shared Memory）

詳しくは「シェアドメモリ」を参照してください。

SNMP

（Simple Network Management Protocol）

ネットワーク管理するために開発されたプロトコルの 1 つです。

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。

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。

UPS

（Uninterruptible Power System）

ストレージシステムが停電や、瞬停のときでも停止しないようにするために搭載してある予備の電源のことです。

URL

（Uniform Resource Locator）

リソースの場所や種類の両方を記載しているインターネット上の住所を記述する標準方式です。

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。

vClone Parent 属性のボリューム

Snapshot Advanced の用語で、Family 内に vClone 属性のボリュームが存在する場合、そのメタデータの共有元になるボリュームを指します。

vClone 属性のボリューム

Snapshot Advanced の用語で、仮想クローン作成によって取得したスナップショットデータを格納するボリュームを指します。

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）を作成することができます。

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。

Windows

Microsoft Windows Operating System

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

外部ボリュームグループに作成した LDEV のことです。マッピングした外部ストレージシステムのボリュームを実際にホストや他プログラムプロダクトから使用するためには、外部ボリュームグループに LDEV を作成する必要があります。

外部ボリュームグループ

外部ストレージシステムのボリュームをマッピングしている、本ストレージシステム内の仮想的なボリュームです。

外部ボリュームグループはパリティ情報を含みませんが、管理上はパリティグループと同じように取り扱います。

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 で使用する仮想ボリュームを DP-VOL とも呼びます。

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。

管理ツールの操作端末

ストレージシステム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。

クラスタ

ディスクセクターの集合体です。OS は各クラスタに対しユニークナンバーを割り当てし、それらがどのクラスタを使うかに応じて、ファイルの経過記録をとります。

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。

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。

Out-of-band 方式で接続された RAID Manager、もしくは内蔵 CLI を用いて設定してください。

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。

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。

システムプールボリューム、システムプール VOL

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。

詳細 API

リクエストラインに simple を含まない REST API です。ストレージシステムの情報取得や構成変更することができます。

本マニュアルの 03 版以前では、「REST API」と表記しています。

冗長パス

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。交替パスとも言います。

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。

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

Snapshot Advanced 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 Advanced では、特定時点のデータの複製のことを指します。

スペアドライブ

通常リード、ライトが行われるドライブとは別に搭載されているドライブを指し、1 台のドライブに故障が発生したとき、そのドライブに記憶されていたデータがスペアドライブにコピーされることで、システムとしては元と同様に使用できます。

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 Advanced では、セカンダリボリューム（仮想ボリューム）ではなく、プールにデータが格納されます。

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。

ゾーニング

ホストとリソース間トラフィックを論理的に分離します。ゾーンに分けることにより、処理は均等に分散されます。

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。

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。

通常ボリューム

仮想ボリュームを除く内部ボリュームまたは外部ボリューム（Universal Volume Manager を使用して外部ストレージシステムのボリュームをマッピングしたボリューム）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。

データ削減共有ボリューム

データ削減共有ボリュームは、Adaptive Data Reduction の容量削減機能を使用して作成する仮想ボリュームです。Snapshot Advanced ペアのボリュームとして使用できます。データ削減共有ボリュームは、Redirect-on-Write のスナップショット機能を管理するための制御データ（メタデータ）を持つボリュームです。

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。

パリティドライブ

RAID5 を構成するときに、1 つの RAID グループの中で 1 台のドライブがパリティドライブとなり、残りのドライブがデータドライブとなります。パリティドライブには複数台のデータドライブのデータから計算されたデータが記憶されます。これにより 1 つの RAID グ

ループ内で 1 台のドライブが故障した場合でも、パリティドライブから再計算することでデータを損なわずにストレージシステムを使用できます。

RAID6 を構成するときに、1 つの RAID グループの中で 2 台のドライブがパリティドライブとなり、残りのドライブがデータドライブとなります。パリティドライブには複数台のデータドライブのデータから計算されたデータが記憶されます。これにより 1 つの RAID グループ内で 2 台のドライブが故障した場合でも、パリティドライブから再計算することでデータを損なわずにストレージシステムを使用できます。

非 ADP 用のパリティグループ

ADP 機能が無効なパリティグループのことです。

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冗長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。

ファームウェア

ストレージシステムで、ハードウェアの基本的な動作を制御しているプログラムです。

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。

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

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

データ管理目的として互いに関連している 2 つのボリュームを指します（例、レプリケーション、マイグレーション）。ペアは通常、お客様の定義によりプライマリもしくはソースボリューム、およびセカンダリもしくはターゲットボリュームで構成されます。

ペア状態

ペアオペレーション前後にボリュームペアに割り当てられた内部状態。ペアオペレーションが実行されている、もしくは結果として障害となっているときにペア状態は変化します。ペア状態はコピーオペレーションを監視し、およびシステム障害を検出するために使われます。

ペアテーブル

ペア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。

ポートモード

ストレージシステムのチャネルボードのポート上で動作する、通信プロトコルを選択するモードです。ポートの動作モードとも言います。

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。

ホストデバイス

ホストに提供されるボリュームです。HDEV（Host Device）とも呼びます。

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。

ラック

電子機器をレールなどで棚状に搭載するフレームのことです。通常幅 19 インチで規定されるものが多く、それらを 19 型ラックと呼んでいます。搭載される機器の高さは EIA 規格で規定され、ボルトなどで機器を固定するためのネジ穴が設けられています。

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。

リンクアグリゲーション

複数のポートを集約して、仮想的にひとつのポートとして使う技術です。

これによりデータリンクの帯域幅を広げるとともに、ポートの耐障害性を確保します。

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 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

管理ツールの操作端末を接続しているストレージシステムを指します。

索引

A

AES 256.....2

X

XTS モード.....2

あ

暗号化
    解除.....7
    既存データ.....7
    仕様.....2
    無効.....15
    有効.....14
暗号化鍵.....3
    バックアップ.....5,13
    変更.....7
    リストア.....6,15
暗号化環境設定
    初期化.....17

か

監査ログ機能.....8

さ

システム要件.....9

た

データの暗号化.....6
トラブルシューティング.....18

は

バックアップ
    暗号化鍵.....5,13
併用.....9

ら

リストア
    暗号化鍵.....6,15

iStorage V51/V110/V310/V310F
Encryption License Key
ユーザガイド

IV-UG-012-004-05

2026 年 10 月 第 5 版 発行

日本電気株式会社

© NEC Corporation 2024-2026