HITACHI
Inspire the Next

セキュリティ設定ガイド

Hitachi Virtual Storage Platform One Block 85

4051-1J-U68-10

ストレージシステムを操作する場合は、必ずこのマニュアルを読み、操作手順、および指示事項をよく理解してから操作してください。

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。

商標類
AIX は，米国およびその他の国における International Business Machines Corporation の商標です。
FlashCopy は，米国およびその他の国における International Business Machines Corporation の商標です。
IBM は，米国およびその他の国における International Business Machines Corporation の商標です。
Internet Explorer は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Linux は，Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Oracle®、Java、MySQL 及び NetSuite は、Oracle、その子会社及び関連会社の米国及びその他の国における登録商標です。
Red Hat は，米国およびその他の国で Red Hat, Inc.の登録商標もしくは商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
Veritas、Veritas ロゴは、米国およびその他の国における Veritas Technologies LLC またはその関連会社の商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。
その他記載の会社名、製品名などは、それぞれの会社の商標または登録商標です。

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 4 月（4051-1J-U68-10）

目次

はじめに 7
対象ストレージシステム 8
マニュアルの参照と適合プログラムバージョン 8
対象読者 8
マニュアルで使用する記号について 8
ユーザの操作権限（ロール）について 9
REST API の管理ツールについて 9
発行履歴 9

1.セキュリティ設定の概要 11
1.1 概要 12
1.2 想定する利用者 12
1.3 主要セキュリティ機能 13
1.3.1 ストレージ管理者および保守員のアクセス制御機能 13
(1) ロール 13
(2) リソースグループ 14
1.3.2 ホストのアクセス制御機能 14
1.3.3 ストレージ管理者および保守員の識別・認証機能 14
1.3.4 管理ツールの操作端末とストレージシステム間およびストレージシステムと外部認証サーバ間の暗号通信 15
1.3.5 格納データ暗号化機能 15
1.3.6 監査ログ機能 15
1.3.7 Media Sanitization 機能 15
1.4 各管理ツールが利用するポート情報 16
1.5 最新のソフトウェアの適用 16

2.物理セキュリティ 17
2.1 運用環境の物理セキュリティについて 18

3.ユーザ管理と認証・認可 19
3.1 ビルトインアカウントのパスワード変更 20
3.2 ユーザ管理モデル 20
3.2.1 ユーザグループとロールおよびリソースグループの関係 20
3.2.2 ロールと許可されている操作 22

3.2.3 ビルトイングループ 23
3.3 ユーザ管理 25
3.3.1 ユーザアカウントポリシーの設定 25
(1) ユーザアカウントポリシーを利用する場合のユーザ管理 26
(2) ユーザアカウントのパスワードポリシー設定 27
(3) メールサーバの設定 29
(4) テストメールの送信 30
(5) ユーザ個別のパスワードポリシーの適用 31
(6) ユーザ個別のメールアドレスの設定 32
(7) ユーザアカウント状態の確認 33
(8) アカウントロックの解除 33
(9) アカウントの有効化 34
3.3.2 ユーザの作成 34
3.3.3 ユーザアカウントの削除 36
3.3.4 ユーザアカウントの無効化 36
3.3.5 パスワードの変更 37
3.4 外部認証 37
3.4.1 外部認証サーバ・外部認可サーバの要件 38
3.4.2 外部認証サーバに接続する 38
3.5 TLS 通信機能 41
3.5.1 ストレージシステムと外部サーバ間の SSL/TLS 通信 41
3.5.2 SSL/TLS 通信の設定の流れ 44
(1) 秘密鍵を作成 45
(2) 公開鍵を作成 45
(3) 署名付き証明書を取得 46
(4) 署名付きの信頼できる証明書を取得 47
(5) CSR 作成および自己署名証明書作成 47
(6) SSL/TLS 証明書を PKCS#12 形式に変換 47
(7) Web サーバ接続用証明書をストレージシステムへアップロード 48
3.5.3 TLS セキュリティ設定を管理する 49
(1) SSL/TLS 通信のセキュリティ設定項目 49
(2) SSL/TLS セキュリティ設定を変更する 50
(3) SSL/TLS 通信のセキュリティ設定を初期化する 52

4.Audit Log 55
4.1 監査ログの Syslog サーバへの転送を設定する 56
4.2 Syslog サーバに監査ログのテストメッセージを送信する 57

5.SNMP 59
5.1 SNMP の送信情報を設定する 60
5.2 アラートが SNMP トラップ送信されるようにする（SNMP v3 の場合） 60
5.3 SNMP エンジン ID を SNMP マネージャに登録する（SNMP v3 の場合） 61
5.4 SNMP マネージャへトラップをテスト送信する 62

6.LUN Manager/Security 63
6.1 LUN セキュリティ（ポートセキュリティ）を設定する 64
6.2 Namespace セキュリティを設定する 64

7.iSCSI CHAP 認証 65
7.1 iSCSI ターゲットを作成してホストを登録する 66
7.2 iSCSI ターゲットに CHAP ユーザ名を設定する 66
7.3 iSCSI ターゲットから CHAP ユーザ名を削除する 66

8.Encryption License Key 67
8.1 鍵管理サーバを利用する 68
8.1.1 鍵管理サーバの要件 68
8.1.2 鍵管理サーバのルート証明書の取得 68
8.1.3 クライアント証明書の作成 68
8.2 暗号化環境の設定 69
8.2.1 鍵管理サーバの使用有無と暗号化環境の設定内容 69
8.2.2 暗号化環境を設定する 70
8.3 暗号化鍵を作成する 72
8.4 暗号化鍵のバックアップ 72
8.5 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 73
8.6 鍵管理サーバに接続して暗号化鍵をバックアップする 74
8.7 暗号化を有効にする 74
8.8 お問い合わせ先 74

付録 A このマニュアルの参考情報 75
A.1 操作対象リソースについて 76
A.2 このマニュアルで使用している略語 76
A.3 このマニュアルでの表記 76
A.4 KB（キロバイト）などの単位表記について 76

用語解説 77

索引 99

はじめに

このマニュアルでは、セキュリティ機能について説明しています。

- 対象ストレージシステム
- マニュアルの参照と適合プログラムバージョン
- 対象読者
- マニュアルで使用する記号について
- ユーザの操作権限（ロール）について
- REST API の管理ツールについて
- 発行履歴

対象ストレージシステム

このマニュアルでは、次に示す Hitachi Virtual Storage Platform One Block 80 の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。

- Hitachi Virtual Storage Platform One Block 85

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プログラムバージョン

このマニュアルは、次の DKCMAIN プログラムバージョンに適合しています。

A0-05-41-XX

メモ

- このマニュアルは、上記バージョンの DKCMAIN プログラムをご利用の場合に最も使いやすくなるよう作成されていますが、上記バージョン未満の DKCMAIN プログラムをご利用の場合にもお使いいただけます。
- 各バージョンによるサポート機能については、別冊の『バージョン別追加サポート項目一覧』を参照ください。

対象読者

このマニュアルは、次の方を対象読者として記述しています。

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

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、製品を安全にご使用いただくための注意書きを、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。

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

Virtual Storage Platform One Block 80 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、『VSP Block Storage 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	説明
シンプル 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	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。設定にはシンプル 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。

発行履歴

マニュアル資料番号	発行年月	変更内容
4051-1J-U68-10	2026 年 4 月	適合 DKCMAIN ファームウェアバージョン：A0-05-41-XX ・ Fibre Channel Board 32Gb V2 および Fibre Channel Board 64Gb V2 をサポートした。 　◦ 6 LUN Manager/Security ・ 製品表記の見直しによる修正をした。 　◦ A.3 このマニュアルでの表記
4051-1J-U68-00	2026 年 1 月	新規 適合 DKCMAIN ファームウェアバージョン：A0-05-21-XX

1

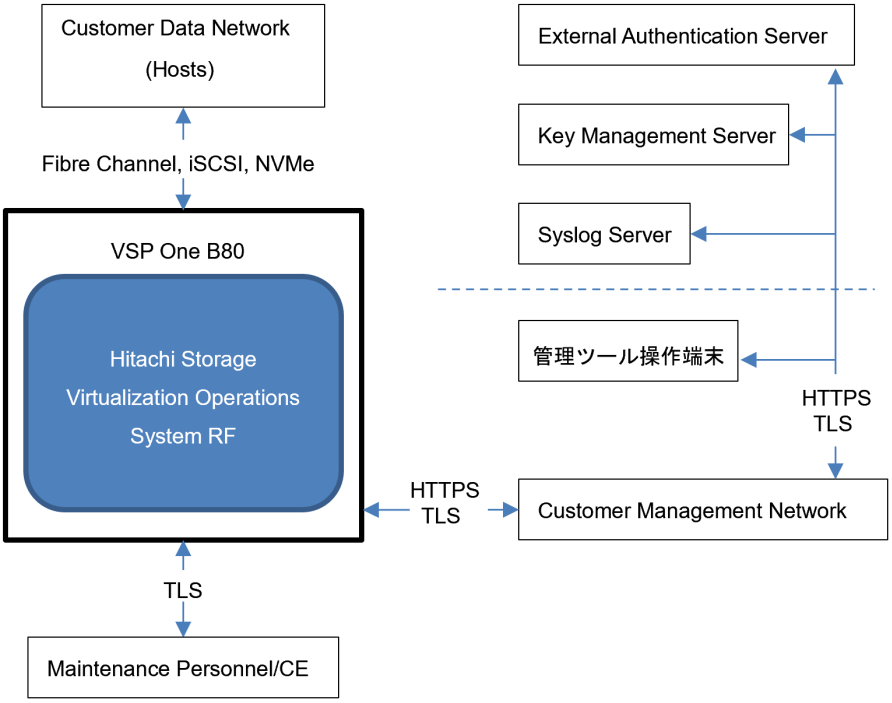
セキュリティ設定の概要

本章ではセキュリティ設定の概要について説明します。

- 1.1 概要
- 1.2 想定する利用者
- 1.3 主要セキュリティ機能
- 1.4 各管理ツールが利用するポート情報
- 1.5 最新のソフトウェアの適用

1.1 概要

本ストレージシステムでは、ユーザ認証・認可、監査ログによる追跡、データの暗号化など、セキュリティ機能が利用できます。



1.2 想定する利用者

以下のような利用者を想定しています。

- セキュリティ管理者
  セキュリティ管理者は、maintenance utility を使用して管理者アカウントの登録、変更、削除ができます。また、管理 LAN で使用する TLS のバージョン、暗号アルゴリズムを設定、変更することができます。
  また、リソースグループと呼ばれるストレージリソースの集合の管理権限を特定のユーザに割り当てることができます。その他、ホストの識別、格納データの暗号化操作を実施できます。
- ストレージリソース管理者
  maintenance utility を使用して、セキュリティ管理者に割り当てられたリソース（ポート、キャッシュメモリ、ドライブなど）を管理できる管理者。
- 監査ログ管理者
  本ストレージシステムで取得している監査ログを管理できる管理者。maintenance utility を用いて、監査ログの参照やダウンロード、および syslog に関する設定が可能です。
- 保守員
  本ストレージシステムを利用する顧客が保守契約を結んだ、保守専門の組織に所属する人。本ストレージシステムを設置する際の初期立上げ処理、部品の交換や追加などの保守作業に伴う設定変更、異常時の復旧処理などを担当します。

保守員は、保守員用の PC を使用し、本ストレージシステムの保守用ポートに接続して保守作業を実施します。直接、ストレージシステム内の機器に触ったり、内部 LAN に接続した機器を操作したりできるのは、保守員だけです。保守員はストレージシステム内のすべてのリソースが割り当てられていて保守員ロールで許可されている操作を実施できます。

- ストレージ利用者
  本ストレージシステムの利用者でホストを表します。本ストレージシステムと接続されたホストから、本ストレージシステムに保存されたデータを使用します。

以下、セキュリティ管理者、ストレージリソース管理者、監査ログ管理者をまとめて、ストレージ管理者と呼びます。

1.3 主要セキュリティ機能

本ストレージシステムが提供するセキュリティ機能の概要を以下に示します。

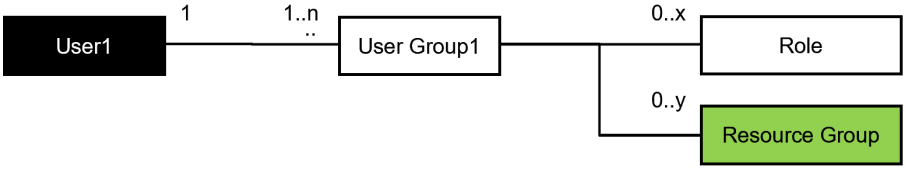
1.3.1 ストレージ管理者および保守員のアクセス制御機能

本ストレージシステム内に複数の会社・部署・システム・アプリケーションのデータが混在する大規模ストレージ集約環境では、ストレージの運用を会社ごと、部署ごとなどにストレージリソース管理者を設置し、分割して個別に管理する、いわゆるマルチテナンシ機能が必要になります。マルチテナンシ機能によって、資源の効率的利用によるコスト削減と、分割による管理容易化の実現が期待できます。

マルチテナンシ環境では、誤って他の組織のボリュームを壊さない、データが他の組織に漏洩しない、また他のストレージリソース管理者の操作に影響を及ぼさないなどのセキュリティ上の仕組みが必要となります。

ストレージ管理者および保守員のアクセス制御機能はユーザグループの単位で、ロール（権限）を付与し､そのロールで管理できるリソースの集合をリソースグループとして付与します。ユーザ(管理者)、ユーザグループ、リソースグループ、およびロールの対応関係を次の図に示します。

本機能によって、各ユーザに柔軟なリソース配置が行えるようにすると共に上述のセキュリティを実現します。



ユーザは、1 つ以上のユーザグループに所属します。ユーザグループは、ロールおよびリソースグループが割り当てられ、認可情報として使用します。ユーザグループの情報は本ストレージシステム内または外部認証サーバから取得して使用します。各アカウントは付与されたリソースに対してロールによって許可された管理操作だけを実行できます。

(1) ロール

セキュリティ管理者は、maintenance utility を使用してユーザアカウントを作成し、ユーザグループに登録します。

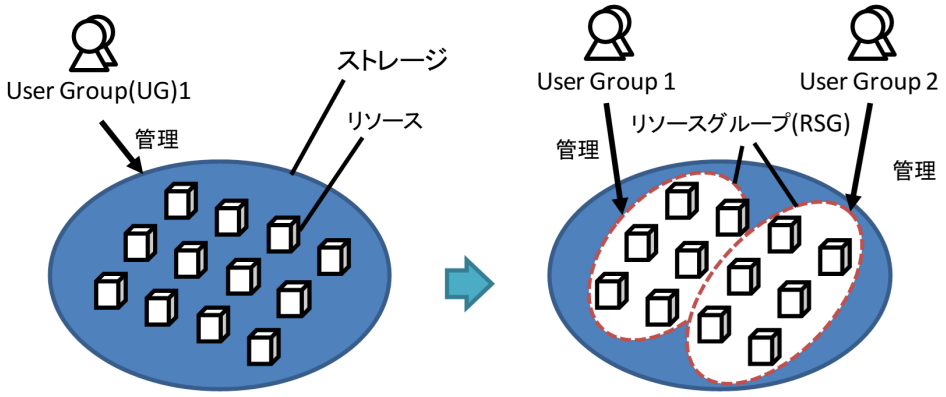
ユーザにどの操作を許可するかは、ユーザグループに付与されているロールで決定します。ロールには、次の分類があります。

ロールの分類と操作内容

ロール	実施可能な操作
セキュリティ管理者ロール	セキュリティ管理者に付与するロールで、ユーザ管理操作、リソース管理操作、ホストの識別設定操作、格納データ暗号化操作、外部認証サーバの管理が可能。
監査ログ管理者ロール	監査ログ管理者に付与するロールで、監査ログに関する操作が可能。
ストレージ管理者ロール	ストレージリソース管理者に付与するロールで、許可されたリソースグループ内のストレージ管理操作が可能。
保守員ロール	保守員に付与するロールで、ストレージシステムの保守操作が可能。

(2) リソースグループ

ストレージリソースを複数のグループに分割したものをリソースグループ（RSG）と呼びます。各リソースグループは番号（RSG 番号）を付与して識別します。また、リソースグループはユーザグループに割り当てられ、各ストレージリソース管理者は、自身の所属するユーザグループに割当てられたリソースグループの範囲で管理操作を行うことができます。保守員は、すべてのリソースグループが割当てられるため、すべてのストレージリソースに対して保守操作を実施できます。



1.3.2 ホストのアクセス制御機能

ユーザデータを格納する論理ボリューム（LDEV）は、VSP One Block Administrator を利用して生成されます。ホストから論理ボリューム（LDEV）へアクセスを行うためには、ホストを接続したポートと論理ボリューム（LDEV）の関連付けを行います。具体的には、ホストとアクセスを許可する論理ボリューム（LDEV）とを関係付ける LU 番号を付与して LU パスを設定します。当該の論理ボリューム（LDEV）に対するデータの読み書きは、LU パス設定が行なわれたホストからのみ可能となり、LU パス設定が行なわれていないホストからのデータの読み書きは許可されません。

1.3.3 ストレージ管理者および保守員の識別・認証機能

VSP One Block Administrator や maintenance utility は、顧客によって、セキュリティ機能の設定を含む本ストレージシステムの管理を行うために使用されます。VSP One Block Administrator を用いてストレージシステムの管理（各機能の構成の変更など）を行う場合、およびユーザや保守員が maintenance utility に接続する場合には、本ストレージシステムによってユーザの識別と認証が行われます。ストレージシステムの設定によって識別・認証に失敗した場合は、一時的なアカウントロックまたはアカウント無効化される場合があります。詳細は『システム管理者ガイド』を参照してください。

ユーザの認証方式には以下に示す 2 種類をサポートします。

- ストレージシステム内部認証方式
  本ストレージシステム内に利用者の ID とパスワードを登録し、認証する方式。利用者の認証に使用するパスワードは 6 文字から 256 文字（保守員のパスワードは 127 文字）の英数字、記号の組み合わせを可能としています。
- 外部認証サーバ方式
  本ストレージシステムで利用者の ID、パスワードを管理せず、外部に設置した認証サーバに ID とパスワードを送信して認証結果を受け取る方式。外部認証サーバで認証成功後に認証サーバからユーザグループ情報を取得し、認可情報として使用することもできます。利用者認証のプロトコルとして LDAP（暗号化は LDAPS）をサポートします。

1.3.4 管理ツールの操作端末とストレージシステム間およびストレージシステムと外部認証サーバ間の暗号通信

管理ツールの操作端末とストレージシステム間の通信データの漏洩、改ざんを防ぐために、通信は TLS によって暗号化します。また、ストレージシステムと外部認証サーバ間の通信は、LDAPS を使用することで、ストレージ管理者および保守員のパスワードを保護します。

1.3.5 格納データ暗号化機能

本ストレージシステムは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。暗号化および復号は、暗号モジュール（ENCM）を利用します。データを暗号化すると、ストレージシステム内のドライブを交換するとき、または、これらが盗難にあったときに情報の漏えいを防ぐことができます。また､以下の鍵管理機能が備わっています。

- 暗号鍵作成機能
- 暗号鍵削除機能
- 暗号鍵バックアップ、リストア機能
- 外部鍵管理サーバ連携機能（暗号鍵作成、バックアップ、リストア）

格納データ暗号化機能はセキュリティ管理者ロールを持ったユーザアカウントだけが実施できます。

1.3.6 監査ログ機能

監査ログ機能では、ログインの成功・失敗、構成や設定の変更などのセキュリティに関連するイベントを記録しています。

監査ログ 1 行あたりの最大文字数は、半角 1,024 文字で、Syslog サーバにリアルタイムで送付できます。また、そのコピーはストレージシステム（ESM）には最大 250,000 行分、ストレージシステム（DKC）には最大 300,000 行分の情報が格納されます。

maintenance utility は、監査ログを参照するインタフェースを提供します。

1.3.7 Media Sanitization 機能

Media Sanitization は、ダイナミックスペアリングの完了を契機に、ダイナミックスペアリングの要因となったドライブ（不具合が発生したドライブ）のアクセス可能な領域にゼロデータを書き込み、およびコンペアすることで、ドライブのデータを消去します。

Media Sanitization の有効化は保守員が行います。サポート窓口にお問い合わせください。

有効化されると自動で機能します。ユーザによる操作は不要です。

1.4 各管理ツールが利用するポート情報

各管理ツールで利用するポートは次のとおりです。

ストレージシステムのポートの設定は、『システム管理者ガイド』のネットワーク拒否設定の変更の操作手順を参照してください。

管理ツール	プロトコル	TCP/UDP	送信元（管理ツールの操作端末）ポート番号	送信先（ストレージシステム）ポート番号
• maintenance utility • VSP One Block Administrator • シンプル API • 詳細 API	HTTP※	TCP	any	80
	HTTPS	TCP	any	443
内蔵 CLI	SSH	TCP	any	20522
RAID Manager	『RAID Manager インストール・設定ガイド』			

注※

デフォルトは無効です。

1.5 最新のソフトウェアの適用

脆弱性対策は、最新のソフトウェアおよびマイクロプログラムで実施されます。最新のソフトウェアおよびマイクロプログラムの適用を定期的に実施してください。

2

物理セキュリティ

本章では物理セキュリティについて説明します。

- 2.1 運用環境の物理セキュリティについて

2.1 運用環境の物理セキュリティについて

- 組織の責任者は、ストレージ管理者のうち、セキュリティ管理者、監査ログ管理者には、本ストレージシステム全体の管理・運用を行うために十分な能力を持ち、手順書で定められたとおりの操作を行い、不正行為を働かないことを信頼できる人物を割り当てられなければなりません。
- 組織の責任者は、許可されたストレージ管理者のみが、許可された目的でのみ、本ストレージシステムに物理的にアクセスできるように適切に設置および管理しなければなりません。
- ストレージリソース管理者は、セキュリティ管理者から許可された範囲内で本ストレージシステムの管理・運用を行うため、手順書で定められたとおりの操作を行えるように研修が行われ、不正行為を働かないことを信頼できる人物が割り当てられなければなりません。
- セキュリティ管理者は、本ストレージシステム、ホスト（ファイバチャネル接続アダプタを含む)、SAN 環境を構成する機器（ファイバチャネルスイッチ、ケーブル）をストレージ管理者および保守員だけが入退出を許可されているセキュアなエリアに設置し、許可されていない設定値の変更や接続先の付け替えなどから完全に保護されていなければなりません。
- セキュリティ管理者は、外部認証サーバ、鍵管理サーバをセキュリティ管理者だけが許可されているセキュアなエリアに設置し、許可されていない設定値の変更や接続先の付け替えなどから完全に保護されていなければなりません。
- セキュリティ管理者は、外部認証サーバにストレージシステムとの通信を保護することができるプロトコル（LDAPS）を使用しなければなりません。また、ユーザ識別情報およびユーザグループ情報を本ストレージシステムと整合の取れた状態で適切に登録および管理しなければなりません。
- セキュリティ管理者は、保守員が使用する管理ユーザアカウント（maintenance アカウント）のパスワード変更を、初回の利用時に必ず行ってください。また、このときに変更したパスワードは、保守員が保守作業を行う際に必要となります。保守契約をされているお客様は、変更後のパスワードを日立サポートサービスに連絡してください。
- ストレージ管理者は､管理 PC が不正に利用されないように適切に設置および管理しなければなりません。
- 監査ログ管理者は、Syslog サーバを監査ログ管理者だけが入退室を許可されているセキュアなエリアに設置し、監査ログの改ざん・消去、許可されていない設定値の変更から完全に保護されていなければなりません。
- 運用環境では、ドライブからユーザデータが漏洩しないように、暗号モジュール（ENCM）を利用してユーザデータを暗号化できる Encryption License Key 機能を使用しなければなりません。

3

ユーザ管理と認証・認可

本章では、本ストレージシステムを使用するにあたり、ユーザ管理機能について説明します。

セキュリティ管理者は、事前にユーザ認証に認証サーバを使用するかどうかを決めておきます。認証サーバを使用する場合、ユーザはシステムで使用中のパスワードを使用して、maintenance utility や VSP One Block Administrator などの管理ツールにログインできます。認証サーバを使用しない場合は、管理ツール専用のパスワードを使用します。認証サーバを使用するかどうかは、ユーザごとに選択できます。

- 3.1 ビルトインアカウントのパスワード変更
- 3.2 ユーザ管理モデル
- 3.3 ユーザ管理
- 3.4 外部認証
- 3.5 TLS 通信機能

3.1 ビルトインアカウントのパスワード変更

ストレージシステムには、ビルトインアカウントが登録されています。

最初に、ビルトインユーザで maintenance utility にログインし、パスワードの変更を実施してください。ユーザ名は「maintenance」、パスワードは「raid-maintenance」です。ビルトインユーザには、全権限があります。

前提条件

- ユーザ認証に、認証サーバを使用していないこと

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザグループ］の一覧から、ビルトインアカウントが所属するユーザグループをクリックします。
4. ［ユーザ］タブのユーザ一覧から、ビルトインアカウントを選択します。
   （ユーザアカウントの左横にあるチェックボックスにチェックマークを入れます。）
5. ［編集］を選択します。
6. ユーザ編集画面が表示されます。各項目を入力します。
   各項目の詳細は、『システム管理者ガイド』のパスワードの変更を参照してください。

   メモ
   パスワードに設定可能な文字列は、パスワードポリシーに従う必要があります。詳細は「3.3.1 ユーザアカウントポリシーの設定」を参照してください。

7. 設定内容を確認し［完了］をクリックします。
8. 警告メッセージが表示された場合は、［OK］をクリックします。
9. 確認メッセージが表示されます。［適用］をクリックします。
10. 完了メッセージが表示されます。［閉じる］をクリックします。

3.2 ユーザ管理モデル

3.2.1 ユーザグループとロールおよびリソースグループの関係

セキュリティ管理者は、各管理ツールで使用できるユーザアカウントを作成し、ユーザグループに登録します。

ロールとユーザグループ

ユーザにどの操作を許可するかは、ロールで決まります。ロールは、ユーザごとではなくユーザグループごとに設定します。ユーザに許可する操作を変更するには、次の 2 つの方法があります。

- 適切なロールが割り当てられたユーザグループに、ユーザを所属させる。

- ユーザが所属しているユーザグループに割り当てられているロールを変更する。

リソースグループとユーザグループ

ユーザにどのリソースの操作を許可するかは、リソースグループで決まります。リソースグループは、ユーザごとではなくユーザグループごとに設定します。ユーザが操作できるリソースを変更するには、次の 2 つの方法があります。

- 適切なリソースグループが割り当てられたユーザグループに、ユーザを所属させる。
- ユーザが所属しているユーザグループに割り当てられているリソースグループを変更する。

リソースグループについての詳細は、『オープンシステム構築ガイド』または『メインフレームシステム構築ガイド』を参照してください。

ユーザ登録例

- システム全体のセキュリティに影響する設定操作は、管理者だけが実行。
- リソースグループ 10 のストレージ設定操作は、ユーザ A が実行。
- リソースグループ 20 のストレージ設定操作は、ユーザ B が実行。

上記のように運用したい場合は、次のようにユーザをユーザグループに所属させてください。

ユーザ	ユーザを所属させるユーザグループ	ユーザグループに割り当てるロール	ユーザグループに割り当てるリソースグループ
管理者	ユーザグループ 1	セキュリティ管理者（参照・編集）	全リソースグループ※1
ユーザ A	ユーザグループ 10	ストレージ管理者※2	リソースグループ 10
ユーザ B	ユーザグループ 20	ストレージ管理者※2	リソースグループ 20

注※1

セキュリティ管理者ロールを割り当てたユーザグループは、「全リソースグループ」が自動的に「該当」になります。

注※2

ストレージ管理者のロールは複数種類あります。

ユーザグループに関する注意事項

- ユーザを複数のユーザグループに所属させた場合、各ユーザグループのロールに許可されている操作が、各ユーザグループに割り当てられているどのリソースグループに対しても有効になります。
- 「全リソースグループ割り当て」が「該当」のユーザは、ストレージシステム内のすべてのリソースにアクセスできます。例えば、1 人の担当者がセキュリティ管理者と一部のリソースに対するストレージ管理者を兼ねる場合、1 つのユーザアカウントにセキュリティ管理者ロールおよびストレージ管理者ロールを割り当てると、すべてのリソースに対してストレージ編集操作が可能となります。
  このようなことが問題になる場合は、次の 2 つのユーザアカウントをストレージシステムに登録して、使い分けてください。
  - 「全リソースグループ割り当て」が「該当」であるセキュリティ管理者のユーザアカウント

- 「全リソースグループ割り当て」が「非該当」で、一部のリソースグループだけを割り当てるストレージ管理者のユーザアカウント

1 人のユーザが複数のユーザグループを使い分けたい場合は、認証サーバを使用せずに、ストレージシステム専用のユーザアカウントを作成してください。

- セキュリティ管理者、監査ログ管理者および保守のロールを割り当てたユーザグループは、全リソースグループが自動的に「該当」になります。これらのロールをすべて削除した場合、全リソースグループが自動的に「非該当」になるため、リソースグループを割り当て直してください。

3.2.2 ロールと許可されている操作

ロールは、ストレージシステムに対してユーザが操作できる項目を規定するためのグループです。

ロールは、ストレージシステム内にあらかじめ用意されており、独自に作成できません。

ロール	操作できる項目
ストレージ管理者（参照）	• ストレージシステムに関する情報の参照
ストレージ管理者（初期設定）	• ストレージシステムに関する情報の設定 • SNMP の設定 • Email 通知機能に関する設定 • ライセンスキーの設定
ストレージ管理者（システムリソース管理）	• MP ユニットの設定 • リソース排他の強制解除 • LUN セキュリティの設定 • リモートコピーの操作全般 • ポート属性の設定
ストレージ管理者（プロビジョニング）	• キャッシュの設定 • LDEV、プール、仮想ボリュームの設定 • LDEV のフォーマット • 外部ボリュームの設定 • Dynamic Provisioning に関する設定 • ホストグループ、パス、WWN の設定 • NVM サブシステム、Namespace、パス、ホスト NQN の設定 • Volume Migration の設定（RAID Manager を使用した場合の Volume Migration ペアの削除を除く） • LDEV のアクセス属性の設定 • LUN セキュリティの設定 • Namespace セキュリティの設定 • global-active device で使用する Quorum ディスクの作成、削除 • global-active device ペアの作成および削除 • Compatible PAV のエイリアスボリューム設定
ストレージ管理者（ローカルバックアップ管理）	• ローカルコピーのペア操作 • ローカルコピー用の環境設定 • Volume Migration のペア解除

ロール	操作できる項目
ストレージ管理者（リモートバックアップ管理）	• リモートコピーの操作全般 • global-active device ペアの操作（作成および削除を除く）
ストレージ管理者（パフォーマンス管理）	• エクスポートツール 2 の操作
セキュリティ管理者（参照）	• ユーザアカウントおよび暗号設定に関する情報の参照 • maintenance utility による外部認証の情報参照 • セッションタイムアウト時間の参照 • コモンクライテリア認証設定の参照 • TLS セキュリティ設定の参照
セキュリティ管理者（参照・編集）	• ユーザアカウントの設定 • ユーザアカウントポリシーの設定 • maintenance utility による外部認証の設定 • 暗号鍵の生成と削除 • 暗号の設定 • 暗号鍵のバックアップ、リストア • 外部サーバへの接続設定 • SSL/TLS 通信で使用する証明書の設定 • コモンクライテリア認証の設定 • リソースグループの設定 • 仮想管理設定の編集 • CSR 作成および自己署名証明書作成 • global-active device の予約属性の設定 • セッションタイムアウト時間の編集 • TLS セキュリティ設定の変更
監査ログ管理者（参照）	• 監査ログに関する画面の参照、および監査ログのダウンロード
監査ログ管理者（参照・編集）	• 監査ログに関する設定、および監査ログのダウンロード
保守（ベンダ専用）	• ベンダ保守に関する操作（通常日立の保守員が実施する操作です。）
保守（ユーザ）	• 装置状態の参照 • 簡易の保守操作 • SIM のコンプリート

3.2.3 ビルトイングループ

ユーザグループは、あらかじめ複数用意されています（ビルトイングループ）。ビルトイングループに設定されているロールおよびリソースグループの設定は変更できません。ビルトイングループと、設定されているロールおよびリソースグループを次に示します。

リソースグループについての詳細は、『オープンシステム構築ガイド』または『メインフレームシステム構築ガイド』を参照してください。

ビルトイングループに設定されているロールを次の表に示します。

ビルトイングループ	ロール	リソースグループ
Storage Administrator (View Only)	• ストレージ管理者（参照）	meta_resource
Storage Administrator (View & Modify)	• ストレージ管理者（初期設定） • ストレージ管理者（システムリソース管理） • ストレージ管理者（プロビジョニング） • ストレージ管理者（パフォーマンス管理） • ストレージ管理者（ローカルバックアップ管理） • ストレージ管理者（リモートバックアップ管理）	meta_resource
Audit Log Administrator (View Only)	• 監査ログ管理者（参照） • ストレージ管理者（参照）	全リソースグループ
Audit Log Administrator (View & Modify)	• 監査ログ管理者（参照・編集） • ストレージ管理者（参照）	全リソースグループ
Security Administrator (View Only)	• セキュリティ管理者（参照） • 監査ログ管理者（参照） • ストレージ管理者（参照）	全リソースグループ
Security Administrator (View & Modify)	• セキュリティ管理者（参照・編集） • 監査ログ管理者（参照・編集） • ストレージ管理者（参照）	全リソースグループ
Administrator	• セキュリティ管理者（参照・編集） • 監査ログ管理者（参照・編集） • ストレージ管理者（初期設定） • ストレージ管理者（システムリソース管理） • ストレージ管理者（プロビジョニング） • ストレージ管理者（パフォーマンス管理） • ストレージ管理者（ローカルバックアップ管理） • ストレージ管理者（リモートバックアップ管理）	全リソースグループ
System	• セキュリティ管理者（参照・編集） • 監査ログ管理者（参照・編集） • ストレージ管理者（初期設定） • ストレージ管理者（システムリソース管理） • ストレージ管理者（プロビジョニング） • ストレージ管理者（パフォーマンス管理） • ストレージ管理者（ローカルバックアップ管理） • ストレージ管理者（リモートバックアップ管理）	全リソースグループ
Maintenance User	• ストレージ管理者（参照） • 保守（ユーザ）	全リソースグループ
Support Personnel	• ストレージ管理者（初期設定） • ストレージ管理者（システムリソース管理） • ストレージ管理者（プロビジョニング）	全リソースグループ

ビルトイングループ	ロール	リソースグループ
	• ストレージ管理者（パフォーマンス管理） • ストレージ管理者（ローカルバックアップ管理） • ストレージ管理者（リモートバックアップ管理） • 保守（ベンダ専用） • 保守（ユーザ）	

3.3 ユーザ管理

maintenance utility にビルトインアカウントでログインし、装置利用に必要なユーザを登録します。

ユーザは、下記 4 つを登録することを推奨します。

- Security Administrator(View & Modify)グループに属するセキュリティ管理者
- Audit Log Administrator(View & Modify)グループに属する監査ログ管理者
- Storage Administrator(View & Modify)グループに属するストレージリソース管理者
- Support Personnel グループに属する保守員

3.3.1 ユーザアカウントポリシーの設定

ユーザアカウントは、ユーザ定義のパスワードとログイン要件によって不正利用から保護されています。セキュリティ管理者は、maintenance utility でユーザアカウントのユーザアカウントポリシーを有効にして、要件を設定できます。ユーザアカウントのパスワードポリシーは、ストレージシステム全体だけでなく、ユーザ個別にも適用できます。

パスワードポリシーで、初回ログイン時のパスワード変更を設定している場合は、初回ログイン時にパスワード変更を要求する画面が表示されます。また、パスワードの有効期限を設定している場合は、パスワードの有効期限が 14 日以内になると、ログイン時に有効期限に関するメッセージが表示されます。

ユーザ個別のパスワードポリシー状態は、ユーザアカウントのバックアップファイルに含まれています。バックアップファイルを使用してユーザ情報をリストアする場合に、ファイルの情報が古くパスワードの有効期限が切れていると、ユーザアカウントは無効化されます。その場合は、セキュリティ管理者がアカウントを有効化する必要があります。

ユーザアカウントのセキュリティイベントは、ストレージシステムの監査ログに記録されます。ただし、次の 3 つのイベントは、監査ログに記録されません。

- パスワードの有効期限が切れた場合のアカウントの無効化
- ログイン試行の最大回数を超えた場合のアカウントの無効化またはアカウントロック
- ロックアウトモードがアカウントロックの場合に、時間経過でアカウントロックが解除された場合

パスワードの有効期限を設定する場合の注意点を示します。

- maintenance utility は、パスワードの期限が切れる 30 日前、および 14 日前から当日までの間、パスワードの期限切れを警告する SIM（SIM リファレンスコード「7c21*xx*」）を、00:30 に送信します。*xx* は、パスワードの期限が切れるまでの日数を、16 進数(Hex)で示しています。

この SIM を受信した場合は、パスワードを変更（「3.3.5 パスワードの変更」を参照）またはパスワードの有効期間を無期限に変更（「(5)　ユーザ個別のパスワードポリシーの適用」を参照）してください。

- パスワードの期限が切れる当日までに上記の対処を行わないと、maintenance utility は、パスワードの期限が切れたことを示す SIM（SIM リファレンスコード「7c2200」）を、翌日の 00:00 に送信します。この SIM を受信した場合は、ユーザアカウントを、再度有効に設定（「(9)　アカウントの有効化」を参照）してください。この操作は、セキュリティ管理者（参照・編集）ロールを持つユーザアカウントで行ってください。このユーザアカウントが不明な場合は、保守員まで連絡ください。

(1)　ユーザアカウントポリシーを利用する場合のユーザ管理

ユーザアカウントポリシーを利用する場合は、ユーザ管理の各設定に使用する管理ツール（インターフェース）が異なります。VSP One Block Administrator を利用する構成では、各設定と指定の管理ツールを、次の表に示します。

ユーザアカウントポリシー利用時の、ユーザ管理操作と管理ツールの指定

システム管理者による ユーザ管理操作	VSP One Block Administrator を利用する構成
ユーザアカウント管理	maintenance utility※1
他のユーザのパスワード変更	
ユーザアカウントポリシー	
リソースグループ管理	RAID Manager または詳細 API
ユーザグループ管理	詳細 API
初回ログインのパスワード変更※2	maintenance utility※1
自分自身のパスワード変更	

システム管理者以外による ユーザ管理操作	VSP One Block Administrator を利用する構成
初回ログインのパスワード変更※2	maintenance utility※1
自分自身のパスワード変更	

注※1

管理ツールの操作端末から IP アドレスを直接指定して起動してください。詳細は『システム管理者ガイド』の各ツールのログイン方法を参照してください。

注※2

ユーザアカウントポリシーの設定状態によっては、対象ユーザの初回ログイン時にパスワード変更が求められる場合があります。詳細は「(2)　ユーザアカウントのパスワードポリシー設定」および「(5)　ユーザ個別のパスワードポリシーの適用」を参照してください。

ユーザ管理操作に指定とは異なる管理ツールを使用した場合の注意事項

ユーザ管理操作	VSP One Block Administrator を利用する構成で、 maintenance utility 以外から操作した場合
初回ログインのパスワード変更	[初回ログイン時にパスワード変更を要求する] を設定済みのユーザの場合は、maintenance utility を除く全インターフェ

ユーザ管理操作	VSP One Block Administrator を利用する構成で、maintenance utility 以外から操作した場合
	ースからログインができなくなります。VSP One Block Administrator にログインを試みた際は、メッセージとともに maintenance utility のログイン画面へのリンクが表示されます。

(2) ユーザアカウントのパスワードポリシー設定

ユーザアカウントのパスワードポリシーを設定します。この設定は、ストレージシステム全体に適用されます。

注意

- パスワード有効期限が切れたユーザはログインができなくなります。
- パスワードの有効期限が切れないようにするには、パスワードの有効期限が切れる日の 23 時 59 分までに、パスワードを変更する必要があります。パスワードの有効期限が切れた場合は、セキュリティ管理者がそのユーザアカウントを有効にしてパスワードをリセットする必要があります。 詳細は「(9) アカウントの有効化」を参照してください。
- セキュリティ管理者（参照・編集）ロールを持つ最後のユーザは、パスワード有効期限が切れた場合でも継続してログインできます。
- セキュリティ管理者（参照・編集）ロールを持つ最後のユーザが複数で、同時にパスワード有効期限が切れた場合でも、この複数のユーザは継続してログインできます。
- セキュリティ管理者（参照・編集）ロールを持つユーザの場合、パスワード変更禁止期間内でも、他のユーザについて、パスワード変更を実施できます。
- パスワード文字数は使用する管理ツールによって制限があります。複数の管理ツールを使用する場合は、どの管理ツールにも適用可能な範囲でパスワードポリシーを設定してください。各管理ツールのパスワード文字数制限については、「ユーザ名とパスワードの文字数と使用可能文字」を参照してください。
- ユーザアカウントポリシーと、各ユーザアカウントに対して、異なるパスワードの有効日数を設定できます。なお、ユーザアカウントポリシーに設定する有効日数を変更すると、変更された日数分が、各ユーザアカウントのパスワードの有効日数に反映されます。例えば、あるユーザアカウントのパスワードの有効日数が 50 日（250 日を設定してから 200 日が経過）の場合、ユーザアカウントポリシーの有効日数を 350 日から、250 日に変更すると（有効日数を 100 日少なくなるように変更）、ユーザアカウントの有効日数も 100 日少なくなるように変更されるため、ユーザアカウントのパスワードの有効期限が、すでに 50 日超過しているものとして扱われます。これによって、ユーザアカウントポリシーの有効日数を変更した翌日の 00:00 に、このユーザアカウントは無効化されます。上記のような不具合を回避するため、ユーザアカウントポリシーにパスワードの有効日数を設定する際は、各ユーザアカウントに対しても、同じパスワードの有効日数に設定することを推奨します。

メモ

- ストレージシステム全体でのパスワードポリシー設定後、既存のユーザにはパスワードポリシーは適用されていません。既存のユーザにパスワードポリシーを適用するためには、パスワードポリシーの設定後に、対象ユーザのパスワードを変更する必要があります。ユーザ個別でのパスワードポリシーの適用方法は、「(5) ユーザ個別のパスワードポリシーの適用」 を参照してください。
- パスワードポリシー変更前のパスワードが、変更後のパスワードポリシーに従わなくなった場合でも、対象ユーザのパスワードを変更するまでは、変更前のパスワードを使用できます。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。

2. ［管理］－［ユーザアカウントポリシー］を選択します。
3. ［ユーザアカウントポリシー］画面で、［設定］をクリックします。
4. ［ユーザアカウントポリシー設定］画面で、［Policy］タブを選択します。
5. 各項目を入力します。

   初期設定時には、各項目にはデフォルト値が表示されます。デフォルト値は、パスワードポリシー設定前とは異なります。

［Policy］タブ

パスワードポリシー

項目		説明	デフォルト値
最小文字数	数字（0-9）	パスワードの最小文字数（数字（0-9））を設定します。 ・ ［0-256］：ユーザアカウントのパスワードに含める最小数字数	0
	英大文字（A-Z）	パスワードの最小文字数（英大文字（A-Z））を設定します。 ・ ［0-256］：ユーザアカウントのパスワードに含める最小英大文字数	0
	英小文字（a-z）	パスワードの最小文字数（英小文字（a-z））を設定します。 ・ ［0-256］：ユーザアカウントのパスワードに含める最小英小文字数	0
	記号	パスワードの最小文字数（記号）を設定します。 ・ ［0-256］：ユーザアカウントのパスワードに含める最小記号数	0
	合計	パスワードの最小文字数（合計）を設定します。 ・ ［6-256］：ユーザアカウントのパスワードに含める最小文字数	8
利用可能なキーワードを制限する		自分のユーザ名をパスワードに含むことを制限します。 ・ ［はい］：ユーザ名の使用を制限します。 ・ ［いいえ］：ユーザ名の使用を制限しません。	いいえ
再利用を禁止するパスワードの履歴数		再利用を禁止するパスワードの履歴数を設定します。1 を設定した場合は、変更前のパスワードの再利用を禁止します。 ・ ［1-10］：再利用を禁止するパスワードの履歴数	1
初回ログイン時にパスワード変更を要求する		初回ログインパスワード変更要求を設定します。 ・ ［はい］：初回ログイン時にパスワード変更を要求します。 ・ ［いいえ］:初回ログイン時にパスワード変更を要求しません。	はい
パスワード変更禁止期間（日）		パスワード変更禁止期間を設定します。 ・ ［0-10］：パスワード変更禁止期間の日数	0
パスワード有効期間（日）		パスワード有効期間を設定します。パスワード変更禁止期間よりも長い日数を設定してください。 ・ ［1-365］：有効期間の日数 ・ ［空白］：無期限	42

ロックアウトポリシー

項目	説明	デフォルト値
ロックアウトモード	ログイン失敗が設定した回数を超過した場合の動作を設定します。 ・ ［アカウントロック］：アカウントをロックします。 ・ ［アカウント無効化］：アカウントを無効化します。	アカウントロック
ログイン試行可能回数	ログイン試行回数を設定します。 ・ ［1-999］：ログイン試行回数 ・ ［空白］：無制限	3
ロックアウト期間（秒）	アカウントロック期間を設定します。 ・ ［60-345600］：アカウントロック期間	60

6. 設定内容を確認して、［適用］をクリックします。
7. 完了メッセージが表示されます。［OK］をクリックします。

(3) メールサーバの設定

パスワードの有効期限が間近な場合や有効期限切れの場合のメール通知に利用する、メールサーバを設定します。メールサーバの設定が完了したら、テストメールを送信して、設定が正しいことを確認してください。テストメール送信の詳細は「(4) テストメールの送信」を参照してください。

前提条件

・ 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザアカウントポリシー］を選択します。
3. ［ユーザアカウントポリシー］画面で、［設定］をクリックします。
4. ［ユーザアカウントポリシー設定］画面で、［Email］タブを選択します。
5. 各項目を入力します。

［Email］タブ

項目		説明
Email 設定		パスワード有効期限に間近、または有効期限切れをメールで通知するかどうかを選択します。 ・ ［有効］：メールで通知します。 ・ ［無効］：メールで通知しません。
メールサーバ設定	メールサーバ	メールサーバの情報を設定します。［Email 設定］で［有効］を選択した場合は、設定してください。 ・ ［Identifier］：ホスト名を指定します。 ・ ［IPv4］：IPv4 アドレスを指定します。 ・ ［IPv6］：IPv6 アドレスを指定します。IPv6 アドレスの省略形も設定できます。
	SMTP 認証	SMTP 認証をするかどうかを選択します。 ・ ［有効］：SMTP 認証をします。 ・ ［無効］：SMTP 認証をしません。

項目		説明
	アカウント	SMTP 認証で使用するアカウントを設定します。［SMTP 認証］で［有効］を選択した場合は設定してください。 • 文字数：255 文字まで • 使用可能文字：半角英数字と記号（" ¥ ; : , * ? < > | / # & + = [ ] ' { } ^ とスペースを除く）
	パスワード	SMTP 認証で使用するパスワードを設定します。［SMTP 認証］で［有効］を選択した場合は設定してください。 • 文字数：255 文字まで • 使用可能文字：半角英数字と記号（" ¥ ; : , * ? < > | / # & + = [ ] ' { } ^ とスペースを除く）
メールアドレス（From）		送信元のメールアドレスを指定します。 • 文字数：255 文字まで • 使用可能文字：半角英数字と記号（" ( ) , : ; < > [¥] とスペースを除く）
メールアドレス（Reply To）		返信先のメールアドレスを指定します。このアドレスを指定すると、メール受信者からの返信先メールアドレスを指定します。この設定を省略すると、メール受信者からの返信はメールアドレス（From）に送信されます。 • 文字数：255 文字まで • 使用可能文字：半角英数字と記号（" ( ) , : ; < > [¥] とスペースを除く）
テスト送信メールアドレス		パスワード有効期限に間近、または有効期限切れのメール通知をテストする送信先のメールアドレスを指定します。 • 文字数：255 文字まで • 使用可能文字：半角英数字と記号（" ( ) , : ; < > [¥] とスペースを除く）

6. 設定内容を確認して、［適用］をクリックします。
7. 完了メッセージが表示されます。［OK］をクリックします。

(4) テストメールの送信

パスワードの有効期限が間近な場合や有効期限切れの場合のメール通知に利用するメールサーバの設定を確認するために、テストメールを送信します。

前提条件

- ユーザアカウントポリシーで、［テスト送信メールアドレス］が指定されていること。
- 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. maintenance utility にログインします。
2. ［管理］－［ユーザアカウントポリシー］を選択します。
3. ［ユーザアカウントポリシー］画面で、［設定］をクリックします。
4. ［ユーザアカウントポリシー設定］画面で、［Email］タブを選択して画面下の［テスト Email 送信］クリックします。
5. 完了メッセージが表示されます。［OK］をクリックします。
6. 宛先として指定したメールアドレスに、テストメールが到着したことを確認します。

テストメールには下記の情報が含まれています。

Email のフォーマット

名称	内容
Date	メールが発行された日時
To	メールの送信先アドレス
From	メールの送信元アドレス
Reply-To	メールの返信先アドレス
Subject	メールのタイトル
User Name	通知の送信先ユーザ名
Detail	メールの通知理由
Serial Number	ストレージシステムのシリアル番号
Action	対処方法
URL（IPv4）	maintenance utility の URL（IPv4）
URL（IPv6）	maintenance utility の URL（IPv6）

(5) ユーザ個別のパスワードポリシーの適用

パスワードポリシーを、ユーザ個別に適用するかどうかを設定します。

注意

- 保守員の初回ログイン時にパスワード変更要求画面が表示されないように、保守員用アカウント（maintenance）には［初回ログイン時にパスワード変更を要求する］で［いいえ］を選択してください。または、初回ログイン時のパスワード変更を、システム管理者が実施してください。
- ストレージシステムシステム全体でのパスワードポリシー設定後、既存のユーザにはパスワードポリシーは適用されていません。既存のユーザにパスワードポリシーを適用するためには、パスワードポリシーの設定後に、対象ユーザのパスワードを変更する必要があります。
- パスワードポリシー変更前のパスワードが、変更後のパスワードポリシーに従わなくなった場合でも、対象ユーザのパスワードを変更するまでは、変更前のパスワードを使用できます。
- maintenance utility 以外を利用するユーザの場合、初回ログイン時とパスワード有効期限が切れた場合に認証エラーとなります。初回ログイン時のパスワード変更と有効期限前のパスワード変更は maintenance utility で実施してください。

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. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザグループ］画面で、対象ユーザが存在する［ユーザグループ］を選択します。
4. ［ユーザ］タブのユーザ一覧から、パスワードを変更したいユーザアカウントの左横にあるチェックボックスをチェックします。
5. ［編集］をクリックします。
6. ［ユーザ編集］画面で、［新しいパスワード］と［パスワード再入力］に新規のパスワードを入力します。
7. 次の項目を選択します。

項目	説明
初回ログイン時にパスワード変更を要求する	初回ログイン時のパスワード変更要求を設定します。 • ［はい］：初回ログイン時にパスワード変更を要求します。 • ［いいえ］：初回ログイン時にパスワード変更を要求しません。
パスワード有効期間	パスワード有効期間（日）（ユーザ単位）を設定する。 • ［システムポリシーに従う］：ユーザアカウントポリシーの設定に従います。 • ［無制限］：設定しません（無期限）。

8. パスワードの有効期間に間近な場合や有効期限切れの場合の通知メールの設定は、「(6)　ユーザ個別のメールアドレスの設定」を参照し、Email アドレスを入力します。
9. 設定内容を確認し、［完了］をクリックします。
10. 警告メッセージが表示された場合は、［OK］をクリックします。
11. 確認メッセージが表示されます。［適用］をクリックします。
12. 完了メッセージが表示されます。［閉じる］をクリックします。

(6)　ユーザ個別のメールアドレスの設定

パスワードの有効期限に間近な場合や有効期限切れの場合にユーザに通知する、メールアドレスを設定します。

本項目の設定と 「(3)　メールサーバの設定」によって、「パスワード有効期限切れ切迫・有効期限切れ」の通知メールを配信できるようになります。

メモ

- パスワードの有効期限が間近な場合は、通知メールは以下の時期から配信されます。
  - 有効期限が切れる日付の 30 日前に 1 回
  - 有効期限が切れる日付の 14 日前から 1 日前まで 1 日 1 回
- パスワードの有効期限切れの場合は、通知メールは以下の時期に配信されます。
  - 有効期限超過時に 1 回
- パスワードの有効期限に間近な場合や有効期限切れの場合に通知されるメールは、毎日 0 時 30 分に 1 回配信されます。配信に失敗した場合は、0 時 45 分に再送されます。再送にも失敗した場合は、メール送信に失敗したことを知らせる SIM（7c2000）が送信されます。SIM が送信された場合は、次の項目を確認して不具合を訂正してください。
  - 「(3)　メールサーバの設定」で設定した内容
  - 『システム管理者ガイド』の maintenance utility の操作時にトラブルが発生した場合の対処方法に示す障害内容と対処方法

  訂正完了後、「(4)　テストメールの送信」を実施し、メールが送信できることを確認してください。

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. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザグループ］画面で、対象ユーザが存在するユーザグループを選択します。
4. ［ユーザ］タブのユーザ一覧から、メールアドレスを設定したいユーザアカウントの左横にあるチェックボックスをチェックします。
5. ［編集］をクリックします。

6. ［ユーザ編集］画面で、メールアドレスを設定します。

項目	説明
Email アドレス	パスワードの有効期限に間近な場合や有効期限切れの場合にユーザに通知する、メールアドレスを設定します。 ・ 文字数：255 文字まで ・ 使用可能文字：半角英数字と記号（! # $ % & ` + - * / ' ^ { } _ . @ ~ = ? | ）

7. 設定内容を確認して、［完了］をクリックします。
8. 完了メッセージが表示されます。［OK］をクリックします。

(7) ユーザアカウント状態の確認

対象ユーザのアカウント状態を確認します。アカウント状態には、アカウントロック、無効、有効の 3 種類があります。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザグループ］画面で、対象ユーザが存在するユーザグループを選択します。
4. ［ユーザ］タブのユーザ一覧で、対象ユーザの［アカウント状態］列を確認します。
   - ［Locked］が表示されている場合は、対象ユーザのアカウントはアカウントロックされている状態です。
   - ［Disabled］が表示されている場合、対象ユーザのアカウントは無効化された状態です。
   - ［Enabled］が表示されている場合、対象ユーザのアカウントは有効な状態です。

(8) アカウントロックの解除

ユーザアカウントポリシーのロックアウトモードがアカウントロックに設定された場合は、ログイン試行回数を超えた際に、指定した期間、アカウントがロックされます。

アカウントロック期間内にアカウントロックを解除したい場合は、ユーザのパスワードを変更することでロックを解除できます。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザグループ］画面で、対象ユーザが存在するユーザグループを選択します。
4. ［ユーザ］タブのユーザ一覧から、アカウントロックを解除したいユーザアカウントの左横にあるチェックボックスをチェックします。
5. ［編集］をクリックします。
6. ［ユーザ編集］画面で、［新しいパスワード］と［パスワード再入力］に新規のパスワードを入力します。

メモ　設定するパスワードは、設定したパスワードポリシーに従う必要があります。詳細は「(2)　ユーザアカウントのパスワードポリシー設定」を参照してください。

7. 設定内容を確認して、[完了] をクリックします。
8. 警告メッセージが表示された場合は、[OK] をクリックします。
9. 確認メッセージが表示されます。[適用] をクリックします。
10. 完了メッセージが表示されます。[閉じる] をクリックします。

(9)　アカウントの有効化

ユーザアカウントポリシーのロックアウトモードがアカウント無効化に設定された場合は、ログイン試行回数を超えた際に、アカウントが無効化されます。また、パスワードの有効期限切れの際にも、アカウントが無効化されます。無効化されたアカウントは、有効化することができます。管理者が無効化したアカウントも、この手順で有効化できます。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。
2. [管理] ー [ユーザ管理] を選択します。
3. [ユーザグループ] 画面で、対象ユーザが存在するユーザグループを選択します。
4. [ユーザ] タブのユーザ一覧で、有効化したいユーザアカウントの左横にあるチェックボックスをチェックします。
5. [編集] をクリックします。
6. [ユーザ編集] 画面で、[アカウント状態] の [有効] をクリックします。
7. パスワードの有効期限切れの場合は、[新しいパスワード] と [パスワード再入力] に新規のパスワードを入力します。他の場合はパスワードの再設定は不要です。

メモ
パスワードの有効期限切れで、新規パスワードを入力しない場合は、アカウントを有効化した翌日の 0 時 0 分に、パスワードが再度有効期限切れになります。

8. 設定内容を確認して、[完了] をクリックします。
9. 確認画面が表示されます。設定内容を確認し [適用] をクリックします。
10. 完了メッセージが表示されます。[閉じる] をクリックします。

3.3.2 ユーザの作成

ユーザを作成し、適切な権限が設定されたユーザグループに登録する方法について説明します。作成できるユーザ数は、ビルトインユーザを含めて最大 512 です。

ユーザ名とパスワードの文字数と使用可能文字

ユーザアカウントとパスワードは使用する管理ツールによって文字数と使用可能文字が異なります。複数のツールを使用する場合は、どのツールにも適用可能な範囲で指定してください。

ユーザアカウントの制限

管理ツール	制限	
maintenance utility	文字数	半角 256 文字以内
	使用可能文字	半角英数字および下記の記号 ! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~
内蔵 CLI	文字数	半角 256 文字以内
	使用可能文字※1	半角英数字および下記の記号 - . @ _ ! # $ % & ' * + = ? ^ ` { | } ~
RAID Manager	文字数	半角 63 文字以内
	使用可能文字※2	半角英数字および下記の記号 - . @ _ /
• VSP One Block Administrator • 詳細 API	文字数	半角 256 文字以内
	使用可能文字※3	半角英数字および下記の記号 ! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~
エクスポートツール 2	文字数	半角 256 文字以内
	使用可能文字	半角英数字および下記の記号 ! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~

注※1

内蔵 CLI にアクセスする操作端末の機種によっては、一部の記号に対して、エスケープが必要となる場合があります。

注※2

RAID Manager サーバの OS が Windows の場合、スラッシュ（/）は使用できません。

注※3

VSP One Block Administrator からコマンドコンソールを使用する場合、スラッシュ（/）は使用できません。

パスワードの制限

管理ツール	制限※1	
maintenance utility	文字数	半角 6～256 文字以内
	使用可能文字	半角英数字 ASCII 文字でキーイン可能なスペース以外のすべての記号
• 内蔵 CLI • RAID Manager	文字数	半角 6～63 文字以内
	使用可能文字※2	半角英数字および下記の記号 - . @ _ , :
• VSP One Block Administrator • 詳細 API	文字数	半角 6～63 文字以内
	使用可能文字	ASCII 文字でキーイン可能なスペース以外のすべての記号
エクスポートツール 2	文字数	半角 6～63 文字以内
	使用可能文字	ASCII 文字でキーイン可能なスペース以外のすべての記号

注※1

使用できる文字数および文字列はパスワードポリシーによって異なります。詳細は「(2) ユーザアカウントのパスワードポリシー設定」を参照してください。

注※2

内蔵 CLI または、RAID Manager がインストールされているホストの OS が UNIX の場合、スラッシュ（/）も指定できます。また、RAID Manager がインストールされているホストの OS が Windows の場合、円マーク（¥）も指定できます。

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザグループ］－［ユーザ作成］または［ユーザ］－［作成］を選択します。
4. ユーザ作成画面が表示されます。各項目を入力します。
   各項目の詳細は、『システム管理者ガイド』のユーザアカウントの作成を参照してください。
5. 設定内容を確認し［完了］をクリックします。
6. 確認画面が表示されます。設定内容を確認し［適用］をクリックします。
7. 完了メッセージが表示されます。［閉じる］をクリックします。

3.3.3 ユーザアカウントの削除

長期間使用されていないユーザアカウントを削除できます。ただしビルトインアカウント（maintenance）は削除できません。ログイン中のユーザのユーザアカウントを削除しても、ログアウトするまで、そのユーザは maintenance utility を含む管理ツールを利用できます。

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザ］タブのユーザ一覧から、削除したいユーザアカウントを選択します。
   （ユーザアカウントの左横にあるチェックボックスにチェックマークを入れます。）
4. ［削除］を選択します。
5. ユーザ削除画面が表示されます。
   ユーザアカウントを確認し［適用］をクリックします。
6. 完了メッセージが表示されます。［閉じる］をクリックします。

3.3.4 ユーザアカウントの無効化

無効にしたいユーザアカウントとは別のアカウントで操作してください（自分自身を無効にできません）。ビルトインアカウント（maintenance）も無効化できます。

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザ］タブのユーザ一覧から、無効化したいユーザアカウントを選択します。

（ユーザアカウントの左横にあるチェックボックスにチェックマークを入れます。）

4. ［編集］を選択します。
5. ユーザ編集画面が表示されます。
   ［アカウント状態］の［無効］を選択します。
6. 設定内容を確認し［完了］をクリックします。
7. 確認画面が表示されます。設定内容を確認し［適用］をクリックします。
8. 完了メッセージが表示されます。［閉じる］をクリックします。

3.3.5 パスワードの変更

前提条件

- ユーザ認証に、認証サーバを使用していないこと

操作手順

1. maintenance utility にログインします。
2. ［管理］－［ユーザ管理］を選択します。
3. ［ユーザグループ］の一覧から、パスワードを変更したいユーザが所属するユーザグループをクリックします。
4. ［ユーザ］タブのユーザ一覧から、パスワードを変更したいユーザアカウントを選択します。
   （ユーザアカウントの左横にあるチェックボックスにチェックマークを入れます。）
5. ［編集］を選択します。
6. ユーザ編集画面が表示されます。各項目を入力します。
   各項目の詳細は、『システム管理者ガイド』のパスワードの変更を参照してください。

> **メモ**
> パスワードに設定可能な文字列は、パスワードポリシーに従う必要があります。詳細は「3.3.1 ユーザアカウントポリシーの設定」を参照してください。

7. 設定内容を確認し［完了］をクリックします。
8. 警告メッセージが表示された場合は、［OK］をクリックします。
9. 確認メッセージが表示されます。［適用］をクリックします。
10. 完了メッセージが表示されます。［閉じる］をクリックします。

3.4 外部認証

認証サーバに LDAP サーバを使用した外部認証と認可に必要な項目を設定します。外部認証を有効にすると、ユーザアカウントごとに外部認証・認可サーバの使用、不使用を選択できます。

設定は、maintenance utility で行います。

> **メモ**
> - 外部認証サーバを使用するには、外部認証サーバへの接続設定やネットワークの設定が必要です。設定値は外部認証サーバの管理者に問い合わせてください。ネットワークの設定に関しては、ネットワークの管理者に問い合わせてください。

- 外部認証サーバとの通信には、外部認証サーバのルート証明書の証明書ファイルをストレージシステムに設定する必要があります。証明書の要件については、「3.5.1 ストレージシステムと外部サーバ間の SSL/TLS 通信」を参照ください。
- 外部認証サーバに登録されているユーザの所属先ユーザグループと、ストレージシステムにローカルに登録されているユーザの所属先ユーザグループが異なる場合、ストレージシステムでの所属先ユーザグループが優先されます。
- ユーザアカウントを maintenance utility で作成しない場合、ユーザグループの割り当て（認可）は外部認証サーバに設定してください。この場合、ストレージシステムに定義されているユーザグループと同じ名称のグループを外部認証サーバに定義してください。ビルトイングループの名称は、「3.2.3 ビルトイングループ」を参照してください。ユーザアカウントを maintenance utility で作成する場合、認証の手段として外部認証を選択できますが、ユーザグループの割り当て（認可）は maintenance utility での設定が適用されます。ユーザグループの割り当て（認可）を外部認証サーバに設定しても適用されません。

3.4.1 外部認証サーバ・外部認可サーバの要件

LDAP ディレクトリサーバを使用する場合、次の条件を満たしていることを確認してください。また、LDAP ディレクトリサーバを使用する場合はストレージシステムにルート証明書を設定する必要があります。証明書については、LDAP ディレクトリサーバの管理者に問い合わせてください。

- 認証サーバのプロトコル
  LDAPv3 Simple bind 認証
- 通信プロトコル
  TLS1.2 と TLS1.3
- 証明書ファイルの種類※
  CA（Certification Authority）のルート証明書
- 証明書ファイルの形式※
  X509 DER 形式
  X509 PEM 形式
- DNS サーバの SRV レコードに登録してある情報を使用してサーバを検索する場合の条件
  LDAP サーバで、DNS サーバの環境設定が完了していること
  DNS サーバに、LDAP ディレクトリサーバのホスト名、ポート番号、ドメイン名が登録されていること

注※

証明書の要件など詳細については、「3.5.1 ストレージシステムと外部サーバ間の SSL/TLS 通信」を参照ください。

3.4.2 外部認証サーバに接続する

認証サーバに LDAP サーバを使用した外部認証および認可を設定します。

前提条件

- LDAP サーバの要件を確認しておくこと。
- 要件を満たしている LDAP サーバが構築済みであること。
- 管理 LAN 上に LDAP サーバを設置していること。
- ルート証明書の証明書ファイルを用意しておくこと。
  証明書の要件など詳細については、「3.5.1 ストレージシステムと外部サーバ間の SSL/TLS 通信」を参照してください。

- 外部認証設定に必要な情報を確認しておくこと。
- ストレージシステムと LDAP サーバ間にファイアウォールを設置している場合は、通信に使用するポート番号を開放済みであること。

メモ

- ストレージシステムにユーザアカウントが登録されていない場合、ユーザグループの割り当て（認可）は外部認証サーバでの設定が適用されます。
  外部認証サーバで各ユーザアカウントのユーザグループを設定してください。設定の際、ストレージシステムに定義されているユーザグループと同じ名称のグループを外部認証サーバに定義してください。ビルトイングループの名称については、「3.2.3 ビルトイングループ」を参照してください。
- ストレージシステムにユーザアカウントが登録されている場合、認証の手段として外部認証を選択できますが、ユーザグループの割り当て（認可）は maintenance utility での設定が適用されます。
  ユーザグループの割り当て（認可）を外部認証サーバに設定しても適用されません。

操作手順

1. maintenance utility の［管理］メニューから［外部認証］－［サーバ設定］－［LDAP］を選択します。
   ［サーバ設定（LDAP）］画面が表示されます。
2. 以下の項目を設定します。

項目		説明
証明書ファイル名		ルート証明書の証明書ファイルを指定します。［参照］ボタンをクリックし、証明書ファイルを指定してください。
DNS Lookup		外部認証・認可サーバの指定方法を選択します。 ・ ［有効］：DNS サーバの SRV レコードで、外部認証・認可サーバを指定します。 ・ ［無効］：ホスト名、または IP アドレスで、外部認証・認可サーバを指定します。
認証プロトコル		［DNS Lookup］で無効を選択した場合、LDAP プロトコルを選択します。 次のプロトコルが選択できます。 ・ LDAP over SSL/TLS ・ STARTTLS
外部ユーザグループ連携		指定した LDAP ディレクトリサーバを認可サーバとしても使用するかを選択します。 ・ ［有効］：使用する ・ ［無効］：使用しない
プライマリサーバ		［DNS Lookup］で無効を選択した場合、［ホスト名］と［ポート番号］に LDAP ディレクトリサーバの情報を設定します。
	プライマリサーバホスト名	［DNS Lookup］で無効を選択した場合、LDAP ディレクトリサーバのホスト名、または IP アドレスを入力します。
	プライマリサーバポート番号	［DNS Lookup］で無効を選択した場合、LDAP ディレクトリサーバのポート番号を入力します。
	プライマリサーバドメイン名称	LDAP ディレクトリツリーのドメイン名称を入力します。
	プライマリサーバユーザ名属性	認証で使用するユーザ ID の値が定義されている属性名を入力します。 ・ 使用可能文字：半角英数字と記号（! # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~）

項目		説明
		• 階層モデルの場合 : ユーザを特定できる値が格納されている属性名を設定します。 • フラットモデルの場合 : ユーザエントリの RDN の属性名を設定します。
	プライマリサーバ タイムアウト	LDAP ディレクトリサーバとの接続タイムアウトを検出するまでの時間（秒）を入力します。
	プライマリサーバ リトライ間隔	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔（秒）を入力します。
	プライマリサーバ リトライ回数	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数を入力します。
	プライマリサーバ Base DN	認証するユーザを検索するときに基点となる DN を入力します。 • 使用可能文字 : 半角英数字とすべての記号 • 階層モデルの場合 : すべての検索対象のユーザを含む階層の DN を入力します。 • フラットモデルの場合 : 検索対象のユーザより 1 つ上の階層の DN を入力します。 記号（+ ; , < = >など）を入力する場合は、1 文字ごとに記号の直前に円記号（¥）を入力してエスケープしてください。 ただし、¥、/、"を入力するときは、次のとおり円記号（¥）を入力したあと に ASCII コードを入力してください。 • 「¥」は、「¥5c」と入力します。 • 「/」は、「¥2f」と入力します。 • 「"」は、「¥22」と入力します。
	プライマリサーバ 検索用ユーザ DN	検索用ユーザの DN を入力します。［プライマリサーバ - ユーザ名属性］に sAMAccountName を指定した場合、または［外部ユーザグループ連携］で有効を選択した場合にのみ、入力が必要です。 • 使用可能文字 : 半角英数字とすべての記号 記号（+ ; , < = >など）を入力する場合は、1 文字ごとに記号の直前に円記号（¥）を入力してエスケープしてください。 ただし、¥、/、"を入力するときは、次のとおり円記号（¥）を入力したあとに ASCII コードを入力してください。 • 「¥」は、「¥5c」と入力します。 • 「/」は、「¥2f」と入力します。 • 「"」は、「¥22」と入力します。
	プライマリサーバ パスワード	検索用ユーザのパスワードを入力します。LDAP ディレクトリサーバに登録しているパスワードと同じ値を入力してください。 ［プライマリサーバ - ユーザ名属性］に sAMAccountName を指定した場合、または［外部ユーザグループ連携］で有効を選択した場合にのみ、入力が必要です。 • 使用可能文字 : 半角英数字と記号（! # $ % & ' ( ) * + - . = @ ¥ ^ _ | / : ; < > ? [ ] ` { } ~ " ,とスペース）
セカンダリサーバ		［DNS Lookup］で無効を選択した場合、LDAP ディレクトリサーバの代替サーバを使用するかを選択します。 • ［有効］: 代替サーバを使用する • ［無効］: 代替サーバを使用しない
	セカンダリサーバ ホスト名	［セカンダリサーバ］で有効を選択した場合、プライマリサーバと同様の設定項目を入力します。

項目	説明
セカンダリサーバポート番号	[セカンダリサーバ] で有効を選択した場合、LDAP ディレクトリサーバの代替サーバのポート番号を入力します。
テストユーザ名	[サーバ構成テスト] で使用するユーザ名を入力します。 • 使用可能文字: 半角英数字と記号 (! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~)
パスワード	[サーバ構成テスト] で使用するユーザのパスワードを入力します。 • 使用可能文字 : 半角英数字と記号 (! # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~)

3. 設定内容を確認して、[サーバ構成テスト] の [チェック] をクリックします。
4. テストの結果を確認して、[適用] をクリックします。
5. [外部認証] 画面で、設定内容が反映されていることを確認します。
6. LDAP サーバに登録されているユーザアカウントのユーザ名、パスワードで、VSP One Block Administrator にログインできることを確認します。
   外部認証を行うユーザアカウントが複数存在する場合は、外部認証を行うすべてのユーザアカウントでログインできることを確認してください。

メモ
認証サーバのみ使用 ([外部ユーザグループ連携] を無効) にした場合、サーバ構成のテストに成功しても、ストレージシステムに登録されていないユーザアカウントによるアクセスはできません。
認証・認可サーバの使用 ([外部ユーザグループ連携] を有効) でストレージシステムにアクセスできない場合は、LDAP サーバの設定を見直してください。

3.5 TLS 通信機能

3.5.1 ストレージシステムと外部サーバ間の SSL/TLS 通信

ストレージシステムは、特定の外部サーバと通信する際に、SSL/TLS 通信を使用します。ストレージシステムと外部サーバの SSL/TLS 通信時の要件および、証明書検証について説明します。

プロトコルの暗号スイートを、次に示します。

プロトコル	暗号スイート
TLS1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS1.3	TLS_AES_128_GCM_SHA256
	TLS_AES_256_GCM_SHA384

プロトコルの暗号スイートは、変更できます (「3.5.3 TLS セキュリティ設定を管理する」を参照)。

鍵交換でのアルゴリズムと鍵長を、次に示します。

鍵交換アルゴリズム	鍵長
DHE	2048bit
	3072bit
	4096bit
ECDHE	secp256r1
	secp384r1
	secp521r1

鍵交換でのアルゴリズムと鍵長は、変更できます（「3.5.3 TLS セキュリティ設定を管理する」を参照）。

証明書の署名でサポートされている署名アルゴリズム、鍵長、ハッシュアルゴリズムを、次に示します。

表 1 サポートされている署名アルゴリズム・鍵長・ハッシュアルゴリズム

署名アルゴリズム	鍵長	ハッシュアルゴリズム
RSA	2048/3072/4096bits	SHA-256
		SHA-384
		SHA-512
ECDSA	secp256r1（P-256）	SHA-256
	secp384r1（P-384）	SHA-384
	secp521r1 （P-521）	SHA-512

署名アルゴリズム、鍵長、およびハッシュアルゴリズムは、変更できます（「3.5.3 TLS セキュリティ設定を管理する」を参照）。

ストレージシステムと外部サーバ間で SSL/TLS 通信を実施する際の証明書は、次の要件を満たす必要があります。

表 2 証明書の要件

#	要件項目	要件内容	対象の証明書			
			サーバ証明書	中間 CA 証明書	クライアント証明書	ルート証明書
1	形式	証明書が X.509v3 に従い、かつ次のどちらかの形式であること ・ DER ・ PEM（base64 encoded）	○	○	○	○
2	接続先	・ 証明書に含まれる、subjectAlternativeName 拡張属性の値と接続先（ホスト名または IP アドレス）が一致すること	○	×	△	×

#	要件項目	要件内容	対象の証明書			
			サーバ証明書	中間 CA 証明書	クライアント証明書	ルート証明書
		• ワイルドカードは RFC2818 に従っていること				
3	署名のアルゴリズム/鍵長/ハッシュアルゴリズム	「表 1 サポートされている署名アルゴリズム・鍵長・ハッシュアルゴリズム」の署名アルゴリズム、鍵長、ハッシュアルゴリズムを使用していること※	○	○	○	○
4	拡張属性（keyUsage）	keyCertSign が設定されていること	×	○	△	○
5	拡張属性（extendedKeyUsage）	Server Authentication Purpose（1.3.6.1.5.5.7.3.1） が設定されていること	○	×	×	×
		OCSP Signing Purpose（1.3.6.1.5.5.7.3.9）が設定されていないこと	×	○	△	○
6	拡張属性（basicConstraints）	basicConstraints 拡張属性を含み、CA 信頼フラグが TRUE であること	×	○	×	○
		basicConstraints 拡張属性を含み、CA フラグが FALSE であること	○	×	△	×
7	拡張属性（subjectKeyIdentifier）	設定されていること	○	○	△	○

凡例

○：必須項目
△：通信対象サーバの要件に依存する項目
×：不要項目

注※

「3.5.3 TLS セキュリティ設定を管理する」に示す操作で、セキュリティモードを設定することによって、署名アルゴリズム、鍵長、およびハッシュアルゴリズムの絞り込みができます。

ストレージシステムは、外部サーバ設定（例：Syslog サーバ設定）で実施する証明書のアップロード時または外部サーバとの通信時に、証明書チェーンの有効性を検証します。検証対象を次に示します。

検証対象

- syslog サーバ※1
- 外部認証サーバ※2
- 鍵管理サーバ※3

- 外部ストレージシステムの REST API サーバ※4

注※1

- クライアント証明書が 3 段以上のチェーン構成の場合、すべての中間証明書とルート証明書を syslog サーバのトラストストア（TrustStore）に設定してください。
- CRLDP の URI（Uniform Resource Identifier）は http 形式で記載されている必要があります。
- 複数の CRLDP エントリはサポートしていません。

注※2

- CRLDP の URI は http 形式で記載されている必要があります。
- 複数の CRLDP エントリはサポートしていません。

注※3

CRL を用いた失効検証は実施できません。証明書の失効を確認したい場合は、OCSP を用いた失効検証を実施する、または接続先サーバの管理者に問い合わせてください。

注※4

CRL または OCSP を用いた失効検証は実施できません。証明書の失効を確認したい場合は、接続先サーバの管理者に問い合わせてください。

検証項目は、検証のタイミングによって変わります。

検証タイミングごとの検証内容については、『システム管理者ガイド』の証明書のアップロード時に実施する証明書検証項目および外部サーバとの通信時に実施する証明書検証項目を参照してください。

3.5.2 SSL/TLS 通信の設定の流れ

SSL/TLS 通信に必要な設定の流れを次に示します。

<table>
<tr><th rowspan="2">作業項目</th><th colspan="2">操作方法、参照先</th><th rowspan="2">必須/任意</th></tr>
<tr><th>OpenSSL</th><th>maintenance utility</th></tr>
<tr><td>OpenSSL の入手</td><td>秘密鍵と公開鍵を作成するには、鍵作成用のプログラム（OpenSSL）が必要です。
OpenSSL のホームページ（http://www.openssl.org/）からダウンロードしてください。OpenSSL のバージョンは 3.0.7 以降を使用してください。</td><td>－</td><td>任意</td></tr>
<tr><td>秘密鍵の作成</td><td>「(1)　秘密鍵を作成」</td><td rowspan="3">「(5)　CSR 作成および自己署名証明書作成」</td><td>必須</td></tr>
<tr><td>公開鍵の作成</td><td>「(2)　公開鍵を作成」</td><td>必須</td></tr>
<tr><td>署名付き証明書の取得</td><td>・ 自己署名付きの証明書の場合:「(3)　署名付き証明書を取得」
・ 認証局発行の証明書の場合:「(4)　署名付きの信頼できる証明書を取得」</td><td>必須</td></tr>
<tr><td>証明書アップロードの前処理</td><td colspan="2">・「(6)　SSL/TLS 証明書を PKCS#12 形式に変換」</td><td>必須※</td></tr>
</table>

作業項目	操作方法、参照先		必須/任意
	OpenSSL	maintenance utility	
証明書のアップロード	• 「(7) Web サーバ接続用証明書をストレージシステムへアップロード」		必須
TLS セキュリティ設定の変更	• 「3.5.3 TLS セキュリティ設定を管理する」		任意
トラブルシュート	『システム管理者ガイド』のセキュリティ警告が表示されたときの対処方法を参照してください。		―

注※

PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合のみ

(1) 秘密鍵を作成

秘密鍵（.key ファイル）を作成する手順を説明します。

操作手順

1. OpenSSL をインストールします。この例では C:¥openssl フォルダにインストールしています。
2. OpenSSL をインストールした場合は、openssl フォルダのプロパティを表示し、読み込み専用属性が付いている場合は解除します。
3. Windows のコマンドプロンプトを起動します。
4. カレントディレクトリを鍵ファイルを出力するフォルダ（例:C:¥key）に移動し、次に示すコマンドを実行します。
   OpenSSL をインストールした場合：`C:¥key>c:¥openssl¥bin¥openssl genrsa -out server.key 2048`
   秘密鍵として、server.key ファイルが C:¥key フォルダに作成されます。

(2) 公開鍵を作成

公開鍵（.csr ファイル）を作成する手順を説明します。

操作手順

1. Windows のコマンドプロンプトで次に示すコマンドを実行します。

```
openssl req -new -noenc -out c:¥key¥server.csr -keyout c:¥key
¥server.key -config c:¥key¥req.txt

req.txt の例を示します。

[ req ]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[ dn ]
C = JP
ST = Kanagawa
L = Yokohama
O = Hitachi Vantara
OU = Storage
```

```
CN = VSP

[req_ext]
subjectKeyIdentifier = hash
extendedKeyUsage = serverAuth
keyUsage = critical, digitalSignature, keyEncipherment
basicConstraints = CA:FALSE
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = hitachivantra.example.com
IP.1 = 192.168.0.1
```

extendedKeyUsage には証明書の使用用途を設定します。サーバ認証用途で使用する場合は serverAuth を設定し、クライアント認証用途で使用する場合は clientAuth を設定してください。
basicConstraints には CA フラグを設定します。自己署名証明書を作成する場合は、自己を署名するために CA:TRUE を設定してください。
[alt_names]以降に表示される DNS.1 にストレージシステムのホスト名を、IP.1 にはストレージシステムの IP アドレスを入力してください。 この項目に入力した名称が、SSL/TLS 通信をするときのサーバ名称（ホスト名）になります。サーバ名称は任意に決定できますが、入力したサーバ名称とストレージシステムの名称（ホスト名）を一致させてください。

2. 公開鍵として、server.csr が C:¥key フォルダに作成されます。

(3) 署名付き証明書を取得

秘密鍵と公開鍵を作成したら、公開鍵の署名付き証明書ファイルを取得してください。署名付き証明書ファイルの取得には、次の 3 つの方法があります。

- 自己署名をして証明書を作成する方法
- 自社内で運用している認証局の証明書を取得する方法
- 信頼された社外の認証局に依頼して、証明書を取得する方法

認証局に依頼する場合は、管理ツールの操作端末をホスト名で指定してください。また、別途費用がかかります。

なお、自己署名証明書は暗号化通信のテストなどの目的でだけ使用することをお勧めします。

自己署名付きの証明書を取得する

認証局に署名を依頼せずに、自己署名をして、署名付きの公開鍵証明書（サーバ証明書）を作成できます。自己署名をするには、Windows のコマンドプロンプトで、次に示すコマンドを実行します。

```
OpenSSL をインストールした場合：C:¥key>c:¥openssl¥bin¥openssl x509 -req -
sha256 -days 10000 -in server.csr -signkey server.key -copy_extensions
 copyall -out server.crt
```

この例では、有効期間を 10,000 日に設定しています。また、上記のコマンドを実行すると、ハッシュアルゴリズムに SHA-256 が使用されます。

メモ
セキュリティ上の問題が起きるため、ハッシュアルゴリズムには、MD5 や SHA-1 を使用しないで、SHA-256 を使用してください。

server.crt ファイルが C:¥key フォルダに作成されます。この server.crt ファイルが署名付きの公開鍵証明書になります。

(4) 署名付きの信頼できる証明書を取得

署名付きの信頼できる証明書を取得したい場合は、VeriSign などの認証局に証明書発行要求用ファイル（csr ファイル）を送付し、署名付きの公開鍵証明書（crt ファイル）を取得します。認証局へ依頼する手続きについては、依頼する認証局のホームページなどを参照してください。

(5) CSR 作成および自己署名証明書作成

『システム管理者ガイド』の maintenance utility を利用して秘密鍵および公開鍵を生成するを参照してください。

(6) SSL/TLS 証明書を PKCS#12 形式に変換

PEM 形式の証明書ファイルと秘密鍵ファイルを合わせてストレージシステムへアップロードする場合、PKCS#12 形式に変換する必要があります。SSL/TLS 証明書を PEM 形式または DER 形式でアップロードする場合、または SSL/TLS 証明書をストレージシステムへアップロードしない場合は、変換は不要です。

秘密鍵と SSL/TLS 証明書を PKCS#12 形式に変換する手順を説明します。

メモ

- この手順では、秘密鍵のファイル名を client.key、SSL/TLS 証明書のファイル名を client.crt に設定しています。
- この手順では、c:¥key に PKCS#12 形式の SSL/TLS 証明書ファイルを出力します。
- OpenSSL を使用する場合は、3.0.7 以降のバージョンを使用してください。
- FIPS モードが ON の場合に PKCS12 ファイルを作成するとき、メッセージ認証符号による MAC 完全性を付与しないでください。（例 : OpenSSL を使用して PKCS12 ファイルを作成する場合、-nomac オプションを付与する。）（FIPS モードが有効な OpenSSL は MAC 完全性付与をサポートしていません）

前提条件

- 秘密鍵と SSL/TLS 証明書を同じフォルダに格納していること。

操作手順

1. Windows のコマンドプロンプトを管理者権限で起動します。
2. 次のコマンドを実行します。
   OpenSSL をインストールした場合：C:¥key>c:¥openssl¥bin¥openssl△pkcs12△-export△-in△client.crt△-inkey△client.key△-out△client.p12
   △：半角スペース
3. 任意のパスワードを入力します。
   このパスワードは、PKCS#12 形式の SSL/TLS 証明書をストレージシステムにアップロードするときに使用します。
   PKCS#12 形式の SSL/TLS 証明書を作成するときのパスワードに使用できる文字は、次のとおりです。128 文字以下の文字列で指定します。
   A～Z a～z 0～9 ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~
4. C:¥key フォルダに、client.p12 ファイルが作成されます。この client.p12 ファイルが PKCS#12 形式に変換された SSL/TLS 証明書です。
5. コマンドプロンプトを閉じます。

(7) Web サーバ接続用証明書をストレージシステムへアップロード

［証明書ファイル更新］画面を使って、管理ツールの操作端末とストレージシステムの SSL/TLS 通信に使用する Web サーバ接続用証明書をストレージシステムへアップロードして、更新します。

保守作業を行う場合、保守員が保守用 PC（MPC）を保守用ポートに接続します。この際、MPC とストレージシステム間の通信に使用する MPC 接続用証明書が必要となります。この証明書はお客様が作成し、保守員に渡してください。

注意

- アップロードする Web サーバ接続用証明書の要件については、『システム管理者ガイド』のストレージシステムと管理ツールの操作端末間の SSL/TLS 通信を参照ください。
- ストレージシステムへアップロードする証明書ファイルは、次のどれかの形式である必要があります。
  - PKCS#12 形式
  - PEM 形式
  - DER 形式
- PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合は、PKCS#12 形式に変換してください（「(6)　SSL/TLS 証明書を PKCS#12 形式に変換」を参照）。
- PEM 形式または DER 形式でアップロードする場合は、事前に秘密鍵と CSR（公開鍵）を作成してください（『システム管理者ガイド』の maintenance utility を利用して秘密鍵および公開鍵を生成するを参照）。この際、［目的］に［Web Server］を選択してください。この CSR に基づいて署名された証明書を準備してください。
- 中間証明書が存在する場合は、中間証明書を含んだ証明書チェーンで構成された、署名付き公開鍵証明書を準備してください。
- アップロードする証明書の証明書チェーンの階層数は、ルート CA 証明書を含めて 20 階層以下です。
- アップロードする証明書の公開鍵暗号方式は、RSA です。

操作手順

1. maintenance utility にログインします。
2. 左下の［メニュー］－［システム管理］－［証明書ファイル更新］を選択します。
3. 証明書ファイル更新画面が表示されます。
   更新対象の証明書の左横のチェックボックスを選択してください。

管理モデル	選択対象の証明書
VSP One Block Administrator を利用する	［Web サーバ］

4. アップロードする証明書ファイルの形式を選択します。

形式	説明
PKCS#12	サーバ証明書ファイルと秘密鍵ファイルを含む形式です。
PEM or DER	サーバ証明書ファイルのみの形式です。 ［期待する Subject Key Identifier］欄と、Subject Key Identifier 情報が一致する証明書ファイルをアップロードしてください。証明書ファイルの Subject Key Identifier 情報は、証明書の拡張属性に記載されています。［PEM or DER］を選択しても［期待する Subject Key Identifier］欄に"-"（ハイフン）が表示される場合は、鍵情報の取得に失敗している可能性があります。3 分程度あけて、再度、『システム管理者ガイド』の maintenance utility を利用して秘密鍵および公開鍵を生成するを参照し、秘密鍵および CSR（公開鍵）の作成をしてください。

5. ［ファイルを選択］ボタンをクリックして、アップロードする証明書ファイルを指定します。
   手順 4 で PKCS#12 形式を選択した場合は、続けて PKCS#12 のパスワードを入力します。
6. 設定内容を確認し［適用］をクリックします。
7. 完了メッセージが表示されます。［閉じる］をクリックします。

3.5.3 TLS セキュリティ設定を管理する

管理ツールの操作端末と ESM との 、SSL/TLS 通信で使用する TLS バージョンと暗号スイートを含む、SSL/TLS 通信のセキュリティを管理します。

管理ツールの操作端末と ESM との通信では、次のプロトコルとポート番号の通信で SSL/TLS 通信のセキュリティ設定が適用されます。

プロトコル	ポート番号
HTTPS	443

メモ
ストレージシステムと保守員が使用する保守用 PC の通信で使用される MPC Communication Protocol（Port：10500）には、SSL/TLS 通信のセキュリティ設定が適用されません。

次に示すサーバやリモートストレージを使用する場合、これらの機器と ESM 間でも、SSL/TLS 通信のセキュリティ設定が適用されます。

- Syslog サーバ
- 鍵管理サーバ
- 外部認証/認可サーバ
- リモートコピーの副サイトのストレージシステム

(1) SSL/TLS 通信のセキュリティ設定項目

次に示す項目を設定できます。

- SSL/TLS 通信のセキュリティモード

項目	説明	デフォルト値
FIPS	FIPS に準拠した SSL/TLS 通信のセキュリティ設定	有効（無効化不可）
CNSA1.0	CNSA1.0 に準拠した SSL/TLS 通信のセキュリティ設定	無効

- SSL/TLS 通信で使用を許可するプロトコルと暗号スイート
  プロトコルを無効にすると、対応する暗号スイートも無効になります。

プロトコル	暗号スイート	CNSA1.0 モード有効時	デフォルト値
TLS1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	選択不可	有効
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	選択可	有効
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	選択不可	有効

プロトコル	暗号スイート	CNSA1.0 モード有効時	デフォルト値
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	選択可	有効
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	選択不可	有効
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	選択可	有効
TLS1.3	TLS_AES_128_GCM_SHA256	選択不可	有効
	TLS_AES_256_GCM_SHA384	選択可	有効

- SSL/TLS 通信時の鍵交換で許可する、最小の鍵長

アルゴリズム	最小鍵長	CNSA1.0 モード有効時
DHE	2048bits（デフォルト）	選択不可
	3072bits	選択可
ECDHE	secp256r1（デフォルト）	選択不可
	secp384r1	選択可
	secp521r1	選択可

注意

SSL/TLS 通信時の証明書で許可される署名アルゴリズム、鍵長、ハッシュアルゴリズムは、セキュリティ動作モードによって設定されます。

署名アルゴリズム	鍵長	ハッシュアルゴリズム	CNSA1.0 モード有効時のサポート状況
RSA	2048bits	SHA-256	未サポート
		SHA-384	未サポート
		SHA-512	未サポート
	3072bits	SHA-256	未サポート
		SHA-384	サポート
		SHA-512	サポート
	4096bits	SHA-256	未サポート
		SHA-384	サポート
		SHA-512	サポート
ECDSA	secp256r1	SHA-256	未サポート
	secp384r1	SHA-384	サポート
	secp521r1	SHA-512	サポート

(2) SSL/TLS セキュリティ設定を変更する

管理ツールの操作端末と ESM との SSL/TLS 通信のセキュリティ設定を変更したい場合は、SSL/TLS 通信で使用する TLS バージョンと、暗号スイートを含むセキュリティを設定してください。

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. maintenance utility にログインします。
2. 左下の［メニュー］－［システム管理］－［TLS セキュリティ選択］を選択します。［TLS セキュリティ選択］画面が表示されます。
3. 各項目を設定します。設定項目の詳細は「(1)　SSL/TLS 通信のセキュリティ設定項目」を参照してください。

注意

1. TLS1.2 を使用する場合は、ESM にアップロードした証明書の鍵タイプと対応した暗号スイートを選択してください。
   - 鍵タイプが RSA の場合は、名称に RSA を含む暗号スイートを選択してください。
   - 鍵タイプが ECDSA の場合は、名称に ECDSA を含む暗号スイートを選択してください。
2. TLS1.3 を使用する場合は、証明書の鍵タイプ（RSA または ECDSA）に関係なく、暗号スイートを選択できます。ただし、通信時に利用される鍵交換アルゴリズムの下限鍵長は、証明書の鍵長に対応したものを選択してください。証明書の鍵長よりも大きな鍵交換アルゴリズムの下限鍵長を選択すると、通信が失敗する場合があります。
3. TLS1.2 および TLS1.3 のどちらも、セキュリティモードによって利用できる署名アルゴリズムが制限され、通信が失敗する場合があります。
4. セキュリティモードの、CNSA1.0 モードが有効な場合、ストレージシステム上のすべての SSL/TLS 通信に対して、以下の追加制限が適用されます。
   - RSA 署名アルゴリズムを使用する場合、ハッシュアルゴリズム SHA-256 は使用不可
   - RSA 署名アルゴリズムを使用する場合、鍵長 2048bits の証明書は使用不可
   - ECDSA 署名アルゴリズムを使用する場合、鍵長 secp256r1、ハッシュアルゴリズム SHA-256 は使用不可

   SSL/TLS 通信時に、上記の条件を満たさない証明書を使用している場合は、証明書検証や TLS ハンドシェイクが失敗し、通信できなくなる場合があります。証明書の署名アルゴリズム、鍵長、ハッシュアルゴリズムが要件を満たしているか、事前に確認ください。
5. TLS セキュリティ設定を変更した場合、ブラウザからストレージシステムへのアクセスや、ストレージシステムから外部サーバなどへの TLS 通信に失敗する可能性があります。ブラウザや外部サーバに登録している証明書が、変更する TLS セキュリティ設定に対応しているか事前に確認してください。確認が取れない場合、事前に TCP ポート(SSH) (TCP:20522)が有効であるかを確認し、有効でない場合は一時的に TCP ポートの（SSH）または（TCP:20522）を有効にしてください。
6. TLS セキュリティ設定後に、ブラウザや外部サーバとの通信に成功した場合は、TCP ポートの（SSH）または（TCP:20522）の設定を元に戻してください。設定画面へ接続ができない場合は、「(3)　SSL/TLS 通信のセキュリティ設定を初期化する」を参照して、TLS セキュリティ設定を初期化した後に、再度 TLS セキュリティを設定してください。再度設定した後も、TLS 通信失敗が解消されない場合は、お問い合わせください。

---

4. 通信テストの［チェック］をクリックすると、次の通信路について、手順 3 で指定したセキュリティ設定を使った通信テストが開始されます。
   - ESM-Syslog サーバ
   - ESM-LDAP サーバ
   - ESM-鍵管理サーバ
5. 手順 4 で実施した各通信路の通信テストの結果を確認します。

状態	意味	アイコン
Normal	すべてのサーバとの通信テストが成功した状態	
Skipped	通信路の設定がないため、通信テストをスキップした状態	
Warning	通信テストが成功したサーバと、失敗したサーバが混在している状態	
Error	すべてのサーバとの通信テストが失敗した状態	
Processing	通信テスト中の状態	
Wainting	通信テスト前の状態	

6. 画面上に記載されている、TLS 通信の失敗の可能性、および推奨事項についての内容を確認してから、［TLS 通信が失敗する可能性があることを理解しました。］のチェックボックスを選択してください。
7. ［適用］をクリックします。
8. 完了メッセージが表示されます。
   この際に、下記の項目をすべて満たす場合、SNMP の設定見直しが必要である旨を記載したメッセージと、SIM「7d23xx」が出力されます。この場合は、ロールとして「ストレージ管理者（初期設定）」を持つストレージ管理者に対応を依頼してください。
   - ［TLS セキュリティ選択］のセキュリティモードで、CNSA1.0 モードが有効
   - アラート通知設定と SNMP 設定で、暗号化プロトコルまたは認証プロトコルに、CNSA1.0 非準拠のプロトコルを設定
9. 内容を確認して、［OK］をクリックします。ESM が再起動され、ログイン画面が表示されます。
10. 左下の［メニュー］－［システム管理］－［TLS セキュリティ選択］を選択します。
11. ［TLS セキュリティ選択］画面で、設定が正しく変更されているか確認します。

(3)　SSL/TLS 通信のセキュリティ設定を初期化する

管理ツールの操作端末と ESM を SSH 接続すると、内蔵 CLI で SSL/TLS 通信のセキュリティ設定を初期化できます。「(2)　SSL/TLS セキュリティ設定を変更する」で設定変更した結果、maintenance utility に接続ができなくなってしまった場合に操作してください。

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、または保守（ベンダ専用）ロール

操作手順

1. 管理ツールの操作端末と ESM を SSH 接続します。
2. mgmtcom tlssettingreset を実行します。
   完了メッセージが表示されます。
3. maintenance utility にログインします。
4. 画面左下の［メニュー］－［システム管理］－［TLS セキュリティ選択］を選択します。
   ［TLS セキュリティ選択］ 画面が表示されます。

5. TLS セキュリティ設定の各項目が、デフォルトの値に初期化されていることを確認します。

4

Audit Log

本章では Audit Log を使用するために必要なセキュリティ設定について説明します。

maintenance utility で syslog サーバの設定をすると、監査ログ情報が syslog サーバに常時転送され、syslog 情報ファイルとして蓄積されます。

- 4.1 監査ログの Syslog サーバへの転送を設定する
- 4.2 Syslog サーバに監査ログのテストメッセージを送信する

4.1 監査ログの Syslog サーバへの転送を設定する

監査ログを Syslog サーバに転送する設定手順を示します。

前提条件

- 管理 LAN 上に Syslog サーバを設置していること。
- ストレージシステムと Syslog サーバ間にファイアウォールを設置している場合は、Syslog の転送に使用するポートが開放されていること。
- Syslog 転送設定で必要な設定内容を確認しておくこと。

注意

- Syslog 転送プロトコルに、UDP/RFC3164 を使う場合は、ネットワークの設計時に UDP の特性を考慮してください。詳細については、IETF が発行する文書 RFC3164 を参照してください。
- Syslog 転送プロトコルに、TLS/RFC5424 を使う場合は、Syslog サーバのルート証明書の証明書ファイルや、クライアントの証明書ファイルをストレージシステムに設定する必要があります。証明書の要件については、「3.5.1 ストレージシステムと外部サーバ間の SSL/TLS 通信」を参照ください。
- ストレージシステムへアップロードするクライアントの証明書ファイルは、次のどれかの形式である必要があります。
  - PKCS#12 形式
  - PEM 形式
  - DER 形式
- PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合は、PKCS#12 形式に変換してください「(6)　SSL/TLS 証明書を PKCS#12 形式に変換」を参照)。
- PEM 形式または DER 形式でアップロードする場合は、事前に秘密鍵と CSR（公開鍵）を作成してください（『システム管理者ガイド』の maintenance utility を利用して秘密鍵および公開鍵を生成するを参照)。この際、［目的］に［Audit Syslog Client (Primary)］、［Audit Syslog Client (Secondary)］または［Audit Syslog Client (Primary and Secondary)］を選択してください。この CSR に基づいて署名された証明書を準備してください。

操作手順

1. maintenance utility の［管理］メニューから［監査ログ設定］を選択します。
   ［監査ログ設定］画面が表示されます。
2. ［監査ログ設定］画面の［Syslog サーバ設定］をクリックします。
   ［監査ログ Syslog サーバ設定］画面が表示されます。
3. ［監査ログ Syslog サーバ設定］画面で、各設定項目を指定します。

設定項目	説明
転送プロトコル	Syslog 転送プロトコルを選択します。
プライマリサーバ	［有効］を選択して、以下の設定項目を指定します。 ・ Syslog サーバ ホスト名、または IP アドレス、および転送に使用するポート番号を入力します。

設定項目	説明
	• クライアント証明書ファイルフォーマット、クライアント証明書ファイル名、パスワード、およびルート証明書ファイル名 Syslog 転送プロトコルに、TLS/RFC5424 を使用する場合だけ指定します。
セカンダリサーバ	Syslog サーバの代替サーバがある場合は、[有効] を選択して、プライマリサーバと同様に設定項目を指定します。
ロケーション識別名	監査ログ発行元のストレージシステムを識別するために、任意の名称を設定します。
リトライ、リトライ間隔	Syslog 転送プロトコルに、TLS/RFC5424 を使用する場合だけ指定します。
詳細情報出力	監査ログの詳細情報を転送する場合は、[有効] を選択します。

4. [適用] をクリックします。
5. 完了メッセージが表示されるので、[OK] ボタンをクリックしてください。
   [監査ログ設定] 画面が表示されます。
6. [監査ログ設定] 画面で、監査ログ転送が正しく設定されていることを確認します。

次の作業

4.2 Syslog サーバに監査ログのテストメッセージを送信する

4.2 Syslog サーバに監査ログのテストメッセージを送信する

監査ログの転送設定が完了したら、Syslog サーバに監査ログテストメッセージを送信します。

前提条件

- 監査ログの転送設定が完了していること。

操作手順

1. maintenance utility の [管理] メニューから [監査ログ設定] を選択します。
   [監査ログ設定] 画面が表示されます。
2. [監査ログ設定] 画面の [Syslog サーバへテストメッセージ送信] をクリックします。
3. Syslog サーバにテストメッセージが到着したことを確認します。
   テストメッセージには以下の情報が含まれています。
   機能名：AuditLog、操作名：Send Test Message

5

SNMP

本章では SNMP を使用するための設定について説明します。

SNMP プロトコルのバージョンは SNMP v1、v2c、v3 をサポートします。ここでは、推奨する SNMP v3 の場合の手順について説明します。

- 5.1 SNMP の送信情報を設定する
- 5.2 アラートが SNMP トラップ送信されるようにする（SNMP v3 の場合）
- 5.3 SNMP エンジン ID を SNMP マネージャに登録する（SNMP v3 の場合）
- 5.4 SNMP マネージャへトラップをテスト送信する

5.1 SNMP の送信情報を設定する

ストレージシステムの障害を SNMP トラップで通知するために必要な情報を設定します。

本ストレージシステムでは、SNMPv1、v2c、v3 をサポートしていますが、セキュリティの観点から SNMPv3 を使用することを推奨します。ここでは SNMPv3 の設定方法について説明します。

5.2 アラートが SNMP トラップ送信されるようにする（SNMP v3 の場合）

ストレージシステムの障害発生時に、アラートが SNMP トラップ送信されるように、SNMP エージェントを設定します。本項は、SNMP v3 を使用する場合の操作手順です。

前提条件

- SNMP エージェントに必要な設定内容を確認しておくこと。

操作手順

1. maintenance utility の［管理］メニューから［アラート通知］を選択します。
   ［アラート通知］画面が表示されます。
2. ［アラート通知］画面の［設定］をクリックします。
   ［アラート通知設定］画面が表示されます。
3. ［アラート通知設定］画面の［アラート通知］で、アラート通知対象の SIM を選択します。
   対象の SIM の選択は、すべての通知方法（Email、Syslog、SNMP）で共通の設定です。
4. ［アラート通知設定］画面の［SNMP］タブを選択して、以下の項目を指定します。

設定項目	説明
SNMP エージェント	［有効］を選択します。
SNMP バージョン	［v3］を選択します。

5. トラップ送信先を指定します。以下の手順に従ってください。
   a. ［トラップ送信設定］の［追加］をクリックします。
      ［トラップ送信設定追加］画面が表示されます。
   b. ［トラップ送信設定追加］画面で、以下の項目を指定します。

設定項目	説明
トラップ送信先	トラップ送信先の IP アドレスを指定します。
ユーザ名	SNMP マネージャに登録したユーザ名を入力します。
認証	［有効］を選択した場合は、［プロトコル］で認証方式を選択し、［パスワード］を入力します。
暗号化	［有効］を選択した場合は、［プロトコル］で暗号化方式を選択し、［鍵］と［鍵再入力］を入力します。

   c. ［OK］をクリックします。
      入力した情報が［アラート通知設定］画面の［トラップ送信設定］に反映されます。

6. リクエスト許可設定を行う場合は、以下の手順に従ってください。

   a. ［リクエスト許可設定］の［追加］をクリックします。
   ［リクエスト許可設定追加］画面が表示されます。

   b. ［リクエスト許可設定追加］画面で、以下の項目を指定します。

設定項目	説明
ユーザ名	SNMP マネージャに登録したユーザ名を入力します。
認証	［有効］を選択した場合は、［プロトコル］で認証方式を選択し、［パスワード］と［パスワード再入力］を入力します。
暗号化	［有効］を選択した場合は、［プロトコル］で認証方式を選択し、［鍵］と［鍵再入力］を入力します。

   c. ［OK］をクリックします。
   入力した情報が［アラート通知設定］画面の［リクエスト許可設定］に反映されます。

7. ［システムグループ情報］を入力します。
8. ［SNMP エンジン ID］を入力します。

   - SNMP エンジン ID を指定する必要がない場合：
   ［ID をランダムに生成］を選択してください。
   - SNMP エンジン ID を指定したい場合：
   10～64 桁の 16 進数を、文字数が偶数になるように（16 進数のため）入力してください。

9. 設定内容を確認し［適用］をクリックします。
   ［アラート通知］画面が表示されます。
10. ［SNMP］タブを選択し、設定内容が正しいことを確認します。

次の作業

5.3 SNMP エンジン ID を SNMP マネージャに登録する（SNMP v3 の場合）

5.3 SNMP エンジン ID を SNMP マネージャに登録する（SNMP v3 の場合）

SNMP エージェントは、各 AMC に実装されています。SNMP v3 プロトコルを使用する場合は、SNMP マネージャに、各 AMC の SNMP エンジン ID を登録してください。

前提条件

- SNMP v3 プロトコルを指定した、SNMP トラップ送信の設定が完了していること。

操作手順

1. Web ブラウザから、どちらか一方の AMC の IP アドレスを指定して、maintenance utility を起動します。

```
http（s）：//（AMC の IP アドレス）/MaintenanceUtility
```

2. ［管理］メニューから［アラート通知］を選択します。
   ［アラート通知］画面が表示されます。

3. ［SNMP］タブの［SNMP エンジン ID］の値を確認します。
4. 各 AMC の SNMP エンジン ID を SNMP マネージャに登録します。
   登録方法は、お使いの SNMP マネージャのマニュアルを参照してください。

次の作業

5.4 SNMP マネージャへトラップをテスト送信する

5.4 SNMP マネージャへトラップをテスト送信する

アラートの SNMP トラップ送信の設定が完了したら、SNMP マネージャにトラップをテスト送信します。

前提条件

- SNMP トラップ送信の設定が完了していること。
- 管理 LAN 上に通信可能な SNMP マネージャを設置していること。
- ストレージシステムと SNMP マネージャ間にファイアウォールを使用している場合は、161 番、162 番のポートを開放済みであること。

操作手順

1. maintenance utility の［管理］メニューから［アラート通知］を選択します。
   ［アラート通知］画面が表示されます。
2. ［SNMP］タブの［テスト SNMP トラップ送信］をクリックします。
3. トラップ送信先に指定した SNMP マネージャに、トラップが到着したことを確認します。
   - テスト SNMP トラップには、”RefCode ： 7FFFFF, This is Test Report.”が含まれています。
   - 7FFFFF は、テスト用の SIM リファレンスコードです。

6

LUN Manager/Security

本章では LUN Manager/Security を使用するための設定について説明します。

ストレージシステムに保存されている重要なデータを不当なアクセスから保護するには、論理ボリュームにセキュリティを適用する必要があります。本ストレージシステムで、FC（SCSI）または iSCSI を使用する環境では、ポートの LUN セキュリティ（ポートセキュリティ）を有効にすることで、LU を不当なアクセスから保護できます。LUN Manager の初期設定では、どのポートでも LUN セキュリティ（ポートセキュリティ）は無効になっています。システムを構築するときは、必ずポートの LUN セキュリティ（ポートセキュリティ）を有効にしてください。

FC-NVMe、NVMe/TCP を使用する環境では、NVM サブシステムの Namespace セキュリティを有効にすることで、Namespace を不当なホストアクセスから保護できます。NVM サブシステムを初期作成するとき、Namespace セキュリティはデフォルトで有効になっています。システムを構築するときは、必ず NVM サブシステムの Namespace セキュリティを有効にして運用してください。

- 6.1 LUN セキュリティ（ポートセキュリティ）を設定する
- 6.2 Namespace セキュリティを設定する

6.1 LUN セキュリティ（ポートセキュリティ）を設定する

操作手順については、『VSP One Block Administrator ユーザガイド』を参照してください。

6.2 Namespace セキュリティを設定する

NVM サブシステムを特定のホスト以外の不当なアクセスから保護したり、Namespace をホストに対してプライベートに割り当てる設定をするには、Namespace セキュリティスイッチを有効にする必要があります。

また、Namespace セキュリティスイッチを有効にした場合は、ホストサーバに構成定義されるホスト NQN（NVMe Qualifier Name）を、NVM サブシステムおよび Namespace に登録する必要があります。Namespace セキュリティの設定手順については、『オープンシステム構築ガイド』を参照してください。

7

iSCSI CHAP 認証

本章では iSCSI CHAP を使用するための設定について説明します。

ホストがストレージシステムにログイン要求を送信したとき、ストレージシステムは iSCSI CHAP 認証に基づき、ログイン要求を許可するか拒否するか判断します。

- 7.1 iSCSI ターゲットを作成してホストを登録する
- 7.2 iSCSI ターゲットに CHAP ユーザ名を設定する
- 7.3 iSCSI ターゲットから CHAP ユーザ名を削除する

7.1 iSCSI ターゲットを作成してホストを登録する

操作手順やリクエストラインの設定情報、参照情報については『VSP Block Storage REST API リファレンスガイド』を参照してください。

7.2 iSCSI ターゲットに CHAP ユーザ名を設定する

操作手順やリクエストラインの設定情報、参照情報については『VSP Block Storage REST API リファレンスガイド』を参照してください。

7.3 iSCSI ターゲットから CHAP ユーザ名を削除する

操作手順やリクエストラインの設定情報、参照情報については『VSP Block Storage REST API リファレンスガイド』を参照してください。

8

Encryption License Key

本章では Encryption License Key を使用するための設定について説明します。

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、または、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および暗号モジュール（ENCM）が必要です。

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。

- 8.1 鍵管理サーバを利用する
- 8.2 暗号化環境の設定
- 8.3 暗号化鍵を作成する
- 8.4 暗号化鍵のバックアップ
- 8.5 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
- 8.6 鍵管理サーバに接続して暗号化鍵をバックアップする
- 8.7 暗号化を有効にする
- 8.8 お問い合わせ先

8.1 鍵管理サーバを利用する

8.1.1 鍵管理サーバの要件

鍵管理サーバを使用する場合、鍵管理サーバは次の要件を満たしている必要があります。最新の検証済み鍵管理サーバ、および、そのファームウェアバージョンについては、「8.8 お問い合わせ先」へお問い合わせください。

- 前提プロトコル
  - Key Management Interoperability Protocol 1.0、1.1、1.2、1.3、1.4（KMIPv1.0、v1.1、v1.2、v1.3、v1.4）
- 前提製品

ベンダ	製品名
Thales/Gemalto	CipherTrust Manager k170v/k470v/k470/k570

- 証明書
  ルート証明書とクライアント証明書をストレージシステムにアップロードする必要があります。また、鍵管理サーバにサーバ証明書を設定する必要があります。
  これらの証明書については鍵管理サーバの管理者にお問い合わせください。証明書の管理については鍵管理サーバの管理者とご相談の上、適切に管理してください。ストレージシステムと鍵管理サーバ間の SSL/TLS 通信や証明書の要件については、『システム管理者ガイド』のストレージシステムと外部サーバ間の SSL/TLS 通信を参照ください。
  証明書には期限があります。期限が切れると鍵管理サーバと接続できなくなるため、証明書を準備するときは期限の設定にご注意ください。
  クライアント証明書は、PKCS#12 形式に変換する必要があります。また、PKCS#12 形式に変換する前のクライアント証明書は、鍵管理サーバの CA 局（Certificate Authority）によって署名されている必要があります。
  PKCS#12 形式のクライアント証明書に設定されたパスワードがわからない場合は、鍵管理サーバの管理者にお問い合わせください。
- その他
  鍵管理サーバは最大 2 台登録できます。2 台登録する場合は、2 台でクラスタ化されている必要があります。鍵管理サーバは 2 台登録することを推奨します。

8.1.2 鍵管理サーバのルート証明書の取得

鍵管理サーバのルート証明書は、鍵管理サーバ上で作成および取得できます。詳細については、鍵管理サーバのマニュアルを参照してください。

8.1.3 クライアント証明書の作成

クライアント証明書を取得するには、クライアント証明書を作成するためのプログラムが必要です。

クライアント証明書を作成するためのプログラムは、OpenSSL のホームページ（http://www.openssl.org/）からダウンロードしてください。ここでは、OpenSSL が C:¥openssl フォルダにインストールされているものとします。また、クライアント証明書は、PKCS#12 形式に変換する必要があります。

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

操作手順

詳細は『Encryption License Key ユーザガイド』を参照してください。

1. 秘密鍵（.key ファイル）を作成します。
   秘密鍵を作成する方法については、「(1)　秘密鍵を作成」を参照してください。
2. 公開鍵（.csr ファイル）を作成します。
   公開鍵を作成する方法については、「(2)　公開鍵を作成」を参照してください。
3. 作成した公開鍵を鍵管理サーバの CA 局に署名してもらうことで証明書を取得します。この証明書をクライアント証明書として使用します。
   詳細については、鍵管理サーバのマニュアルを参照してください。
4. Windows のコマンドプロンプト上で、カレントディレクトリを PKCS#12 形式のクライアント証明書ファイルを出力するフォルダがあるディレクトリに移動します。
5. 秘密鍵（.key ファイル）およびクライアント証明書をこのフォルダに移動し、次に示すコマンドを実行します。なお、この例では次の条件でコマンドを実行しています。

   - PKCS#12 形式のクライアント証明書ファイルを出力するフォルダ：c:¥key
   - 秘密鍵のファイル名：client.key
   - クライアント証明書のファイル名：client.crt

   ```
   C:¥key>c:¥openssl¥bin¥openssl pkcs12 -export -in client.crt -inkey
   client.key -out client.p12
   ```

6. 任意のパスワードを入力します。
   このパスワードは、PKCS#12 形式のクライアント証明書をストレージシステムにアップロードするときに使用します。
   PKCS#12 形式のクライアント証明書を作成するときに入力するパスワードは 0 文字以上 128 文字以下で、使用できる文字は次のとおりです。

   - 数字（0 から 9）
   - 英大文字（A から Z）
   - 英小文字（a から z）
   - 半角記号 31 種：! # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~

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

8.2 暗号化環境の設定

8.2.1 鍵管理サーバの使用有無と暗号化環境の設定内容

鍵管理サーバの使用有無によって、設定する項目が異なります。

次の表で、鍵管理サーバの設定、暗号化環境に設定する内容を確認してください。

暗号化環境			鍵管理サーバの設定 (POST kms-settings)	暗号化環境の設定 (PATCH encryption-settings/instance)		
暗号化	鍵管理サーバ		各属性	暗号化環境を有効にする (isEnabled)	鍵管理サーバを使用する (usesKms)	ローカル鍵生成を禁止する (prohibitsLocalKeyGeneration)
使用する	使用しない		設定しない	有効	無効	無効
	使用する	ローカル鍵生成を禁止しない	設定する	有効	有効	無効
		ローカル鍵生成を禁止する				有効※
使用しない（初期化）	―		―	無効	無効	―

注※

「ローカル鍵生成を禁止する」を有効にした場合、設定が完了すると元に戻すことができません。有効に設定しても問題がないことをよく確認してください。

8.2.2 暗号化環境を設定する

鍵管理サーバを使用するには、鍵管理サーバへの接続設定やネットワークの設定が必要です。鍵管理サーバへの接続設定に必要な値については、各サーバの管理者にお問い合わせください。ネットワークの設定については、ネットワークの管理者に確認してください。

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

注意
鍵管理サーバにバックアップされる暗号化鍵はクライアント証明書と関連づけられて管理されます。このため、クライアント証明書を紛失した場合、故障などによってコントローラを交換するとコントローラを交換する前にバックアップした暗号化鍵をリストアできなくなります。
また、鍵管理サーバへの接続設定のバックアップにはクライアント証明書は含まれません。このため、設定完了後は必ず鍵管理サーバへの接続設定をバックアップするとともに、鍵管理サーバの管理者と相談の上、クライアント証明書を別途保管してください。

メモ
鍵管理サーバは、最大 2 台登録できます。2 台登録する場合は、2 台でクラスタ化されている必要があります。鍵管理サーバは、2 台登録することを推奨します。

注意
「ローカル鍵生成を禁止する」を有効にした場合、設定が完了すると元に戻すことができません。有効にしても問題がないことをよく確認してください。

注意
鍵管理サーバを使用する設定の場合、ストレージシステムの電源を ON にしたときに鍵管理サーバからバックアップした暗号化鍵を取得します。このとき、鍵管理サーバとの通信が確立されている必要があります。鍵管理サーバとの通信が確立されていない場合、ストレージシステムは起動しますが、すべてのボリュームが閉塞します。このため、ストレージシステムと鍵管理サーバが通信できることを確認してからストレージシステムの電源を ON にしてください。

前提条件

- 鍵管理サーバに、IP アドレスではなくホスト名を指定して接続する場合は、ストレージシステムの管理ポートのネットワーク情報に、DNS サーバが設定されていること。
- 鍵管理サーバを使用する場合は、鍵管理サーバに登録されているクライアント証明書と鍵管理サーバのルート証明書を用意すること。それぞれの証明書については、鍵管理サーバの管理者に確認してください。

操作手順

鍵管理サーバを使用していない場合は、手順 4 だけを実施してください。

1. 鍵管理サーバを使用する場合、まずクライアント証明書とルート証明書のアップロードを実施します。
   リクエストライン：

   ```
   POST <ベース URL>/v1/objects/kms-certificates
   ```

   ヒント
   クライアント証明書をアップロードする場合は、属性 `fileType` に `ClientCertFile` を、ルート証明書をアップロードする場合は、属性 `fileType` に `RootCertFile` を指定します。

2. 鍵管理サーバとの接続を設定します。
   リクエストライン：

   ```
   POST ＜ベース URL ＞/v1/objects/kms-settings
   ```

3. 鍵管理サーバを使用する場合、鍵管理サーバとの通信テストを実施します。
   リクエストライン：

   ```
   POST ＜ベース URL ＞/v1/objects/kms-settings/＜オブジェクト ID ＞/actions/
   test-connectivity/invoke
   ```

4. 暗号化環境を有効に設定します。鍵管理サーバを使用するかどうかによって設定値が異なります。「8.2.1 鍵管理サーバの使用有無と暗号化環境の設定内容」を参照してください。
   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
   ```

関連概念

- 8.2.1 鍵管理サーバの使用有無と暗号化環境の設定内容

8.3 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
VSP One B80	4,096

鍵管理サーバの使用有無によって、暗号化鍵の生成場所やバックアップ方法が異なります。

鍵管理サーバの使用有無	鍵の生成場所	暗号化鍵のバックアップ方法
鍵管理サーバを使用している	鍵管理サーバ (鍵を使用するのは、ストレージシステム内)	自動的にバックアップされます。
鍵管理サーバを使用していない	ストレージシステム	手動でのバックアップが必要です。 「8.5 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」を参照して、バックアップしてください。

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
```

8.4 暗号化鍵のバックアップ

暗号化鍵のバックアップは、鍵管理サーバの使用有無によって、次のように異なります。

- 鍵管理サーバを使用している場合
  - 鍵管理サーバへのバックアップは、自動的に一次バックアップ、二次バックアップが取得されます。手動での二次バックアップ操作は不要です。

- 個別にバックアップを取り直したい場合や手動バックアップを取得するようにガイドされた場合は、鍵管理サーバに暗号鍵をバックアップしてください。

- 鍵管理サーバを使用していない場合
  - 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する方法と、鍵管理サーバに接続してバックアップする方法があります。

暗号化鍵を管理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。

関連タスク

- 8.5 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
- 8.6 鍵管理サーバに接続して暗号化鍵をバックアップする

8.5 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

鍵管理サーバを使用していない場合、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
```

8.6 鍵管理サーバに接続して暗号化鍵をバックアップする

鍵管理サーバを使用している場合は、暗号化鍵を鍵管理サーバにバックアップできます。

操作手順

1. 鍵管理サーバに、暗号化鍵をバックアップします。

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

注意
鍵管理サーバにバックアップできる鍵の数は、自動バックアップと合わせて一世代になります。バックアップ時に古い鍵は上書きされます。

8.7 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だけです。

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、暗号化が有効なパリティグループを新規作成します。詳しくは、『Encryption License Key ユーザガイド』の暗号化設定の変更を参照してください。

操作手順については、「8.8 お問い合わせ先」へお問い合わせください。

8.8 お問い合わせ先

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

A

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
- A.2 このマニュアルで使用している略語
- A.3 このマニュアルでの表記
- A.4 KB（キロバイト）などの単位表記について

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『オープンシステム構築ガイド』または『メインフレーム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
ID	IDentifier
iSCSI	Internet Small Computer System Interface
LDEV	Logical DEVice
OS	Operating System
SIM	Service Information Message
SM	Shared Memory

A.3 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
VSP One B80	次の製品を区別する必要がない場合の表記です。 • Virtual Storage Platform One Block 85 • 将来サポートされる Virtual Storage Platform One Block 8x（x は 5 以外の 1 桁の数字）

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

1block（ブロック）は 512 バイトです。

1Cyl（シリンダ）を KB に換算した値は、ボリュームのエミュレーションタイプによって異なります。オープンシステムの場合、1Cyl は 960KB です。メインフレームシステムの場合、1Cyl は 870KB です。3380-xx、6586-xx について、CLI の LDEV 容量の表示は、ユーザがデータを格納できるユーザ領域の容量を表示するため、1Cyl を 720KB としています。xx は任意の数字または文字を示します。

用語解説

（英字）

AMC

（Array Management Controller）
HSNBX に搭載される ESM アプリケーションが動作するハードウェア。

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。

CBX

（Controller Box）
CBX は DKC、コントローラシャーシと同義語です。詳しくは、「コントローラシャーシ」を参照してください。CBX2 台を指す場合は CBX ペアと記載する場合があります。

CC

（Concurrent Copy）
IBM 社の Concurrent Copy 機能のことです。

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

Thin Image 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。

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。

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-Separated 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）
任意のサイズに設定できる論理ボリュームです。

CYL

（Cylinder（シリンダ））
複数枚の磁気ディスクから構成される磁気ディスク装置で、磁気ディスクの回転軸から等距離にあるトラックが磁気ディスクの枚数分だけ垂直に並び、この集合を指します。

DKB

（Disk Board）
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）
DKC は CBX、コントローラシャーシと同義語です。また、システムを総称する論理的な呼称として DKC が使われる場合があります。詳しくは、「コントローラシャーシ」を参照してください。

DKU

（Disk Unit）
各種ドライブを搭載するためのシャーシ（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。

EAV

（Extended Address Volume）
IBM 社のストレージシステムが提供している、従来の 3390 型ボリュームではサポートできない大容量のボリュームを定義するための機能です。最大で、1,182,006 シリンダ/ボリュームまで定義できます。

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。

ESE-VOL

（Extent Space - Efficient Volume）
IBM 製品と互換性のある仮想ボリュームで、User Directed Space Release 機能によるページ解放が可能なボリュームです。

ESM

（Embedded Storage Manager）
本ストレージシステム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。

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。

External ポート

外部ストレージシステムを接続するために使用する、ストレージシステムのポートです。

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

Thin Image 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。

FICON

（Fibre Connection）
メインフレームシステム用の光チャネルの一種です。FICON では、ファイバチャネルの標準に基づいて ESCON®の機能が拡張されており、全二重データによる高速データ転送がサポートされています。

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。

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。

Hyper PAV

IBM OS の機能で、PAV の発展機能です。あるベースデバイスに割り当てたエイリアスデバイスが、同一 CU 内のベースデバイスすべてのエイリアスデバイスとして共有化されます。本ストレージシステムで Compatible Hyper PAV 機能を使用することにより、IBM OS から本ストレージシステム上のデバイスに対してこの機能を使えるようになります。

I/O モード

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

I/O レート

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

In-Band 方式

RAID Manager のコマンド実行方式の 1 つです。コマンドを実行すると、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。

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/LU

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

LUN セキュリティ

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

LUN パス、LU パス

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

LUSE ボリューム

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

MCU

(Main Control Unit)
リモートコピーペアのプライマリボリューム（正 VOL）を制御するディスクコントロールユニットです。ユーザによって管理ツールの操作端末から要求されたリモートコピーコマンドを受信・処理し、RCU に送信します。

Mfibre

(Mainframe Fibre)
IBM のメインフレームのファイバチャネルを示す用語です。

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。

MTIR

(Multi Target Incremental Resynchronization)
IBM 社の Multiple Target PPRC 機能で、2 つの副サイト間で作成されるペアです。

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。

MVS

(Multiple Virtual Storage)
IBM 社のメインフレームシステム用 OS です。

Namespace

複数 LBA 範囲をまとめた、論理ボリュームの空間のことです。

Namespace Globally Unique Identifier

Namespace を識別するための、グローバルユニーク性を保証する 16Byte の識別情報です。SCSI LU での NAA Format6 で表現される、WWN に類似する情報です。

Namespace ID

NVM サブシステム上に作成された Namespace を、NVM サブシステムの中でユニークに識別するための識別番号です。

NGUID

（Namespace Globally Unique Identifier）
詳しくは、「Namespace Globally Unique Identifier」を参照してください。

NQN

（NVMe Qualified Name）
NVMe-oF 通信プロトコルで、NVMe ホストまたは NVM サブシステムを特定するためのグローバルユニークな識別子です。

NSID

（Namespace ID）
Namespace を特定するための、4Byte の識別情報です。

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。

NVMe over Fabrics

NVMe-oF 通信プロトコルによる通信を、様々な種類のネットワークファブリックに拡張する NVMe のプロトコルです。

NVMe/TCP

TCP/IP ネットワーク越しにホストとストレージ間で、NVMe-oF 通信プロトコルによる通信をするための NVMe over Fabrics 技術のひとつです。

NVMe コントローラ

NVMe ホストからのコマンド要求を処理する、物理的または論理的な制御デバイスです。

NVM サブシステム

NVM のデータストレージ機能を提供する制御システムです。

NVM サブシステムポート

ホストとコントローラが、NVMe I/O をするための Fabric に接続する通信ポートです。

Open/MF コンシステンシーグループ

Open/MF コンシステンシー維持機能を使用した、コンシステンシーグループのことです。
Open/MF コンシステンシーグループ内の TrueCopy ペアおよび TrueCopy for Mainframe ペアを、同時に分割したり再同期したりできます。

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/AMC/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

Thin Image 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。

PAV

IBM OS の機能で、一つのデバイスに対して複数の I/O 操作を並行して発行できるようにする機能です。本ストレージシステムで Compatible PAV 機能を使用することにより、IBM OS から本ストレージシステム上のデバイスに対してこの機能を使えるようになります。

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。

PPRC

（Peer-to-Peer Remote Copy）
IBM 社のリモートコピー機能です。

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

RAID

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

RAID Manager

コマンドインタフェースでストレージシステムを操作するためのプログラムです。

RCU

（Remote Control Unit）
リモートコピーペアのセカンダリボリューム（副 VOL）を制御するディスクコントロールユニットです。リモートパスによって MCU に接続され、MCU からコマンドを受信して処理します。

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。

RCU Target ポート

Initiator ポートと接続します。RCU Target ポートは、ホストのポートとも通信できます。

RDEV

（Real Device）
IBM 用語です。DASD の実装置アドレスを意味します。

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。

S/N

(Serial Number)
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。

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。

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。原因となるエラーを解決し、VSP One Block Administrator 画面上で SIM が解決したことを報告することを、「SIM をコンプリートする」と言います。

SM

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

SMS

(Storage Management Subsystem)
IBM 社のメインフレームの OS が提供するツールで、データセットを容易かつ効率的に割り当てることができます。

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。

SSID

ストレージシステムの ID です。ストレージシステムでは、搭載される LDEV のアドレスごと（64、128、256）に 1 つの SSID が設定されます。

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。

Super PAV

IBM OS の機能で、Hyper PAV の拡張機能です。あるベースデバイスに割り当てたエイリアスデバイスが、複数 CU 内のすべてのベースデバイスのエイリアスデバイスとして共有化されます。本ストレージシステムで Super PAV 機能を有効にすれば、IBM OS から本ストレージシステム上のデバイスに対してこの機能を使えるようになります。

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。

TSE-VOL

（Track Space - Efficient Volume）
DP-VOL 同様の仮想ボリュームですが、IBM 製品の FlashCopy、および Compatible Software for IBM® FlashCopy® SE のターゲットボリュームとしてのみ使用できます。IBM ホストから認識できるよう互換を保持しています。DP-VOL とプールを共用するため、TSE-VOL を使用するためには、Compatible Software for IBM® FlashCopy® SE だけではなく、Dynamic Provisioning for Mainframe のライセンスもインストールする必要があります。

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。

Vary Offline

メインフレームシステム用ホストとオンライン接続しているデバイスを、オフライン状態に切り替える操作です。Vary Offline の操作をするには、メインフレームシステム用ホストからコマンドを実行します。

Vary Online

デバイスをメインフレームシステム用ホストとオンライン接続するための操作です。Vary Online の操作をするには、メインフレームシステム用ホストからコマンドを実行します。

vClone Parent 属性のボリューム

Thin Image 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

Thin Image 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）
IBM 用語です。DASD の仮想アドレスを意味します。
または、Hitachi 用語でパリティグループ内にある論理ボリュームのグループを意味します。VDEV は任意のサイズの論理ボリューム（CV）とフリースペースから構成されます。VDEV 内に任意のサイズの論理ボリューム（CV）とフリースペース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。

VSP One Block Administrator

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。

VTOC

（Volume Table of Contents）
ディスク上の複数データセットのアドレスや空き領域を管理するための情報を格納するディスク領域です。

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。

zHyperWrite 機能

IBM 社の DS シリーズ ディスクアレイ装置でサポートしている zHyperWrite の互換機能です。上位アプリケーションである DB2 のログを書き込むときに行われる二重化処理で、TrueCopy for Mainframe の更新コピーを使用して二重化処理を行うのではなく、ホストから TrueCopy for Mainframe のプライマリボリュームおよびセカンダリボリュームに対して書き込みを行います。zHyperWrite の詳細については、IBM のマニュアルを参照してください。

（ア行）

アクセス属性

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

アクセスパス

ストレージシステム内の、データとコマンドの転送経路です。

インクリメンタルリシンク

IBM 社の Multiple Target PPRC 機能で、MTIR ペア間で実行される差分コピーです。

インスタンス

特定の処理を実行するための機能集合のことです。

インスタンス番号

インスタンスを区別するための番号です。1 台のサーバ上で複数のインスタンスを動作させるとき、インスタンス番号によって区別します。

エクステント

IBM 社のストレージシステム内で定義された論理デバイスは、ある一定のサイズに分割されて管理されます。この、分割された最小管理単位の名称です。

エミュレーション

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

（カ行）

外部ストレージシステム

本ストレージシステムに接続されているストレージシステムです。

外部パス

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

外部ボリューム

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。

鍵管理サーバ

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

書き込み待ち率

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

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、または Dynamic Provisioning for Mainframe 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。

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。

構成定義ファイル

RAID Manager を動作させるためのシステム構成を定義するファイルを指します。

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。

コピーグループ

プライマリボリューム（正側ボリューム）、およびセカンダリボリューム（副側ボリューム）から構成されるコピーペアを 1 つにグループ化したものです。または、正側と副側のデバイスグループを 1 つにグループ化したものです。RAID Manager でレプリケーションコマンドを実行する場合、コピーグループを定義する必要があります。

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。

コレクションコピー

ストレージシステム内のディスク障害を回復するためのコピー動作のことです。予備ディスクへのコピー、または交換ディスクへのコピー等が含まれます。

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。

コントローラシャーシ

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。コントローラシャーシは DKC、CBX と同義語です。

（サ行）

サーバ証明書

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

サイドファイル

コンカレントコピーで使用している内部のテーブルです。
コピー未完了部分に更新 I/O が発生した際、バックアップデータ（スナップショット）をサイドファイルに退避することで、コピー先のデータ整合性を正しく保つために使用されます。

サイドファイルキャッシュ

コンカレントコピー実施中に生成されるバックアップデータ（スナップショット）を格納する領域で、キャッシュ内に一時的に確保されます。

サブシステム NQN

NVM サブシステムに定義された NQN です。
NQN の詳細については、「NQN」を参照してください。

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。

差分データ

ペアボリュームがサスペンドしたときの状態からの正ボリュームへの更新データのことです。

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。

システムディスク

ストレージシステムが使用するボリュームのことです。一部の機能を使うためには、システムディスクの作成が必要です。

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

Universal Replicator と Universal Replicator for Mainframe 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。

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。

状態遷移

ペアボリュームのペア状態が変化することです。

冗長パス

チャネルボード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。

シンプル 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。

スナップショットグループ

Thin Image 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

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

スワップ

プライマリボリューム/セカンダリボリュームを逆転する操作のことです。

正 VOL、正ボリューム

詳しくは「プライマリボリューム」を参照してください。

正サイト

通常時に、業務（アプリケーション）を実行するサイトを指します。

セカンダリボリューム

ペアとして設定された 2 つのボリュームのうち、コピー先のボリュームを指します。なお、プライマリボリュームとペアを組んでいるボリュームをセカンダリボリュームと呼びますが、Thin Image 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。

絶対 LUN

SCSI/iSCSI/Fibre ポート上に設定されているホストグループとは関係なく、ポート上に絶対的に割り当てられた LUN を示します。

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。

専用 DASD

IBM 用語です。z/VM 上の任意のゲスト OS のみ利用可能な DASD を意味します。

ソースボリューム

Compatible FlashCopy®、および Volume Migration の用語で、Compatible FlashCopy®の場合はボリュームのコピー元となるボリュームを、Volume Migration の場合は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。

（タ行）

ターゲットボリューム

Compatible FlashCopy®、および Volume Migration の用語で、Compatible FlashCopy®の場合はボリュームのコピー先となるボリュームを、Volume Migration の場合はボリュームの移動先となる領域を指します。

チャネルエクステンダ

遠隔地にあるメインフレームホストをストレージシステムと接続するために使われるハードウェアです。

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。Thin Image 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。

データ削減共有ボリュームには、容量削減設定が有効なデータ削減共有ボリュームと、容量削減設定が無効なデータ削減共有ボリュームという 2 種類があります。詳しくは、「容量削減設定が有効なデータ削減共有ボリューム」または「容量削減設定が無効なデータ削減共有ボリューム」を参照してください。

転送レート

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

同期コピー

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

トポロジ

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

ドライブボックス

各種ドライブを搭載するためのシャーシ（筐体）です。

（ナ行）

内部ボリューム

本ストレージシステムが管理するボリュームを指します。

（ハ行）

パリティグループ

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

非対称アクセス

global-active device でのクロスパス構成など、サーバとストレージシステムを複数の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、Dynamic Provisioning for Mainframe、および Thin Image 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 および Dynamic Provisioning for Mainframe ではプールボリュームに通常のデータを格納し、Thin Image Advanced ではスナップショットデータをプールボリュームに格納します。

副 VOL、副ボリューム

詳しくは「セカンダリボリューム」を参照してください。

副サイト

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

プライマリボリューム

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

フラッシュメモリ

各プロセッサに搭載され、ソフトウェアを格納している不揮発性のメモリです。

ブロック

ボリューム容量の単位の一種です。1 ブロックは 512 バイトです。

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たり、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。Dynamic Provisioning の場合、1 ページは 42MB、Dynamic Provisioning for Mainframe の場合、1 ページは 38MB 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-Namespace パス

日立ストレージシステムで、Namespace セキュリティを使用する際に、ホスト NQN ごとに各 Namespace へのアクセス可否を決定するための設定です。
Namespace パスとも呼びます。

ホスト NQN

NVMe ホストに定義された NQN です。
NQN の詳細については、「NQN」を参照してください。

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

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

ホストモード

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

（マ行）

マイグレーションボリューム

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。

ミニディスク DASD

IBM 用語です。z/VM 上で定義される仮想 DASD を意味します。

（ヤ行）

容量削減設定が無効なデータ削減共有ボリューム

Adaptive Data Reduction の容量削減機能が有効、かつ、容量削減設定（「圧縮」または「重複排除および圧縮」）が無効である仮想ボリュームを指します。

容量削減設定が有効なデータ削減共有ボリューム

Adaptive Data Reduction の容量削減機能が有効、かつ、容量削減設定（「圧縮」または「重複排除および圧縮」）が有効である仮想ボリュームを指します。

（ラ行）

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。

レコードセット

非同期コピーの更新コピーモードでは、正 VOL の更新情報と制御情報をキャッシュに保存します。これらの情報をレコードセットといいます。ホストの I/O 処理とは別に、RCU に送信されます。

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

Audit Log 55

E

Encryption License Key 67

I

iSCSI CHAP 65

L

LDAP 37, 38
LUN セキュリティ 63

M

Media Sanitization 機能 15

N

Namespace セキュリティ 64

P

PKCS#12 形式 68

S

SNMP 59
　SNMP エンジン ID 登録 61
　SNMP トラップ送信 60
　SNMP の送信情報を設定 60
SSL/TLS 44

W

Web サーバ接続用証明書 48

あ

アクセス制御 13, 14
暗号化
　有効 74
暗号化鍵
　作成 72
　バックアップ 72–74
暗号化環境設定 69

か

外部認証 37
鍵管理サーバ 68
　要件 68
監査ログ 15
　Syslog サーバに転送 55, 56

く

クライアント証明書 68

こ

公開鍵 45

し

署名付き証明書 46

は

バックアップ
　暗号化鍵 72

ひ

秘密鍵 45
ビルトインアカウント 20
ビルトイングループ 23

ほ

ポート 16

ゆ

ユーザ管理 25
　パスワードを変更 37
　ユーザアカウントの削除 36
　ユーザアカウントの無効化 36
　ユーザアカウントポリシーの設定 25
　ユーザの作成 34

よ

要件
　外部認証サーバ・外部認可サーバ 38
　鍵管理サーバ 68
　証明書 41

る

ルート証明書 68

ろ

ロール 22

日立ヴァンタラ株式会社
〒 244-0817 神奈川県横浜市戸塚区吉田町 292 番地