HITACHI
Inspire the Next

セキュリティ設定ガイド

Hitachi Virtual Storage Platform 5000 シリーズ

4047-1J-U68-60

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

著作権

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。
Emulex は，米国Emulex Corporation の登録商標です。
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。
GPFS は，米国およびその他の国におけるInternational Business Machines Corporation の商標です。
HACMP 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。
IRIX は，Silicon Graphics，Inc.の登録商標です。
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。
NetWare は，米国Novell，Inc.の登録商標です。
Oracle とJava は，Oracle Corporation 及びその子会社，関連会社の米国及びその他の国における登録商標です。
QLogic は，QLogic Corporation の登録商標です。
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 は，Symantec Corporation の米国およびその他の国における商標または登録商標です。
VMware は，米国およびその他の地域における VMware，Inc. の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。
Windows Server 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。
XFS は，Silicon Graphics，Inc.の商標です。
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

2022 年 5 月 (4047-1J-U68-60)

目次

はじめに 1
対象ストレージシステム..... 2
マニュアルの参照と適合プログラムバージョン..... 2
対象読者..... 3
本書に記載されている画面図について..... 3
発行履歴..... 3
1. セキュリティ設定の概要..... 7
1.1 概要..... 8
1.2 想定する利用者..... 8
1.3 主要セキュリティ機能..... 9
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 9
1.3.2 ホストのアクセス制御機能 11
1.3.3 ストレージ管理者および保守員の識別・認証機能 11
1.3.4 Storage Navigator (ストレージ管理UIソフトウェア)－SVP PC (管理保守IF PC)間およびSVP PC (管理保守IF PC)－外部認証サーバ間の暗号化通信..... 12
1.3.5 格納データ暗号化機能 12
1.3.6 シュレッディング機能 12
1.3.7 監査ログ機能 13
1.3.8 Media Sanitization機能..... 13
1.4 ポート番号..... 13
1.5 最新のソフトウェアの適用..... 14
2. 物理セキュリティ..... 15
2.1 運用環境の物理セキュリティについて..... 16
3. Hitachi Storage Navigator..... 17
3.1 ビルトインアカウントのパスワード変更..... 18
3.2 ユーザ管理モデル..... 18
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 18
3.2.2 ロール 19
3.2.3 ビルトイングループ 22

3.3 ユーザ管理 24
3.3.1 ユーザの作成 24
3.3.2 ユーザアカウントの削除 27
3.3.3 ユーザアカウントの無効化 27
3.3.4 パスワードの変更(ユーザ) 29
3.4 外部認証サーバと認可サーバを使用したユーザ管理 29
3.4.1 認証サーバを用いた外部認証の要件 30
3.4.2 認可サーバを用いた外部認可の要件 33
3.4.3 外部認証サーバに接続する 35
3.4.4 認可サーバとの連携を有効にする 36
3.4.5 認証サーバの情報を参照する。 36
3.5 TLS バージョンと暗号スイートを管理する 37
3.6 サーバ証明書の更新 40
3.6.1 秘密鍵を作成する 40
3.6.2 公開鍵を作成する 41
3.6.3 署名付き証明書の取得 43
3.6.4 Hitachi Storage Navigator サーバ証明書の更新 44
3.7 HTTP 通信を無効にする 46
3.8 HTTP Strict Transport Security を有効にする (保守員作業) 47
4. SMI-S Provider 49
4.1 SMI-S サーバ証明書の更新 50
5. Audit Log 53
5.1 監査ログ情報を Syslog サーバに転送する 54
6. SNMP 57
6.1 SNMP の送信情報を設定する 58
6.2 SNMP トラップの通知先を設定する(SNMPv3) 58
6.3 リクエスト許可対象を設定する(SNMPv3) 60
7. LUN Manager/Security 61
7.1 LUN セキュリティを設定する 62
8. iSCSI CHAP 認証 65
8.1 iSCSI ターゲットを作成し、ホストを登録する 66
8.2 CHAP ユーザを登録する 68
8.3 CHAP ユーザを削除する 69
8.4 ターゲット CHAP ユーザを削除する 70
8.5 ポート CHAP ユーザを削除する 70
9. Encryption License Key 73
9.1 鍵管理サーバを利用する 74
9.1.1 鍵管理サーバの要件 74
9.1.2 鍵管理サーバのルート証明書の取得 74

9.1.3 クライアント証明書の作成 74
9.2 暗号化環境を設定する 75
9.3 暗号化鍵を作成する 78
9.4 暗号化鍵をバックアップする 79
9.5 Storage Navigator 動作 PC 内に暗号化鍵をファイルとしてバックアップするときに設定するパスワードの最小文字数を設定する 80
9.6 Storage Navigator 動作 PC 内にファイルとして暗号化鍵をバックアップする 80
9.7 鍵管理サーバに接続して暗号化鍵をバックアップする 81
9.8 データの暗号化を有効にする 82

はじめに

このマニュアルは、Hitachi Virtual Storage Platform 5000 シリーズ（以下、VSP 5000 シリーズと略します）用の『セキュリティ設定ガイド』です。
本書では、Hitachi Virtual Storage Platform 5000 シリーズが提供する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
- □ 本書に記載されている画面図について
- □ 発行履歴

対象ストレージシステム

このマニュアルでは、次に示すVSP 5000シリーズ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。

- Virtual Storage Platform 5100
- Virtual Storage Platform 5200
- Virtual Storage Platform 5500
- Virtual Storage Platform 5600
- Virtual Storage Platform 5100H
- Virtual Storage Platform 5200H
- Virtual Storage Platform 5500H
- Virtual Storage Platform 5600H

このマニュアルでは特に断りのない限り、VSP 5000 シリーズのストレージシステムを単に「ストレージシステム」と称することがあります。

VSP 5100H, VSP 5200H, VSP 5500H, VSP 5600Hは、ハイブリッドフラッシュアレイモデルです。オールフラッシュアレイモデルとハイブリッドフラッシュアレイモデルの対応関係を次の表に示します。両方のモデルで、設定可能値や操作は基本的に同じです。このため、このマニュアルでは、両方のモデルを代表して、オールフラッシュアレイモデルの名称を使って説明します。オールフラッシュアレイモデルとハイブリッドフラッシュアレイモデルで、設定可能値や操作が異なる場合にのみ、それぞれのモデルの名称を使って説明します。

オールフラッシュアレイモデル	ハイブリッドフラッシュアレイモデル
VSP 5100	VSP 5100H
VSP 5200	VSP 5200H
VSP 5500	VSP 5500H
VSP 5600	VSP 5600H

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、DKCMAINプログラムバージョン90-08-42-XXに適合しています。

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

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

本書に記載されている画面図について

このマニュアルに掲載されている画面図はサンプルであり、実際に表示される画面と若干異なる場合があります。また、画面に表示される項目名は、ご利用環境により異なる場合があります。

このマニュアルでは、Windows コンピュータ上の画面を掲載しています。

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

発行履歴

マニュアル資料番号	発行年月	変更内容
4047-1J-U68-60	2022年5月	適合DKCMAIN ファームウェアバージョン：90-08-42-XX • Storage Navigator動作PCとSVP間で使用するポート番号とプロトコルを修正した。 ・ 1.4 ポート番号 ・ 3.5 TLSバージョンと暗号スイートを管理する
4047-1J-U68-50	2021年8月	適合DKCMAIN ファームウェアバージョン：90-08-01-XX • ストレージシステムの新しいモデルとして次のモデルを追加した。 ・ VSP 5200, 5200H ・ VSP 5600, 5600H
4047-1J-U68-40	2021年6月	適合DKCMAIN ファームウェアバージョン：90-07-01-XX • ホストとストレージシステム間のFC-NVMeによる接続をサポートした。 ・ 7 LUN Manager/Security ・ 7.2 Namespaceセキュリティを設定する
4047-1J-U68-31	2020年7月	適合DKCMAIN ファームウェアバージョン：90-04-04-XX • Syslogサーバのホスト名指定を可能にした。 ・ 5.1 監査ログ情報をSyslogサーバに転送する
4047-1J-U68-30	2020年4月	適合DKCMAIN ファームウェアバージョン：90-04-01-XX • TLS セキュリティ設定に関する記載を変更した。

マニュアル資料番号	発行年月	変更内容
		・ 3.4.1 認証サーバを用いた外部認証の要件 ・ 3.4.2 認可サーバを用いた外部認可の要件 ・ 3.6.4 Hitachi Storage Navigatorサーバ証明書の更新 ・ SMI-Sサーバ証明書の更新 • Media Sanitizationに関する説明を記載した。 ・ 10. Media Sanitization
4047-1J-U68-20	2020 年 2 月	適合DKCMAIN ファームウェアバージョン：90-03-01-XX • TLS セキュリティ設定に関する記載を変更した。 ・ 1.1 概要 ・ 1.2 想定する利用者 ・ 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 ・ 1.3.2 ホストのアクセス制御機能 ・ 1.3.3 ストレージ管理者および保守員の識別・認証機能 ・ 1.3.4 Storage Navigator（ストレージ管理UIソフトウェア）－SVP PC（管理保守IF PC)間およびSVP PC（管理保守IF PC）－外部認証サーバ間の暗号化通信 ・ 1.4 ポート番号 ・ 2.1 運用環境の物理セキュリティについて ・ 3. Hitachi Storage Navigator ・ 3.1 ビルトインアカウントのパスワード変更 ・ 3.2.2 ロール ・ 3.3.2 ユーザアカウントの削除 ・ 3.3.4 パスワードの変更(ユーザ) ・ 3.4.1 外部認証サーバの要件 ・ 3.4.2 認可サーバの要件 ・ 3.5 TLSバージョンと暗号スイートを管理する ・ 3.6.1 秘密鍵を作成する ・ 3.6.4 Hitachi Storage Navigatorサーバ証明書の更新 ・ 4.1 SMI-Sサーバ証明書の更新 ・ 9. Encryption License Key ・ 9.1.1 鍵管理サーバの要件 ・ 9.3 暗号化鍵を作成する ・ 9.5 Storage Navigator 動作PC 内に暗号化鍵をファイルとしてバックアップするときに設定するパスワードの最小文字数を設定する
4047-1J-U68-10	2019 年 11 月	適合DKCMAIN ファームウェアバージョン：90-02-01-XX
4047-1J-U68-01	2019 年 9 月	適合DKCMAIN ファームウェアバージョン：90-01-51-XX

マニュアル資料番号	発行年月	変更内容
4047-1J-U68-00	2019 年 8 月	新規 適合DKCMAIN ファームウェアバージョン：90-01-61-XX

1

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

Hitachi Virtual Storage Platform シリーズは、Hitachi Storage Virtualization Operating System(SVOS) RF および Hitachi Device Manager - Storage Navigator により提供されるストレージシステムです。ユーザ認証・認可、監査ログによる追跡、データの暗号化、データの消去など、セキュリティ機能が利用できます。

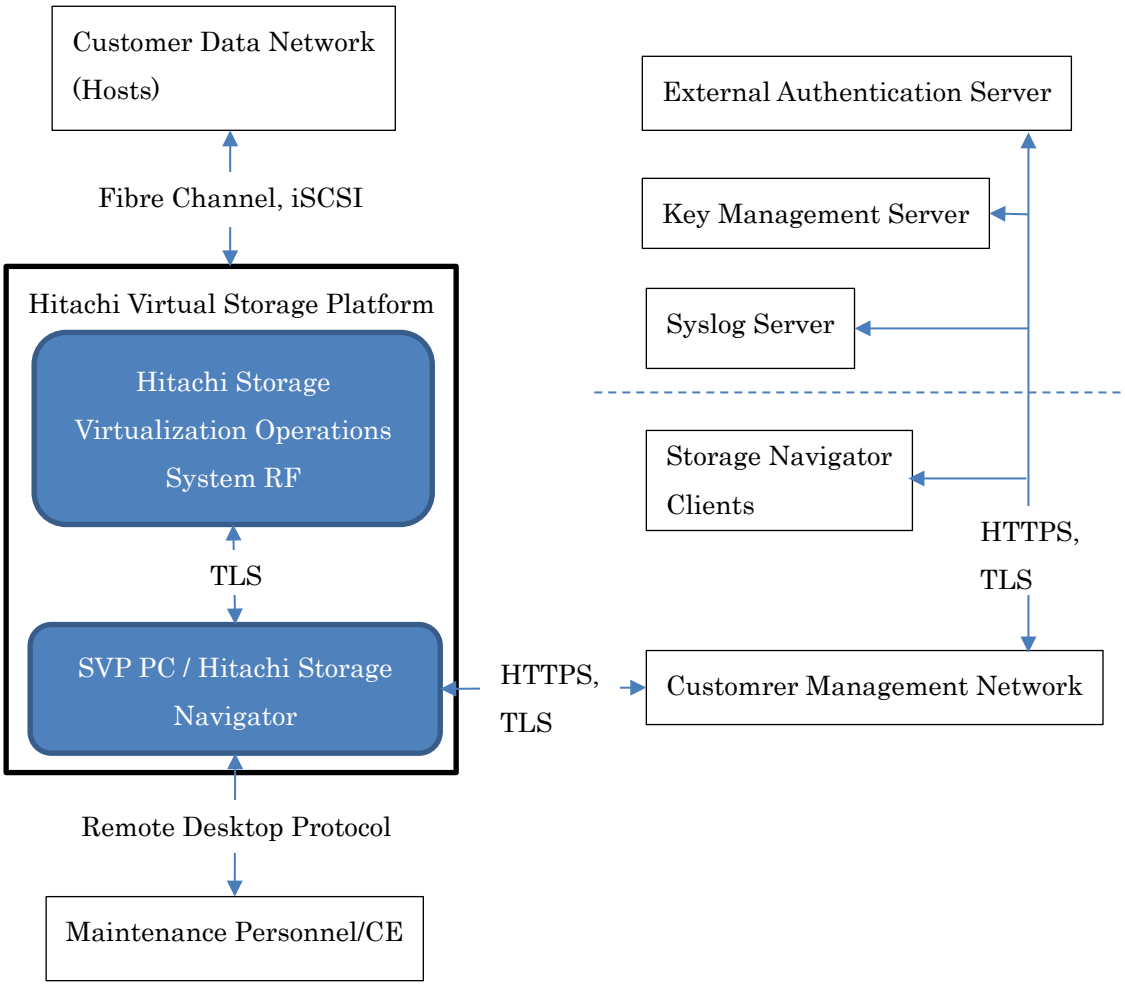


図 1-1　セキュリティ構成図

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、Hitachi Storage Navigator(ストレージ管理ユーザインタフェース(UI)ソフトウェア)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：

Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア) 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、ディスク等)を管理できる管理者。

・ 監査ログ管理者：

Hitachi Virtual Storage Platform で取得している監査ログを管理できる管理者。Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア) 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：

Hitachi Virtual Storage Platform 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。Hitachi Virtual Storage Platform 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 を使用して、Hitachi Virtual Storage Platform に対する保守・管理用のインタフェースを提供している SVP PC (管理保守インタフェース(IF) PC)と呼ばれる PC へアクセスし、保守作業を実施します。直接、ディスクストレージ装置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。保守員はディスクストレージ装置内の全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：

Hitachi Virtual Storage Platform の利用者でホストを表します。Hitachi Virtual Storage Platform と接続されたホストから、Hitachi Virtual Storage Platform 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

Hitachi Virtual Storage Platform 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

Hitachi Virtual Storage Platform 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り、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等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図 1-2 に示します。

本機能により、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。

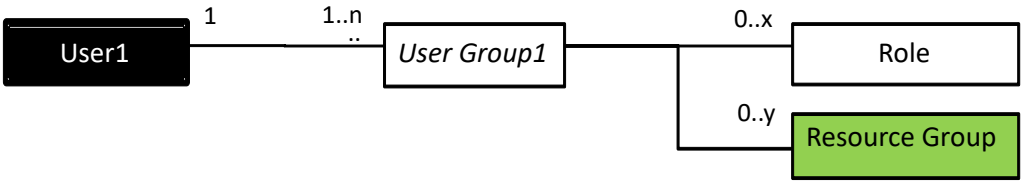


図 1-2 ユーザ、ユーザグループ、ロール、リソースグループの関係

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 Hitachi Virtual Storage Platform 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のみを実行できます。

(1) ロール

セキュリティ管理者は、Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)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。

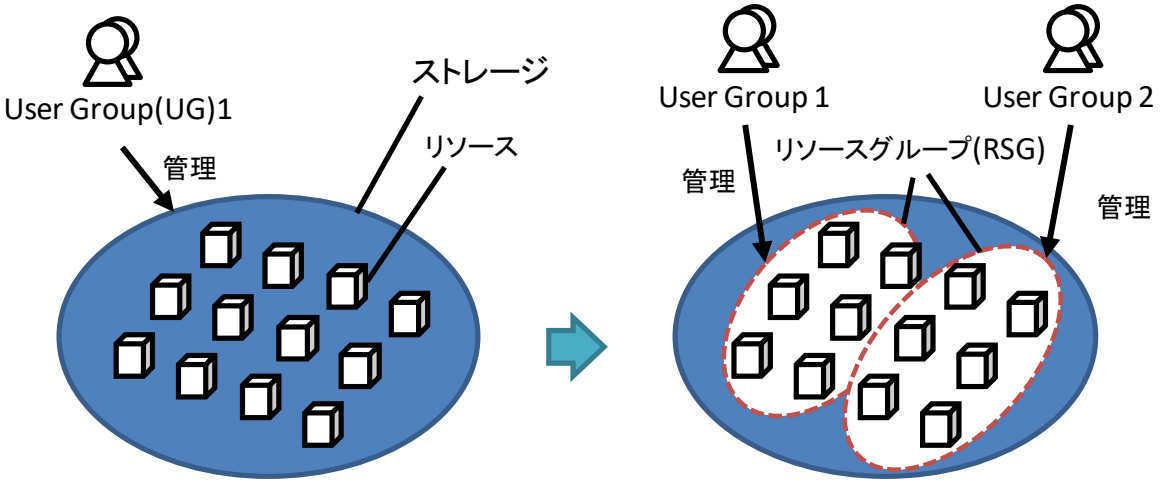
表 1-1 ロールの分類と操作内容

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、ディスクストレージ装置の保守

ロール	実施可能な操作
	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、全てのリソースグループが割当てられるため、全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、Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)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

Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)は、顧客によって、セキュリティ機能の設定を含む Hitachi Virtual Storage Platform の管理を行うために使用されます。Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)を用いてディスクサブシステムの管理（各機能の構成や設定の変更等）を行う場合、および保守員が SVP PC にリモートデスクトップ接続を行う場合に Hitachi Virtual Storage Platform によりユーザの識別と認証が行なわれます。識別・認証に 3 回連続で失敗した場合は、当該ユーザの識別・認証を 1 分間拒否します。

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。

(1)ストレージシステム内部認証方式

Hitachi Virtual Storage Platform 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。

(2)外部認証サーバ方式

Hitachi Virtual Storage Platform 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)、RADIUS(認証プロトコルは CHAP)、および Kerberos をサポートします。

1.3.4 Storage Navigator (ストレージ管理 UI ソフトウェア)－SVP PC (管理保守 IF PC) 間および SVP PC (管理保守 IF PC)－外部認証サーバ間の暗号化通信

Hitachi Virtual Storage Platform と管理 PC 間の通信データの漏洩、改ざんを防ぐため、Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)と SVP PC 間の通信は TLS により暗号化します。また、SVP PC－外部認証サーバ間の通信は LDAPS、RADIUS(認証プロトコルは CHAP) 、および Kerberos プロトコルのいずれかを使用することにより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

Hitachi Virtual Storage Navigator 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、DKB に搭載されているハードウェア(LSI)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ディスクドライブを交換するとき、あるいは、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。

(1) 暗号鍵作成機能

(2) 暗号鍵削除機能

(3) 暗号鍵バックアップ、リストア機能

(4) 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 シュレッディング機能

論理ボリューム(LDEV)内のすべてのデータを、ダミーデータで上書きすることで、データを復元できないようにする機能で、ボリューム再利用時のデータ漏洩/不正利用を防ぐことが可能になります。

シュレッディング機能を実行すると、ユーザデータが書き込まれたボリューム全体にダミーデータが書込まれ、ユーザデータは復元できなくなります。本機能では、DoD5220.22-M に準拠し、少なくとも 3 回はダミーデータをボリュームに書き込むことを推奨し、デフォルトの設定では、ボリューム全体に 3 回ダミーデータが書込まれるようになっています。

シュレッディング機能はストレージ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。

1.3.7　監査ログ機能

監査ログ機能は、SVP プログラム(Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)を含む)および Hitachi Storage Virtualization Operating System RF によって提供されます。Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)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、そのコピーは最大 250,000 行分の情報が SVP PC 内に格納されます。

Hitachi Storage Navigator (ストレージ管理 UI ソフトウェア)は、監査ログを参照するインタフェースを提供します。

1.3.8　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　ポート番号

Hitachi Storage Navigator が使用するポート番号を以下に示します。

ストレージシステムと連携するミドルウェアやアプリケーションなどのソフトウェアが使用するポートについては、各ソフトウェアのマニュアルを参照してください。

プロトコル	送信元		送信先	
	ポート番号	ハードウェア	ポート番号	ハードウェア
HTTP	any/TCP	Storage Navigator動作PC	80/TCP	SVP
HTTPS	any/TCP	Storage Navigator動作PC	443/TCP	SVP
RMI	any/TCP	Storage Navigator動作PC	11099/TCP	SVP
RMI	any/TCP	Storage Navigator動作PC	51099/TCP	SVP
RMI	any/TCP	Storage Navigator動作PC	51100/TCP	SVP
SMI-S	any/TCP	Storage Navigator動作PC	427/TCP	SVP
SMI-S	any/TCP	Storage Navigator動作PC	5989/TCP	SVP
SNMP※1	any/UDP	Storage Navigator動作PC	161/UDP	SVP
SNMP Trap※1	any/UDP	SVP	162/UDP	Storage Navigator動作PC

プロトコル	送信元		送信先	
	ポート番号	ハードウェア	ポート番号	ハードウェア
RAID Manager	any/UDP	ホスト	31xxx～33xxx/UDP※2	SVP
RAID Manager	34xxx～36xxx/UDP※2	SVP	any/UDP	ホスト
raidinf	any/TCP	Storage Navigator動作PC	5443/TCP	SVP

注※1 : Storage Navigator 動作 PC を SNMP マネージャとして使用する場合に、このポート番号を使用します。

注※2 : xxx は、3 桁の数字です。RAID Manager によるホストと SVP 間の通信で使用されるポート番号については、『RAID Manager ユーザガイド』を参照してください。

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ファームウェアに実施されます。最新のソフトウェアおよびファームウェアの適用、ならびに、SVP PC へのセキュリティパッチ適用を定期的に実施してください。

2

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

- 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、Hitachi Virtual Storage Platform 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通りの操作を行い、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、Hitachi Virtual Storage Platform 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において Hitachi Virtual Storage Platform の管理・運用を行うため、手順書で定められた通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、Hitachi Virtual Storage Platform、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のみ入退出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、鍵管理サーバをセキュリティ管理者のみ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。
- 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のみ入退室が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。
- 保守員は、組織の責任者の指示に従い、保守員 PC をセキュアなエリアに適切に設置する。保守員 PC は保守員以外の人間が利用できないようにし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 Hitachi Virtual Storage Platform がサポートしている SVP PC との通信を保護することができるプロトコル(LDAPS、RADIUS(認証プロトコルは CHAP)、および Kerberos)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 Hitachi Virtual Storage Platform 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。
- 運用環境では、ディスクドライブからユーザデータが漏洩しないように、DKB に搭載されているハードウェア(LSI)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。

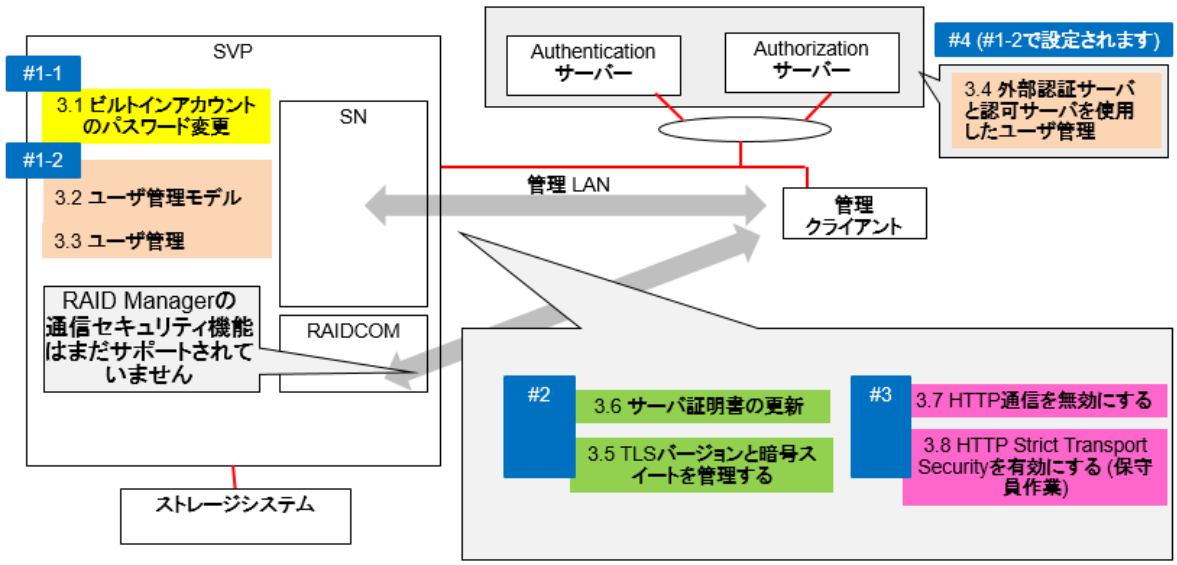
3

3. Hitachi Storage Navigator

本章では、Hitachi Storage Navigator を使用するにあたって必要な設定について説明します。Storage Navigator のユーザを登録する流れを説明します。

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、Storage Navigator にログインできます。認証サーバを使用しない場合は、Storage Navigator 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。

下図中の、手順 #1 から#4 までを実行することで Storage Navigator のセキュリティ設定が実行できます。なお、REST インタフェースのセキュリティ設定も同時に実行されます。



3.1　ビルトインアカウントのパスワード変更

Hitachi Storage Navigator 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 Storage Navigator 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。

手順

(1)　Hitachi Storage Nagvigator にビルトインアカウントでログインする。

(2)　［設定］ -［ユーザ管理］ -［パスワード変更］を選択して、ビルトインユーザアカウントのパスワードを変更する。

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、Hitachi Storage Navigator ユーザの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。登録されたユーザは、Hitachi Storage Navigator だけでなく、RAID Manager も使用できます。

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。

<u>ユーザグループに関する注意事項</u>

- 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 Storage Navigator 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、Storage Navigator 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

ロールはあらかじめ複数用意されており、独自にロールを作成できません。ロールと許可

されている操作を次に示します。

ロール	許可されている操作
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 • 鍵管理サーバにある暗号鍵の情報参照
セキュリティ管理者（参照・編集）	• ユーザアカウントの設定 • 暗号鍵の生成 • 暗号の設定 • 暗号鍵の生成場所の参照と切り替え • 暗号鍵のバックアップ、リストア • 鍵管理サーバにあるバックアップされた暗号鍵の削除 • Storage Navigator 動作PC 内に暗号鍵をバックアップするときのパスワードポリシーの参照と変更 • 外部サーバへの接続設定 • 外部サーバへの接続設定のバックアップ、リストア • SSL 通信で使用する証明書の設定 • リソースグループの設定 • 仮想管理設定の編集 • global-active device の予約属性の設定 • TLS セキュリティ設定 • CSR 作成設定
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
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 • ストレージシステムの構成レポートの参照、削除、およびダウンロード • [すべて更新] によるストレージシステムの全情報の取得および Storage

ロール	許可されている操作
	Navigator の画面表示の更新
ストレージ管理者（システムリソース管理）	• CLPR の設定 • MP ユニットの設定 • タスクの削除およびリソース排他の強制解除 • SIM のコンプリート ※2 • ポート属性の設定 • LUN セキュリティの設定 • Server Priority Manager の設定 • 階層割り当てポリシーの設定
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、シュレッディング • 外部ボリュームの設定 • Compatible PAV のエイリアスボリューム設定 • Dynamic Provisioning に関する設定 • ホストグループ、パス、WWN 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 • 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 • SIM のコンプリート ※2 • 仮想管理設定の編集

ロール	許可されている操作
	• global-active device の予約属性の設定
ストレージ管理者（パフォーマンス管理）	• モニタリングの設定 • モニタリングの開始、停止
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 • RAID Manager を使用したVolume Migration のペア解除
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）
保守（ベンダ専用）※1	• SVP に関する操作（通常日立の保守員に許可する操作です） • ダンプツールを使用したダンプファイルのダウンロード

注※1：保守（ベンダ専用）ロールは、通常日立の保守員に割り当てられるロールですが、ユーザのアカウントに割り当てると、ダンプツールを使用してダンプファイルをダウンロードできるようになります。

注※2：SIM のコンプリートは、ストレージ管理者（システムリソース管理）ロールとストレージ管理者（プロビジョニング）ロールの両方が割り当てられているユーザに許可されています。

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
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
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
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

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
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） • 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）	全リソースグループ

3.3 ユーザ管理

Hitachi Storage Navigator 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。

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

ユーザ名およびパスワードの要件

ユーザ名およびパスワードの文字数および使用できる文字は、Storage Navigator、SVP、RAID Manager、および raidinf コマンドのうち、ユーザがどのアプリケーションを使用するかによって異なります。ユーザが複数のアプリケーションを使う場合は、使用するすべてのアプリケーションの条件を満たすようにユーザ名およびパスワードを指定してください。

Storage Navigator へログインする場合のユーザ名およびパスワードを次に示します。

項目	文字数	指定できる文字
ユーザ名	1～256 文字	• 半角英数字 • 次の記号 # $ % & ' * + - . / = ? @ ^ _ ` { | } ~ ［ツールパネル］画面から起動する画面で入力するユーザ名に、#は使用できません。
パスワード	6～256 文字	• 半角英数字 • すべての記号 ［ツールパネル］画面から起動する画面で入力するパスワードに、" と¥は使用できません。

SVP へログインする場合のユーザ名およびパスワードを次に示します。

項目	文字数	指定できる文字
ユーザ名	1～128 文字	• 半角英数字 • 次の記号 ! # $ % & ' - . @ ^ _ ` { } ~
パスワード	6～127 文字	• 半角英数字 • すべての記号

RAID Manager および raidinf コマンドへログインする場合のユーザ名およびパスワードを次に示します。

項目	文字数	指定できる文字
ユーザ名	1～63 文字	• 半角英数字 • 次の記号※1 - . @ _
パスワード	6～63 文字	• 半角英数字 • 次の記号※2 - , . : @ _

注※1：RAID Manager および raidinf コマンドがインストールされているホストが UNIX の場合、スラッシュ（/）も指定できます。

注※2：RAID Manager および raidinf コマンドがインストールされているホストが Windows の場合、円マーク（¥）も指定できます。RAID Manager および raidinf コマンドがインストールされているホストが UNIX の場合、スラッシュ（/）も指定できます。

操作手順

(1) Storage Navigator の［管理］ツリーから［ユーザグループ］を選択します。

(2) ［ユーザグループ］タブでユーザを所属させたいユーザグループをクリックします。ユーザに与えたい権限に応じて、どのユーザグループに所属させるかを決めてください。

(3) ［ロール］タブで、そのユーザグループに設定されている権限をユーザに与えてよいかを確認します。

(4) 次のどちらかの方法で、［ユーザ作成］画面を表示します。

・［ユーザ］タブで［ユーザ作成］をクリックします。

・［ユーザ］タブを選択し、［設定］メニューから［ユーザ管理］-［ユーザ作成］を選択します。

(5) ユーザ名を入力します。

(6) アカウントを有効にするか無効にするかを選択します。アカウントが無効の場合、Storage Navigator にログインできません。

(7) 認証サーバを使う場合は［External］を選択します。認証サーバを使わず、Storage Navigator だけでユーザ認証する場合、［Local］を選択します。

(8) ［Local］を選択した場合は、作成するユーザのパスワードを 2 か所に入力します。

(9) ［完了］をクリックします。

(10) ［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

(11) ［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとしてキューイングされ、順に実行されます。

(12) ［タスク］画面で、操作結果を確認します。実行前であれば、［タスク］画面でタス

クを一時中断したりキャンセルしたりできます。

3.3.2 ユーザアカウントの削除

ユーザアカウントが必要なくなったときは、次の方法でユーザアカウントを削除します。ビルトインユーザは削除できません(無効化はできます)。

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はそのユーザは Storage Navigator を操作できます。

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) Storage Navigator の［管理］ツリーから［ユーザグループ］を選択します。

(2) ［ユーザグループ］タブで、ユーザが所属するユーザグループを選択します。

(3) ［ユーザ］タブで削除したいユーザのチェックボックスを選択します。
複数のユーザを選択できます。

(4) 次のどちらかの方法で、［ユーザ削除］画面を表示します。
·［他のタスク］ - ［ユーザ削除］をクリックします。
·［設定］メニューから［ユーザ管理］ - ［ユーザ削除］を選択します。

(5) 設定内容を確認し、［適用］をクリックします。

3.3.3 ユーザアカウントの無効化

ユーザを一時的に Storage Navigator にログインさせなくするには、ユーザアカウントを無効にします。

前提条件

·必要なロール：セキュリティ管理者（参照・編集）ロール
·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ます（自分自身を無効にできません)。

操作手順

(1) Storage Navigator の［管理］ツリーから［ユーザグループ］を選択します。

(2) ［ユーザグループ］タブで、ユーザが所属するユーザグループをクリックします。

(3) ［ユーザ］タブでユーザのチェックボックスを選択します。

(4) 次のどちらかの方法で、［ユーザ編集］画面を表示します。
·［ユーザ編集］をクリックします。
·［設定］メニューから［ユーザ管理］ - ［ユーザ編集］を選択します。

(5)　［アカウント状態］のチェックボックスを選択し、［無効］を選択します。

(6)　［完了］をクリックします。

(7)　［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

(8)　［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとしてキューイングされ、順に実行されます。

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

再びユーザが Storage Navigator にログインできるようにするには、上記の手順に従い、［ユーザ編集］画面で［有効］をクリックします。

3.3.4　パスワードの変更(ユーザ)

ユーザは管理者から通知されたユーザ名とパスワードで Hitachi Storage Navigaotr にログインし、パスワードを変更します。

前提条件

・パスワード変更対象のユーザが外部認証サーバを使用していないこと。

操作手順

(1)　管理者から通知されたユーザ名とパスワードで Hitachi Storage Navigator にログインします。

(2)　［設定］ - ［ユーザ管理］ - ［パスワード変更］を選択して、自分のパスワードを変更します。

(3)　［完了］をクリックします。

(4)　［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

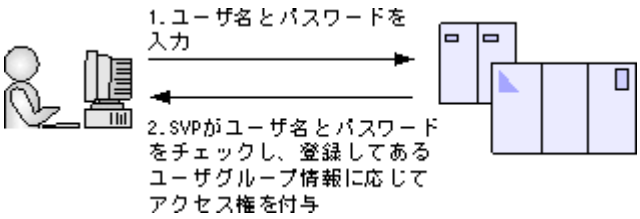
(5)　［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとしてキューイングされ、順に実行されます。

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

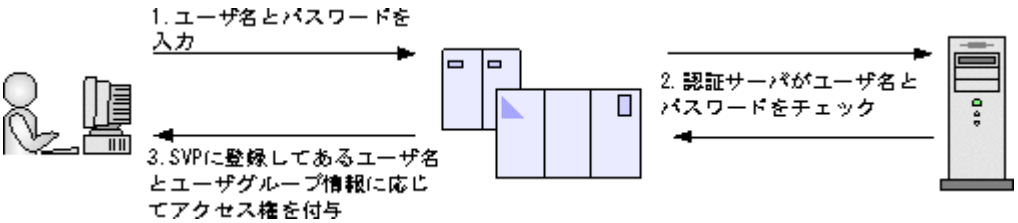
3.4　外部認証サーバと認可サーバを使用したユーザ管理

認証サーバを使用すると、ユーザは、認証サーバが管理するパスワードを使用して Storage Navigator にログインできます。認証サーバが管理するパスワードを使用するか、Storage Navigator 独自のパスワードを使用するかは、ユーザごとに決定できます。

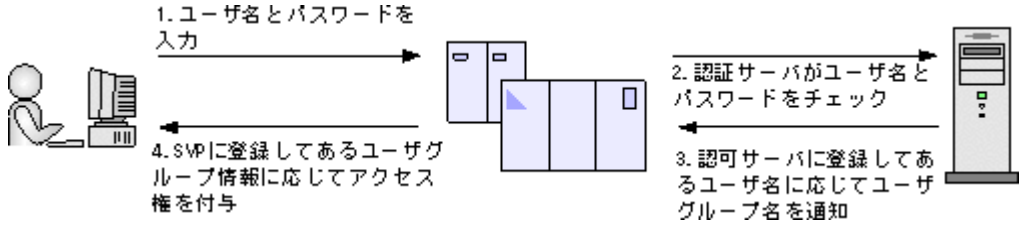
認証サーバを使用しない場合のユーザ認証の流れを次の図に示します。



認証サーバを使用する場合のユーザ認証の流れを次の図に示します。



認証サーバに加えて認可サーバとも連携すると、認可サーバに登録してあるユーザグループを Storage Navigator のユーザに割り当てられます。



また、DNS サーバの SRV レコードに認証サーバの情報を登録しておくと、ホスト名やポート番号を意識しないで認証サーバを使用できます。SRV レコードに複数台の認証サーバを登録すると、あらかじめ設定しておいた優先度に基づき、使用する認証サーバを決定できます。

3.4.1 認証サーバを用いた外部認証の要件

認証サーバのプロトコルには、LDAP、RADIUS または Kerberos が使用できます。

LDAP の場合

項目	要件
認証形式	• LDAPv3 Simple bind 認証
TLS セキュリティ設定	「3.5 TLSバージョンと暗号スイートを管理する」で設定したTLS セキュリティ設定をサポートしていること。 デフォルトのTLS セキュリティ設定は、「3.5 TLSバージョンと暗号スイートを管理する」を参照してください。
Storage Navigatorに設定するルート証明書ファイルの形式	• X509 DER 形式 • X509 PEM 形式
Storage Navigatorに設定するルート証明書の要件	• アップロードする証明書の公開鍵がRSAである場合、［TLSセキュリティ設定］画面の［下限鍵長（鍵交換）］で設定した鍵長以上であること。 • 証明書の公開鍵がECDSAである場合、公開鍵のパラメータが次のいずれかであること。 ◦ ECDSA_P256（secp256r1） ◦ ECDSA_P384（secp384r1） ◦ ECDSA_P521（secp521r1） • 証明書の署名ハッシュアルゴリズムが次のいずれかであること。 ◦ SHA-256

項目	要件
	◦ SHA-384 ◦ SHA-512
接続先のサーバに設定されている証明書の要件	• 証明書の公開鍵がRSAである場合、鍵長が2048bit以上であること。 • 証明書の公開鍵がECDSAである場合、公開鍵のパラメータが次のいずれかであること。 ◦ ECDSA_P256（secp256r1） ◦ ECDSA_P384（secp384r1） ◦ ECDSA_P521（secp521r1） • 証明書の署名ハッシュアルゴリズムが次のいずれかであること。 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 • 「3.4.3 外部認証サーバに接続する」の操作手順で、［プライマリホスト名］や［セカンダリホスト名］にホスト名を設定した場合、サーバに設定されている証明書のsubjectAltNameまたはCommonNameにサーバのホスト名を記載してください。 • 「3.4.3 外部認証サーバに接続する」の操作手順で、［プライマリホスト名］や［セカンダリホスト名］にIPアドレスを設定した場合、サーバに設定されている証明書のsubjectAltNameまたはCommonNameにサーバのIPアドレスを記載してください。 • DNS Lookupを使用して、外部認証サーバに接続する場合は、サーバに設定されている証明書のsubjectAltNameまたはCommonNameにサーバのホスト名を記載してください。 • CRLを用いて失効検証をする場合、CRLリポジトリのURIを接続先のサーバに設定されている中間証明書とサーバ証明書のcRLDistributionPoint（CRL配布点）に設定してください。CRLリポジトリはSVPからアクセスできるネットワーク上に存在し、SVPとCRLリポジトリが通信できる状態である必要があります。SVPとCRLリポジトリが通信できない場合、外部認証に失敗します。 • OCSPを用いて失効検証をする場合、OCSPレスポンダのURIを接続先のサーバに設定されている中間証明書とサーバ証明書のauthorityInfoAccess

項目	要件
	（機関アクセス情報）に正しく設定してください。OCSPレスポンダはSVPからアクセスできるネットワーク上に存在し、SVPとOCSPレスポンダが通信できる状態である必要があります。SVPとOCSPレスポンダが通信できない場合、外部認証に失敗します。

メモ

- 認証サーバのルート証明書は、認証サーバの管理者から取得してください。
- 証明書には期限があります。期限が切れると認証 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証明書の期限にご注意ください。
- 証明書の管理については、認証サーバの管理者とご相談の上、適切に管理してください。

RADIUS の場合

項目	要件
認証形式	• RFC2865 準拠 RADIUS ◦ PAP 認証 ◦ CHAP 認証

Kerberos の場合

項目	要件
認証形式	• Kerberos v5
暗号タイプ	Windows の場合 • AES128-CTS-HMAC-SHA1-96 • RC4-HMAC • DES3-CBC-SHA1 • DES-CBC-CRC • DES-CBC-MD5 Solaris または Linux の場合 • DES-CBC-MD5

注意

- 接続できる認証サーバは正・副 2 台です。正サーバと副サーバでは、IP アドレスおよびポート以外は同一の設定にしてください。

- 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は、次の条件を満たしていることを確認してください。なお、RADIUS サーバの場合は、SRV レコードを使用できません。

  LDAP サーバの場合

  ◦ 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 サーバのホスト名、ポート番号、ドメイン名などが登録してあること。

  Kerberos サーバの場合

  ◦ DNS サーバに、Kerberos サーバのホスト名、ポート番号、ドメイン名などが登録してあること。
- RADIUS サーバへのアクセスには UDP/IP が使われるため、プロセス間でネゴシエーションした上での暗号通信ができません。セキュアな環境で RADIUS サーバにアクセスするには、IPsec などの通信のパケットレベルでの暗号化が必要です。
- Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、Windows Server 2012 R2 を認証サーバとして使用する場合、既定の設定では DHE を用いた SSL 通信ができません。

  これらのサーバを認証サーバとして使用する場合は、Storage Navigator での SSL 通信の設定を実施し、鍵交換として DHE を使用する暗号スイートを無効化してください。

3.4.2 認可サーバを用いた外部認可の要件

認可サーバを使用する場合、認可サーバは次の要件を満たしている必要があります。

項目	要件
前提OS	• Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016
前提ソフトウェア	• Active Directory
検索用ユーザの認証プロトコル	• LDAP v3 Simple bind 認証
TLSセキュリティ設定	「3.5 TLSバージョンと暗号スイートを管理する」で設定したTLS セキュリティ設定をサポートしていること。 デフォルトのTLSセキュリティ設定は、「3.5 TLSバージョンと暗号スイートを管理する」を参照してください。
Storage Navigatorに設定するルート証明書ファイルの形式	• X509 DER 形式 • X509 PEM 形式
Storage Navigator に設定するルート証明書の要件	• アップロードする証明書の公開鍵がRSAである場合、［TLSセキュリティ設定］画面の［下限鍵長（鍵交換）］で設定した鍵長以上であること。

項目	要件
	• 証明書の公開鍵がECDSAである場合、公開鍵のパラメータが次のいずれかであること。 ◦ ECDSA_P256（secp256r1） ◦ ECDSA_P384（secp384r1） ◦ ECDSA_P521（secp521r1） • 証明書の署名ハッシュアルゴリズムが次のいずれかであること。 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512
接続先のサーバに設定されている証明書の要件	• 証明書の公開鍵がRSA である場合、鍵長が2048bit 以上であること。 • 証明書の公開鍵がECDSA である場合、公開鍵のパラメータが次のいずれかであること。 ◦ ECDSA_P256（secp256r1） ◦ ECDSA_P384（secp384r1） ◦ ECDSA_P521（secp521r1） • 証明書の署名ハッシュアルゴリズムが次のいずれかであること。 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 • 「3.4.3 外部認証サーバに接続する」の操作手順で、［プライマリホスト名］や［セカンダリホスト名］にホスト名を設定した場合、サーバに設定されている証明書のsubjectAltName またはCommonName にサーバのホスト名を記載してください。 • 「3.4.3 外部認証サーバに接続する」の操作手順で、［プライマリホスト名］や［セカンダリホスト名］にIP アドレスを設定した場合、サーバに設定されている証明書のsubjectAltName またはCommonName にサーバのIP アドレスを記載してください。 • DNS Lookup を使用して、外部認証サーバに接続する場合は、サーバに設定されている証明書のsubjectAltName またはCommonName にサーバのホスト名を記載してください。 • CRL を用いて失効検証をする場合、CRL リポジトリのURI を接続先のサーバに設定されている中間証明書とサーバ証明書のcRLDistributionPoint（CRL 配布点）に設定してください。CRL リポジトリはSVP からアクセスできるネットワーク上に存在し、SVP とCRL リポジトリが通信できる状態である必要があります。SVP とCRL リポジトリが通信できない場合、認可サーバとの通信に失敗します。 • OCSP を用いて失効検証をする場合、OCSP レスポンダのURI を接続先のサーバに設定されている中間証明書とサーバ証明書のauthorityInfoAccess（機関アクセス情報）に正しく設定してください。OCSP レスポンダはSVP からアクセスできるネットワーク上に存在し、SVP とOCSP レスポンダが通信できる状態である必要があります。SVP とOCSP レスポンダが通信できない場合、認可サーバとの通信に失敗します。

メモ

・認可サーバのルート証明書は、認可サーバの管理者から取得してください。

・証明書には期限があります。期限が切れると認可サーバと接続できなくなるため、証明書を

準備するときは証明書の期限にご注意ください。

・ 証明書の管理については、認可サーバの管理者とご相談の上、適切に管理してください。

注意

・ 認証サーバとして LDAP サーバまたは Kerberos サーバを使用する場合、認可サーバとも連携するときは、認証サーバと認可サーバは同一のホストを使用してください。

・ 認証サーバとして RADIUS サーバを使用する場合、認証サーバは正・副 2 台を指定できますが、認可サーバは 1 台しか指定できません。

・ Windows Server 2008、Windows Server 2008 R2、Windows Server 2012、 Windows Server 2012 R2 を認可サーバとして使用する場合、既定の設定では DHE を用いた SSL 通信ができません。

これらのサーバを認可サーバとして使用する場合は、Storage Navigator での SSL 通信の設定を実施し、鍵交換として DHE を使用する暗号スイートを無効化してください。

3.4.3 外部認証サーバに接続する

認証サーバおよび認可サーバを使用するには、サーバへの接続設定やネットワークの設定が必要です。特にサーバへの接続設定には、利用する認証サーバと認可サーバの詳細な設定情報が必要です。サーバへの接続設定に使用する LDAP、RADIUS、および Kerberos 用の設定値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関してはネットワークの管理者にお問い合わせください。

認証サーバおよび認可サーバに接続するための設定方法について説明します。

前提条件

·必要なロール：セキュリティ管理者（参照・編集）ロール

·保守員へ DNS サーバの IP アドレスを伝え、SVP の設定が完了していること。

·LDAP を使用する場合は LDAP サーバのサーバ証明書が必要です。証明書については、各サーバの管理者にお問い合わせください。

操作手順

(1) ［設定］ - ［ユーザ管理］ - ［外部認証サーバプロパティ参照］を選択します。

(2) 認証サーバを設定済みの場合は、プロパティ画面で［サーバ設定］をクリックします。

(3) ［認証サーバ選択］画面で、使用する認証サーバの種類を選択します。

外部認証サーバを使用しない場合は、［無効］を選択し［完了］をクリックします。

(4) 認証サーバへ接続するための設定項目を入力します。2 台目の認証サーバを使用する場合や認可サーバを使用する場合は、それぞれのサーバの項目も入力します。

(5) すでに認証サーバおよび認可サーバが使用できる場合、接続テストするときには［サーバ構成テスト］の［チェック］をクリックします。

接続テストに失敗した場合はエラーメッセージが表示されます。

(6)　［完了］をクリックします。
(7)　［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。
(8)　［適用］をクリックします。
タスクが登録され、［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークを付けた場合は、［タスク］画面が表示されます。

設定したにも関わらず、認証サーバおよび認可サーバが使用できない場合は、サーバへの接続設定の内容やネットワークに問題があるおそれがあります。サーバの管理者およびネットワークの管理者にお問い合わせください。
設定完了後、認証サーバおよび認可サーバが使用できることを確認したら、認証サーバへの接続設定をバックアップしてください。

3.4.4　認可サーバとの連携を有効にする

認証サーバの設定が完了したら、認可サーバとの連携を有効にします。なお、Hitachi Storage Navigator は、Active Directory のネストグループに対応しています。

Active Directory に設定するユーザグループの DN は、1 文字以上 250 文字以下で入力してください。また、一度に登録できるユーザグループ名は最大 20 です。

認可サーバのユーザグループを Storage Navigator で使用する

Active Directory の各ユーザの memberOf 属性の値に設定されているユーザグループと同じ名称のユーザグループを作成してください。ユーザグループ名を入力したあとに、［チェック］をクリックして、入力したユーザグループ名が認可サーバに登録されていることを確認してください。

Storage Navigator のユーザグループを認可サーバに登録する

Storage Navigator で作成済みのユーザグループを認可サーバに登録するには、Active Directory の各ユーザの memberOf 属性の値に、Storage Navigator のユーザグループと同じ名称のユーザグループの DN を設定してください。

3.4.5　認証サーバの情報を参照する。

認証サーバの情報を参照する方法について説明します。

操作手順

［設定］ - ［ユーザ管理］ - ［外部認証サーバプロパティ参照］を選択します。

3.5 TLS バージョンと暗号スイートを管理する

Storage Navigator からストレージシステムをよりセキュアに遠隔操作するためには、SSL/TLS 通信を構築します。

Storage Navigator では、セキュリティ管理者（参照・編集）ロールを持つユーザが、ツールパネルから SVP 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設定を実施できます。

・ Storage Navigator 動作 PC と SVP 間の通信では、次のプロトコルおよびポート番号の通信において 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
RMI	11099
RMI	51100
SMI-S	5989
raidinf	5443

また、次のサーバを使用する場合、これらのサーバと SVP 間においても、前述の 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
・ Hitachi Command Suite サーバ

・ VSP 5000 シリーズでは、Perfect Forward Secrecy を満たす暗号スイートを選択しておくことを推奨します。

・TLS1.2

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

・TLS1.3

TLS_AES_256_GCM_SHA384

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) 該当する SVP に接続している Storage Navigator をすべて終了させます。

(2) Storage Navigator 動作 PC 上で Web ブラウザを起動します。

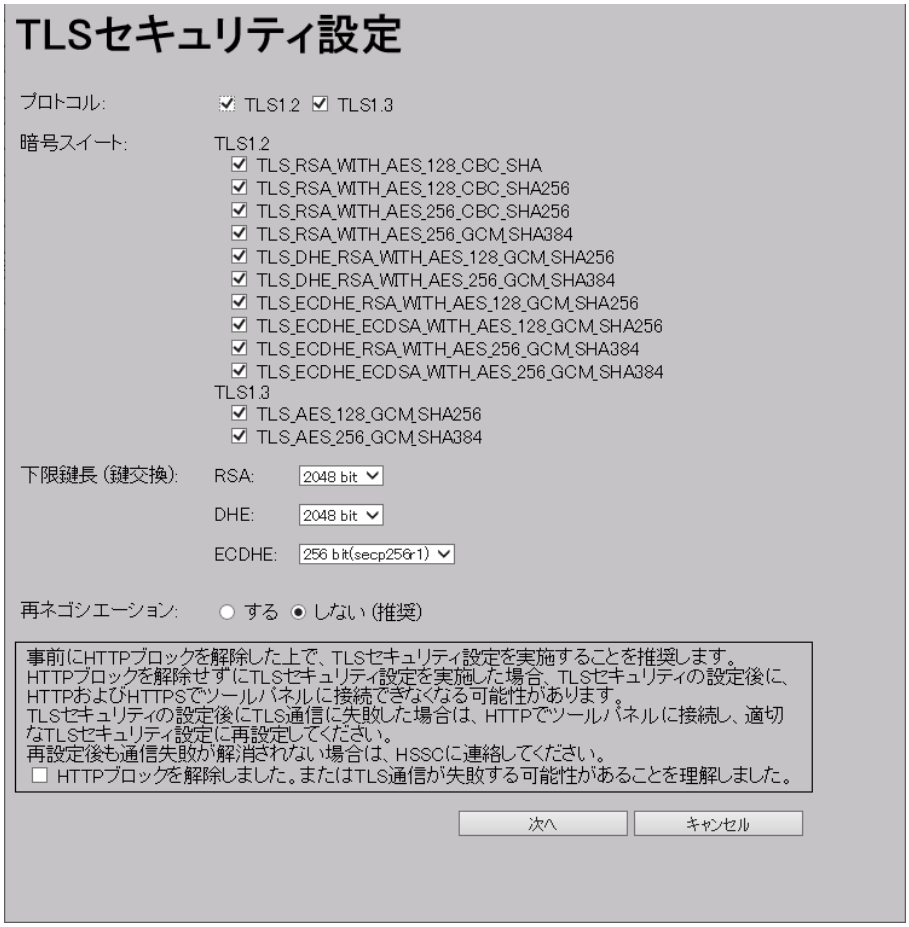
(3) HTTPS 接続で次の URL を指定して、［ツールパネル］画面を開きます。

```
https://SVPのIPアドレスまたはホスト名/cgi-bin/utility/toolpanel.cgi
```

(4) ［ツールパネル］画面で、［TLS セキュリティ設定］をクリックします。
［TLS セキュリティ設定］のログイン画面が開きます。
SSL/TLS 通信が構築されている場合、ログイン画面が表示される前に［セキュリティの警告］画面が表示されるので、［OK］をクリックしてください。さらに、証明書に関する［セキュリティの警告］画面が表示される場合があります。この場合、［証明書の表示］をクリックして証明書が正しいことを確認し、［はい］をクリックしてください。

(5) ［TLS セキュリティ設定］のログイン画面で管理者のユーザ ID（User ID）とパスワード（Password）を入力し、［ログイン］をクリックします。［TLS セキュリティ設定］画面が表示されます。

(6) ［TLS セキュリティ設定］画面で、セキュリティ設定の各項目を設定します。



注意

TLS1.2 を使用する場合は、SVP 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。

暗号スイートを誤って設定すると、SVP との SSL 通信に失敗し、Storage Navigator にログインできなくなる等の問題が発生します。

TLS1.3 を使用する場合は、証明書の鍵タイプ(RSA または ECDSA)にかかわらず、どちらの暗号スイートも選択できます。

(7) 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、［HTTP ブロックを解除しました。または TLS 通信に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。

(8) ［次へ］をクリックします。

［TLS セキュリティ設定 ］の通信テスト画面が表示されます。

(9) 次の通信路について手順 6 で指定したセキュリティ設定を使った通信テストが自動で開始されます。

- SVP – Syslog サーバ

・ SVP – 鍵管理サーバ
・ SVP – LDAP サーバ
・ SVP – HCS サーバ

(10) 手順 9 で実施された各通信路の通信テストの結果を確認します。
［TLS セキュリティ設定 ］の通信テスト画面で、通信結果として次のいずれかが表示されるまで待ちます。
・ Normal: 通信成功
・ Skipped: Storage Navigator で接続設定がされていない
・ Error: 通信失敗

(11) 通信結果が確認できたら、［TLS セキュリティ設定 ］の通信テスト画面で［送信］をクリックします。
設定の変更をしてよいかどうかを確認するメッセージ画面が表示されます。

(12) ［OK］をクリックします。
セキュリティ設定を反映するため、SVP の Web サーバが再起動されます。SVP の Web サーバの再起動が完了すると、［TLS セキュリティ設定 ］の設定完了画面が表示されます。

(13) ［OK］をクリックします。ログイン画面に戻ります。

(14) セキュリティ設定のバックアップを取得してください。

3.6 サーバ証明書の更新

3.6.1 秘密鍵を作成する

ここでは例として、Windows OS の PC で OpenSSL を使用して、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 のホームページ（http://www.openssl.org/）から OpenSSL をダウンロードし、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 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。
作成する秘密鍵の鍵タイプにより実行するコマンドが異なります。
・ RSA の場合

```
C:¥key>c:¥openssl¥bin¥openssl genrsa -out server.key 〈鍵長〉
```

・ ECDSA の場合

C:¥key>c:¥openssl¥bin¥openssl ecparam -genkey -name 〈鍵長〉 -out server.key

〈鍵長〉 には次のいずれかを指定できます。

・ RSA の場合：2048、3072、または 4096

・ ECDSA の場合：prime256v1 (secp256r1) 、 secp384r1、または secp521r1

コマンド入力例

・ 鍵タイプが RSA で、鍵長が 2048bit の場合

```
C:¥key>c:¥openssl¥bin¥openssl genrsa -out server.key 2048
```

・ 鍵タイプが ECDSA で、鍵長が 256bit (secp256r1) の場合

```
C:¥key>c:¥openssl¥bin¥openssl ecparam -genkey -name prime256v1 -out server.key
```

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。

3.6.2 公開鍵を作成する

ここでは例として、OS に Windows を使用して公開鍵 (.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。

C:¥key>c:¥openssl¥bin¥openssl req -sha256 -new -key server.key -config c:¥openssl¥bin¥openssl.cfg -out server.csr

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。

注意

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 、SHA-384、または SHA-512 のいずれかを使用してください。

(2) 対話形式で、サーバ証明書に書かれる情報を入力します。入力する情報を次に説明します。

- Country Name (2 letter code)[AU]：国名を 2 文字で入力します (例：JP) 。
- State or Province Name (full name)[Some-State]：都道府県名を指定します (例：Kanagawa) 。
- Locality Name (eg,city)[]:市区町村名または地域名を指定します(例:Odawara)。
- Organization Name (eg,company)[Internet Widgits Pty Ltd]：例えば、会社名を入力します (例：Hitachi) 。
- Organization Unit Name (eg,section)[]：例えば、部署名を入力します (例：ITPD)
- Common Name (eg,YOUR name)[]：サーバの IP アドレス (またはホスト名) を入力します。

  この項目に入力した名称が、SSL 通信するときのサーバ名称 (ホスト名) になります。

メモ

この項目に入力する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 SVP の名称（ホスト名）を一致させてください。

クライアント側の hosts ファイルか DNS サーバで、この項目に入力したサーバ名称と SVP の IP アドレスの名前解決（対応付け）をしてください。自己署名する場合は、SVP の IP アドレスを入力してください。例では、自己署名用に IP アドレスを入力しています。

- Email Address []：メールアドレスを入力します（例では入力していません）。
  そのほかに次の項目が表示されますが、入力しなくてもかまいません。
- A challenge password []：
- An optional company name []：

コマンドプロンプト画面の入力例を次に示します。

```
......++++++
..++++++
e is 65537 (0x10001)


C:¥key>c:¥openssl¥bin¥openssl  req  -sha256  -new  -key  server.key -config
c:¥openssl¥bin¥openssl.cfg -out server.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:JP
State or Province Name (full name) [Some-State]:Kanagawa
 Locality Name (eg, city) []:Odawara
Organization  Name  (eg,  company)  [Internet  Widgits  Pty  Ltd]:Hitachi
Organization Unit Name (eg, section) []：ITPD
Common Name (eg, YOUR name) []:192.168.0.1
Email Address []:
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

3.6.3　署名付き証明書の取得

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
- VeriSign などの認証局に依頼して公式の証明書を取得する方法

認証局に依頼する場合は、SVP をホスト名で指定してください。また、別途費用が掛かります。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を作成できます。自己署名するには、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。

C:¥key>c:¥openssl¥bin¥openssl x509 -req -sha256 -days 10000 -in server.csr
-signkey server.key -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。

注意
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, SHA-384, または SHA-512 のいずれか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。

署名付きの信頼できる証明書を取得する

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。この証明書を利用する場合は、コストと要件が増えますが、信頼性は向上します。

3.6.4 Hitachi Storage Navigator サーバ証明書の更新

サーバ証明書はツールパネルから更新します。

サーバ証明書が適用されるポート

プロトコル	ポート番号
HTTPS	443
RMI	11099
raidinf	5443
RMI	51100

前提条件

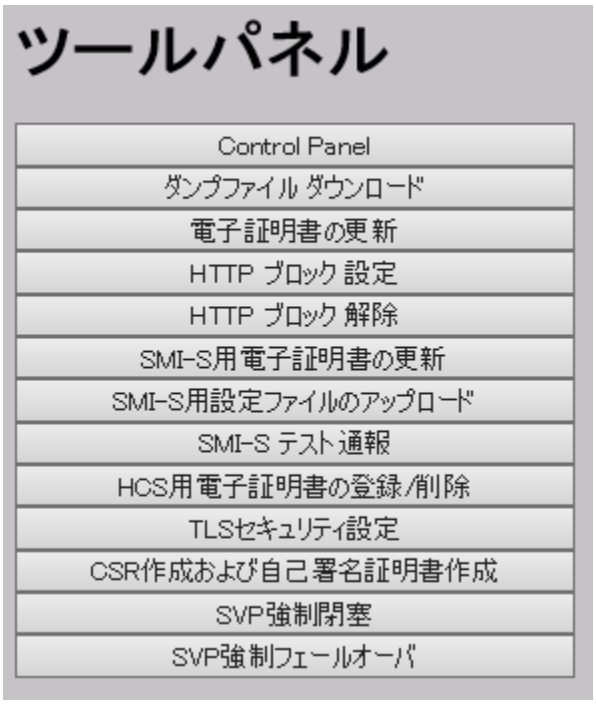
- 秘密鍵（server.key ファイル）が作成済みであること。ファイル名が server.key 以外の場合は、server.key に変更してください。
- 署名付き公開鍵証明書（server.crt ファイル）が取得済みであること。ファイル名が server.crt 以外の場合は、server.crt に変更してください。
- 秘密鍵（server.key ファイル）のパスフレーズが解除されていること。
- 必要なロール：ストレージ管理者（初期設定）ロール
- 外部ユーザグループ連携が無効の外部認証ユーザ、またはローカル認証ユーザであること。
- アップロードする証明書の公開鍵が RSA である場合、［TLS セキュリティ設定］画面の［下限鍵長（鍵交換）］で設定した鍵長以上であること。
- アップロードする証明書の公開鍵が ECDSA である場合、公開鍵のパラメータが次のいずれかであること。
  - ECDSA_P256（secp256r1）
  - ECDSA_P384（secp384r1）
  - ECDSA_P521（secp521r1）
- アップロードする証明書の署名ハッシュアルゴリズムが次のいずれかであること。
  - SHA-256
  - SHA-384
  - SHA-512
- アップロードする証明書の subjectAltName または CommonName に SVP のホスト名または IP アドレスが記載されていること。
- CRL を用いて失効検証をする場合、CRL リポジトリの URI が中間証明書とサーバ証明書の cRLDistributionPoint（CRL 配布点）に設定されていること。
- OCSP を用いて失効検証をする場合、OCSP レスポンダの URI が中間証明書とサーバ証明書の authorityInfoAccess（機関アクセス情報）に設定されていること。

・ Storage Navigator 動作 PC において、証明書の失効検証をする場合、CRL リポジトリまたは OCSP レスポンダが、Storage Navigator 動作 PC からアクセスできるネットワーク上に存在し、Storage Navigator 動作 PC と通信できる状態であること。Storage Navigator 動作 PC と、CRL リポジトリや OCSP レスポンダが通信できない場合、失効検証が実施されない状態で Storage Navigator に接続します。
・ 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を構築した署名付き公開鍵証明書（server.crt ファイル）を準備しておくこと。
・ アップロードする証明書の証明書チェーンの階層数は、ルート CA 証明書を含めて 20 階層以下であること。

操作手順

(1) 該当する SVP に接続している Storage Navigator をすべて終了させます。
(2) Storage Navigator 動作 PC 上で Web ブラウザを起動します。
(3) 次の URL を指定して、[ツールパネル] 画面を開きます。

```
https://SVPのIPアドレスまたはホスト名/cgi-bin/utility/toolpanel.cgi
```



(4) [ツールパネル] 画面で、[電子証明書の更新] をクリックします。[電子証明書の更新] のログイン画面が開きます。
SSL 通信が構築されている場合、ログイン画面が表示される前に [セキュリティの警告] 画面が表示されるので、[OK] をクリックしてください。さらに、証明書に関する [セキュリティの警告] 画面が表示される場合があります。この場合、[証明書の表示] をクリックして証明書が正しいことを確認し、[はい] をクリックしてください。
(5) [電子証明書の更新] のログイン画面で管理者のユーザ ID (User ID) とパスワード

（Password）を入力し、[ログイン] をクリックします。[電子証明書の更新] 画面が表示されます。

(6) ［電子証明書の更新］画面で、署名付き公開鍵証明書（server.crt ファイル）および秘密鍵（server.key ファイル）の両方を指定します。
［証明書ファイル(server.crt ファイル)］と［秘密鍵ファイル(server.key ファイル)］にはそれぞれファイル名を入力します。［参照］をクリックして表示される画面で、ファイルを選択することもできます。

(7) 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、[HTTP ブロックを解除しました。または 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。

(8) ［アップロード］をクリックします。[電子証明書の更新] の実行確認画面が表示されます。

(9) ［OK］をクリックして、証明書を更新します。証明書の更新が開始されます。
証明書の更新が完了すると、更新を反映するため SVP の Web サーバが再起動されます。SVP の Web サーバの再起動が完了すると、[電子証明書の更新] の更新完了画面が表示されます。

(10) ［電子証明書の更新］更新完了画面で、[OK] をクリックします。ログイン画面に戻ります。
ログイン画面が表示される前に、証明書に関する［セキュリティの警告］画面が表示される場合があります。この場合、[証明書の表示] をクリックして証明書が正しいことを確認し、[はい] をクリックしてください。

メモ
証明書の更新でエラーが発生した場合、エラーメッセージが表示されます。問題点を解決して、［電子証明書の更新］へのログインから再度実行してください。

3.7 HTTP 通信を無効にする

Hitachi Storage Navigaotr が使用する HTTP 80 番のポートへのアクセスを無効化します。この設定によって、Hitachi Storage Navigator Client（Web クライアント）と SVP PC 間の通信は、443 番のポート（HTTPS）だけを使用します。

Hitachi Command Suite のプログラムから Storage Navigator にアクセスする場合、SVP への HTTP 通信をブロックして SSL 通信だけを可能にすると Storage Navigator にアクセスできなくなるおそれがあります。Hitachi Command Suite のプログラムを使用する場合は、Hitachi Command Suite のプログラムが Storage Navigator との接続に SSL 通信を使用できるかどうか確認してください。

前提条件

・ 必要なロール：ストレージ管理者（初期設定）ロール

操作手順

(1) 該当する SVP に接続している Storage Navigator をすべて終了させます。

(2) Web ブラウザを起動して次の URL を入力し、ツールパネルを起動します

```
https://SVPのIPアドレスまたはホスト名/cgi-bin/utility/toolpanel.cgi
```

(3) ［ツールパネル］画面で、［HTTP ブロック設定］をクリックします。

(4) ［HTTP ブロック設定］のログイン画面で管理者のユーザ ID（User ID）とパスワード（Password）を入力し、［ログイン］をクリックします。［HTTP ブロック設定］の設定変更画面が表示されます。

(5) ［OK］をクリックします。設定の変更を再確認する画面が表示されます。

(6) ［OK］をクリックします。HTTP 通信をブロックする設定が開始され、SVP の Web サーバが再起動されます。SVP の Web サーバの再起動が完了すると、［HTTP ブロック設定］の設定完了画面が表示されます。

3.8 HTTP Strict Transport Security を有効にする（保守員作業）

Hitachi Storage Navigaotrは、HTTP Strict Transport Security(以下HSTS) (*1)を有効することができます。保守員による作業が必要になるため、サポート窓口にお問い合わせください。

*1: HSTSは、WebサーバがWebブラウザに対してHTTPSを使用するように伝達するセキュリティ機構です。

注:HSTS を有効にした場合、HTTP で Storage Navigator、および Hitachi Command Suite に接続できない問題が発生する場合があります。

HTTP で接続できない場合、HTTPS で接続してください。

4. SMI-S Provider

本章では SMI-S Provider を使用するための設定について説明します。

4.1 SMI-S サーバ証明書の更新

サーバ証明書はツールパネルから更新します。

下記待ち受けポートに本サーバ証明書は適用されます。

プロトコル	ポート番号
SMI-S	5989

前提条件

- サーバの秘密鍵と公開鍵が必要です。詳細については下記を参照してください。
  3.6.1 秘密鍵を作成する
  3.6.2 公開鍵を作成する
  3.6.3 署名付き証明書の取得
- TLS1.2 を使用する場合は、SVP にアップロードする証明書および SMI-S サーバにアップロードする証明書の鍵タイプと対応した暗号スイートが設定されていること。
  ツールパネルの[TLS セキュリティ設定画面]で、暗号スイートの設定状態を確認してください。
  - 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されていること。
  - 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されていること。

  証明書の鍵タイプと対応した暗号スイートが設定されていないと、管理ソフトウェアからストレージシステムに接続できません。
- 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を構築した署名付き公開鍵証明書（server.crt ファイル）を準備しておくこと。
- アップロードする証明書の証明書チェーンの階層数は、ルート CA 証明書を含めて 20 階層以下であること。

操作手順（詳細は『Storage Navigator ユーザガイド』を参照してください。）

(1) Web ブラウザを起動して次の URL を入力し、ツールパネルを起動します。

```
https://SVPのIPアドレスまたはホスト名/cgi-bin/utility/toolpanel.cgi
```

(2) [SMI-S 用電子証明書の更新]をクリックして、SMI-S 用電子証明書の更新を起動します。

(3) ユーザ ID とパスワードを入力して、［ログイン］をクリックします。

(4) 証明書ファイル(.crt ファイル)に、［参照］ボタンをクリックし、証明書ファイル（server.crt ファイル）を指定します。

(5) 秘密鍵ファイル（.key ファイル）に、［参照］ボタンをクリックし、秘密鍵ファイ

ル（server.key ファイル）を指定します。

(6)　[アップロード]ボタンをクリックし、証明書をアップロードします。

アップロード後、Web サーバが自動的にリブートし、アップロードした証明書が適用されます。

5

5. 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。Storage Navigator 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。

5.1 監査ログ情報を Syslog サーバに転送する

監査ログ情報を syslog サーバに転送するためのプロトコルとして、次のどちらかを選択できます。選択したプロトコルによって syslog 情報ファイルのフォーマットが異なります。

- TLS1.2/RFC5424（推奨）
- UDP/RFC3164

メモ

UDP/RFC3164 は非推奨です。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（Internet Engineering Task Force）が発行する文書 RFC3164 を参照してください。

メモ

SVP を交換したときなど、syslog サーバへの転送設定が再度必要になる場合があります。[監査ログ設定編集] 画面の［Syslog］タブでの設定内容を、記録しておいてください。

前提条件

- 必要なロール：監査ログ管理者(参照・編集)ロール
- ストレージシステムの SVP に syslog サーバを LAN 接続しておくこと。
- syslog サーバが監査ログ情報を受け取れるよう設定されていること。
- TLS1.2/RFC5424 を使う場合は、syslog サーバの証明書やクライアントの証明書が必要です。詳細については下記を参照してください。
  - 3.6.1 秘密鍵を作成する
  - 3.6.2 公開鍵を作成する
  - 3.6.3 署名付き証明書の取得
- 新 Syslog プロトコル(TLS1.2/RFC5424)を使用する場合には、Syslog サーバの証明書の subjectAltName または CommonName に、Syslog サーバのホスト名または IP アドレスを指定しておくこと。
- 転送先の Syslog サーバをホスト名で指定する場合は、DNS サーバに syslog サーバのホスト名、ドメイン名などを登録しておくこと。

注意

監査ログ情報を受け取る syslog サーバの設定をせずに、監査ログ情報の転送を開始すると、syslog サーバにログが保存されずログを喪失します。syslog サーバの設定方法は、syslog サーバのマニュアルを参照してください。

操作手順　（詳細は『監査ログリファレンスガイド』を参照してください。）

(1) ［設定］メニューから［セキュリティ管理］－［監査ログ設定編集］を選択して、［監査ログ設定編集］画面の［Syslog］タブを表示します。
(2) ［転送プロトコル］で、監査ログ情報の送信に使用するプロトコルを選択します。
(3) ［プライマリサーバ］の［有効］を選択し、次の項目を設定します。
- IP アドレス/ホスト名
  転送先の syslog サーバを、IPv4、IPv6、またはホスト名で指定してください。ホスト名で指定するには、［Identifier］を選択します。ホスト名は、半角英数字と記号（! $ % - . @ _ ` ~）を使って 255 文字以内で指定してください。

  メモ
  マイクロプログラムバージョンによっては、ホスト名による指定は設定できません。

- ポート番号
- クライアント証明書ファイル名、パスワード、ルート証明書ファイル名

［転送プロトコル］で「新 Syslog プロトコル（TLS1.2/RFC5424)」を選択した場合だけ設定します。
(4) セカンダリサーバ（代替サーバ）へ監査ログ情報を転送する場合、［セカンダリサーバ］の［有効］を選択し、次の項目を設定します。
- IP アドレス/ホスト名
- ポート番号
- クライアント証明書ファイル名、パスワード、ルート証明書ファイル名

［転送プロトコル］で「新 Syslog プロトコル（TLS1.2/RFC5424)」を選択した場合だけ設定します。
(5) ストレージシステムを識別するために、［ロケーション識別名］に任意の名称を設定します。
(6) ［転送プロトコル］で［新 Syslog プロトコル(TLS1.2/RFC5424)］を選択している場合は、タイムアウト、リトライ間隔、およびリトライ回数を設定します。
(7) syslog サーバに監査ログの詳細情報を転送したい場合は、［詳細情報出力］で［有効］を選択します。
(8) ［Syslog サーバへテスト送信］をクリックして、設定内容をテストします。
(9) Syslog サーバにテスト用ログ（機能名：AuditLog、操作名：Send Test Message）が送信されたことを確認します。
(10) ［完了］をクリックします。
(11) ［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。
(12) ［適用］をクリックします。
タスクが登録され、［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークを付けた場合は、［タスク］画面が表示されます。

(13) タスクが完了したら、syslog サーバが syslog サーバ設定のログを受信していることを確認してください。ログの機能名は「AuditLog」、操作名は「Set Syslog Server」です。

メモ

syslog サーバが監査ログ情報を受信できていない場合は、設定した IP アドレス/ホスト名とポート番号が syslog サーバの IP アドレス/ホスト名とポート番号に一致しているかどうか、クライアント証明書の設定内容、パスワード、およびルート証明書ファイル名が正しいかを確認してください。設定が正しい場合は syslog サーバ側の設定を確認してください。Storage Navigator 側の設定が正しい場合は syslog サーバ側の設定内容を確認してください。転送先の syslog サーバをホスト名で指定する場合は、DNS サーバに、syslog サーバのホスト名、ドメイン名などが登録してあることを確認してください。設定方法については syslog サーバのマニュアルを参照してください。

6

6. 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。

6.1 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。

注意

設定したストレージシステム名は、必ず記録しておいてください。SVP の交換などによって設定内容が消去されることがあるからです。

前提条件

- 必要なロール：ストレージ管理者(初期設定)ロール

操作手順 （詳細は『障害通知ガイド』を参照してください。）

(1) ［設定］メニューから［環境設定管理］ - ［アラート設定編集］を選択します。
［アラート設定編集］画面が表示されます。アラート設定編集ウィザードについては、『HitachiDevice Manager - Storage Navigator ユーザガイド』を参照してください。

(2) ［アラート通知］で、アラート通知する対象の SIM を［ホスト報告］または［全て］から選択します。

(3) ［SNMP］タブを選択します。
SNMP 用の［アラート設定編集］画面が表示されます。

(4) ［SNMP エージェント］で、［有効］を選択します。

(5) ［システムグループ情報］で、ストレージシステム名、連絡先、および場所を入力します。
［システムグループ情報］を変更した場合、Storage Navigator の［ストレージシステム］画面のストレージシステム名、連絡先、および場所も変更されます。

(6) ［完了］をクリックします。

(7) ［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

(8) ［適用］をクリックします。
タスクが登録され、[「適用」をクリックした後にタスク画面を表示]のチェックボックスにチェックマークを付けた場合は、［タスク］画面が表示されます。

6.2 SNMP トラップの通知先を設定する(SNMPv3)

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 SNMP トラップの通知先を追加する手順について説明します。

前提条件

・必要なロール：ストレージ管理者(初期設定)ロール

操作手順 （詳細は『障害通知ガイド』を参照してください。）

1.［設定］メニューから［環境設定管理］ - ［アラート設定編集］を選択します。
［アラート設定編集］画面が表示されます。アラート設定編集ウィザードについては、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。
2.［SNMP］タブを選択します。
SNMP 用の［アラート設定編集］画面が表示されます。
3.［SNMP エージェント］で［有効］を選択します。
4.［SNMP バージョン］で［v3］を選択します。
5.［登録したトラップ送信設定］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。
6.［トラップ送信先］で入力する IP アドレスのバージョンを［IPv4］または［IPv6］から選択し、SNMP トラップを発行したい IP アドレスを入力します。

メモ
IPv4 と IPv6 は、すべて 0 のアドレスは設定できません。
IPv6 アドレスを入力する場合は、コロンで区切られた最大 4 桁の 16 進数（0～FFFF）を 8 個入力してください。IPv6 アドレスの省略形も指定できます。

7.［ユーザ名］でユーザ名を入力します。
ユーザ名として入力できるのは、一部の記号（¥ , / ; : * ? " < > | & % ^）を除く、32 文字までの半角英数字と記号です。先頭または末尾にスペースを入力しないでください。
8.［認証］で認証を有効にするか無効にするかを選択します。
［認証］で［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］でパスワードを入力します。
9.［暗号化］で暗号化を有効にするか無効にするかを選択します。
メモ
［認証］で［無効］を選択した場合、［暗号化］は無効となり、設定できません。
［暗号化］で［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］で鍵を入力します。その後、［鍵再入力］で、確認用に再度鍵を入力します。

10.［OK］をクリックします。
入力したユーザ名と IP アドレスの組み合わせが［登録したトラップ送信設定］に追加されます。
11.［完了］をクリックします。
12.［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。
13.［適用］をクリックします。
タスクが登録され、［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークを付けた場合は、［タスク］画面が表示されます。

6.3 リクエスト許可対象を設定する(SNMPv3)

SNMP プロトコルのバージョンが SNMP v3 の場合に、リクエスト許可対象を設定する手順について説明します。

前提条件

・ 必要なロール：ストレージ管理者(初期設定)ロール

操作手順 （詳細は『障害通知ガイド』を参照してください。）

1.［設定］メニューから［環境設定管理］ - ［アラート設定編集］を選択します。
［アラート設定編集］画面が表示されます。アラート設定編集ウィザードについては、『Hitachi Device Manager - Storage Navigator ユーザガイド』を参照してください。
2.［SNMP］タブを選択します。
SNMP 用の［アラート設定編集］画面が表示されます。
3.［SNMP エージェント］で［有効］を選択します。
4.［SNMP バージョン］で［v3］を選択します。
5.［登録した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。
6.［ユーザ名］でユーザ名を入力します。
ユーザ名として入力できるのは、一部の記号（¥ , / ; : * ? " < > | & % ^）を除く、32 文字までの半角英数字と記号です。先頭または末尾にスペースを入力しないでください。
7.［認証］で認証を有効にするか無効にするかを選択します。
［認証］で［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］でパスワードを入力します。その後、［パスワード再入力］で、確認用に再度パスワードを入力します。
8.［暗号化］で暗号化を有効にするか無効にするかを選択します。

メモ
［認証］で［無効］を選択した場合、［暗号化］は無効となり、設定できません。
［暗号化］で［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］で鍵を入力します。その後、［鍵再入力］で、確認用に再度鍵を入力します。

9.［OK］をクリックします。
入力したユーザ名が［登録したリクエスト許可設定］に追加されます。
10.［完了］をクリックします。
11.［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。
12.［適用］をクリックします。
タスクが登録され、［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークを付けた場合は、［タスク］画面が表示されます。

7

7. 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。VSP 5000 シリーズで、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 セキュリティを有効にしてください。
FC-NVMe 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。

7.1 LUN セキュリティを設定する

複数のホストグループを設定する場合は、セキュリティスイッチ（LUN Security）を有効にする必要があります。また、セキュリティスイッチを有効にした場合は、ホストバスアダプタの WWN を指定する必要があります。

前提条件

この操作を実行する場合、次のロールのうち、どちらか 1 つが必要です。

・ストレージ管理者（システムリソース管理）ロール

・ストレージ管理者（プロビジョニング）ロール

操作手順　（詳細は『オープンシステム構築ガイド』を参照してください。）

1.［ストレージシステム］ツリーの［ポート / ホストグループ / iSCSI ターゲット］を選択します。

2.［ポート］タブを選択します。

3. ポートを選択します。

4. 次のどちらかの方法で、［ポート編集］画面を表示します。

・［ポート編集］をクリックします。

・［アクション］メニューから［ポート/ホストグループ管理］－［ファイバ］－［ポート編集］を選択します。

5.［ポート編集］画面で、［ポートセキュリティ］のチェックボックスを選択して［有効］を選択します。

6.［完了］をクリックします。

LUN セキュリティを切り替えてもよいかどうかを確認するメッセージが表示されます。

［OK］をクリックすると、［設定確認］画面が表示されます。

7.［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

8.［適用］をクリックします。

タスクが登録され、[「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、［タスク］画面が表示されます。

7.2 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。

8

8. 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。

8.1　iSCSI ターゲットを作成し、ホストを登録する

前提条件

・必要なロールを次に示します。

◦ストレージ管理者（プロビジョニング）ロール

◦セキュリティ管理者（参照・編集）ロール

操作手順　（詳細は『オープンシステム構築ガイド』を参照してください。）

1. 次のどれかの方法で、［iSCSI ターゲット作成］画面を表示します。

・［よく使うタスク］から［iSCSI ターゲット作成］を選択します。

・ストレージシステムの全 iSCSI ターゲットを表示する場合、［ストレージシステム］ツリーから［ポート / ホストグループ / iSCSI ターゲット］を選択します。［ホストグループ / iSCSI ターゲット］タブで［iSCSI ターゲット作成］をクリックします。

・ポート単位で iSCSI ターゲットを表示する場合、［ストレージシステム］ツリーから［ポート / ホストグループ / iSCSI ターゲット］を選択し、ツリーからポートをクリックします。

［iSCSI ターゲット］タブで［iSCSI ターゲット作成］をクリックします。

・［アクション］メニューから［ポート/ホストグループ管理］－［iSCSI］－［iSCSI ターゲット作成］を選択します。

2.［iSCSI ターゲットエイリアス］を設定します。

［デフォルト名を使用］チェックボックスを選択すると、値が自動で入力されます。

3.［iSCSI ターゲット名］を設定します。

iqn 形式または eui 形式を選択してください。［デフォルト名を使用］チェックボックスを選択すると、値が自動で入力されます。

4.［リソースグループ名（ID)］から、iSCSI ターゲットを作成するリソースグループを選択します。

・［Any］を選択した場合、ユーザに割り当てられているすべてのポートのうち、iSCSI ターゲットを追加できるポートが［利用可能なポート］に表示されます。

・［Any］以外を選択した場合、選択したリソースグループに割り当てられているポートのうち、iSCSI ターゲットを追加できるポートが［利用可能なポート］に表示されます。

ヒント

1 つのポートにつき最大 255 個の iSCSI ターゲットを作成できます。

5.［ホストモード］からホストモードを選択します。

ホストモードを選択するときは、ホストのプラットフォームなどを考慮してください。

6. ホストモードのオプションを設定する必要がある場合は、［ホストモードオプション］を選択します。

［ホストモードオプション］を選択すると、画面が拡張されてホストモードのオプションのリストが表示されます。［モード番号］はオプションの番号を示します。設定したいオプションを選択

した状態で［有効］をクリックします。

7. iSCSI ターゲットに登録するホストを選択します。

登録したいホストがほかのポートとケーブルで接続している（または過去にケーブルで接続していた）場合、登録したいホストのホストバスアダプタのチェックボックスを［利用可能なホスト］テーブルから選択してください。

登録するホストがない場合、ホストを選択しないで手順 14 に進んでください。この場合、ホストの登録されていない iSCSI ターゲットが作成されます。

登録したいホストがストレージシステムのポートにまだケーブル接続されていない場合は、手順 8 に進んでください。

8.［利用可能なホスト］テーブルの下にある［新規ホスト追加］をクリックします。

［新規ホスト追加］画面が表示されます。

9. iqn 形式または eui 形式を選択してください。

10.［HBA iSCSI 名］に HBA の iSCSI 名を入力します。

11. 必要であれば、［ホスト名］にホストバスアダプタのニックネームを入力します。

12.［OK］をクリックして［新規ホスト追加］画面を閉じます。

13. 登録したいホストの iSCSI 名を［利用可能なホスト］テーブルから選択します。

14.（iSCSI ターゲットを追加する）ポートを選択します。

複数のポートを選択した場合、1 回の操作で複数のポートに同じ iSCSI ターゲットを追加できます。

15.［認証方法］で［CHAP］を選択します。

· ［相互 CHAP］:［有効］または［無効］を選択します。［有効］を選択した場合、双方向認証モードになります。［無効］を選択した場合、単方向認証モードになります。

· ［ユーザ名］:［相互 CHAP］で［無効］を選択した場合、設定は任意です。［相互 CHAP］で［有効］を選択した場合、必ず設定してください。

· ［シークレット］および［シークレット再入力］:［相互 CHAP］で［無効］を選択した場合、設定は任意です。［相互 CHAP］で［有効］を選択した場合、必ず設定してください。

16. iSCSI ターゲットに登録する CHAP ユーザを選択します。

登録したい CHAP ユーザがほかのポートとケーブルで接続している（または過去にケーブルで接続していた）場合、登録したい CHAP ユーザを［利用可能な CHAP ユーザ］テーブルから選択してください。

登録する CHAP ユーザがない場合、CHAP ユーザを選択しないで手順 20 に進んでください。この場合、CHAP ユーザの登録されていない iSCSI ターゲットが作成されます。

登録したい CHAP ユーザがストレージシステムのポートにまだケーブル接続されていない場合は、手順 17 に進んでください。

17.［利用可能な CHAP ユーザ］テーブルの下にある［新規 CHAP ユーザ追加］をクリックします。

［新規 CHAP ユーザ追加］画面が表示されます。

18. ユーザ名およびシークレットを入力します。

19.［OK］をクリックして［新規 CHAP ユーザ追加］画面を閉じます。

20.［追加］をクリックして iSCSI ターゲットを追加します。

手順 2 から手順 20 までを繰り返すと、複数の iSCSI ターゲットを作成できます。

ヒント

行のチェックボックスを選択して［詳細］をクリックすると［iSCSI ターゲットプロパティ］画面が表示されます。行のチェックボックスを選択して［削除］をクリックすると、削除してもよいかを尋ねるメッセージが表示されます。削除して問題ない場合は［OK］をクリックしてください。

21. 設定を完了し設定内容を確認する場合は、［完了］をクリックします。

引き続き LU パスを設定したい場合は、［次へ］をクリックします。LU パスの設定については、関連項目を参照してください。

22.［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

行のラジオボタンを選択して［詳細］をクリックすると［iSCSI ターゲットプロパティ］画面が表示されます。

23.［適用］をクリックします。

タスクが登録され、［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、［タスク］画面が表示されます。

8.2 CHAP ユーザを登録する

iSCSI ターゲットに CHAP ユーザを追加します。

前提条件

必要なロールを次に示します。

・ストレージ管理者（プロビジョニング）ロール

・セキュリティ管理者（参照・編集）ロール

操作手順　（詳細は『オープンシステム構築ガイド』を参照してください。）

1. 次のどれかの方法でタブを表示します。

・ストレージシステムの全 iSCSI ターゲットを表示する場合、［ストレージシステム］ツリーから［ポート / ホストグループ / iSCSI ターゲット］を選択し、［ホストグループ / iSCSI ターゲット］タブを選択します。

・ポート単位で iSCSI ターゲットを表示する場合、［ストレージシステム］ツリーから［ポート / ホストグループ / iSCSI ターゲット］を選択し、各ポートを選択します。ポートの［iSCSI ターゲット］タブを選択します。

2. CHAP ユーザを追加する iSCSI ターゲットを選択します。

3. 次のどちらかの方法で、［CHAP ユーザ追加］画面を表示します。

・［他のタスク］－［CHAP ユーザ追加］をクリックします。

・［アクション］メニューから［ポート/ホストグループ管理］－［iSCSI］－［認証］－［CHAP ユーザ追加］を選択します。

4. 画面左側の［利用可能な CHAP ユーザ］テーブルから CHAP ユーザを選択し、［追加］をクリックします。

選択された CHAP ユーザが、画面右側の［選択した CHAP ユーザ］テーブルに表示されます。登録したい CHAP ユーザがない場合、次の手順を実行して CHAP ユーザを新規登録してください。

a. ［利用可能な CHAP ユーザ］テーブルの下にある［新規 CHAP ユーザ追加］をクリックします。

［新規 CHAP ユーザ追加］画面が表示されます。

b. ［ユーザ名］および［シークレット］を入力します。

c. ［OK］をクリックして［新規 CHAP ユーザ追加］画面を閉じます。

5.［完了］をクリックします。

6.［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

7.［適用］をクリックします。

タスクが登録され、[「適用」をクリックした後にタスク画面を表示] のチェックボックスにチェックマークが付いている場合は、［タスク］画面が表示されます。

8.3 CHAP ユーザを削除する

CHAP ユーザを削除します。

前提条件

必要なロールを次に示します。

・ ストレージ管理者（プロビジョニング）ロール

・ セキュリティ管理者（参照・編集）ロール

操作手順 （詳細は『オープンシステム構築ガイド』を参照してください。）

1. 次のどれかの方法で、［CHAP ユーザ］タブを表示します。

・ ストレージシステムの全 CHAP ユーザを表示する場合、[ストレージシステム] ツリーから［ポート / ホストグループ / iSCSI ターゲット］を選択し、［CHAP ユーザ］タブを選択します。

・ ポート単位で CHAP ユーザを表示する場合、[ストレージシステム] ツリーから［ポート /ホストグループ / iSCSI ターゲット］を選択し、各ポートを選択します。ポートの［CHAP ユーザ］タブを選択します。

・ iSCSI ターゲット単位で CHAP ユーザを表示する場合、[ストレージシステム] ツリーから［ポート / ホストグループ / iSCSI ターゲット］を選択し、各ポートを選択したあと各 iSCSI ターゲットを選択します。iSCSI ターゲットの［CHAP ユーザ］タブを選択します。

2. CHAP ユーザを選択します。

3. 次のどちらかの方法で、［CHAP ユーザ削除］画面を表示します。

・ ［CHAP ユーザ削除］をクリックします。

・ ［アクション］メニューから［ポート/ホストグループ管理］－［iSCSI］－［認証］－［CHAP ユーザ削除］を選択します。

4.［CHAP ユーザ削除］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

5.［適用］をクリックして設定をストレージシステムに適用します。

設定した内容はタスクとしてキューイングされ、順に実行されます。

ヒント

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

6.［タスク］画面で、操作結果を確認します。

実行前であれば、［タスク］画面でタスクを一時中断したりキャンセルしたりできます。

8.4 ターゲット CHAP ユーザを削除する

iSCSI ターゲットに設定された CHAP ユーザを削除します。

前提条件

必要なロールを次に示します。

・ストレージ管理者（プロビジョニング）ロール

・セキュリティ管理者（参照・編集）ロール

操作手順 （詳細は『オープンシステム構築ガイド』を参照してください。）

1. 次のどれかの方法でタブを表示します。

・ストレージシステムの全 iSCSI ターゲットを表示する場合、［ストレージシステム］ツリーから［ポート / ホストグループ /iSCSI ターゲット］を選択し、［ホストグループ /iSCSI ターゲット］タブを選択します。

・ポート単位で iSCSI ターゲットを表示する場合、［ストレージシステム］ツリーから［ポート / ホストグループ / iSCSI ターゲット］を選択し、各ポートを選択します。ポートの［iSCSI ターゲット］タブを選択します。

2. iSCSI ターゲットを選択します。

3. 次のどちらかの方法で、［ターゲット CHAP ユーザ削除］画面を表示します。

・［他のタスク］－［ターゲット CHAP ユーザ削除］をクリックします。

・［アクション］メニューから［ポート/ホストグループ管理］－［iSCSI］－［認証］－［ターゲット CHAP ユーザ削除］を選択します。

4.［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

行のラジオボタンを選択して［詳細］をクリックすると［iSCSI ターゲットプロパティ］画面が表示されます。

5.［適用］をクリックします。

タスクが登録され、［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、［タスク］画面が表示されます。

8.5 ポート CHAP ユーザを削除する

ポートに設定された CHAP ユーザを削除します。

前提条件

必要なロールを次に示します。

・ ストレージ管理者（プロビジョニング）ロール

・ セキュリティ管理者（参照・編集）ロール

操作手順　（詳細は『オープンシステム構築ガイド』を参照してください。）

1.［ストレージシステム］ツリーの［ポート / ホストグループ / iSCSI ターゲット］を選択します。

2.［ポート］タブを選択します。

3. ポート CHAP ユーザを削除するポート名を選択します。

4. 次のどちらかの方法で、［ポート CHAP ユーザ削除］画面を表示します。

・ ［ポート CHAP ユーザ削除］をクリックします。

・ ［アクション］メニューから［ポート/ホストグループ管理］－［iSCSI］－［認証］－［ポート CHAP ユーザ削除］を選択します。

5.［設定確認］画面で設定内容を確認し、［タスク名］にタスク名を入力します。

6.［適用］をクリックします。

タスクが登録され、［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、［タスク］画面が表示されます。

9

9. 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ハードディスクを交換するとき、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および暗号化に対応したディスクボード（DKB）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。

9.1　鍵管理サーバを利用する

9.1.1　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、販売元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）

・前提ソフトウェア

◦SafeNet KeySecure k460

9.1.2　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。

9.1.3　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、『3.6.1 秘密鍵を作成する』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、『3.6.2 公開鍵を作成する』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 SVP にアップロードするときに使用します。
PKCS#12 形式のクライアント証明書を作成するときに入力するパスワードは 0 文字以上 128 文字以下で、使用できる文字は次のとおりです。
・ 数字（0 から 9）
・ 英大文字（A から Z）
・ 英小文字（a から z）
・ 半角記号 31 種： ! # $ % & ' ( ) * + , - . / : ; < = > ? @ [¥] ^ _ ` { | } ~
この例では、client.p12 ファイルが c:¥key フォルダに作成されます。この client.p12 ファイルが PKCS#12 形式に変換されたクライアント証明書です。

9.2 暗号化環境を設定する

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

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

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

注意
［鍵管理サーバで暗号化鍵生成］にある［鍵暗号化鍵を鍵管理サーバで保護する］および［注意事項に同意する］のチェックボックスを選択して設定を完了すると、装置の電源を ON にしたときに鍵管理サーバからバックアップした鍵暗号化鍵を取得します。このとき、鍵管理サーバとの通

信が確立されている必要があります。このため、SVP と鍵管理サーバが通信できることを確認してから装置の電源を ON にしてください。

注意

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

メモ

SVP を交換した後に鍵管理サーバへの接続を復旧する場合は、バックアップしておいた鍵管理サーバへの接続設定をリストアしてください。

SVP を交換する前の［暗号化環境設定編集］画面の設定で、[鍵管理サーバ]で[有効]を選択した場合、バックアップしておいた鍵管理サーバへの接続設定をリストアした後に、保管しておいたクライアント証明書と鍵管理サーバのルート証明書を再度設定してください。鍵管理サーバへの接続設定をバックアップしていなかった場合は、鍵管理サーバへの接続を再度設定してください。クライアント証明書を保管していなかった場合は、新たにクライアント証明書を作成して、作成したクライアント証明書と鍵管理サーバのルート証明書を設定してください。

SVP を交換する前の［暗号化環境設定編集］画面の設定で、[鍵管理サーバ]で[有効]を選択し、かつ[鍵暗号化鍵を鍵管理サーバで保護する]のチェックボックスを選択した場合、SVP を交換した後に新たにクライアント証明書を作成したときは、鍵管理サーバへの接続を設定した後に鍵暗号化鍵を更新してください。このとき鍵管理サーバから更新前の鍵暗号化鍵を削除できないため鍵暗号化鍵削除処理は失敗しますが、鍵暗号化鍵は更新されています。

メモ

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

・定期バックアップを実行する場合は、［暗号化環境設定編集］画面で次のことを確認してください。

・［鍵管理サーバ］で［有効］を選択していること・鍵管理サーバのプライマリサーバが使用可能な状態であること。［サーバ構成テスト］の［チェック］をクリックして、接続テストが正常終了することを確認してください。

・定期バックアップタスクの詳細を参照するには、ストレージ管理者（システムリソース管理）ロール、またはタスクを実行したユーザである必要があります。タスクの管理については、マニュアル『Hitachi DeviceManager - Storage Navigator ユーザガイド』を参照してください。

前提条件

・必要なロール：セキュリティ管理者（参照・編集）ロール

・鍵管理サーバに、IP アドレスではなくホスト名を指定して接続する場合は、DNS サーバの IP アドレスを保守員へ伝え、SVP の設定を依頼すること。

・鍵管理サーバを使用する場合は鍵管理サーバに登録されているクライアント証明書と鍵管理サーバのルート証明書を用意すること。それぞれの証明書については、鍵管理サーバの管理者にお問い合わせください。

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

1. Storage Navigator の［管理］ツリーから［暗号化鍵］を選択し、［暗号化鍵］画面を表示します。

2. 画面右側の［暗号化鍵］タブを選択します。

3. 次のどちらかの方法で、［暗号化環境設定編集］画面を表示します。

・［暗号化鍵］タブで［暗号化環境設定編集］をクリックします。

・［設定］メニューから［セキュリティ管理］-［暗号化鍵］-［暗号化環境設定編集］を選択します。

4.［鍵管理サーバ］で［有効］または［無効］を選択します。

5. 鍵管理サーバへ接続する場合にプライマリサーバとセカンダリサーバの設定項目を入力します。

6. すでに鍵管理サーバが使用可能な場合、接続テストするときには[サーバ構成テスト]の[チェック］をクリックします。

接続テストに失敗した場合はエラーの詳細が結果に表示されます。

7. 定期バックアップを実行する場合、［鍵管理サーバへ暗号化鍵定期バックアップを有効にする］にチェックマークを付けます。さらに［定期バックアップ時刻］で暗号化鍵をバックアップしたい時間を指定して、［定期バックアップユーザ］で定期バックアップユーザのユーザ名とパスワードを入力します。

8. 鍵管理サーバで暗号化鍵を生成する場合、［鍵管理サーバで暗号化鍵生成］にチェックマークを付けます。さらに鍵暗号化鍵を鍵管理サーバに保存する場合、［鍵暗号化鍵を鍵管理サーバで保護する］にチェックマークを付けてから、［注意事項に同意する］をチェックします。

9. 暗号化鍵を鍵管理サーバに保存し、装置電源 OFF 時に装置内の暗号化鍵を削除する場合、［PS OFF 時に装置内の暗号化鍵を削除する］にチェックマークを付けてから、［注意事項に同意する］をチェックします。

10. 暗号化鍵を鍵管理サーバ上で作成し、かつ、暗号化鍵をストレージシステム内に作成できないようにする場合は、［ローカル鍵生成を無効にする］にチェックマークを付けます。チェックマークを付けると、注意事項が表示されます。注意事項の内容をご確認の上、同意される場合は［注意事項に同意する］にチェックマークを付けてください。

注意

［鍵管理サーバで暗号化鍵生成］にある［ローカル鍵生成を無効にする］および［注意事項に同意

する］のチェックボックスは、チェックマークを付けて設定を完了すると元に戻すことができません。チェックマークを付けるときには、設定をしても問題がないことをよく確認してください。

11.［完了］をクリックします。

［設定確認］画面が表示されます。

12. 設定内容を確認し、［タスク名］にタスク名を入力します。

13.［適用］をクリックして設定をストレージシステムに適用します。設定した内容はタスクとしてキューイングされ、順に実行されます。

ヒント

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

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

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

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

ストレージシステムの設定ファイルをバックアップする手順については、『Hitachi Device Manager -Storage Navigator ユーザガイド』を参照してください。

9.3 暗号化鍵を作成する

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

ストレージシステムごとに作成できる暗号化鍵の数は次のとおりです。

モデル	ストレージシステムごとに作成できる暗号化鍵の数
VSP 5000 シリーズ	4,096

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

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

前提条件

・ 必要なロール：セキュリティ管理者（参照・編集）ロール

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

1. Storage Navigator の［管理］ツリーから［暗号化鍵］を選択し、［暗号化鍵］画面を表示します。

2. 画面右側の［暗号化鍵］タブを選択します。

3. 次のどちらかの方法で、［鍵生成］画面を表示します。

・［暗号化鍵］タブで［鍵生成］をクリックします。

・［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［鍵生成］を選択します。

4.［鍵生成］画面で暗号化鍵の数を指定します。

未使用鍵（属性が「空き」の暗号化鍵）が設定されます。鍵 ID は自動で割り当てられます。

5.［完了］をクリックします。

［設定確認］画面が表示されます。

6. 設定内容を確認し、［タスク名］にタスク名を入力します。

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

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

9.4　暗号化鍵をバックアップする

暗号化鍵を作成後は、すぐに二次バックアップを行ってください。

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

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

注意

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

二次バックアップには、Storage Navigator 動作 PC 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 Storage Navigator 動作 PC 内にファイルとしてバックアップするときはパスワードを設定します。このパスワードは暗号化鍵をリストアするときに必要です。このパスワードに使用する最小文字数を［パスワードポリシー編集（暗号化鍵バックアップ）］画面で設定できます。鍵管理サーバに接続してバックアップしている場合、鍵管理サーバがバックアップできる鍵の数には上限があります。このため、鍵管理サーバ上の暗号化鍵は定期的に削除してください。

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

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

9.5 Storage Navigator 動作 PC 内に暗号化鍵をファイルとしてバックアップするときに設定するパスワードの最小文字数を設定する

前提条件

・必要なロール：セキュリティ管理者（参照・編集）ロール

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

1.［設定］メニューから［セキュリティ管理］-［暗号化鍵］-［パスワードポリシー編集（暗号化鍵バックアップ）］を選択し、［パスワードポリシー編集（暗号化鍵バックアップ）］画面を表示します。

2. 各項目について、使用する最小文字数を設定します。

3.［完了］をクリックします。

［設定確認］画面が表示されます。

4. 設定内容を確認し、［タスク名］にタスク名を入力します。

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

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

9.6 Storage Navigator 動作 PC 内にファイルとして暗号化鍵をバックアップする

前提条件

・必要なロール：セキュリティ管理者（参照・編集）ロール

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

1. Storage Navigator の［管理］ツリーから［暗号化鍵］を選択し、［暗号化鍵］画面を表示します。

2. 画面右側の［暗号化鍵］タブを選択します。

3. 次のどちらかの方法で、［ファイルへ鍵バックアップ］画面を表示します。

・［暗号化鍵］タブで［鍵バックアップ］-［ファイルへ］をクリックします。

・［設定］メニューから［セキュリティ管理］-［暗号化鍵］-［ファイルへ鍵バックアップ］を選択します。

4.［パスワード］にパスワードを入力します。

このパスワードは暗号化鍵をリストアするときに必要です。

5.［パスワード再入力］に、確認用に再度パスワードを入力します。
6.［完了］をクリックします。
［設定確認］画面が表示されます。
7. 設定内容を確認し、［タスク名］にタスク名を入力します。
8.［設定確認］画面の［適用］をクリックします。
準備の完了を知らせるメッセージが表示されます
9.［OK］をクリックします。
暗号化鍵ファイルを保存する画面が表示されます。
10. 暗号化鍵ファイルの保存場所とファイル名を指定します。
暗号化鍵ファイルの拡張子は[.ekf]としてください。
11.［保存］をクリックして画面を閉じます。
キャンセルはできません。また、［設定確認］画面の［「適用」をクリックした後にタスク画面を表示］のチェックボックスにチェックマークが付いている場合は、タスク一覧画面が表示されます。
保存した暗号化鍵ファイルとパスワードは、ユーザが責任を持って保管してください。

9.7　鍵管理サーバに接続して暗号化鍵をバックアップする

前提条件

・ 必要なロール：セキュリティ管理者（参照・編集）ロール

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

1. Storage Navigator の［管理］ツリーから［暗号化鍵］を選択し、［暗号化鍵］画面を表示します。
2. 画面右側の［暗号化鍵］タブを選択します。
3. 次のどちらかの方法で、［サーバへ鍵バックアップ］画面を表示します。
［暗号化鍵］画面を使用する場合：
a. 次のどちらかの方法で、［サーバへ鍵バックアップ］画面を表示します。
［暗号化鍵］タブで［鍵バックアップ］ - ［サーバへ］をクリックします。
［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバへ鍵バックアップ］を選択します。
［サーバ内鍵バックアップ参照］画面を使用する場合：
a. 次のどちらかの方法で、［サーバ内鍵バックアップ参照］画面を表示します。
［暗号化鍵］タブで［サーバ内鍵バックアップ参照］をクリックします。
［設定］メニューから［セキュリティ管理］ - ［暗号化鍵］ - ［サーバ内鍵バックアップ参照］を選択します。
b. ［サーバへ鍵バックアップ］をクリックします。
4.［説明］に暗号化鍵をバックアップする目的を入力します。入力は任意です。
5.［完了］をクリックします。

［設定確認］画面が表示されます。

6. 設定内容を確認し、［タスク名］にタスク名を入力します。

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

ヒント

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

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

9.8 データの暗号化を有効にする

暗号化の設定は、パリティグループに属するボリュームがすべて閉塞状態であるか、パリティグループに属するボリュームが 0 個の場合だけできます。パリティグループ内に 1 つでも閉塞状態でないボリュームがある場合は、暗号化の設定ができません。『オープンシステム構築ガイド』を参照し、ボリュームを閉塞した上で、暗号化を設定してください。

暗号化を設定するパリティグループにプールボリュームが定義されている場合は、暗号化を有効にできません。『オープンシステム構築ガイド』を参照し、当該プールボリュームをプールから削除した上で、暗号化を設定してください。

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

パリティグループに対して、データの暗号化を有効にする手順を次に示します。

前提条件

・ 必要なロール：セキュリティ管理者（参照・編集）ロール（フォーマットを同時にする場合は、セキュリティ管理者（参照・編集）ロールとストレージ管理者（プロビジョニング）ロール）・ パリティグループにプールボリュームが定義されていないこと

・ パリティグループの容量拡張設定が無効であること

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

1. Storage Navigator の［管理］ツリーから［パリティグループ］を選択し、［パリティグループ］画面を表示します。

2. 画面右側の［パリティグループ］タブを選択するか、ツリーから［Internal］を選択した上で画面右側の［パリティグループ］タブを選択します。

3. 画面右側の［パリティグループ］タブのテーブルの［LDEV 状態］欄で LDEV の状態を確認します。

・ ［Blocked］と表示されている場合、LDEV は閉塞状態です。

· ［Blocked］と表示されていない場合、LDEV は閉塞状態ではありません。LDEV が 0 個であることを確認するか、LDEV が存在する場合は、閉塞状態にしてください。

4. パリティグループのチェックボックスを選択します。

パリティグループを選択しない場合は、すべてのパリティグループが暗号化を設定する対象となります。

5. 次のどちらかの方法で、［暗号化編集］画面を表示します。

· ［パリティグループ］タブで［暗号化編集］をクリックします。

· ［アクション］メニューから［パリティグループ管理］ - ［暗号化編集］を選択します。

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

注意

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

7.［追加］をクリックし ます。

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

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

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

8.［完了］をクリックします。

［設定確認］画面が表示されます。

9. 設定内容を確認し、［タスク名］にタスク名を入力します。

10.［設定確認］画面の［適用］をクリックします。

変更内容をストレージシステムに適用するかどうかを尋ねるメッセージが表示されます。

11.［OK］をクリックしてメッセージを閉じます。

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