NEC

iStorage V10e/V100/V300

システム管理者ガイド

iStorage

IV-UG-002-003-12

このたびは iStorage V10e, V100, V300 をお買い上げいただき、誠にありがとうございます。

本書の内容については万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、お買い求めの販売窓口にご連絡ください。

輸出時の注意

本製品を輸出される場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

なお、ご不明な場合は、弊社担当営業にお問い合わせください。

商標類

AMI は，American Megatrends Inc.の登録商標です。

Cisco は，Cisco Systems, Inc.またはその関連会社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。

Emulex は,Broadcom の商標です。"Broadcom"は Broadcom Inc.および/またはその子会社を指します。

Ethernet とイーサネットは,富士フイルムビジネスイノベーション株式会社の登録商標です。

Google Chrome は Google Inc.が所有する商標または登録商標です。

IBM，GPFS は，世界の多くの国で登録された International Business Machines Corporation の商標です。

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,Windows,Windows NT,Windows Server,Windows Vista,Microsoft Edge,および 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。

Red Hat は,米国およびその他の国での Red Hat, Inc.の登録商標もしくは商標です。

Sun,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。

SUSE は，米国およびその他の国における SUSE LLC の登録商標または商標です。

VMware は,米国およびその他の国における Broadcom, Inc.の登録商標または商標です。

その他記載の会社名、製品名は、それぞれの会社の商標、もしくは登録商標です。

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。

本書の内容については万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、お買い求めの販売窓口にご連絡ください。

当社では、本装置の運用を理由とする損失、逸失利益等の請求につきましては、いかなる責任も負いかねますので、あらかじめご了承ください。

ストレージシステムの保証

二重化されている部位の一点故障の場合でもそれが重大事故につながる恐れがある場合、ストレージシステムは停止することがあります。

バックアップ

ホストやストレージシステム自身のハードウェア、ソフトウェアの不慮の事故により、お客様の大切なデータが失われても弊社では保証できません。

そのような場合にデータの回復ができるよう、お客様自身で全データをバックアップしておいてください。データの被害を最小限に抑えられます。

廃棄

このマーク表示は WEEE（Waste Electrical and Electronic Equipment Directive 2002/96/EC）に基づくものです。

このマークは、このマークが表示されている製品を、一般のゴミとして廃棄してはならず、廃棄を行う国や地域の規則に従って適切な回収システムを使用しなければならないことを示します。

バッテリのリサイクル

この製品にはニッケル水素電池を使用しております。ニッケル水素電池はリサイクル可能な貴重な資源です。バッテリを交換の際は、弊社担当営業、お買い求めいただいた販売店または保守サービス会社に連絡してください。(このニッケル水素電池は資源有効利用促進法で指定再資源化製品に指定され、リサイクルの必要があります。)

バッテリに貼ってあるマークは、リサイクル可能な部品であることを示すスリーアローマークです。

オープンソースライセンス

UEFI Development Kit 2010

This product includes UEFI Development Kit 2010 written by the UEFI Open Source Community. (http://sourceforge.net/apps/mediawiki/tianocore/index.php?title=UDK2010)

Copyright (c) 2004, Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. Neither the name of the Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes software developed by Net-SNMP development team. (http://www.net-snmp.org/)

This product includes software developed by Lighttpd Developers. (http://www.lighttpd.net/)

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

This product includes software developed by the OpenBSD Project. (http://www.openssh.com/)

This product includes software developed by The Tcpdump team. (http://www.tcpdump.org/)

This product includes software compiled with tools developed by Google Inc. (http://code.google.com/)

This product includes software developed by kgabis. (http://kgabis.github.io/parson/)

This product includes software developed by Theodore Y.

This product includes software developed by Daniel Veillard. (http://www.xmlsoft.org/)

This product includes software developed by Free Software Foundation. (http://www.gnu.org/software/libiconv/)

This product includes software developed by Open Market, Inc. (fastCGI)

This product includes software developed by Oracle Corporation. (https://java.com/)

This product includes software developed by The Apache Software Foundation. (https://commons.apache.org/proper/commons-cli/)

This product includes software developed by Azul Systems, Inc.(https://www.azul.com/)

その他のライセンス

This product includes BIOS/BMC software developed by AMI.

ご注意

• iStorage V10e, V100, V300 を使用するために必ずこのガイドを読み、操作手順と指示事項をよく理解してから操作してください。

• このガイド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。

• このガイドの著作権は日本電気株式会社にあります。このガイドのすべて、または一部分を書面による了解無しに転載、または複写することはできません。

発行

2025 年 10 月

著作権

© NEC Corporation 2021-2025

目次

第 1 章 概要 1

1.1 システム構成 1

1.2 ストレージシステムの機能とユーザインタフェース 3

1.3 マニュアル体系 4

1.4 ストレージシステムの管理モデル 6

1.5 HA Storage Advisor Embedded を利用して管理する構成 6

1.5.1 構成概要 6

1.5.2 管理 PC の要件 8

1.5.3 管理 LAN の要件 10

1.5.4 利用例 10

1.5.5 各ツールのログイン方法 11

1.5.6 HA Storage Advisor Embedded 利用の構成の注意事項 12

1.5.7 HA Storage Advisor Embedded でソフトウェアを利用する場合の注意事項 13

1.5.8 ストレージシステムのボリュームをサーバに割り当てるための設定 14

1.5.8.1 サーバからホストグループ/iSCSI ターゲットを管理するための要件 15

1.5.8.2 サーバからホストグループ/iSCSI ターゲットを管理する場合の運用 16

1.6 Storage Navigator を利用して管理する構成 17

1.6.1 構成概要 17

1.6.2 管理サーバ（SVP）の要件 19

1.6.2.1 SVP のハードウェア条件 19

1.6.2.2 管理サーバ（SVP）に必要なソフトウェア 21

1.6.2.3 管理サーバ（SVP）の電源 ON/OFF に関する注意事項 25

1.6.2.4 IP アドレスを変更する場合の注意事項 25

1.6.3 管理するための PC（管理クライアント）要件 25

1.6.3.1 ストレージシステムを管理するための PC（管理クライアント） 25

1.6.3.2 管理クライアントを利用するために必要なソフトウェア 26

1.6.4 ストレージシステムを利用するために必要なソフトウェア 27

1.6.5 管理 LAN の要件 29

1.6.6 特定機能を利用するために必要な SVP ソフトウェア 29

第 2 章 初期構築の概要 31

2.1 初期構築までの流れ 31

第 3 章 Maintenance Utility の機能 33

3.1 ファームウェア 33

3.1.1 ファームウェアバージョンの確認 33

3.1.2 ファームウェアの更新 33
3.2 ユーザ管理 34
3.2.1 ロール、リソースグループ、およびユーザグループの目的 34
3.2.2 ロール 34
3.2.3 リソースグループ 36
3.2.4 ユーザグループ 36
3.2.5 管理ツールとビルトイングループ 37
3.2.6 ユーザグループを作成する場合の参考情報 38
3.2.6.1 Maintenance Utility の操作に必要なロール 38
3.2.6.2 HA Storage Advisor Embedded の操作に必要なロール 39
3.2.6.3 内蔵 CLI の操作に必要なロール 39
3.2.6.4 RAID Manager の操作に必要なロール 39
3.2.6.5 エクスポートツール 2 の操作に必要なロール 40
3.2.7 ユーザ名とパスワードの文字数と使用可能文字 40
3.2.8 ユーザアカウントポリシーの設定 41
3.2.8.1 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 42
3.2.8.2 ユーザアカウントのパスワードポリシー設定 44
3.2.8.3 メールサーバの設定 47
3.2.8.4 テストメールの送信 48
3.2.8.5 ユーザ個別のパスワードポリシーの適用 49
3.2.8.6 ユーザ個別のメールアドレスの設定 51
3.2.8.7 ユーザアカウント状態の確認 52
3.2.8.8 アカウントロックの解除 53
3.2.8.9 アカウントの有効化 53
3.2.9 ユーザアカウントの作成 54
3.2.10 パスワードの変更 55
3.2.11 ユーザアカウントの無効化 57
3.2.12 ユーザアカウントの削除 57
3.2.13 ユーザアカウントのバックアップ 58
3.2.14 ユーザアカウントのリストア 58
3.3 アラート通知 59
3.3.1 メール通知の設定 61
3.3.2 テストメールの送信 61
3.3.3 アラート通知を蓄積するための Syslog の設定 63
3.3.4 アラート通知を蓄積するための Syslog サーバへのテストメッセージの送信 64
3.3.5 SNMP エージェントの設定 66
3.3.6 テスト SNMP トラップの送信 66
3.3.7 SNMP エンジン ID を確認する 67

3.4 ライセンス 68
3.4.1 ライセンスキーの参照 68
3.4.2 ライセンスキーの追加 69
3.4.3 ライセンスキーの有効化 69
3.4.4 ライセンスキーの無効化 70
3.4.5 ライセンスキーのアンインストール 70
3.5 ネットワーク設定 71
3.5.1 ネットワーク設定の変更 71
3.5.2 ネットワーク拒否設定の変更 73
3.6 日時設定 73
3.6.1 日時設定の変更 73
3.6.2 システム日時の更新 75
3.7 監査ログ 76
3.7.1 監査ログを蓄積するための Syslog の設定 76
3.7.2 監査ログを蓄積するための Syslog サーバへテストメッセージを送信 77
3.7.3 ストレージシステムに保存された監査ログをエクスポートする 78
3.8 外部認証 80
3.8.1 LDAP ディレクトリサーバの要件 81
3.8.2 LDAP の設定 82
3.8.3 無効化 83
3.9 システムモニタ 83
3.9.1 システムモニタの表示 83
3.10 初期設定 84
3.10.1 初期設定ウィザードによる設定変更 84
3.11 電源管理 86
3.11.1 ストレージシステムの電源 ON 86
3.11.2 ストレージシステムの電源 OFF 87
3.11.3 UPS のモード編集 88
3.12 システム管理 88
3.12.1 パスワードの変更 88
3.12.2 ログインメッセージの編集 90
3.12.3 暗号化スイートの選択 90
3.12.4 証明書ファイルの更新 91
3.12.5 システムロックの強制解除 92
3.12.6 GUM のリブート 92
3.12.7 システムダンプのダウンロード 93
3.12.8 スモールシステムダンプのダウンロード 94

3.12.9 構成情報バックアップのダウンロード 95
3.12.10 ボリューム状態の参照 95
3.13 アラートの表示 95
3.13.1 アラート表示 95
3.13.2 FRU に関するアラート表示 95
第 4 章 ストレージシステム運用上の注意 96
4.1 Storage Navigator 使用時の注意 96
4.2 ストレージシステムのサービスを開始できる台数 96
4.3 ウィルス検出プログラムの使用に関する注意事項 97
4.4 ストレージシステムに対するネットワーク監視（Ping 応答またはリンクアップ/リンクダウンによる監視） 98
4.5 電源オフ時間の注意 99
4.6 SVP のデフラグツールに関する注意事項 100
第 5 章 トラブルシュート 101
5.1 トラブルの発生からトラブルシューティングまでの流れ 101
5.2 トラブルを認識する状況とトラブルシューティング手順の参照先 103
5.3 トラブルシューティング作業前の確認 105
5.4 ストレージ管理ソフトウェアおよび SVP ソフトウェアの操作時にトラブルが発生した場合の対処手順 107
5.4.1 ストレージ管理ソフトウェアおよび SVP ソフトウェア インストール時のトラブルシューティング 107
5.4.2 Storage Device List 操作時のトラブルシューティング 111
5.4.3 Storage Navigator 操作時のトラブルシューティング 118
5.4.4 ストレージ管理ソフトウェアおよび SVP ソフトウェアの操作時に発生するその他の障害 121
5.5 Maintenance Utility の操作時にトラブルが発生した場合の対処手順 122
5.6 ホストがストレージを認識できない場合の対処手順 127
5.7 管理 GUI でアラートを確認した場合の対処手順 128
5.7.1 アラート詳細の確認方法 131
5.7.2 FRU（Field Replacement Unit）に関するアラートの確認 133
5.7.3 管理 GUI を起動する際にトラブルが発生した場合の対処手順 137
5.8 障害通知を受け取った場合の対処手順 137
5.9 バックグラウンドサービスログを使用したトラブルシューティング 137
5.9.1 Storage Device List サーバ 139

5.9.2 SVP RMI-API フォワードサーバ 141
5.9.3 Web アプリケーションサーバ 143
5.9.4 Storage Navigator サーバ 144
5.9.5 SVP RMI-API サーバ 147
5.9.6 外部認証中継サービス 156
5.9.7 通信サービス 158
5.9.8 KMIP コミュニケータ 162
5.10 仮想メモリの設定方法 162
5.11 ダンプファイルの採取方法 163
5.11.1 ダンプツールを使用した採取 163
5.11.2 手動によるダンプファイルの採取 167
5.12 SVP のパフォーマンスに関する問題がある場合の対処手順 169
5.13 ネットワークトレース採取ツールの使用方法 172
5.14 ストレージシステムに対するネットワーク監視で通信不可または疎通不可が発生した場合の対処 174
5.15 USN ジャーナルの使用容量が不足した場合の対処 174
5.16 RAID Manager の停止手順 176
付録 A. 初期設定作業 178
A.1 初期設定作業の概要 178
A.1.1 初期設定作業の目的 178
A.1.2 初期設定作業の項目 178
A.1.3 初期設定作業を実施するための前提条件 179
A.2 管理クライアントの初期設定を行う 180
A.2.1 管理クライアントの IP アドレスを設定する 180
A.2.2 管理クライアントにロケールを設定する 181
A.2.3 管理クライアントに WMIC 機能を追加する 181
A.3 管理クライアントに必要なソフトウェアをインストールする 181
A.4 SVP とストレージシステムおよび管理クライアントのネットワーク設定をする 181
A.4.1 ストレージシステムと SVP の IP アドレスを設定する 182
A.4.2 管理クライアントと SVP を接続するためのファイアウォールの設定 185
A.4.3 SVP とストレージシステムを接続するためのファイアウォールの設定 186
A.4.4 管理サーバ（SVP）のファイアウォールの設定 186
A.5 管理サーバ（SVP）の初期設定を行う 187
A.5.1 SVP のシステム日時を設定する 188
A.5.2 管理サーバ（SVP）にロケールを設定する 188

A.5.2.1 Windows 10 の場合 188
A.5.2.2 Windows Server 2016 の場合 188
A.5.2.3 Windows Server 2019 の場合 189
A.5.2.4 Windows 11 の場合 189
A.5.2.5 Windows Server 2022 の場合 190
A.5.3 管理サーバ（SVP）に WMIC 機能を追加する 190
A.6 管理サーバ（SVP）に必要なソフトウェアをインストールする 191
A.6.1 インストール作業手順 192
A.7 管理サーバ（SVP）にストレージシステムを登録する 199
A.7.1 管理サーバ（SVP）にストレージシステムを登録する 199
A.8 デスクトップヒープの指定値を変更する 206
A.8.1 デスクトップヒープの指定値をバッチファイルで変更する 206
A.8.2 デスクトップヒープの指定値を Windows のデフォルト値に戻す 207
A.9 ストレージシステムの初期設定を行う 208
A.9.1 Storage Navigator にログインする 208
A.9.2 SVP から直接ログインする 208
A.9.3 管理クライアントから Storage Navigator にログインする 211
A.9.3.1 Storage Device Launcher をインストールしたユーザでログインする手順（ユーザに管理者権限がある場合） 212
A.9.3.2 Storage Device Launcher をインストールしたユーザでログインする手順（ユーザに管理者権限がない場合） 215
A.9.3.3 Storage Device Launcher をインストールしていないユーザの場合 217
A.9.4 管理クライアントに Web Console Launcher を設定する 217
A.9.5 SVP の Web Console Launcher を設定する 218
A.9.6 ストレージシステム情報を編集する 218
A.9.6.1 Storage Navigator からストレージシステム情報を編集する 218
A.10 初期設定作業を確認する 219
付録 B. 初期構築作業 221
B.1 初期構築作業の概要 221
B.1.1 初期構築作業の目的 221
B.1.2 初期構築作業の流れ 221
B.1.3 初期構築作業を実施するための前提条件 222
B.2 ライセンスの設定 222
B.3 監査ログの設定 222
B.4 障害通知設定 222
B.4.1 Windows イベントログでストレージシステムの障害情報を監視する 223
B.4.1.1 ストレージシステムの障害情報を Windows イベントログに出力する 223

B.4.1.2 Windows イベントログの参照.....224
B.4.1.3 ストレージシステムの障害情報の出力例.....225
B.4.1.4 ストレージシステムの運用に支障が無いイベント.....226
B.5 ホストに割り当てる LDEV の作成と LUN パス定義の手順.....227
B.5.1 Storage Navigator から LDEV 作成と LUN パス定義をする.....228
B.6 ホスト接続ポートの設定の手順.....232
B.6.1 Storage Navigator からポートを設定する.....232
B.6.1.1 Fibre Channel ポートの設定（Storage Navigator）.....232
B.6.1.2 iSCSI ポートの設定（Storage Navigator）.....233
B.7 ホストグループ/iSCSI ターゲットの編集の手順.....234
B.7.1 Storage Navigator からホストグループ/iSCSI ターゲットを編集する.....235
B.7.1.1 ホストグループの編集（Storage Navigator）.....235
B.7.1.2 iSCSI ターゲットの編集（Storage Navigator）.....236
B.7.2 ホストモード一覧.....237
B.7.3 ホストモードオプション一覧.....239
B.8 初期構築作業完了後の確認.....244
付録 C. SSL 通信の設定.....245
C.1 SSL とは.....245
C.2 ストレージシステムの SSL 通信.....245
C.3 SSL 通信の設定の流れ.....249
C.4 SVP のサーバ証明書を更新するときの注意事項.....251
C.5 秘密鍵を作成.....251
C.6 公開鍵を作成.....252
C.7 署名付き証明書を取得.....254
C.8 署名付きの信頼できる証明書を取得.....255
C.9 SSL 証明書のパスフレーズを解除.....255
C.10 SSL 証明書を PKCS#12 形式に変換.....257
C.11 SVP と管理クライアント間の SSL 通信の署名付き証明書を SVP へアップロード.....258
C.12 SVP と管理クライアント間の SSL 通信の証明書をデフォルトに変更.....259
C.13 SVP と管理クライアント間の SSL 通信の証明書の確認（Microsoft Edge）.....260
C.14 SVP と管理クライアント間の SSL 通信の証明書の確認（Google Chrome）.....261
C.15 SVP 接続用証明書と 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.....261

C.16 SVP 接続用証明書を SVP へアップロード....262
C.17 SVP 接続用証明書をデフォルトに変更....263
C.18 Web サーバ接続用証明書を SVP へアップロード....263
C.19 SVP へアップロードした Web サーバ接続用証明書の確認....265
C.20 Web サーバ接続用証明書をデフォルトに変更....265
C.21 SVP への HTTP 通信を拒否....266
C.22 SVP への HTTP 通信のブロックを解除....267
C.23 HSTS を有効化する....267
C.24 HSTS を無効化する....268
C.25 セキュリティ警告が表示されたときの対処方法....269
C.26 RSA 鍵交換の暗号スイート....271
C.26.1 SVP の RSA 鍵交換の暗号スイートを無効化する....272
C.26.2 SVP の RSA 鍵交換の暗号スイートを有効化する....273
C.27 DHE 鍵の下限長の設定....274
付録 D. SVP による外部認証サーバとの連携....277
D.1 外部サーバとの連携設定の手順....277
D.1.1 認証サーバの要件....279
D.1.1.1 認証サーバのプロトコル....279
D.1.1.2 LDAP サーバの設定に使用できる証明書ファイルの形式....280
D.1.1.3 Kerberos サーバの暗号タイプ....280
D.1.1.4 接続できる認証サーバ....281
D.1.1.5 サーバ検索....281
D.1.1.6 暗号通信....281
D.1.2 認証サーバに接続するための設定をする....281
D.1.3 コンフィグファイルの作成....283
D.1.3.1 LDAP 用コンフィグファイルの作成....283
D.1.3.2 RADIUS 用コンフィグファイルの作成....285
D.1.3.3 Kerberos 用コンフィグファイルの作成....288
付録 E. ドライブ管理....292
E.1 ドライブ管理（Storage Navigator 編）....292
E.1.1 スペアドライブの割り当てと削除....292
E.1.2 パリティグループの作成....293
E.1.3 パリティグループの削除....294
E.1.4 LDEV の作成....295
E.1.5 LDEV を LUN パスに割り当て....297

E.1.6 LDEV のフォーマット 299
E.1.7 LDEV の削除 300
E.1.8 LDEV からの LUN パス削除 301
E.1.9 タスクの状態確認 302

付録 F. Fibre Channel ポートおよび iSCSI ポートの管理 304

F.1 Fibre Channel ポートおよび iSCSI ポートの管理（Storage Navigator 編） 304
F.1.1 Fibre Channel ポートの設定変更 304
F.1.2 iSCSI ポートの設定変更 305
F.1.3 ホストグループの削除 306
F.1.4 iSCSI ターゲットの削除 307
F.1.5 iSCSI ポートでの CHAP 認証の使用 308
F.1.5.1 単方向 CHAP 認証の構築 309
F.1.5.2 単方向 CHAP 認証のユーザ削除 311
F.1.5.3 単方向 CHAP 認証の設定変更 312

付録 G. SVP の管理と機能 314

G.1 SVP の管理 314
G.1.1 SVP の電源を ON する 314
G.1.2 SVP の電源を OFF する 314
G.1.3 SVP を再起動する 315
G.1.4 SVP への接続を解除する 315
G.1.5 SVP のシステム日時とタイムゾーンを変更する 315

G.2 SVP の機能 316
G.2.1 セットアッププログラムを使用したストレージ管理ソフトウェア、SVP ソフトウェア、ファームウェアの更新 316
G.2.1.1 SSL 通信の署名付き証明書について 318
G.2.1.2 GUI による更新 319
G.2.1.3 SSL 通信の署名付き証明書の再インストール 331
G.2.2 SVP の IP アドレスを変更 331
G.2.3 SVP へのストレージシステム追加登録 333
G.2.3.1 セットアッププログラムによるストレージシステム追加登録 334
G.2.3.2 Storage Device List によるストレージシステム追加登録 345
G.2.4 Storage Device List を使用した SVP ソフトウェアの更新 349
G.2.5 Storage Device List からストレージシステム情報を変更 352
G.2.6 ストレージシステム単位のサービスを停止 354
G.2.7 ストレージシステム単位のサービスの開始 354
G.2.8 Storage Device List からストレージシステムの削除 355
G.2.9 SVP のソフトウェア設定情報のバックアップとリストア 356
G.2.9.1 SVP のソフトウェア設定情報のバックアップ 356

G.2.9.2 SVP のソフトウェア設定情報のリストア 359
G.2.10 ストレージ管理ソフトウェア、および SVP ソフトウェアの削除（アンインストール） 360
G.2.11 OSS のバージョン確認 362
G.2.12 ストレージシステムの切り替え 362
G.2.13 サービス状態一覧 364
G.2.14 ストレージシステムの登録先 SVP を変更 365
G.2.14.1 移行元 SVP の作業をする 365
G.2.14.2 移行先 SVP の作業をする 366
G.2.15 Log Dump の自動採取 367
G.2.15.1 Log Dump 自動採取機能の仕様 368
G.2.15.2 Log Dump 自動採取機能を利用するための準備 369
G.2.15.3 Log Dump Ex Tool 画面を起動する 369
G.2.15.4 Log Dump 自動採取機能を有効にする 370
G.2.15.5 Log Dump 自動採取機能の対象ストレージシステムを変更する 371
G.2.15.6 Log Dump 自動採取機能を停止する 372
G.2.15.7 Log Dump 自動採取機能を再開する 373
G.2.16 Log Dump Ex Tool 画面の操作 373
G.2.16.1 Log Dump の採取対象に SIM コードを追加する 373
G.2.16.2 Log Dump の採取対象から SIM コードを削除する 376
G.2.16.3 Log Dump の採取対象から SIM コードを除外する 378
G.2.16.4 Log Dump の除外対象から SIM コードの除外設定を解除する 380
G.2.16.5 Log Dump をコピーする 383
G.2.16.6 Log Dump の採取中に採取処理を中止する 384
G.2.17 Log Dump の採取が失敗した場合の対応 386
G.2.18 Log Dump の採取処理で発生するイベントと対処方法 388
G.2.19 Log Dump Ex Tool が表示するメッセージ 389
G.2.20 Jetty の定期リブート 390
G.2.20.1 Jetty 定期リブートの設定 390
G.2.20.2 Jetty 定期リブートの解除 391
G.2.20.3 Jetty 定期リブートの設定内容の参照 392
G.2.21 DNS サフィックスの設定 393

付録 H. ホスト接続の参考情報 394

H.1 Fibre Channel ホスト 394
H.1.1 複数ホストでの構築 394
H.1.2 ゾーニング 395
H.1.3 ホスト側に設定するコマンド多重数 396
H.1.4 デバイスタイムアウト値の推奨値 396
H.2 iSCSI ホスト 396

H.2.1 iSCSI の概要 397
H.2.2 iSCSI I/F の仕様 397
H.2.3 iSCSI 規格 399
H.2.4 注意事項 400
H.2.5 OS に依存する注意事項 402
H.2.6 iSCSI に関するトラブルシューティング 403
H.2.7 デバイスタイムアウト値の推奨値 405

付録 I. ファイアウォール使用環境で必要な設定 406

I.1 ファイアウォールの概要 406

付録 J. SVP に保存された監査ログのエクスポート 407

J.1 SVP に保存された監査ログをエクスポートする 407

付録 K. 管理クライアントから SVP への接続方法 409

K.1 管理クライアントから SVP にリモートデスクトップ接続する 409

付録 L. SVP で使用するポート番号の変更・初期化 411

L.1 SVP で使用するポート番号を変更する 411
L.2 SVP で使用するポート番号を初期化する 414
L.3 SVP で使用するポート番号変更時の影響 415
L.4 自動割り振りされたポート番号を再割り振りする 416
L.5 自動割り振りされたポート番号を初期化する 417
L.6 自動割り振りされるポート番号の範囲を変更する 419
L.7 自動割り振りされるポート番号の範囲を初期化する 421
L.8 SVP で使用されるポート番号の参照 422
L.9 ポート番号を使用しているアプリケーションを確認する 423

付録 M. 障害通知メール、Syslog メッセージ、SNMP メッセージの内容 426

M.1 障害通知メールの内容 426
M.2 Syslog メッセージの内容 426
M.3 SNMP メッセージの内容 430

付録 N. このマニュアルの参考情報 432

N.1 モデルやファームウェアバージョンによる転送プロトコルの表示の差異 432

用語集 433

索引 439

はじめに

このマニュアルは iStorage V10e, V100, V300 用のユーザガイドです。

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。
また、 総称を、iStorage V シリーズと称することがあります。

ここでは、マニュアルの概要と読み方を説明します。また、サポートを受けられるときのお問い合わせ先と、ストレージシステムを安全にお取り扱いいただくための注意事項を説明します。

マニュアルの概要

マニュアルの目的や対象読者、関連マニュアルについて説明します。

マニュアルの目的

このマニュアルではストレージシステムの導入作業として、設置、初期設定、および初期構築を行い、基本的な運用を開始できるようにすることを目的とします。

また、ストレージシステムの導入時と運用時に不具合が発生した場合、その解決のためのトラブルシューティングを行うことも目的とします。

対象読者

このマニュアルは、次の方を対象読者として記述しています。

- ストレージシステムを運用管理する方
- Windows コンピュータを使い慣れている方
- Web ブラウザを使い慣れている方
- ネットワークに関する知識がある方

マニュアルの位置づけ

このマニュアルは、ストレージシステムの導入時にお読みいただくマニュアルです。運用時にハードウェアの不具合が発生した場合も、このマニュアルをお読みください。

プログラムプロダクトを使用したストレージシステムの構築や運用は、「関連するマニュアル（xvi ページ）」に記載のマニュアルを参照してください。

関連するマニュアル

このマニュアルの関連マニュアルを次に示します。必要に応じてお読みください。

- 『ハードウェア リファレンスガイド』

- 『ドキュメントマップ』
- 『システム構築ガイド』
- 『HA Device Manager - Storage Navigator ユーザガイド』
- 『Performance Manager (Performance Monitor, Server Priority Manager, QoS) ユーザガイド』
- 『SNMP Agent ユーザガイド』
- 『監査ログ リファレンスガイド』

マニュアルの読み方

このマニュアルの構成と、マニュアル内の表記について説明します。

マニュアルの構成

このマニュアルは、次に示す章と付録から構成されています。

章	内容
第 1 章　概要（1 ページ）	本ストレージ装置の管理手法と、必要な物品、注意事項を記載しています。
第 2 章　初期構築の概要（31 ページ）	ストレージ導入時のおおまかな流れを説明しています。
第 3 章　Maintenance Utility の機能（33 ページ）	Maintenance Utility のメニューについて記載しています。
第 4 章　ストレージシステム運用上の注意（96 ページ）	ストレージシステムを運用する上で注意が必要な事項を記載しています。
第 5 章　トラブルシュート（101 ページ）	導入時や運用時に不具合が発生した場合のトラブルシューティングについて記載しています。
付録 A.　初期設定作業（178 ページ）	ストレージシステムの初期設定作業について記載しています。
付録 B.　初期構築作業（221 ページ）	ストレージシステムの初期構築作業について記載しています。
付録 C.　SSL 通信の設定（245 ページ）	通信のセキュリティをより高めるための SSL 通信の設定について記載しています。
付録 D.　SVP による外部認証サーバとの連携（277 ページ）	システム管理に関する設定や操作について記載しています。
付録 E.　ドライブ管理（292 ページ）	ストレージのドライブ設定などについて記載しています。
付録 F.　Fibre Channel ポートおよび iSCSI ポートの管理（304 ページ）	ホストへ接続する Fibre Channel ポートと iSCSI ポートの設定や、ホストグループ、または iSCSI ターゲットの削除などを、Storage Navigator から行う方法を記載しています。
付録 G.　SVP の管理と機能（314 ページ）	SVP の管理方法と、SVP のストレージ管理機能について記載しています。
付録 H.　ホスト接続の参考情報（394 ページ）	ホストをストレージシステムに接続するときの参考情報について記載しています。
付録 I.　ファイアウォール使用環境で必要な設定（406 ページ）	ファイアウォールのポリシー・ルールを作成する場合に必要となる、ストレージシステムで使用するポート情報について記載しています。

章	内容
付録 J. SVP に保存された監査ログのエクスポート（407 ページ）	監査ログのエクスポート手順について記載しています。
付録 K. 管理クライアントから SVP への接続方法（409 ページ）	管理クライアントから SVP へリモートデスクトップ接続する手順について記載しています。
付録 L. SVP で使用するポート番号の変更・初期化（411 ページ）	SVP で使用するポート番号を任意のポート番号に変更する方法について記載しています。
付録 M. 障害通知メール、Syslog メッセージ、SNMP メッセージの内容（426 ページ）	障害通知メール、Syslog メッセージ、および SNMP メッセージの内容について記載しています。
用語解説	マニュアルで使用している用語の意味を記載しています。
索引	索引を記載します。

ファームウェアバージョン確認

このマニュアルは原則として最新のファームウェアバージョンを記載しています。

一部、機能によりファームウェアバージョンを確認していただく場合があります。

ファームウェアバージョンは、「3.1 ファームウェア（33 ページ）」を参照して確認してください。

マニュアルの参照と適合ファームウェアバージョン

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

- iStorage V100, V300 の場合

  93-07-27-XX 以降

- iStorage V10e の場合

  88-08-17-XX 以降

メモ

このマニュアルは、上記バージョンのファームウェアをご利用の場合に最も使いやすくなるよう作成されていますが、上記バージョン未満のファームウェアをご利用の場合にもお使いいただけます。

マニュアルで用いる表記

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。

マニュアルでの注意表記

このマニュアルでは、注意書きや補足情報を、次のとおり記載しています。

⚠ 注意

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

メモ

解説、補足説明、付加情報などを示します。

ヒント

より効率的にストレージシステムを利用するのに役立つ情報を示します。

マニュアルに掲載している画面図

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

操作方法

OS により操作が異なる場合があります。

インストールメディア（SVP メディア）の保管について

ストレージシステムとセットで納入されるインストールメディアを紛失しないよう、適切に保管願います。インストールメディアは、ストレージシステムの追加登録、SVP 交換などの保守作業の際に必要となります。

インストールメディアを紛失した場合、発注や発送などに時間を要します。これにより、ストレージシステムの保守やシステム稼働に支障が生じる場合があります。

マニュアルに掲載されている機能、ソフトウェアについて

以下の機能、およびソフトウェアは、ストレージシステムの一部のモデルにおいてサポートしていません。

サポートしていないストレージシステムを利用する場合、マニュアルに掲載されている機能、およびソフトウェアに関する記述は無効となります。

機能・ソフトウェア	サポートしていないストレージシステム
Dynamic Tiering	iStorage V10e
Realtime Tiering	
Data Retention Utility	
Server Priority Manager	

機能・ソフトウェア	サポートしていないストレージシステム
Volume Shredder	
Synchronous Replication	
Asynchronous Replication	
Active Mirror	

サポート

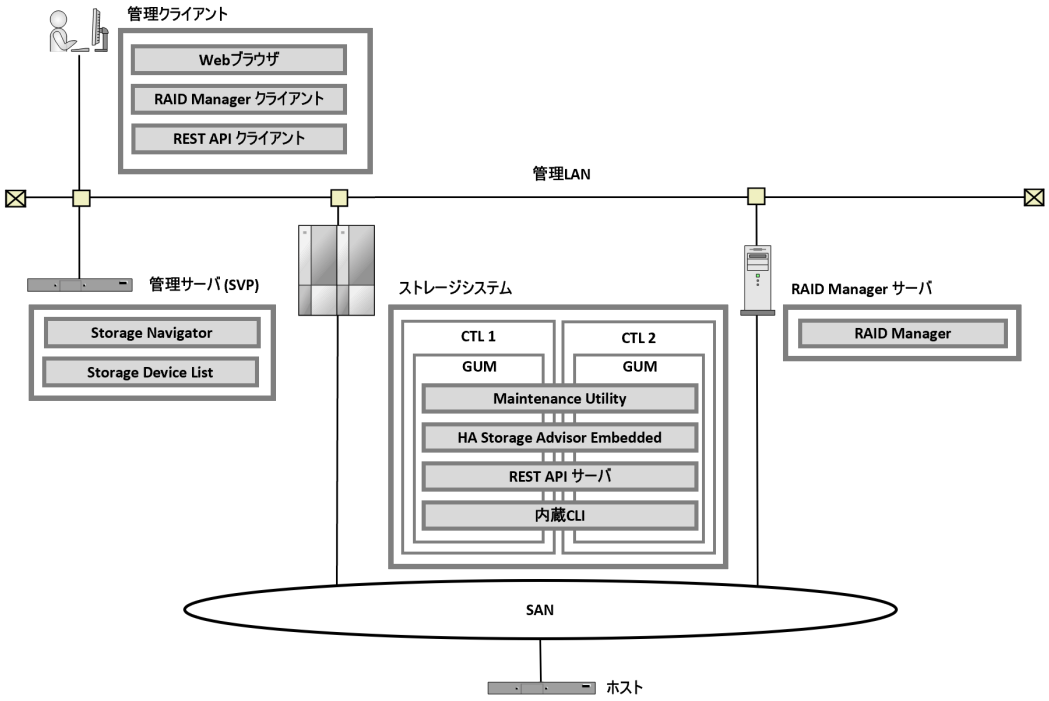
ストレージシステムの導入時および運用時のお問い合わせ先は、次のとおりです。

- PP サポートサービスにお問い合わせください。

第 1 章
概要

1.1　システム構成

本ストレージシステムの基本的なシステム構成を次の図に示します。



管理クライアント

各管理ツールにアクセスするための PC です。

管理クライアントには SVP と同じコンピュータを使用することもできます。

- Web ブラウザ

  GUI ベースの各管理ツールにアクセスするためのソフトウェアです。

- RAID Manager クライアント

  RAID Manager のサーバへリクエストを依頼するためのコマンドプロンプト、またはターミナルです。

- REST API クライアント

  REST API サーバへリクエストを依頼するためのソフトウェアです。

SVP（SuperVisor PC）

ストレージシステムの管理用サーバです。iStorage V10e の場合、SVP を使用しない構成を組むこともできます。

- Storage Navigator

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

- Storage Device List

  SVP に管理対象のストレージシステムを登録するためのソフトウェアです。

  - iStorage V100, V300 の場合、ストレージシステムを 1 台だけ登録できます。
  - iStorage V10e の場合、ストレージシステムを最大 8 台まで登録できます。

メモ

SVP とストレージシステム間の通信に SSL 通信を適用する際は、Storage Device List と、その Storage Device List に登録されているすべてのストレージシステムに、同じサーバ証明書（「C.1　SSL とは（245 ページ）」を参照）をアップロードしてください。詳細は「C.2　ストレージシステムの SSL 通信（245 ページ）」を参照願います。

ストレージシステム

本ストレージシステムです。

- CTL1、CTL2

  ストレージシステムと外部を接続するコントローラです。CTL1 と CTL2 の冗長構成です。

- GUM（Gateway for Unified Management)

  ストレージシステムの基本的な管理機能を持つコンピュータです。CTL1 と CTL2 それぞれに存在します。

- Maintenance Utility

  ストレージシステムのシステムやネットワークの設定、ユーザ情報やライセンスキーを管理する GUI ベースの管理ツールです。HA Storage Advisor Embedded や Storage Navigator からも画面を開けます。

- HA Storage Advisor Embedded

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

- REST API サーバ

  ストレージシステムの構成やリソースを操作する REST API のクライアントに応答するサーバです。

- 内蔵 CLI

  RAID Manager の簡易版です。

RAID Manager サーバ

RAID Manager を使用するためのサーバです。

- RAID Manager

  ストレージシステムの構成やリソースを操作するコマンドラインの管理ツールです。

管理 LAN

ストレージシステムを設定、管理するためのネットワークのセグメントです。

1.2　ストレージシステムの機能とユーザインタフェース

ストレージシステムの主な機能と管理ツール（ユーザインタフェース）の対応状況を次の表に示します。利用したい機能に対応するユーザインタフェースを選択してください。複数のユーザインタフェースの併用も可能です。

利用するユーザインタフェースやモデルによって、使用できる機能は異なります。詳細は各ユーザガイドを参照するか、お問い合わせください。

ストレージシステムの機能	機能の概要	ユーザインタフェース				
		HSAE	SN	API	内蔵CLI	RM
Dynamic Provisioning	ボリューム容量の仮想化	○	○	○	○	○
dedupe and compression	格納データの圧縮と重複データ排除による容量削減	○	○	○	○	○
Dynamic Tiering	アクセス頻度によりデータを最適なドライブへ移動	○	○	○	○	○
Realtime Tiering	アクセス頻度によりデータを最適なドライブへリアルタイムに移動	－	○	○	○	○
Resource Partition Manager	アプリケーションや業務単位で、ストレージリソースを分割	－	○	○	○	○
Virtual LUN	パリティグループに任意のサイズの論理ボリュームを作成	○	○	○	○	○
LUN Manager	ホストと論理ボリューム間にデータ入出力の経路（LU パス）を設定	○	○	○	○	○
Data Retention Utility	論理ボリュームにアクセス権を設定	－	○	－	－	○
Virtual Partition Manager	アプリケーションや業務単位で、キャッシュメモリを分割	－	○	○	○	○
Performance Monitor、性能グラフ	ストレージリソースの利用率やトラフィックの測定とグラフ表示	○	○	－	－	－
Quality of Service（QoS）	ボリューム単位に異なる性能レベル（I/O レートや転送レート）を設定	○	－	○	○	○

ストレージシステムの機能	機能の概要	ユーザインタフェース				
		HSAE	SN	API	内蔵CLI	RM
Server Priority Manager	サーバからストレージのアクセス回数やデータ量を制限	―	○	○	○	○
Volume Migration	運用中のボリューム上のデータを別のボリュームに移動	―	○	○	―	○
SNMP Agent, SNMP Manager	SNMP によるストレージ監視	○	○	○	―	―
Audit Log	監査ログの設定	―	○	○	―	―
Encryption License Key	ドライブ内データの暗号化	○	○	○	―	―
Volume Shredder	ボリューム内データの完全消去	―	○	○	○	○
Universal Volume Manager	他のストレージ内ボリュームの利用	―	○	○	○	○
Local Replication	同一ストレージ内でのボリュームコピー	―	○	○	―	○
Snapshot	ストレージシステム内データの更新差分（スナップショット）の保存、ボリュームコピー	○	○	○	○	○
Synchronous Replication	遠隔拠点間のボリュームコピー（短距離での同期コピー）	―	○	○	―	○
Asynchronous Replication	遠隔拠点間のボリュームコピー（遠距離での非同期コピー）	―	○	○	―	○
Active Mirror	ボリュームミラーリングによるデータ二重化	○	○	○	―	○

凡例

- HSAE：HA Storage Advisor Embedded
- SN：Storage Navigator
- API：REST API
- RM：RAID Manager
- ○：対応、―：非対応

1.3　マニュアル体系

本ストレージには、ストレージシステムの設置や初期設定作業、ユーザーインタフェースの使い方、各ストレージ機能の詳細といったさまざまなマニュアルが用意されています。目的に応じて参照してください。

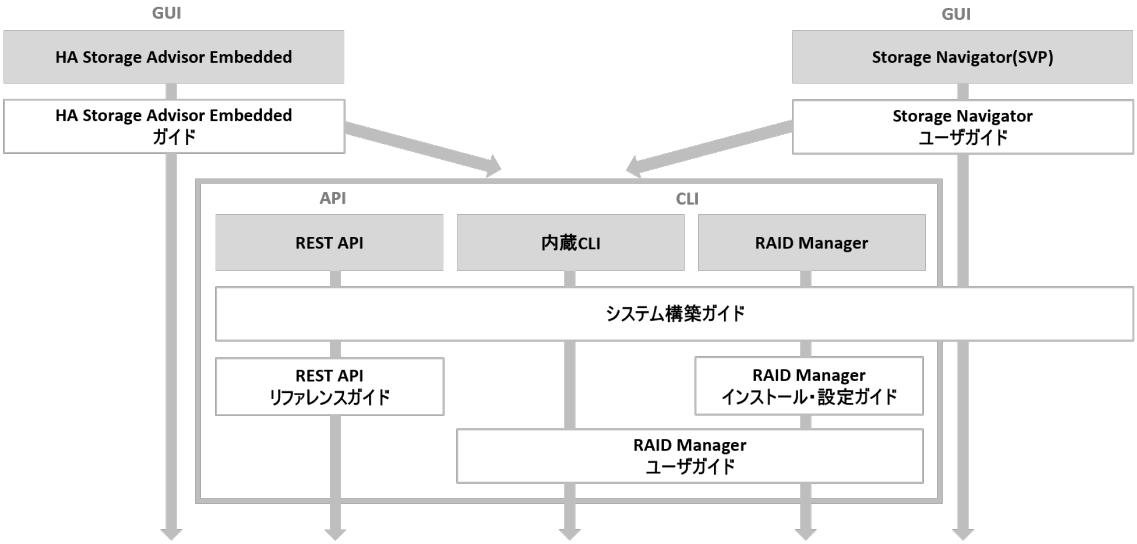
1. ストレージシステムの導入から初期構築

ハードウェアの概要・仕様
- ハードウェア リファレンスガイド

ストレージシステムの設定と初期構築
- システム管理者ガイド

ユーザガイドの一覧
- ドキュメントマップ

2. ストレージシステムの運用管理ツール



3. ストレージシステムの各機能詳細

システム管理
- システム管理者ガイド
- システム構築ガイド
- SNMP Agent ユーザガイド
- 監査ログ リファレンスガイド
- RAID Manager コマンドリファレンス

ボリューム管理
- システム構築ガイド
- Universal Volume Manager ユーザガイド
- RAID Manager コマンドリファレンス

レプリケーション
- Local Replication ユーザガイド
- Snapshot ユーザガイド
- Synchronous Replication ユーザガイド
- Asynchronous Replication ユーザガイド
- Active Mirror ユーザガイド
- RAID Manager コマンドリファレンス

パフォーマンス最適化
- Performance Manager ユーザガイド
- Virtual Partition Manager ユーザガイド
- Volume Migration ユーザガイド
- RAID Manager コマンドリファレンス

ユースケース
- コンパスドキュメント

セキュリティ
- Encryption License Key ユーザガイド
- Volume Shredder ユーザガイド
- システム構築ガイド
- RAID Manager コマンドリファレンス

トラブルシューティング
- SIMリファレンス
- Storage Navigator メッセージガイド
- RAID Manager ユーザガイド

ハードウェア
- ハードウェア リファレンスガイド

1.4　ストレージシステムの管理モデル

本マニュアルでは、HA Storage Advisor Embedded と、Storage Navigator をメインにしたストレージシステムの管理モデルを紹介します。ストレージシステムの用途に合わせて、どちらの構成を利用するかを判断してください。

- HA Storage Advisor Embedded を利用する構成

  詳細な設定を行わずにすぐ運用を始めたい場合に適しています。ストレージシステムを単体で使用するなど比較的小規模なストレージ管理に向いています。

- Storage Navigator を利用する構成

  ストレージリソースを詳細に設定管理する場合に適しています。複数のストレージシステムを連携させ、ストレージシステム間でリモートレプリケーションを行うなど比較的大規模なストレージ管理に向いています。

GUI の特徴比較

HA Storage Advisor Embedded	Storage Navigator
物理ドライブと RAID レベルを選択するだけで自動で容量効率が良いドライブ構成でプールを作成できます。	複数のドライブタイプを意識して、複数のプールやホストグループを作成できます。
プールからボリュームを簡単に作成できます。	性能チューニングオプション等を定義しながら作成・管理できます。
サーバにボリュームを割り当てる、という直観的な操作で、サーバが使うボリュームの定義とアクセスパスの設定が自動で行われます。	性能を考慮してアクセスパスの細かな設定が行えます。

1.5　HA Storage Advisor Embedded を利用して管理する構成

1.5.1　構成概要

ストレージ装置の管理ポート 2 ポートを LAN に接続して利用します。管理 PC をその LAN に接続してください。

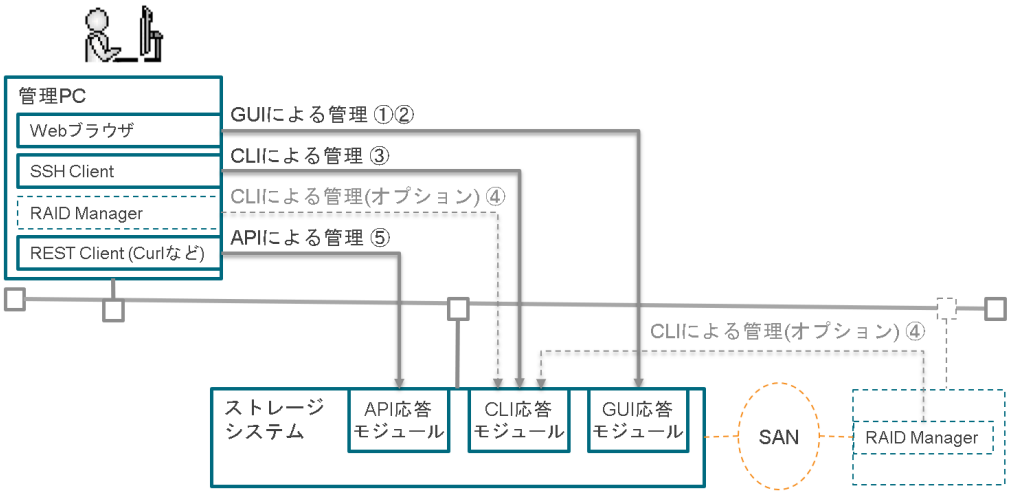


図 1-1　HA Storage Advisor Embedded 利用の構成

表 1-1　HA Storage Advisor Embedded 利用の場合の管理インターフェース

No	管理インターフェース	インストール先	管理ツール	主な用途
1	GUI	ストレージシステムに組み込み済	Maintenance Utility	• ストレージシステムのハードウェアの基本設定 • 管理ユーザの初期登録など
2			HA Storage Advisor Embedded	構成設定操作
3	CLI		内蔵 CLI※1	構成設定操作
4		外部サーバ※2	RAID Manager	• 構成設定操作 • レプリケーション操作
5	API	ストレージシステムに組み込み済	REST API	• 構成設定操作 • レプリケーション操作※3

注※1

内蔵 CLI は RAID Manager のサブセットです。raidcom で始まるコマンドが使用できます。

制限情報については、『RAID Manager ユーザガイド』を参照してください。

注※2

ストレージシステムの管理ポートが接続されている LAN の同一セグメントに接続されているプラットフォームである必要があります。プラットフォーム条件は、『RAID Manager インストール・設定ガイド』を参照してください。

注※3

REST API によるレプリケーション操作の詳細は、『REST API リファレンスガイド』および『HA Storage Advisor Embedded ガイド』を参照してください。

1.5.2　管理 PC の要件

1 台の PC で HA Storage Advisor Embedded、Maintenance Utility、内蔵 CLI を利用する場合、下記が条件となります。

なお、次に示す条件以外に、使用する OS の動作に必要なハードウェア条件にも従ってください。

管理 PC のハードウェア条件

項目	仕様
プロセッサ（CPU）	• Windows 11、Windows Server 2022、Windows Server 2025 2.1GHz 以上で 2 コア以上の 64 ビット互換プロセッサ 推奨:2.1GHz 以上で 4 コア以上の 64 ビット互換プロセッサ • Windows 11、Windows Server 2022、Windows Server 2025 以外 Pentium 4 640 3.2GHz 以上※ 推奨：Core 2 Duo E6540 2.33GHz 以上
メモリ（RAM）	• Windows 11、Windows Server 2022、Windows Server 2025 8GB 以上 推奨：16GB 以上 • Windows 11、Windows Server 2022、Windows Server 2025 以外 2GB 以上 推奨：3GB 以上
HDD または SSD	500MB 以上
ディスプレイ	True Color 32bit 以上 解像度：1280×1024 ピクセル以上
キーボードとマウス	必須
ネットワークカード（LAN）	100Base-TX/1000Base-T

注※

CPU ベンダ、およびプロセッサ・ファミリには依存しません。

ベンダーのサポート期間内のソフトウェア（OS を含む）を使用してください。サポート期間を過ぎているソフトウェアでの動作は保証できません。

管理 PC のソフトウェア条件

OS	アーキテクチャ	ブラウザ	他のソフトウェア
Windows Server 2025※7	64	Microsoft Edge※1、※5 Google Chrome※3	SSH ターミナルソフトウェア
Windows Server 2022※6	64	Microsoft Edge※1、※5 Google Chrome※3	
Windows Server 2019	64	Microsoft Edge※1、※5	
Windows Server 2016	64	Microsoft Edge※1、※5	

OS	アーキテクチャ	ブラウザ	他のソフトウェア
		Google Chrome※3	
Windows 11	64	Microsoft Edge※1、※5 Google Chrome※3	
Windows 10※2	32/64	Microsoft Edge※1、※5 Google Chrome※3	
RHEL 7.4	64	Mozilla Firefox※4	
RHEL 7.5	64	Mozilla Firefox※4	

注※1

Microsoft Edge を使用する場合は、ブラウザのポップアップブロックを無効に設定してください。また、スリープタブ機能をオフにするか、スリープ状態にしないサイトに HA Storage Advisor Embedded を追加してください（スリープ状態から一定時間経過による HA Storage Advisor Embedded のセッション無効化を防止できます）。

Microsoft のサポートポリシーに従い、各 OS で動作する最新のバージョンの Microsoft Edge だけをサポートします。

日本語で利用したい場合はブラウザの優先する言語を日本語に、英語で利用したい場合はブラウザの優先する言語を英語 (アメリカ合衆国)に設定してください。

注※2

Windows 10 のコマンドプロンプトの画面上で、不要なマウス操作を行わないでください。コマンドプロンプトから実行した処理が途中で停止してしまい、プロンプトが返ってこない事象が報告されています。

注※3

Google Chrome を使用する場合は、ブラウザのポップアップブロックを無効に設定してください。また、Web storage（DOM ストレージ）を有効に設定してください。

最新のバージョンを使用してください。

日本語で利用したい場合はブラウザのロケール（言語）を日本語（日本）［ja-JP］に、英語で利用したい場合はブラウザ のロケールを英語（米国）［en-US］に設定してください。

注※4

Mozilla Firefox を使用する場合は、ブラウザのポップアップブロックを無効に設定してください。

最新のバージョンを使用してください。

日本語で利用したい場合はブラウザのロケール（言語）を日本語（日本）［ja］に、英語で利用したい場合はブラウザ のロケールを英語［en］に設定してください。

注※5

Microsoft Edge の Internet Explorer モード（IE モード）はサポートしていません。

注※6

Windows Server 2022 は、次の DKCMAIN ファームウェアバージョンでサポートします。

- iStorage V100, V300 の場合：93-06-83-XX/00 以降
- iStorage V10e の場合：88-08-11-XX/00 以降

注※7

Windows Server 2025 は、次の DKCMAIN ファームウェアバージョンでサポートします。

- iStorage V100, V300 の場合：93-07-26-XX/00 以降
- iStorage V10e の場合：88-08-16-XX/00 以降

メモ

- サポートしている OS の最新情報は、PP サポートサービスで提供しています。
- Google Chrome は、Windows Server 2019 をサポートしていません。Windows Server 2019 では、Microsoft Edge を使用してください。
- Google Chrome は、RHEL 7.4 および RHEL 7.5 をサポートしていません。RHEL 7.4 および RHEL 7.5 では、Mozilla Firefox を使用してください。

1.5.3　管理 LAN の要件

管理 PC と管理ポートの間にファイアウォールが存在する場合、下記のポート番号が利用できるようにファイアウォールを設定する必要があります。

管理ツール	プロトコル	ポート番号
Maintenance Utility	HTTP	80
	HTTPS	443
HA Storage Advisor Embedded	HTTP	80
	HTTPS	443
内蔵 CLI	SSH	20522
RAID Manager	『RAID Manager インストール・設定ガイド』を参照してください。	
REST API	HTTP	80
	HTTPS	443

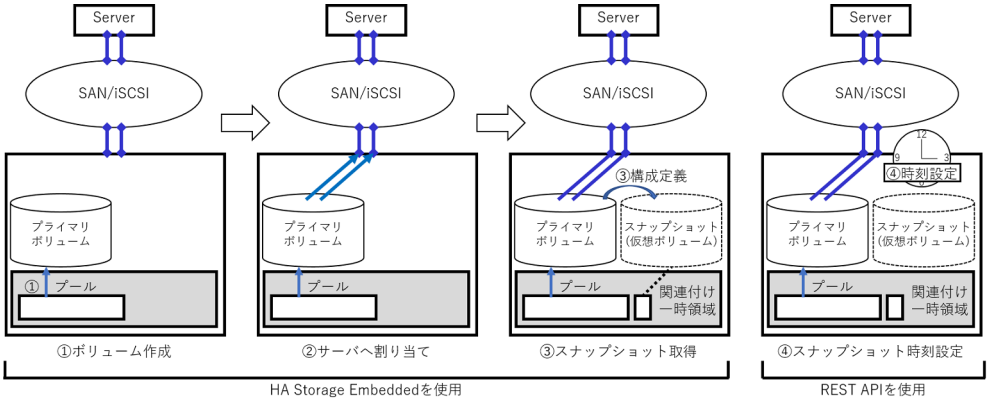
1.5.4　利用例

HA Storage Advisor Embedded を使用してボリュームの作成、ボリュームのサーバへの割り当て、およびスナップショットの取得までを行います。REST API を使用すると、REST API を

呼び出すプログラムの動作環境を使用して、スナップショットの取得時刻をスケジュールできます。

ストレージ要件の例

1 個のボリュームを準備し、スナップショットを取る。



ストレージを利用するための構成ステップ概略

各管理ツールを下記のステップで利用することにより、上記ストレージ要件の構成を適切に設定できます。

ボリュームを作成してサーバに割り当てるための作業の流れは、『HA Storage Advisor Embedded ガイド』の「ボリュームを利用するための準備の流れ」と「ボリューム割り当ての流れ」を参照してください。スナップショットを取得するための作業の流れは、「スナップショットによるバックアップの流れ」を参照してください。

1. スナップショットの取得対象となるボリューム（プライマリボリューム）を作成
2. プライマリボリュームをサーバに割り当て
3. スナップショットの取得
4. REST API を呼び出すプログラムの動作環境を使用して、スナップショットの取得時刻を定期的なスケジュールとして設定

1.5.5　各ツールのログイン方法

利用できる管理ユーザアカウントの初期値を下記に示します。このユーザアカウントは Maintenance Utility、HA Storage Advisor Embedded、REST API で共通です。

ユーザアカウント：`maintenance`

パスワード：`raid-maintenance`

- 上記のユーザアカウントのパスワード変更は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、保守時に保守員が作業をする場合にも必要となります。
- 上記のユーザアカウントは、「保守（ベンダ専用）」ロールを持っています。このため、このユーザアカウントでログインすると、通常は保守員が実施する操作ができてしまいます。「保守（ベンダ専用）」ロールを持たないユーザアカウントを作成して、各ツールにログインすることを推奨します。
- 上記以外の管理ユーザ、管理グループの登録・管理については、「3.2　ユーザ管理（34 ページ）」を参照してください。

管理ツール	主な手順または参照先
Maintenance Utility	ブラウザのウィンドウに、CTL1 の管理ポートの IP アドレスを使用して下記のように入力してください。CTL1 に障害が発生してエラーとなる場合は、CTL2 管理ポートの IP アドレスを使用してください。 http://(IP アドレス)/MaintenanceUtility/ または https://(IP アドレス)/MaintenanceUtility/
HA Storage Advisor Embedded	ブラウザのウィンドウに、CTL1 の管理ポートの IP アドレスを使用して下記のように入力してください。CTL1 に障害が発生してエラーとなる場合は、CTL2 管理ポートの IP アドレスを使用してください。 http://(IP アドレス)/ または https://(IP アドレス)/
内蔵 CLI	SSH ターミナルソフトウェアから、CTL1 の管理ポートの IP アドレスを指定して、内蔵 CLI にログインしてください。CTL1 に障害が発生してエラーとなる場合は、CTL2 管理ポートの IP アドレスを使用してください。 Host Name (IP アドレス) Port (20522)
RAID Manager	アプリケーションを起動する際にストレージ装置と通信が行われます。 アプリケーションのインストールに関しては、『RAID Manager インストール・設定ガイド』を、アプリケーションの起動に関しては、『RAID Manager ユーザガイド』を参照してください。

1.5.6　HA Storage Advisor Embedded 利用の構成の注意事項

プール運用が前提の構成において利用してください

HA Storage Advisor Embedded を利用する場合、ボリュームは必ずプールから切り出して作成されます。CLI 等を用いて、パリティグループや、パリティグループから生成されるネイティブボリュームを使用すると、HA Storage Advisor Embedded では管理できなくなります。

iStorage V10e では暗号化ボリュームの作成に制限があります

iStorage V10e では、HA Storage Advisor Embedded で暗号化されたボリュームを作成できません。暗号化されたボリュームを作成したい場合は、REST API を使用してボリュームを作成

してください。詳細は『REST API リファレンスガイド』を参照してください。なお、iStorage V100, V300 では、暗号化されたボリュームを作成できます。

コピー系の機能の操作とトラブルシューティング

Snapshot は、HA Storage Advisor Embedded で操作できます。トラブルシューティングにも対応しています。

以下のコピー系の機能は、HA Storage Advisor Embedded で操作できません。操作とトラブルシューティングは、RAID Manager または Storage Navigator を利用してください。

- Local Replication
- Synchronous Replication
- Asynchronous Replication
- Active Mirror

1.5.7　HA Storage Advisor Embedded でソフトウェアを利用する場合の注意事項

HA Storage Advisor Embedded で各ソフトウェアを利用する際の注意事項について説明します。次の表中に記載する HA Storage Advisor Embedded で操作できない項目を利用したい場合は、RAID Manager、または SVP を用意して Storage Navigator で実施してください。

表 1-2　HA Storage Advisor Embedded でソフトウェアを利用する場合の注意事項

プログラムプロダクト	サポート状況
dedupe and compression	HA Storage Advisor Embedded で利用できます。詳細な管理は RAID Manager を利用してください。
LUN Manager Software	HA Storage Advisor Embedded ではサーバモデルを使用して利用できます。詳細な設定を実施したい場合は RAID Manager を利用してください。 VLAN によるセグメント分割にストレージを対応させる場合は、あらかじめ RAID Manager を使用して仮想ポートを作成しておくことで、その後のボリューム管理等は HA Storage Advisor Embedded で行えます。 また、iSCSI サーバの CHAP 認証を利用したい場合は RAID Manager または Storage Navigator を利用してください。
Dynamic Provisioning Software	HA Storage Advisor Embedded で利用できます。プールを縮小される際は RAID Manager を利用してください。
Dynamic Tiering Software	Dynamic Tiering プールの作成・削除・参照は HA Storage Advisor Embedded で操作できます。詳細な設定等は RAID Manager または Storage Navigator を利用してください。
Snapshot Software	HA Storage Advisor Embedded で利用できます。定期的な運用、コンシステンシーグループの設定は、RAID Manager を利用してください。HA Storage Advisor Embedded で構成定義したオブジェクトも扱えます。 ただし Snapshot を Snapshot Pool を用いて設定する場合は、RAID Manager または Storage Navigator を利用してください。
Performance Monitor Software	使用する場合は SVP が必要になります。モニタリング対象には HA Storage Advisor Embedded 管理のオブジェクトも含まれます。

プログラムプロダクト	サポート状況
Server Priority Manager Software	RAID Manager を利用してください。HA Storage Advisor Embedded で構成定義するポートも扱えます。
SNMP Agent Software	Maintenance Utility を利用してください。HA Storage Advisor Embedded で構成定義するオブジェクトの障害も、SNMP により通知されます。
Data Retention Utility	RAID Manager を利用してください。HA Storage Advisor Embedded で構成定義するオブジェクトも扱えます。
Virtual Partition Manager Software	RAID Manager を利用してください。HA Storage Advisor Embedded で構成定義するオブジェクトも扱えます。
Realtime Tiering	RAID Manager を利用してください。HA Storage Advisor Embedded で構成定義するオブジェクトも扱えます。
Local Replication Software	RAID Manager を利用してください。Storage Navigator との併用を推奨します。HA Storage Advisor Embedded で構成定義したオブジェクトも扱えます。
Synchronous Replication Software	RAID Manager を利用してください。Storage Navigator との併用を推奨します。HA Storage Advisor Embedded で構成定義したオブジェクトも扱えます。
Asynchronous Replication Software	RAID Manager を利用してください。Storage Navigator との併用を推奨します。HA Storage Advisor Embedded で構成定義したオブジェクトも扱えます。
Volume Shredder Software	RAID Manager を利用してください。HA Storage Advisor Embedded で構成定義したオブジェクトも扱えます。
Open Volume Management Software	プールから作成されるボリュームの管理は、HA Storage Advisor Embedded で管理できます。パリティグループから作成されるボリュームの管理には RAID Manager または Storage Navigator を利用してください。
Universal Volume Manager Software	RAID Manager または Storage Navigator を利用してください。
Resource Partition Manager Software※1	HA Storage Advisor Embedded で作成したリソースは、すべて meta_resource に割り当てられます。リソースグループでリソース管理をしたい場合は RAID Manager、または Storage Navigator を利用してください。
Active Mirror	RAID Manager を利用してください。
Encryption License Key	REST API で利用できます。iStorage V100, V300 は、HA Storage Advisor Embedded で暗号化されたプールを作成できます。

注※1

仮想ストレージマシンを利用する場合は、RAID Manager または Storage Navigator で設定・管理を行ってください。 HA Storage Advisor Embedded は、仮想 ID による操作をサポートしていないため、仮想ストレージマシン上のリソースの管理はできません。

1.5.8　ストレージシステムのボリュームをサーバに割り当てるための設定

HA Storage Advisor Embedded を使用する場合、ストレージシステムのボリュームをサーバに割り当てるために、サーバのオブジェクトを作成します。一方、RAID Manager や Storage Navigator を使用する場合、ホストグループ/iSCSI ターゲットを作成します。

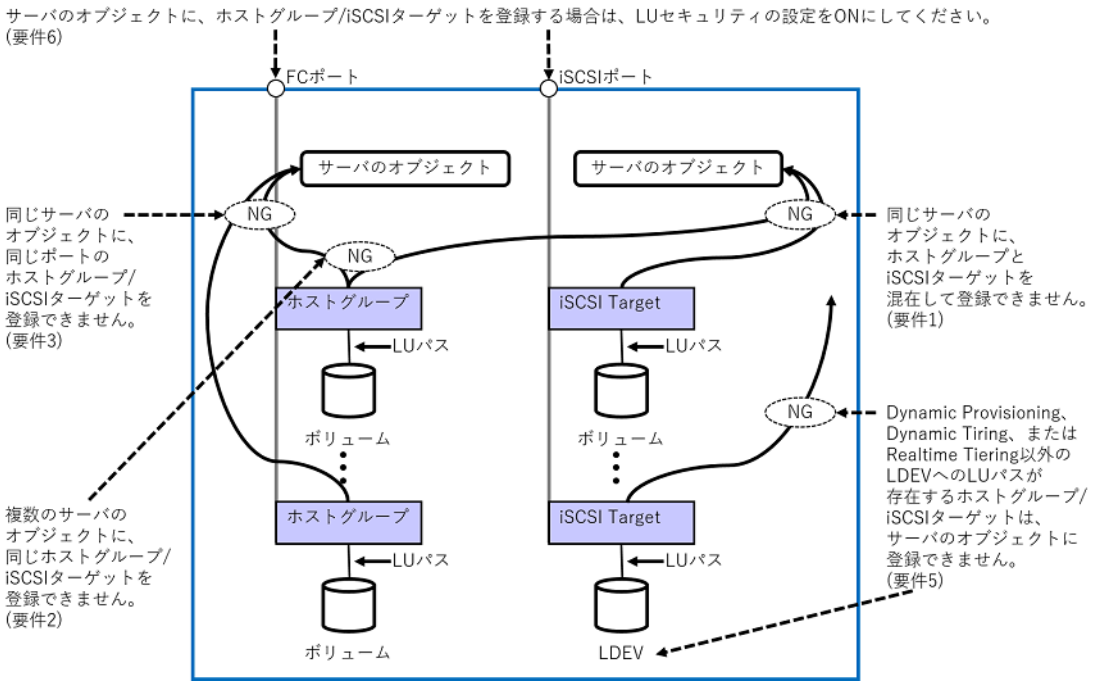
RAID Manager には、ホストグループ/iSCSI ターゲットをサーバのオブジェクトに反映させるコマンドが用意されています。

1.5.8.1　サーバからホストグループ/iSCSI ターゲットを管理するための要件

HA Storage Advisor Embedded が管理しているサーバのオブジェクト（以下、サーバのオブジェクト）から、ホストグループ/iSCSI ターゲットを管理するためには、以下の要件を満たす必要があります。

表 1-3　サーバからホストグループ/iSCSI ターゲットを管理するための要件

No.	要件
1	1 つのサーバのオブジェクトには、ホストグループ、または iSCSI ターゲットのどちらか一方を登録します。Fibre Channel と iSCSI の HBA の両方が実装されているホストを、サーバのオブジェクトとして管理する場合は、Fibre Channel 用のサーバのオブジェクトと、iSCSI 用のサーバのオブジェクトを作成してください。（下図の要件 1 を参照）
2	複数のサーバのオブジェクトに、同じホストグループ/iSCSI ターゲットを登録できません。ホストグループ/iSCSI ターゲットは、1 つのサーバのオブジェクトに登録して管理してください。（下図の要件 2 を参照）
3	同じサーバのオブジェクトに、同じポートのホストグループ/iSCSI ターゲットを登録できません。同じポートに複数のホストグループ/iSCSI ターゲットが存在する場合は、それぞれのホストグループ/iSCSI ターゲットに対してサーバのオブジェクト作成してください。（下図の要件 3 を参照）
4	サーバのオブジェクトに登録できるホストの WWN、または、iSCSI Name は 32 個までです。それ以上の HBA が実装されているホストを、サーバのオブジェクトとして管理する場合は、1 台のホストに対して複数のサーバのオブジェクトを作成してください。
5	Dynamic Provisioning、Dynamic Tiering、または Realtime Tiering 以外の LDEV への LU パスが存在するホストグループ/iSCSI ターゲットは、サーバのオブジェクトに登録できません。（下図の要件 5 を参照）
6	サーバのオブジェクトに、ホストグループ/iSCSI ターゲットを登録する場合は、 LU セキュリティの設定を ON にしてください。（下図の要件 6 を参照）
7	サーバのオブジェクトに、ID が 0 のホストグループ/iSCSI ターゲットを登録できません。ID が 0 以外のホストグループ/iSCSI ターゲットを使用してください。
8	仮想ストレージマシンに割り当てられたホストグループ/iSCSI ターゲットは、サーバのオブジェクトに登録できません。



1.5.8.2　サーバからホストグループ/iSCSI ターゲットを管理する場合の運用

サーバのオブジェクトを使用して、ホストグループ/iSCSI ターゲットを管理する場合の運用に関する項目を示します。

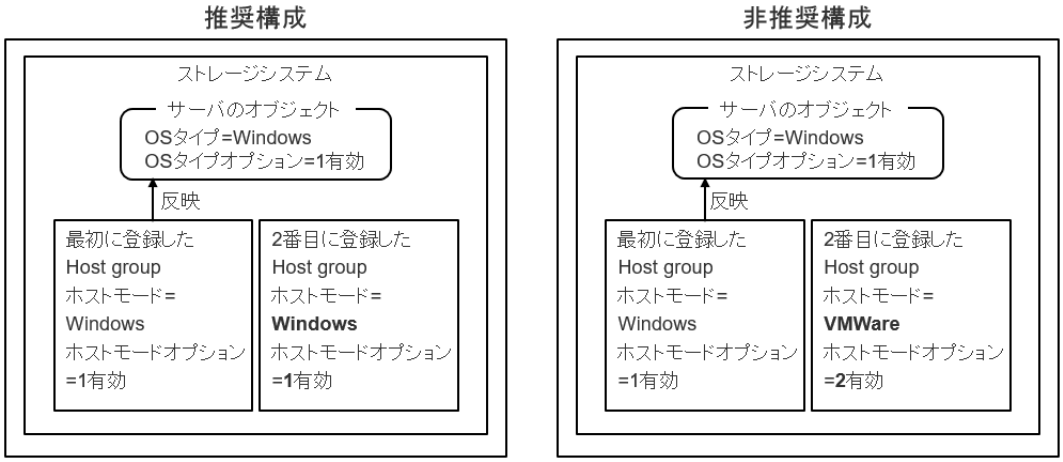
サーバのオブジェクトに、複数のホストグループ/iSCSI ターゲットを登録する場合、そのホストモード及びホストモードオプションを同一に設定することを推奨します。サーバのオブジェクトに登録されたホストグループ/iSCSI ターゲットは、raidcom get host_grp -key server コマンドで確認できます。

raidcom add server コマンドで作成したサーバのオブジェクトにホストグループ/iSCSI ターゲットを登録する場合、最初に登録したホストグループ/iSCSI ターゲットの、ホストモード及びホストモードオプションが、サーバのオブジェクトの OS タイプ及び OS タイプオプションに反映されます。次に登録したホストグループ/iSCSI ターゲットの、ホストモード及びホストモードオプションが、最初に登録したホストグループ/iSCSI ターゲットのホストモード及びホストモードオプションと異なると、サーバのオブジェクトの OS タイプまたは、OS タイプオプションと、ホストグループ/iSCSI ターゲットのホストモード及びホストモードオプションとの間に差異が生じるため管理が複雑になります。

サーバのオブジェクトの OS タイプ及び OS タイプオプションと、ホストグループ/iSCSI ターゲットのホストモード及びホストモードオプションとの間に設定の差異がある場合の挙動は以下の通りです。

- HA Storage Advisor Embedded で接続情報を追加すると、サーバのオブジェクトの OS タイプ及び OS タイプオプションと一致するホストグループ及びホストモードオプションが設定されたホストグループ/iSCSI ターゲットが、指定したポートに自動的に作成されます。

- HA Storage Advisor Embedded で OS タイプまたは OS タイプオプションの設定を変更すると、サーバのオブジェクトに登録されたすべてのホストグループ/iSCSI ターゲットに変更内容が反映されます。このためホストグループ/iSCSI ターゲット毎に異なるホストモード及びホストモードオプションを設定することはできません。



1.6　Storage Navigator を利用して管理する構成

1.6.1　構成概要

ストレージシステムを構築、運用、および管理するためのサーバが必要です。この管理サーバを SVP（SuperVisor PC）と呼びます。

- SVP は、お客様の LAN を介して、ストレージシステムにアクセスします。
- SVP のハードウェアは、「1.6.2　管理サーバ（SVP）の要件（19 ページ）」を満たしてください。
- SVP には、「1.6.4　ストレージシステムを利用するために必要なソフトウェア（27 ページ）」に示すストレージ管理ソフトウェア、および SVP ソフトウェアをインストールしてください。

SVP で動作する Storage Navigator には、管理クライアントから接続します。管理クライアントには SVP と同じコンピュータを使用することもできます。

本書は、「付録 A.　初期設定作業（178 ページ）」に示す作業をする際に、SVP を直接操作する前提で記述しています。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、ストレージシステムと SVP のネットワーク設定、SVP の初期設定、および SVP で動作するソフトウェアのインストールを行うこともできます。リモートデスクトップ接続を行う場合は、「付録 K.　管理クライアントから SVP への接続方法（409 ページ）」を参照してください。また、SVP に DVD ドライブが搭載されていない場

合は、リモートデスクトップ接続のオプションにより管理クライアントの DVD ドライブを使用します。

⚠ 注意

- iStorage V10e の場合、1 台の SVP で最大 8 台のストレージシステムを管理できますが、1 台のストレージシステムを、複数台の SVP で管理できません。必ず 1 台の SVP で管理してください。
- SVP は、クラスターソフトウェアによる冗長化に対応していません。
- SVP を新しいプラットフォームに移行する場合は、必ず移行前の SVP のサービスを停止した後に、移行作業を行ってください。

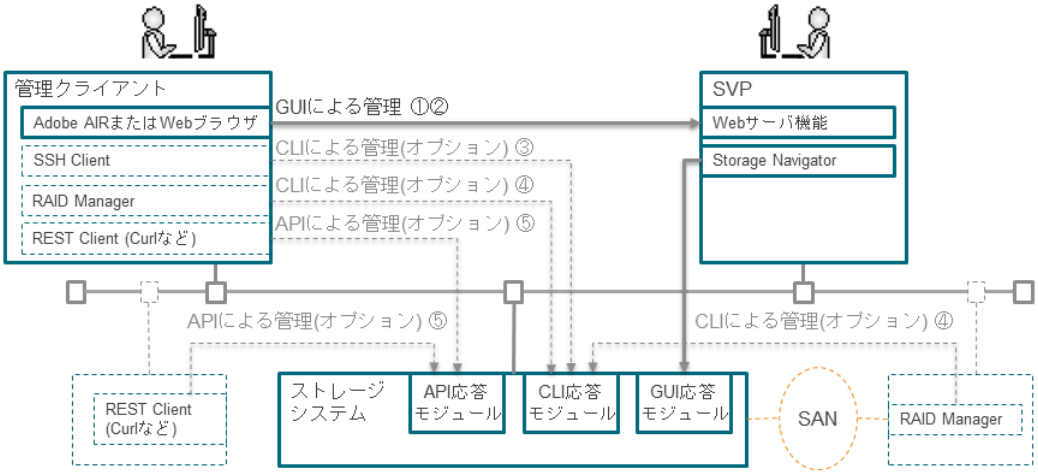


図 1-2　Storage Navigator 利用の構成

表 1-4　Storage Navigator 利用の場合の管理インターフェース

No	管理インターフェース	インストール先	管理ツール	主な用途
1	GUI	ストレージシステムに組み込み済	Maintenance Utility	ストレージシステムのハードウェアの基本設定
2		SVP	Storage Navigator	• 構成設定操作 • レプリケーション操作
3	CLI	ストレージシステムに組み込み済	内蔵 CLI※1	構成設定操作
4		外部サーバ※2	RAID Manager	• 構成設定操作 • レプリケーション操作
5	API	ストレージシステムに組み込み済	REST API	• 構成設定操作 • レプリケーション操作※3

注※1

内蔵 CLI は RAID Manager のサブセットです。raidcom ではじまるコマンドが使用できます。

制限情報については、『RAID Manager ユーザガイド』を参照してください。

注※2

ストレージシステムの管理ポートが接続されている LAN の同一セグメントに接続されているプラットフォームである必要があります。プラットフォーム条件は、『RAID Manager インストール・設定ガイド』を参照してください。

注※3

実行できないレプリケーション操作が一部あります。実行可能な API の詳細は、『REST API リファレンスガイド』を参照してください。

1.6.2　管理サーバ（SVP）の要件

SVP としてご用意いただくプラットフォームの要件を示します。

1.6.2.1　SVP のハードウェア条件

表 1-5　SVP のハードウェア条件

項目	仕様
プロセッサ（CPU）	• Windows 11、Windows Server 2022 2.1GHz 以上で 2 コア以上の 64 ビット互換プロセッサ※2 推奨：2.1GHz 以上で 4 コア以上の 64 ビット互換プロセッサ※2 • Windows 11、Windows Server 2022 以外 Celeron P4505 1.87GHz（2Core）相当以上※1※2 推奨：Celeron G1820 2.7GHz（2Core）相当以上※2
メモリ（RAM）	• iStorage V100, V300 2.9GB ＋ OS や他のアプリケーションが使用するメモリ※3 • iStorage V10e 1GB ＋ 1.5GB×管理するストレージシステムの台数 ＋ OS や他のアプリケーションが使用するメモリ※3
HDD または SSD	120GB 以上※4
ネットワークカード（LAN）	1 ポート（1000Base-T）※5
電源	冗長電源を推奨
ディスプレイ	True Color 32bit 以上 解像度：1280×1024 ピクセル以上※6
DVD ドライブ	1 台※6
キーボードとマウス	1 セット※6

注※1

CPU ベンダ、およびプロセッサ・ファミリには依存しません。

注※2

iStorage V10e の場合、1 台の SVP に最大 8 台のストレージシステムを登録できます。

1 台の SVP に登録されている複数のストレージシステムを同時に起動する場合は、1 台のストレージシステムにつき 1 Core 分の CPU が必要です。Hyper Thread 対応の CPU であれば、1Thread 分必要となります。

注※3

SVP に必要なメモリ容量は、OS の種類、および管理するストレージシステムの台数により異なります。

Microsoft 社が公開しているシステム要件を参照して、OS の動作に必要な最小メモリ容量を確認してください。

以下に例を示します。

OS	OS の動作に必要な最小メモリ容量
Windows 11（64bit 版）	4GB
Windows 10（64bit 版）	2GB
Windows Server 2022（デスクトップ エクスペリエンス搭載サーバー オプションを使用）	2GB
Windows Server 2019（デスクトップ エクスペリエンス搭載サーバー オプションを使用）	2GB
Windows Server 2016	512MB
Windows Server 2016（デスクトップ エクスペリエンス搭載サーバー オプションを使用）	2GB

注※4

1 台のストレージシステムを管理するために必要な HDD 容量です。

複数台のストレージシステムを同時に管理する場合に必要な HDD 容量は、次のとおりです。

必要な HDD 容量＝ 100GB（基本）＋ 20GB×管理するストレージシステムの台数

基本には、OS が使用する HDD 容量を含みません。

例：3 台のストレージシステムを管理する場合

必要な HDD 容量＝ 100GB（基本）＋ 20GB×3 ＝ 160GB

SVP に複数のストレージシステムを登録する場合、ストレージシステムを管理するためのソフトウェア（ストレージ管理ソフトウェア、および SVP ソフトウェア）を、システムドライブ（Windows がインストールされているドライブ）とは別のドライブにインストールすることを推奨します。

注※5

管理 LAN と保守 LAN を分離して運用する場合等、複数 LAN 環境で運用する場合は、別途必要な数のポートを準備してください。

SVP は、管理対象としているストレージシステムから下記のモニタデータを受信し、HDD または SSD に格納します。

- PerformanceMonitor データ：約 400KB/モニタ間隔

  （モニタ間隔は 1 分から 15 分までの時間を 1 分単位で指定可）

転送速度が上記より下回ると、SVP の処理時間に遅延が生じる可能性があります。モニタデータを上回る転送速度のネットワーク環境に接続してください。

注※6

管理クライアントから SVP にリモートデスクトップ接続して、ストレージシステムと SVP のネットワーク設定、SVP の初期設定、および SVP で動作するソフトウェアのインストールを行う場合は不要です。

関連リンク

参照先トピック

ストレージシステムを利用するために必要なソフトウェア（27 ページ）

1.6.2.2　管理サーバ（SVP）に必要なソフトウェア

SVP からストレージシステムを管理するために、ストレージ管理ソフトウェア、および SVP ソフトウェアをインストールしてください。インストールには本製品に同梱された SVP ファームウェアメディア（メディア名称「装置添付ソフトウェア １／２」）を使用します。

ストレージ管理ソフトウェア、および SVP ソフトウェアのサポート言語は英語と日本語です。既定のシステム UI 言語が、日本語、または英語の Windows のみ使用できます。なお、既定のシステム UI 言語が日本語の場合、ロケールを英語に変更できます。また、既定のシステム UI 言語が英語の場合、ロケールを日本語に変更できます（「A.5.2　管理サーバ（SVP）にロケールを設定する（188 ページ）」を参照）。

ストレージ管理ソフトウェア、および SVP ソフトウェアを使用するには、管理者権限を持ったユーザアカウントでログインした状態で、SVP を稼働させる必要があります。

ベンダーのサポート期間内のソフトウェア（OS を含む）を使用してください。サポート期間を過ぎているソフトウェアでの動作は保証できません。

表 1-6　SVP に必要なソフトウェア

項目	仕様
SVP の OS	＜ OS ＞ • Windows 10 Professional/Enterprise （64bit 版）※1、※3 • Windows 11 Professional/Enterprise※1、※3、※4、※7

項目	仕様
	• Windows Server 2016（デスクトップエクスペリエンス搭載サーバ）（64bit 版）※2、※3 • Windows Server 2019（デスクトップエクスペリエンス搭載サーバ）（64bit 版）※2、※3 • Windows Server 2022（デスクトップエクスペリエンス搭載サーバ）（64bit 版）※2、※3、※5 ＜仮想化ソフトウェア（SVP が仮想マシンの場合）※6 ＞ • VMware ESXi 7.0 • VMware ESXi 8.0 • Windows Server 2016 Hyper-V • Windows Server 2019 Hyper-V • Windows Server 2022 Hyper-V
Storage Navigator と一緒にインストールされるサードパーティーのソフトウェア	• Java • Java（Client） • Strawberry Perl • Apache • Jetty • OpenSSL • PuTTY（ssh2 対応）

注※1

- SVP の OS が Windows 10/11 Professional または Windows 10/11 Enterprise の場合、管理クライアントは SVP と同じコンピュータを使用してください。

  1 台のコンピュータを仮想化ソフトウェアにより、複数の仮想マシンとして使用する場合も同様です。SVP の OS が Windows 10/11 Professional または Windows 10/11 Enterprise であれば管理クライアントは SVP と同じ仮想マシンを使用してください。

- Windows のコマンドプロンプトの画面上で、不要なマウス操作を行わないでください。コマンドプロンプトから実行した処理が途中で停止してしまい、プロンプトが返ってこない事象が報告されています。

- SVP の OS を Windows 10 Professional/Enterprise から、Windows 11 Professional/Enterprise に更新した場合は、再度、デスクトップヒープの指定値を変更してください（設定方法は「A.8　デスクトップヒープの指定値を変更する（206 ページ）」を参照）。

注※2

これらの OS の SVP では、管理クライアントとして Storage Navigator 画面によるストレージシステムの操作ができません。このため、SVP を管理クライアントとして兼用できません。これらの OS の SVP を使用する場合は、別の管理クライアント用コンピュータが必要です。

注※3

既定のシステム UI 言語が、日本語、または英語の Windows のみ使用できます。なお、既定のシステム UI 言語が日本語の場合、ロケールを英語に変更できます。また、既定のシステム UI 言語が英語の場合、ロケールを日本語に変更できます。

注※4

Windows 11 は、次の SVP ソフトウェアバージョンでサポートします。

- iStorage V100, V300 の場合：93-06-81-XX/XX 以降
- iStorage V10e の場合：全バージョン

注※5

- Windows Server 2022 は、次の DKCMAIN ファームウェアバージョンでサポートします。
  - iStorage V100, V300 の場合：93-06-83-XX/00 以降
  - iStorage V10e の場合：88-08-11-XX/00 以降
- SVP の OS を Windows Server 2016 または Windows Server 2019 から、Windows Server 2022 に更新した場合は、再度、デスクトップヒープの指定値を変更してください。設定方法は「A.8　デスクトップヒープの指定値を変更する（206 ページ）」を参照してください。

注※6

仮想化ソフトウェアと SVP の OS の組み合わせには制限があります。サポートしている組み合わせの詳細は、PP サポートサービスで提供している OS サポート情報を参照してください。

注※7

Windows11 バージョン 24H2 以降の場合、初期の状態では WMIC（Windows Management Instrumentation Command line）機能はありません。

一方、次に示す SVP ソフトウェアの Storage Navigator は、WMIC 機能を使用するため、SVP に WMIC 機能を追加する必要があります。

- iStorage V100, V300 の場合：93-07-25-XX/XX 以前
- iStorage V10e の場合：88-08-17-XX/XX 以前

なお、1 台の SVP で複数のストレージシステムを管理する場合、ストレージシステムごとに Storage Navigator をインストールします。いずれかの Storage Navigator が、上記の SVP ソフトウェアバージョンに該当する場合は、WMIC 機能を追加してください。

WMIC 機能を追加する操作手順の詳細は「A.5.3　管理サーバ（SVP）に WMIC 機能を追加する（190 ページ）」を参照してください。

メモ

- サポートしている OS の最新情報は、PP サポートサービスで提供しています。
- ストレージ管理ソフトウェアと一緒にインストールされるサードパーティーのソフトウェアは、ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリ（デフォルトは、「C:\Mapp」）にインストールされます。このため、お客様がすでにこれらのソフトウェアを、SVP の C:\Program Files にインストールされていても上書きされません。
- Java と、Java（Client）は使われ方が異なります。Java は SVP ソフトウェアの内部処理で使われます。内部処理用のため、Windows のコントロールパネル等には表示されません。Java（Client）はブラウザが Storage Navigator や Maintenance Utility を表示する際に使われます。
- SVP に環境変数の_JAVA_OPTIONS を設定しないでください。SVP が正常に起動しなくなる可能性があります。
- SVP には、ストレージ管理ソフトウェア、および SVP ソフトウェアのほかに以下のソフトウェアをインストールすることができます。
  - HA Device Manager
  - HA Replication Manager（Application Agent）
  - iStorage Performance Navigator
  - ESMPRO/ServerManager
  - ESMPRO/ServerAgent
  - ESMPRO/AutomaticRunningController
  - ESMPRO/AC
  - WebSAM AlertManager（旧 ESMPRO/AlertManager）
  - WebSAM JobCenter
  - WebSAM JobCenter Lite
  - WebSAM iStorageManager
  - WebSAM SigmaSystemCenter
  - WebSAM SystemManager G Agent
  - NetBackup
  - ArcServe Backup
  - Veeam Backup & Replication
  - Backup Exec
  - ウィルス検出プログラム

関連リンク

参照先トピック

ストレージシステムを利用するために必要なソフトウェア（27 ページ）

1.6.2.3　管理サーバ（SVP）の電源 ON/OFF に関する注意事項

iStorage V100, V300 のストレージシステムは、SVP を常時監視しています。ストレージシステムが SVP と 15 分間連続して通信できない場合、ストレージシステムは GUM-SVP 間通信障害（7d0cxx）を通知します。そのため、iStorage V100, V300 を管理している SVP には、電源 ON と OFF に関する制約があります。

電源 ON に関する制約

SVP を電源 ON にした後、装置の電源を ON にする。または、装置の電源を ON にした後、15 分以内に SVP の電源を ON にすること。

電源 OFF に関する制約

装置の電源を OFF にした後、SVP の電源を OFF にする。または、SVP の電源を OFF にした後、15 分以内に装置の電源を OFF にすること。

1.6.2.4　IP アドレスを変更する場合の注意事項

iStorage V100, V300 のストレージシステムまたは iStorage V100, V300 を管理している SVP の IP アドレスの変更により、ストレージシステムが SVP と 15 分間連続して通信できない場合、ストレージシステムは GUM-SVP 間通信障害（7d0cxx）を通知します。

1.6.3　管理するための PC（管理クライアント）要件

管理クライアントは、LAN 経由で SVP を操作するための PC です。

1.6.3.1　ストレージシステムを管理するための PC（管理クライアント）

下記のハードウェア条件を満たす PC を準備してください。

表 1-7　管理クライアントのハードウェア条件

項目	仕様
プロセッサ（CPU）	• Windows 11 2.1GHz 以上で 2 コア以上の 64 ビット互換プロセッサ 推奨：2.1GHz 以上で 4 コア以上の 64 ビット互換プロセッサ • Windows 11 以外 Pentium 4 640 3.2GHz 相当以上※ 推奨：Core 2 Duo E6540 2.33GHz 相当以上
メモリ（RAM）	• Windows 11 8GB 以上 推奨：16GB 以上 • Windows 11 以外

項目	仕様
	2GB 以上 推奨：3GB 以上
HDD または SSD の空き容量	500MB ＋(80MB×ストレージシステム)以上 Storage Navigator を使用する場合は、500MB に加えて、Storage Navigator による管理対象のストレージシステムごとに 80MB の空き容量が必要です。
ディスプレイ	True Color 32bit 以上 解像度：1280×1024 ピクセル以上
DVD ドライブ	必須
キーボードとマウス	必須
ネットワークカード（LAN）	100Base-TX/1000Base-T

注※

CPU ベンダ、およびプロセッサ・ファミリには依存しません。

1.6.3.2　管理クライアントを利用するために必要なソフトウェア

管理クライアントの OS には、Windows が使用できます。Windows OS でのソフトウェア要件を示します。

SVP にインストールするストレージ管理ソフトウェア、および SVP ソフトウェアのサポート言語は英語と日本語です。このため管理クライアントのロケールも英語、または日本語のどちらかに設定してください（「A.2.2　管理クライアントにロケールを設定する（181 ページ）」を参照）。

Storage Navigator を使用するには次に示す OS が必要です。OS 以外の Storage Navigator の前提ソフトウェアは Adobe AIR 環境にバンドルされます。また、Maintenance Utility やストレージシステム構成情報のレポート表示などに Web ブラウザが必要です。

ベンダーのサポート期間内のソフトウェア（OS を含む）を使用してください。サポート期間を過ぎているソフトウェアでの動作は保証できません。

項目	仕様
OS	• Windows 10（64bit）※1 • Windows 11※1、※3、※5
Web ブラウザ	• Windows 10 の場合 　- Microsoft Edge※2、※4 　- Google Chrome • Windows 11 の場合 　- Microsoft Edge※4 　- Google Chrome

注※1

SVP の OS が Windows 10/11 Professional または Windows 10/11 Enterprise の場合、管理クライアントは SVP と同じコンピュータを使用してください。

注※2

Microsoft Edge は、次の SVP ソフトウェアバージョンでサポートします。

- iStorage V100, V300 の場合：93-05-21-XX/XX 以降
- iStorage V10e の場合：全バージョン

注※3

Windows 11 は、次の SVP ソフトウェアバージョンでサポートします。

- iStorage V100, V300 の場合：93-06-81-XX/XX 以降
- iStorage V10e の場合：全バージョン

注※4

Microsoft Edge の Internet Explorer モード（IE モード）はサポートしていません。

注※5

Windows11 バージョン 24H2 以降の場合、初期の状態では WMIC（Windows Management Instrumentation Command line）機能はありません。

一方、次に示す SVP ソフトウェアの Storage Navigator は、WMIC 機能を使用するため、管理クライアントに WMIC 機能を追加する必要があります。

- iStorage V100, V300 の場合：93-07-25-XX/XX 以前
- iStorage V10e の場合：88-08-17-XX/XX 以前

WMIC 機能を追加する操作手順の詳細は「A.2.3　管理クライアントに WMIC 機能を追加する（181 ページ）」を参照してください。

メモ

サポートしている OS の最新情報は、PP サポートサービスで提供しています。

1.6.4　ストレージシステムを利用するために必要なソフトウェア

ストレージシステムの管理と運用は、専用の管理ソフトウェア（以下、管理 GUI）から行います。

管理 GUI は、GUI（Graphical User Interface）上で操作を行います。

以下、本書に関連するソフトウェアを示します。

プラットフォーム	分類	名称	主な機能
SVP にインストールするソフトウェア	ストレージ管理ソフトウェア（1 台の SVP に 1 セットインストール）	Storage Device List	• ストレージシステムを SVP に登録、表示、選択するための GUI を提供
		RAID Manager※1	• レプリケーション機能の操作 • ペア状態の表示 • 外部プログラムへのアクセスに使用
		OSS	• Storage Device List、RAID Manager などのソフトウェアが使用するオープンソースのプログラム
		Web Console Launcher	• HA Device Manager - Storage Navigator のサブ画面を表示
		Storage Device Launcher	• Adobe AIR 環境で動作する Storage Navigator の起動
	SVP ソフトウェア（SVP の管理対象となるストレージシステムの台数分インストール）	HA Device Manager - Storage Navigator※2	• ストレージシステムのハードウェア管理（構成情報の設定、論理デバイスの定義、ステータス表示） • 性能管理（チューニング） • ファームウェアとの情報授受
管理クライアントにインストールするソフトウェア	管理 GUI アクセス用のソフトウェア	OSS	• ストレージ管理ソフトウェア、SVP ソフトウェア、およびファームウェアの GUI 操作に使用するオープンソースのプログラム
		Web Console Launcher	• HA Device Manager - Storage Navigator のサブ画面を表示
		Storage Device Launcher	• Adobe AIR 環境で動作する Storage Navigator の起動
ストレージシステムに組み込まれているソフトウェア	ファームウェア	Maintenance Utility※3	• ストレージシステムのハードウェアの基本設定 • 障害監視、部品交換

注※1

本書では RAID Manager の操作方法は対象外ですが、インストールに関連する記述はあります。

注※2

Storage Navigator で利用可能な機能は、内容ごとに複数のマニュアルで説明されています。

各機能とマニュアルの対応は、『ドキュメントマップ』を参照してください。

注※3

Maintenance Utility はコントローラシャーシに搭載されている GUM（Gateway for Unified Management）コントローラに組み込まれています。インストールの必要はありません。

GUM コントローラは冗長化されています。一方の GUM コントローラの Maintenance Utility の設定を変更すると、自動的に他方の GUM コントローラの Maintenance Utility にも反映されます。

なお、GUM はコントローラシャーシが通電されていれば動作するため、ストレージシステムが電源 OFF の状態でも Maintenance Utility にアクセスできます。

メモ

- 管理 GUI のメニューの説明は、画面内の?をクリックして表示されるヘルプメニューを参照してください。
- ヘルプの表示については、ブラウザの種類またはバージョンによって、表示の拡大/縮小の設定がヘルプウィンドウに反映されない場合があります。
- Storage Device List と SVP ソフトウェア（Storage Navigator）は、SVP にインストールして使用します。Storage Device List は SVP に 1 つだけインストールします。SVP ソフトウェアは Storage Device List に登録するイメージで、ストレージシステム毎にインストールします。

1.6.5　管理 LAN の要件

管理 LAN 内で通信するためには管理サーバ（SVP）、管理クライアント、管理 LAN へのファイアウォールに対して適切にポート番号を設定する必要があります。詳細は、「付録 A.　初期設定作業（178 ページ）」を参照してください。

1.6.6　特定機能を利用するために必要な SVP ソフトウェア

iStorage V100, V300 で、次の表に示すストレージシステムの機能を利用するには、対応したバージョンの SVP ソフトウェアが必要です。該当する機能を利用したい場合は、DKCMAIN ファームウェアだけでなく SVP ソフトウェアもアップデートしてください。

表 1-8　ストレージシステムの特定機能をサポートする SVP ソフトウェアバージョン

機能	DKCMAIN ファームウェア	SVP ソフトウェア
ドライブボックス（2.5 型 SAS、3.5 型 SAS）	93-05-21-XX/XX 以降	93-05-21-XX/XX 以降
2.5 型 SAS フラッシュドライブ（3.8TB、7.6TB、15TB）		
3.5 型ニアライン SAS ドライブ（14TB）		
Dynamic Tiering		
Realtime Tiering		
ドライブボックス（2.5 型 NVMe）	93-06-21-XX/XX 以降	93-06-21-XX/XX 以降
3.5 型ニアライン SAS ドライブ（18TB）		
SNMP Agent		

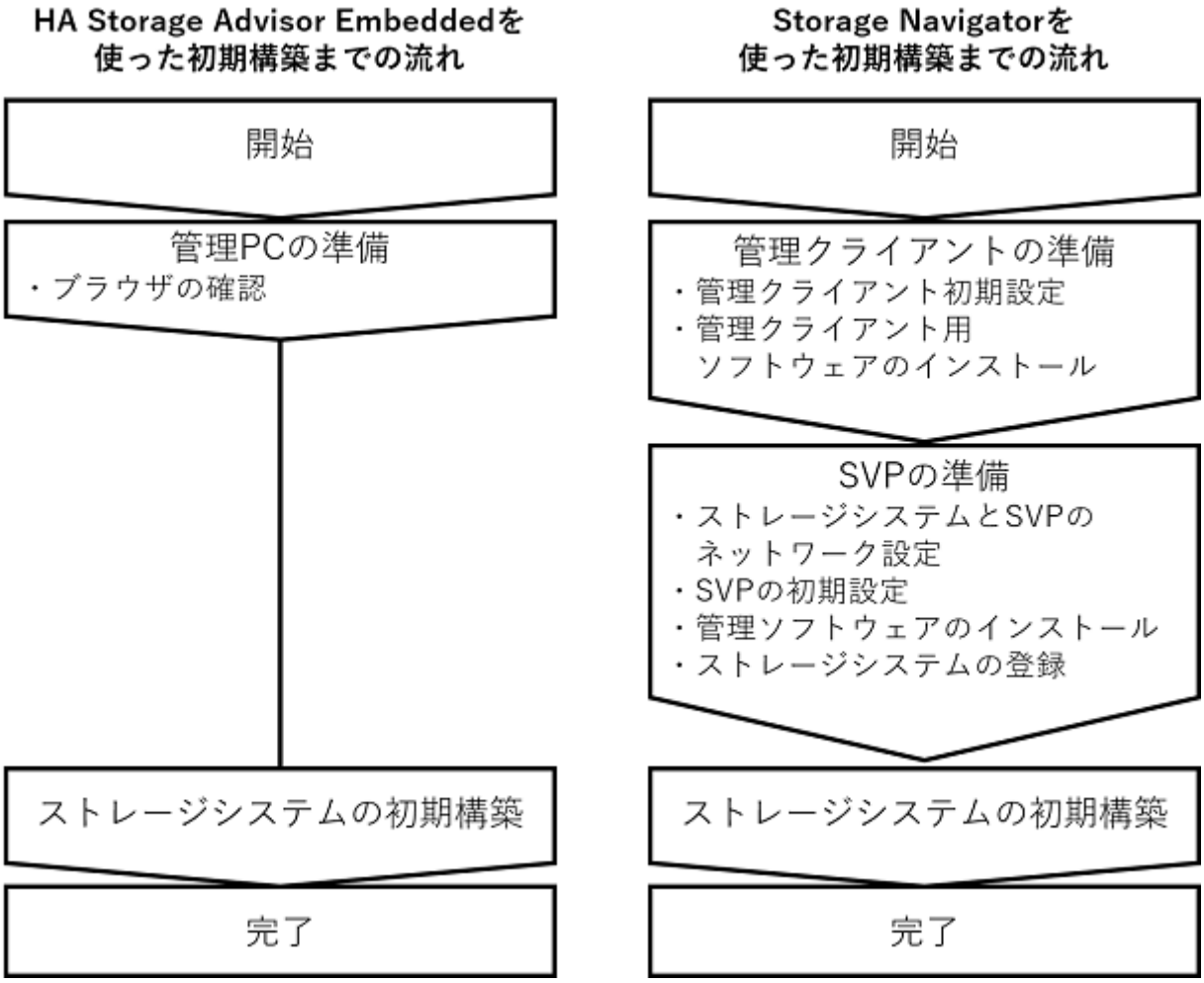
機能	DKCMAIN ファームウェア	SVP ソフトウェア
エクスプレス通報サービス		
Quality of Service（QoS）	93-06-81-XX/XX 以降	93-06-81-XX/XX 以降

第 2 章
初期構築の概要

2.1　初期構築までの流れ

HA Storage Advisor Embedded を利用するには、管理 PC を用意してストレージシステムにアクセスします。これにより簡単にストレージシステムの初期構築が行えます。ストレージシステムの管理ポートを設定した後の手順は、REST API でも初期構築ができます。詳細は『HA Storage Advisor Embedded ガイド』を参照ください。

Storage Navigator を利用するには、初めに管理クライアントと SVP を準備します。詳細は「付録 A.　初期設定作業（178 ページ）」を参照ください。その後、ストレージシステムの初期構築を行います。詳細は「付録 B.　初期構築作業（221 ページ）」を参照ください。



メモ

- SVP の障害に備え、SVP に設定されている IP アドレス、コンピュータ名、Windows アカウントなどの設定情報を、バックアップまたは記録してください。

- SVP ソフトウェア（Storage Navigator）には、各種の設定情報があります。この設定情報は、SVP を交換、あるいは SVP ソフトウェアを再インストールする際に、再度設定する必要があります。この状況に備えて、設定情報をバックアップしてください（「G.2.9　SVP のソフトウェア設定情報のバックアップとリストア（356 ページ）」を参照）。なお SVP で RAID Manager をご使用される場合は、RAID Manager の設定情報もバックアップしてください（『RAID Manager ユーザガイド』の「ユーザ作成ファイル（スクリプトファイル）」および「サービスとして RAID Manager を起動する（Windows システム）手順」を参照）。
- ストレージシステムの構成情報は、コントローラのシェアドメモリに保持されます。シェアドメモリは揮発性ですが、停電時などに備えストレージシステム内の不揮発メモリにも保持されます。しかし障害などにより構成情報が全て失われた場合、ストレージシステムの復旧が困難になる恐れがあります。このため、ストレージシステムの初期設定後、および構成変更後に、構成情報のバックアップをダウンロードして頂くことを推奨します。これにより構成情報をストレージの外部（管理 PC など）に保存することができます。

  バックアップの取得が必要となる構成変更は、ボリュームの作成と削除、パス定義の作成と削除、およびハードウェアの増減設です。バックアップされる構成情報は、ボリュームやパス定義など、Maintenance Utility 以外で設定する構成情報も含まれます。アラート通知などの管理に関する情報は含まれません。構成情報のバックアップ方法は「3.12.9　構成情報バックアップのダウンロード（95 ページ）」を参照願います。バックアップが取得できるようになるまで、1 時間程度かかります。バックアップの取得（ダウンロード）自体は、数分で終わります。障害復旧の際に、ダウンロードした構成情報を保守員にお渡し頂く場合がありますのでご承知おきください。
- 管理 PC とストレージシステム、管理クライアントと SVP、および SVP とストレージシステムの通信に SSL を適用する場合は、「付録 C.　SSL 通信の設定（245 ページ）」を参照願います。
- 各ソフトウェアのインストーラーや Windows のツール実行時に、ユーザーアカウント制御（UAC）画面（変更を許可するかどうかを確認する画面）が表示されることがあります。その場合は、変更を許可して先に進んでください。

⚠ 注意

現在設定されているシステム日時が実際の日時より進んでいる場合に、システム日時を修正すると、構成情報のバックアップが取得されない可能性があります。この事象が予想される場合は、既存のバックアップファイルを、別のフォルダに移動してください。

第 3 章
Maintenance Utility の機能

ストレージシステムの管理で使用する Maintenance Utility の操作手順について説明します。

Maintenance Utility へのログイン方法については、「1.5.5　各ツールのログイン方法（11 ページ）」を参照してください。

3.1　ファームウェア

3.1.1　ファームウェアバージョンの確認

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ファームウェア］を選択します。
3. ［DKCMAIN］欄にファームウェアバージョンが表示されます。

メモ

iStorage V100, V300 のファームウェアバージョンは 93-XX-XX-XX/XX です。

iStorage V10e のファームウェアバージョンは 88-XX-XX-XX/XX です。

3.1.2　ファームウェアの更新

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ファームウェア］を選択します。
3. ［更新］をクリックします。
4. セキュリティ警告画面が表示されます。［続行］をクリックします。
5. 完了メッセージが表示されます。［OK］をクリックします。

メモ

- ファームウェア更新画面を開く場合は、Web Console Launcher を設定した管理クライアントまたは SVP から Maintenance Utility に接続してください。

- ファームウェアの更新方法の詳細は、「G.2.1　セットアッププログラムを使用したストレージ管理ソフトウェア、SVP ソフトウェア、ファームウェアの更新（316 ページ）」を参照してください。
- ファームウェアの更新後に HA Storage Advisor Embedded をご使用する場合は、HA Storage Advisor Embedded を起動するブラウザのキャッシュをクリアしてください。

3.2　ユーザ管理

ストレージを管理するユーザを Maintenance Utility から設定する手順を説明します。

ストレージシステム導入時のビルトインアカウントについては、「1.5.5　各ツールのログイン方法（11 ページ）」を参照ください。

⚠ 注意

ユーザ管理に関する設定を行う場合、Maintenance Utility を、管理クライアントから IP アドレスを直接指定して起動するか、または HA Storage Advisor Embedded のメニューから起動してください。

Storage Navigator のメニューから Maintenance Utility を起動した場合、ユーザ管理に関する設定はできません。

3.2.1　ロール、リソースグループ、およびユーザグループの目的

ロール、リソースグループ、およびユーザグループは、ユーザがストレージシステムを操作できる項目と範囲を規定するための手法です。

3.2.2　ロール

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 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

ロール	操作できる項目
	• 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 • リモートコピーの操作全般
ストレージ管理者（プロビジョニング）	• キャッシュの設定 • パリティグループの作成 • 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 • 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 • Active Mirror で使用する Quorum ディスクの作成、削除 • Active Mirror ペアの作成および削除
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 • Active Mirror ペアの操作（作成および削除を除く）
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 • 管理クライアント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 • ファイバチャネル認証（FC-SP）の設定 • リソースグループの設定 • 仮想管理設定の編集 • Active Mirror の予約属性の設定
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

ロール	操作できる項目
保守（ベンダ専用）	• SVP に関する操作（通常保守員が実施する操作です）
保守（ユーザ）	• 装置状態の参照 • OS のセキュリティパッチインストール操作 • OSS のアップデート操作 • 簡易の保守操作

3.2.3　リソースグループ

リソースグループは、ストレージシステムのリソースに対してユーザが操作できる範囲を規定するためのグループです。リソースグループについての詳細は、『システム構築ガイド』を参照してください。

3.2.4　ユーザグループ

ユーザグループはロールとリソースグループを組み合わせたグループです。ユーザグループはビルトイングループとしてあらかじめ用意されています。ユーザグループは Storage Navigator で追加作成できます。

ユーザがストレージシステムを操作できる範囲は、ユーザーアカウントにユーザグループを割り当てることで規定します。ひとつのユーザーアカウントに複数のユーザグループを割り当てることもできます。

なお、ビルトイングループの Support Personnel は割り当てないでください。Support Personnel グループにはロールの「保守（ベンダ専用）」が含まれており、保守員が行う操作も許可されるため障害の要因となります。同様の理由により、ユーザグループを Storage Navigator で作成する場合も、ロールの「保守（ベンダ専用）」を割り当てないでください。

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

ビルトイングループ	ロール	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） • 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）	全リソースグループ

3.2.5　管理ツールとビルトイングループ

管理ツールのすべての項目を操作する場合、下記のビルトイングループを割り当てます。ただし保守員専用の項目は対象外です。

管理ツール	ビルトイングループ
Maintenance Utility	Administrator
	Maintenance User
HA Storage Advisor Embedded	Administrator
	Maintenance User
内蔵 CLI または RAID Manager	Administrator
エクスポートツール 2	Administrator
Storage Navigator	Administrator

管理ツール	ビルトイングループ
	Maintenance User
REST API	Administrator
	Maintenance User

3.2.6　ユーザグループを作成する場合の参考情報

管理ツールの操作項目ごとにロールが規定されています。ユーザグループの作成時に参考にしてください。

3.2.6.1　Maintenance Utility の操作に必要なロール

Maintenance Utility の操作に必要なロールを示します。

操作項目	必要なロール
ファームウェア更新	保守（ユーザ）
アラート通知設定	ストレージ管理者（初期設定）
ライセンスキー設定	ストレージ管理者（初期設定）
ネットワーク設定	ストレージ管理者（初期設定）
日時設定	ストレージ管理者（初期設定）
監査ログ設定	監査ログ管理者（参照・編集）
外部認証	セキュリティ管理者（参照・編集）
システムモニタ	iStorage V100, V300 の場合：不要 iStorage V10e の場合：保守（ユーザ）
初期設定	ストレージ管理者（初期設定）
ストレージシステム電源 ON	保守（ユーザ）
ストレージシステム電源 OFF	保守（ユーザ）
ログインメッセージ編集	ストレージ管理者（初期設定）
暗号化スイート選択	セキュリティ管理者（参照・編集）
証明書ファイル更新	セキュリティ管理者（参照・編集）
システムロック強制解除	ストレージ管理者（初期設定）
GUM リブート	保守（ユーザ）
システムダンプダウンロード	不要
スモールシステムダンプダウンロード	不要
構成情報バックアップダウンロード	保守（ユーザ）
ボリューム状態参照	保守（ユーザ）
ユーザ管理	セキュリティ管理者（参照・編集）
システム情報設定	ストレージ管理者（初期設定）
Locate LED の点灯/消灯	保守（ユーザ）
パスワード変更	不要
ユーザアカウントポリシーの設定	セキュリティ管理者（参照・編集）

操作項目	必要なロール
システムセーフモード起動	保守（ベンダ専用）
アラート表示	保守（ユーザ）
FRU に関するアラート表示	保守（ユーザ）

3.2.6.2　HA Storage Advisor Embedded の操作に必要なロール

HA Storage Advisor Embedded の操作に必要なロールを示します。

- 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）

  DKCMAIN ファームウェアバージョンが以下のバージョンの場合は必要です。

  - iStorage V100, V300 の場合：93-06-41-XX/XX 以降
  - iStorage V10e の場合：全バージョン
- ストレージ管理者（プロビジョニング）
- 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）
- セキュリティ管理者（参照・編集）

一部の操作（『HA Storage Advisor Embedded ガイド』の「Storage Advisor Embedded を使用するユーザのアカウントと権限」を参照）を実行する場合は、次のロールも必要になります。

- 保守（ユーザ）

3.2.6.3　内蔵 CLI の操作に必要なロール

- セキュリティ管理者（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）

3.2.6.4　RAID Manager の操作に必要なロール

- セキュリティ管理者（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）

3.2.6.5　エクスポートツール 2 の操作に必要なロール

ストレージ管理者（パフォーマンス管理）

3.2.7　ユーザ名とパスワードの文字数と使用可能文字

ユーザーアカウントとパスワードは使用する管理ツールにより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 • Storage Navigator	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 • RAID Manager	文字数	半角 63 文字以内
	使用可能文字※	半角英数字および下記の記号 - . @ _
• HA Storage Advisor Embedded • REST API	文字数	半角 63 文字以内
	使用可能文字	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 63 文字以内
	使用可能文字	半角英数字および下記の記号 ! # $ % & ' * + - . / = ? @ ^ _ ` { | } ~

注※

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 Linux の場合、スラッシュ（/）も指定できます。

パスワードの制限

管理ツール	制限※1	
• Maintenance Utility • Storage Navigator	文字数	半角 6～256 文字以内
	使用可能文字	半角英数字

管理ツール	制限※1	
		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 - . @ _ , :
• HA Storage Advisor Embedded • REST 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り異なります。

詳細は「3.2.8.2　ユーザアカウントのパスワードポリシー設定（44 ページ）」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 Linux 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。

3.2.8　ユーザアカウントポリシーの設定

次の GUM ファームウェア以降でユーザ認証に認証サーバを使用していない場合は、ユーザアカウントポリシーを設定できます。ユーザアカウントポリシーでは、ユーザのパスワードポリシーや、ログイン失敗時のアカウントのロックや無効化といったロックアウトポリシー、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先を設定できます。

ユーザアカウントポリシーのサポートバージョン

機種	バージョン
iStorage V100, V300	GUM ファームウェアバージョン 93-07-22/00 以降
iStorage V10e	GUM ファームウェアバージョン 88-08-15/00 以降

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（「3.2.10　パスワードの変更（55 ページ）」を参照）またはパスワードの有効期間を無期限に変更（「3.2.8.5　ユーザ個別のパスワードポリシーの適用（49 ページ）」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（「3.2.8.9　アカウントの有効化（53 ページ）」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。

3.2.8.1　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。Storage Navigator を利用する構成と HA Storage Advisor Embedded を利用する構成別に、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	Storage Navigator を利用する 構成	HA Storage Advisor Embedded を利用する構成
ユーザアカウント管理	Maintenance Utility※1	Maintenance Utility

システム管理者による ユーザ管理操作	Storage Navigator を利用する構成	HA Storage Advisor Embedded を利用する構成
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	Storage Navigator	RAID Manager または REST API
ユーザグループ管理		REST API
初回ログインのパスワード変更※2	Storage Navigator※3 または Maintenance Utility※1	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	Storage Navigator を利用する構成	HA Storage Advisor Embedded を利用する構成
初回ログインのパスワード変更※2	Storage Navigator※3 または Maintenance Utility※1	Maintenance Utility※1
自分自身のパスワード変更		

注※1

管理クライアントから IP アドレスを直接指定して起動してください。詳細は「1.5.5　各ツールのログイン方法（11 ページ）」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り、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「3.2.8.2　ユーザアカウントのパスワードポリシー設定（44 ページ）」および「3.2.8.5　ユーザ個別のパスワードポリシーの適用（49 ページ）」を参照してください。

注※3

ファームウェアバージョン 93-07-22-XX/XX 以降または 88-08-14-XX/XX 以降の SVP ソフトウェア（Storage Navigator）を使用してください。初回ログインのパスワード変更にファームウェアバージョン 93-07-22-XX/XX 未満または 88-08-14-XX/XX 未満の Storage Navigator を使用する場合は、注※1 を参照して、Maintenance Utility に IP アドレスを使用してログインしてください。

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	Storage Navigator を利用する構成で、Storage Navigator から操作した場合	HA Storage Advisor Embedded を利用する構成で、Maintenance Utitlity 以外から操作した場合
ユーザアカウント管理	• ユーザ作成およびユーザ編集時に、以下の設定はできません。 - メールアドレス - パスワード有効期間	-

ユーザ管理操作	Storage Navigator を利用する構成で、Storage Navigator から操作した場合	HA Storage Advisor Embedded を利用する構成で、Maintenance Utitlity 以外から操作した場合
	- 初回ログイン時にパスワード変更を要求する • ユーザアカウント状態のうち、次の項目は Storage Navigator で表示されないため、ユーザアカウント状態に応じた適切な対処が実施できない可能性があります。 - アカウントロック状態 - 初回ログイン時にパスワード変更を要求する - パスワード有効期限（日） • Storage Navigator の［Maintenance Utility］メニューにユーザ管理は表示されません。また、［Maintenance Utility］メニューから任意の項目を選択して Maintenance Utility を起動した場合も、Maintenance Utility 上にユーザ管理画面は表示されません。	
ユーザアカウントポリシー	Storage Navigator の［Maintenance Utility］メニューにユーザアカウントポリシーは表示されません。	
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］が設定済で、バージョン 93-07-22-XX/XX 未満または 88-08-14-XX/XX 未満の SVP ソフトウェア（Storage Navigator）を使用する場合は、Storage Navigator にログインができなくなります。	［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、Storage Navigator または Mainantenace Utility を除く全インターフェースからログインができなくなります。
自分自身のパスワード変更	-	HA Storage Advisor Embedded のナビゲーションバーの歯車アイコンをクリックして［ユーザ管理］を選択して Maintenance Utility を起動した場合、自分自身のパスワードを変更できません。

3.2.8.2　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 「3.2.8.9　アカウントの有効化（53 ページ）」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、「3.2.7　ユーザ名とパスワードの文字数と使用可能文字（40 ページ）」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。これにより、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、「3.2.8.5　ユーザ個別のパスワードポリシーの適用（49 ページ）」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]：ユーザー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]：ユーザー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]：ユーザー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]：ユーザー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]：ユーザー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。

3.2.8.3　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「3.2.8.4　テストメールの送信 (48 ページ)」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。

項目		説明
		• [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。
	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。

3.2.8.4　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）

3.2.8.5　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 および Storage Navigator 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 または Storage Navigator 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、「3.2.8.6　ユーザ個別のメールアドレスの設定（51 ページ）」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。

3.2.8.6　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「3.2.8.3　メールサーバの設定（47 ページ）」により、「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 が送信されます。

  GUM のファームウェアバージョンが以下の場合、SIM リファレンスコードは 7c1000 となります。エラー詳細が「Password expiration notification failed」であることを確認してください。※1
  - iStorage V100, V300 の場合：93-07-24/00 未満
  - iStorage V10e の場合：88-08-18/00 未満

  GUM のファームウェアバージョンが以下の場合、SIM リファレンスコードは 7c2000 となります。
  - iStorage V100, V300 の場合：93-07-24/00 以降
  - iStorage V10e の場合：88-08-18/00 以降

  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。
  - 「3.2.8.3　メールサーバの設定（47 ページ）」で設定した内容
  - 「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」に示す障害内容と対処方法

  訂正完了後、「3.2.8.4　テストメールの送信（48 ページ）」を実施し、メールが送信できることを確認してください。

  注※1

  SIM リファレンスコード 7c1000 のエラー詳細が「Error in server registered by using HSAE」の場合は、RAID Manager ユーザガイドに記載の 7c1xxx のトラブルシュートを実施してください。

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、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。

3.2.8.7　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。

3.2.8.8　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「3.2.8.2　ユーザアカウントのパスワードポリシー設定（44 ページ）」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。

3.2.8.9　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]－[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。

3.2.9　ユーザアカウントの作成

ユーザアカウントは、ビルトインユーザを含めて 20 まで登録できます。

⚠ 注意

初回ログインパスワード変更要求が有効なユーザを作成したい場合、事前にパスワードポリシーの［初回ログイン時にパスワード変更を要求する］を［はい］に設定してください。未設定の場合、ユーザを作成時［初回ログイン時にパスワード変更を要求する］に［はい］を選択しても、本機能は有効になりません。

パスワードポリシーの詳細については、「3.2.8　ユーザアカウントポリシーの設定（41 ページ）」を参照ください。

メモ

ユーザアカウント作成後はコントローラ障害等に備えて、ユーザアカウント情報をバックアップしてください（「3.2.13　ユーザアカウントのバックアップ（58 ページ）」参照）。障害復旧後にバックアップファイルからリストアすることで、元のユーザアカウント情報に戻せます（「3.2.14　ユーザアカウントのリストア（58 ページ）」参照）。

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、Maintenance Utility の Help を参照してください。

   ユーザ作成画面の右下にある［?］をクリックすると Help が表示されます。
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。

3.2.10　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

⚠注意

パスワード変更対象のユーザアカウントが、Storage Device List にも登録されている場合、パスワードをすべて一致させる必要があります。パスワードが一致しない場合、当該ストレージシステムへのログインができず、ストレージの運用ができなくなります。このため操作手順に従ってパスワードを変更してください。パスワードが一致していないと Storage Navigator の操作中に“20122-208003”エラーが発生します。「5.4.3　Storage Navigator 操作時のトラブルシューティング（118 ページ）」を参照して対処してください。また、HCS（HA Command Suite）を使用している場合は、HCS に登録した情報も変更する必要があります。『HA Command Suite ユーザーズガイド』の「ストレージシステムの設定を変更する」手順に従って変更してください。

操作手順

1. ［Storage Device List］画面に登録されているストレージシステムのユーザアカウントを確認してください。ストレージシステムに設定されているユーザアカウントのパス

ワードを変更する場合は、以下の操作を実行してください。その他のユーザアカウントのパスワードを変更する場合は、操作手順 2. に進んでください。

a. Windows の［スタート］メニューから、［HA Device Manager - Storage Navigator］－［Storage Device List］を右クリックし、［管理者として実行］をクリックします。［管理者として実行］が表示されない場合は、［詳細］または［その他］－［ファイルの場所を開く］をクリックします。開かれたエクスプローラーにあるファイルを右クリックし、［管理者として実行］をクリックします。

ヒント

SVP デスクトップ上の［Open StorageDeviceList］アイコンを右クリックして、［管理者として実行］を選択することでも Storage Device List を起動できます。

b. ［Storage Device List］画面で、ユーザアカウントのパスワードを変更したいストレージシステムを選択して［Stop Service］をクリックします。

c. ［Stop Service］画面で［Confirm］をクリックします。

2. Maintenance Utility にログインします。
3. ［管理］－［ユーザ管理］を選択します。
4. ［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。
5. ［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。)
6. ［編集］を選択します。
7. [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、Maintenance Utility の Help を参照してください。

   ユーザ編集画面の右下にある［?］をクリックすると Help が表示されます。

メモ

- 変更するユーザのパスワードには、現在のストレージシステム全体のパスワードポリシーが適用されます。
- 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「3.2.8　ユーザアカウントポリシーの設定（41 ページ）」を参照してください。

8. 設定内容を確認し［完了］をクリックします。
9. 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。
10. 確認メッセージが表示されます。［適用］をクリックします。
11. 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。

12. ［Storage Device List］画面に登録されているストレージシステムに設定されているユーザアカウントのパスワードを変更する場合は、以下の操作を実行してください。その他のユーザアカウントのパスワードを変更する場合は不要です。

    a. ［Storage Device List］画面で、ユーザアカウントのパスワードを変更したいストレージシステムを選択して［Edit］をクリックします。

    b. ［Edit System］画面の［User Information］－［Password］に Maintenance Utility で設定した新しいパスワードを入力します。

    c. ［Apply］をクリックします。

    d. ［Start Service］をクリックします。

3.2.11　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. ユーザグループ一覧から、無効化したいユーザアカウントが所属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、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。）
5. ［編集］を選択します。
6. 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。
7. 設定内容を確認し［完了］をクリックします。
8. 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。
9. 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。

3.2.12　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 を含む管理ソフトウェアを利用できます。

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. ユーザグループ一覧から、削除したいユーザアカウントが所属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、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。）
5. ［削除］を選択します。
6. 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。
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。

3.2.13　ユーザアカウントのバックアップ

ストレージシステムのトラブルに備え、ユーザアカウント情報をバックアップできます。

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. ［ユーザアカウント情報］から［バックアップ］を選択します。
4. 表示された画面にバックアップファイルの保存先とファイル名を指定し、バックアップファイルをダウンロードします。
5. 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。

3.2.14　ユーザアカウントのリストア

ユーザアカウント情報のバックアップファイルを使用してリストアできます。

⚠注意

ユーザアカウントのリストアが完了するまで、ログインなどの認証に関する処理は行わないでください。リストアが失敗する場合があります。

ユーザアカウント情報をバックアップしリストアする場合は、パスワードポリシー機能に対応した GUM ファームウェアバージョン※と未対応のバージョンによる組み合わせで、パスワードポリシーの適用有無が異なります。

注※

パスワードポリシー機能と対応バージョンの詳細は「3.2.8　ユーザアカウントポリシーの設定（41 ページ）」を参照してください。

	バックアップ元（パスワードポリシー非対応版）	**バックアップ元（パスワードポリシー対応版）**
リストア先（パスワードポリシー非対応版）	• すべてのユーザでパスワードポリシーは適用されません。 • リストア後も、バックアップ時の全ユーザがログインし、各操作ができます。	• すべてのユーザでパスワードポリシーは適用されません。 • リストア後も、バックアップ時の全ユーザがログインし、各操作ができます。
リストア先（パスワードポリシー対応版）	• すべてのユーザでパスワードポリシーは適用されません。 • リストア後も、パスワードポリシーが無効化された状態でログインし、各操作ができます。 • 各ユーザにパスワードポリシーを適用するには、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適用済みユーザには、リストア後もパスワードポリシーが適用された状態になります。 - ただし有効期限はバックアップデータ時点の時刻を保持するため、リストア後にログインできなくなる可能性があります。 • パスワードポリシー適用前のユーザには、リストア後もパスワードポリシーは適用されません。 - リストア後も、ログインし各操作ができます。 - 各ユーザにパスワードポリシーを適用するには、パスワードを変更する必要があります

前提条件

- ユーザアカウント情報がバックアップされていること

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. ［ユーザアカウント情報］から［リストア］を選択します。
4. ユーザアカウント情報リストア画面が表示されます。

   リストアするファイル名を指定します。
5. ファイル名を確認し［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　アラート通知

ストレージシステムの障害情報（SIM）を通知するための設定をします。

メールサーバ、Syslog サーバ、SNMP マネージャとの連携によって、ストレージシステムを監視できます。どれか 1 つ以上を設定してください。

メールサーバを利用するとアラート通知をメールで受信できます。この機能によってストレージシステム管理者はストレージシステムを遠隔監視できます。

Syslog サーバを利用するとアラート通知を Syslog サーバに蓄積できるため、障害発生の履歴として保管できます。

SNMP マネージャを利用すると障害の内容を把握できるため、障害回復までの時間を短縮できます。

本ストレージシステムでは、SNMP エージェントが各 CTL に実装されています。各 CTL の SNMP エージェントから SNMP マネージャに Trap 送信します。SNMP v3 プロトコルを使用する場合は、各 CTL の SNMP エンジン ID を SNMP マネージャに登録することが必要です（「3.3.7　SNMP エンジン ID を確認する（67 ページ）」を参照）。

メモ

障害情報は CTL1 または CTL2 の管理ポートから管理 LAN を介して通知されます。CTL が障害により動作を停止している場合は正常な CTL の管理ポートから通知されます。このため CTL1 と CTL2 の管理ポートは必ず管理 LAN に接続してください。一方の CTL の管理ポートだけが管理 LAN に接続されていると、障害情報が正しく通知されない可能性があります。

通信障害の発生などにより最大 256 個の障害情報が滞留しますが、通信障害が解消されると、約 5 分以内に通知されます。

⚠ 注意

SIMRC=3073xx を伴う MP 障害発生時、一部の SIM について障害通知が遅延される最大時間が、GUM ファームウェアバージョンによって異なります。

なお、障害検知および保守運用については他 SIM の障害通知により取得できるため、障害監視運用および保守運用への影響はありません。また、障害通知が遅延している SIM 有無をすぐに確認したい場合は、GUM のリブートを実施ください。GUM のリブート方法については、「3.12.6　GUM のリブート（92 ページ）」を参照してください。

次に示す GUM ファームウェアバージョンの場合は、障害通知が最大 48 時間遅延する可能性があります。

- iStorage V100, V300
  - 93-07-21/XX～93-07-23/XX 未満
  - 93-06-86/XX 未満

次に示す GUM ファームウェアバージョンの場合は、障害通知が最大 2 時間遅延する可能性があります。

- iStorage V10e
  - 全バージョン
- iStorage V100, V300

- 93-07-23/XX 以降
- 93-06-86/XX～93-06-XX/XX

3.3.1　メール通知の設定

宛先のメールアドレス、メールサーバのアドレスなどを設定します。

メールサーバへ転送される障害通知メールのフォーマットについては、「M.1　障害通知メールの内容（426 ページ）」を参照してください。

前提条件

- 管理 LAN 上に SMTP に対応したメールサーバが設置されていること
- ファイアウォールを使用している場合は、ポート番号 25 を開放済みであること（ストレージシステムとメールサーバの通信に、ポート番号 25 を使用するため）。

⚠注意

ストレージシステムからメールサーバに接続する場合の注意点を示します。

SMTP 認証（SMTP-AUTH）の PLAIN または LOGIN を使用してメールサーバに接続します。SMTP-AUTH の CRAM-MD5、DIGEST-MD5 はサポートしていません。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［アラート通知］を選択します。
3. ［設定］を選択します。
4. アラート通知設定画面が表示されます。［Email］タブを選択します。
5. 各項目を入力します。

   各項目の詳細は、Maintenance Utility の Help を参照してください。

   アラート通知設定画面の右下にある［?］をクリックすると Help が表示されます。
6. 設定内容を確認し［確認］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。

3.3.2　テストメールの送信

メール通知の設定を確認するため、テストメールを送信します。

前提条件

- メール通知の設定が完了していること
- メールサーバが正常に稼働していること
- 改行コードを自動的に削除するメールソフトを使用する場合は、改行コードの自動削除機能が解除されていること

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［アラート通知］を選択します。
3. ［Email］タブの［テスト Email 送信］をクリックします。
4. 完了メッセージが表示されます。［OK］をクリックします。

   警告メッセージが表示された場合は［OK］をクリックし、次の項目を確認して不具合を訂正してください。

   - 「3.3.1　メール通知の設定（61 ページ）」で設定した内容
   - メールサーバの動作状況と設定内容
   - 管理 LAN の動作状況
5. 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。

   RefCode : 7fffff

   Detail : This is Test Report.

   7fffff は、テストメールの SIM リファレンスコードです。

   テストメールを受信できない場合は、次の項目を確認して不具合を訂正してください。

   - 「3.3.1　メール通知の設定（61 ページ）」で設定した内容
   - 「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」に示す障害内容と対処方法

メモ

メールに記載される項目と、その内容を示します。

- メールタイトル

  （ストレージシステムの装置名）＋（Report）です。
- 通知する付加情報

  「3.3.1　メール通知の設定（61 ページ）」で設定した内容です。

  未設定の場合は何も表示されません。

- 障害が発生した日付
- 障害が発生した時刻
- ストレージシステムの装置名＋シリアル番号
- SIM リファレンスコード

  アラート画面に表示される SIM リファレンスコードです。
- 障害内容

  アラート画面に表示されるエラー詳細です。
- 保守作業に必要な不良個所の情報

  最大 8 件の不良個所の情報が表示されます。

  1 件の不良個所の情報には、［アクションコード］、［想定障害部品］、および［ロケーション］の項目が 含まれます。

  テストメールには記載されません。

SIM リファレンスコードと障害内容については、『SIM リファレンス』を参照してください。

3.3.3　アラート通知を蓄積するための Syslog の設定

Syslog サーバにアラート通知を送付するため、Syslog サーバのアドレスなどを設定します。※

注※

画面に表示される転送プロトコルは、モデルやファームウェアバージョンによって異なります。

詳細は「N.1　モデルやファームウェアバージョンによる転送プロトコルの表示の差異（432 ページ）」を参照してください。

Syslog サーバへ転送されるアラート通知のフォーマットについては、「M.2　Syslog メッセージの内容（426 ページ）」を参照してください。

前提条件

- 管理 LAN 上に Syslog サーバが設置されていること
- ファイアウォールを使用している場合は、Syslog の転送で使用するポートを開放すること

⚠ 注意

- 転送プロトコルに TLS/RFC5424 を使う場合は、監査ログの Syslog サーバ転送設定で指定したルート証明書およびクライアント証明書と同じ証明書を指定してください。監査ログの Syslog サーバ転送については、「3.7.1　監査ログを蓄積するための Syslog の設定（76 ページ）」を参照してください。

- Syslog サーバを IPv6 で指定する場合、次の IP アドレスは指定できません。
  * 無効値： [::]
  * ループバックアドレス： [::1]
  * マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF]
  * IPv4 射影アドレス： [::FFFF:(IPv4)]
  * リンクローカルアドレス： [FE80::]
  * グローバルユニキャストアドレス： [2001::]
  * グローバルユニキャストアドレス： [2002::]

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［アラート通知］を選択します。
3. ［設定］を選択します。
4. アラート通知設定画面が表示されます。［Syslog］タブを選択します。
5. 各項目を入力します。

   各項目の詳細は、Maintenance Utility の Help を参照してください。

   アラート通知設定画面の右下にある［?］をクリックすると Help が表示されます。
6. 設定内容を確認し［確認］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。

3.3.4　アラート通知を蓄積するための Syslog サーバへのテストメッセージの送信

Syslog の設定を確認するため、テストメッセージを送信します。

前提条件

- Syslog の設定が完了していること
- Syslog サーバが正常に稼働していること

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［アラート通知］を選択します。
3. ［Syslog］タブの［Syslog サーバへテストメッセージ送信］をクリックします。

4. 完了メッセージが表示されます。［OK］をクリックします。
5. 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下記の情報が含まれています。

   RefCode : 7FFFFF

   This is Test Report.

   7FFFFF は、テストメッセージの SIM リファレンスコードです。

   SIM リファレンスコードと障害内容については、『SIM リファレンス』を参照してください。

   テストメッセージを受信できない場合は、次の項目を確認して不具合を訂正してください。

   - 「3.3.3　アラート通知を蓄積するための Syslog の設定（63 ページ）」で設定した内容
   - 「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」に示す障害内容と対処方法

メモ

Syslog に出力される項目と、その内容を示します。

- 通知する付加情報

  「3.3.3　アラート通知を蓄積するための Syslog の設定（63 ページ）」で設定した内容です。

  未設定の場合は何も表示されません。
- 障害が発生した日付
- 障害が発生した時刻
- 装置モデル名称＋シリアル番号
- SIM リファレンスコード

  アラート画面に表示される SIM リファレンスコードです。
- 障害内容

  アラート画面に表示されるエラー詳細です。
- ユーザーシステムコード

  アラート通知画面、ALIVE 設定のユーザーシステムコードです。
- 保守作業に必要な不良個所の情報

  最大 8 件の不良個所の情報が表示されます。

  1 件の不良個所の情報には、［アクションコード］、［想定障害部品］、および［ロケーション］の項目が 含まれます。

  テスト送信には記載されません。

SIM リファレンスコードと障害内容については、『SIM リファレンス』を参照してください。

3.3.5　SNMP エージェントの設定

SNMP マネージャに障害通報を送付するため、SNMP エージェントを設定します。

SNMP マネージャへ転送される SNMP メッセージのフォーマットについては、「M.3　SNMP メッセージの内容（430 ページ）」を参照してください。

SNMP トラップの構成、およびサポート MIB の仕様については、『SNMP Agent ユーザガイド』を参照してください。

前提条件

- 管理 LAN 上に SNMP マネージャが設置されていること

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［アラート通知］を選択します。
3. ［設定］を選択します。
4. アラート通知設定画面が表示されます。［SNMP］タブを選択します。
5. 各項目を入力します。

   各項目の詳細は、Maintenance Utility の Help を参照してください。

   アラート通知設定画面の右下にある［?］をクリックすると Help が表示されます。
6. 設定内容を確認し［確認］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。

メモ

トラップ送信先、あるいはリクエスト許可対象を変更する際に、［トラップ送信先］および［ユーザ名］がグレーアウトによって入力できない場合、設定を変更したい SNMP エージェントの設定を削除した後に、再度 SNMP エージェントを設定してください（削除する方法は『SNMP Agent ユーザガイド』を参照）。

3.3.6　テスト SNMP トラップの送信

SNMP エージェント設定を確認するため、テスト SNMP トラップを送信します。

前提条件

- SNMP エージェントの設定が完了していること
- SNMP マネージャが正常に稼働していること

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［アラート通知］を選択します。
3. ［SNMP］タブの［テスト SNMP トラップ送信］をクリックします。
4. 完了メッセージが表示されます。［OK］をクリックします。
5. SNMP マネージャに、テスト SNMP トラップが到着したことを確認します。

   テスト SNMP トラップには下記の情報が含まれています。

   RefCode : 7FFFFF

   This is a test code.

   7FFFFF は、テスト SNMP トラップの SIM リファレンスコードです。

   SIM リファレンスコードと障害内容については、『SIM リファレンス』を参照してください。

   テスト SNMP トラップを受信できない場合は、次の項目を確認して不具合を訂正してください。

   - 「3.3.5　SNMP エージェントの設定（66 ページ）」で設定した内容
   - 「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」に示す障害内容と対処方法

3.3.7　SNMP エンジン ID を確認する

本ストレージシステムでは、SNMP エージェントが各 CTL に実装されています。SNMP v3 プロトコルを使用する場合は、各 CTL の SNMP エンジン ID を SNMP マネージャに登録してください。

次に示す手順で、各 CTL の SNMP エンジン ID を参照できます。

操作手順

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

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

2. ［管理］ツリーから［アラート通知］を選択します。

［SNMP］タブの［SNMP エンジン ID］の値を確認します。

3. 手順 1 に戻って、もう一方の CTL の SNMP エンジン ID を確認します。

3.4　ライセンス

プログラムプロダクトを購入するとライセンスキーが発行されます。このライセンスキーをスト レージシステムに追加することにより、プログラムプロダクトの機能が利用可能となります。

プログラムプロダクトの概要については、『ドキュメントマップ』を参照してください。

3.4.1　ライセンスキーの参照

ストレージシステムにインストールされているライセンスキーを確認します。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ライセンス］を選択します。
3. ［ライセンスキー］の一覧表を参照します。

一覧表の内容

一覧表に表示されるライセンスキーの状態を示します。

ライセンスキーの状態	状態	キータイプ	ライセンス容量	期間（日数）
未インストール	Not Installed	空白	空白	空白
Permanent キーでインストール	Installed	Permanent	許可容量	—
Term キーでインストール Term キーを有効に設定	Installed	Term	許可容量	残日数
Term キーでインストール Term キーを無効に設定	Installed （Disabled）	Term	許可容量	空白
Term キーでインストール 有効期限切れの状態	Not Installed	空白	空白	空白

3.4.2　ライセンスキーの追加

前提条件

- ライセンスキーコードまたはライセンスキーファイルを準備しておくこと

  ライセンスキーはコード（英数字の文字列）の形式で提供されます。このコードが記載されているメモ（ライセンスキーコード）、またはファイル（ライセンスキーファイル）を準備してください。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ライセンス］を選択します。
3. ［インストール］をクリックします。
4. ライセンスインストール画面が表示されます。

   ［ライセンスキーコード］にライセンスキーコードを入力、または［ライセンスキーファイル］でライセンスキーファイルを選択します。
5. 設定内容を確認し［適用］をクリックします。

   メモ

   インストールに失敗すると、エラーメッセージが表示されます。詳細はエラーメッセージ画面で確認してください。

3.4.3　ライセンスキーの有効化

ストレージシステムに追加されているライセンスキーから、使用したいプログラムプロダクトのライセンスキーを選択して有効化できます。

前提条件

- ライセンスキーが追加されていること

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ライセンス］を選択します。
3. ［ライセンスキー］のプログラムプロダクト一覧から、有効化したいプログラムプロダクトを選択します。

（有効化できるプログラムプロダクトのライセンスキーは、［状態］が［Installed (Disabled)］に限られます。）

（［プログラムプロダクト名］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. ［有効化］をクリックします。
5. 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。
6. 完了メッセージが表示されます。［OK］をクリックします。

（操作手順 3. で選択したプログラムプロダクトのライセンスキーの［状態］が［Installed］に変わります。）

3.4.4　ライセンスキーの無効化

ストレージシステムに追加されているライセンスキーから、使わないプログラムプロダクトのライセンスキーを選択して無効化できます。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ライセンス］を選択します。
3. ［ライセンスキー］のプログラムプロダクト一覧から、無効化したいプログラムプロダクトを選択します。

（無効化できるプログラムプロダクトのライセンスキーは、［状態］が［Installed］に限られます。）

（［プログラムプロダクト名］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. ［無効化］をクリックします。
5. 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。
6. 完了メッセージが表示されます。［OK］をクリックします。

（操作手順 3. で選択したプログラムプロダクトのライセンスキーの［状態］が［Installed (Disabled)］に変わります。）

3.4.5　ライセンスキーのアンインストール

ストレージシステムに追加されているライセンスキーから、使わないプログラムプロダクトのライセンスキーを選択して削除できます。

キー種別が Permanent 以外の場合、ライセンスキーをアンインストールすると、インストールで使用したライセンスキーファイルは使用できなくなります。再度ライセンスキーを使

用するには、ライセンスキーファイルの再発行が必要です。ライセンスキーファイルの再発行については、弊社担当営業にお問い合わせください。

キー種別が Permanent の場合、ライセンスキーをアンインストールしても、インストールで使用したライセンスキーファイルを使用できます。このためライセンスキーファイルの再発行は不要です。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ライセンス］を選択します。
3. ［ライセンスキー］のプログラムプロダクト一覧から、削除したいプログラムプロダクトを選択します。

   （削除できるプログラムプロダクトのライセンスキーは、［状態］が［Installed］に限られます。）

   （［プログラムプロダクト名］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. ［アンインストール］をクリックします。
5. 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。
6. 完了メッセージが表示されます。［OK］をクリックします。

   （操作手順 3. で選択したプログラムプロダクトのライセンスキーの［状態］が［Not Installed］に変わります。）

3.5　ネットワーク設定

3.5.1　ネットワーク設定の変更

⚠注意

- 処理が完了していないタスクがある状態で IP アドレスを変更しないでください（タスクの状態確認の方法については、「E.1.9　タスクの状態確認（302 ページ）」を参照してください）。タスクが異常終了する可能性があります。
- SVP を使用している場合は、SVP に登録したストレージシステムの IP アドレスも変更する必要があります。「G.2.5　Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。
- DNS サーバを設定した場合、DNS サーバに下記の項目を登録してください。

  ホスト名：localhost

  IP アドレス：127.0.0.1

- Maintenance Utility では、DNS サーバを IPv6 で指定できません。
- 管理サーバ（SVP）からストレージシステムの CTL1 と CTL ２にホスト名を使って接続できます（別途、管理サーバ（SVP）の Storage Device List で設定）。

  ホスト名で接続する場合は、この手順で設定した CTL1 と CTL2 の IP アドレスを DNS サーバに登録してください。DNS サーバ登録時の注意事項を示します。

  - CTL1 と CTL2 の IP アドレスに別々のホスト名を割り当ててください。同じホスト名に割り当てると、正常に通信できないおそれがあります。
  - 異なるストレージシステムの CTL の IP アドレスを同じホスト名に割り当てないでください。正常に通信できないおそれがあります。
  - 以下の規則に従ったホスト名を使用してください。
    * ホスト名の最大文字数は 255 文字です。
    * 半角英数字と以下の記号を使用できます。なお、半角スペースは使用できません。

      ! $ % - . @ _ ` ~
  - SVP の Windows に対する設定も必要です。［コントロールパネル］から DNS サフィックスを追加する画面を表示して、CTL1、CTL2 に設定するホストのドメイン名を追加してください。（「G.2.21　DNS サフィックスの設定（393 ページ）」参照）。
  - DNS サーバに登録済の CTL1 と CTL2 の IP アドレスを変更した場合は、DNS サーバの設定変更後に、SVP のコマンドプロンプトで「ipconfig /flushdns」コマンドを実行してください。このコマンドを実行しない場合、SVP の DNS キャッシュが最大 1 時間クリアされないため、SVP からストレージシステムに接続できません。
- プロトコルを IPv4/IPv6 両方に設定した後で、IPv4 のみ（または IPv6 のみ）に切り替えると、ネットワーク設定の参照画面には、IPv4/IPv6 両方の設定値が表示されます。プロトコルの設定を確認するには、参照画面から［ネットワーク設定］をクリックして設定画面を開いてください。設定画面で、プロトコルの選択状態を確認できます。また、設定画面では、無効なプロトコルの IP アドレス情報は淡色表示されます。
- IP アドレスを IPv6 で指定する場合、次の IP アドレスは指定できません。
  - 無効値： [::]
  - ループバックアドレス： [::1]
  - マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF]
  - IPv4 射影アドレス： [::FFFF:(IPv4)]
  - リンクローカルアドレス： [FE80::]
  - グローバルユニキャストアドレス： [2001::]
  - グローバルユニキャストアドレス： [2002::]

操作手順

1. Maintenance Utility にログインします。

2. ［管理］－［ネットワーク設定］を選択します。
3. ［ネットワーク設定］をクリックします。
4. ネットワーク設定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、Maintenance Utility の Help を参照してください。

   ネットワーク設定画面の右下にある［?］をクリックすると Help が表示されます。
5. 設定内容を確認し［確認］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。

3.5.2　ネットワーク拒否設定の変更

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［ネットワーク設定］を選択します。
3. ［ネットワーク拒否設定］をクリックします。
4. ネットワーク拒否設定が表示されます。各項目の有効、無効を選択します。

   各項目の詳細は、Maintenance Utility の Help を参照してください。

   ネットワーク拒否設定画面の右下にある［?］をクリックすると Help が表示されます。
5. 設定内容を確認し［確認］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。

3.6　日時設定

3.6.1　日時設定の変更

UTC タイムゾーンの選択と NTP サーバの使用、不使用を選択します。

⚠注意

- 他のユーザがストレージシステムにアクセスしている間は、日時設定の変更ができません。
- SVP を使用している場合は、SVP のシステム日時も更新する必要があります。「A.5　管理サーバ（SVP）の初期設定を行う（187 ページ）」を参照してください。
- 現在設定されているシステム日時が実際の日時より進んでいる場合に、システム日時を修正すると、構成情報のバックアップが取得されない可能性があります。この事象が予想される場合は、既存のバックアップファイルを、別のフォルダに移動してください。
- NTP サーバを使用する場合は、バージョンが NTPv4 を使用してください。

- NTP サーバを使用する場合は、ストレージシステムと NTP サーバ間の通信にポート番号 123 を使用します。このためストレージシステムと NTP サーバ間のネットワークに対して、ポート番号 123 の通信を許可するように設定してください。
- NTP サーバを IPv6 で指定する場合、次の IP アドレスは指定できません。
  - 無効値： [::]
  - ループバックアドレス： [::1]
  - マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF]
  - IPv4 射影アドレス： [::FFFF:(IPv4)]
  - リンクローカルアドレス： [FE80::]
  - グローバルユニキャストアドレス： [2001::]
  - グローバルユニキャストアドレス： [2002::]
- NTP サーバを使用した日時設定に失敗した場合は「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」に示す障害内容と対処方法を参照してください。
- システムの時刻を設定済み日付より後ろに変更した場合は、変更した日付分、パスワード有効期間が消費されます。消費した日付は、システムの時刻を前に戻した場合でも元に戻りません。有効期間を増やしたい場合は、再度設定を行ってください。

  例：

  ①システム日付の変更前：

  2023 年 9 月 1 日

  有効期間：10 日

  ②システム日付の変更後：

  2023 年 9 月 2 日

  有効期間：9 日

  ③システム日付を変更前の状態に戻す：

  2023 年 9 月 1 日

  有効期間：9 日

メモ

定期的に NTP サーバとの同期を確認してください。1 日 1 回確認することを推奨します。同期に失敗すると SIM リファレンスコード「7ffa00」が出力されます。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［日時設定］を選択します。

3. ［設定］をクリックします。
4. 日時設定画面が表示されます。各項目を入力します。
   - NTP サーバを使用する場合：
     a. ［NTP サーバを使用］の［はい］を選択します。
     b. ［NTP サーバ］に IP アドレス、またはホスト名を入力します。
     c. ［同期時刻］に NTP サーバと同期する時刻を指定します。
     本作業の完了と同時に日時を同期させたい場合は［今すぐ同期する］をチェックします。
   - NTP サーバを使用しない場合：
     a. ［NTP サーバを使用］の［いいえ］を選択します。
     b. ［日時］で、現在の日時を選択します。
5. 設定内容を確認し［適用］をクリックします。
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。

3.6.2　システム日時の更新

日時設定画面に表示されているシステム日時を更新します。

メモ

NTP サーバを使用している場合は、ストレージシステムが Ready 状態になった時点で、自動でシステム日時が更新されます。

⚠ 注意

現在設定されているシステム日時が実際の日時より進んでいる場合に、システム日時を修正すると、構成情報のバックアップが取得されない可能性があります。この事象が予想される場合は、既存のバックアップファイルを、別のフォルダに移動してください。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［日時設定］を選択します。
3. ［システム日時］の右横にある［更新］をクリックします。

3.7　監査ログ

ストレージシステムは、監査ログとして「誰が」「いつ」「どのような操作をしたか」を記録してい ます。監査ログを保管することで、ストレージシステムの監査に備えることができます。

メモ

- ストレージシステムに保存されている監査ログは Syslog サーバに常時自動で転送できます。Maintenance Utility の［監査ログエクスポート］を使用して手動でダウンロードすることもできます。
- ストレージシステムに保存できる監査ログの容量には限りがあります。最大保存容量に達すると、新しい情報が上書きされ、古い情報は消去されるため、監査ログを Syslog サーバへ転送することを推奨します。
- 監査ログのフォーマットおよび詳細は、『監査ログ リファレンスガイド』を参照してください。
- SVP に保存されている監査ログは Storage Navigator からエクスポートします。作業手順については、「J.1　SVP に保存された監査ログをエクスポートする（407 ページ）」を参照してください。

  ストレージシステムに保存される監査ログと、SVP に保存される監査ログは、内容が異なります。詳細は『HA Device Manager - Storage Navigator ユーザガイド』を参照してください。

3.7.1　監査ログを蓄積するための Syslog の設定

監査ログを Syslog サーバへ転送して蓄積するためのアドレス、ロケーション識別名などを設定します。転送プロトコルは、TLS と UDP から選択できます。※

注※

画面に表示される転送プロトコルは、モデルやファームウェアバージョンによって異なります。

詳細は「N.1　モデルやファームウェアバージョンによる転送プロトコルの表示の差異（432 ページ）」を参照してください。

Syslog サーバへ転送される監査ログのフォーマットについては、『監査ログ リファレンスガイド』を参照してください。

前提条件

- 管理 LAN 上に Syslog サーバが設置されていること
- TLS/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用意されていること

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

⚠ 注意

- Syslog サーバの設定に不具合がある状態で監査ログを転送すると、Syslog サーバに監査ログが保存されず、ストレージシステムからも削除されてしまいます。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。
- 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。
- 転送プロトコルに TLS/RFC5424 を使う場合は、アラートの Syslog サーバ転送設定で指定したルート証明書およびクライアント証明書と同じ証明書を指定してください。アラートの Syslog サーバ転送については、「3.3.3　アラート通知を蓄積するための Syslog の設定（63 ページ）」を参照してください。
- Syslog サーバを IPv6 で指定する場合、次の IP アドレスは指定できません。
  - 無効値： [::]
  - ループバックアドレス： [::1]
  - マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF]
  - IPv4 射影アドレス： [::FFFF:(IPv4)]
  - リンクローカルアドレス： [FE80::]
  - グローバルユニキャストアドレス： [2001::]
  - グローバルユニキャストアドレス： [2002::]

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［監査ログ設定］を選択します。
3. ［Syslog サーバ設定］をクリックします。
4. 監査ログ設定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、Maintenance Utility の Help を参照してください。

   監査ログ設定画面の右下にある［?］をクリックすると Help が表示されます。
5. 設定内容を確認し［確認］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。

3.7.2　監査ログを蓄積するための Syslog サーバへテストメッセージを送信

Syslog サーバへの転送の設定を確認するため、テストメッセージを送信します。

前提条件

- Syslog の設定が完了していること
- Syslog サーバが正常に稼働していること

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［監査ログ設定］を選択します。
3. ［Syslog サーバへテストメッセージ送信］をクリックします。
4. 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下記の情報が含まれています。

   [AuditLog]

   This is a test message

   テストメッセージを受信できない場合は、次の項目を確認して不具合を訂正してください。

   - 「3.7.1　監査ログを蓄積するための Syslog の設定（76 ページ）」で設定した内容
   - 「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」に示す障害内容と対処方法

3.7.3　ストレージシステムに保存された監査ログをエクスポートする

ストレージシステム内部の監査ログには、GUM の監査ログと DKC の監査ログがあります。GUM の監査ログは、CTL1 および CTL2 のそれぞれに蓄積されています。一つ目の CTL から GUM の監査ログのエクスポートを終えた後、もう一方の CTL からも GUM の監査ログをエクスポートしてください。

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［監査ログ設定］を選択します。
3. ［監査ログエクスポート］－［GUM］、または［監査ログエクスポート］－［DKC］を選択します。
4. 確認画面が表示されます。［OK］をクリックします。
5. 白い画面またはセキュリティ確認画面が表示されます。

⚠注意

白い画面またはセキュリティ確認画面は、エクスポートが完了するまで閉じないでください。エクスポートが失敗する可能性があります。

⚠注意

https 接続時に証明書が不正な場合にはセキュリティ確認画面が表示されます。30 秒以内に以下の操作を行ってください。30 秒を過ぎると監査ログをエクスポートできません。操作手順 3.からやり直してください。

＜ Microsoft Edge の場合＞

［詳細設定］－［<IP アドレスまたはホスト名>に進む（安全ではありません）］をクリックしてください。

＜ Google Chrome の場合＞

［詳細設定］－［<IP アドレス>にアクセスする（安全ではありません）］をクリックしてください。

6. ファイルのダウンロード画面が表示されます。エクスポートはファイルのダウンロードとして行われます。［DKC］を選択したときは、ファイルのダウンロード画面が表示されるまで 2～3 分かかります。

メモ

- ファイルのダウンロード画面は Maintenance Utility の画面に表示されます。白い画面またはセキュリティ確認画面で Maintenance Utility の画面が隠れている場合は、Maintenance Utility の画面をクリックしてダウンロード画面を確認してください。
- ファイルのダウンロード画面は、ブラウザによって形式が異なります。
- ブラウザの設定によって、ファイルのダウンロード画面が表示されずにファイルのダウンロードを開始する場合があります。

7. ファイルのダウンロード画面で［名前を付けて保存］をクリックします。
8. ダウンロード先およびファイル名を入力して［保存］をクリックします。
9. ダウンロードの進捗状況を確認します。

メモ

- ダウンロードするファイルは動的に生成されるため、ファイルサイズおよびファイル転送完了予定時間は、不明または非表示となります。
- ファイルのダウンロード時間は、ネットワークの速度に左右されます。

10. ダウンロードが完了したことを確認します。

メモ

白い画面またはセキュリティ確認画面が残っている場合は手動で閉じてください。

⚠ 注意

DKC の監査ログに記録されている、下記の情報に関する注意点を示します。

- ロケーション識別名

  「3.7.1　監査ログを蓄積するための Syslog の設定（76 ページ）」で［ロケーション識別名］を変更した場合、タイミングによっては、ロケーション識別名を変更する前に発生したイベントを記録しているレコード内のロケーション識別名が、ロケーション識別名を変更した後のロケーション識別名になる可能性があります。

- 日付・時刻情報の時差情報

  「3.6.1　日時設定の変更（73 ページ）」の［UTC タイムゾーン］で、時差が変わる UTC タイムゾーンに変更した場合、タイミングによっては、UTC タイムゾーンを変更する前に発生したイベントのレコード内の時差情報が、UTC タイムゾーンを変更した後の時差情報になる可能性があります。

3.8　外部認証

外部認証サーバによるユーザアカウントの認証とユーザグループの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。

構成と使用する認証サーバによって、外部認証の設定手段が異なります。

構成	認証サーバ	Maintenance Utility	SVP の外部認証設定
SVP を使用しない管理モデル	LDAP	○	×
	Kerberos	×	×
	RADIUS	×	×
SVP を使用する管理モデル	LDAP	×※	○
	Kerberos	×	○
	RADIUS	×	○

凡例

○：設定可能、×：設定不可

注※

SVP を使用する管理モデルでは、運用上の制約として Maintenance Utility で設定しないでください。

SVP で外部認証を使用する場合は、「D.1　外部サーバとの連携設定の手順（277 ページ）」を参照してください。

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。
- ストレージシステムの管理を、SVP を使用しない管理モデルから、SVP を使用する管理モデルへ変更する場合は、Maintenance Utility の外部認証機能を無効にしたのちに、当該のストレージシステムを SVP の Storage Device List へ登録してください。無効に切り替える方法は、「3.8.3　無効化（83 ページ）」を参照してください。なお SVP の外部認証機能が設定されていない場合は、「D.1　外部サーバとの連携設定の手順（277 ページ）」を参照して設定してください。
- ストレージシステムの管理を、SVP を使用する管理モデルから、SVP を使用しない管理モデルへ変更する場合は、SVP の Storage Device List からストレージシステムを削除したのちに、Maintenance Utility の外部認証機能を設定してください（設定方法は「3.8.2　LDAP の設定（82 ページ）」を参照）。なお SVP の外部認証機能は、Storage Device List に登録されているすべてのストレージシステムに対して同時に機能します。このため Storage Device List に登録されているストレージシステムを個別に、SVP の外部認証と Maintenance Utility の外部認証を切り替えることはできません。
- 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、「3.2.4　ユーザグループ（36 ページ）」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。

3.8.1　LDAP ディレクトリサーバの要件

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サーバ証明書が必要です。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

- 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※

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される「基本制限(BasicConstraints)」「キー使用法(KeyUsage)」「サブジェクトキー識別子(SubjectKeyIdentifier)」をサポートしています。

3.8.2　LDAP の設定

⚠ 注意

LDAP ディレクトリサーバを IPv6 で指定する場合、次の IP アドレスは指定できません。

- 無効値： [::]
- ループバックアドレス： [::1]
- マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF]
- IPv4 射影アドレス： [::FFFF:(IPv4)]
- リンクローカルアドレス： [FE80::]
- グローバルユニキャストアドレス： [2001::]
- グローバルユニキャストアドレス： [2002::]

メモ

Maintenance Utility でユーザアカウントを作成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。ユーザアカウントの作成方法は、Maintenance Utility の Help を参照してください。ユーザ作成画面の［認証］で選択できます。

前提条件

- LDAP ディレクトリサーバが管理 LAN に接続されていること

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［外部認証］－［サーバ設定］－［LDAP］を選択します。
3. LDAP の設定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、Maintenance Utility の Help を参照してください。

   設定画面の［?］をクリックすると Help が表示されます。
4. 設定内容を確認し［サーバ構成テスト］の［チェック］をクリックします。

   メモ

   ［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。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を許可する場合は、［外部ユーザグループ連携］を有効にしてください。外部ユーザグループ連携の設定方法は、Maintenance Utility の Help の「外部ユーザグループ連携」を参照してください。サーバ構成のテスト方法は、Maintenance Utility の Help の「サーバ構成テスト」を参照してください。
5. テストの結果を確認し［適用］をクリックします。
6. コントローラ 1 の管理ポートとコントローラ 2 の管理ポートが異なるネットワークセグメントに接続されている場合、認証の問い合わせが、外部認証サーバまたは DNS サーバに到達できない可能性があります。

   このようなネットワーク構成の場合は、コントローラ 2 から Maintenance Utility にログインして操作手順 2.と操作手順 4.を行ってください。

3.8.3　無効化

操作手順

1. Maintenance Utility にログインします。
2. ［管理］－［外部認証］－［サーバ設定］－［無効化］を選択します。
3. 確認画面が表示されます。［適用］をクリックします。
4. 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。

3.9　システムモニタ

3.9.1　システムモニタの表示

ストレージシステムの稼働状況を確認できます。

前提条件

- 「1.5.2　管理 PC の要件（8 ページ）」のブラウザ要件を満たしていること。

  本操作は、HA Storage Advisor Embedded のシステムモニタ画面を表示します。このため、HA Storage Advisor Embedded がサポートするブラウザを使用する必要があります。

操作手順

1. Maintenance Utility にログインします。
2. 左下の［メニュー］－［システムモニタ］を選択します。
3. システムモニタ画面が表示されます。稼働状況を確認します。

3.10　初期設定

3.10.1　初期設定ウィザードによる設定変更

初期設定ウィザードを使用すると、システム情報、日時設定、およびネットワーク設定を変更できます。設定が不要な項目はスキップできます。

⚠注意

- 他のユーザがストレージシステムにアクセスしている間は、日時設定の変更ができません。
- SVP を使用している場合は、SVP のシステム日時も更新する必要があります。「A.5　管理サーバ（SVP）の初期設定を行う（187 ページ）」を参照してください。
- 処理が完了していないタスクがある状態で IP アドレスを変更しないでください（タスクの状態確認の方法については、「E.1.9　タスクの状態確認（302 ページ）」を参照してください）。タスクが異常終了する可能性があります。
- SVP を使用している場合は、SVP に登録したストレージシステムの IP アドレスも変更する必要があります。「G.2.5　Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。
- 日時設定画面で設定する NTP サーバを IPv6 で指定する場合、およびネットワーク設定画面で CTL1 と CTL2 の IP アドレスを IPv6 で指定する場合、次の IP アドレスは指定できません。
  - 無効値：[::]
  - ループバックアドレス：[::1]
  - マルチキャストアドレス：[FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF]
  - IPv4 射影アドレス：[::FFFF:(IPv4)]
  - リンクローカルアドレス：[FE80::]
  - グローバルユニキャストアドレス：[2001::]

- グローバルユニキャストアドレス： [2002::]

操作手順

1. Maintenance Utility にログインします。
2. 左下の［メニュー］－［初期設定］を選択します。
3. システム情報設定画面が表示されます。

   変更が不要な場合は［スキップ＞］をクリックします。

   システム情報を変更する場合は、各項目を再設定します。

   システム情報を変更した場合は、設定内容を確認して［適用&次へ＞］をクリックします。
4. 日時設定画面が表示されます。

   変更が不要な場合は［スキップ＞］をクリックします。

   UTC タイムゾーンを変更する場合は、［UTC タイムゾーン］を再設定します。

   NTP サーバを使用する場合は、［同期時刻］に NTP サーバに日時を問い合わせる時間を指定します。

   NTP サーバを使用しない場合は、［日時］に日付と時刻を設定します。

   日時設定を変更した場合は、設定内容を確認して［適用&次へ＞］をクリックします。
5. ネットワーク設定画面が表示されます。各項目を入力します。

   変更が不要な場合は［スキップ＞］をクリックします。

   ネットワーク設定を変更する場合は、各項目を再設定します。

⚠ 注意

- 管理サーバ（SVP）からストレージシステムの CTL1 と CTL 2 にホスト名を使って接続できます（別途、管理サーバ（SVP）の Storage Device List で設定）。

  ホスト名で接続する場合は、ここで設定した CTL1 と CTL2 の IP アドレスを DNS サーバに登録してください。DNS サーバ登録時の注意事項を示します。

  - Maintenance Utility では、DNS サーバを IPv6 で指定できません。
  - CTL1 と CTL2 の IP アドレスに別々のホスト名を割り当ててください。同じホスト名に割り当てると、正常に通信できないおそれがあります。
  - 異なるストレージシステムの CTL の IP アドレスを同じホスト名に割り当てないでください。正常に通信できないおそれがあります。
  - 以下の規則に従ってホスト名を使用してください。
    * ホスト名の最大文字数は 255 文字です。

* 半角英数字と以下の記号を使用できます。なお、半角スペースは使用できません。

  ! $ % - . @ _ ` ~

SVP の Windows に対する設定も必要です。［コントロールパネル］から DNS サフィックスを追加する画面を表示して、CTL1、CTL2 に設定するホストのドメイン名を追加してください（「G.2.21　DNS サフィックスの設定（393 ページ）」参照）。

- プロトコルを IPv4/IPv6 両方に設定した後で、IPv4 のみ（または IPv6 のみ）に切り替えると、ネットワーク設定の参照画面には、IPv4/IPv6 両方の設定値が表示されます。プロトコルの設定を確認するには、参照画面から［ネットワーク設定］をクリックして設定画面を開いてください。設定画面で、プロトコルの選択状態を確認できます。また、設定画面では、無効なプロトコルの IP アドレス情報は淡色表示されます。

各項目の詳細は、Maintenance Utility の Help を参照してください。

ネットワーク設定画面の右下にある［?］をクリックすると Help が表示されます。

ネットワーク設定を変更した場合は、設定内容を確認して［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。

3.11　電源管理

3.11.1　ストレージシステムの電源 ON

ストレージシステムが停止していても、ストレージシステムに給電されている限り、リモートで電源 ON が行えます。

⚠ 注意

- コントローラシャーシのメインスイッチからストレージシステムの電源を OFF にした場合は、リモートからの電源 ON が行えません。

  コントローラシャーシのメインスイッチを使用して電源を ON にしてください。

前提条件

- 電源供給元のブレーカが ON であること
- コントローラシャーシの POWER LED（橙）が点灯していること
- SVP を使用している場合は、SVP が起動していること

操作手順

1. Maintenance Utility にログインします。
2. 左下の［メニュー］－［電源管理］－［ストレージシステム電源 ON］を選択します。
3. 確認画面が表示されます。［適用］をクリックします。
4. 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。

メモ

電源 ON にかかる時間の目安は、『ハードウェア リファレンスガイド』の「ストレージシステムの電源を ON にする」を参照してください。

3.11.2　ストレージシステムの電源 OFF

ストレージシステムの電源を OFF します。

⚠ 注意

CTL の閉塞時は、Maintenance Utility から電源 OFF できません。『ハードウェア リファレンスガイド』の「ストレージシステムの電源を OFF にする」を参照してください。

前提条件

- ストレージシステムへのデータアクセスが停止していること

  ストレージシステム内部のボリュームと、他のストレージシステムのボリュームとの間でペアが作成されていないこと

操作手順

1. Maintenance Utility にログインします。
2. 左下の［メニュー］－［電源管理］－［ストレージシステム電源 OFF］を選択します。
3. 確認画面が表示されます。［適用］をクリックします。
4. パスワード入力画面が表示されます。

   Maintenance Utility にログインしているユーザアカウントのパスワードを入力して、［OK］をクリックします。
5. 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. ストレージシステムの電源が OFF になったことを確認します。

   操作手順 5.のあとにストレージシステムからログアウトしている場合は、再度 Maintenance Utility でストレージシステムにログインします。

   Maintenance Utility の画面左上の表示を確認します。

- 停止している場合：Unknown
- 停止の処理が完了していない場合：Power-off in progress

メモ

電源 OFF にかかる時間の目安は、『ハードウェア リファレンスガイド』の「ストレージシステムの電源を OFF にする」を参照してください。

3.11.3　UPS のモード編集

UPS と連動するためのモードを編集します。

メモ

iStorage V シリーズは、UPS との連動をサポートしていません。

操作手順

1. Maintenance Utility にログインします。
2. 左下の［メニュー］－［電源管理］－［UPS モード編集］を選択します。
3. UPS モード編集画面が表示されます。UPS モードを指定します。
4. 設定内容を確認し［適用］をクリックします。
5. 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。

3.12　システム管理

3.12.1　パスワードの変更

ログインしているユーザアカウントのパスワードを変更します。

⚠ 注意

ログインしているユーザアカウントが、Storage Device List に登録されているストレージシステムに設定されているユーザアカウントと同じ場合の注意点を示します。Maintenance Utility から設定するパスワードと Storage Device List から設定するパスワードを一致させる必要があります。このため操作手順に従ってパスワードを変更してください。パスワードが一致していないと Storage Navigator の操作中に“20122-208003”エラーが発生します。「5.4.3　Storage Navigator 操作時のトラブルシューティング（118 ページ）」を参照して対処してください。

操作手順

1. ［Storage Device List］画面に登録されているストレージシステムのユーザアカウントを確認してください。ストレージシステムに設定されているユーザアカウントのパスワードを変更する場合は、以下の操作を実行してください。その他のユーザアカウントのパスワードを変更する場合は、操作手順 2. に進んでください。

   a. Windows の［スタート］メニューから、［HA Device Manager - Storage Navigator］－［Storage Device List］を右クリックし、［管理者として実行］をクリックします。［管理者として実行］が表示されない場合は、［詳細］または［その他］－［ファイルの場所を開く］をクリックします。開かれたエクスプローラーにあるファイルを右クリックし、［管理者として実行］をクリックします。

   ヒント

   SVP デスクトップ上の［Open StorageDeviceList］アイコンを右クリックして、［管理者として実行］を選択することでも Storage Device List を起動できます。

   b. ［Storage Device List］画面で、ユーザアカウントのパスワードを変更したいストレージシステムを選択して［Stop Service］をクリックします。

   c. ［Stop Service］画面で［Confirm］をクリックします。

2. Maintenance Utility を起動します。
3. 左下の［メニュー］－［システム管理］－［パスワード変更］を選択します。
4. パスワード変更画面が表示されます。パスワードを変更します。
5. ［完了］をクリックします。
6. 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。
7. 確認画面が表示されます。［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。
9. ［Storage Device List］画面に登録されているストレージシステムに設定されているユーザアカウントのパスワードを変更する場合は、以下の操作を実行してください。その他のユーザアカウントのパスワードを変更する場合は不要です。

   a. ［Storage Device List］画面で、ユーザアカウントのパスワードを変更したいストレージシステムを選択して［Edit］をクリックします。

   b. ［Edit System］画面の［User Information］－［Password］に Maintenance Utility で設定した新しいパスワードを入力します。

   c. ［Apply］をクリックします。

   d. ［Start Service］をクリックします。

3.12.2　ログインメッセージの編集

Maintenance Utility のログイン画面に、任意のメッセージ（ログインメッセージ）を表示することができます。ログインメッセージの表示/非表示の選択方法と、ログインメッセージの編集方法について説明します。

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］－［ログインメッセージ編集］を選択します。
3. ログインメッセージ編集画面が表示されます。

   ログインメッセージを編集する場合は、［ログインメッセージ］の［有効］を選択したのち、ログインメッセージを入力します。

   ログインメッセージを表示しない場合は、［ログインメッセージ］の［無効］を選択します。
4. 設定内容を確認し［適用］をクリックします。
5. 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。

3.12.3　暗号化スイートの選択

管理 PC とストレージシステム、および SVP とストレージシステムの通信に使用する暗号化スイートを選択します。

⚠注意

- SVP とストレージシステム間のプロトコルを設定したい場合は SVP での設定も必要になります。
- iStorage V10e で次の暗号スイートのいずれかを選択した場合、必ず SVP の RSA 鍵交換の暗号スイートも有効化してください（「C.26.2　SVP の RSA 鍵交換の暗号スイートを有効化する（273 ページ）」を参照）。
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_CBC_SHA

  また、「TLS_RSA_WITH_AES_128_CBC_SHA および TLS_RSA_WITH_AES_128_CBC_SHA256 を無効にする」を選択した場合、必ず SVP の RSA 鍵交換の暗号スイートも無効化してください（「C.26.1　SVP の RSA 鍵交換の暗号スイートを無効化する（272 ページ）」を参照）。
- 暗号化スイートを選択すると、それに付随して選択できる暗号化スイートが、SSL 通信の接続経路ごとに変わります（詳細は「C.2　ストレージシステムの SSL 通信（245 ページ）」を参照）。

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］－［暗号化スイート選択］を選択します。
3. 暗号化スイート選択画面が表示されます。暗号化スイートを選択します。
4. 設定内容を確認し［適用］をクリックします。
5. 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。

3.12.4　証明書ファイルの更新

［証明書ファイル更新］画面を使って、管理 PC とストレージシステム、および SVP とストレージシステムの SSL 通信に使用する SVP 接続用証明書と 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。

⚠ 注意

- X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される「基本制限(BasicConstraints)」「キー使用法(KeyUsage)」「サブジェクトキー識別子(SubjectKeyIdentifier)」をサポートしています。
- 証明書ファイルは PKCS#12 形式を使用してください。
- PEM 形式のサーバ証明書ファイルと秘密鍵ファイルをお持ちの場合は、PKCS#12 形式に変換してください。また、PKCS#12 形式に変換する前のサーバ証明書ファイルを、SVP に登録してください。
- 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 5 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から、証明書ファイルを指定してください。

管理モデル	選択対象の証明書
HA Storage Advisor Embedded を利用する	［Web サーバ］
Storage Navigator を利用する。	［Web サーバ］および［SVP 接続］

4. 設定内容を確認し［適用］をクリックします。
5. 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。

3.12.5　システムロックの強制解除

システムロック状態になると、管理 GUI から操作ができなくなります。ストレージシステムにエラーが発生していない、また進行中のタスクがないなど、ストレージシステムの動作に問題がない場合は、強制的にシステムロック状態を解除できます。

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］－［システムロック強制解除］を選択します。
3. 確認画面が表示されます。［OK］をクリックします。
4. 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。

3.12.6　GUM のリブート

⚠ 注意

- コントローラボード 1 、コントローラボード 2 の順に、両方のコントローラボードの GUM をリブートしてください。

  両方のコントローラの GUM を同時にリブートすると、管理 PC や SVP との通信が切断したり、アラート通知が上がらなくなります。
- maintenance ユーザ以外のアカウントを使用する場合は、アカウントに "保守（ユーザ）" ロールが付与されていることを確認してください。

  "保守（ユーザ）" ロールは、 "Maintenance User" ユーザグループに含まれています。

  詳細は、「3.2.4　ユーザグループ（36 ページ）」 を参照してください。

操作手順

1. コントローラボード 1 の管理ポートの IP アドレスを指定して Maintenance Utility にログインします。
2. 左下の［メニュー］－［システム管理］－［GUM リブート］を選択します。
3. ［リブート］をクリックします。
4. 警告画面が表示されます。［OK］をクリックします。
5. 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. GUM のリブートが始まります。

ログアウト画面が表示されます。［X］ をクリックして画面を閉じます。

7. Web ブラウザのアドレスバーに GUM をリブートしたコントローラボードの IP アドレスを入力してログインできることを確認します。

メモ

ログインできない場合は、 1～2 分待ってから再度ログインしてください。ログインできるようになるまで、最大で 20 分かかる場合があります。

8. コントローラボード 2 の管理ポートの IP アドレスを指定して Maintenance Utility にログインします。
9. 手順 2～手順 7 を実施して、コントローラボード 2 の GUM をリブートします。

3.12.7　システムダンプのダウンロード

メモ

- 保守員に対して AutoDump が実行されていないことを確認してください。保守用の PC から AutoDump が実行されている状態で本機能を実施すると、ダンプデータが欠落する可能性があります。
- ダウンロードの時間は、15~20 分程度です。（ネットワークの状態、ダウンロードする PC の状態などにより、変わる可能性があります。）

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］－［システムダンプダウンロード］を選択します。
3. 警告画面が表示されます。［OK］をクリックします。
4. 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。
5. 白い画面またはセキュリティ確認画面が表示されます。

⚠ 注意

白い画面またはセキュリティ確認画面は、システムダンプのダウンロードが完了するまで閉じないでください。ダウンロードが失敗する可能性があります。

⚠ 注意

https 接続時に証明書が不正な場合にはセキュリティ確認画面が表示されます。30 秒以内に以下の操作を行ってください。30 秒を過ぎるとシステムダンプをダウンロードできません。操作手順 2.からやり直してください。

＜ Microsoft Edge の場合＞

［詳細設定］－［<IP アドレスまたはホスト名>に進む（安全ではありません）］をクリックしてください。

＜ Google Chrome の場合＞

［詳細設定］－［<IP アドレス>にアクセスする（安全ではありません）］をクリックしてください。

6. 2～3 分待つと、ファイルのダウンロード画面が表示されます。

メモ

- ファイルのダウンロード画面は Maintenance Utility の画面に表示されます。白い画面またはセキュリティ確認画面で Maintenance Utility の画面が隠れている場合は、Maintenance Utility の画面をクリックしてダウンロード画面を確認してください。
- ファイルのダウンロード画面は、ブラウザによって形式が異なります。
- ブラウザの設定によって、ファイルのダウンロード画面が表示されずにファイルのダウンロードを開始する場合があります。

7. ファイルのダウンロード画面で［名前を付けて保存］をクリックします。
8. ダウンロード先およびファイル名を入力して［保存］をクリックします。

ファイル名に装置識別番号を付けることを推奨します。

（例）装置識別番号：934000600001

ファイル名：hdcp_dump_934000600001.dmp

9. ダウンロードの進捗状況を確認します。

メモ

- ダウンロードするファイルは動的に生成されるため、ファイルサイズおよびファイル転送完了予定時間は、不明または非表示となります。
- ファイルのダウンロードが 2～3 分ほど転送されない場合がありますが、ダンプファイル元の CTL を切り替えている時間のため問題ありません。
- ファイルのダウンロード時間は、ネットワークの速度に左右されます。

10. ダウンロードが完了したことを確認します。

メモ

白い画面またはセキュリティ確認画面が残っている場合は手動で閉じてください。

3.12.8　スモールシステムダンプのダウンロード

システムダンプと同様の手順で「スモールシステムダンプ」を選択し採取してください。

3.12.9　構成情報バックアップのダウンロード

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］－［構成情報バックアップダウンロード］を選択します。
3. 構成情報バックアップダウンロード画面が表示されます。

   ［最新のバックアップ］を選択します。
4. 設定内容を確認し［適用］をクリックします。

   バックアップが取得できるようになるまで、1 時間程度かかります。

   バックアップファイルのダウンロードは、数分で終わります。
5. ダウンロードの終了後に［閉じる］をクリックします。

3.12.10　ボリューム状態の参照

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］－［ボリューム状態参照］を選択します。
3. ボリューム状態画面が表示されます。内容を確認し［閉じる］をクリックします。

3.13　アラートの表示

保守員からアラートの確認をお願いする場合があります。依頼があった場合、次の手順を参照してください。

3.13.1　アラート表示

「5.7.1　アラート詳細の確認方法（131 ページ）」を参照してください。

3.13.2　FRU に関するアラート表示

「5.7.1　アラート詳細の確認方法（131 ページ）」を参照してください。

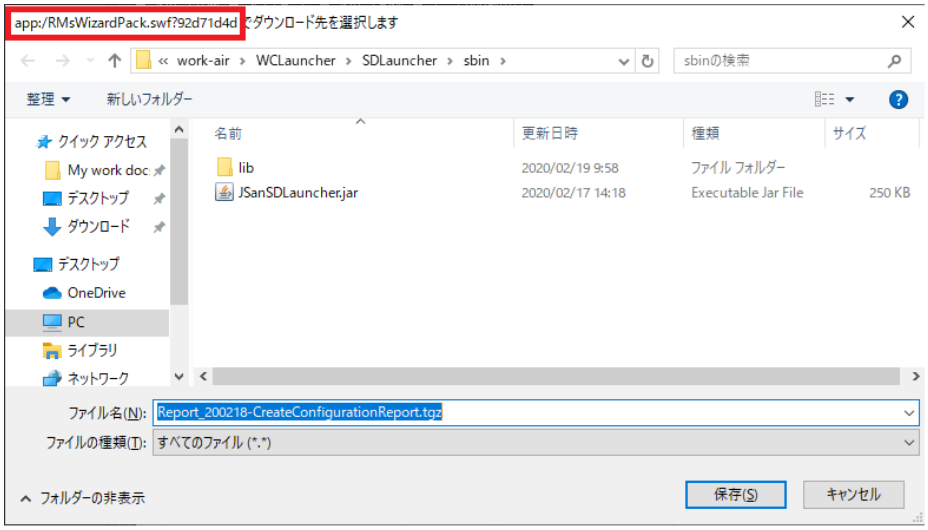
第 4 章
ストレージシステム運用上の注意

ストレージシステムを運用する上で注意が必要な事項を説明します。

4.1　Storage Navigator 使用時の注意

Storage Navigator の使用時は次のことに注意してください。

- Storage Navigator は、Web ブラウザの画面遷移機能をサポートしません。
- Storage Navigator から［作成］、［編集］などをクリックして表示される画面で、“ロード中です。”と画面が表示されたまま変化しなくなる場合があります。この場合、画面右上の［×］（閉じる）をクリックして画面を閉じ、再度 Storage Navigator にログインしてください。
- その他の注意については、『HA Device Manager - Storage Navigator ユーザガイド』を参照してください。
- Adobe AIR 環境で動作する Storage Navigator では、ダウンロード・アップロード等でファイルを選択する画面のタイトルに Adobe AIR 環境に依存する文字列が表示されます。



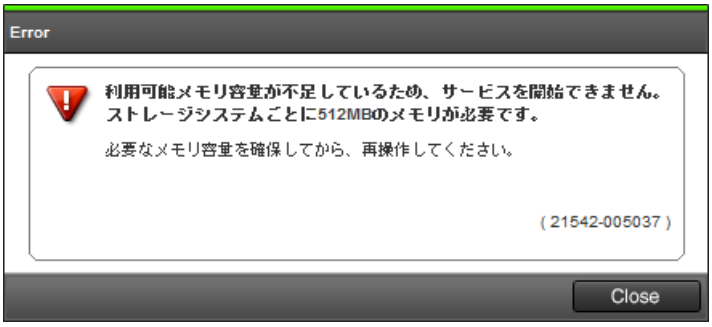
4.2　ストレージシステムのサービスを開始できる台数

SVP は複数台のストレージシステムを登録することができます。ただし、iStorage V100, V300 の場合、1 台の SVP に複数のストレージシステムを登録できません。

また、登録した複数台のストレージシステムのサービスを、同時に開始できます。

ストレージシステムのサービスを開始する場合に、次のメッセージが表示されたときは、目的のストレージシステムのサービスが開始されません。

「G.2.12　ストレージシステムの切り替え（362 ページ）」を参照して、ストレージシステムを切り替えてください。



4.3　ウィルス検出プログラムの使用に関する注意事項

ウィルス検出プログラム※がインストールされた SVP で Storage Navigator を使用する場合は、Storage Navigator の動作に影響することがあります。

このため、ウィルス検出プログラムで次のディレクトリを、リアルタイムのウィルススキャン対象から除外してください。

```
C:\Mapp\wk
```

「C:\Mapp」は、Storage Navigator のインストールディレクトリを示します。 インストールディレクトリに「C:\Mapp」以外を指定した場合は、指定したインストールディレクトリに置き換えてください。

除外したディレクトリに対しても、定期的にウィルススキャンを実施してください。

除外したディレクトリに対してウィルススキャンを実施する場合、事前に下記の操作を行ってください。

- Storage Navigator を使用しない時間を確保
- Storage Device List に登録されている全ストレージシステムのサービスの状態を[Stopped]に変更
- ウィルススキャンの除外設定を解除

ファイアウォール機能をサポートしているセキュリティ対策プログラムを使用する場合は、ファイアウォール通過設定が必要です。設定対象のポート番号は、「A.4.1　ストレージシステムと SVP の IP アドレスを設定する（182 ページ）」の表を参照してください。

注※

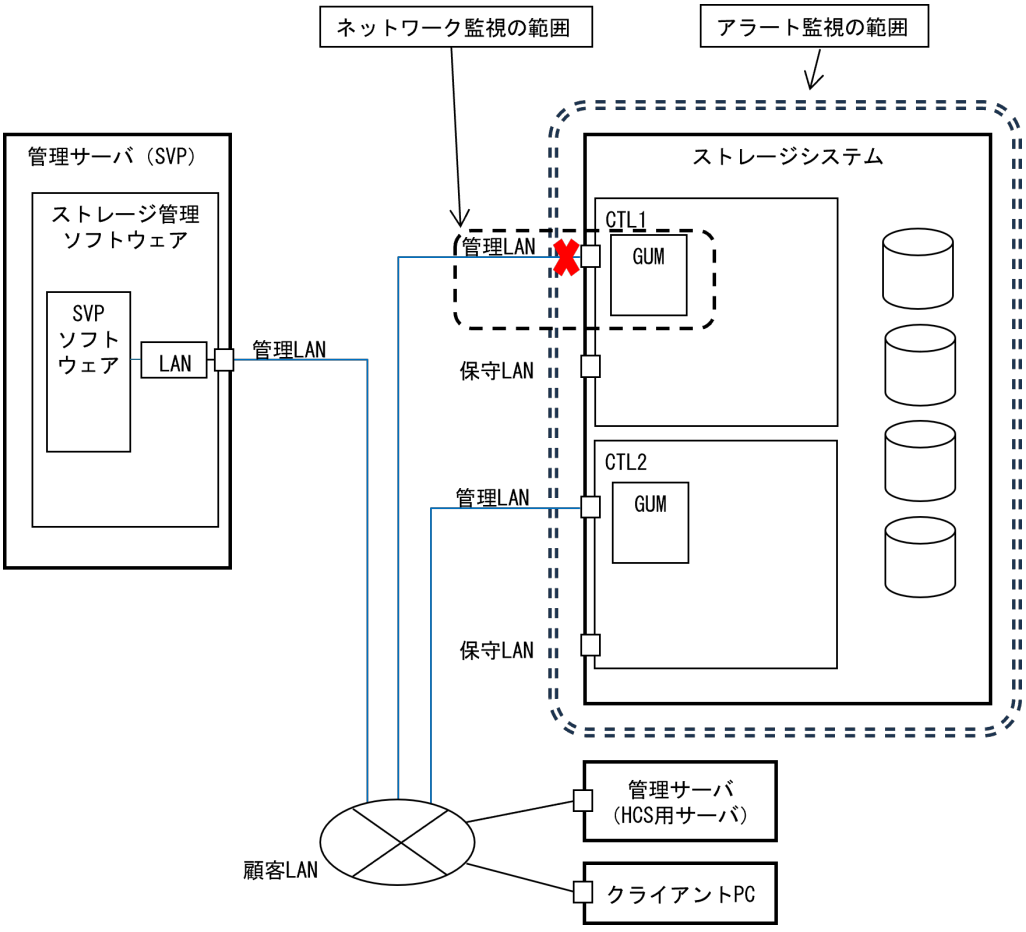
OS 標準でインストールされている Windows Defender などのウィルス検出プログラムも対象となります。

4.4　ストレージシステムに対するネットワーク監視（Ping 応答またはリンクアップ/リンクダウンによる監視）

ストレージシステムの監視手段には、アラート監視とネットワーク監視があります。

アラート監視ではストレージシステム全体の監視が可能ですが、ネットワーク監視では GUM※1 の監視のみ可能であり、コントローラの故障や他部品の故障※2 を監視することはできません。そのため、ストレージシステムの監視には、アラート監視を推奨します。

アラート監視については、「3.3　アラート通知（59 ページ）」を参照してください。



注※1

GUM（Gateway for Unified Management）：ストレージシステムのコントローラ内に実装しており、LAN 通信制御および WEB サーバ機能、SNMP、NTP 機能などを制御します。

コントローラ 1 側が GUM1、コントローラ 2 側が GUM2 の冗長構成となっています。

注※2

コントローラやハードディスクなどの故障・閉塞が発生した場合でも、GUM が停止/閉塞していない場合は、GUM との LAN 通信は可能なため、ネットワーク監視では異常状態にはなりません。

⚠ 注意

GUM は、フェールセーフ機能によりリブートすることがあります。

ネットワーク監視において一時的に異常※として報告された場合であっても、アラート監視でアラート報告がない場合は、GUM リブートによる一時的なネットワークリンクダウンであるため、ネットワークリンクアップ状態回復後の追加対処は不要です。

注※

Linkup/down の検知、ネットワーク通信異常による GUM の停止または Ping 疎通不可など。

ネットワーク監視をする場合は、GUM のリブート時間を考慮して、5 分程度の間に 2 回以上連続して応答がなかった場合に障害と判断してください。

メモ

以下のような場合に、GUM はフェールセーフ機能により自動的にリブートを実施し正常状態に回復します。

- GUM の動作が一時的に不安定な状態となった場合
- MP（マイクロプロセッサ）と GUM の生存監視にて GUM からの応答が一定時間なかった場合

フェールセーフ機能による GUM リブートは、GUM に限定したリブート動作です。GUM リブートによるストレージシステムの業務 I/O 動作への影響はありません。また、SNMP による監視をしている場合は、ColdStart トラップが発行されます。

4.5　電源オフ時間の注意

- 書き込み容量が増加すると、電源オフ状態でのデータ保持期間が短くなり、書かれているデータが読み出せなくなります。
- SSD を搭載している装置は、継続して 3 ヶ月以上電源オフ状態にしないよう注意してください。

  電源オフ状態が 3 ヶ月以上継続したことが障害の要因と判明した場合、保守サービスの対象外となります。

4.6　SVP のデフラグツールに関する注意事項

デフラグツールが実行されている SVP で Storage Navigator を使用すると、Storage Navigator の動作に影響することがあります。このため、デフラグツールを停止したのちに、Storage Navigator を使用してください。

SVP に、デフラグツールのスケジュールが設定されている場合の、スケジュールの停止方法を示します。

操作手順

1. ［スタートメニュー］－［Windows 管理ツール］の［ドライブのデフラグと最適化］を右クリックし、［その他］－［管理者として実行］を選択します。
2. ［はい］をクリックします。
3. デフラグの対象となるドライブを選択します。
4. ［設定の変更］をクリックします。ポップアップ画面が表示されます。
5. ［スケジュールに従って実行する(推奨)］のチェックを外します。
6. ［OK］をクリックします。
7. デフラグの対象となるドライブが複数ある場合は、手順 3～6 を繰り返してください。
8. ［閉じる］をクリックします。

メモ

- Windows 以外のデフラグツールを使用している場合は、当該のデフラグツールも停止してください。
- デフラグツールを使用するアプリケーションが実行されている場合は、当該のアプリケーションも停止してください。

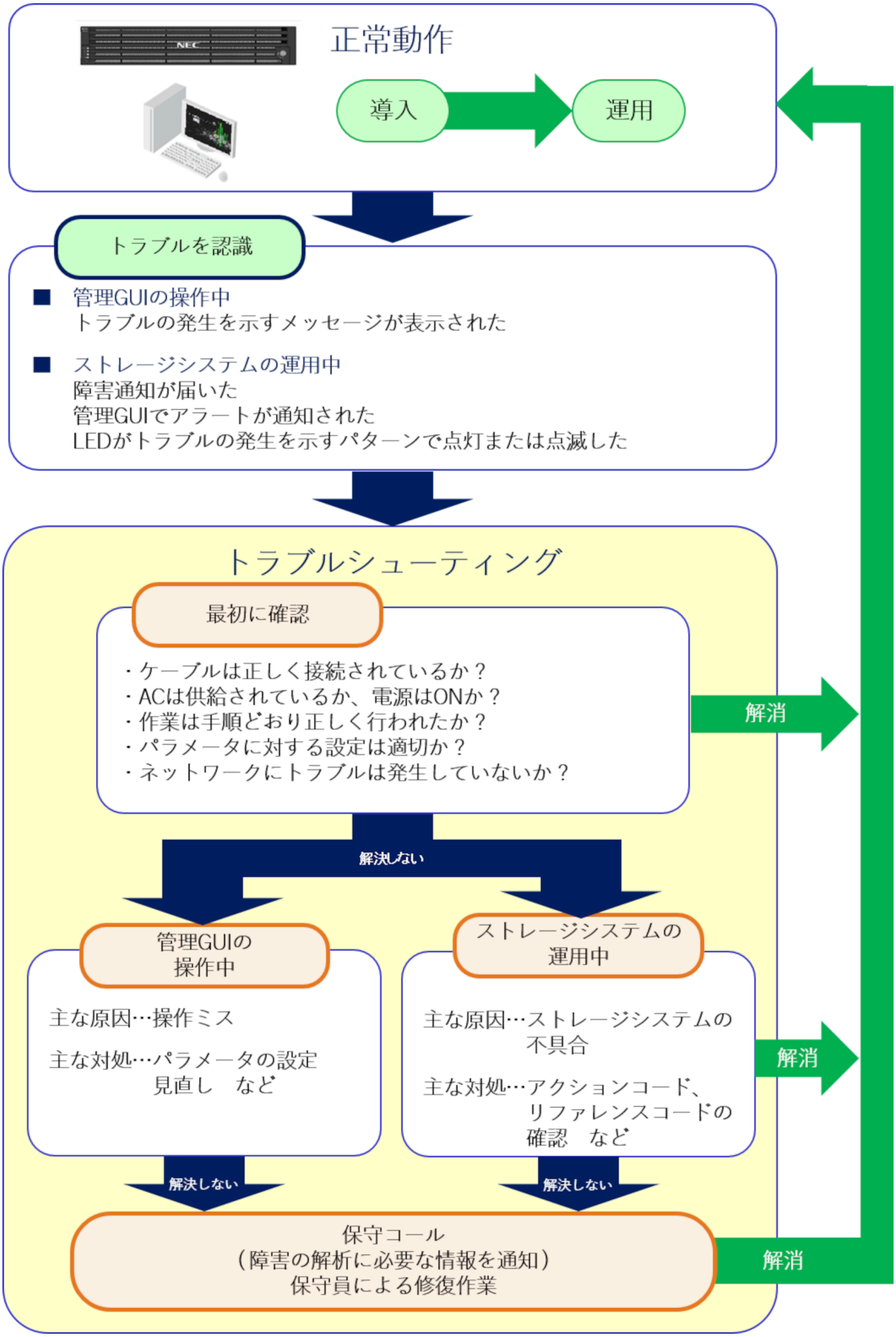
第 5 章
トラブルシュート

ストレージシステムの導入時や運用時にトラブルが発生した場合、その原因を検証し、システムを正常な状態に戻すためにトラブルシューティングを行います。

ストレージシステムに不具合や障害などのトラブルが発生した場合、その状況に応じたトラブルシューティングを行います。

5.1　トラブルの発生からトラブルシューティングまでの流れ

ストレージシステムのトラブルを認識してから、原因の特定と解決をするまでの作業の流れを次に示します。

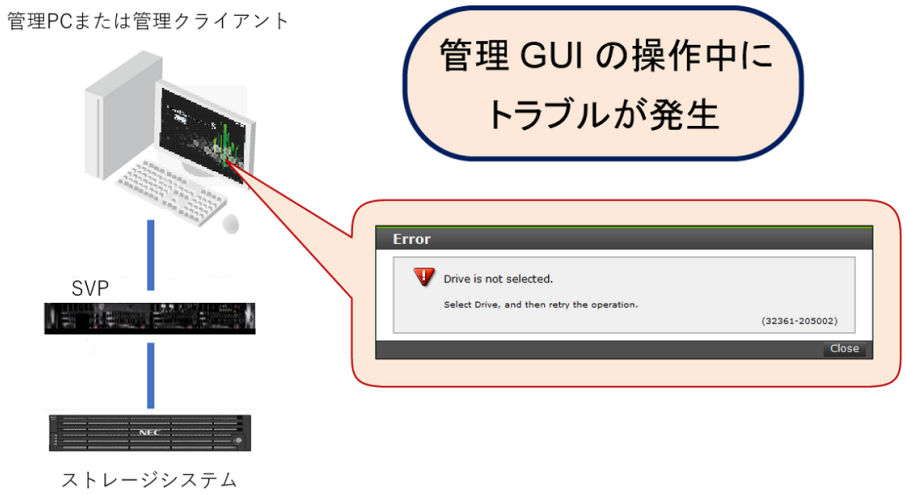

正常動作
導入
運用
トラブルを認識
■ 管理GUIの操作中
トラブルの発生を示すメッセージが表示された
■ ストレージシステムの運用中
障害通知が届いた
管理GUIでアラートが通知された
LEDがトラブルの発生を示すパターンで点灯または点滅した
トラブルシューティング
最初に確認
・ケーブルは正しく接続されているか？
・ACは供給されているか、電源はONか？
・作業は手順どおり正しく行われたか？
・パラメータに対する設定は適切か？
・ネットワークにトラブルは発生していないか？
解消
解決しない
管理GUIの
操作中
主な原因…操作ミス
主な対処…パラメータの設定
見直し　など
ストレージシステムの
運用中
主な原因…ストレージシステムの
不具合
主な対処…アクションコード、
リファレンスコードの
確認　など
解消
解決しない
解決しない
保守コール
（障害の解析に必要な情報を通知）
保守員による修復作業
解消

5.2　トラブルを認識する状況とトラブルシューティング手順の参照先

ストレージ管理者がトラブルを認識する状況は、管理 GUI の操作中、初期構築作業が完了したストレージシステムをホストに認識させるための作業中およびストレージシステムの運用中などです。これらの状況別にトラブルシューティングの参照先を示します。また、トラブルシューティングで利用する機能の参照先も示します。

管理 GUI の操作中にトラブルを認識する場合

初期設定、初期構築などの作業中に発生するトラブルは、主に管理 GUI で設定するパラメータの誤り、あるいは設定漏れに起因しています。



Storage Navigator のインストール途中または操作中にトラブルを認識した場合は、「5.3　トラブルシューティング作業前の確認（105 ページ）」および「5.4　ストレージ管理ソフトウェアおよび SVP ソフトウェアの操作時にトラブルが発生した場合の対処手順（107 ページ）」を参照してください。

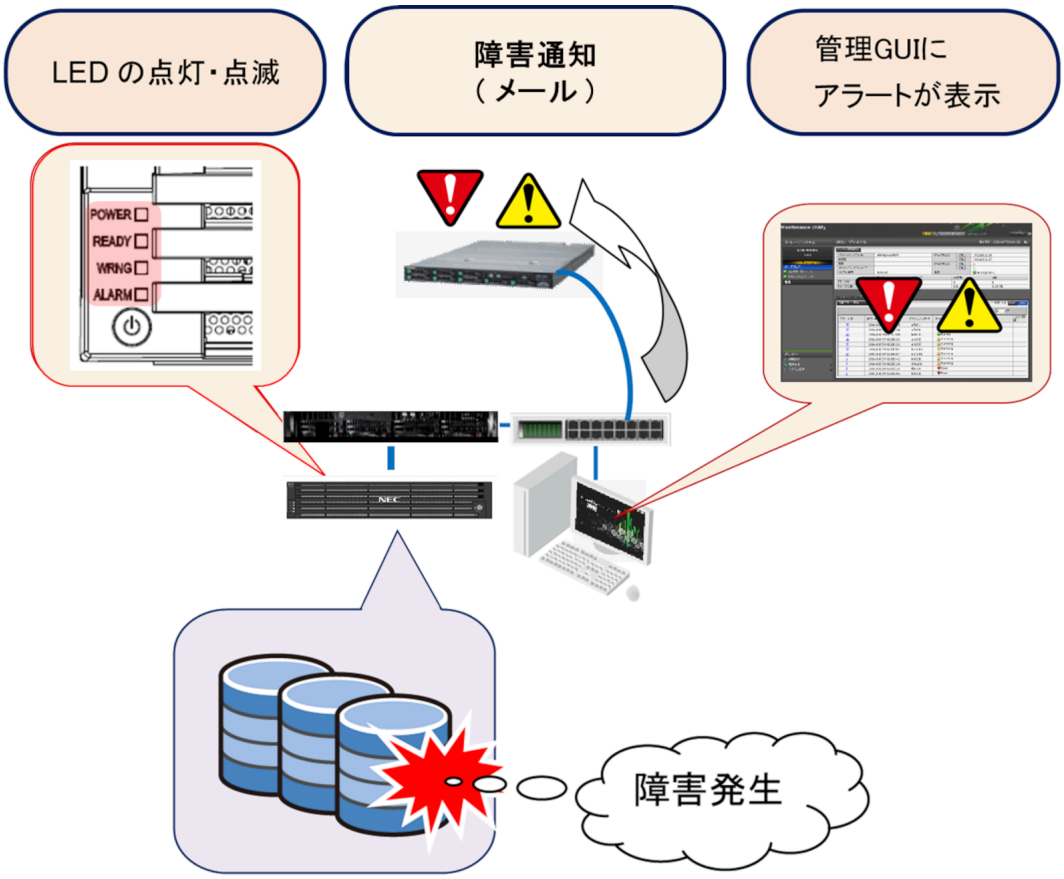
Maintenance Utility の操作中にトラブルを認識した場合は、「5.3　トラブルシューティング作業前の確認（105 ページ）」および「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」を参照してください。

ストレージシステムをホストに認識させる作業中にトラブルを認識する場合

ホストおよびネットワーク周辺機器などの設定作業中にトラブルを認識した場合は、「5.3　トラブルシューティング作業前の確認（105 ページ）」および「5.6　ホストがストレージを認識できない場合の対処手順（127 ページ）」を参照してください。

ストレージシステムの運用中にトラブルを認識する場合

ストレージシステムの運用中にトラブルを認識するための手段は、主に 3 とおりがあります。



- 障害通知によりトラブルを認識する場合

  障害通知を設定すると、管理 GUI から離れていても、メール、Syslog あるいは SNMP によりトラブルの発生を認識することができます。「5.3　トラブルシューティング作業前の確認（105 ページ）」および「5.8　障害通知を受け取った場合の対処手順（137 ページ）」を参照してください。

- 管理 GUI の画面に表示されるアラートによりトラブルを認識する場合

  管理 GUI が起動されていると、トラブルの発生時にアラートが表示されます。「5.3　トラブルシューティング作業前の確認（105 ページ）」および「5.7　管理 GUI でアラートを確認した場合の対処手順（128 ページ）」を参考に、アクションコードと SIM リファレンスコードを特定し、保守員に連絡してください。

- LED の点灯パターンによりトラブルを認識する場合

  ストレージシステムに不具合が発生すると、コントローラシャーシのフロントパネルにある LED が、トラブルの発生を通知します。「5.3　トラブルシューティング作業前の確認（105 ページ）」および『ハードウェア リファレンスガイド』の「LED の点灯パターンによりトラブルを確認した 場合の対処手順」を参照してください。

トラブルシューティングに利用する機能

トラブルシューティングに利用する機能の参照先を示します。

- バックグラウンドサービスログを活用したトラブルシューティング

  バックグラウンドサービスは、Storage Navigator と同時に SVP にインストールされる管理ソフトウェアです。ストレージシステムの状態を常時監視し、動作状況をログファイルに出力します。トラブルシューティングの手がかりとして利用してください。バックグラウンドサービスログを参照してもトラブルが解決しない場合は保守員に連絡してください。トラブルの種類によっては、保守員の依頼によりバックグラウンドサービスログに出力されるトラブルシュートコードを連絡していただく場合があります。 詳細は、「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」を参照してください。

- ダンプファイルの採取によるトラブルシューティング

  保守員からダンプファイルの送付をお願いする場合があります。保守員がダンプファイルを早期に参照することにより、トラブルシューティングに要する時間が短縮される可能性が高まります。ダンプファイルの採取方法は、「3.12.7　システムダンプのダウンロード（93 ページ）」を参照してください。SVP を使用している場合は、「5.11　ダンプファイルの採取方法（163 ページ）」も参照してください。ダンプファイルを自動で採取する方法は、「G.2.15　Log Dump の自動採取（367 ページ）」を参照してください。

メモ

お客様が用意した管理クライアントの本体、SVP の本体、ネットワーク機器などのトラブルは、それぞれのマニュアルを参照してください。

5.3　トラブルシューティング作業前の確認

トラブルシューティングに先立ち、下記のチェックシートに示す項目を確認してください。確認する際トラブルシュートコードが分かっている場合は、「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」の内容を確認してください。

項番	要因	確認項目	チェック欄
1	ケーブルの接続不良	ストレージシステムやネットワーク周辺機器のケーブルが正しく接続されているか※1	
2		ストレージシステムや周辺機器に AC が供給されているか	
3	外部機器の誤動作	ストレージシステムがアクセスするサーバが正常に動作しているか※2	
4		ネットワークにトラブルが発生していないか※3	
5	ストレージシステムの設定不良	作業は正しく手順どおり行ったか※4	
6		パラメータに対する設定は正確か※5	
7	外部機器の設定不良	ストレージシステムがアクセスするサーバの設定は正確か※6	

項番	要因	確認項目	チェック欄
8	SVP の動作が不安定※7	USN ジャーナルの容量を確認 詳細は「5.15　USN ジャーナルの使用容量が不足した場合の対処（174 ページ）」を参照	

注※1

ネットワークケーブル、FC ケーブルのコネクタ抜けなど、単純な事象に起因するトラブルも多くあります。

注※2

ストレージシステムは、複数の外部サーバと連動します。これらの外部サーバが正常に動作していることを確認してください。

注※3

ネットワークに障害が発生するとストレージシステムにも影響が及びます。

注※4

初期設定作業は、「付録 A.　初期設定作業（178 ページ）」の手順に従って設定してください。初期構築作業は、「付録 B.　初期構築作業（221 ページ）」の手順に従って構築してください。正しい手順で設定、構築しないとトラブルの原因となる場合があります。

注※5

初期設定作業あるいは初期構築作業では、管理 GUI のプルダウンメニューから適切な選択肢を選ぶ、あるいはパラメータの入力カラムに値を設定するなどの操作が多くあります。設定を誤るとトラブルにつながる場合もあります。

注※6

ストレージシステムがアクセスするサーバのパラメータに不適切な選択肢を選んだり、誤った値を設定するとトラブルにつながる場合があります。また、ストレージシステムを使用するユーザを、NIS サーバ、LDAP サーバへ登録する必要がある場合もあります。

注※7

次に示すような、不安定な状態が発生します。

- Storage Device List や Storage Navigator が起動できない。
- Storage Device List や Storage Navigator の起動中または操作時に、エラーメッセージが表示される。
- 管理サーバ（SVP）のエクスプローラーでファイルをコピーできない。

5.4　ストレージ管理ソフトウェアおよび SVP ソフトウェアの操作時にトラブルが発生した場合の対処手順

ストレージ管理ソフトウェア、および SVP ソフトウェアのインストール中および操作中にトラブルを認識した場合、次の状況別にトラブルシューティングを行ってください。

- 「5.4.1　ストレージ管理ソフトウェアおよび SVP ソフトウェア インストール時のトラブルシューティング（107 ページ）」
- 「5.4.2　Storage Device List 操作時のトラブルシューティング（111 ページ）」
- 「5.4.3　Storage Navigator 操作時のトラブルシューティング（118 ページ）」

上記のトラブルシューティングで、操作画面に表示されるメッセージだけでは対処方法が特定できない場合、「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」を参照してください。

トラブルシューティングを行ってもトラブルが解消しない場合や、対処方法の記載がないトラブルに関しては、保守員に連絡してください。トラブルの状況と、エラーメッセージの表示があればそのメッセージ番号を保守員に伝えてください。

5.4.1　ストレージ管理ソフトウェアおよび SVP ソフトウェア インストール時のトラブルシューティング

項番	障害内容	対処方法
1	インストールが失敗し、メッセージが表示された。	「表 1-5　SVP のハードウェア条件（19 ページ）」および「表 1-6　SVP に必要なソフトウェア（21 ページ）」を満たす機器にインストールしてください。
2	インストールの成功が表示されたが、Storage Device List が起動しない、またはストレージシステムを登録できない。	「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」を参照して、ストレージ管理ソフトウェアのバックグラウンドサービスの状態を確認して対処してください。 「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照して、ダンプファイルを採取してください。 ダンプツールを使用して採取することはできません。
3	ストレージ管理ソフトウェア、および SVP ソフトウェアのファイルを Windows エクスプローラーなどから直接フォルダ（例:C:\Mapp）を削除してしまった。	次の手順でストレージ管理ソフトウェア、および SVP ソフトウェアを再度インストールしてください。 1. インストールされていたストレージ管理ソフトウェア、および SVP ソフトウェアのバージョンを確認し、同一バージョンの SVP ファームウェアメディアを用意してください。 2. 上記メディアで、ストレージ管理ソフトウェア、および SVP ソフトウェアを再度インストールしてください（「A.6　管理サーバ（SVP）に必要なソフトウェアをインストールする（191 ページ）」参照）。
4	インストール中に“(21443-200026)”が発生した。	• SVP にインストールされている RAID Manager を使用している場合は、RAID Manager を停止してから、再度インストールしてください。停止方法は「5.16　RAID Manager の停止手順（176 ページ）」を参照してください。（再度インストールすると、RAID Manager は自動で起動されます。）

項番	障害内容	対処方法
		• RAID Manager が未インストールまたは、RAID Manager を停止後、再度インストールしても問題が解決しない場合は、ポート番号キー名「RestAPIServerStop」のポート番号が、他のソフトウェアのポート番号と重複している可能性があります。次の手順を実施してください。 1. 「RestAPIServerStop」のポート番号が、他のアプリケーションのポート番号と重複していないか確認してください（「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照）。 2. ポート番号が重複している場合、「RestAPIServerStop」のポート番号、または重複しているソフトウェアのポート番号を変更してください(「RestAPIServerStop」のポート番号を参照する場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照)。 3. 再度インストールしてください。
5	インストールが“(21443-200027) エラー”により失敗し、エラー詳細コードが“1060”または“1072”と表示された。	• ストレージ管理ソフトウェア、および SVP ソフトウェアを一旦アンインストールして、再度インストールしてください（「A.6　管理サーバ（SVP）に必要なソフトウェアをインストールする（191 ページ）」参照）。 • 繰り返し発生する場合は、SVP を再起動したあと、ストレージ管理ソフトウェア、および SVP ソフトウェアを一旦アンインストールして、再度インストールしてください。 • 上記を実施しても問題が解決しない場合は、以下の情報を保守員へ送付してください。 - SVP の Windows イベントログ（システムと Application）※1 - SVP のサービスの一覧※2 - C:\SetupTrace フォルダ内の全ファイル
6	SVP ソフトウェアの更新時に“(21542-005016) エラー”が発生した。	イベントビューアーが起動している場合は、イベントビューアーを終了したのちに、再度 SVP ソフトウェアを更新してください。 それでも解決しない場合、下記の方法で"BackSvc.exe"、もしくは"FrontSvc.exe"のプロセスが存在するか確認してください。 • Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022 の場合 タスクマネージャを起動して詳細タブ画面で表示項目（例：名前）を右クリックして「列の選択」をクリックする。列の選択ウィンドウで「イメージパス名」にチェックをつけて［OK］ボタンをクリックし、「イメージパス名」を確認してください。 存在する場合、Windows のコマンドプロンプトを管理者権限で起動して下記を実行してください。 sc stop HtBack sc stop HtFront 上記を実行したのちに、再度 SVP ソフトウェアを更新してください。上記を実行した場合は、必ず Windows のコマンドプロンプトを管理者権限で起動して下記を実行してください。 sc start HtFront sc start HtBack それでも解決しない場合は、下記の方法で"Astcmd.exe"、もしくは"Astnet.exe"のプロセスが存在するか確認してください。

項番	障害内容	対処方法
		• Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022 の場合 タスクマネージャを起動して詳細タブ画面で「名前」を確認してください。 存在する場合、当該プロセスを強制終了したのちに、再度 SVP ソフトウェアを更新してください。 それでも解決しない場合は、下記の方法で SVP ソフトウェアのインストール先フォルダ(例 : C:\Mapp)を含むプロセスが存在するか確認してください。 • Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022 の場合 タスクマネージャを起動して詳細タブ画面で表示項目(例：名前)を右クリックして「列の選択」をクリックする。列の選択ウィンドウで「イメージパス名」にチェックをつけて[OK]ボタンをクリックし、「イメージパス名」を確認する。 存在する場合、当該プロセスを強制終了したのちに、再度 SVP ソフトウェアを更新してください。
7	ストレージシステムの登録、もしくは、SVP ソフトウェアの更新時に、“(21542-005024) エラー”または“(21542-005040) エラー”が発生した。	ソフトウェアインストール用ファイルが壊れている可能性があります。 メディアからコピーしたファイルで実行している場合、正しくコピーされていない可能性があります。コピーしたファイルがコピー元と相違がないかを確認してから、再操作してください。この問題が再発するときは、直接ソフトウェアインストール用メディアを使用し、再操作してください。
8	ストレージシステムの登録、もしくは、SVP ソフトウェアの更新時に、“(21542-005012) エラー”が発生した。	「表 1-5　SVP のハードウェア条件 (19 ページ)」および「表 1-6　SVP に必要なソフトウェア (21 ページ)」を満たしていることを確認してください。 条件を満たしている場合、インストールしている機器に一時的もしくは継続的になんらかの問題が起きている可能性があります。インストールしている機器に問題が起きていないか、イベントログ等にて確認し、問題を解決した後に再度操作してください。
9	ストレージ管理ソフトウェアの削除時に“(21443-005017) エラー”が発生した。	イベントビューアーが起動している場合は、イベントビューアーを終了したのちに、再度ストレージ管理ソフトウェアを削除してください。 それでも解決しない場合、下記の方法で"BackSvc.exe"、もしくは"FrontSvc.exe"のプロセスが存在するか確認してください。 • Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022 の場合 タスクマネージャを起動して詳細タブ画面で「名前」を確認してください。 存在する場合、Windows のコマンドプロンプトを管理者権限で起動して下記を実行してください。 sc stop HtBack sc stop HtFront 上記を実行したのちに、再度ストレージ管理ソフトウェアを削除してください。上記を実行した場合は、必ず Windows のコマンドプロンプトを管理者権限で起動して下記を実行してください。 sc start HtFront sc start HtBack

項番	障害内容	対処方法
		それでも解決しない場合は、下記の方法で"Astcmd.exe"、もしくは"Astnet.exe"のプロセスが存在するか確認してください。 • Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022 の場合 タスクマネージャを起動して詳細タブ画面で「名前」を確認してください。 存在する場合、当該プロセスを強制終了したのちに、再度ストレージ管理ソフトウェアを削除してください。 それでも解決しない場合は、下記の方法でストレージ管理ソフトウェアのインストール先フォルダ(例 : C:\Mapp)を含むプロセスが存在するか確認してください。 • Windows 10、Windows 11、Windows Server 2016、Windows Server 2019、Windows Server 2022 の場合 タスクマネージャを起動して詳細タブ画面で表示項目(例 : 名前)を右クリックして「列の選択」をクリックする。列の選択ウィンドウで「イメージパス名」にチェックをつけて[OK]ボタンをクリックし、「イメージパス名」を確認する。 存在する場合、当該プロセスを強制終了したのちに、再度ストレージ管理ソフトウェアを削除してください。
10	ストレージ管理ソフトウェア、または SVP ソフトウェアの更新時、もしくは削除時に“(21443-200017) エラー”が発生した。	• コマンドプロンプトが起動中、かつコマンドプロンプトのカレントディレクトリのフォルダが削除対象の場合に発生します。 コマンドプロンプトのカレントディレクトリを削除対象外のフォルダに移動するか、もしくはコマンドプロンプトを閉じてください。その後、再度ストレージ管理ソフトウェアを削除してください。 再度、削除を実施した際に、ストレージ管理ソフトウェア、または SVP ソフトウェアがインストールされていない旨のメッセージが出力されることがあります。以下のどちらかを実施してください。 - インストールし直す為に削除した場合 1. エクスプローラーから、ストレージ管理ソフトウェア、および SVP ソフトウェアのインストール先フォルダを削除します。 2. ストレージ管理ソフトウェア、および SVP ソフトウェアをインストールします。 - 不要となって削除した場合 1. エクスプローラーから、ストレージ管理ソフトウェア、および SVP ソフトウェアのインストール先フォルダを削除します。 2. ストレージ管理ソフトウェア、および SVP ソフトウェアをインストールします。 3. ストレージ管理ソフトウェア、および SVP ソフトウェアを削除します。 • OS のファイルシステムに一時的な異常などが発生すると、ファイルの削除処理が異常終了する場合があります。 SVP を再起動し（「G.1.3　SVP を再起動する（315 ページ）」を参照）、ストレージ管理ソフトウェア、および SVP ソフトウェアをインストールしてください。そのあと、再度ストレージ管理ソフトウェア、および SVP ソフトウェアを削除してください。

項番	障害内容	対処方法
12	ストレージ管理ソフトウェアの更新時に“(21443-200051）エラー ”が発生した。	SVP 上で次のプログラムが起動している場合は、プログラムを終了してから、再度ストレージ管理ソフトウェアを更新してください。 プログラム名と終了方法を示します。 • Storage Navigator のサブ画面：画面を閉じます。 • Storage Navigator：画面を閉じます。

注※1

コントロールパネルの［管理ツール］または［Windows ツール］－［イベントビューアー］で、［Windows ログ］の［システム］を選択し、メニューの［操作］－［すべてのイベントを名前をつけて保存］を選択してください（OS 種類によって操作が異なることがあります)。

次に［Windows ログ］の［Application］を選択し、メニューの［操作］－［すべてのイベントを名前をつけて保存］を選択してください。

注※2

コントロールパネルの［管理ツール］または［Windows ツール］－［サービス]で、［サービス］画面を起動してください（OS 種類によって操作が異なることがあります)。［操作(A)］－［一覧のエクスポート(L)...］でサービスの一覧を出力してください。

5.4.2　Storage Device List 操作時のトラブルシューティング

メモ

- 次の表に掲載されていないメッセージは、<SVP のインストールディレクトリ>\wk\supervisor\sdlist\help\sdl_message_ja.html を参照してください。

項番	メッセージ番号	障害内容	対処方法
1	21041-006004	“Add system”画面で［Apply］をクリックしたが、“(21041-006004）エラー”が発生して装置アイコンの作成ができない。	下記の項目を実施して、再実行してください。 • SVP のインストール先ドライブの空き容量が、20GB 以上ある事を確認してください。 • ウィルス検出プログラム（Windows Defender も対象）のサービスを停止していることを確認してください。 • SVP ファームウェアメディアを SVP 上にコピーして行っている場合、再度メディアからコピーしなおしてください。 • SVP のインストールドライブ装置に物理的な破損やアクセスエラーなどの問題が無いか確認してください。
2	21041-007006 または	“Add system”画面で［Apply］をクリックしたが、“(21041-007006）エラー”、または	SVP とストレージシステムの接続が失敗しています。 下記の項目を確認してください。 • ストレージシステムが起動しているか • 管理 LAN が正常に動作しているか

項番	メッセージ番号	障害内容	対処方法
	21041-007008	“(21041-007008) エラー”が発生した。	• Storage Device List で設定したユーザー名とパスワードが正しいか • ストレージシステムの IP アドレス、またはホスト名 起動中のストレージシステムが管理 LAN に接続されていない状態で、装置のアイコンを作成したい場合、[Manual] を選択して必要な項目を入力してください。
3	21041-007018	[Edit] をクリックしたが、“(21041-007018) エラー”が発生し、ストレージシステムの情報が変更できない。	StorageDeviceList を管理者権限で起動していない可能性があります。 • StorageDeviceList を終了して、管理者権限で起動してください。 • Storage Device List を管理者権限で起動してもエラーが発生する場合、SVP を再起動し、再度 Storage Device List を管理者権限で起動してください。
4	21041-007019	[Start Service]、または[Stop Service] をクリックしたが、“(21041-007019) エラー”が発生した。 または、StorageDeviceList からストレージシステムを削除できない。	StorageDeviceList を管理者権限で起動していない可能性があります。 • StorageDeviceList を終了して、管理者権限で起動してください。 • Storage Device List を管理者権限で起動してもエラーが発生する場合、SVP を再起動し、再度 Storage Device List を管理者権限で起動してください。
5	21542-005003	[Add System] 画面または [Edit System] 画面で [Apply] をクリックしたときに、“(21542-005003) エラー”が発生した。	IP アドレスを入力した場合、異なる IP アドレスを入力してください。 ホスト名を入力した場合、DNS サーバによって名前解決された IP アドレスが重複しています。 DNS サーバの設定を確認してください。
6	21542-005011	[Add System] 画面で [Apply] をクリックしたが、“(21542-005011) エラー”が発生して装置アイコンが作成されない。	インストールに必要なドライブ容量が不足しています。 インストールするドライブに 20GB 以上の空き容量を確保してください。
7	21542-005012	[Add System] 画面で [Apply] をクリックしたが、“(21542-005012) エラー”が発生して装置アイコンが作成されない。 [Edit System] 画面で [Apply] をクリックしたが、“(21542-005012) エラー”が発生して SVP ソフトウェアの更新ができない。	「表 1-5　SVP のハードウェア条件 (19 ページ)」を満たしていることを確認してください。 条件を満たしている場合、インストールしている機器に一時的もしくは継続的になんらかの問題が起きている可能性があります。インストールしている機器に問題が起きていないか、イベントログ等にて確認し、問題を解決した後に再度操作してください。
8	21542-005014	ストレージシステムの削除時に“(21542-005014) エラー”が発生した。	1. イベントビューアーが起動している場合は、イベントビューアーを終了してください。 2. 削除するストレージシステムの装置識別番号と同じ名称のフォルダ、およびその配下のフォルダやファイルに対して、フォルダを開く、ファイルを開く、コマンドプロンプトのカレントディレクトリを移動するなどの操作をしている場合は、操作を終了してください。 3. 再度ストレージシステムを削除してください。

項番	メッセージ番号	障害内容	対処方法
9	21542-005019	［Start Service］をクリックしたが、“(21542-005019) エラー”のメッセージが表示されサービスが開始されない。	複数のサービスを同時には起動できません。 起動中のサービスを停止してください。
10	21542-005024	［Add System］画面で［Apply］をクリックしたが、“(21542-005024) エラー”が発生して装置アイコンが作成されない。 ［Edit System］画面で［Apply］をクリックしたが、“(21542-005024) エラー”が発生して SVP ソフトウェアの更新ができない。	ソフトウェアインストール用ファイルが壊れている可能性があります。 メディアからコピーしたファイルで実行している場合、正しくコピーされていない可能性があります。コピーしたファイルがコピー元と相違がないかを確認してから、再操作してください。この問題が再発するときは、直接ソフトウェアインストール用メディアを使用し、再操作してください。
11	21542-005026	［Start Service］をクリックしたが、“(21542-005026) エラー”が発生して、サービスの開始ができない。	SVP の IP アドレスに無効な値が設定されています。 ［Storage Device List］画面右上［SVP IP Address］をクリックし、［Change SVP IP Address］から SVP の IP アドレスを設定してください（「G.2.2　SVP の IP アドレスを変更（331 ページ）」を参照）。 その後、再度［Start Service］をクリックしてください。
12		装置アイコンの［Start Service］が"Auto"の状態で SVP を再起動したところ、装置アイコンに［Error］が表示された。 ［Error］をクリックすると"BASE"の"Status"に“(21542-005026) エラー”が表示された。	SVP の IP アドレスに無効な値が設定されています。 ［Storage Device List］画面右上［SVP IP Address］をクリックし、［Change SVP IP Address］から SVP の IP アドレスを設定してください（「G.2.2　SVP の IP アドレスを変更（331 ページ）」を参照）。 その後、［Start Service］をクリックしてください。
13		Storage Navigator を起動後、"Please wait... Storage Navigator is loading."の画面※1 が表示されたままで、ログインできない。	• SVP の IP アドレスを変更した場合、Storage Device List に変更後の IP アドレスが反映されていない可能性があります。［Storage Device List］画面右上［SVP IP Address］をクリックし、［Change SVP IP Address］から SVP の IP アドレスを設定してください（「G.2.2　SVP の IP アドレスを変更（331 ページ）」を参照）。その後、再度［Start Service］をクリックしてください。 なお、管理 LAN に接続している LAN ポートの IP アドレス（Storage Device List に表示されている IP アドレス）以外の LAN ポートの IP アドレスを変更した場合も、「G.2.2　SVP の IP アドレスを変更（331 ページ）」の操作を行ってください。ただし、操作手順 3. で IP アドレスを入力しなおす必要はありません。操作手順 4.に進み、［Apply］をクリックしてください。 • SVP が 2 台以上接続されている可能性があります。1 台のストレージシステムに同時に接続できる SVP は 1 台です。他に接続されている SVP が存在する場合は切断してください。その後にお使いの SVP を再起動してください。 他に接続されている SVP が存在しない場合は、Maintenance Utility から GUM リブートを実施してください（「3.12.6　GUM のリブート（92 ページ）」参

項番	メッセージ番号	障害内容	対処方法
			照）。GUM をリブートしてから、お使いの SVP を再起動してください。
14	21542-005028	［Stop Service］をクリックしたが、“21542-005028”が表示された。	Storage Device List から選択したストレージシステムが、他の管理者（保守員を含む）により操作されている場合に表示されます。 次のことを確認してから、再操作してください。 • 他の管理者（保守員を含む）による操作が完了していること • すべての Storage Navigator の設定画面が閉じられていること 上記以外の場合は、「3.12.5　システムロックの強制解除 (92 ページ)」を参照し、システムロックを強制解除してから、再操作してください。
15	21542-005037	［Start Service］をクリックしたが、“(21542-005037) エラー”が発生して、サービスの開始ができない。	SVP のメモリが不足している可能性があります。 「1.6.2.1　SVP のハードウェア条件（19 ページ)」に示すメモリを搭載してください。
16	21542-005040	［Add System］画面で［Apply］をクリックしたが、“(21542-005040) エラー”が発生して装置アイコンが作成されない。 ［Edit System］画面で［Apply］をクリックしたが、“(21542-005040) エラー”が発生して SVP ソフトウェアの更新ができない。	ソフトウェアインストール用ファイルが壊れている可能性があります。 メディアからコピーしたファイルで実行している場合、正しくコピーされていない可能性があります。コピーしたファイルがコピー元と相違がないかを確認してから、再操作してください。この問題が再発するときは、直接ソフトウェアインストール用メディアを使用し、再操作してください。
17	21542-005050	装置アイコンの作成で［Apply］ボタンをクリックしたが、“(21542-005050) エラー”が発生して装置アイコンの作成ができない。	装置登録に必要な OSS がインストールされていないため、装置登録が失敗しました。 以下の項目のいずれかを実施してください。 • 装置登録を行う際に使用した SVP ファームウェアメディアを使用して、ストレージ管理ソフトウェアを更新インストール、および装置登録を行ってください。 • ストレージ管理ソフトウェア、および SVP ソフトウェアをアンインストールしてください。その後、装置登録を行う際に使用した SVP ファームウェアメディアを使用して、ストレージ管理ソフトウェアを新規インストール、および装置登録を行ってください。 • 下記に示すバージョンの SVP ファームウェアメディアを使用して装置登録を行ってください。 - 登録装置が iStorage V10e の場合：88-08-15-x0/00 以降 - 登録装置が iStorage V100, V300 の場合：93-06-で始まる場合は 93-06-85-x0/00 以降、93-07-で始まる場合は 93-07-22-x0/00 以降
18	21542-008001	装置アイコンに［Warning］が表示された。［Warning］をクリックすると、"Status"に	左記のエラーコードが発生しているサービスで、処理のタイムアウトが発生しました。

項番	メッセージ番号	障害内容	対処方法
		“21542-008001”が表示された。	繰り返し発生する場合、「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」を参照し、該当する対処方法を実施してください。 ［Warning］または［Error］の表示と同時にバックグラウンドサービスが本トラブルに関するログを出力しています。 バックグラウンドサービスログが存在しない、または対処方法を実施しても現象が改善しない場合、サービスを停止させるか、SVP をリブートしてください。
19	21542-008002	装置アイコンに［Warning］（または［Error］）が表示された。［Warning］（または［Error］）をクリックすると、"Status"に“21542-008002”が表示された。	左記のエラーコードが発生しているサービスでエラーが発生しました。 「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」を参照し、該当する対処方法を実施してください。 ［Warning］または［Error］の表示と同時にバックグラウンドサービスが本トラブルに関するログを出力しています。 バックグラウンドサービスログが存在しない、または対処方法を実施しても現象が改善しない場合、サービスを停止させるか、SVP をリブートしてください。
20	21041-006002	装置アイコンをクリックしたところ“（21041-006002）エラー”が発生して Storage Navigator が開始されない。	デフォルトの Web ブラウザが設定されていません。 インストールされている Web ブラウザの設定からデフォルトの Web ブラウザ（または既定の Web ブラウザ）に設定した後、再実行してください。
21	21041-006005	Storage Device List の起動時に、“（21041-006005）エラー”が発生して起動に失敗した。	Supervisor サービス（DKCMan/MAPPAppServer/MAPPWebServer）との通信に失敗しています。 「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」を参照して、ストレージ管理ソフトウェアのバックグラウンドサービスの状態を確認して対処してください。 それでも解決しない場合は、Windows のスタートメニューより、［コントロールパネル］－［システムとセキュリティ］－［管理ツール］または［Windows ツール］－［サービス］を選択し、DKCMan、MAPPAppServer、および MAPPWebServer の状態が“開始”となっていることを確認した後、Storage Device List を管理者権限で再起動してください。 “開始”になっていない場合は、サービス名を右クリックして、［開始］を実行するか、［プロパティ］から［スタートアップの種類］を［自動］に変更して SVP を再起動してください（「G.1.3　SVP を再起動する（315 ページ）」参照）。
22		Storage Device List の起動中に、“（21041-006005）エラー”が発生して起動に失敗した。	SVP で使用するサービスの再起動を伴う操作をしている場合は、このエラーが表示されても問題ありません。その操作が完了するまでお待ちください。操作の正常終了を確認した後、エラーメッセージ画面の［Close］をクリックしてください。再起動を伴う操作をしていない場合は、項番 19 の対処方法に従ってください。
23	21513-008004	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に	使用する装置に対してすでに他の SVP が接続されています。 通信サービスのログのトラブルシュートコード TRCOMM000004 に記載されている IP アドレスの PC

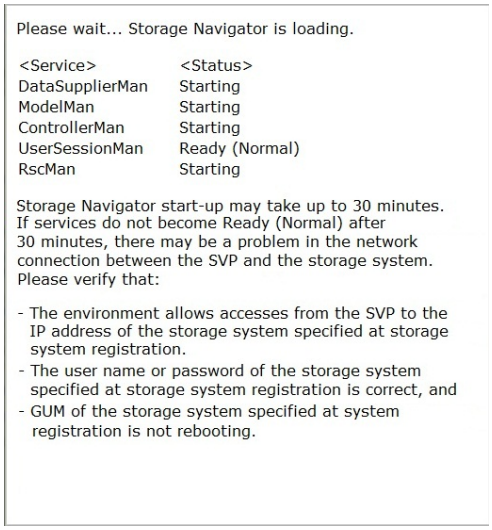
項番	メッセージ番号	障害内容	対処方法
		“21513-008004”が表示された。	で起動しているストレージシステムのサービスを停止させてください。
24	21513-008005	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に“21513-008005”が表示された。	［Add System］画面で設定した CTL ごとの IP Address と、GUM に設定されている CTL 番号が不一致です。 Storage Device List で CTL ごとの IP Address 設定を修正してください。
25	21513-008006	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に“21513-008006”が表示された。	［Add System］画面で設定した装置モデルと、ストレージシステムに設定されている装置モデルが不一致です。 Storage Device List で装置を一旦削除して、正しい装置モデルで再登録してください。
26	21513-008007	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に“21513-008007”が表示された。	［Add System］画面で設定した Config 型式と、ストレージシステムにインストールされている Config 型式が不一致です。 Storage Device List で装置を一旦削除して、 正しい Config 型式で再登録してください。
27	21513-008008	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に“21513-008008”が表示された。	［Add System］画面で設定した装置製番と、ストレージシステムに設定されている装置製番が不一致です。 Storage Device List で装置を一旦削除して、正しい装置製番で再登録してください。
28	21513-008009	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に“21513-008009”が表示された。	［Add System］画面で設定したユーザー名称とパスワードが誤っている可能性があります。 Storage Device List でユーザー名称とパスワードを再設定してください。
29	21513-008011	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に“21513-008011”が表示された。	情報更新に失敗しました。 自動で再実行されますが、表示後 5 分ほど待っても消去されない場合は、Storage Device List で該当の装置を選択し、停止を行ったあとに起動してください。 それでも回復しない場合は、SVP を再起動してください。
30	21513-008012	装置アイコンに［Warning］が表示された。 ［Warning］をクリックすると、"Status"に“21513-008012”が表示された。	使用する装置に対して既に他の SVP が接続されている可能性があります。 使用する装置に対して、他のストレージシステムのサービス起動している PC がないか確認してください。既にストレージシステムのサービスが起動済みの SVP があればサービスを停止させてください。
31	-	Storage Device List の画面でストレージシステムをクリックしたが、Storage Navigator のログイン画面が表示されない	StorageDeviceList を管理者権限で起動していない可能性があります。 • StorageDeviceList を終了して、管理者権限で起動してください。 • Storage Device List を管理者権限で起動してもエラーが発生する場合、SVP を再起動し、再度 Storage Device List を管理者権限で起動してください。

項番	メッセージ番号	障害内容	対処方法
32	-	［Start Service］をクリックした後、20 分以上待っても、“Processing”から”Ready”に変わらない。	該当装置の Storage Navigator に必要な Java のバージョンがインストールされているか確認してください。 必要な Java がインストールされていない場合は、以下の手順に従ってください。 1. SVP をリブートします。 2. ストレージ管理ソフトウェアと SVP ソフトウェアを削除します（「G.2.10　ストレージ管理ソフトウェア、および SVP ソフトウェアの削除（アンインストール）（360 ページ）」を参照）。 3. ストレージ管理ソフトウェアと SVP ソフトウェアを一旦アンインストールして、再度インストールします（「A.6　管理サーバ（SVP）に必要なソフトウェアをインストールする（191 ページ）」を参照）。 4. Storage Device List にストレージシステムを登録します。 5. ストレージシステムに対応するサービスを開始します。
33	-	ストレージシステムの削除に失敗し、Storage Device List が起動しなくなった。	1. Windows のブラウザなどを使用して、削除するストレージシステムの装置識別番号と同じ名称のフォルダを削除してください。 例えば、装置識別番号が 934000600001 の場合は以下のフォルダを削除します。 <installDir>\wk\934000600001 2. SVP を再起動してください。
34	-	正しいユーザ名とパスワードを入力しているがログインできない。	以下の原因が考えられます。 • 管理者がユーザアカウントを無効化している。 ユーザアカウントポリシーを設定している場合は、以下の原因が考えられます。 • パスワード有効期限切れにより、アカウントが無効化された。 • ログイン試行可能回数を超えたため、アカウントが無効化された。 • ログイン試行可能回数を超えたため、アカウントがロックされた。 • 初回ログインである。 • API 認証などで自動的に認証を行っている場合にログイン試行回数に達したため、アカウントがロックまたは無効化された。 以下の対処が必要です。 セキュリティ管理者（参照・編集）ロールを持つユーザと連携し、原因に応じて、以下の対応を実施してください。 • アカウントがロックされている場合は、「3.2.8.8　アカウントロックの解除（53 ページ）」を参照して、アカウントロックを解除してください。 • アカウントが無効化されてる場合は、「3.2.8.9　アカウントの有効化（53 ページ）」を参照して、アカウントを有効化してください。 - パスワード有効期限切れの場合は、パスワードの変更も実施してください。

項番	メッセージ番号	障害内容	対処方法
			• 初回ログインで失敗している場合は、以下の対処を実施してください。 - 該当ユーザの初回ログイン時パスワード変更要求を無効にする（「3.2.8.2　ユーザアカウントのパスワードポリシー設定（44 ページ）」参照）。 - Maintenance Utility で、初回ログインを該当ユーザのアカウントで実施する。

注※1

画面例：



5.4.3　Storage Navigator 操作時のトラブルシューティング

項番	障害内容	対処方法
1	装置登録成功後、操作中に何らかのエラーが発生した。または、ハングアップした。	「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」を参照して、Storage Navigator のバックグラウンドサービスの状態を確認して対処してください。バックグラウンドサービスに障害が発生していない場合は、項番 2 以降に従い対処してください。 保守ポートを使用している場合は、保守ポートの状態異常が原因で、管理ポートに接続した SVP に通信障害が発生している可能性があります。保守ポートのネットワーク状態を確認してください。 対処をしても障害が解消しない場合は、「5.11.1　ダンプツールを使用した採取（163 ページ）」を参照して、ダンプファイルを採取し、保守員に送付してください。 採取に失敗した場合は、「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照して、手動で該当するファイルを採取してください。

項番	障害内容	対処方法
2	登録装置のサービスを止めずに登録しているユーザアカウント情報を変更したため、Storage Navigator の操作中に“20122-208003”エラーが発生した。	Storage Device List で、登録装置の［Stop Service］を実行してください。その後、［Edit］をクリックして、有効なユーザアカウント情報に登録し直してから、［Start Service］を実行してください。
3	Storage Navigator の操作中に［Unable to launch application］と表示されている［Application Error］画面が表示された。	1. ［Application Error］画面の［OK］をクリックします。 2. Storage Navigator から、［Application Error］画面が表示される直前の操作を行ってください。 3. 再度［Application Error］画面が表示された場合は、下記の操作手順 4. 以降に従い Java コンソールの画面のコピーを採取して、保守員にお渡しください。 保守員が Java コンソールの画面のコピーを早期に参照することにより、トラブルシューティングに要する時間が短縮される可能性が高まります。 4. ［Application Error］画面の［OK］をクリックします。 5. Java コンソールの表示を設定します。 SVP の Windows 画面で［スタート］－［コントロールパネル］－［Java］を選択し、［Java コントロール・パネル］を表示します。 6. ［詳細］タブを選択します。 7. ［Java コンソール］の［コンソールを表示する］を選択して、［OK］、または［了解］をクリックします。 8. Storage Navigator から、［Application Error］画面が表示される直前の操作を行ってください。 Java コンソールが表示されます。 9. ［Application Error］画面が表示されたら、［Java コンソール］の［コピー］をクリックします。 ［Application Error］画面が表示されない場合は、Storage Navigator が正常に動作しています。操作手順 13. 以降に従い［Java コンソール］を閉じてください。 10. テキストエディタなどを起動して、コピーしたテキストを貼り付けます。 11. テキストファイルを保存します。 12. ［Application Error］画面の［OK］をクリックします。 13. ［コントロールパネル］－［Java］を選択し、［Java コントロール・パネル］を表示します。 14. ［詳細］タブを選択します。 15. ［Java コンソール］の［コンソールを表示しない］を選択して、［OK］、または［了解］をクリックします。

項番	障害内容	対処方法
		16.［コントロールパネル］画面を閉じます。
4	Web Console Launcher のメッセージとして、［Unable to launch application］と表示されている［Application Error］画面が表示された。	C:\Mapp\wk\supervisor\WCLauncher\log のフォルダをコピーして、保守員にお渡しください。 「C:\Mapp」は、Web Console Launcher のインストールディレクトリを示します。 インストールディレクトリに「C:\Mapp」以外を指定した場合は、指定したインストールディレクトリに置き換えてください。
5	Storage Device List に登録されているストレージシステムのサービスが起動と停止を繰り返す。	「4.3　ウィルス検出プログラムの使用に関する注意事項（97 ページ）」と「A.8　デスクトップヒープの指定値を変更する（206 ページ）」を参照し、ウィルス検出プログラムの設定とデスクトップヒープの指定値を変更してください。 設定変更後に、Storage Device List の該当装置のサービスを停止してから、再度起動してください。 上記を実施しても回復しない場合は、「5.11　ダンプファイルの採取方法（163 ページ）」を参照してダンプを採取したあと、保守員に連絡してください。
6	Storage Navigator のサブ画面を起動するときに、ファイルを開くプログラムを選択するためのダイアログボックスが表示される。	ダイアログボックスを閉じて、「G.2.16　Log Dump Ex Tool 画面の操作（373 ページ）」に示す手順を実施してから、再度操作してください。
7	Storage Navigator で登録したタスクが「実行待ち」の状態から「実行中」に進まない。	Storage Navigator で複数のタスクを連続して登録すると、後から登録したタスクが「実行待ち」の状態となる場合があります。 「実行待ち」のタスクがある状態で、下記の操作や障害により、SVP とストレージシステム間の通信ができない状態になると、ストレージシステムにシステムロックが発生します。 • SVP をシャットダウンした • SVP を管理 LAN から外した • 管理 LAN に障害が発生した その後、SVP とストレージシステム間の通信ができる状態に戻しても、システムロックによりタスクが「実行待ち」の状態から進まなくなります。 この場合、Maintenance Utility でシステムロックを解除してください。（「3.12.5　システムロックの強制解除（92 ページ）」参照）
8	Storage Navigator の操作中に、下記に示すいずれかのトラブルが発生した。 • Storage Navigator にログインしようとしたが、[20121-107022]エラーが発生した。 • Storage Navigator の操作中に、[20121-107097]エラーが発生した。 • Storage Navigator の操作中に、Loading 状態からフリーズした。 • Storage Navigator の操作中に、ブラウザに 503(Service Unavailable)が表示され、Storage Navigator の画面が表示されなくなった。	Storage Device List から該当の装置を選択し、サービスを停止してから再度起動してください。 トラブルが再発する場合は、「G.2.20.1　Jetty 定期リブートの設定（390 ページ）」を参照して Jetty の定期リブート設定を有効にしてください。

項番	障害内容	対処方法
9	Storage Navigator の動作が遅い。	• SVP がハードウェア条件を満たしているか確認してください（「1.6.2.1　SVP のハードウェア条件（19 ページ）」を参照）。 • SVP でウィルス検出プログラムが動作していないか確認してください（「4.3　ウィルス検出プログラムの使用に関する注意事項（97 ページ）」参照）。 • SVP でデフラグツールが動作していないか確認してください（「4.6　SVP のデフラグツールに関する注意事項（100 ページ）」参照）。
10	Storage Navigator にログインしようとしたが、「the capacity of memory is insufficient to login」が表示されログインに失敗する。	SVP に環境変数の_JAVA_OPTIONS が設定されている場合は削除してください。
11	ユーザアカウントを削除する際に、“00222 107010 内部論理矛盾が発生したため、処理を継続できません。”というエラー画面が表示された。	Storage Navigator の画面から当該のユーザアカウントが削除されている場合は、Maintenance Utility で、CTL1 と CTL2 の GUM をリブートしてください（「3.12.6　GUM のリブート（92 ページ）」参照）。
12	次の操作を行うと、 Microsoft Edge が起動した後に、HTTP エラーの 404 が発生、または画面に何も表示されなかった。 • Storage Navigator のサブ画面を表示 • Storage Navigator メニューから［ツール］-［ダウンロード］画面を表示	Web ブラウザのデフォルトが Internet Explorer の SVP に、110.0 以降の Microsoft Edge がインストールされている場合に発生します（Internet Explorer の起動時に、Microsoft Edge へリダイレクトされる機能が影響）。 デフォルトの Web ブラウザを Microsoft Edge に変更してください。
13	その他の障害	障害の内容に対応する『HA Device Manager - Storage Navigator ユーザガイド』の以下の章を参照し、対処してください。 •「Storage Navigator のログインエラーと対策」 •「Storage Navigator の異常終了、応答なし(ハングアップ)エラーと対策」 •「Storage Navigator の画面の表示に関するエラーと対策」 •「Storage Navigator のそのほかのエラーと対策」 •「Storage Navigator サブ画面でのトラブルシューティング」

上記以外の障害が発生した場合は、SVP が「1.6.2.2　管理サーバ（SVP）に必要なソフトウェア（21 ページ）」に示す要件を満たしているか、確認してください。

5.4.4　ストレージ管理ソフトウェアおよび SVP ソフトウェアの操作時に発生するその他の障害

項番	障害内容	対処方法
1	SVP の操作中に、"情報の損失を防ぐためにプログラムを終了してください"と、警告メッセージが表示された。	SVP をリブートしてください。

5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順

Maintenance Utility の操作中にトラブルを認識した場合、下記の表を参照し、トラブルシューティングを行ってください。トラブルシューティングを行ってもトラブルが解消しない場合、保守員に連絡してトラブルの状況を伝えてください。

分類	障害内容	対処方法
ネットワーク設定	• Maintenance Utility に接続できない。	• ストレージシステムを、ホスト名で登録している場合、SVP の Windows に設定が必要です。DNS サフィックスに、CTL1、CTL2 に設定しているホストのドメイン名を追加してください「G.2.21　DNS サフィックスの設定（393 ページ）」を参照。 • ネットワーク設定で指定した IP アドレスがストレージシステムのネットワーク環境に合っていない、または次の IP アドレスが設定された可能性があります。ネットワーク設定で指定した IP アドレスを保守員へ連絡してください。 - 無効値： [::] - ループバックアドレス： [::1] - マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF] - IPv4 射影アドレス： [::FFFF:(IPv4)] - リンクローカルアドレス： [FE80::] - グローバルユニキャストアドレス： [2001::] - グローバルユニキャストアドレス： [2002::]
	• メールサーバへのテストメールの送信が失敗する。 • Syslog サーバへのテストメッセージの送信が失敗する。 • SNMP マネージャへのテスト SNMP トラップの送信が失敗する。 • NTP サーバを使用した日時設定に失敗する。	次に示す項目を確認してください。不具合が確認された場合は訂正してください。 • 送信先（メールサーバ、Syslog サーバ、SNMP マネージャ、または NTP サーバ）の IP アドレスを確認してください。 • 送信先をホスト名で指定する場合、Maintenance Utility のネットワーク設定で、DNS サーバが設定されているか確認してください（「3.5　ネットワーク設定（71 ページ）」を参照）。 • DNS サーバに送信先のホスト名が登録されているか確認してください。
ネットワーク障害	• Maintenance Utility に接続できない。 • Maintenance Utility の操作中に 32061-204002 エラーが発生する。	LAN ケーブルが抜けていないか確認してください。LAN ケーブルが抜けている場合は、ケーブルを接続してから操作を再開します。
	• メールサーバへのテストメールの送信が失敗する。 • Syslog サーバへのテストメッセージの送信が失敗する。	次に示す項目を確認してください。不具合が確認された場合は訂正、または交換してください。 • 送信先（メールサーバ、Syslog サーバ、SNMP マネージャ、または NTP サーバ）が動作しているか確認してください。 • 送信先の IP アドレスおよびホスト名を確認してください。 • 送信先とストレージシステム間で、ネットワークの疎通を確認してください。

分類	障害内容	対処方法
	• SNMP マネージャへのテスト SNMP トラップの送信が失敗する。 • パスワード期限切れ通知が失敗する。 SIM コード 7c1000、または 7c2000 が発生した。※3 • NTP サーバを使用した日時設定に失敗する。	• 送信先とストレージシステム間に存在するルータやスイッチなどのネットワーク機器が正常に動作しているか確認してください。 • 送信先とストレージシステムのみ存在するネットワーク機器にファイアウォールが設定されている場合、ファイアウォールの設定内容を確認してください。 • LAN ケーブルに不具合が無いか確認してください。
JavaScript のセキュリティ対策	Maintenance Utility 画面が開いた後、1 分以上経過しても画面が真っ白なままになっている。	次の手順で信頼済みサイトに Maintenance Utility 画面を追加してから、再度、Maintenance Utility 画面を開きます。 ＜ Microsoft Edge の場合＞ 1. Windows 画面で［スタート］－［Windows システムツール］－［コントロールパネル］－［ネットワークとインターネット］－［インターネットオプション］を選択します。 2. ［セキュリティ］タブを選択します。 3. ［信頼済みサイト］－［サイト］をクリックします。 4. ［このゾーンのサイトにはすべてサーバーの確認（https:）を必要とする］のチェックを外します。 5. ［この Web サイトをゾーンに追加する］に CTL#1 の IP アドレスを入力し、［追加］をクリックして、［閉じる］をクリックします。 6. 同様に、CTL#2 の IP アドレスも追加します。 7. ［インターネットのプロパティ］画面に戻ったら、［OK］をクリックして画面を閉じます。 ＜ Google Chrome の場合＞ 1. Windows 画面で［スタート］－［Windows システムツール］－［コントロールパネル］－［ネットワークとインターネット］－［インターネットオプション］を選択します。 2. ［セキュリティ］タブを選択します。 3. ［信頼済みサイト］－［サイト］をクリックします。 4. ［このゾーンのサイトにはすべてサーバーの確認 （https:） を必要とする］のチェックを外します。 5. ［この Web サイトをゾーンに追加する］に CTL1 の IP アドレスを入力し、［追加］をクリックして、［閉じる］をクリックします。※1 6. 同様に、CTL2 の IP アドレスも追加します。※1 7. ［インターネットのプロパティ］画面に戻ったら、［OK］をクリックして画面を閉じます。
Web ブラウザキャッシュクリア	• Maintenance Utility 画面へのログインに失敗する。 • Maintenance Utility 画面が開いた後、1 分以上経過しても画面が真っ白な	Web ブラウザのキャッシュをクリアしてから、再度 Maintenance Utility 画面を開きます。

分類	障害内容	対処方法
	ままになっている。	
Web ブラウザ表示	Web ブラウザ表示に不具合がある。 例 • Web ブラウザ内のボタンがグレーアウトのためクリックできない • 表示されない項目がある	ブラウザを再起動してください。
	システムモニタを起動しても、次のメッセージが表示され、Loading 状態でフリーズする。 "This page cannot be opened because Internet Explorer is no longer supported. Please use a supported browser."	GUM のファームウェアバージョンが下記の場合は、Internet Explorer 11 を使用できません。Microsoft Edge を使用してください。 • iStorage V100, V300 の場合：93-06-81/00 以降 • iStorage V10e の場合：全バージョン
強制再読み込み	Maintenance Utility 画面の画像が正しく表示されない。	Web ブラウザの強制再読み込みを実施します。 1. Maintenance Utility からログアウトします。 2. Ctrl キーと F5 キーを同時に押し、強制再読み込をします。
ネットワーク	Maintenance Utility 画面操作中に画面が固まったままになっている。	装置のネットワークを確認してください。その後、ログインし直してください。 “システムロック中”と表示されている場合は［システムロック中］をクリックし、ロックを解除してください。
Smart Screen フィルター機能	ボタンをクリック後に同じ画面が複数表示される。	＜ Microsoft Edge の場合＞ 次の手順でセキュリティを設定してから、再度、Maintenance Utility 画面を開きます。 1. 画面右上の［設定など］から［設定］－［プライバシー、検索、サービス］を選択します。 2. ［セキュリティ］の［Microsoft Defender SmartScreen］を無効にします。 ＜ Google Chrome の場合＞ 次の手順でプライバシーを設定してから、再度、Maintenance Utility 画面を開きます。 1. Web ブラウザ上部のメニューから「設定」を選択します。 2. ［詳細設定を表示］をクリックします。 3. ［プライバシー］－［危険なサイトからユーザとデバイスを保護する］のチェックを外します。
レイアウト	Maintenance Utility 画面で入力設定後に画面の表示内容が乱れる。	スラッシュ（/）を連続して入力設定する場合に、画面が乱れます。このまま Maintenance Utility を利用しても問題ありません。
ファームウェア更新	ファームウェア更新画面の起動時に、次のいずれかのエラーが発生する。	「A.7　管理サーバ (SVP) にストレージシステムを登録する (199 ページ)」で障害が発生した場合は、ツールを終了し、「A.7　管理サーバ (SVP) にストレージシステムを登録する (199 ページ)」で再度作業を実施してください。

分類	障害内容	対処方法
画面起動失敗	• Web ブラウザに、“このページは表示できません”というエラー画面が表示される。 • アプリケーション・エラーが表示される。	Maintenance Utility からファームウェア更新で発生した場合は、エラー画面を閉じたあと、再度ファームウェア更新を実行してください。
ファームウェア更新画面起動失敗	ファームウェア更新画面の起動時に、次のいずれかの画面が表示されてファームウェア交換ができない。 • (32061-208061、33361-203116) • (30162-205057、33361-203116) 「ファームウェア更新中です。」	システムロックを強制解除して、再度ファームウェアを更新してください（「3.12.5　システムロックの強制解除（92 ページ）」参照）。 なお、Maintenance Utility 画面の右上のステータスに、「システム未ロック」と表示されていても、システムロックの強制解除は可能です。
ファームウェア更新画面起動時のファイルのダウンロード要求	ファームウェア更新画面の起動時に、.wclr ファイルの保存に関するメッセージが表示される。	＜ Microsoft Edge の場合＞ 「この種類のファイルはデバイスに損害を与える可能性があるため、<ファイル名>.wclr はブロックされました。」と表示される場合があります。このメッセージが表示されたら、［その他のアクション］－［保存］をクリックして対象のファイルを保存してください。 ＜ Google Chrome の場合＞ 「この種類のファイルはコンピュータに損害を与える可能性があるため、<ファイル名>.wclr はブロックされました。」と表示される場合があります。このメッセージが表示されたら、［その他のアクション］－［保存］をクリックして対象のファイルを保存してください。
Syslog 設定の失敗	アラート通知、または監査ログを蓄積するための Syslog の設定をする際に、“34062-203102 ストレージシステムがビジーです。”というエラー画面が表示された。	この現象は、Storage Navigator による管理が行われている際（Storage Navigator のサービスが［Ready］の状態）に発生します。 エラー画面に表示されている対処方法を実施後、再度設定してください。 上記を実施しても問題が解決しない場合は、次のいずれかを実施後、再度設定してください。 • Storage Navigator のサービスを停止したのち、再度開始する。 • SVP をリブートする。
Application Error の発生	［Unable to launch application］と表示されている［Application Error］画面が表示された。	1. ［Application Error］画面の［OK］をクリックします。 2. Maintenance Utility から、［Application Error］画面が表示される直前の操作を行ってください。 3. 再度［Application Error］画面が表示された場合は、下記の操作手順 4. 以降に従い Java コンソールの画面のコピーを採取して、保守員にお渡しください。 保守員が Java コンソールの画面のコピーを早期に参照することにより、トラブルシューティングに要する時間が短縮される可能性が高まります。 4. ［Application Error］画面の［OK］をクリックします。 5. Java コンソールの表示を設定します。 SVP の Windows 画面で［スタート］－［コントロールパネル］－［Java］を選択し、［Java コントロール・パネル］を表示します。

分類	障害内容	対処方法
		6. ［詳細］タブを選択します。 7. ［Java コンソール］の［コンソールを表示する］を選択して、［OK］、または［了解］をクリックします。 8. Maintenance Utility から、［Application Error］画面が表示される直前の操作を行ってください。 Java コンソールが表示されます。 9. ［Application Error］画面が表示されたら、［Java コンソール］の［コピー］をクリックします。 ［Application Error］画面が表示されない場合は、Maintenance Utility が正常に動作しています。操作手順 13. 以降に従い［Java コンソール］を閉じてください。 10. テキストエディタなどを起動して、コピーしたテキストを貼り付けます。 11. テキストファイルを保存します。 12. ［Application Error］画面の［OK］をクリックします。 13. ［コントロールパネル］－［Java］を選択し、［Java コントロール・パネル］を表示します。 14. ［詳細］タブを選択します。 15. ［Java コンソール］の［コンソールを表示しない］を選択して、［OK］、または［了解］をクリックします。 16. ［コントロールパネル］画面を閉じます。
操作抑制	Maintenance Utility を操作しようとすると、Web ブラウザに、“他のユーザが操作中のため操作できません。しばらくしてから、再操作してください。”という画面が表示される。	Maintenance Utility が、他の管理者（保守員を含む）により操作されている場合に表示されます。 次のことを確認してから、再操作してください。 • 他の管理者（保守員を含む）による操作が完了していること • Storage Navigator を利用して管理している場合、すべての Storage Navigator の設定画面が閉じられていること 上記以外の場合は、「3.12.5　システムロックの強制解除 (92 ページ)」を参照し、システムロックを強制解除してから、再操作してください。
システムモニタの表示	システムモニタの表示中にエラーメッセージが表示され、モニタリングが停止した。	• エラーメッセージで指摘されている設定内容を確認して、不具合がある場合は修正したのちに、システムモニタの表示を再度実行してください。 • 上記の操作を行っても、エラーメッセージが繰り返し表示される場合は、システムモニタを表示させている CTL の GUM をリブートしてください（「3.12.6　GUM のリブート (92 ページ)」を参照）。
ユーザアカウントの管理	ユーザアカウントを削除する際に、“30662 203050 ストレージシステムの内部処理でエラーが発生しました。”というエラー画面が表示された。	Maintenance Utility の画面から当該のユーザアカウントが削除されている場合は、Maintenance Utility で、CTL1 と CTL2 の GUM をリブートしてください（「3.12.6　GUM のリブート (92 ページ)」参照）。
ログイン	正しいユーザ名とパスワードを入力しているがログインできない。	以下の原因が考えられます。 • 管理者がユーザアカウントを無効化している。 ユーザアカウントポリシーを設定している場合は、以下の原因が考えられます。 • パスワード有効期限切れにより、アカウントが無効化された。 • ログイン試行可能回数を超えたため、アカウントが無効化された。

分類	障害内容	対処方法
		• ログイン試行可能回数を超えたため、アカウントがロックされた。 • API 認証などで自動的に認証を行っている場合にログイン試行回数に達したため、アカウントがロックまたはアカウントが無効化された。 以下の対処が必要です。 セキュリティ管理者（参照・編集）ロールを持つユーザと連携し、原因に応じて、以下の対応を実施してください。 • アカウントがロックされている場合は、「3.2.8.8　アカウントロックの解除（53 ページ）」を参照して、アカウントロックを解除してください。 • アカウントが無効化されてる場合は、「3.2.8.9　アカウントの有効化（53 ページ）」を参照して、アカウントを有効化してください。 - パスワード有効期限切れの場合は、パスワードの変更も実施してください。
パスワード	パスワード変更に失敗する。	パスワードポリシーに違反している可能性が考えられます。 「3.2.8.2　ユーザアカウントのパスワードポリシー設定（44 ページ）」を参照して、パスワードポリシーに準ずるパスワードを設定してください。

注※1

CTL1/CTL2 の IP アドレスは、Storage Device List 画面のアイコンまたは、Storage Navigator のストレージシステム情報に表示されています。

注※2

追加時に［セキュリティ警告－HTTP ロケーション］が表示された場合、［続行］をクリックします。

注※3

GUM のファームウェアバージョンが以下の場合、SIM コードは 7c1000 となります。

- iStorage V100, V300 の場合：93-07-24/00 未満
- iStorage V10e の場合：88-08-18/00 未満

GUM のファームウェアバージョンが以下の場合、SIM コードは 7c2000 となります。

- iStorage V100, V300 の場合：93-07-24/00 以降
- iStorage V10e の場合：88-08-18/00 以降

5.6　ホストがストレージを認識できない場合の対処手順

ホストからストレージシステムを認識できない、または認識しなくなった場合の主な原因と、その対処手順を説明します。

トラブルの原因が iSCSI にあると推定された場合は、「H.2.6　iSCSI に関するトラブルシューティング（403 ページ）」を参照してください。

- ホストに障害が発生している場合の現象、主な要因および対処手順

項番	現象	主な原因	対処手順
1	HBA、NIC または CNA のリンクアップランプが消灯	Fibre Channel ケーブルまたは iSCSI ケーブルの取り付け不良	ケーブルのコネクタに付いているラッチ（ツメ）を確実にフックしてください。
2		HBA、NIC または CNA とホストのコネクタの接続不良	HBA、NIC または CNA をホストのコネクタから外し、再度差し込んでください。
3		HBA、NIC または CNA が故障	ホスト側で HBA、NIC または CNA の状態を確認してください。 故障が確認された場合は交換してください。
4	BIOS または EFI の設定画面にストレージシステムのポートに設定されている WWN が非表示	ストレージシステムまたはネットワーク周辺機器の電源が OFF	ホストの電源 ON より前に、ストレージシステムおよびネットワーク周辺機器（スイッチなど）の電源を ON にしてください。
5	外見上は異常なし	HBA、NIC または CNA のファームウェアが非対応	• HBA、NIC または CNA のファームウェアを更新してください。 • iSCSI 接続の場合、iSCSI に対応した NIC または CNA を使用してください。

- ネットワーク周辺機器に障害が発生している場合の現象、主な要因および対処手順

項番	現象	主な原因	対処手順
1	ネットワーク周辺機器のランプがすべて消灯	ネットワーク周辺機器の電源が OFF	ネットワーク周辺機器の電源を ON にしてください。
2	ホストとスイッチ間のケーブルまたはストレージとスイッチ間のケーブルのコネクタが挿入されているポートのリンクアップランプが消灯	FC ケーブルまたは iSCSI ケーブルの取り付け不良	ケーブルのコネクタに付いているラッチ（ツメ）を確実にフックしてください。
3	外見上は異常なし	ゾーニングの設定不良または VLAN の設定不良	• FC 接続の場合は、ゾーニング設定を見直してください。 • iSCSI 接続の場合は、VLAN 設定を見直してください。

5.7　管理 GUI でアラートを確認した場合の対処手順

管理 GUI でアラートを確認した場合、Maintenance Utility の操作画面を表示してください。

Maintenance Utility は、ストレージシステムの状態を常時監視し、画面左上に表示します。

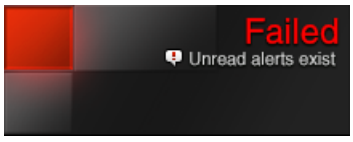
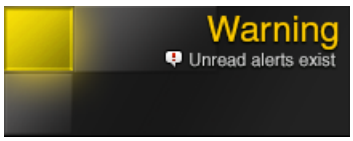
トラブルが発生すると「Warning」または「Failed」と表示されます。下記の操作によりトラブルの詳細を調べてください。

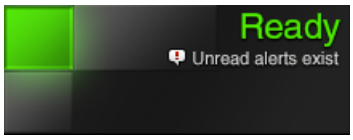
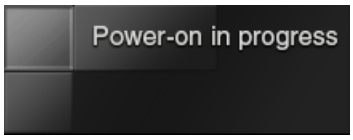
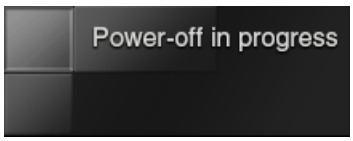
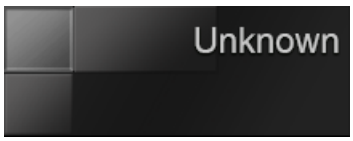
ストレージシステム状態が Failed、Warning の場合は、Maintenance Utility 画面で参照していないアラート（SIM: Service Information Message）の有無と、そのアラートの SIM リファレンスコードとアクションコードを確認して保守員に連絡してください。

操作手順

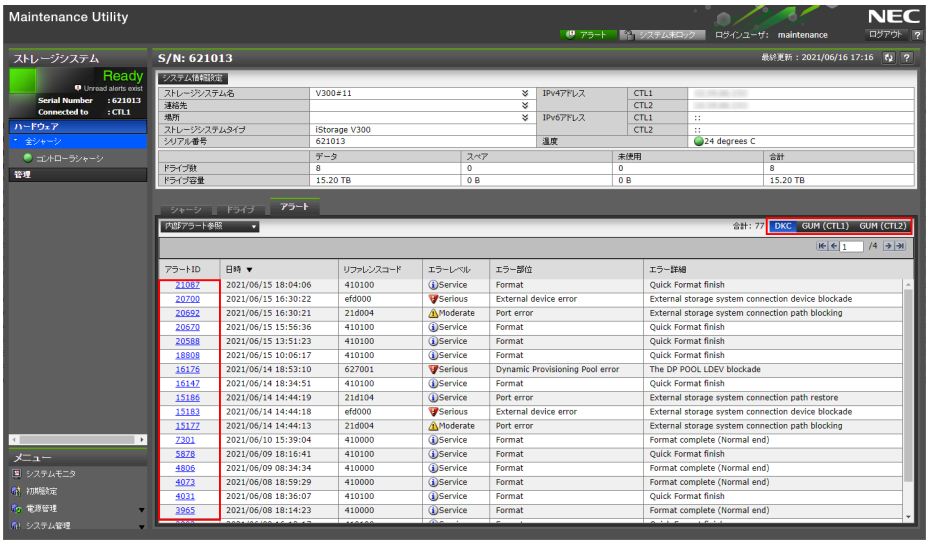
1. ストレージシステムの状態を確認します。
2. ヘッダエリアで、[アラート] をクリックします。

   [アラート] タブが表示されます。

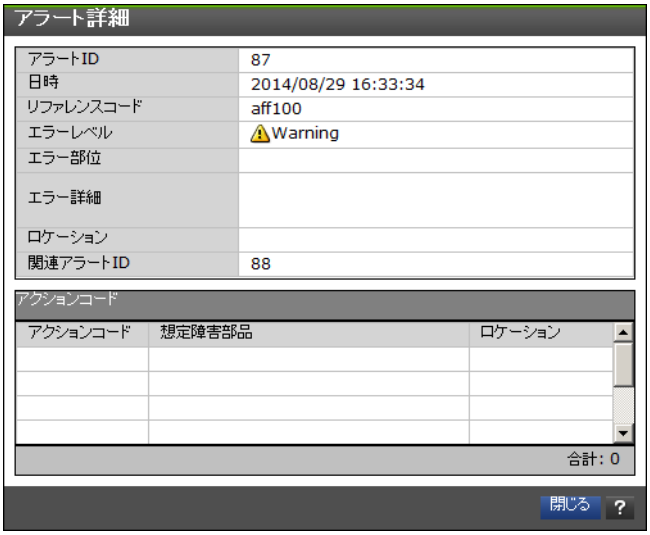
ストレージシステムの状態	説明	未参照アラート（SIM）	ナビゲーションエリア	[アラート] ボタンのアイコン/色
Failed	システムダウンが発生している可能性のあることを示します。	なし		赤
		あり		赤
Warning	部品状態に Blocked、Warning があることを示します。	なし		オレンジ
		あり		オレンジ

ストレージシステムの状態	説明	未参照アラート（SIM）	ナビゲーションエリア	[アラート] ボタンのアイコン/色
Ready	部品状態がすべて正常であることを示します。	なし		緑
		あり		緑
Power-on in progress	電源 ON 中であることを示します。			—
Power-off in progress	電源 OFF 中であることを示します。			—
Unknown	そのほか（電源を ON にする前の状態など）			—

3. ［アラート］タブで、［DKC］、［GUM （CTL1)］、および［GUM （CTL2)］をクリックし、参照していないアラート（SIM）がないか確認します。



4. ［アラート ID］の文字列をクリックすると、［アラート詳細］画面が表示されます。アラートの内容を確認します。



5. 手順 4 で確認した SIM リファレンスコード、アクションコードを保守員に連絡してください。

5.7.1　アラート詳細の確認方法

保守員からアラート詳細に表示される内容の確認をお願いする場合があります。

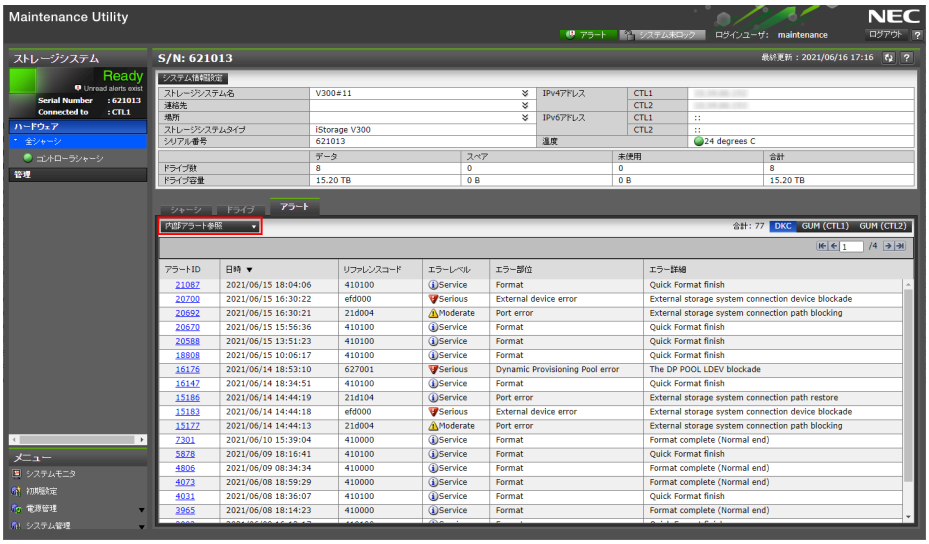
依頼があった場合、次の手順に従って確認してください。

操作手順

1. ヘッダエリアで、[アラート] をクリックします。

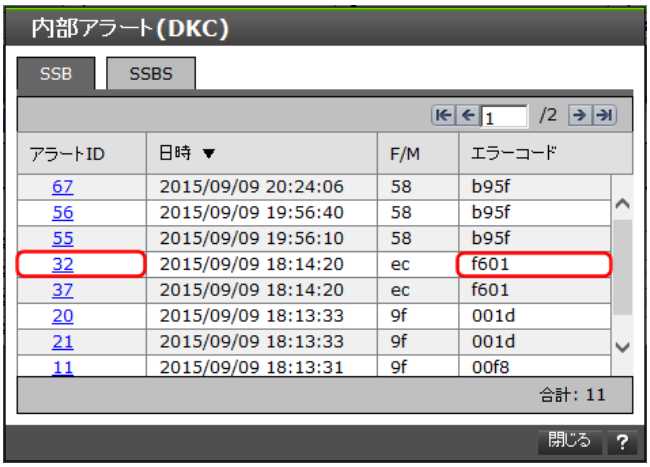
   [アラート] タブが表示されます。

2. [内部アラート参照] リストから、[内部アラート (DKC)] または [内部アラート (GUM)] を選択します。

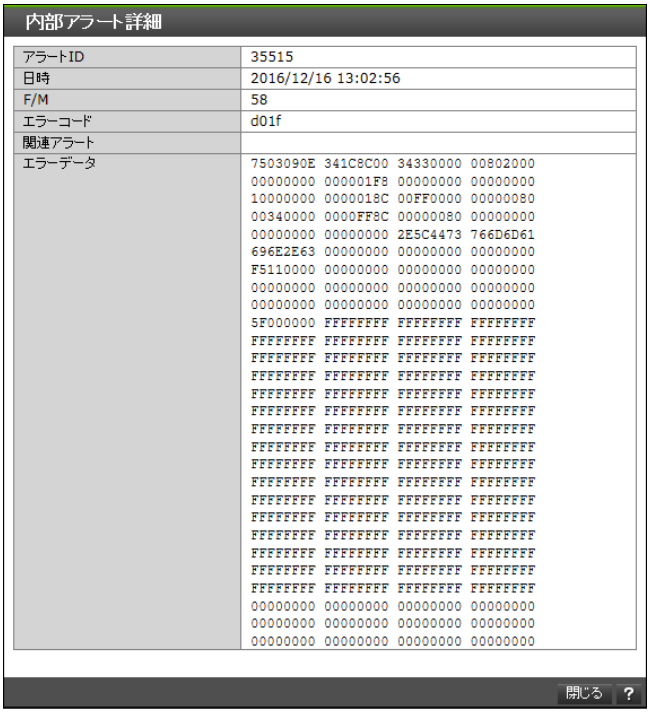


3. ［SSB］タブまたは［SSBS］タブを選択します。 SSB は重要度の高いエラーの詳細情報、SSBS は重要度の低いエラーの詳細情報です。

4. 保守員が指定する［エラーコード］に対応する［アラート ID］の文字列をクリックします。



［アラート詳細］が表示されます。保守員の指示に従ってください。



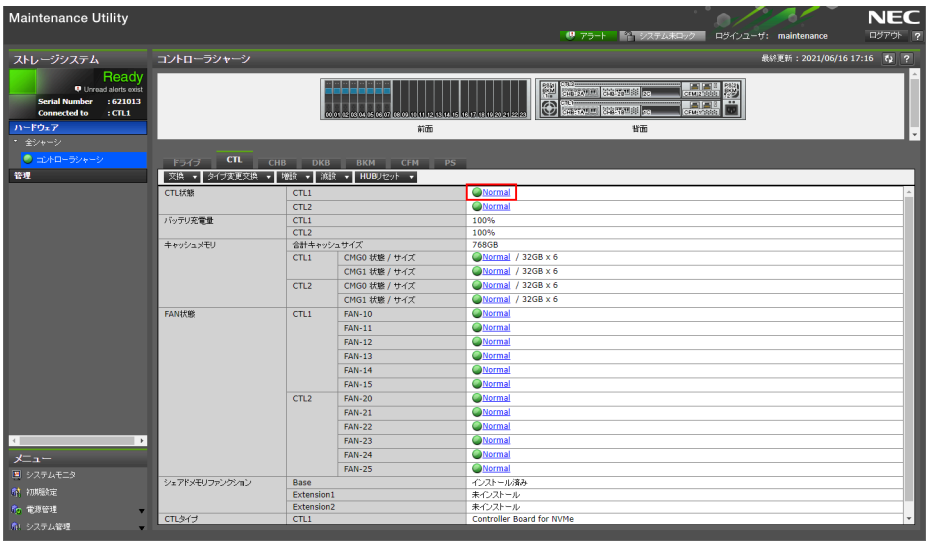
5.7.2　FRU（Field Replacement Unit）に関するアラートの確認

保守員から FRU に関するアラートの確認をお願いする場合があります。依頼があった場合、次の手順に従って確認してください。

操作手順

1. Maintenance Utility 画面の［ハードウェア］メニューから、対象のハードウェアを選択します。ハードウェアの［状態］リンクをクリックします。

コントローラシャーシの場合



ハードウェアごとの［関連アラート］画面起動方法は次のとおりです。

部位	メイン画面	タブ	［状態］リンク
コントローラシャーシ	［コントローラシャーシ］画面	ドライブ	状態
		CTL	CTL 状態
			CMG 状態
		BKM	BKM 状態
			バッテリ状態
		CFM	状態
		CHB	状態
			SFP 状態※
		PS	状態
	［Small Form-Factor Pluggable］画面	-	SFP 状態
ドライブボックス	［ドライブボックス］画面	ドライブ	状態
		ENC	状態
		PS	状態

注※

［SFP 状態］をクリックすると、［Small Form-factor Pluggable］画面が表示されます。

再度、［SFP 状態］をクリックすると［関連アラート］画面が表示されます。

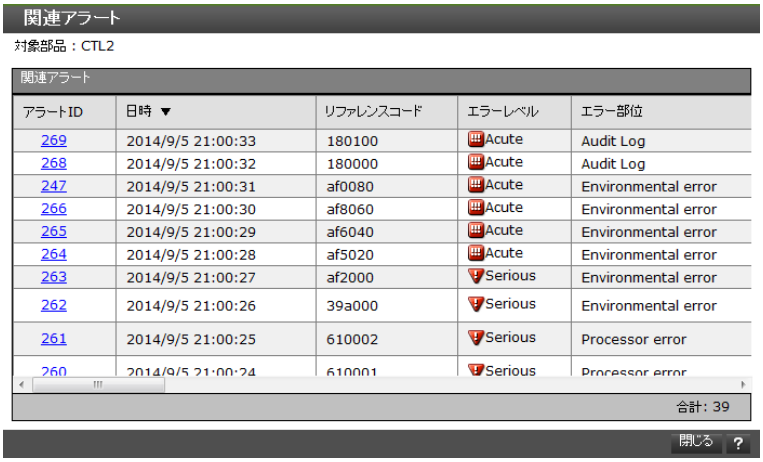
状態の意味を、次に示します。

状態	意味	部品の枠の色	状態のアイコン
Normal	正常な状態です。	なし	
Warning	• 故障が疑われる部品です。 • 他の関連部品の故障が原因で表示される可能性もあります。 • 他の関連部品の故障が原因の場合、対象の部品を交換することで最新の状態が反映されます。	オレンジ	
Failed	当該部品が故障しています。 ［ドライブ状態限定］ • 故障が疑われる部品です。 • 他の関連部品の故障が原因で表示される可能性もあります。 • 他の関連部品の故障が原因の場合、対象の部品を交換することで最新の状態が反映されます。	赤	
Blocked	Maintenance Utility からの閉塞指示が必要な部品のみ表示され、当該部品が交換できる状態です。	赤	
Not fix	［SFP 状態限定］ 種別未確定状態です。	オレンジ	

状態	意味	部品の枠の色	状態のアイコン
Warning （Port n failed）	［ドライブ状態限定］ ドライブポートに障害のある状態です。 n：障害ドライブポート番号	オレンジ	
Copying n %（TYPE to DRIVE）	［ドライブ状態限定］ コピー中の状態です。 n：コピー進捗率 TYPE：“Correction copy”、“Copy back”、“Dynamic sparing”、“Drive copy” DRIVE：コピー先ドライブロケーション（“Correction copy”で当該ドライブがコピー先の場合は“this Drive”が表示されます）。 コピー状態が複数ある場合は、コピー状態ごとに改行して情報が表示されます。	オレンジ	
Copying n %（TYPE from DRIVE）	［ドライブ状態限定］ コピー中の状態です。 n：コピー進捗率 TYPE：“Copy back”、“Dynamic sparing”、“Drive copy” DRIVE：コピー元ドライブロケーション コピー状態が複数ある場合は、コピー状態ごとに改行して情報が表示されます。	オレンジ	
Pending （TYPE to DRIVE）	［ドライブ状態限定］ コピーが中断している状態です。 TYPE：“Correction copy”、“Copy back”、“Dynamic sparing”、“Drive copy” DRIVE：コピー先ドライブロケーション（“Correction copy”で当該ドライブがコピー先の場合は“this Drive”が表示されます）。 コピー状態が複数ある場合は、コピー状態ごとに改行して情報が表示されます。	オレンジ	
Pending （TYPE from DRIVE）	［ドライブ状態限定］ コピーが中断している状態です。 TYPE：“Copy back”、“Dynamic sparing”、“Drive copy” DRIVE：コピー元ドライブロケーション コピー状態が複数ある場合は、コピー状態ごとに改行して情報が表示されます。	オレンジ	
Copy incomplete	［ドライブ状態限定］ コピー不完全状態です。	オレンジ	
Reserved	［ドライブ状態限定］	オレンジ	

状態	意味	部品の枠の色	状態のアイコン
	スペアドライブを使用できない状態です。		

2. ［関連アラート］画面が表示され、ストレージシステムが検出したアラートのうち、選択したハードウェアの交換が必要な可能性があるアラートが一覧表示されます。



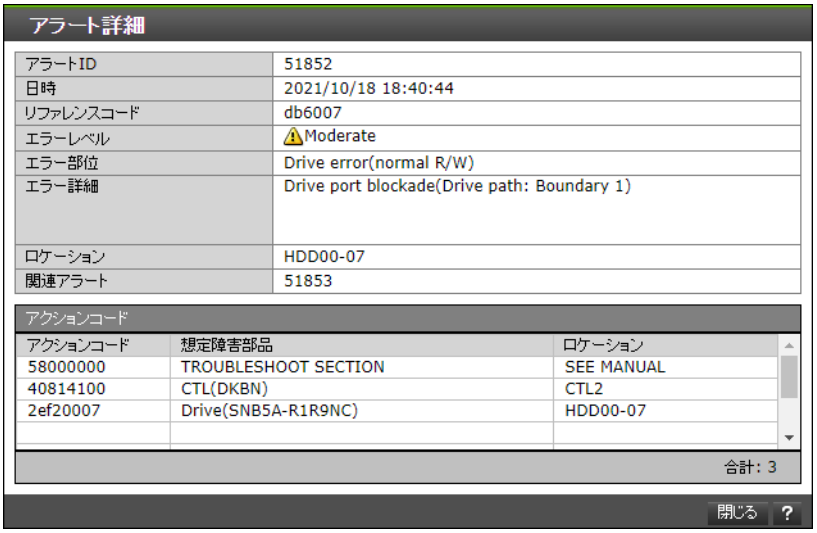
［関連アラート］画面に表示される条件は次のとおりです。

- 指定した部位、および関連する部位のアクションコードを含んだアラートのみが表示されます。
- 最新のアラートから 257 件以上古いアラートは表示されません。
- ［関連アラート］画面に表示されたアラートのうち、最新のアラートから、1 時間以上前に検出されたアラートは表示されません。

メモ

［関連アラート］画面にアラートが表示されない場合は、「5.7　管理 GUI でアラートを確認した場合の対処手順（128 ページ）」のみを行ってください。

3. ［アラート ID］の文字列をクリックすると、［アラート詳細］画面が表示されます。



4. 手順 3 で確認した SIM リファレンスコード、アクションコードを保守員に連絡してください。

5.7.3　管理 GUI を起動する際にトラブルが発生した場合の対処手順

項番	障害内容	対処方法
1	管理 PC または管理クライアントから管理 GUI を起動すると、しばらくして"Server Busy. Wait a few minutes and then try again"というメッセージが表示される。	Maintenance Utility のネットワーク設定の変更「3.5.1　ネットワーク設定の変更（71 ページ）」で、DNS サーバを設定している場合、DNS サーバに以下の項目を登録してください。 • ホスト名：localhost • IP アドレス：127.0.0.1

5.8　障害通知を受け取った場合の対処手順

「3.3　アラート通知（59 ページ）」でストレージシステム障害をメールや Syslog、SNMP により通知する設定をしている場合、障害発生時にそれぞれの通知手段で障害が通知されます。

障害通知を受け取ったら、Maintenance Utility からアラートを確認します（「5.7　管理 GUI でアラートを確認した場合の対処手順（128 ページ）」を参照してください）。アラートを確認したら、SIM リファレンスコードとアクションコードを保守員に連絡してください。

次の場合、GUM の状態監視で GUM の停止を検出したため、救済措置として、GUM がリブートされた可能性があります。

- SNMP による監視で、ColdStart トラップを検出した場合
- ストレージシステムに対するネットワーク監視で、通信不可または疎通不可が発生した場合

GUM はリブート完了後、正常状態に自動で回復します。このため、LAN ポートがリンクアップしていて、ネットワークの通信障害または疎通障害が回復していれば、対処は不要です。

ヒント

SIM リファレンスコードとアクションコードは、障害通知されるメールやログに記載されます。

5.9　バックグラウンドサービスログを使用したトラブルシューティング

バックグラウンドサービスログは、SVP で動作しているバックグラウンドサービスのログです。

操作画面で表示されるメッセージのみでは対処方法が特定できない場合に、バックグラウンドサービスログを参照してください。SVP が正常に起動したかどうかも、バックグラウンドサービスログから確認できます。

ログファイルは、次の名前で格納されます。

ログファイル種類	ログファイル名
Storage Device List ログ	system_<通番>.log
Storage Navigator ログ	system_<装置製番>_<通番>.log

バックグラウンドサービスログは次のディレクトリに格納されます。

```
<installDir>\wk\supervisor\system\log
```

ヒント

- <installDir>: ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。（例 C:\Mapp）
- <通番> : ログファイルの通番が 0 始まりで付与されます。

バックグラウンドサービスには次のものがあります。

表 5-2　Storage Device List のバックグラウンドサービス一覧

Storage Device List バックグラウンドサービス	サービス名
Storage Device List サーバ	SDLSrv
SVP RMI-API フォワードサーバ	RMI-API Forward Server
Web アプリケーションサーバ	Web Application Server

表 5-3　Storage Navigator のバックグラウンドサービス一覧

Storage Navigator バックグラウンドサービス	サービス名
Web アプリケーションサーバ	Web Application Server
Storage Navigator サーバ	Storage Navigator
SVP RMI-API サーバ	RMI-API Server
外部認証中継サービス	External Authenticator
通信サービス	Communication
KMIP コミュニケータ	KMIP Communicator

ログの出力フォーマットは次のとおりです

[発生日時][障害レベル][トラブルシュートコード][サービス名][ログ内容]

項目	説明
発生日時	下記のフォーマットで日時が出力されます。 YYYY/MM/DD hh:mm:ss.SS
障害レベル	下記の障害レベルが出力されます。 • INFO：参考情報（起動や終了イベントなど） • WARN：警告情報

項目	説明
	（設定値などが不足しており、デフォルト状態で動いている。） • ERROR：エラーにより起動できない状態になっている。
トラブルシュートコード	トラブルの原因ごとに割り当てられている番号です。
サービス名	サービス名が出力されます。
ログ内容	メッセージが出力されます。

各バックグラウンドサービスは次のようなログを出力します。

このログにより、各バックグラウンドサービスの初期化処理が正常に終了して起動しているのか、また、サービス動作中に何か異常が発生しているのかを確認できます。

```
[2018/01/01 13:00:00.000][INFO][TRSTNA000001][Web Application Server][Initi
alizing]
[2018/01/01 13:00:15.000][INFO][TRSTNA000002][Web Application Server][Ready
]
[2018/01/01 13:00:30.000][INFO][TRSTNA001001][Storage Navigator][Initializi
ng]
[2018/01/01 13:01:00.000][INFO][TRSTNA001002][Storage Navigator][Ready]
```

5.9.1　Storage Device List サーバ

- 正常時ログ出力例

```
[2018/03/18 15:40:50.372][INFO ][TRSDLS000001][SDLSrv][Initializing]
・・・
[2018/03/18 15:41:28.009][INFO ][TRSDLS000002][SDLSrv][Ready]
```

- 異常時ログ出力例

```
[2018/03/19 17:12:14.551][INFO ][TRSDLS000006][SDLSrv][Stopping]
[2018/03/19 17:12:14.934][ERROR][TRSDLS000011][SDLSrv][Stopping : Syste
m is locked (SN:600001).]
[2018/03/19 17:12:15.216][ERROR][TRSDLS000008][SDLSrv][Ready : Failed t
o stop.]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TRSDLS000001	INFO	Storage Device List サーバの初期化処理が開始されました。 TRSDLS000002 が出力され、初期化処理が正常に完了していることを確認してください。
TRSDLS000002	INFO	Storage Device List サーバの初期化処理が正常に完了しました。
TRSDLS000003	ERROR	Storage Device List サーバの初期化処理がエラー終了しました。このログの前後に出力されているトラブルシュートコードを参照して、対応する対処方法を実施してください。 これ以外のエラーログが出力されていない場合、SVP を再起動してください。SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。

トラブルシュートコード	障害レベル	対処方法
TRSDLS000004	ERROR	ログに表示されたポート番号が使用できません。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。 該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。 変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照して、“DKCManPrivate”のポート番号を変更してください。
TRSDLS000005	ERROR	Storage Device List サーバの初期化処理がタイムアウトしました。 次の手順を実行して Storage Device List サーバを起動してください。 1. Windows のスタートメニューより、［コントロールパネル］－［システムとセキュリティ］－［管理ツール］または［Windows ツール］－［サービス］を選択します。※ 2. 一覧から DKCMan を選択し、［サービスの開始］を選択します。 繰り返し操作しても結果が変わらない場合は、SVP を再起動してください。SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRSDLS000006	INFO	Storage Device List サーバの停止処理が開始されました。 TRSDLS000007 が出力され、停止処理が正常に完了していることを確認してください。
TRSDLS000007	INFO	Storage Device List サーバの停止処理が正常に完了しました。
TRSDLS000008	ERROR	Storage Device List サーバの停止処理がエラー終了しました。このログの前後に出力されているトラブルシュートコードを参照して、対応する対処方法を実施してください。 これ以外のエラーログが出力されていない場合、Storage Device List サーバを停止するには以下の手順を実行してください。 1. Windows のスタートメニューより、［コントロールパネル］－［システムとセキュリティ］－［管理ツール］または［Windows ツール］－［サービス］を選択します。※ 2. DKCMan のプロパティを表示し、［全般］タブの［スタートアップの種類］を、［手動］に設定します。 3. SVP をリブートします。
TRSDLS000009	ERROR	SVP の環境構築処理が実行中のため、Storage Device List サーバが停止できません。しばらくしてから再操作してください。
TRSDLS000010	ERROR	ログに表示された装置製番（SN）の装置は、サービスの停止処理がサポートされていません。Storage Device List サーバを停止するには次の手順を実行してください。 1. Windows のスタートメニューより、［コントロールパネル］－［システムとセキュリティ］－［管理ツー

トラブルシュートコード	障害レベル	対処方法
		ル］または［Windows ツール］－［サービス］を選択します。※ 2. DKCMan のプロパティを表示し、［全般］タブの［スタートアップの種類］を、［手動］に設定します。 3. SVP をリブートします。
TRSDLS000011	ERROR	ログに表示された装置製番（SN）のシステムは、別のユーザがロックを取得しているためサービスが停止できません。別のユーザからのロックを解除してから、再操作してください。
TRSDLS000012	ERROR	Storage Device List サーバの停止処理がタイムアウトしました。繰り返し発生する場合は、次の手順で Storage Device List サーバを停止してください。 1. Windows のスタートメニューより、［コントロールパネル］－［システムとセキュリティ］－［管理ツール］または［Windows ツール］－［サービス］を選択します。※ 2. DKCMan のプロパティを表示し、［全般］タブの［スタートアップの種類］を、［手動］に設定します。 3. SVP をリブートします。
TRSDLS000013	WARN	サービスのステータス取得に失敗しました。 3 分待ってもこのワーニングが消えない場合、Storage Device List からこのストレージシステムを停止し、再度、起動してください。それでも回復しない場合は、SVP を再起動してください。 SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。

注※

Windows のユーザーアカウント制御が起動した場合は［続行］を選択してください。

5.9.2　SVP RMI-API フォワードサーバ

- 正常時ログ出力例

```
[2018/03/17 15:49:09.638][INFO ][TRRMIS002001][RMI-API Forward Server][
Initializing]
[2018/03/17 15:49:16.544][INFO ][TRRMIS002002][RMI-API Forward Server][
Ready]
[2018/03/17 18:50:59.982][INFO ][TRRMIS002012][RMI-API Forward Server][
Stopping]
[2018/03/17 18:51:00.003][INFO ][TRRMIS002013][RMI-API Forward Server][
Stopped]
```

- 異常時ログ出力例

```
[2018/03/17 15:49:09.638][INFO ][TRRMIS002001][RMI-API Forward Server][
Initializing]
[2018/03/17 15:49:10.001][ERROR][TRRMIS002005][RMI-API Forward Server][
Failed : Environment is invalid.]
```

```
[2018/03/17 15:49:10.102][INFO ][TRRMIS002004][RMI-API Forward Server][
Failed]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TRRMIS002001	INFO	RMI-API Forward Server のサービスが起動されるときに出力されます。 RMI-API Forward Server のサービスが正常に起動されているかを確認するには本ログと TRRMIS002002 が出力されていることを確認してください。
TRRMIS002002	INFO	RMI-API Forward Server のサービスの起動が正常に完了したときに出力されます。
TRRMIS002003	WARN	RMI-API Forward Server のサービスは起動したが、処理で警告が発生しています。 TRRMIS002001 から本ログまでに出力されているトラブルシュートコードを確認し対処してください。
TRRMIS002004	ERROR	RMI-API Forward Server のサービスの起動に失敗しています。 TRRMIS002001 から本ログまでに出力されているトラブルシュートコードを確認し対処してください。
TRRMIS002005	ERROR	RMI-API Forward Server のサービスの起動に必要な環境設定情報の取得に失敗しています。 SVP を再起動してください。SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS002006	ERROR	
TRRMIS002007	WARN	
TRRMIS002008	WARN	RMI-API Forward Server のサービスに必要なポート番号が使用できません。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照して、“RMIIFRegist”のポート番号を変更してください。
TRRMIS002009	WARN	RMI-API Forward Server のサービスに必要なポート番号が使用できません。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照して、“DKCManPrivate”のポート番号を変更してください。
TRRMIS002010	WARN	TRRMIS002008 の対処方法と同様になります。 TRRMIS002008 の対処方法を参照してください。
TRRMIS002011	WARN	TRRMIS002009 の対処方法と同様になります。 TRRMIS002009 の対処方法を参照してください。
TRRMIS002012	INFO	RMI-API Forward Server のサービスが停止したときに出力されます。

トラブルシュートコード	障害レベル	対処方法
		RMI-API Forward Server のサービスが正常に停止されているかを確認するには本ログと TRRMIS002013 が出力されていることを確認してください。
TRRMIS002013	INFO	RMI-API Forward Server のサービスの停止が正常に完了したときに出力されます。

5.9.3　Web アプリケーションサーバ

- 正常時ログ出力例

```
[2017/12/02 16:21:47.113][INFO ][TRMAAS000001][Web Application Server][
Initializing]
[2017/12/02 16:21:48.410][INFO ][TRMAAS000002][Web Application Server][
Ready]
```

- 異常時ログ出力例

```
[2017/12/03 09:47:22.020][INFO ][TRMAAS000001][Web Application Server][
Initializing]
[2017/12/03 09:48:25.004][ERROR][TRMAAS000004][Web Application Server][
Failed : Failed to connect to the starting port of the web server.Port=
8080.]
[2017/12/03 09:48:25.174][INFO ][TRMAAS000007][Web Application Server][
Stopped]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TRMAAS000001	INFO	Web アプリケーションサーバが起動されるときに出力されます。 Web アプリケーションサーバが正常に起動されているかを確認するには、本トラブルシュートコードと TRMAAS000002 が出力されているかを確認してください。
TRMAAS000002	INFO	Web アプリケーションサーバの起動が完了したときに出力されます。
TRMAAS000003	WARN	Web アプリケーションサーバのサービスに必要なポート番号が使用できません。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、“MAPPWebServer”、“MAPPWebServerHttps”、“RMIClassLoader”、“RMIClassLoaderHttps”の内、他のアプリケーションで使用されているポート番号を変更してください。ポート番号の変更操作については、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照してください。
TRMAAS000004	ERROR	Web アプリケーションサーバのサービスに必要なポート番号が使用できません。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411

トラブルシュートコード	障害レベル	対処方法
		ページ)」を参照して、“CommonJettyStart”のポート番号を変更してください。
TRMAAS000005	ERROR	Web アプリケーションサーバのサービスに必要なポート番号が使用できません。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ)」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ)」を参照して、“CommonJettyStop”のポート番号を変更してください。
TRMAAS000006	INFO	Web アプリケーションサーバが停止するときに出力されます。 Web アプリケーションサーバが正常に停止したかを確認するには、本トラブルシュートコードと TRMAAS000007 が出力されているかを確認してください。
TRMAAS000007	INFO	Web アプリケーションサーバの停止が正常に完了したときに出力されます。

5.9.4　Storage Navigator サーバ

- 正常時ログ出力例（起動時）

```
[2018/03/19 18:08:31.046][INFO ][TRSTNA000001][Web Application Server][
Initializing]
[2018/03/19 18:08:31.592][INFO ][TRSTNA000002][Web Application Server][
Ready]
[2018/03/19 18:09:12.903][INFO ][TRSTNA001001][Storage Navigator][Initi
alizing]
[2018/03/19 18:15:29.387][INFO ][TRSTNA001002][Storage Navigator][Ready
]
```

- 正常時ログ出力例（終了時）

```
[2018/03/19 21:11:49.942][INFO ][TRSTNA000004][Web Application Server][
Stopping]
[2018/03/19 21:11:50.478][INFO ][TRSTNA000005][Web Application Server][
Stopped]
[2018/03/19 21:11:50.859][INFO ][TRSTNA001004][Storage Navigator][Stopp
ing]
[2018/03/19 21:11:52.209][INFO ][TRSTNA001005][Storage Navigator][Stopp
ed]
```

- 異常時ログ出力例（起動時）

```
[2018/03/20 11:15:33.543][INFO ][TRSTNA000001][Web Application Server][
Initializing]
[2018/03/20 11:15:34.364][ERROR][TRSTNA000003][Web Application Server][
Initializing : Failed to start a Storage Navigator.]
```

- 異常時ログ出力例（終了時）

```
[2018/03/20 12:24:36.175][INFO ][TRSTNA000004][Web Application Server][
Stopping]
[2018/03/20 12:24:38.931][INFO ][TRSTNA000005][Web Application Server][
Stopped]
[2018/03/20 12:24:39.142][INFO ][TRSTNA001004][Storage Navigator][Stopp
ing]
[2018/03/20 12:25:40.634][WARN][TRSTNA001006][Storage Navigator][Stoppe
d : Timeout has occurred.]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TRSTNA000001	INFO	Web アプリケーションサーバが起動されるときに出力されます。 Web アプリケーションサーバが正常に起動されているかを確認するには、本トラブルシュートコードと TRSTNA000002 が出力されているか確認してください。
TRSTNA000002	INFO	Web アプリケーションサーバの起動が完了したときに出力されます。
TRSTNA000003	ERROR	Web アプリケーションサーバの起動に失敗しています。 1. Storage Device List から、該当の装置を選択し、停止を行ったあとに、再度起動してください。 2. それでも回復しない場合は、SVP の再起動を行ってください。 3. SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRSTNA000004	INFO	Web アプリケーションサーバが停止するときに出力されます。
TRSTNA000005	INFO	Web アプリケーションサーバの停止が完了したときに出力されます。
TRSTNA000006	ERROR	Web アプリケーションサーバの停止でエラーが発生しました。 SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRSTNA000007	WARN	Storage Navigator サービスが予期せず停止し、再起動中です。 3 分待っても現象が変わらない場合は、Storage Device List から装置を停止し、再度起動してください。 それでも回復しない場合は、SVP を再起動してください。 SVP を再起動しても回復しない場合は、「G.2.1.2　GUI による更新（319 ページ）」を参照して、Storage Device List からサービスを停止し、ストレージ管理ソフトウェア、および SVP ソフトウェアを更新してください。 ストレージ管理ソフトウェア、および SVP ソフトウェアを更新しても回復しない場合は、「5.10　仮想メモリの設定方法（162 ページ）」を参照して、仮想メモリの設定を変更し、SVP を再起動してください。 上記の操作を行っても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。

トラブルシュートコード	障害レベル	対処方法
TRSTNA000008	ERROR	「L.6　自動割り振りされるポート番号の範囲を変更する（419 ページ）」を参照して、“DeviceJettyStart”のポート番号の範囲を使用されていない範囲に変更してください。 対応後、SVP を再起動してください。
TRSTNA000009	ERROR	「L.6　自動割り振りされるポート番号の範囲を変更する（419 ページ）」を参照して、“DeviceJettyStop”のポート番号の範囲を使用されていない範囲に変更してください。 対応後、SVP を再起動してください。
TRSTNA000010	ERROR	Web アプリケーションサーバが強制停止されました。 サーバ稼働中に SVP を再起動した場合に出力されることがあります。 Storage Device List から該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRSTNA000011	ERROR	Web アプリケーションサーバが強制停止されました。 サーバ稼働中に SVP を再起動した場合に出力されることがあります。 Storage Device List から該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRSTNA001001	INFO	Storage Navigator サービスが起動されるときに出力されます。 Storage Navigator サービスが正常に起動しているかを確認するには、本トラブルシュートコードと TRSTNA001002 が出力されているか確認してください。
TRSTNA001002	INFO	Storage Navigator サービスが正常に起動しました。
TRSTNA001003	WARN	このトラブルシュートコードは、Storage Navigator のサービスの起動中に出力される場合があります。 TRSTNA001001 が出力されてから最大 10 分お待ちください。 10 分経過しても TRSTNA001002 が出力されない場合は、「A.8　デスクトップヒープの指定値を変更する（206 ページ）」および「4.3　ウィルス検出プログラムの使用に関する注意事項（97 ページ）」に示す設定が完了しているか確認してください。設定が完了していない場合は設定してください。 上記の手順を実施した後、Storage Device List を使用して、該当の装置のサービスを停止してから再度サービスを起動してください。 上記を実施しても回復しない場合は、「5.11　ダンプファイルの採取方法（163 ページ）」を参照してダンプを採取した後、保守員に連絡してください。
TRSTNA001004	INFO	Storage Navigator サービスが停止するときに出力されます。

トラブルシュートコード	障害レベル	対処方法
		Storage Navigator サービスが正常に停止したかを確認するには、本トラブルシュートコードと TRSTNA001005 が出力されているかを確認してください。
TRSTNA001005	INFO	Storage Navigator サービスの停止が完了したときに出力されます。
TRSTNA001006	WARN	Storage Navigator サービス停止時に、タイムアウトが発生しました。 次回起動時に、起動完了（TRSTNA001002）にならない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRSTNA001007	ERROR	Storage Navigator のサービスが強制停止されました。 サービス稼働中に SVP を再起動した場合に出力されることがあります。 Storage Device List から該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRSTNA001008	ERROR	Storage Navigator のサービスが強制停止されました。 サービス稼働中に SVP を再起動した場合に出力されることがあります。 Storage Device List から該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。

5.9.5　SVP RMI-API サーバ

正常時ログ出力例

- 正常時ログ出力例

  SVP RMI-API サーバでは複数のサービスの起動ログが出力されます。SVP RMI-API サーバの正常起動の確認をするには、TRRMIS000002、TRRMIS001002、TRRMIS002502 のログを確認してください。また、正常終了の確認をするには、TRRMIS000016、TRRMIS001007、TRRMIS002511 のログを確認してください。

```
[2018/03/17 15:49:07.750][INFO ][TRRMIS001001][RMI-API Server][Initializing]
[2018/03/17 15:49:08.000][INFO ][TRRMIS001002][RMI-API Server][Ready]
[2018/03/17 15:49:09.638][INFO ][TRRMIS002501][RMI-API Server][Initializing]
```

```
[2018/03/17 15:49:16.544][INFO ][TRRMIS002502][RMI-API Server][Ready]
[2018/03/17 15:52:03.405][INFO ][TRRMIS000001][RMI-API Server][Initiali
zing]
[2018/03/17 15:52:19.364][INFO ][TRRMIS000002][RMI-API Server][Ready]
・・・
[2018/03/17 18:50:59.982][INFO ][TRRMIS002510][RMI-API Server][Stopping
]
[2018/03/17 18:51:00.003][INFO ][TRRMIS002511][RMI-API Server][Stopped]
[2018/03/17 18:51:06.645][INFO ][TRRMIS001006][RMI-API Server][Stopping
]
[2018/03/17 18:51:06.927][INFO ][TRRMIS000015][RMI-API Server][Stopping
]
[2018/03/17 18:51:08.249][INFO ][TRRMIS000016][RMI-API Server][Stopped]
[2018/03/17 18:51:10.695][INFO ][TRRMIS001007][RMI-API Server][Stopped]
```

- 異常時ログ出力例

```
[2018/03/17 15:49:07.750][INFO ][TRRMIS001001][RMI-API Server][Initiali
zing]
[2018/03/17 15:49:08.000][INFO ][TRRMIS001002][RMI-API Server][Ready]
[2018/03/17 15:49:09.638][INFO ][TRRMIS002501][RMI-API Server][Initiali
zing]
[2018/03/17 15:49:16.544][INFO ][TRRMIS002502][RMI-API Server][Ready]
[2018/03/17 15:52:03.405][INFO ][TRRMIS000001][RMI-API Server][Initiali
zing]
[2018/03/17 15:52:03.968][ERROR][TRRMIS000007][RMI-API Server][Failed :
 Port is already in use. Port=51100]
[2018/03/17 15:52:04.003][INFO ][TRRMIS000015][RMI-API Server][Stopping
]
[2018/03/17 15:52:04.125][INFO ][TRRMIS000016][RMI-API Server][Stopped]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TRRMIS000001	INFO	RMI-API Server のサービスが起動されるときに出力されます。 本ログはエラー発生時にはリトライにより複数回出力されます。 RMI-API Server のサービスが正常に起動されているかを確認するには本ログと TRRMIS000002 が出力されていることを確認してください。
TRRMIS000002	INFO	RMI-API Server のサービスの起動が正常に完了したときに出力されます。
TRRMIS000003	WARN	RMI-API Server のサービスの必要な環境設定ファイルの読み込みに失敗しました。 SVP を再起動してください。 SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000004	WARN	RMI-API Server のサービスの必要な環境設定情報の取得に失敗したため、ログ内容に示すデフォルト値で動作しています。 SVP を再起動してください。

トラブルシュートコード	障害レベル	対処方法
		SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000005	WARN	RMI-API Server のサービスの必要な環境設定情報の取得に失敗したため、ログ内容に示すデフォルト値で動作しています。 SVP を再起動してください。 SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000006	WARN	RMI-API Server のサービスで使用するポート番号がすでに使用されています。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。 該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。 変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照して、“RMIIFRegist”のポート番号を変更してください。
TRRMIS000007	ERROR	RMI-API Server のサービスで使用するポート番号がすでに使用されています。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。 該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。 変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照して、“PreRMIServer”のポート番号を変更してください。
TRRMIS000008	WARN	RMI-API Server のサービスで、ログ内容に示すファイル操作に失敗しました。他のアプリケーションが該当のファイルにアクセスしている可能性があります。他のすべてのアプリケーションを閉じたあと、Storage Device List から、該当の装置を一旦停止し、再度起動してください。
TRRMIS000009	ERROR	RMI-API Server のサービスで、予期せぬエラーが発生しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。 再度起動しても現象が変わらない場合、Storage Device List からこの装置を一旦削除して、再登録してください。 装置の再登録後も回復しない場合は、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000010	WARN	RMI-API Server のサービスで、必要なサービスへの接続に失敗しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。

トラブルシュートコード	障害レベル	対処方法
		再度起動しても現象が変わらない場合、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000011	ERROR	RMI-API Server のサービスで、必要なサービスへの接続に失敗しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。 再度起動しても現象が変わらない場合、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000012	WARN	RMI-API Server のサービスで使用する IP アドレスが不正です。 Storage Device List で設定した SVP の IP アドレスが正しいか確認し、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000013	ERROR	RMI-API Server のサービスで使用する IP アドレスが不正です。 Storage Device List で設定した SVP の IP アドレスが正しいか確認し、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000014	WARN	RMI-API Server のサービスで使用するポート番号の取得に失敗したため、ログ内容に示すデフォルト値で動作しています。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ポート番号が他のアプリケーションで使用されていないか確認してください。 該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照して、“PreRMIServer”のポート番号を変更してください。
TRRMIS000015	INFO	RMI-API Server のサービスが終了するときに出力されます。 本ログは、エラー発生時にはリトライにより複数回出力されます。 RMI-API Server のサービスが正常に終了しているかを確認するには本ログと TRRMIS000016 の出力を確認してください。
TRRMIS000016	INFO	RMI-API Server のサービスの停止が正常に完了したときに出力されます。
TRRMIS000017	WARN	RMI-API Server のサービスで、必要なサービスへの接続に失敗しました。 SVP を再起動してください。

トラブルシュートコード	障害レベル	対処方法
		SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000018	ERROR	RMI-API Server のサービスで、必要なサービスへの接続に失敗しました。 SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000019	ERROR	RMI-API Server のサービスで、ログ内容に示すファイル操作に失敗しました。 他のアプリケーションが該当のファイルにアクセスしている可能性があります。他のすべてのアプリケーションを閉じてください。
TRRMIS000020	WARN	RMI-API Server のサービスで、必要なサービスへの接続に失敗したため、クライアントが RMI-API Server へ接続できていません。 以下に示すパスの中に、DkcId32.dll が存在していないか確認してください。 • Windows システムディレクトリ（例:C:\Windows\system32） • Windows ディレクトリ（例:C:\Windows） • 環境変数 PATH で定義されているディレクトリ DkcId32.dll が存在する場合は、DLL を削除してから SVP を再起動してください。 SVP の再起動後も回復しない場合、または DkcId32.dll が上記パス内に存在していない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。 ※本ログは、RMI-API Server が一度でも接続エラーを検知した場合に出力されます。 リトライにより成功していて、Storage Navigator（または外部より RMI 接続しているクライアント）が正常に動作している場合、本ログは無視してください。
TRRMIS000021	WARN	RMI-API Server のサービスで、予期せぬエラーが発生しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。 再度起動しても現象が変わらない場合、Storage Device List からこの装置を一旦削除して、再登録してください。 装置の再登録後も回復しない場合は、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000022	WARN	RMI-API Server のサービスで、予期せぬエラーが発生しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。 再度起動しても現象が変わらない場合、Storage Device List からこの装置を一旦削除して、再登録してください。

トラブルシュートコード	障害レベル	対処方法
		装置の再登録後も回復しない場合は、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000023	ERROR	RMI-API Server のサービスで、予期せぬエラーが発生しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。 再度起動しても現象が変わらない場合、Storage Device List からこの装置を一旦削除して、再登録してください。 装置の再登録後も回復しない場合は、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000024	ERROR	RMI-API Server のサービスで、予期せぬエラーが発生しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。 再度起動しても現象が変わらない場合、Storage Device List からこの装置を一旦削除して、再登録してください。 装置の再登録後も回復しない場合は、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS000025	ERROR	RMI-API Server のサービスで、予期せぬエラーが発生しました。 Storage Device List から、該当の装置を一旦停止し、再度起動してください。 再度起動しても現象が変わらない場合、Storage Device List からこの装置を一旦削除して、再登録してください。 装置の再登録後も回復しない場合は、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS001001	INFO	RMI-API Server のサービスが起動されるときに出力されます。RMI-API Server のサービスが正常に起動されているかを確認するには本ログと TRRMIS001002 が出力されていることを確認してください。
TRRMIS001002	INFO	RMI-API Server のサービスの起動が正常に完了したときに出力されます。
TRRMIS001003	WARN	RMI-API Server のサービスで使用するポート番号の取得に失敗したため、ログ内容に示すデフォルト値で動作しています。 「L.9　ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照し、ポート番号が他のアプリケーションで使用されていないか確認してください。

トラブルシュートコード	障害レベル	対処方法
		該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、「L.1　SVP で使用するポート番号を変更する（411 ページ）」を参照して、“RMIClassLoader”のポート番号を変更してください。
TRRMIS001004	WARN	RMI-API Server のサービスで必要な環境設定情報の取得に失敗したため、ログ内容に示すデフォルト値で動作しています。 Storage Device List で設定した SVP の IP アドレスが正しいか確認し、SVP を再起動してください。 SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS001005	WARN	RMI-API Server のサービス起動に必要なほかのサービスの起動待ちログです。まずは「5.9　バックグラウンドサービスログを使用したトラブルシューティング（137 ページ）」に記載されている「Storage Device List ログ」に TRMAAS000003、TRMAAS000004、TRMAAS000005 が出力されているか確認してください。出力されている場合は、トラブルシュートコードの対処を実施してください。 本ログは 10 分に 1 回、最大 6 回まで出力されます。 TRRMIS001002 出力後、本ログが 6 回出力されたのちに、まだ Storage Navigator が起動できない場合、以下の手順を実行してください。なお、直前の操作内容により手順が異なります。 • SVP と管理クライアント間の SSL 通信の署名付き証明書を SVP へアップロードした場合 1. SVP へアップロードした SSL 通信の署名付き公開鍵証明書または秘密鍵に問題がある場合があります。署名付き公開鍵証明書、または秘密鍵を確認のうえ更新してください（「C.11　SVP と管理クライアント間の SSL 通信の署名付き証明書を SVP へアップロード（258 ページ）」を参照）。 2. 更新しても RMA-API Server のサービスが「TRRMIS001005」で起動できない場合、署名付き証明書をデフォルトに戻してください（「C.12　SVP と管理クライアント間の SSL 通信の証明書をデフォルトに変更（259 ページ）」を参照）。デフォルトに戻してサービスが起動できた場合、アップロードした署名付き証明書に問題がありますので、再度見直してください。 • SVP ソフトウェア設定情報のリストアを実施した場合 1. リストア先の SVP ソフトウェアと、同じバージョンの SVP ソフトウェアで取得したバックアップファイルを使用して、再度リストアしてください。 2. 同じバージョンのバックアップファイルがなく、署名付き証明書が設定済みの場合、署名付き証明書を更新してください（「C.11　SVP と管理クライアント間の SSL 通信の署名付き証明書を SVP へアップロード（258 ページ）」を参照）。 3. 同じバージョンのバックアップファイルがなく、署名付き証明書を設定していない場合、署名付き証明書をデフォルトに戻してください（「C.12　SVP と

トラブルシュートコード	障害レベル	対処方法
		管理クライアント間の SSL 通信の証明書をデフォルトに変更（259 ページ）」を参照）。 • 上記以外の場合 1. Storage Device List から、該当の装置を一旦停止し、再度起動してください。本ログと共に TRRMIS001003、TRRMIS001004 が出力されている場合は、該当のトラブルシュートコードの対処方法も確認してください。 2. 再度起動しても現象が変わらない場合、SVP を再起動してください。 3. SVP の再起動後も回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、および装置の登録を行ってください。
TRRMIS001006	INFO	RMI-API Server のサービスが終了するときに出力されます。SVP RMI-API Server のサービスが正常に終了しているかを確認するには本ログと TRRMIS001007 の出力を確認してください。
TRRMIS001007	INFO	RMI-API Server のサービスの停止が正常に完了したときに出力されます。
TRRMIS001008	WARN	RMI-API Server のサービスの一部の機能が正常に動作していません。 装置の停止が正常に行えません。 SVP を再起動してください。
TRRMIS001009	ERROR	RMI-API Server のサービスで、予期せぬエラーが発生しました。 「5.11.1　ダンプツールを使用した採取（163 ページ）」を参照して、ダンプファイルの採取を行ってください。 採取に失敗した場合は、「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照して、手動で該当するファイルを採取してください。
TRRMIS001998	ERROR	RMI-APIServer のサービスが異常終了しました。
TRRMIS001999	ERROR	サービスが強制停止されました。本メッセージは、サービス起動中に SVP を再起動した場合に出力されることがあります。 Storage Device List から該当の装置を一度停止して、再度起動してください。
TRRMIS002501	INFO	RMI-API Server のサービスが起動されるときに出力されます。 RMI-API Server のサービスが正常に起動されているかを確認するには本ログと TRRMIS002502 が出力されていることを確認してください。
TRRMIS002502	INFO	RMI-API Server のサービスの起動が正常に完了したときに出力されます。
TRRMIS002503	WARN	RMI-API Server のサービスは起動したが、処理で警告が発生しています。 TRRMIS002501 から本ログまでに出力されているトラブルシュートコードを確認し対処してください。
TRRMIS002504	ERROR	RMI-API Server のサービスの起動に失敗しています。 TRRMIS002501 から本ログまでに出力されているトラブルシュートコードを確認し対処してください。

トラブルシュートコード	障害レベル	対処方法
TRRMIS002505	ERROR	RMI-API Server のサービスの起動に必要な環境設定情報の取得に失敗しています。 Storage Device List から該当の装置を停止し、再度起動してください。 再度起動しても現象が変わらない場合は、SVP を再起動してください。SVP の再起動後も現象が変わらない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS002506	ERROR	
TRRMIS002507	ERROR	
TRRMIS002508	ERROR	RMI-API Server のサービスに必要なポート番号が使用できません。 「L.9　ポート番号を使用しているアプリケーションを確認する (423 ページ)」を参照し、ログに出力されているポート番号が他のアプリケーションで使用されていないか確認してください。該当するアプリケーションのポート番号を変更できる場合は変更し、SVP を再起動してください。変更できない場合は、「L.1　SVP で使用するポート番号を変更する (411 ページ)」を参照して、“DKCManPrivate” のポート番号を変更してください。
TRRMIS002509	ERROR	
TRRMIS002510	INFO	RMI-API Server のサービスが停止したときに出力されます。 RMI-API Server のサービスが正常に停止されているかを確認するには本ログと TRRMIS002511 が出力されていることを確認してください。
TRRMIS002511	INFO	RMI-API Server のサービスの停止が正常に完了したときに出力されます。
TRRMIS002512	ERROR	RMI-API Server のサービスが停止しています。 5 分待っても現象が変わらない場合は、以下の手順を順番に実行してください。 1. Storage Device List から該当の装置を停止し、再起動してください。 2. 上記にて回復しない場合は、SVP を再起動してください。 3. 上記にて回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS002513	ERROR	RMI-API Server のサービスが強制停止されました。このエラーは、サービス稼働中に SVP を再起動した場合に発生することがあります。SVP を再起動もしくは装置を停止した場合、Storage Device List から該当の装置を再度起動してください。その他の場合、RMI-API Server のサービスが自動的に再起動されます。3 分待っても現象が変わらない場合は、以下の手順を順番に実行してください。 1. Storage Device List から該当の装置を停止し、再度起動してください。 2. 上記にて回復しない場合は、Storage Device List からこの装置を一旦削除して、再度登録してください。 3. 上記にて回復しない場合は、SVP を再起動してください。 4. 上記にて回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。

トラブルシュートコード	障害レベル	対処方法
TRRMIS002514	ERROR	RMI-API Server のサービスとの通信で異常が発生しました。RMI-API Server のサービスが自動的に再起動されます。1 分待っても現象が変わらない場合は、以下の手順を順番に実行してください。 1. Storage Device List で設定した SVP の IP アドレスが正しいか確認し、正しくない場合は設定してください。 2. 上記にて回復しない場合は、Storage Device List から該当の装置を停止し、再度起動してください。 3. 上記にて回復しない場合は、SVP を再起動してください。 4. 上記にて回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TRRMIS002515	ERROR	RMI-API Server のサービスは異常停止しています。 TRRMIS002501 から本ログまでに出力されているトラブルシュートコードを確認し対処してください。

5.9.6　外部認証中継サービス

- 正常時ログ出力例（起動時）

```
[2018/03/19 18:08:31.265][INFO ][TREXAU000001][External Authenticator][
Initializing]
[2018/03/19 18:08:31.858][INFO ][TREXAU000002][External Authenticator][
Ready]
```

- 正常時ログ出力例（終了時）

```
[2018/03/19 21:11:48.812][INFO ][TREXAU000004][External Authenticator][
Stopping]
[2018/03/19 21:11:48.943][INFO ][TREXAU000005][External Authenticator][
Stopped]
```

- 異常時ログ出力例（起動時）

```
[2018/03/20 22:15:36.265][INFO ][TREXAU000001][External Authenticator][
Initializing]
[2018/03/20 22:15:36.364][ERROR][TREXAU000003][External Authenticator][
Stopped : An unexpected error has occurred.]
```

- 異常時ログ出力例（終了時）

```
[2018/03/20 22:20:14.317][INFO ][TREXAU000004][External Authenticator][
Stopping]
[2018/03/20 22:20:15.113][ERROR][TREXAU000006][External Authenticator][
Stopped : An unexpected error has occurred.]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TREXAU000001	INFO	外部認証中継サービスが起動されるときに出力されます。

トラブルシュートコード	障害レベル	対処方法
		外部認証中継サービスが正常に起動されているかを確認するには、本トラブルシュートコードと TREXAU000002 が出力されていることを確認してください。
TREXAU000002	INFO	外部認証中継サービスが正常に起動されています。
TREXAU000003	ERROR	外部認証中継サービスの起動に失敗しています。 Storage Device List から、該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TREXAU000004	INFO	外部認証中継サービスが停止するときに出力されます。 外部認証中継サービスが正常に停止されているかを確認するには、本トラブルシュートコードと TREXAU000005 が出力されていることを確認してください。
TREXAU000005	INFO	外部認証中継サービスが正常に停止するときに出力されます。
TREXAU000006	ERROR	外部認証中継サービスの停止でエラーが発生しました。 次回起動時に、外部認証中継サービスが正常起動（TREXAU000002）していない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TREXAU000007	ERROR	外部認証中継サービスが起動されていません。 Storage Device List から、該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TREXAU000010	ERROR	外部認証中継サービスが強制停止されました。サービス稼働中に SVP を再起動した場合に出力されることがあります。 Storage Device List から該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。 SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。
TREXAU000011	ERROR	外部認証中継サービスが強制停止されました。サービス稼働中に SVP を再起動した場合に出力されることがあります。 Storage Device List から該当の装置を選択し、停止を行ったあとに、起動を行ってください。 それでも回復しない場合は、SVP の再起動を行ってください。

トラブルシュートコード	障害レベル	対処方法
		SVP を再起動しても回復しない場合は、Storage Navigator を一旦アンインストールして、再度インストール、装置の登録を行ってください。

5.9.7　通信サービス

- 正常時ログ出力例

```
[2018/05/27 16:03:04.875][INFO ][TRCOMM000001][Communication][Ready : C
onnection to GUM2 opened.]
[2018/05/27 16:03:16.972][INFO ][TRCOMM000001][Communication][Ready : C
onnection to GUM1 opened.]
・・・
```

- 異常時ログ出力例

```
[2018/05/27 16:03:17.288][ERROR][TRCOMM000004][Communication][Failed :
Connection to GUM2 failed. Already connected MPC's IP Address is (1)10.
xx.yy.zz]
[2018/05/27 16:03:17.428][ERROR][TRCOMM000009][Communication][Failed :
Authentication failed by GUM2.]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TRCOMM000001	INFO	通信サービス起動後に GUM との通信経路接続が正常に完了したときに出力されます。
TRCOMM000002	INFO	通信サービス起動後に GUM との通信経路において機器認証が正常に完了したときに出力されます。これ以降、通信が可能となります。
TRCOMM000003	INFO	通信サービス起動後に GUM との通信経路において整合性チェックが正常に完了したときに出力されます。 (装置製番不一致、Config 型式不一致、モデル不一致が発生していない状態を示す)
TRCOMM000004	ERROR	使用する装置に対して既に他の SVP が接続されているときに出力されます。 バックグラウンドサービスログに記載されている IP アドレス※の PC で起動しているストレージシステムのサービスを停止させてください。
TRCOMM000005	WARN	[Add System] 画面で設定した CTL ごとの IP アドレスと、GUM に設定されている CTL 番号の不一致を検出したときに出力されます。 Storage Device List から CTL ごとの IP Address 設定を修正してください。 対処後にバックグラウンドサービスログを確認します。 [xxxxx yyyyyy][INFO][TRCOMM000003][Communication][Ready : Consistency check completed by GUM1.] [xxxxx yyyyyy][INFO][TRCOMM000003][Communication][Ready : Consistency check completed by GUM2.] TRCOMM000005 発生以降の時間で上記のチェック成功のログが出力されていれば回復しています。

トラブルシュートコード	障害レベル	対処方法
TRCOMM000006	WARN	［Add System］画面で設定した装置モデルと、ストレージシステムに設定されている装置モデルの不一致を検出したときに出力されます。 Storage Device List から装置を一旦削除して、正しい装置モデルで再登録してください。 対処後にバックグラウンドサービスログを確認します。 [xxxxx yyyyyy][INFO][TRCOMM000003][Communication] [Ready : Consistency check completed by GUM1.] [xxxxx yyyyyy][INFO][TRCOMM000003][Communication] [Ready : Consistency check completed by GUM2.] TRCOMM000006 発生以降の時間で上記のチェック成功のログが出力されていれば回復しています。
TRCOMM000007	WARN	［Add System］画面で設定した Config 型式と、ストレージシステムにインストールされている Config 型式の不一致を検出したときに出力されます。 Storage Device List から装置を一旦削除して、正しい Config 型式で再登録してください。 対処後にバックグラウンドサービスログを確認します。 [xxxxx yyyyyy][INFO][TRCOMM000003][Communication] [Ready : Consistency check completed by GUM1.] [xxxxx yyyyyy][INFO][TRCOMM000003][Communication] [Ready : Consistency check completed by GUM2.] TRCOMM000007 発生以降の時間で上記のチェック成功のログが出力されていれば回復しています。
TRCOMM000008	WARN	［Add System］画面で設定した装置製番と、ストレージシステムに設定されている装置製番の不一致を検出したときに出力されます。 Storage Device List から装置を一旦削除して、正しい装置製番で再登録してください。 対処後にバックグラウンドサービスログを確認します。 [xxxxx yyyyyy][INFO][TRCOMM000003][Communication] [Ready : Consistency check completed by GUM1.] [xxxxx yyyyyy][INFO][TRCOMM000003][Communication] [Ready : Consistency check completed by GUM2.] TRCOMM000008 発生以降の時間で上記のチェック成功のログが出力されていれば回復しています。
TRCOMM000009	ERROR	GUM との接続時の認証が失敗したときに出力されます。 本ログが出力された後（1 分以内）に TRCOMM000002 のトラブルシュートコードが出力されている場合、 一時的な通信障害によって出力されているため、対処は不要です。 TRCOMM000002 が出力されていない場合は、［Add System］画面で設定したユーザー名称とパスワードが誤っている可能性があります。 Storage Device List からユーザー名称とパスワードを再設定してください。 対処後にバックグラウンドサービスログを確認します。 [xxxxx yyyyyy][INFO][TRCOMM000002][Communication] [Ready : Authentication completed by GUM1.] [xxxxx yyyyyy][INFO][TRCOMM000002][Communication] [Ready : Authentication completed by GUM2.]

トラブルシュートコード	障害レベル	対処方法
		TRCOMM000009 発生以降の時間で上記の認証成功のログが出力されていれば回復しています。 正しいユーザ名・パスワードを入力しているがログインできない場合、以下の原因が考えられます。 • 管理者がユーザアカウントを無効化している。 ユーザアカウントポリシーを設定している場合に、正しいユーザ名・パスワードを入力しているがログインできない場合、以下の原因が考えられます。 • パスワード有効期限切れにより、アカウントが無効化された。 • ログイン試行可能回数を超えたため、アカウントが無効化された。 • ログイン試行可能回数を超えたため、アカウントがロックされた。 • 初回ログインである。 • API 認証などで自動的に認証を行っている場合にログイン試行回数に達したため、アカウントがロックまたはアカウントが無効化された。 以下の対処が必要です。 セキュリティ管理者（参照・編集）ロールを持つユーザと連携し、原因に応じて、以下の対応を実施してください。 • アカウントがロックされている場合は、「3.2.8.8　アカウントロックの解除（53 ページ）」を参照して、アカウントロックを解除してください。 • アカウントが無効化されてる場合は、「3.2.8.9　アカウントの有効化（53 ページ）」を参照して、アカウントを有効化してください。 - パスワード有効期限切れの場合は、パスワードの変更も実施してください。 • 初回ログインで失敗している場合は、以下の対処を実施してください。 - 該当ユーザの初回ログイン時パスワード変更要求を無効にする（「3.2.8.2　ユーザアカウントのパスワードポリシー設定（44 ページ）」参照）。 - Maintenance Utility で、初回ログインを該当ユーザのアカウントで実施する。
TRCOMM000010	INFO	通信サービス起動後に GUM との通信経路が切断されたときに出力されます。 通信経路あるいは GUM の動作状態を確認してください。
TRCOMM000011	ERROR	情報更新に失敗したときに出力されます。 自動で再実行しますが、当該ログ出力後 5 分ほど待っても TRCOMM000002 のログが出力されない場合は、Storage Device List から該当の装置を選択し、停止したあとに、再度起動してください。 それでも回復しない場合は、SVP の再起動を行ってください。
TRCOMM000012	ERROR	使用する装置に対して既に他の SVP が接続されている可能性があります。 使用する装置に対してストレージシステムのサービスを起動している他の PC がないか確認してください。既に

トラブルシュートコード	障害レベル	対処方法
		ストレージシステムのサービスが起動済みの SVP があればサービスを停止させてください。
TRCOMM000013	INFO	通信サービスが起動されるときに出力されます。 通信サービスが正常に起動されているかを確認するには、本ログと TRCOMM000002 が出力されていることを確認してください。
TRCOMM000014	INFO	通信サービスが停止されるときに出力されます。 通信サービスが正常に停止されているかを確認するには、本ログと TRCOMM000015 が出力されていることを確認してください。
TRCOMM000015	INFO	通信サービスが正常に停止したときに出力されます。
TRCOMM000016	WARN	ストレージシステムとの接続に失敗したときに出力されます。 1. SVP に 2 つ以上の LAN ポートがあると出力される場合があります。「A.4.1　ストレージシステムと SVP の IP アドレスを設定する（182 ページ）」を参照してください。 2. Storage Device List に設定された CTL1 と CTL2 の IP アドレス、またはホスト名を確認してください。 • IP アドレスが誤っている場合 このストレージシステムのサービスを停止してから、正しい IP アドレスを設定してください。設定後に、サービスを再起動してください。 • ホスト名が誤っている場合 DNS サーバに設定されているホスト名と CTL の IP アドレスを確認してください。設定が誤っている場合は、このストレージシステムのサービスを停止してから、DNS サーバの設定、または、Storage Device List のホスト名の設定を変更してください。設定変更後に、サービスを再起動してください。 • IP アドレスまたはホスト名が正しい場合 「C.15　SVP 接続用証明書と 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（261 ページ）」と「C.16　SVP 接続用証明書を SVP へアップロード（262 ページ）」を参照し、証明書を再設定してください。 3. 手順 2 で解決しない場合は、管理クライアントのブラウザにコントローラボードの IP アドレスを入力して、Maintenance Utility にログインできることを確認します。 ログインできない場合は、管理クライアントとストレージシステム間の通信経路、または GUM の動作状態に問題がある可能性があります。「5.5　Maintenance Utility の操作時にトラブルが発生した場合の対処手順（122 ページ）」を参照して対処してください。 4. Maintenance Utility にログインできることを確認した後に、バックグラウンドサービスログを確認します。 約 10 分の間に、TRCOMM000016 が複数出力されている場合は、Storage Device List で、対象のストレージシステムのサービスを再起動（[Stop Service]→[Start Service]）してください。 5. バックグラウンドサービスログを確認します。

トラブルシュートコード	障害レベル	対処方法
		回復している場合には、TRCOMM000016 出力以降に、以下のメッセージが出力され、かつ、再度 TRCOMM000016 が出力されません。 [xxxxx yyyyyy][INFO][TRCOMM000002] [Communication] [Ready : Authentication completed by GUM1.] [xxxxx yyyyyy][INFO][TRCOMM000002] [Communication] [Ready : Authentication completed by GUM2.] 6. バックグラウンドサービスログに、操作手順 5.のメッセージが出力されていない場合は、GUM をリブートしてください（3.12.6　GUM のリブート（92 ページ）参照）。
TRCOMM000017	ERROR	通信サービスが異常終了しました。
TRCOMM000018	ERROR	通信サービスが強制停止されました。 通信サービス起動中に SVP を再起動した場合に出力されることがあります。 Storage Device List からこのストレージシステムのサービスを停止し、再度起動してください。

注※

ルータで IP アドレス変換を行っている場合は、PC 本体の IP アドレスと異なる場合があります。その場合は、ネットワーク管理者に確認してください。

5.9.8　KMIP コミュニケータ

- 異常時ログ出力例

```
[2017/11/19 10:49:49.617][ERROR][TRKMIP000001][KMIPCom][Failed : SSL se
ttings are invalid.]
```

トラブルシュートコードと対処方法は次のとおりです。

トラブルシュートコード	障害レベル	対処方法
TRKMIP000001	ERROR	KMIP コミュニケータサービスで、予期せぬエラーが発生しました。 「5.11.1　ダンプツールを使用した採取（163 ページ）」を参照して、ダンプファイルの採取を行ってください。 採取に失敗した場合は、「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照して、手動で該当するファイルを採取してください。

5.10　仮想メモリの設定方法

ストレージシステム単位でサービスを開始すると、バックグラウンドサービスログに TRSTNA000007 が出力され、サービスが起動できない場合があります。以下の手順に従い、仮想メモリの初期サイズ、および最大サイズを変更してください。

すでに Windows の仮想メモリが設定されていても変更してください。

操作手順

1. ［コントロールパネル］から［システム］－［システムの詳細設定］を選択して、システムのプロパティを開きます。
2. システムのプロパティの［詳細設定］－［パフォーマンス］－［設定］を選択しパフォーマンス オプションを開きます。
3. パフォーマンス オプションの［詳細設定］－［仮想メモリ］－［変更］を選択し仮想メモリを開きます。
4. 仮想メモリで以下の設定を行います。
   a. ［すべてのドライブのページングファイルのサイズを自動的に管理する］のチェックを OFF にします。
   b. ドライブで任意のドライブを選択します。(C ドライブ以外を推奨)
   c. カスタムサイズを選択し、初期サイズ、最大サイズの両方をダイアログ下部に表示されている［推奨］の値を設定します。
5. SVP を再起動します。

5.11　ダンプファイルの採取方法

5.11.1　ダンプツールを使用した採取

ダンプファイルは、保守員が障害の解析を行うために使用します。ダンプツールを使用すると、Storage Navigator の構成情報を採取できます。

次の契機でダンプファイルを採取します。

- Storage Navigator 操作のトラブルシューティング

  SVP から情報を採取して、保守員にお渡しください。

- ストレージ管理ソフトウェア、および SVP ソフトウェアを削除する前

  SVP のソフトウェア設定情報をバックアップしてください（詳細は「G.2.9.1　SVP のソフトウェア設定情報のバックアップ（356 ページ）」を参照）。

ダンプツールには、次の種類があります。

特別な指示が無い限り、通常ダンプツールを使用して採取してください。

- 通常ダンプツール（ファイル名：Dump_Normal.bat）：

  通常ダンプファイルを取得する場合に使います。通常ダンプファイルには、SVP に関するすべての情報、およびストレージシステムに関する最小限の情報が含まれます。

Storage Navigator の表示に問題があるなど、システムに重大な障害がない場合に使います。

- 詳細ダンプツール（ファイル名：Dump_Detail.bat）：

  詳細ダンプファイルを取得する場合に使います。通常ダンプの内容に加え、ストレージシステムに関するすべての情報が含まれます。Storage Navigator が起動しなくなった場合やストレージシステムの問題有無を判定する場合に使います。

- 初期解析ダンプツール（ファイル名：Dump_MoreRapid.bat）

  初期解析ダンプファイルを取得する場合に使います。初期解析に必要な SSB および SIM を解析できる最小限のダンプの内容に絞っています。障害発生時にできる限り早く問題個所の解析を始める必要がある場合に使います。このダンプツールは、次の SVP ソフトウェアバージョンで使用できます。

  - iStorage V100, V300 の場合：93-06-21-XX/XX 以降
  - iStorage V10e の場合：全バージョン

メモ

複数のタスクが存在すると、ダンプファイルのサイズが大きくなる場合があります。このため、障害が発生した時点から、1 ヶ月以上前のタスクを削除した後に、ダンプファイルを採取することを推奨します。

前提条件

- SVP にログイン済みであること。
- Storage Navigator が起動していること。※
- ほかのユーザがダンプツールを使用中でないこと。
- 保守作業が進行中でないこと。
- ほかのストレージシステムのダンプツールが使用中でないこと。
- Storage Navigator のインストールディレクトリがウィルス検出プログラムのリアルタイムウィルススキャン対象から除外されていること。ウィルス検出プログラムの設定については、「4.3　ウィルス検出プログラムの使用に関する注意事項（97 ページ）」を参照してください。
- ダンプファイルの出力先として指定するフォルダがウィルス検出プログラムのリアルタイムウィルススキャン対象から除外されていること。

注※

- Storage Navigator の起動に関するトラブルの場合は、Storage Navigator が起動していない状態でダンプツールを使用して SVP に関する情報を採取してください。

- Storage Navigator を起動していなくても、Storage Device List に表示されるストレージシステムの状態が、［Ready］であればダンプツールを使用できます。［Warning］、または［Error］でもダンプツールを使用できますが、DKC のダンプと GUM のダンプが採取されない場合があります。DKC のダンプと GUM のダンプの有無は、操作手順 4.に示す「DumpResult.txt」で確認できます。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールがインストールされているディレクトリに移動します。

   例えば、装置識別番号が 934000600001 の場合、ツールがインストールされているディレクトリは、C:\Mapp\wk\934000600001\DKC200\mp\pc です。

   この場合、次のように入力します。

   cd /d C:\Mapp\wk\934000600001\DKC200\mp\pc

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. ダンプファイルの出力先フォルダを指定して、通常ダンプツール（Dump_Normal.bat）、詳細ダンプツール（Dump_Detail.bat）、または初期解析ダンプツール（Dump_MoreRapid.bat）を実行します。

   実行例はコマンドプロンプトで「Dump_Detail.bat <出力先ディレクトリ（絶対パス）>」と入力します。

   例えば、詳細ダンプツールの実行結果を C:\Result_934000600001 に出力する場合、次のように入力します。

   Dump_Detail.bat C:\Result_934000600001

   メモ

   - ツールがインストールされているフォルダにある他のファイルを誤って操作しないように注意してください。
   - コマンドを入力する時にダンプツールのバッチファイルと出力先のディレクトリの間には、半角スペースが必要です。
   - ダンプファイル名は hdcp.tgz 固定です。ストレージシステムごとにダンプファイルを管理するために、出力先のフォルダ名に装置識別番号を付けることを推奨します。

     （例）装置識別番号：934000600001

フォルダ名：C:\Result_934000600001

- ネットワークドライブ配下のフォルダは出力先として指定できません。
- ツールの実行中、コマンドプロンプト画面には「Executing…」が表示されます。ツールの実行が完了すると、コマンドプロンプト画面には「zSv_AutoDump.exe is completed.」が表示されます。
- SVP が高負荷になっているなどの要因で、ツールの実行が完了しても「zSv_AutoDump.exe is completed.」が表示されない可能性があります。また、ツールの実行に失敗すると、コマンドプロンプト画面には「zSv_AutoDump.exe is failed.」が表示されます。

  20 分以上経過しても表示されない場合は、ダンプファイルの出力先にダンプファイルが出力されているか確認してください。

  ダンプファイルが出力されている場合は、ファイルの更新日時がダンプツールの実行開始時間から 20 分経過していることを確認し、操作手順の項番 4 へ進んでください。

  ダンプファイルが出力されていない場合は、コマンドプロンプトを閉じてから、ダンプツールを再実行してください。
- 装置の使用状況により、ダンプファイルの容量は最大 3GB 程度になることがあります。
- ダンプツールを実行すると「zSv_AutoDump.exe is failed.」が表示される場合、Storage Navigator のインストールディレクトリが、ウィルス検出プログラムの除外対象に設定されていない可能性があります。「4.3　ウィルス検出プログラムの使用に関する注意事項（97 ページ）」を参照して除外対象に設定してください。

---

4. 出力されたダンプファイルを確認します。

   次のファイルが格納されています。

   - hdcp.tgz：ダンプファイルです。ダンプファイルを SVP のストレージに多数出力すると SVP のストレージの空き容量が不足する可能性があります。ダンプファイルは、SVP 以外のストレージに移動してください。
   - zSv_AutoDump.log：ダンプツールのログファイルです。ダンプファイルが出力されていない場合、このログファイルを保守員にお渡しください。
   - DumpResult.txt : 下記に示す項目の採取結果が格納されます。採取が成功した場合は「exist」、採取が失敗した場合は「not exist」と表示されます。

項目	内容
DKC dump	DKC のダンプの採取結果
Dump of GUM of CTRL1	GUM（CTL1）のダンプの採取結果
Dump of GUM of CTRL2	GUM（CTL2）のダンプの採取結果

5. コマンドプロンプトを閉じます。
6. OS のトラブルによってダンプツールでのダンプ採取が失敗する可能性があります。

ダンプ採取が失敗した場合は、「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照して、ダンプファイルを採取してください。

5.11.2　手動によるダンプファイルの採取

Storage Navigator のインストールまたはセットアップの途中でトラブルが発生すると、ダンプツールが使えなくなる可能性があります。そのような場合は、次の手動採取ファイル一覧に示すファイルを採取して、保守員にお渡しください。

手動採取ファイル一覧

- %USERPROFILE%\AppData\LocalLow\Sun\Java\Deployment\log*.*
- %WINDIR%\minidump*.dmp
- %WINDIR%\system32\config\AppEvent.Evt
- %WINDIR%\system32\config\SecEvent.Evt
- %WINDIR%\system32\config\SysEvent.Evt
- %WINDIR%\system32\drivers\etc\HOSTS*
- %WINDIR%\system32\drivers\etc\services*
- %WINDIR%\System32\Winevt\Logs\Application.evtx
- %WINDIR%\System32\Winevt\Logs\Security.evtx
- %WINDIR%\System32\Winevt\Logs\System.evtx
- <installDir>\OSS\apache\logs*.log
- <installDir>\OSS\jetty\logs*.log
- <installDir>\OSS\jetty2\logs*.log
- <installDir>\OSS\jetty3\logs*.log
- <installDir>\OSS\jetty11.0\logs*.log
- <installDir>\wk\supervisor\comweb\logs*.*
- <installDir>\wk\supervisor\dkcman\cnf*.*
- <installDir>\wk\supervisor\dkcman\log*.*
- <installDir>\wk\supervisor\mappiniset\logs\MappIniSet*.*
- <installDir>\wk\supervisor\mappiniset\mpprt\cnf
- <installDir>\wk\supervisor\microsetup\log*.*
- <installDir>\wk\supervisor\portmanager\cnf*.*
- <installDir>\wk\supervisor\portmanager\logs\PortManager*.*

- <installDir>\wk\supervisor\restapi\build.json
- <installDir>\wk\supervisor\restapi\data
- <installDir>\wk\supervisor\restapi\logs
- <installDir>\wk\supervisor\restapi\version.json
- <installDir>\wk\supervisor\rmiserver\cnf*.*
- <installDir>\wk\supervisor\rmiserver\log*.*
- <installDir>\wk\supervisor\sdlist\log*.*
- <installDir>\wk\supervisor\system\log*.log
- <installDir>\wk\[装置識別番号]\DKC200\config*.cfg
- <installDir>\wk\[装置識別番号]\DKC200\mp\pc*.dbg
- <installDir>\wk\[装置識別番号]\DKC200\mp\pc*.dmb
- <installDir>\wk\[装置識別番号]\DKC200\mp\pc*.dmp
- <installDir>\wk\[装置識別番号]\DKC200\mp\pc*.inf
- <installDir>\wk\[装置識別番号]\DKC200\mp\pc*.ini
- <installDir>\wk\[装置識別番号]\DKC200\mp\pc*.trc
- <installDir>\wk\[装置識別番号]\DKC200\others\commdata*.*
- <installDir>\wk\[装置識別番号]\DKC200\san\cgi-bin\utility\log*.*
- <installDir>\wk\[装置識別番号]\DKC200\san\SN2\logs*.*
- <installDir>\wk\[装置識別番号]\DKC200\san\SN2\SN2Files\logs*.*
- <installDir>\wk\[装置識別番号]\SMI\logs*.*
- c:\SetupTrace*.*

ヒント

- <installDir>…ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。
- %USERPROFILE%…SVP のインストールログインユーザーのフォルダを示します。
  (=C:\Users\<ユーザー名>)
- %WINDIR%…システムドライブにある Windows フォルダを示します。
  (=C:\Windows)
- [装置識別番号]…(例) 装置識別番号：934000600001 の場合は、以下のフォルダ名になります。
  <installDir>\wk\934000600001\DKC200\mp\pc*.trc
- 運用環境によって存在しないファイルがあります。存在しないファイルは無視してください。

5.12　SVP のパフォーマンスに関する問題がある場合の対処手順

SVP のパフォーマンスに関する下記の現象が認められる場合、SVP のパフォーマンス情報を採取していただき、ダンプファイルと合わせて保守員にお渡しください。

- SVP の動作が遅い
- SVP の CPU 使用率が高い
- Storage Device List、または Storage Navigator の動作が遅いなど

⚠ 注意

本手順で紹介するツールは、SVP 自体のパフォーマンス情報を採取します。Storage Device List に登録されている全てのストレージシステムの装置識別番号のディレクトリ内にインストールされていますが、個々のストレージシステムのパフォーマンス情報を採取するツールではありません。ただしツールを起動したディレクトリに対応するストレージシステムのダンプファイル採取する機能は含まれています。このため、ツールを起動したディレクトリに対応するストレージシステム以外のストレージシステムに対しては、「5.11.1　ダンプツールを使用した採取（163 ページ）」または「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照してダンプファイルを採取して保守員にお渡しください。

SVP のパフォーマンス情報は、下記の操作手順に示すツールで採取します。なお、採取には約 30 分かかります。

その後ダンプファイルが自動で採取されます。

前提条件

- SVP のパフォーマンスに関する問題が発生している状態であること。
- SVP にログイン済みであること。
- Storage Navigator が起動していること。※
- ほかのユーザがダンプツールを使用中でないこと。
- 保守作業が進行中でないこと。
- ほかのストレージシステムのダンプツールが使用中でないこと。
- Storage Navigator のインストールディレクトリがウィルス検出プログラムのリアルタイムウィルススキャン対象から除外されていること。ウィルス検出プログラムの設定については、「4.3　ウィルス検出プログラムの使用に関する注意事項（97 ページ）」を参照してください。

注※

Storage Navigator の起動に関するトラブルの場合は、Storage Navigator が起動していない状態でダンプツールを使用して SVP に関する情報を採取してください。

⚠ 注意

ツールの動作により、SVP のパフォーマンスがさらに悪化する可能性があります。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールがインストールされているディレクトリに移動します。

   例えば、装置識別番号が 934000600001 の場合、ツールがインストールされているディレクトリは、C:\Mapp\wk\934000600001\DKC200\mp\pc です。

   この場合、次のように入力します。

   cd /d C:\Mapp\wk\934000600001\DKC200\mp\pc

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. SVP のパフォーマンス情報とダンプファイルの出力先フォルダを指定してパフォーマンス情報採取ツール（GetSVPPerfInfo.bat）を実行します。

   実行例はコマンドプロンプトで「GetSVPInfo.bat <出力先ディレクトリ（絶対パス）>」と入力します。

   例えば、SVP のパフォーマンス情報とダンプファイルを C:\Result_934000600001 に出力する場合、次のように入力します。

   GetSVPPerfInfo.bat C:\Result_934000600001

   出力先ディレクトリの指定をせず実行した場合、下記のフォルダに出力されます。

   C:\Mapp\wk\934000600001\DKC200\tmp\PerfLog

   934000600001 は装置識別番号です。

   メモ

   - ツールがインストールされているフォルダにある他のファイルを誤って操作しないように注意してください。
   - コマンドを入力する時にダンプツールのバッチファイルと出力先のディレクトリの間には、半角スペースが必要です。

- ネットワークドライブ配下のフォルダは出力先として指定できません。
- ツールの実行中はコマンドプロンプト画面をクリックしたり、閉じたりしないでください。
- ツールの実行中、コマンドプロンプト画面には「Executing…」が表示されます。
- SVP のパフォーマンス情報の取得が終わると自動的にダンプツールによるダンプ採取が始まります。

  ダンプツールの実行中は「5.11.1　ダンプツールを使用した採取（163 ページ）」も参照してください。
- パフォーマンス情報とともに、SVP のシステム情報も採取します。システム情報の採取中にダイアログが表示されますが、キャンセルボタンを押すなどの操作を行わないでください。システム情報の採取中か終了すると、ダイアログは自動で閉じます。
- 処理が全て終了すると、コマンドプロンプト画面に「SVP Performance Information tool is completed.」が表示されます。

---

4. 出力されたダンプファイルを確認します。

   次のファイルが格納されています。

   - CounterResult_YYYYMMDDhhmmss.blg : Windows のパフォーマンスモニターのログです。
   - ProcessList_YYYYMMDDhhmmss.csv：SVP 上で起動しているプロセスの情報です。

   以下のファイルの詳細は「5.11.1　ダンプツールを使用した採取（163 ページ）」を参照してください。

   - Sysinfo_YYYYMMDDhhmmss.txt：SVP のシステム情報です。
   - hdcp.tgz
   - zSv_AutoDump.log
   - DumpResult.txt
5. コマンドプロンプトを閉じます。
6. OS のトラブルによってダンプツールでのダンプ採取が失敗する可能性があります。

   操作手順 4.で示したダンプツールの出力結果が出力されていない場合は、「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照して、ダンプファイルを採取してください。
7. 操作手順 4.で出力された全てのファイルを保守員へ送付してください。

5.13　ネットワークトレース採取ツールの使用方法

SVP が接続されているネットワークに異常な現象が発生した場合、ネットワークトレース採取ツールを使用して、SVP のネットワークトレース（パケットキャプチャ）を採取します。

⚠ 注意

- 保守員から採取の依頼があった場合に使用してください。

  なお、本ツールを使用すると、SVP のネットワークを流れるすべてのパケットの情報を採取します。このため、本ツールを使用する前に、採取した情報を弊社に送付していただくことに同意願います。同意いただけない場合は、保守員にご連絡ください。
- 採取した情報の取り扱いは、十分に注意してください。
- ネットワークトレース採取ツールの使用中は、他の保守作業を行わないでください。

メモ

- SVP ソフトウェアは、以下のバージョンを使用してください。
  - 93-06-22-XX/XX 以降
  - 93-06-02-XX/XX～93-06-21-XX/XX 未満
  - 93-05-05-XX/XX～93-05-21-XX/XX 未満
- ネットワークトレース採取ツールの使用中に、ネットワークの異常な現象を再現させる必要があります。

  事前に SVP でネットワークの異常な現象が再現できることを確認してください。再現できない場合は、保守員にご連絡ください。
- ネットワークトレースを採取したあとに、ダンプを採取します。なおダンプツールは自動で起動します。このため、ネットワークトレースとダンプを格納するために 8GB の空き容量が必要です。
- ネットワークトレース採取ツールの使用中に、SVP の NIC がリンクダウン（瞬断）する場合があります。これはツールが内部で使用している Windows の OS 標準コマンドの「netsh trace」によるもので、特に問題はありません。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールがインストールされているディレクトリに移動します。

   例えば、装置識別番号が 934000600001 の場合、ツールがインストールされているディレクトリは、C:\Mapp\wk\934000600001\DKC200\mp\pc です。

   この場合、次のように入力します。

   cd /d C:\Mapp\wk\934000600001\DKC200\mp\pc

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. SVP のネットワークトレースとダンプファイルの出力先フォルダを指定してネットワークトレース採取ツール（GetNetTrace.bat）を実行します。

   実行例はコマンドプロンプトで「GetNetTrace.bat <出力先ディレクトリ（絶対パス）>」と入力します。

   例えば、SVP のネットワークトレースとダンプファイルを C:\Result_934000600001 に出力する場合、次のように入力します。

   GetNetTrace.bat C:\Result_934000600001

   メモ

   - ツールがインストールされているフォルダにある他のファイルを誤って操作しないように注意してください。
   - コマンドを入力する時にダンプツールのバッチファイルと出力先のディレクトリの間には、半角スペースが必要です。
   - 出力先ディレクトリとしてネットワークドライブは指定できません。
   - ツールの実行中はコマンドプロンプト画面をクリックしたり、閉じたりしないでください。画面を閉じてしまった場合は、SVP を再起動してください。
   - ツールの実行中、コマンドプロンプト画面には「Executing…」が表示されます。

4. コマンドプロンプト画面に、以下のメッセージが表示されますが、なにも操作しないでください。

   Do you want to stop the network tracing session?(Y):

5. ネットワーク関連の現象を再現します。
6. ネットワーク関連の現象が再現したのち、コマンドプロンプト画面で大文字の Y を入力します。これによりネットワークトレースの採取が停止します。

   ネットワーク関連の現象が再現した後は、ただちにネットワークトレース取得の停止を行ってください。少なくとも 1 時間以内に停止しないと、ネットワークトレースが残らない場合があります。

7. ネットワークトレースの取得を停止すると、ダンプツールが自動で起動します。

   ダンプが終了すると、コマンドプロンプト画面に「Network Trace tool END.」が表示されます。

8. ネットワークトレースとダンプファイルの出力先フォルダに出力されたファイルを確認します。

次のファイルが格納されています。

- SVP_NetTrace.etl : ネットワークトレースログ
- SVP_NetTrace.cab : ネットワークトレースログに関する関連情報のログ。本ファイルは出力されない場合もあります。
- hdcp.tgz
- zSv_AutoDump.log
- DumpResult.txt

9. コマンドプロンプトを閉じます。
10. OS のトラブルによってダンプツールでのダンプ採取が失敗する可能性があります。

    操作手順 8.で示したダンプツールの出力結果が出力されていない場合は、「5.11.2　手動によるダンプファイルの採取（167 ページ）」を参照して、ダンプファイルを採取してください。
11. 操作手順 8.で出力された全てのファイルを保守員へ送付してください。

5.14　ストレージシステムに対するネットワーク監視で通信不可または疎通不可が発生した場合の対処

GUM の状態監視で、GUM の停止を検出した場合、救済措置として、GUM がリブートされることがあります。その際、一時的な LAN 通信不可または Ping 疎通不可や、接続 LAN ポートのリンクダウン/リンクアップが発生します。また、SNMP による監視をしている場合は、ColdStart トラップが発行されます。

GUM は、リブート完了後、正常状態に自動で回復します。このため、LAN ポートがリンクアップしていて、ネットワークの通信障害または疎通障害が回復していれば、対処は不要です。

5.15　USN ジャーナルの使用容量が不足した場合の対処

SVP ソフトウェアは、ストレージシステムのサービスが起動している間、SVP ソフトウェアがインストールされているドライブの、ファイルを頻繁に更新します。そのため、USN ジャーナルを採取する機能が有効に設定されていると、USN ジャーナルの容量を消費します。以下の操作手順を参照して、USN ジャーナルの容量が不足していると判断した場合は、USN ジャーナルを削除してください。

メモ

システムドライブ以外のドライブの場合、USN ジャーナルを採取する機能を無効に設定できます（デフォルトは無効です）。無効に設定されている場合は、本トラブルは発生しません。

一方、有効に設定すると USN ジャーナルの容量が不足する場合があります（システムドライブのデフォルトは有効です）。特に 1 台の SVP に複数のストレージシステムを登録している場合は、USN ジャーナルの容量を消費する量が登録している台数分増えるため、容量不足になる時間間隔が短くなります（1 台の SVP に 8 台のストレージシステムを登録している場合、1 年程度）。

容量が不足すると SVP の動作が不安定となり、次に示すような状態が発生します。

- Storage Device List や Storage Navigator が起動できない。
- Storage Device List や Storage Navigator の起動中または操作時に、エラーメッセージが表示される。
- 管理サーバ（SVP）のエクスプローラーでファイルをコピーできない。

上記のような状態が発生した場合は、USN ジャーナルの容量を確認してください（4KB の Cluster Size の NTFS ファイルシステムの場合、USN ジャーナルの容量は 16TB となります。その他の条件の場合は、マイクロソフト社のホームページを参照してください）。

前提条件

ストレージ管理ソフトウェア、および SVP ソフトウェアが停止していること

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. USN ジャーナルの使用容量を確認します。※

   `fsutil usn queryjournal [SVP` **ソフトウェアがインストールされているドライブのドライブレター**`]`

   [] 内：引数

   USN ジャーナルの使用容量に余裕があると判断した場合は、作業を終了してください。
3. USN ジャーナルを削除します。※

   `fsutil usn deletejournal [SVP` **ソフトウェアがインストールされているドライブのドライブレター**`]`
4. システムドライブ以外のドライブの USN ジャーナルを削除した場合は、USN ジャーナルを採取する機能を有効に設定してください。

   メモ

   システムドライブ以外のドライブの USN ジャーナルを削除すると、USN ジャーナルを採取する機能が無効に変わるため、USN ジャーナルを採取できなくなります。
5. USN ジャーナルが削除されたことを確認します（操作手順 2.を参照）。

   削除されていない場合は、再度削除してください（操作手順 3.を参照）。

6. コマンドプロンプトを閉じます。
7. SVP を再起動します。

注※

これらのコマンドは変更される可能性があります。動作しない場合は、マイクロソフト社のホームページを参照し、変更後のコマンドを実行してください。

5.16　RAID Manager の停止手順

RAID Manager のサービスを、コマンドプロンプトまたは PowerShell で停止する手順を説明します。

1. コマンドプロンプトまたは PowerShell を管理者権限で実行し、RAID Manager のデフォルトのサービス名 HORCM の情報を表示します。

メモ

HORCM は RAID Manager のデフォルトのサービス名です。HORCM 以外の名称でサービス名を登録している場合は、HORCM を該当のサービス名に置き換えてください。

- コマンドプロンプトを使用する場合：
  a. コマンドプロンプトを管理者として起動します。
  b. 次のコマンドを実行して、RAID Manager のサービス HORCM の情報を表示します。

```
C:\windows\system32>sc query state= all | findstr HORCM
SERVICE_NAME: HORCM0
DISPLAY_NAME: HORCM0
```

- PowerShell を使用する場合：
  a. Windows + R キーで「ファイル名を指定して実行」を開き、”powershell”と入力し、[OK]で起動します。
  b. 次のコマンドで管理者として実行します。

```
Start-Process powershell -Verb runas
```

  c. 次のコマンドを実行して、RAID Manager のサービス HORCM の情報を表示します。

```
PS C:\Windows\System32> Get-WmiObject win32_service |?{$_.Path
name -like '*\HORCM\Tool\svcexe.exe*'} | select Name, Pathname
Name   Pathname
----   --------
HORCM0 C:\HORCM\Tool\svcexe.exe /S=HORCM0
```

出力結果の“Name”列に表示される文字列が RAID Manager のサービス名です。

ヒント

OS は、1 つのサービスを同時に複数実行する場合、それぞれのサービスを区別できるように、サービス名に個別の番号（インスタンス番号）を付加します（HORCM0 の「0」）など。

2. RAID Manager サービスを停止します。

   - 手順 1 の出力結果に、RAID Manager のデフォルトのサービス名 HORCM を含む行が表示された場合：

     次のコマンドを実行し、実行中のサービス HORCM を停止します。

     インスタンス番号 0 の HORCM を停止する例：

     ```
     net stop HORCM0
     ```

     再び、上記のコマンドを実行して、メッセージ「HORCM0 サービスは開始されていません。」と表示され、サービスが停止したことを確認してください。

     HORCM のサービスが複数起動している場合（複数のインスタンスがある場合）は、すべての HORCM のサービスを停止してください。

   - 手順 1 の出力結果が何も表示されなかった場合：

     次のコマンドを実行して、horcmgr.exe を強制終了します。

     ```
     TASKKILL /IM “horcmgr.exe” /T /F
     ```

     再び、上記のコマンドを実行して、メッセージ「エラー: プロセス“horcmgr.exe”が見つかりませんでした。」と表示され、サービスが停止したことを確認してください。

3. コマンドプロンプトまたは PowerShell を閉じます。

付録 A. 初期設定作業

ストレージシステムを動作させるためには、管理クライアントや SVP、ストレージシステムのネットワーク設定をしたあと、管理 GUI アクセス用のソフトウェア、ストレージ管理ソフトウェア、SVP ソフトウェアのインストール、ストレージシステムの登録、およびストレージシステムの初期設定を行います。

A.1 初期設定作業の概要

ストレージシステムの初期設定作業を行う前に、作業の目的と流れを理解します。

A.1.1 初期設定作業の目的

ストレージシステムを構築して運用する前段階として、構成要素である管理クライアントや SVP、ストレージのネットワーク設定を行い、管理 GUI アクセス用のソフトウェア、ストレージ管理ソフトウェア、SVP ソフトウェアのインストール、ストレージシステムの登録、およびストレージシステムの初期設定を行います。ストレージシステムを使用できる状態にすることが初期設定作業の目的です。

A.1.2 初期設定作業の項目

下記の表を参照して、初期設定を行ってください。

初期設定作業の項目	iStorage V シリーズ
A.1.3 初期設定作業を実施するための前提条件（179 ページ）	○
A.2 管理クライアントの初期設定を行う（180 ページ）	○
A.2.1 管理クライアントの IP アドレスを設定する（180 ページ）	○
A.2.2 管理クライアントにロケールを設定する（181 ページ）	○
A.3 管理クライアントに必要なソフトウェアをインストールする（181 ページ）	○
A.4 SVP とストレージシステムおよび管理クライアントのネットワーク設定をする（181 ページ）	○
A.4.1 ストレージシステムと SVP の IP アドレスを設定する（182 ページ）	○
A.4.2 管理クライアントと SVP を接続するためのファイアウォールの設定（185 ページ）	○
A.4.3 SVP とストレージシステムを接続するためのファイアウォールの設定（186 ページ）	○
A.5 管理サーバ（SVP）の初期設定を行う（187 ページ）	○
A.5.1 SVP のシステム日時を設定する（188 ページ）	○
A.5.2 管理サーバ（SVP）にロケールを設定する（188 ページ）	○
A.6 管理サーバ（SVP）に必要なソフトウェアをインストールする（191 ページ）	○
A.6.1 インストール作業手順（192 ページ）	○
A.7 管理サーバ（SVP）にストレージシステムを登録する（199 ページ）	○

初期設定作業の項目	iStorage V シリーズ
A.7.1 管理サーバ（SVP）にストレージシステムを登録する（199 ページ）	○
A.8 デスクトップヒープの指定値を変更する（206 ページ）	○
A.8.1 デスクトップヒープの指定値をバッチファイルで変更する（206 ページ）	○
A.8.2 デスクトップヒープの指定値を Windows のデフォルト値に戻す（207 ページ）	○
A.9 ストレージシステムの初期設定を行う（208 ページ）	○
A.9.1 Storage Navigator にログインする（208 ページ）	○
A.9.4 管理クライアントに Web Console Launcher を設定する（217 ページ）	○
A.9.5 SVP の Web Console Launcher を設定する（218 ページ）	○
A.9.6 ストレージシステム情報を編集する（218 ページ）	○
A.10 初期設定作業を確認する（219 ページ）	○
付録 C. SSL 通信の設定（245 ページ）	○※

（凡例）

○：設定要

×：設定不要

注※

通信のセキュリティを高めるため、SSL 通信の設定を実施することを推奨します。

A.1.3 初期設定作業を実施するための前提条件

ストレージシステムの初期設定作業を行う前に、次の条件を満たしていることを確認してください。

- ストレージシステムの設置作業が完了していること
- ストレージシステムの電源が ON になっていること
- SVP および管理クライアントが要件を満たしていること
- ストレージシステムに障害が発生していないこと
- ストレージシステムに接続するサーバに障害が発生していないこと

SVP の要件は、「1.6.2 管理サーバ（SVP）の要件（19 ページ）」を参照してください。管理クライアントの要件は、「1.6.3 管理するための PC（管理クライアント）要件（25 ページ）」を参照してください。

ストレージシステムの動作状態は、コントローラシャーシの LED で確認できます。『ハードウェア リファレンスガイド』を参照してください。

A.2 管理クライアントの初期設定を行う

システム運用に必要な管理クライアントの IP アドレス、およびロケール設定を行います。

Windows11 バージョン 24H2 以降で、次に示す SVP ソフトウェアバージョンの Storage Navigator を操作する場合、管理クライアントに WMIC 機能を追加する必要があります。

- iStorage V100, V300 の場合：93-07-25-XX/XX 以前
- iStorage V10e の場合：88-08-17-XX/XX 以前

A.2.1 管理クライアントの IP アドレスを設定する

管理クライアントの LAN ポートの IP アドレスを設定します。

メモ

ストレージシステムの初期設定は、管理クライアントと SVP、ストレージシステムを管理 LAN に接続して行います。このため、管理クライアント、SVP およびストレージシステムのネットワークセグメントが一致している必要があります。お客様のネットワーク環境にあわせて管理クライアントの IP アドレスを設定してください。設定方法は使用している OS のマニュアルを参照してください。

管理クライアントから SVP にリモートデスクトップ接続して SVP の初期設定を行う場合は、ストレージシステムのデフォルトの IP アドレスにあわせて、管理クライアントの IP アドレスを仮設定します。

ストレージシステムのデフォルトの IP アドレスは次のとおりです。

- コントローラボード#1 側管理ポート：192.168.0.16
- コントローラボード#2 側管理ポート：192.168.0.17
- サブネットマスク：255.255.255.0

管理クライアントの IP アドレスは、192.168.0.xxx（xxx：1～254 の範囲で 16、17 以外の数値）で仮設定してください。SVP とストレージシステムの IP アドレスの設定が完了したあと、管理クライアントの IP アドレスをお客様のネットワーク環境にあわせて設定し直してください。その際、管理クライアントとストレージシステムの IP アドレスが、同一セグメントである必要はありません。

関連リンク

参照先トピック

ストレージシステムと SVP の IP アドレスを設定する（182 ページ）

A.2.2 管理クライアントにロケールを設定する

SVP にインストールするストレージ管理ソフトウェア、および SVP ソフトウェアのサポート言語は英語と日本語です。このため管理クライアントのロケールも英語、または日本語のどちらかに設定してください（ロケールの操作手順は「A.5.2 管理サーバ（SVP）にロケールを設定する（188 ページ）」を参照）。

A.2.3 管理クライアントに WMIC 機能を追加する

Windows11 バージョン 24H2 以降で、次に示す SVP ソフトウェアバージョンの Storage Navigator を操作する場合、管理クライアントに WMIC 機能を追加する必要があります。

- iStorage V100, V300 の場合：93-07-25-XX/XX 以前
- iStorage V10e の場合：88-08-17-XX/XX 以前

WMIC 機能を追加する操作手順の詳細は「A.5.3 管理サーバ（SVP）に WMIC 機能を追加する（190 ページ）」を参照してください。

A.3 管理クライアントに必要なソフトウェアをインストールする

管理クライアントから管理 GUI にアクセスするために必要なソフトウェアを、管理クライアントにインストールします。「1.6.3.2 管理クライアントを利用するために必要なソフトウェア（26 ページ）」に従って、必要なソフトウェアを管理クライアントにインストールしてください。

メモ

- 管理クライアントから SVP の Storage Navigator に直接ログインして使用する場合は、管理クライアントのセットアップが必要です。『HA Device Manager - Storage Navigator ユーザガイド』を参照し、セットアップを行ってください。

A.4 SVP とストレージシステムおよび管理クライアントのネットワーク設定をする

SVP 上で、ストレージシステムの LAN ポートと、ストレージシステムに接続する SVP の LAN ポートの IP アドレスを設定します。

また、ストレージシステムと SVP を接続するためのファイアウォール、および管理クライアントと SVP を接続するためのファイアウォールを設定します。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、ネットワーク設定を行うこともできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

A.4.1 ストレージシステムと SVP の IP アドレスを設定する

SVP から Maintenance Utility にアクセスし、ストレージシステムの IP アドレスを設定します。その後、SVP 上で、ストレージシステムに接続する SVP の LAN ポートの IP アドレスを設定します。

メモ

- ストレージシステムのネットワーク設定は、SVP とストレージシステムを管理 LAN に接続して行います。このため、SVP およびストレージシステムのネットワークセグメントが一致している必要があります。お客様のネットワーク環境にあわせてストレージシステムと SVP の IP アドレスを設定してください。
- SVP に 2 つ以上の LAN ポートがあり、1 つの LAN ポートを CTL1 の管理 LAN ポートに直接接続し、別の LAN ポートを CTL2 の管理 LAN ポートに直接接続する場合、SVP の LAN ポートをブリッジモードに設定してください。
- SVP に 2 つ以上の LAN ポートがある場合でも、1 つの LAN ポートをストレージシステムの操作に使用し、その他の LAN ポートをストレージシステムの操作以外の用途で使用する場合は、複数の LAN ポートを使用することができます。なお、ストレージシステムの操作に使用する LAN ポートは、ブリッジモードに設定した LAN ポートも含まれます。ストレージシステムの操作以外の用途で使用する LAN ポートは、管理クライアントを接続するための LAN ポートも含まれます。

ストレージシステムのデフォルト IP アドレスにあわせて、SVP の IP アドレスを仮設定します。

ストレージシステムのデフォルトの IP アドレスは次のとおりです。

- コントローラボード#1 側管理ポート：192.168.0.16
- コントローラボード#2 側管理ポート：192.168.0.17
- サブネットマスク：255.255.255.0

SVP の IP アドレスは、192.168.0.xxx（xxx：1～254 の範囲で 16、17 以外の数値）で仮設定する必要があります。

メモ

SVP とストレージシステムの間のネットワーク経路上には、プロキシなどの中継サーバを接続しないでください。

管理クライアントから SVP にリモートデスクトップ接続して、ネットワーク設定を行う場合、管理クライアントのネットワークセグメントも一致している必要があります。また管理クライアント、SVP、ストレージシステムの間のネットワーク経路上には、プロキシなどの中継サーバを接続しないでください。

⚠ 注意

管理 LAN にプロキシサーバを接続している場合には、「プロキシの設定」画面で除外設定を行ってください。

操作手順

1. SVP の電源を ON します。
2. SVP にログインします。
3. SVP の IP アドレスを仮設定します。

   設定方法は、使用している OS のマニュアルを参照してください。

   メモ

   管理クライアントから SVP にリモートデスクトップ接続して IP アドレスを変更すると、IP アドレスの変更と同時にリモートデスクトップ接続が切断されます。仮設定した IP アドレスを使用して、再度 SVP にリモートデスクトップ接続してください。

4. SVP にファイアウォールが設定されている場合は、下記のポートを SVP に登録してください。

   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	管理クライアント	80/TCP	SVP
HTTPS	any/TCP		443/TCP	
RMI	any/TCP		1099/TCP	
RMI（SSL）	any/TCP		5443/TCP	
RMI	any/TCP		51099/TCP	
RMI	any/TCP		51100-51355/TCP※	
SLP	any/TCP		427/TCP	

注※

記載の範囲からストレージシステム登録時に未使用のポート番号が自動的に割り振られ、ファイアウォールも設定されます。

割り振られたポート番号は、ストレージシステム起動時に使用されます。

5. ブラウザを起動します。
6. コントローラボード#1 の IP アドレス（192.168.0.16）を指定して Maintenance Utility に接続します。

   接続方法は、「1.5.5 各ツールのログイン方法（11 ページ）」を参照してください。

   Maintenance Utility のログイン画面が表示されます。
7. ［ログイン］画面にて、［ユーザ名］に maintenance、［パスワード］に raid-maintenance と入力して［ログイン］をクリックします。

   メモ

   raid-maintenance は、初期値のパスワードです。
8. Maintenance Utility に初めてログインする場合は、ユーザアカウントのパスワードを設定します。
   a. Maintenance Utility のメニューから［システム管理］-［パスワード変更］を選択します。
   b. パスワードを設定して［完了］をクリックします。

      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「3.2.8 ユーザアカウントポリシーの設定（41 ページ）」を参照してください。
9. ストレージシステムの管理ポート(CTL1 と CTL2)の IP アドレスを設定します。
   a. Maintenance Utility の［管理］から［ネットワーク設定］をクリックします。
   b. ［ネットワーク設定］画面の［ネットワーク設定］をクリックします。
   c. CTL1 と CTL2 の IP アドレスを設定して［適用］をクリックします。

   ⚠ 注意

   - 管理サーバ（SVP）からストレージシステムの CTL1 と CTL2 にホスト名を使って接続できます（「A.7 管理サーバ（SVP）にストレージシステムを登録する（199 ページ）」を参照）。

     ホスト名で接続する場合は、ここで設定した CTL1 と CTL2 の IP アドレスを DNS サーバに登録してください。DNS サーバ登録時の注意事項を示します。

     - CTL1 と CTL2 の IP アドレスに別々のホスト名を割り当ててください。同じホスト名に割り当てると、正常に通信できないおそれがあります。
     - 異なるストレージシステムの IP アドレスを同じホスト名に割り当てないでください。正常に通信できないおそれがあります。
     - 以下の規則に従ったホスト名を使用してください。
       * ホスト名の最大文字数は 255 文字です。

* 半角英文字と以下の記号を使用できます。なお、半角スペースは使用できません。

  ! $ % - . @ _ ` ~

SVP の Windows に対する設定も必要です。［コントロールパネル］から DNS サフィックスを追加する画面を表示して、CTL1、CTL2 に設定するホストのドメイン名を追加してください。(「G.2.21 DNS サフィックスの設定（393 ページ）」参照)。

10. ［ログアウト］をクリックして Maintenance Utility を終了します。
11. SVP の IP アドレスを設定します。

    設定方法は、使用している OS のマニュアルを参照してください。

    なお、管理クライアントから SVP にリモートデスクトップ接続して IP アドレスを変更すると、IP アドレスの変更と同時にリモートデスクトップ接続が切断されます。
12. 上記の操作により変更したネットワーク設定に合わせて管理クライアントの IP アドレスを設定し直します。なお、管理クライアントの IP アドレスは、SVP やストレージシステムの IP アドレスと同一セグメントである必要はありません。

    設定方法は、使用している OS のマニュアルを参照してください。

A.4.2 管理クライアントと SVP を接続するためのファイアウォールの設定

管理クライアントと SVP がファイアウォールを越えて通信するために、下記のポートを、管理クライアントと SVP の間に存在するネットワーク環境に登録してください。

なお、管理クライアントを使用せずに、SVP から直接管理 GUI を操作する場合、下表の RMI、SLP 以外のプロトコルのポートの登録は不要です。

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。

プロトコルの種類と、使用するポートは次の表のとおりです。

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	管理クライアント	80/TCP	SVP
HTTPS	any/TCP		443/TCP	
RMI	any/TCP		1099/TCP	
RMI（SSL）	any/TCP		5443/TCP	
RMI	any/TCP		51099/TCP	
RMI	any/TCP		51100-51355/TCP※	
SLP	any/TCP		427/TCP	

注※

記載の範囲からストレージシステム登録時に未使用のポート番号が自動的に割り振られ、ファイアウォールも設定されます。

割り振られたポート番号は、ストレージシステム起動時に使用されます。

ヒント

SVP で使用するポート番号は変更可能です。「付録 L. SVP で使用するポート番号の変更・初期化 (411 ページ)」を参照してください。

SVP で使用するポート番号を変更する際は、変更後のポート番号でファイアウォールが設定されます。

A.4.3 SVP とストレージシステムを接続するためのファイアウォールの設定

SVP とストレージシステムがファイアウォールを越えて通信するために、下記のポートを、SVP とストレージシステムの間に存在するネットワーク環境に登録してください。

プロトコルの種類と、使用するポートは次の表のとおりです。

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
TCP	any/TCP	SVP	10500/TCP	ストレージシステム
HTTP	any/TCP		80/TCP	
HTTPS	any/TCP		443/TCP	

ヒント

SVP で使用するポート番号は変更可能です。「付録 L. SVP で使用するポート番号の変更・初期化 (411 ページ)」を参照してください。

SVP で使用するポート番号を変更する際は、変更後のポート番号でファイアウォールが設定されます。

⚠ 注意

ICMP のファイアウォール設定はしないでください。誤ったアラートが通知される可能性があります。設定の解除方法は、ファイアウォールを管理している管理者に依頼してください。

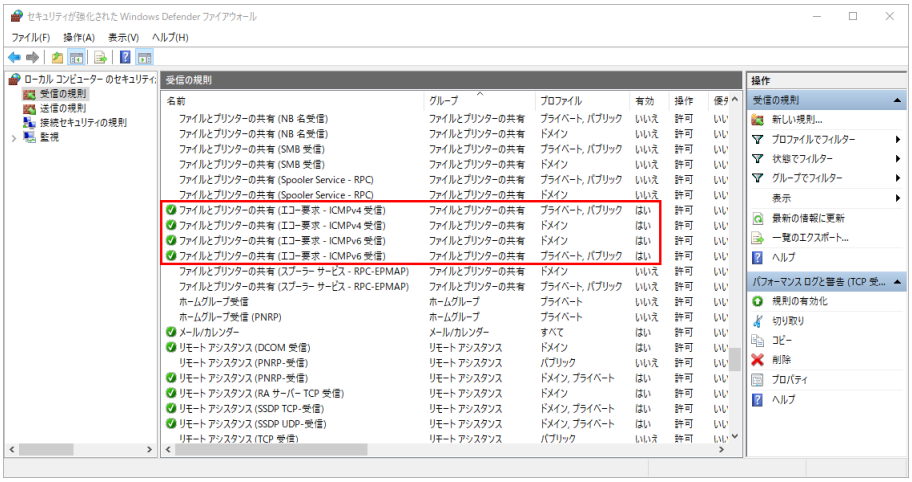
A.4.4 管理サーバ（SVP）のファイアウォールの設定

ストレージシステムとの通信のため、管理サーバ（SVP）に以下のファイアウォール設定を行ってください。

下記の操作手順は Windows 10 の例です。OS のバージョンにより画面表示が異なる場合があります。

操作手順

1. Windows の［スタート］メニューから、［コントロールパネル］－［管理ツール］－［セキュリティが強化された Windows Defender ファイアウォール］を選択します。
2. ［受信の規則］を選択します。
3. 受信の規則の以下の項目を右クリックし、［規則の有効化］を選択します。
   - 「ファイルとプリンターの共有 (エコー要求 - ICMPv4 受信)」（プロファイル："プライベート,パブリック"）
   - 「ファイルとプリンターの共有 (エコー要求 - ICMPv4 受信)」（プロファイル："ドメイン"）
   - 「ファイルとプリンターの共有 (エコー要求 - ICMPv6 受信)」（プロファイル："プライベート,パブリック"）
   - 「ファイルとプリンターの共有 (エコー要求 - ICMPv6 受信)」（プロファイル："ドメイン"）



A.5 管理サーバ（SVP）の初期設定を行う

システム運用に必要な SVP のシステム日時設定、およびロケール設定を行います。

Windows11 バージョン 24H2 以降で、次に示す SVP ソフトウェアバージョンの Storage Navigator を操作する場合、SVP に WMIC 機能を追加する必要があります。

- iStorage V100, V300 の場合：93-07-25-XX/XX 以前
- iStorage V10e の場合：88-08-17-XX/XX 以前

なお、1 台の SVP で複数のストレージシステムを管理する場合、ストレージシステムごとに Storage Navigator をインストールします。いずれかの Storage Navigator が、上記の SVP ソフトウェアバージョンに該当する場合は、WMIC 機能を追加してください。

A.5.1 SVP のシステム日時を設定する

SVP の日時と時刻とタイムゾーンを設定します。SVP に設定した日時と時刻とタイムゾーンは、SVP および障害監視プログラムで使用されます。

設定方法は、使用している OS のマニュアルを参照してください。

A.5.2 管理サーバ（SVP）にロケールを設定する

ストレージ管理ソフトウェア、および SVP ソフトウェアのサポート言語は英語と日本語です。既定のシステム UI 言語が、日本語、または英語の Windows のみ使用できます。なお、既定のシステム UI 言語が日本語の場合、ロケールを英語に変更できます。また、既定のシステム UI 言語が英語の場合、ロケールを日本語に変更できます。

（下記の操作手順は日本語版 Windows の例です。）

A.5.2.1 Windows 10 の場合

操作手順

1. ［スタート］を右クリックして［設定］を選択します。
2. ［時刻と言語］をクリックします。
3. ［関連設定］の［日付、時刻、地域の書式設定］をクリックします。
4. ［関連設定］の［日付、時刻、地域の追加設定］をクリックします。
5. ［地域］を選択します。
6. ［形式］タブを選択します。
7. ［形式］を［英語（米国）］または［日本語（日本）］に設定して［適用］をクリックします。
8. ［管理］タブを選択します。
9. ［設定のコピー］をクリックします。
10. ［ようこそ画面とシステムアカウント］にチェックを入れ［OK］をクリックします。

A.5.2.2 Windows Server 2016 の場合

操作手順

1. ［スタート］－［コントロールパネル］を選択します。
2. ［時計、言語、および地域］をクリックします。
3. ［地域］の下の［日付、時刻、または数値の形式の変更］をクリックします。

4. ［形式］を［英語（米国）］または［日本語（日本）］に設定して［適用］をクリックします。
5. ［管理］タブを選択します。
6. ［設定のコピー］をクリックします。
7. ［ようこそ画面とシステムアカウント］にチェックを入れ［OK］をクリックします。

A.5.2.3 Windows Server 2019 の場合

操作手順

1. ［スタート］－［コントロールパネル］を選択します。
2. ［時計と地域］をクリックします。
3. ［地域］の下の［日付、時刻、または数値の形式の変更］をクリックします。
4. ［形式］を［英語（米国）］または［日本語（日本）］に設定して［適用］をクリックします。
5. ［管理］タブを選択します。
6. ［設定のコピー］をクリックします。
7. ［ようこそ画面とシステムアカウント］にチェックを入れ［OK］をクリックします。

A.5.2.4 Windows 11 の場合

操作手順

1. ［スタート］を右クリックして［設定］を選択します。
2. ［時刻と言語］をクリックします。
3. ［言語と地域］をクリックします。
4. ［言語］の下の［Windows の表示言語］に、［英語（米国）］または［日本語（日本）］を設定します。
5. ［地域］の下の［国または地域］に、［米国］または［日本］を選択します。
6. ［関連設定］の［管理用の言語の設定］をクリックします。
7. ［管理］タブを選択します。
8. ［設定のコピー］をクリックします。
9. ［ようこそ画面とシステムアカウント］にチェックを入れ［OK］をクリックします。

A.5.2.5 Windows Server 2022 の場合

操作手順

1. ［スタート］－［コントロールパネル］を選択します。
2. ［時計と地域］をクリックします。
3. ［地域］の下の［日付、時刻、数値の形式の変更］をクリックします。
4. ［形式］を［英語（米国）］または［日本語（日本）］に設定して［適用］をクリックします。
5. ［管理］タブを選択します。
6. ［設定のコピー］をクリックします。
7. ［ようこそ画面とシステムアカウント］にチェックを入れ［OK］をクリックします。

A.5.3 管理サーバ（SVP）に WMIC 機能を追加する

ストレージ管理ソフトウェア、および SVP ソフトウェアでは WMIC 機能を使用します。

Windows11 バージョン 24H2 以降で、次に示す SVP ソフトウェアバージョンの Storage Navigator を操作する場合、SVP に WMIC 機能を追加する必要があります。

- iStorage V100, V300 の場合：93-07-25-XX/XX 以前
- iStorage V10e の場合：88-08-17-XX/XX 以前

なお、1 台の SVP で複数のストレージシステムを管理する場合、ストレージシステムごとに Storage Navigator をインストールします。いずれかの Storage Navigator が、上記の SVP ソフトウェアバージョンに該当する場合は、WMIC 機能を追加してください。

操作手順

1. Windows の［スタート］を右クリックして［設定］を選択します。［設定］画面が表示されます。
2. ［設定］画面の左メニューの［システム］をクリックします。
3. ［設定］画面の右メニューの［システム］－［オプション機能］をクリックします。［設定］画面の右メニューに［オプション機能］画面が表示されます。
4. ［オプション機能］画面の追加された機能一覧に「WMIC」が存在するか確認します。

   「WMIC」が存在する場合は、［設定］画面を閉じて、操作を終了します。

   「WMIC」が存在しない場合は、次の手順に進んでください。
5. ［オプション機能を追加する］－［機能を表示］をクリックします。［オプション機能を追加する］画面が表示されます。

6. ［オプション機能を追加する］画面で［WMIC］をチェックして［次へ］をクリックします。
7. 追加される内容に「WMIC」が表示されていることを確認し、［追加］をクリックします。

A.6 管理サーバ（SVP）に必要なソフトウェアをインストールする

メモ

Windows がインストールされているドライブとは別に、ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールするためのドライブが用意されている場合は、そのドライブにインストールしてください。

SVP にストレージ管理ソフトウェア、および SVP ソフトウェアをインストールします。本製品に同梱された SVP ファームウェアメディア（メディア名称「装置添付ソフトウェア 1／2」）を使用します。

前提条件

- SVP およびストレージシステムの IP アドレスが設定済、かつ接続されていること。
- ウィルス検出プログラムのサービスを停止していること。ウィルス検出プログラムが稼働している状態で実行すると、インストールのパフォーマンスが低下したり、正しく完了できない可能性があります。
- ストレージ管理ソフトウェア、および SVP ソフトウェア以外のアプリケーションがポート番号を使用していないこと。

  「L.9 ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照して確認してください。

  使用している場合は、ストレージ管理ソフトウェア、および SVP ソフトウェア以外のアプリケーションが使用するポート番号を変更するか、ストレージ管理ソフトウェア、および SVP ソフトウェア以外のアプリケーションを無効にしてポート番号が重複しないよう、「L.1 SVP で使用するポート番号を変更する（411 ページ）」を参照してポート番号を変更してください。

メモ

- ストレージ管理ソフトウェア、および SVP ソフトウェア以外のアプリケーションが使用するポート番号と重複した場合、ストレージ管理ソフトウェア、および SVP ソフトウェアは正しく動作しません。
- ストレージ管理ソフトウェア、および SVP ソフトウェアが使用するポート番号は変更することができます（「付録 L. SVP で使用するポート番号の変更・初期化（411 ページ）」参照）。

- RAID Manager をインストールしていない環境では、ストレージ管理ソフトウェアのインストール時に RAID Manager が自動でインストールされます。
- RAID Manager を既にインストールしている環境では、ストレージ管理ソフトウェアも同じドライブレターのドライブにインストールしてください。同じドライブレターのドライブにインストールできない場合は、既に RAID Manager をインストールしているドライブより後のドライブレターのドライブにインストールしてください。ストレージ管理ソフトウェアを RAID Manager がインストールされているドライブよりも前のドライブレターのドライブにインストールする場合は、RAID Manager のコマンドはフルパスで実行しないと、"raidmgr is not found."などのエラーになります。
- RAID Manager をインストールしている環境では、ストレージ管理ソフトウェアのインストール時に、ストレージ管理ソフトウェア同梱の RAID Manager で更新ができます。ただし、ストレージ管理ソフトウェアをインストールする前に、すべての RAID Manager インスタンスコンポーネントとサービスを停止してください。
- RAID Manager のバージョンを 01-68-03/00 以降に変更すると、変更後の RAID Manager のバージョンが Windows の［コントロールパネル］－［プログラムと機能］に反映されます。ただし、変更の処理（RAID Manager のインストール）のトラブルなどにより、実際にインストールされた RAID Manager のバージョンが、コントロールパネルに反映されないことがあります（反映されていなくても、RAID Manager は正常に動作します）。このため、Windows の［コントロールパネル］－［プログラムと機能］に表示されるバージョンを確認し、インストールしたバージョンと異なる場合は『RAID Manager インストール・設定ガイド』のトラブルシュートを参照して、バージョン情報を修正してください。これにより、Windows のコントロールパネルでも、RAID Manager のバージョンを確認できます。
- RAID Manager のバージョンを 01-68-03/00 以降から、01-68-03/00 未満に変更すると、Windows の［コントロールパネル］－［プログラムと機能］には変更する前の RAID Manager のバージョンが表示され、バージョン情報が削除されない場合があります（削除されていなくても、RAID Manager は正常に動作します）。RAID Manager のバージョン情報が削除されていない場合は、『RAID Manager インストール・設定ガイド』に示すトラブルシュートを参照して、コントロールパネルに表示されるバージョン情報を削除してください。
- RAID Manager のバージョンは RAID Manager の raidqry -h コマンドで確認できます。

A.6.1 インストール作業手順

次の手順に従ってストレージ管理ソフトウェア、および SVP ソフトウェアをインストールしてください。所要時間は 10 分程度です。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールをすることもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

また、SVP に DVD ドライブが搭載されていない場合は、リモートデスクトップ接続のオプションにより管理クライアントの DVD ドライブを使用してください。

⚠ 注意

- ネットワークドライブ配下のフォルダを、インストール先として指定しないでください。

  ネットワークドライブ配下のフォルダにインストールすると、サービスが正常に起動しません。
- インストール先のドライブの空き容量を、20GB 以上確保してください。

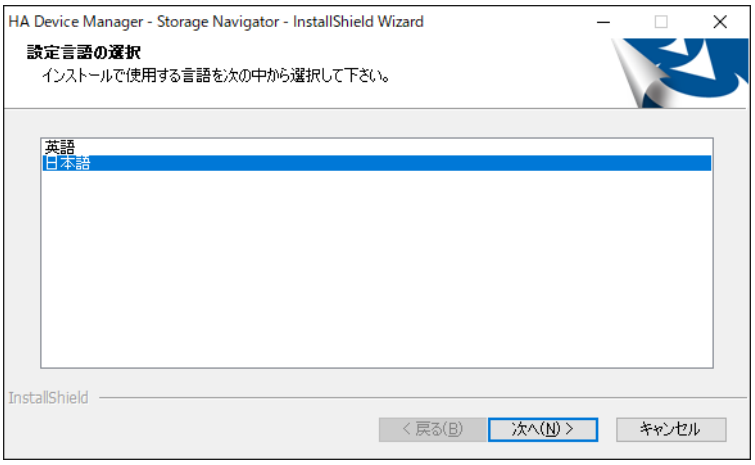
操作手順

1. 本製品に同梱された SVP ファームウェアメディアを、SVP の DVD ドライブに挿入します。

   メモ

   SVP ファームウェアメディアを使用後、DVD ドライブからメディアを取り出して保管してください。

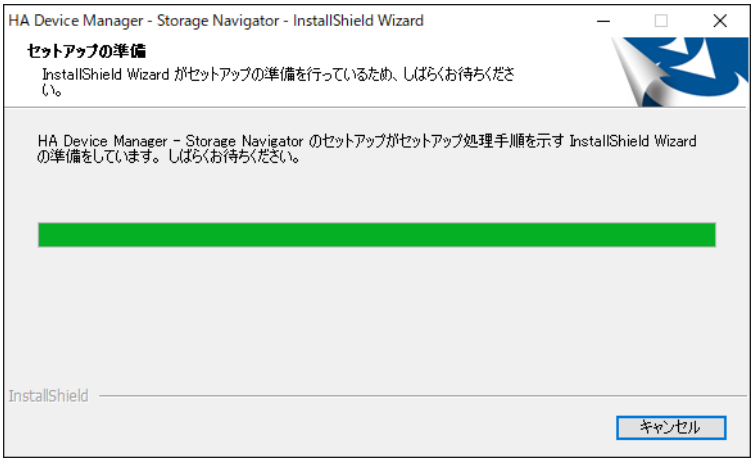
2. ドライブ直下の Setup.exe を右クリックし、[管理者として実行] をクリックします。
3. 使用する言語を選択し、[次へ] をクリックします。



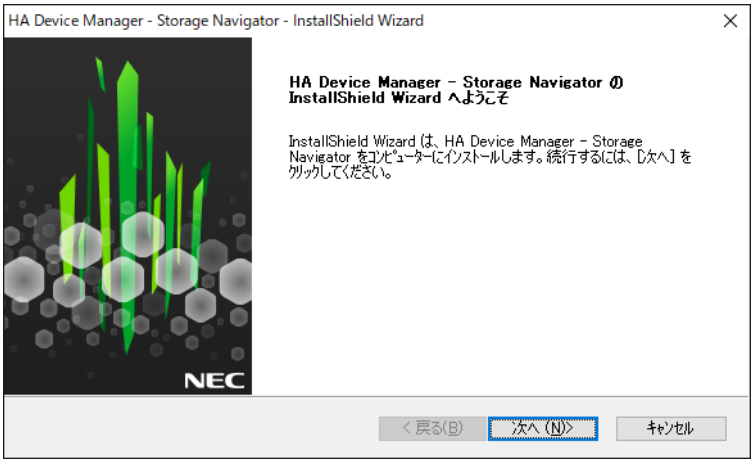
   ヒント

   2 回目以降、この画面は表示されません。

   インストール準備中画面が表示されます。準備が完了するまでお待ちください。



4. 準備が完了したら、Install Shield 画面が表示されます。［次へ］をクリックします。

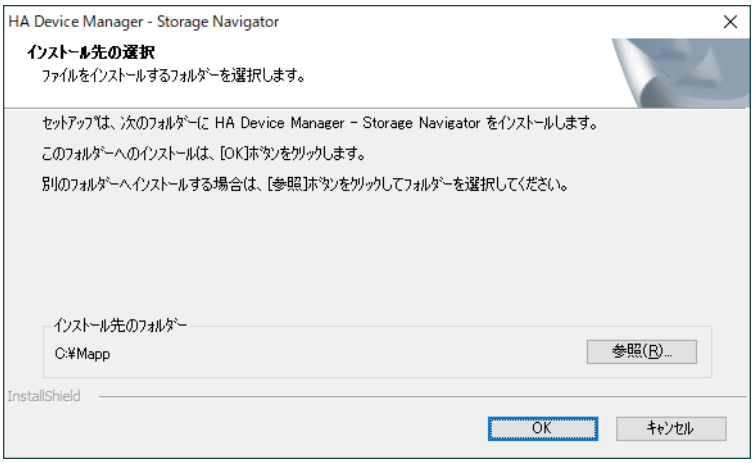


5. OSS（Open Source Software）の使用許諾の確認画面が表示されます。

［使用許諾契約の全条項に同意します］を選択し、［次へ］をクリックします。

6. ストレージ管理ソフトウェア、および SVP ソフトウェアをインストールするディレクトリを選択し、［OK］をクリックします。任意のディレクトリを指定してください。デフォルトは、「C:\Mapp」です。

ディレクトリをデフォルトから変更する場合、ドライブ直下（例：C:\）を指定しないでください。また、指定できるディレクトリの文字は、半角英数字、'-'（ハイフン）、'_'（アンダーバー）です。パスの文字数は 22 文字までです。



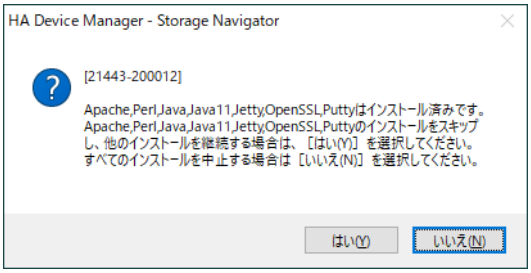
ヒント

同じ SVP ファームウェアメディアを使用してインストールしている場合、2 回目以降、この画面は表示されません。

メモ

- ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールドライブに関する確認メッセージが表示されます。内容を確認し、[OK]をクリックしてください。

- 以下の場合は、スキップの確認メッセージが表示されるので［はい］をクリックしてください。
  - SVP ファームウェアメディアからインストールする OSS のバージョンが、SVP にインストール済のバージョンと同じ場合



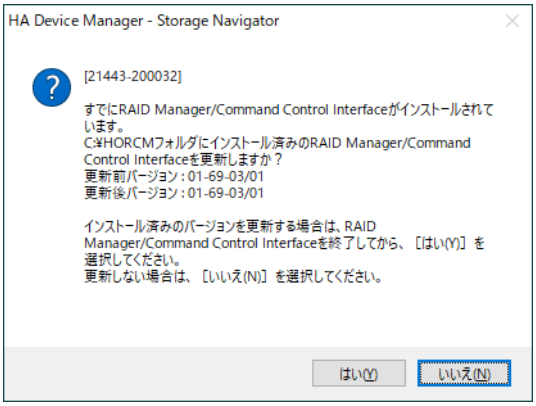
- SVP ファームウェアメディアがインストールする OSS の対象バージョンより古いバージョンがインストールされている場合は、アップデートの確認メッセージが表示されるので［はい］をクリックしてください。

- 別途 RAID Manager をインストールしている場合は、ストレージ管理ソフトウェア同梱の RAID Manager での更新メッセージ“21443-200032” が表示されます。

  RAID Manager をインストールしていない、またはインストールしたフォルダ(HORCM フォルダ)をリネームしている場合は表示されません。

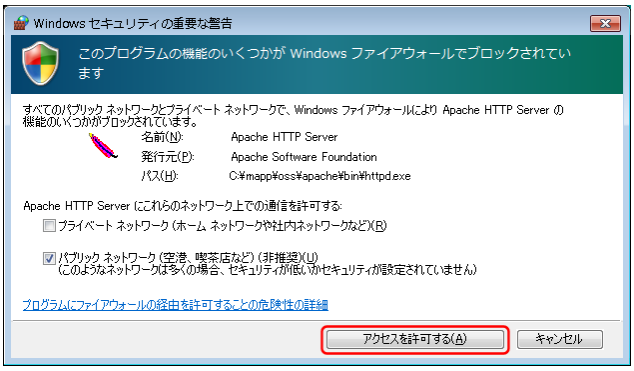
  更新する場合は、RAID Manager の使用を終了した後、［はい］ボタンをクリックしてください。［いいえ］ボタンをクリックすると RAID Manager のバージョンは維持されます。

  複数の RAID Manager をインストールしている場合は、もっとも順番が前のドライブレターのドライブにインストールしている RAID Manager が更新対象となります。



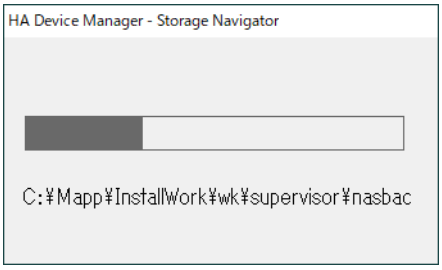
メッセージ画面に「注意」が表示されているときに［はい］ボタンをクリックすると、Windows の［コントロールパネル］－［プログラムと機能］には、すでにインストールされている RAID Manager のバージョンが表示され、変更後のバージョンは反映されません。このため、ストレージ管理ソフトウェアのインストールが完了したら『RAID Manager インストール・設定ガイド』に示す RAID Manager のバージョン削除方法を参照して、コントロールパネルに表示されるバージョン情報を削除してください。

- セキュリティ警告の画面が表示される場合は、［アクセスを許可する］をクリックしてください。

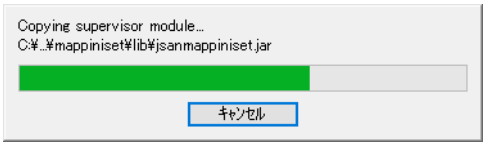


インストール中は、以下の画面が表示されます。

ファイル解凍中

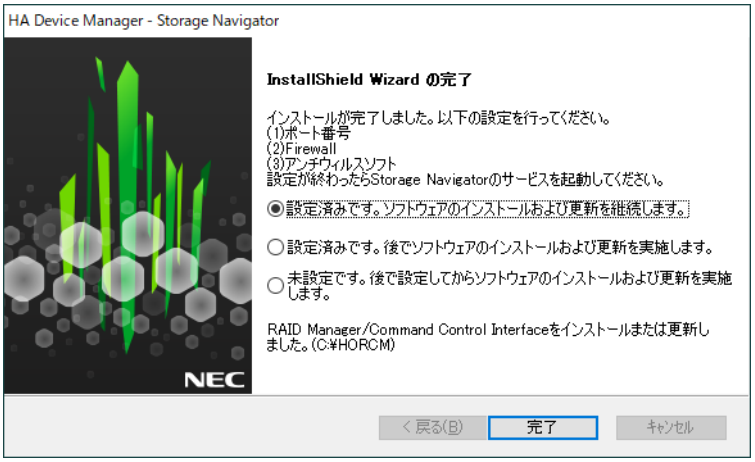


ファイルコピー中



7. 完了メッセージが表示されます。

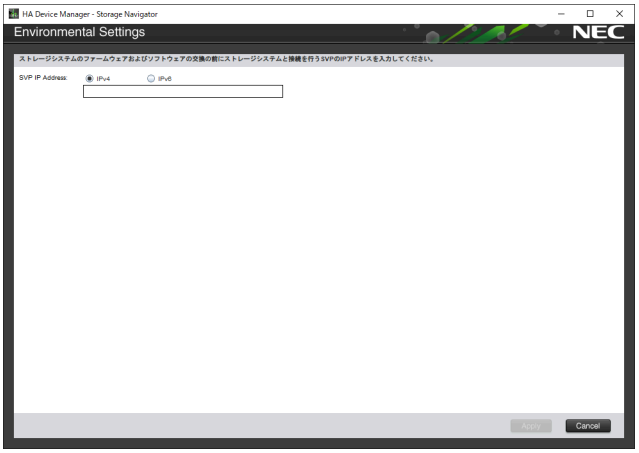
［設定済みです。ソフトウェアのインストールおよび更新を継続します。］を選択し、［完了］をクリックします。



メモ

- [設定済みです。後でソフトウェアのインストールおよび更新を実施します。] は、ここでは選択しないでください。手順 8 の Environmental Settings ツールが起動しません。
- ポート番号、Firewall、ウィルス検出プログラムの設定は、操作手順 8.の完了後に行ってください。

8. ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールが完了すると、Environmental Settings ツールが起動し、しばらくすると SVP の IP アドレス入力画面が表示されます。



- 管理対象のストレージシステムの電源が ON の場合、「A.7 管理サーバ（SVP）にストレージシステムを登録する（199 ページ）」へ進んでください。
- 管理対象のストレージシステムの電源が OFF の場合は、[Cancel] をクリックして一旦終了し、ストレージシステムの電源を ON したあと、再度手順 1 から実施してください。

A.7 管理サーバ（SVP）にストレージシステムを登録する

管理サーバ（SVP）にストレージシステムを登録すると、そのストレージシステム専用の SVP ソフトウェア（Storage Navigator）が割り当てられます。

A.7.1 管理サーバ（SVP）にストレージシステムを登録する

SVP の管理対象となるストレージシステムを、SVP に登録します。

所要時間は登録するストレージシステムあたり 10 分程度です。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、リモートでストレージシステムの登録を行うこともできます。ただし、リモートデスクトップセッションホストを使用した接続はできません。SVP に DVD ドライブが搭載されていない場合は、リモートデスクトップ接続して管理クライアントの DVD ドライブを使用します。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

⚠ 注意

- iStorage V10e の場合、1 台の SVP に最大 8 台のストレージシステムを登録できますが、同時に起動できるストレージシステムの台数は SVP のハードウェアに依存します。「1.6.2.1 SVP のハードウェア条件（19 ページ）」に示す SVP のハードウェア条件を参照して、同時に起動できるストレージシステムの台数を確認してください。
- ストレージシステムを起動すると、SVP 内で動作するプロセスに応じて、デスクトップヒープの消費量が増加します。「A.8 デスクトップヒープの指定値を変更する（206 ページ）」を参照してデスクトップヒープとして使用するメモリ領域を確保してください。

前提条件

- 登録するストレージシステムの電源が ON になっていること。
- SVP およびストレージシステムの IP アドレスが設定済、かつ接続されていること。
- SVP の条件を満たしていること。

  条件は、「1.6.2.1 SVP のハードウェア条件（19 ページ）」を参照してください。

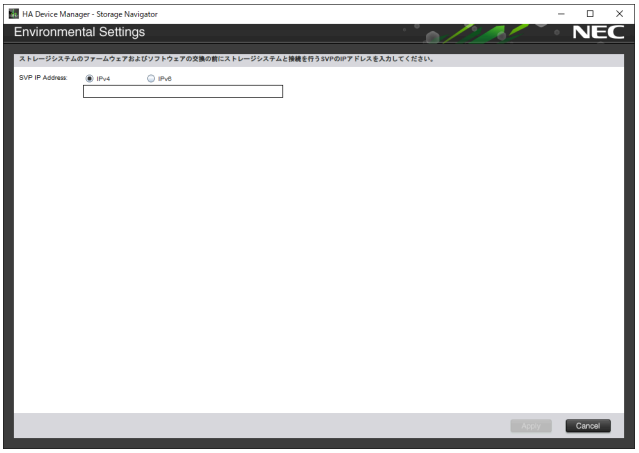
「A.6.1 インストール作業手順（192 ページ）」の手順 8 から継続して作業を実施します。

操作手順

1. SVP とストレージシステムの接続に使用するポートの IP アドレスを入力して、［Apply］をクリックします。

メモ

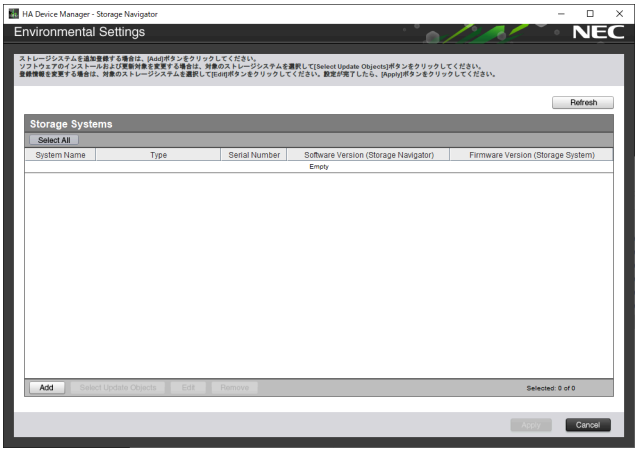
ストレージシステムの各 CTL や管理クライアントと SVP を直結している場合は、ブリッジ接続時に設定した IP アドレスを入力してください。



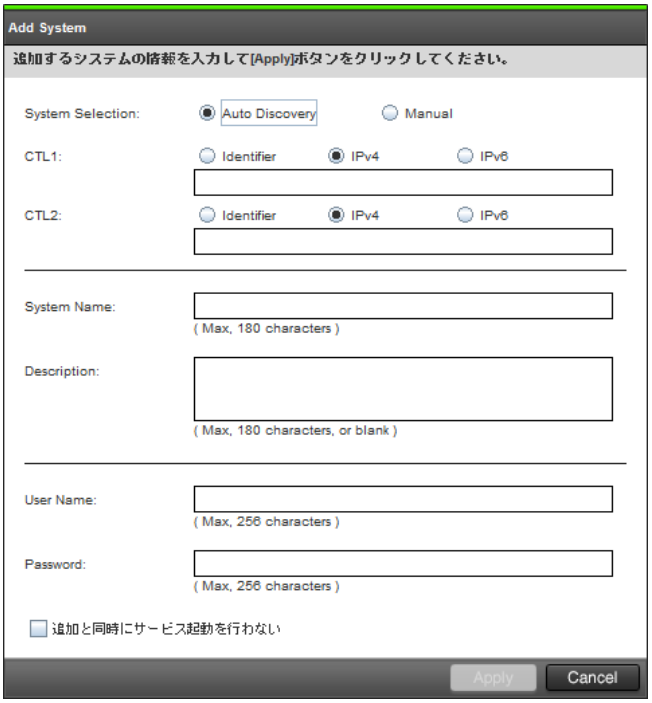
ヒント

IP アドレスの入力以降、この画面は表示されません。

2. 対象ストレージシステムの一覧画面が表示されます。［Add］をクリックします。



3. ［Add System］画面が表示されます。次に従い各設定項目を入力して、［Apply］をクリックします。



項目	内容
System Selection	ストレージシステム情報の入力方法を選択します。 • ［Auto Discovery］(デフォルト選択) : ストレージシステム情報を自動で取得します。 • ［Manual］※1 : ストレージシステム情報を手動で設定します。
CTL1,CTL2	Maintenance Utility のネットワーク画面の CTL1 と CTL2 の IP アドレスを指定します。IP アドレスの代わりに DNS サーバに登録したホスト名でも指定できます。 ホスト名で指定する場合は、[Identifier]を選択し、DNS サーバに登録したホスト名を入力してください。なお、CTL1 と CTL2 に同じホスト名を指定できません。 SVP の Windows に対する設定も必要です。［コントロールパネル］から DNS サフィックスを追加する画面を表示して、CTL1、CTL2 に設定するホストのドメイン名を追加してください (「G.2.21 DNS サフィックスの設定（393 ページ）」参照)。
System Name	ストレージシステムの表示名を設定します。 入力できる文字数は、半角文字で 180 文字までです。 使用可能文字：半角英数字と記号（# $ % & ' * + - . / = ? @ ^ _ ` { | } ~） 半角の空白は使用できません。
Description	ストレージシステムの説明を設定します。Description は、任意の項目です。 入力できる文字数は、半角文字で 180 文字までです。

項目	内容
User Name	ストレージシステムのユーザ名を入力します。 使用可能文字：半角英数字と記号（# $ % & ' * + - . / = ? @ ^ _ ` { | } ~）
Password	ストレージシステムのパスワードを入力します。
追加と同時にサービス起動を行わない※2※3	ストレージシステムを追加するのと同時にサービス起動するかを選択します。 （デフォルトはチェックなし）

注※1

保守員が手動で設定します。

ユーザは［Manual］を選択して設定しないでください。

注※2

複数台のストレージシステムを登録する場合は、このチェックボックスにチェックを入れて、追加と同時にサービスが開始されないように設定することを推奨します。

SVP の再起動時にストレージシステムのサービスを自動で開始させるための設定は、「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。

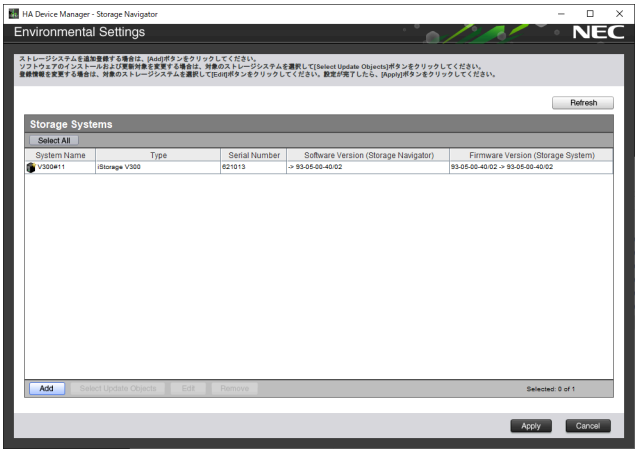
注※3

このチェックボックスをチェックすると、Storage Device List から起動される［Edit System］画面の［SVP 再起動時に自動でサービスを開始する］は、チェックが外れた状態で登録されます。

（デフォルトでは、チェックが入っています。詳細は、「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。）

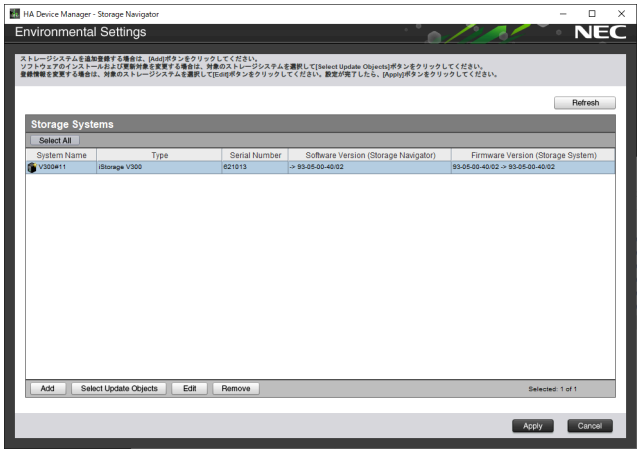
なお、ストレージシステムのサービスが起動されないと、エクスポートツール（ExportTool）は使用できません。

4. 対象ストレージシステムの一覧画面に入力したストレージシステムが追加されます。



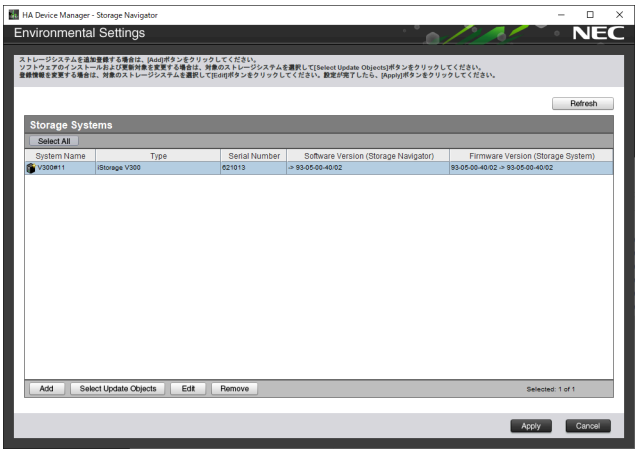
ヒント

間違ったストレージシステムを追加してしまった場合は、削除したいストレージシステムを選択して［Remove］をクリックしてください。



5. ストレージシステム追加と同時にファームウェアを更新するかどうかを選択します。

   更新をするかどうか変更したいストレージシステムを選択して、［Select Update Objects］をクリックします。



6. ［Select Update Objects］画面が表示されます。

［Firmware （Storage System)］※のチェックを外し、［Apply］をクリックします。

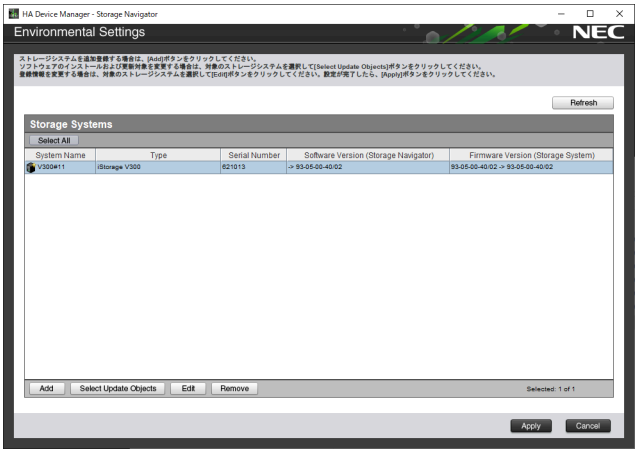
注※

［Firmware （Storage System)］のチェックが最初から外れている場合があります。その場合はそのまま、［Apply］をクリックします。

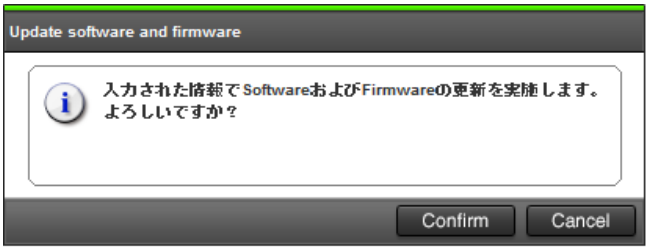
ヒント

登録するストレージシステムは自動的に［Software （Storage Navigator)］がチェックされ、変更できません。

7. 手順 2 以降を繰り返して、使用するすべてのストレージシステムを登録し終わったら、対象ストレージシステムの一覧画面で［Apply］をクリックします。

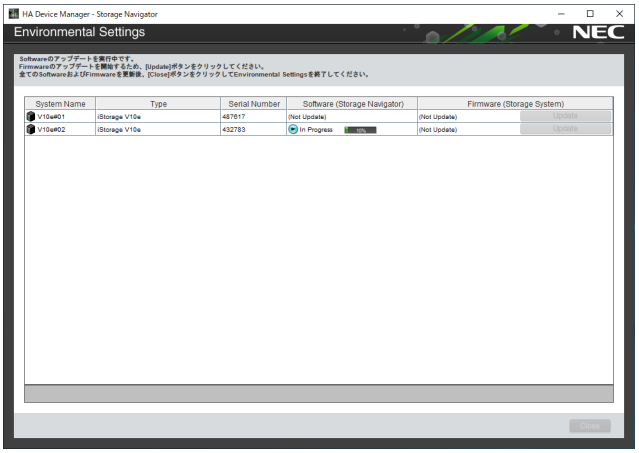


8. ［Update software and firmware］画面が表示されるので、［Confirm］をクリックします。



更新実行画面が表示され、ソフトウェアの更新が自動で開始されます。

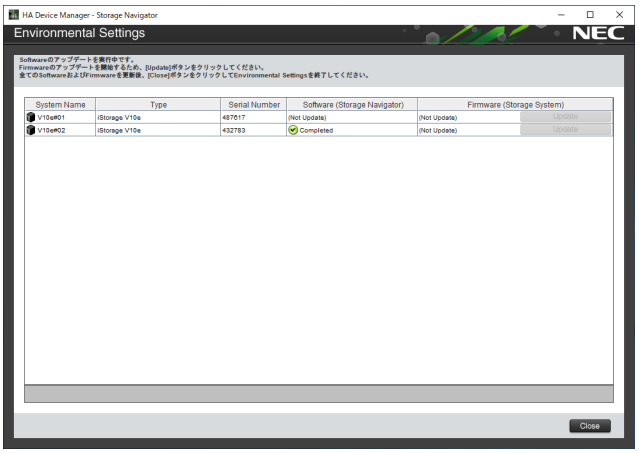
［Software （Storage Navigator)］列で、ソフトウェアの更新の状態が確認できます。



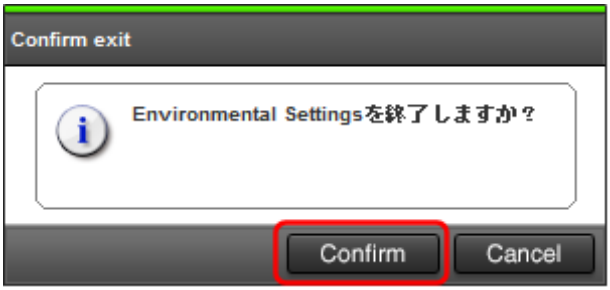
ソフトウェアの更新の状態は、以下の状態があります。

状態	内容
Waiting	ソフトウェアの更新を実施していません。 ソフトウェアの更新は 1 台ずつ実行されます。すでに別のストレージシステムのソフトウェアの更新が実行されている場合は、他のストレージシステムはこの状態になります。
In Progress	ソフトウェアの更新を実行中です。
Completed	ソフトウェアの更新が完了しています。
Failed	ソフトウェアの更新に失敗しました。 ストレージシステムを追加した場合は、追加が完了していない場合があります。クリックしてメッセージに従ってください。
(Not Update)	ソフトウェアの更新対象に選択されていません。 ストレージシステムを追加した場合は、この状態になることはありません。

9. ソフトウェアの更新状態が［Completed］であることを確認し、［Close］をクリックします。



10. ［Confirm］をクリックして、ツールを終了します。



11. お客様の必要に応じてウィルス検出プログラムをインストールしてください（「4.3 ウィルス検出プログラムの使用に関する注意事項（97 ページ）」を参照）。
12. 複数台のストレージシステムのサービスを同時に開始する場合は、「A.8 デスクトップヒープの指定値を変更する（206 ページ） 」を参照して指定値を変更します。

A.8 デスクトップヒープの指定値を変更する

ストレージシステムを起動すると、SVP 内で動作するプロセスに応じて、デスクトップヒープの消費量が増加します。デスクトップヒープが不足すると、ストレージシステムのサービスが正常に開始しない、あるいは GUI の操作が失敗するなどの不具合の原因になります。このためデスクトップヒープを、同時に起動するストレージシステムの台数に対応する指定値に変更してください。

「A.8.1 デスクトップヒープの指定値をバッチファイルで変更する（206 ページ）」を参照して、指定値を変更してください。

デスクトップヒープの指定値を Windows のデフォルト値に戻す場合は、「A.8.2 デスクトップヒープの指定値を Windows のデフォルト値に戻す（207 ページ）」を実施してください。

A.8.1 デスクトップヒープの指定値をバッチファイルで変更する

バッチファイルを実行してデスクトップヒープの指定値を変更します。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
```

```
MappsetHeapMemoryExpand.bat
```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。

   SVP を再起動するメッセージが表示された場合は、SVP を再起動します（「G.1.3 SVP を再起動する（315 ページ）」参照）。

   再起動のメッセージが表示されない場合は手順 4 以降を実行してください。

4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。

5. コマンドプロンプトを閉じます。

A.8.2 デスクトップヒープの指定値を Windows のデフォルト値に戻す

デスクトップヒープの指定値を Windows のデフォルト値に戻します。

メモ

- この手順を実行するとデスクトップヒープの指定値が Windows のデフォルト値に戻ります。他のアプリケーションの動作に影響がある場合があるので、注意して実行してください。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappsetHeapMemoryInit.bat
   ```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. SVP を再起動するメッセージが表示されるので、SVP を再起動します（「G.1.3 SVP を再起動する（315 ページ）」参照）。

   管理クライアントから SVP にリモートデスクトップ接続して SVP を再起動すると、リモートデスクトップ接続が切断します。

A.9 ストレージシステムの初期設定を行う

Storage Navigator から、ストレージシステムのシステム日時の設定と、管理対象のストレージシステム情報の編集をします。Storage Navigator にログインしてから設定および編集をしてください。

A.9.1 Storage Navigator にログインする

ストレージシステムを操作するために、Storage Navigator にログインします。Storage Navigator は、目的のストレージシステムごとにログインする必要があります。

メモ

使用上の注意は、「4.1 Storage Navigator 使用時の注意（96 ページ）」を参照してください。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、リモートでストレージシステムの初期設定を行うこともできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

SVP から直接ログインする場合は「A.9.2 SVP から直接ログインする（208 ページ）」を参照してください。

管理クライアントから Storage Navigaotor にログインする場合は「A.9.3 管理クライアントから Storage Navigator にログインする（211 ページ）」を参照してください。

A.9.2 SVP から直接ログインする

SVP から直接 Storage Navigator にログインすると、Adobe AIR 環境で動作する Storage Navigator が起動します。ただし、SVP の OS が Windows Server の場合、Adobe AIR 環境を使用できません。SVP から直接ログインせずに、管理クライアントからログインしてください。

SVP ソフトウェアバージョンが以下の場合、デフォルトの Web ブラウザとして Microsoft Edge、または Google Chrome を設定してください。それ以外のバージョンでは、Google Chrome を設定してください。

- iStorage V100, V300 の場合：93-05-21-XX/XX 以降
- iStorage V10e の場合：全バージョン

前提条件

- SVP とストレージシステムの電源が ON になっていること。
- SVP およびストレージシステムの IP アドレスが設定済、かつ接続されていること。
- ログインする目的のストレージシステムがサービスを開始していること。

  ストレージシステムのサービスが開始していない場合は、「G.2.7 ストレージシステム単位のサービスの開始（354 ページ）」を参照してください。

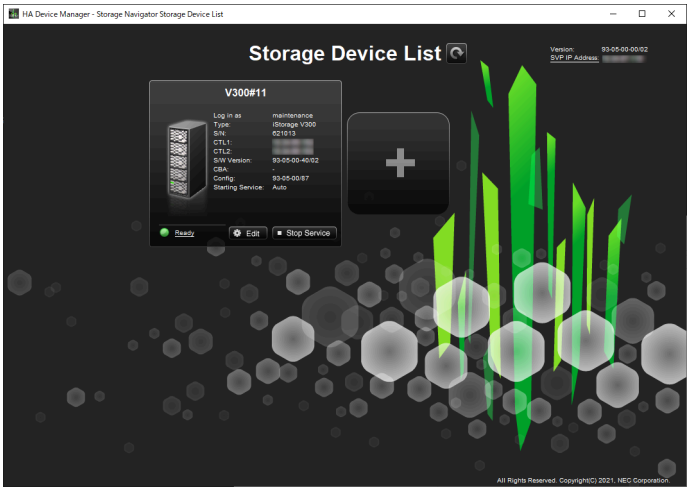
操作手順

1. SVP にログインします。
2. Windows の［スタート］メニューから、［HA Device Manager - Storage Navigator］－［Storage Device List］を右クリックし、［管理者として実行］をクリックします。［管理者として実行］が表示されない場合は、［詳細］または［その他］－［ファイルの場所を開く］をクリックします。開かれたエクスプローラーにあるファイルを右クリックし、［管理者として実行］をクリックします。

   ［Storage Device List］画面が表示されます。

   ヒント

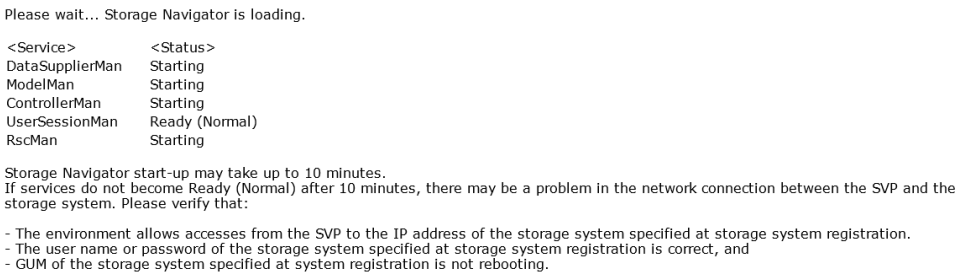
   SVP デスクトップ上の［Open StorageDeviceList］アイコンを右クリックして、［管理者として実行］を選択することでも Storage Device List を起動できます。
3. ［Storage Device List］画面で、サービスを開始しているストレージシステムをクリックします。



ストレージシステムをクリックすると、以下の画面が表示されます。

処理が進むと、<Service>の<Status>が［Starting］から［Ready （Normal)］に変わります。

初回ログイン時は、ログイン画面が表示されるまでに約 10 分から 20 分かかります。

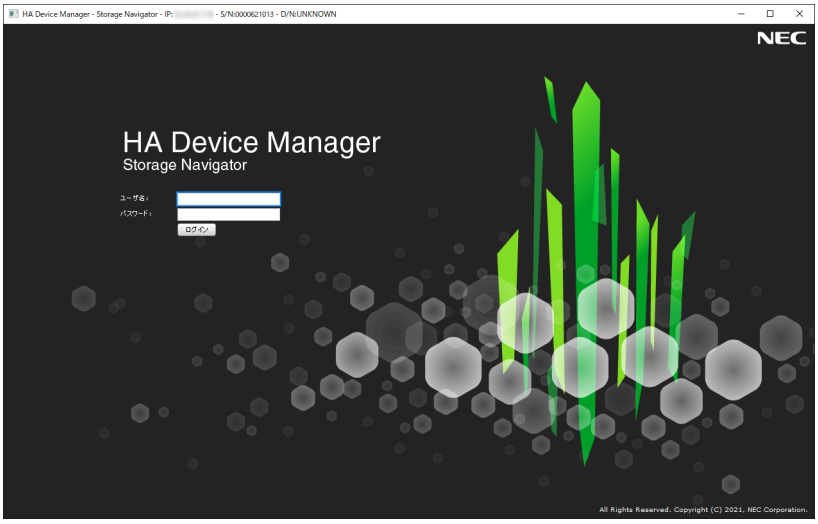


メモ

上記画面が表示されたままで、ログインができない場合は、「5.4.2 Storage Device List 操作時のトラブルシューティング（111 ページ)」を参照して対処してください。

HA Device Manager - Storage Navigator のログイン画面が表示されます。

4. ログイン画面にて、［ユーザ名］に maintenance、［パスワード］に「A.4.1 ストレージシステムと SVP の IP アドレスを設定する（182 ページ)」で設定したパスワードを入力して［ログイン］をクリックします。

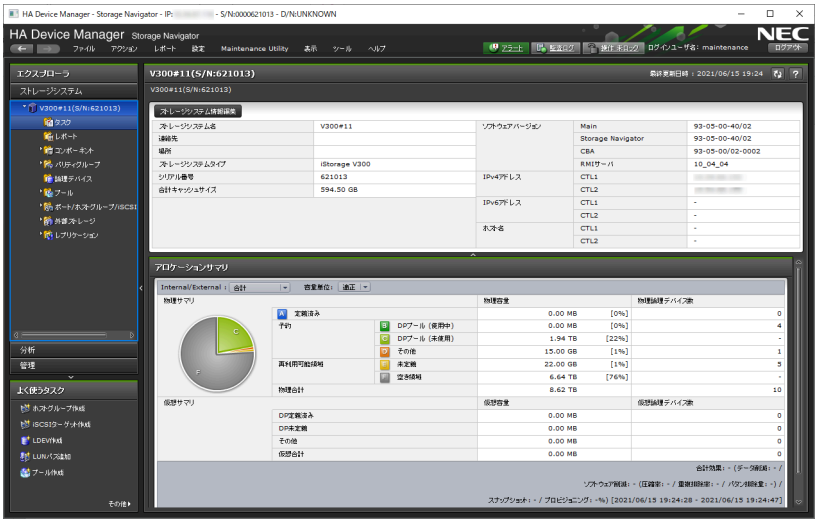


メモ

パスワードの初期値は、raid-maintenance です。

Storage Navigator メイン画面が表示されます。

複数の Storage Navigator にログインしている場合は、メイン画面に表示される装置製番で、目的のストレージシステムであることを確認してください。



A.9.3 管理クライアントから Storage Navigator にログインする

メモ

管理クライアントで、Storage Navigator を使用する場合は、事前に Storage Device Launcher のインストールが必要です。インストール方法は、『Storage Navigator ユーザガイド』を参照してください。

Storage Navigator に、初めてログインしたとき、および、SVP 上の CBA※がアップデートされた後に初めてログインしたときは、CBA が管理クライアントにダウンロードされます。

ダウンロードされるファイルの容量は約 30MB です。ダウンロード後に、ログイン画面が起動するため、起動には約 10 秒かかります。

注※

Captive Bundle Application。Adobe AIR 環境で動作する Storage Navigator アプリケーションです。1 台の管理クライアントで複数のストレージシステムを操作する場合は、ストレージシステムごとに CBA がダウンロードされます。

A.9.3.1 Storage Device Launcher をインストールしたユーザでログインする手順（ユーザに管理者権限がある場合）

管理者権限を持つユーザで管理クライアントにログインしている場合、次の手順に従って、Storage Navigator にログインしてください。

前提条件

- Storage Device Launcher をインストールしてあること。
- SVP とストレージシステムの電源が ON になっていること。
- SVP およびストレージシステムの IP アドレスが設定済、かつ接続されていること。
- ログインする目的のストレージシステムがサービスを開始していること。

  ストレージシステムのサービスが開始していない場合は、「G.2.7 ストレージシステム単位のサービスの開始（354 ページ）」を参照してください。

操作手順

1. Storage Navigator のログイン画面を起動します。

   Storage Device Launcher からログイン画面を起動する場合：

   a. 管理クライアントのデスクトップまたはスタートメニューの［Open StorageDeviceLauncher］を右クリックし、［管理者として実行］をクリックします。［管理者として実行］が表示されない場合は、［詳細］または［その他］ー［ファイルの場所を開く］をクリックします。開かれたエクスプローラーにあるファイルを右クリックし、［管理者として実行］をクリックします。

      ［Storage Device Launcher］画面が表示されます。

      メモ

      - セキュリティ警告や実行をブロックする画面が表示された場合は、そのまま実行しないでください。

        『HA Device Manager - Storage Navigator ユーザーガイド』の「Storage Device Launcher 使用上の注意」を参照して、Storage Device Launcher 実行のバッチファイルのプロパティを変更してから、再操作してください。

- 下記のバージョンの SVP ソフトウェアを使用して、そのバージョンより前のバージョンの SVP ソフトウェアで取得した Storage Device Launcher を更新した場合、次の内容を確認してください。

  更新後、初めて Storage Navigator のログイン画面を起動した時間に、<*Storage Device Launcher のインストールディレクトリ*>\WCLauncher\log の LauncherBatch.log に［Error］の文字列が出力されていないことを確認してください。出力されていた場合は、管理クライアントを再起動して、Storage Navigator のログイン画面を起動してください。

  - iStorage V100, V300 の場合：93-06-81-XX/XX 以降
  - iStorage V10e の場合：全バージョン

  なお、Storage Navigator のログイン画面を起動した時間とは、管理クライアントでの時間です。

b. SVP の IP アドレスまたはホスト名を入力します。

c. HTTPS のポート番号（デフォルトは”443”）を指定します。

d. ［Connect］をクリックします。

Web ブラウザからログイン画面を起動する場合：

a. 管理クライアントの Web ブラウザを管理者権限で起動します。

b. 次の URL を入力します。

```
sdlauncher://SVP の IP アドレスまたはホスト名/
```

HTTPS のポート番号（デフォルトは”443”）を変更している場合は、変更後のポート番号を指定してください。

```
sdlauncher:// SVP の IP アドレスまたはホスト名:[HTTPS ポート番号]/
```

2. ［Storage Device List］画面が表示されます。この画面で目的のストレージシステムを選択します。

メモ

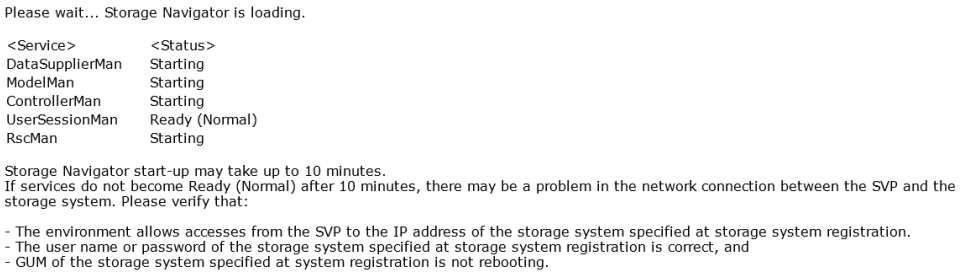
次の状態の場合は、［Storage Device List］は表示されません。手順 3 に進んでください。

- SVP に 1 台のみストレージシステムを登録していて、そのストレージシステムのサービスが Ready の場合
- SVP に複数台のストレージシステムを登録しているが、サービスが Ready のストレージシステムが 1 台の場合

ストレージシステムをクリックすると、以下の画面が表示されます。

処理が進むと、<Service>の<Status>が［Starting］から［Ready （Normal)］に変わります。

初回ログイン時は、ログイン画面が表示されるまでに約 10 分から 20 分かかります。

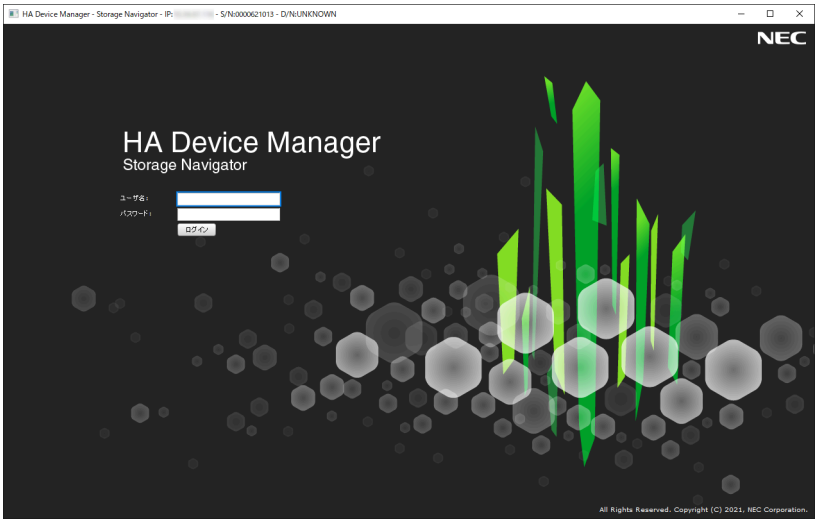


メモ

上記画面が表示されたままで、ログインができない場合は、「5.4.2 Storage Device List 操作時のトラブルシューティング（111 ページ）」を参照して対処してください。

HA Device Manager - Storage Navigator のログイン画面が表示されます。

3. ログイン画面にて、［ユーザ名］に maintenance、［パスワード］に「A.4.1 ストレージシステムと SVP の IP アドレスを設定する（182 ページ）」で設定したパスワードを入力して［ログイン］をクリックします。

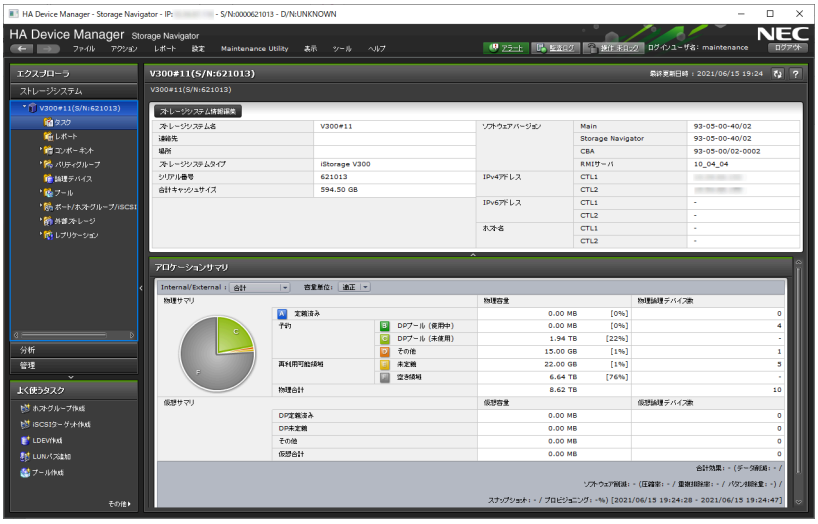


メモ

パスワードの初期値は、raid-maintenance です。

Storage Navigator メイン画面が表示されます。

複数の Storage Navigator にログインしている場合は、メイン画面に表示される装置製番で、目的のストレージシステムであることを確認してください。



A.9.3.2 Storage Device Launcher をインストールしたユーザでログインする手順（ユーザに管理者権限がない場合）

管理者権限を持たないユーザで管理クライアントにログインしている場合、次の手順に従って、Storage Navigator にログインしてください。

前提条件

- 管理クライアントと SVP の SSL 通信で TLS1.2 を有効にしていること。（Adobe AIR は TLS1.3 をサポートしていません。）
- 『HA Device Manager - Storage Navigator ユーザガイド』の「実行するユーザに管理者権限がない場合の起動準備」を実施していること。

操作手順

1. Storage Device Launcher からログイン画面を起動します。
   a. デスクトップの `SDLauncher.bat` のショートカットを実行します。

メモ

- セキュリティ警告や実行をブロックする画面が表示された場合は、そのまま実行しないでください。

  『HA Device Manager - Storage Navigator ユーザガイド』の「Storage Device Launcher 使用上の注意」を参照して、Storage Device Launcher 実行のバッチファイルのプロパティを変更してから、再操作してください。
- 下記のバージョンの SVP ソフトウェアを使用して、そのバージョンより前のバージョンの SVP ソフトウェアで取得した Storage Device Launcher を更新した場合、次の内容を確認してください。

  更新後、初めて Storage Navigator のログイン画面を起動した時間に、<*Storage Device Launcher のインストールディレクトリ*>\WCLauncher\log の LauncherBatch.log に［Error］の文字列が出力されていないことを確認してくださ

い。出力されていた場合は、管理クライアントを再起動して、Storage Navigator のログイン画面を起動してください。

- iStorage V100, V300 の場合：93-06-81-XX/XX 以降
- iStorage V10e の場合：全バージョン

なお、Storage Navigator のログイン画面を起動した時間とは、管理クライアントでの時間です。

b. SVP の IP アドレスまたはホスト名を入力します。

c. HTTPS のポート番号”443”を指定します。

d. ［Connect］をクリックします。

e. セキュリティに関する警告メッセージが表示されたときは、証明書の内容が正しいことを確認して、画面の操作に従ってください。

2. ［Storage Device List］画面が表示されます。この画面で目的のストレージシステムを選択します。

メモ

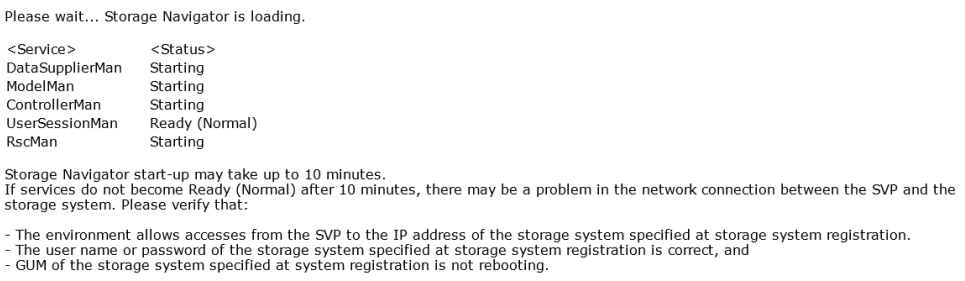
次の状態の場合は、［Storage Device List］は表示されません。手順 3 に進んでください。

- SVP に 1 台のみストレージシステムを登録していて、そのストレージシステムのサービスが Ready の場合
- SVP に複数台のストレージシステムを登録しているが、サービスが Ready のストレージシステムが 1 台の場合

ストレージシステムをクリックすると、以下の画面が表示されます。

処理が進むと、<Service>の<Status>が［Starting］から［Ready （Normal)］に変わります。

初回ログイン時は、ログイン画面が表示されるまでに約 10 分から 20 分かかります。



メモ

上記画面が表示されたままで、ログインができない場合は、「5.4.2 Storage Device List 操作時のトラブルシューティング（111 ページ)」を参照して対処してください。

HA Device Manager - Storage Navigator のログイン画面が表示されます。

3. ユーザ名とパスワードを入力します。
4. ［ログイン］をクリックします。
5. ［セキュリティ情報］画面が表示された場合は、［はい］をクリックします。

   ログインに成功すると、Storage Navigator メイン画面が表示されます。

A.9.3.3 Storage Device Launcher をインストールしていないユーザの場合

『HA Device Manager - Storage Navigator ユーザガイド』の「Storage Device Launcher をインストールする」が行われた管理クライアントに Storage Device Launcher をインストールしていないユーザがログインする場合、次の手順に従って、Storage Navigator にログインしてください。

前提条件

- 管理クライアントと SVP の SSL 通信で TLS1.2 を有効にしていること（Adobe AIR は TLS1.3 をサポートしていません）
- 別のユーザが、Storage Device Launcher をインストールした管理クライアントであること

操作手順

1. 『HA Device Manager - Storage Navigator ユーザガイド』の「Storage Device Launcher をインストールする」で展開されたセットアップファイルの WCLauncher\SDLauncher\SDLauncher.bat を右クリックし、［ショートカットの作成］をクリックします。
2. 作成されたショートカットをデスクトップに移動します。
3. 「A.9.3.2 Storage Device Launcher をインストールしたユーザでログインする手順(ユーザに管理者権限がない場合)（215 ページ)」の操作手順に従い、ログインしてください。

A.9.4 管理クライアントに Web Console Launcher を設定する

管理クライアントから Storage Navigator を操作する場合、事前に管理クライアントに Web Console Launcher を設定します（設定方法は、『HA Device Manager - Storage Navigator ユーザガイド』の「Web Console Launcher を使用して Storage Navigator サブ画面を使用できるようにする」を参照)。

A.9.5 SVP の Web Console Launcher を設定する

ストレージ管理ソフトウェアのインストール時に SVP に Web Console Launcher が設定され、SVP で Storage Navigator サブ画面を使用できるようになります。

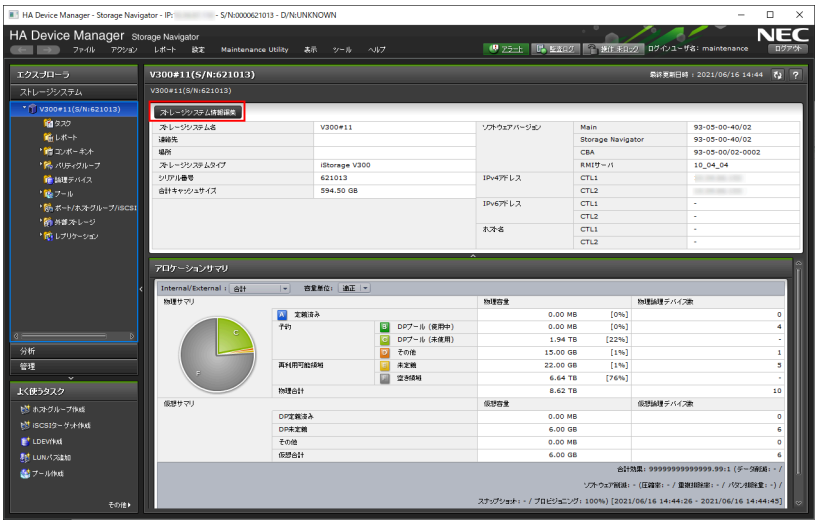
A.9.6 ストレージシステム情報を編集する

ストレージシステム情報（ストレージシステム名／連絡先／設置場所）を登録します。これらの情報は SNMP の障害通知機能を使用するために必要です。ストレージシステム情報は Storage Navigator から編集します。

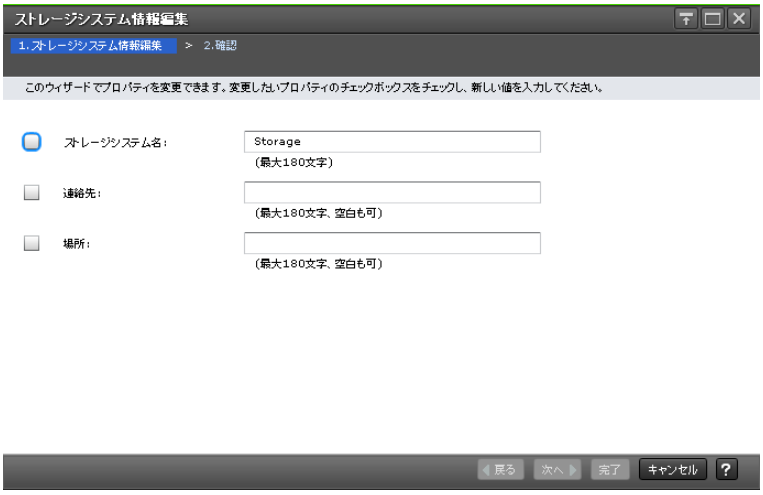
A.9.6.1 Storage Navigator からストレージシステム情報を編集する

操作手順

1. Storage Navigator メイン画面の［ストレージシステム情報編集］をクリックします。



2. ストレージシステム名、連絡先、場所を設定します。



項目	内容
ストレージシステム名	ストレージシステム名を設定します。 一部の記号（\ , / ; : * ? " < > | & % ^）を除く最大 180 文字の半角英数字を入力できます。先頭または末尾に空白を入力しないでください。 本項目を変更すると、Maintenance Utility の［ストレージシステム］画面および［アラート通知］画面の［SNMP］タブのストレージシステム名も変更されます。
連絡先	管理者名や連絡先を設定します。 一部の記号（\ , / ; : * ? " < > | & % ^）を除く最大 180 文字の半角英数字を入力できます。先頭または末尾に空白を入力しないでください。 本項目を変更すると、Maintenance Utility の［ストレージシステム］画面および［アラート通知］画面の［SNMP］タブの連絡先も変更されます。
場所	ストレージシステムの設置場所を設定します。 一部の記号（\ , / ; : * ? " < > | & % ^）を除く最大 180 文字の半角英数字を入力できます。先頭または末尾に空白を入力しないでください。 本項目を変更すると、Maintenance Utility の［ストレージシステム］画面および［アラート通知］画面の［SNMP］タブの場所も変更されます。

3. 設定内容を確認し［完了］をクリックします。
4. 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。

A.10 初期設定作業を確認する

ストレージシステムの初期設定が終了したあと、正常に作業が完了していることを確認します。

ストレージシステムの初期設定作業が正しく完了すると、Storage Navigator、Maintenance Utility がストレージシステムを認識し、システム情報が画面に表示されます。

Storage Navigator のインストールに失敗したり、Storage Navigator、Maintenance Utility からストレージシステムが認識できなかったりする場合は、初期設定作業が正常に完了していません。「第 5 章 トラブルシュート（101 ページ）」へ進み、不具合を解消してください。

また、通信のセキュリティを高めるため、SSL 通信の設定を実施することを推奨します。初期設定作業として「付録 C. SSL 通信の設定（245 ページ）」を実施してください。

SSL 通信の設定後に、初期構築作業を行います。「付録 B. 初期構築作業（221 ページ）」へ進んでください。

付録 B.　初期構築作業

ストレージシステムを動作させるためには、外部サーバとのデータリンクを確立するとともに、ホストサーバで動作する OS に、ストレージシステムのリソースを適切に割り当てるなどの初期構築が必要です。作業には管理 GUI を使用します。

B.1　初期構築作業の概要

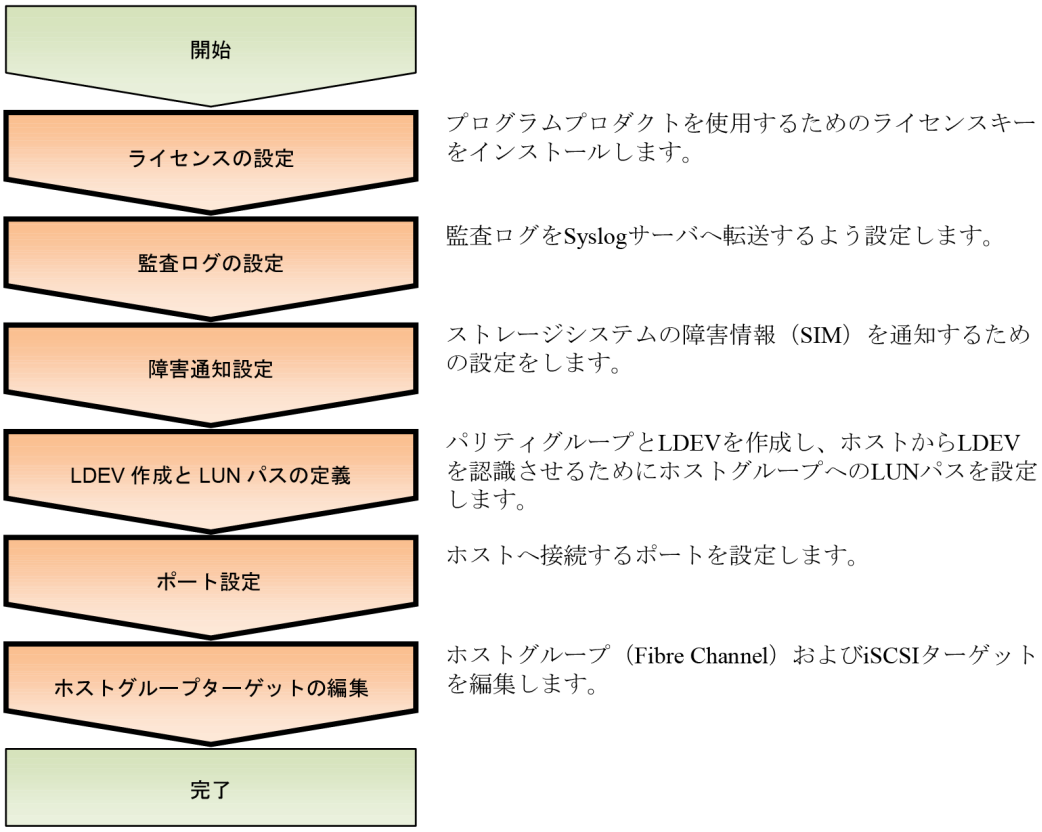
ストレージシステムの初期構築作業を行う前に、作業の目的と流れを理解します。

B.1.1　初期構築作業の目的

ストレージシステムの運用を開始できるようにすることが目的です。管理 GUI からストレージシステムにパリティグループと LDEV（ボリューム）を作成し、ホストサーバにその LDEV を割り当てるために LUN パスを定義します。また、運用時に必要なライセンスや監査ログ、障害通知の設定も行います。

B.1.2　初期構築作業の流れ

初期構築作業は、次の流れに従って作業を行います。



B.1.3 初期構築作業を実施するための前提条件

ストレージシステムの初期構築作業を行う前に、次の条件を満たしていることを確認してください。

- ストレージシステムの初期設定作業が完了していること
- ストレージシステムおよび、ホストサーバ、管理サーバの電源が ON になっていること
- ストレージシステムおよび、ホストサーバ、管理サーバがネットワークに接続されていること
- SVP および管理クライアントが要件を満たしていること
- 管理クライアントから SVP および管理 GUI にアクセスできること
- ストレージシステムに障害が発生していないこと
- ストレージシステムに接続するサーバに障害が発生していないこと
- 必要なドライブおよびドライブボックスの増設が完了していること

SVP の要件は、「1.6.2 管理サーバ（SVP）の要件（19 ページ）」を参照してください。管理クライアントの要件は、「1.6.3 管理するための PC（管理クライアント）要件（25 ページ）」を参照してください。

ストレージシステムの動作状態は、コントローラシャーシの LED で確認できます。『ハードウェア リファレンスガイド』を参照してください。

B.2 ライセンスの設定

プログラムプロダクトとして提供される機能を利用するには、ライセンスキーのインストールが必要です。

ライセンスキーのインストール方法は「3.4 ライセンス（68 ページ）」を参照してください。

プログラムプロダクトの概要については、ドキュメントマップを参照してください。

B.3 監査ログの設定

監査ログを Syslog サーバへ転送するよう設定します。その後、テストメッセージを Syslog サーバへ送信して、正しく設定されているか確認します。

監査ログの設定方法は「3.7 監査ログ（76 ページ）」を参照してください。

B.4 障害通知設定

ストレージシステムの障害情報（SIM）を通知するための設定をします。

障害情報は、メール（Email）、Syslog、SNMP、Windows イベントログを利用して通知できます。どれか 1 つ以上を設定してください。

メール（Email）、Syslog、および SNMP の設定方法は「3.3 アラート通知（59 ページ）」を参照してください。Windows イベントログの設定方法は「B.4.1 Windows イベントログでストレージシステムの障害情報を監視する（223 ページ）」を参照してください。

B.4.1 Windows イベントログでストレージシステムの障害情報を監視する

ストレージシステムで発生した障害情報を Windows 標準機能であるイベントログへ出力することにより、ストレージシステムと Windows の障害情報を一元管理できます。

B.4.1.1 ストレージシステムの障害情報を Windows イベントログに出力する

ストレージシステムの障害情報を Windows イベントログに出力するには、バッチコマンドを実行します。このバッチコマンドを実行すると、以降は SVP を再起動しても、障害情報が Windows イベントログに出力されます。

Storage Device List で対象のストレージシステムのステータスが［READY］であれば、障害情報が Windows イベントログに出力されます。［READY］でない場合は、出力されません。

Windows イベントログへの障害情報出力の開始・停止手順を示します。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. コマンド `cd /d C:\Mapp\wk\`［装置識別番号］`\DKC200\mp\pc` を実行し、カレントディレクトリを移動します。

   例：`cd /d C:\Mapp\wk\934000600102\DKC200\mp\pc`

   - ［］内：引数
   - 装置識別番号：XX ＋装置名+ストレージシステムのシリアル番号で表すディレクトリを指定して ください。

     XXxxxxyyyyyy

     - XX：
       * iStorage V100, V300 の場合：93
       * iStorage V10e の場合：88
     - xxxx：装置名
       * iStorage V100, V300 の場合：4000

* iStorage V10e の場合：2000

- yyyyyy：ストレージシステムのシリアル番号
- 例：ストレージシステムのシリアル番号：600102 の場合

  装置識別番号：934000600102

メモ

カレントディレクトリを移動しないと、手順 3 でバッチファイルを実行してもイベントログが出力されません。

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. バッチファイル（`eventlog.bat` ［出力開始・停止］ ［監視周期］）を実行します。

項目	内容
出力開始・停止	0：障害情報の出力停止 1：障害情報の出力開始 このパラメータを省略した場合は、0：出力停止を意味します。
監視周期	ストレージシステムで発生した障害情報を監視する周期を入力します。 入力範囲は 5 分～720 分です。 出力開始・停止が 1 のときだけ指定します。

メモ

バッチファイルがインストールされているフォルダにある他のファイルを誤って操作しないように注意してください。

4. コマンドが正常に終了すると、プロンプトが表示されます。
5. コマンドプロンプトを閉じます。

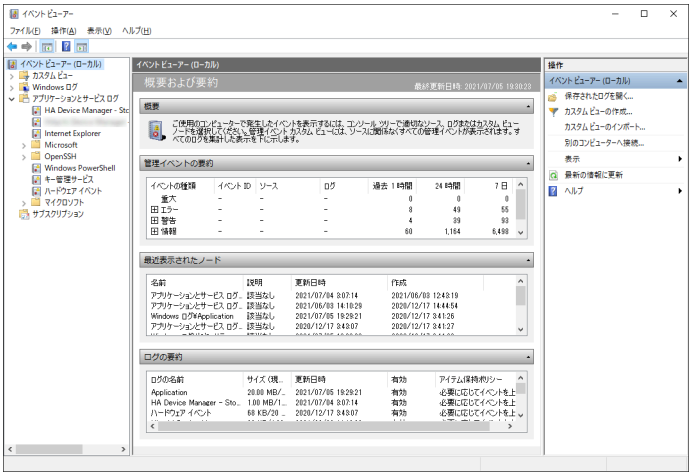
B.4.1.2 Windows イベントログの参照

SVP に出力された Windows イベントログを参照します。

操作手順

1. Windows のスタートメニューより、［コントロールパネル］－［システムとセキュリティ］－［管理ツール］または［Windows ツール］から［イベントビューアー］を起動します。

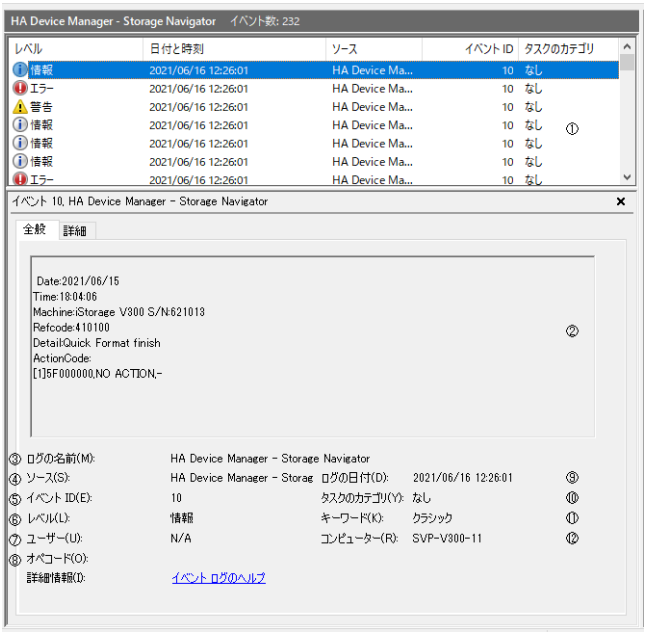
2. イベントビューアーの［アプリケーションとサービス ログ］－［HA Device Manager - Storage Navigator］をクリックします。



3. 障害情報が出力されます。

B.4.1.3 ストレージシステムの障害情報の出力例

ストレージシステムの障害情報例を示します。



項番	項目	内容
①	障害情報一覧	障害情報の一覧が表示されます。
②	障害情報詳細	一覧で選択した障害情報の詳細情報が表示されます。 Date：障害が発生した日付 Time：障害が発生した時刻 Machine：ストレージシステムの装置名とシリアル番号 Refcode：SIM リファレンスコード※ Detail ：障害内容※

項番	項目	内容
		ActionCode：［アクションコード］、［想定障害部品］、および［ロケーション］の項目が含まれます。不良個所の情報は最大 8 件表示されます。
③	ログの名前	ログの種類 「HA Device Manager - Storage Navigator」固定
④	ソース	イベントのアプリケーション名 「HA Device Manager - Storage Navigator」固定
⑤	イベント ID	イベント ID 「10」固定
⑥	レベル	SIM リファレンスコードのアラートレベル※により次のように表示されます。 エラー：Acute または Serious 警告：Moderate 情報：Service
⑦	ユーザー	「N/A」固定
⑧	オペコード	空白
⑨	ログの日付	イベントログを登録した日時
⑩	タスクのカテゴリ	「なし」固定
⑪	キーワード	「クラシック」固定
⑫	コンピューター	イベントが発生したコンピュータ名 「コンピュータ名」

注※

SIM リファレンスコード、障害内容およびアラートレベルは、『SIM リファレンス』を参照してください。

B.4.1.4 ストレージシステムの運用に支障が無いイベント

以下のイベントが発生しても、ストレージシステムの運用には支障がありません。無視してください。

イベント	イベント発生の契機
ログの種類：アプリケーション ソース：Application Error イベント ID：1000 レベル：エラー 障害が発生しているアプリケーション名： DkcMan.exe 障害が発生しているモジュール名： ntdll.dll、または jvm.dll 例外コード：0xc0000005	このイベントは、以下のどちらかのタイミングで発生することがあります。 • ストレージ管理ソフトウェアを更新したとき • SVP をシャットダウンまたは再起動したとき
ログの種類：アプリケーション ソース：Application Error	このイベントは、ストレージシステムのサービス停止時に発生することがあります。

イベント	イベント発生の契機
イベント ID：1000 レベル：エラー 障害が発生しているアプリケーション名： KickJava.exe 障害が発生しているモジュール名： SVPCMN32.dll 例外コード：0xc0000005	
ログの種類：アプリケーション ソース：Application Error イベント ID：1000 レベル：エラー 障害が発生しているアプリケーション名： MpcL7Comm.exe 障害が発生しているモジュール名： MpcL7Mem.dll 例外コード：0xc0000005	このイベントは、以下のいずれかのタイミングで発生することがあります。 • ストレージシステムのサービスを停止したとき • ストレージ管理ソフトウェアを更新したとき • SVP をシャットダウンまたは再起動したとき
ログの種類：アプリケーション ソース：Application Error イベント ID：1000 レベル：エラー 障害が発生しているアプリケーション名： RestPush_Base.exe 障害が発生しているモジュール名： jvm.dll 例外コード：0xc0000005, 又は 0xc000041d	このイベントは、ストレージシステムのサービス停止時に発生することがあります。
ログの種類：システム ソース：TaskScheduler イベント ID：414 レベル：警告 タスクのカテゴリー： タスクの構成が正しくありません 詳細： タスク スケジューラ サービスが、構成の間違いを検出しました。	このイベントは、SVP ソフトウェアの更新時に発生することがあります。

B.5 ホストに割り当てる LDEV の作成と LUN パス定義の手順

パリティグループと LDEV を作成し、ホストから LDEV を認識させるためにホストグループへの LUN パスを設定する手順を説明します。

メモ

DP（Dynamic Provisioning）プールの作成方法は、『システム構築ガイド』を参照してください。

ホストは、ストレージシステムの LDEV（ボリューム）にアクセスしてデータのリード・ライトを行います。LDEV を作成し、ホストへ割り当てるためには、事前にパリティグループを作成する必要があります。パリティグループとは、複数のドライブを組み合わせた 1 つの RAID グループです。パリティグループから切り出した論理的な記憶領域を LDEV として使用します。作成した LDEV をホストに認識させるためには、ホストグループに LDEV の LUN パスを定義します。

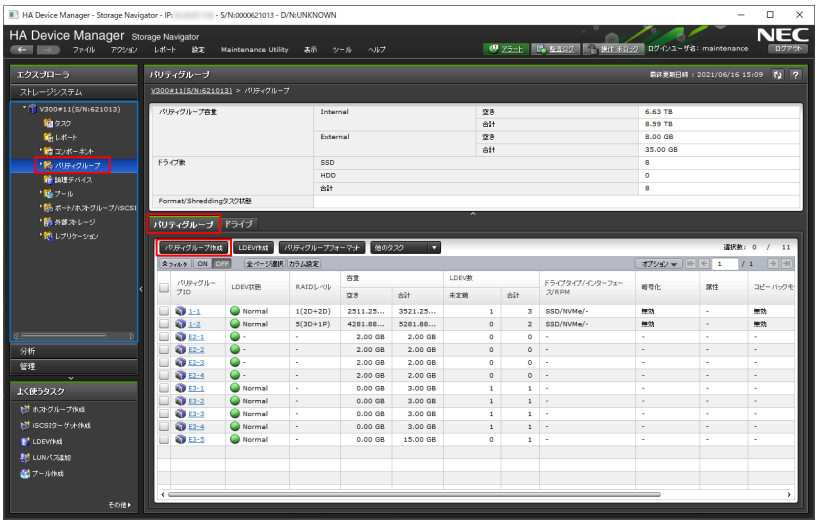
作業は、Storage Navigator から行います。

B.5.1 Storage Navigator から LDEV 作成と LUN パス定義をする

パリティグループ作成、スペアドライブ割り当て、LDEV 作成、LUN パス割り当ての順で設定します。Storage Navigator からは、これらをウィザード形式で設定できます。

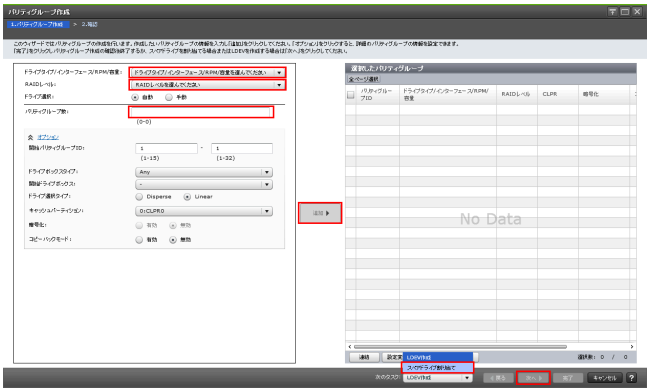
操作手順

1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［パリティグループ］を選択します。
2. ［パリティグループ］タブの［パリティグループ作成］をクリックします。



3. ［ドライブタイプ/インターフェース/RPM/容量］と［RAID レベル］と［パリティグループ数］で作成したいパリティグループ数を入力し［追加］をクリックします。
4. スペアドライブを割り当てる場合は、［次のタスク］から［スペアドライブ割り当て］を選択して［次へ］をクリックします。

   スペアドライブを割り当てない場合は、［次のタスク］から［LDEV 作成］を選択して［次へ］をクリックします。手順 6 に進みます。

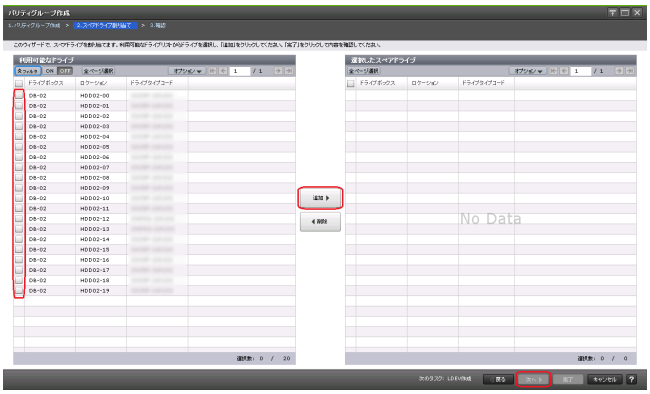


ヒント

- パリティグループを作成した段階で作業を完了する場合は、[完了] をクリックします。
- [オプション] をクリックすると、パリティグループの詳細情報を設定できます。

5. [スペアドライブ割り当て] 画面が表示されます。

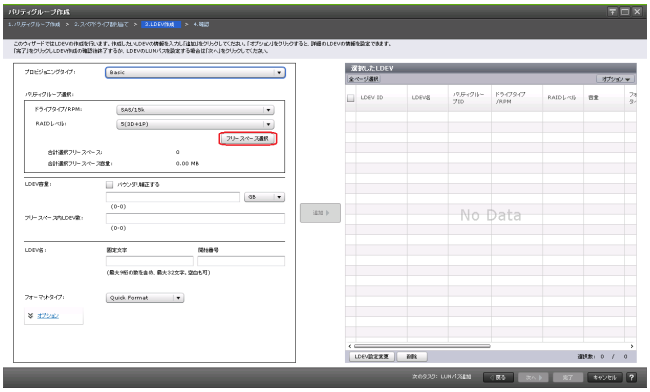
[利用可能なドライブ] リストからドライブを選択し、[追加] をクリックします。[選択したスペアドライブ] に追加されます。LDEV を作成するために [次へ] をクリックします。



ヒント

- スペアドライブを割り当てた段階で作業を完了する場合は、[完了] をクリックします。
- スペアドライブの追加は、[ストレージシステム] ツリーから [パリティグループ] を選択し、[ドライブ] タブの [スペアドライブ追加] からでもできます（参照：「E.1.1 スペアドライブの割り当てと削除（292 ページ）」）。

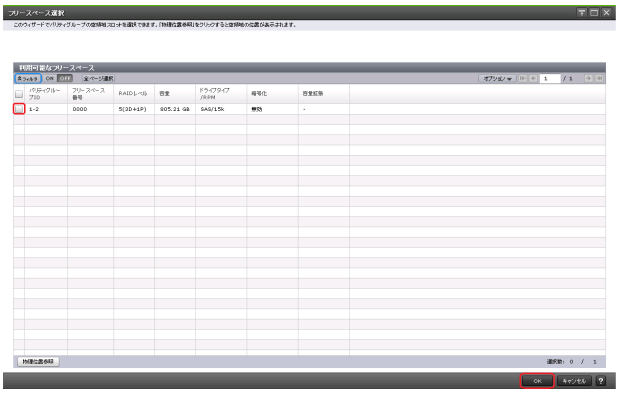
6. [LDEV 作成] 画面で [フリースペース選択] をクリックします。



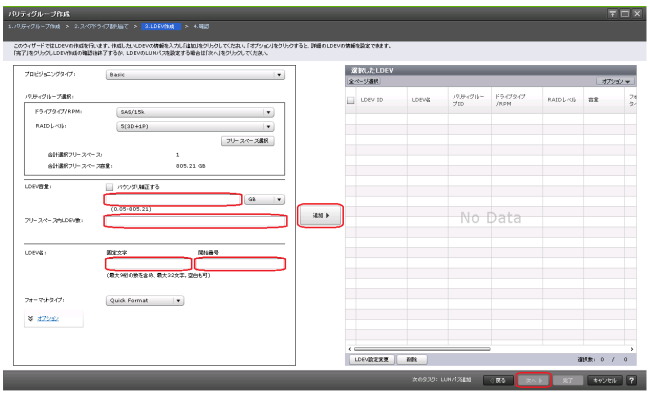
ヒント

- ［オプション］をクリックすると、LDEV の詳細情報を設定できます。
- 論理デバイスの作成は、［ストレージシステム］ツリーから［論理デバイス］を選択し、［LDEV］タブの［LDEV 作成］からでもできます（参照：「E.1.4 LDEV の作成（295 ページ）」）。

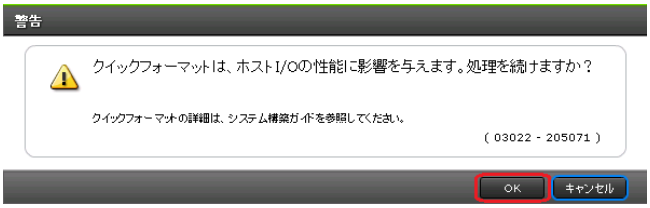
7. ［利用可能なフリースペース］から手順 3 で作成したパリティグループを選択して［OK］をクリックします。



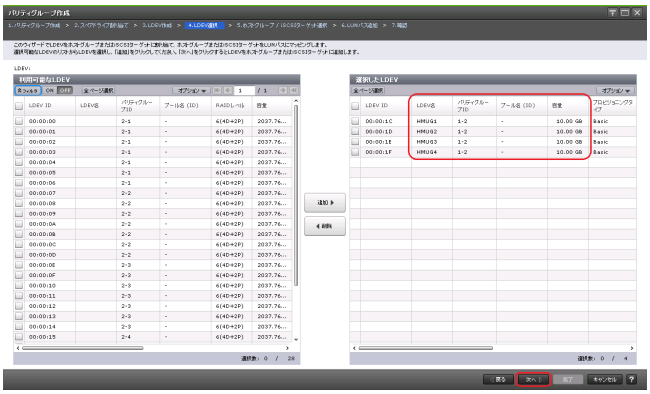
8. ［LDEV 容量］、［フリースペース内 LDEV 数］、［LDEV 名］の［固定文字］、および［LDEV 名］の［開始番号］を入力して［追加］をクリックします。［選択した LDEV］を確認して［次へ］をクリックします。なお、入力した［開始番号］が使用済の場合は、入力した番号以降で使用可能な番号が小さい順に割り当てられます。



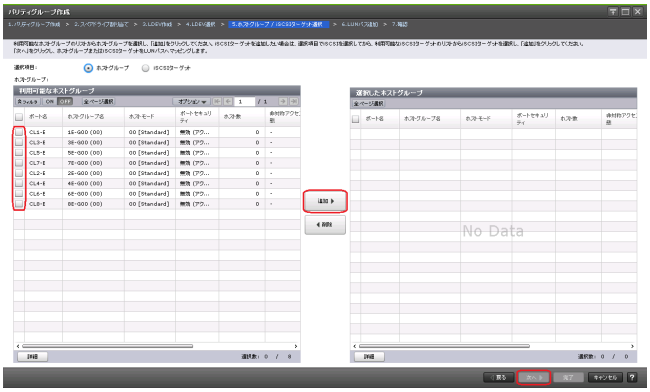
9. クイックフォーマットに関する警告メッセージが表示されます。［OK］をクリックします。



10. ［選択した LDEV］に、手順 8 で作成した LDEV が表示されていることを確認して［次へ］をクリックします。



11. ［ホストグループ/iSCSI ターゲット選択］画面が表示されます。

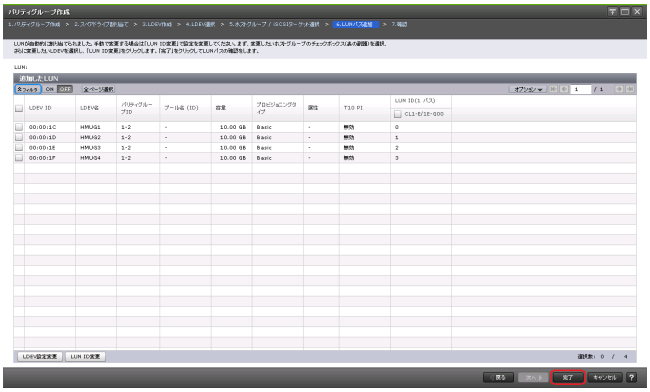


   a. ［選択項目］から［ホストグループ］または［iSCSI ターゲット］を選択します。

   b. ［ホストグループ］を選択した場合は、［利用可能なホストグループ］から、ホストグループを選択して［追加］をクリックします。［iSCSI ターゲット］を選択した場合は、［利用可能な iSCSI ターゲット］から、iSCSI ターゲットを選択して［追加］をクリックします。

   c. ［次へ］をクリックします。

12. ［LUN パス追加］画面が表示されます。内容を確認し［完了］をクリックします。



13. 確認画面が表示されます。内容を確認し、タスク名を指定後、[適用]をクリックします。

メモ

プールを作成する場合、『システム構築ガイド』の Dynamic Provisioning のプールを作成する手順を参照してください。

B.6 ホスト接続ポートの設定の手順

ホストへ接続するストレージシステムのポートを、ネットワーク環境に合わせて設定します。

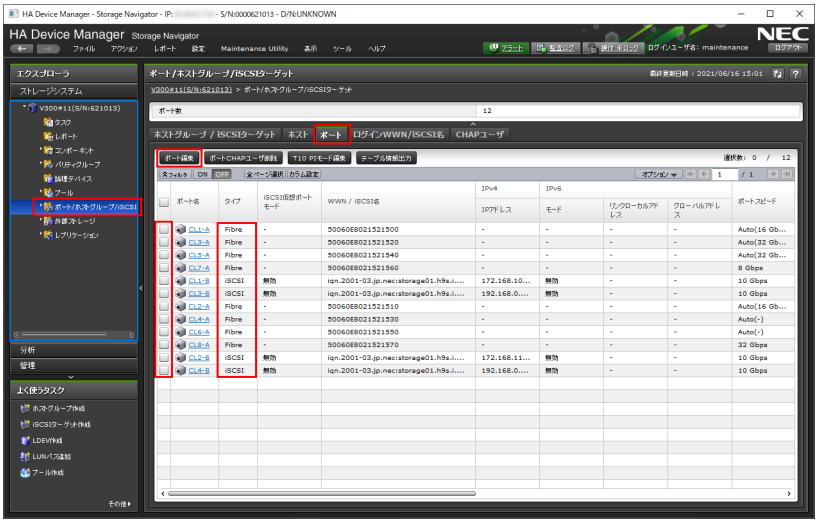
B.6.1 Storage Navigator からポートを設定する

ストレージシステムをホストサーバへ接続するインターフェースに Fibre Channel を使用している場合は「B.6.1.1 Fibre Channel ポートの設定（Storage Navigator）（232 ページ）」を、iSCSI を使用している場合は「B.6.1.2 iSCSI ポートの設定（Storage Navigator）（233 ページ）」を参照し、ポートを設定します。

B.6.1.1 Fibre Channel ポートの設定（Storage Navigator）

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ポート］タブをクリックします。
3. 編集するポート（［タイプ］が Fibre）を選択します。
4. ［ポート編集］をクリックします。



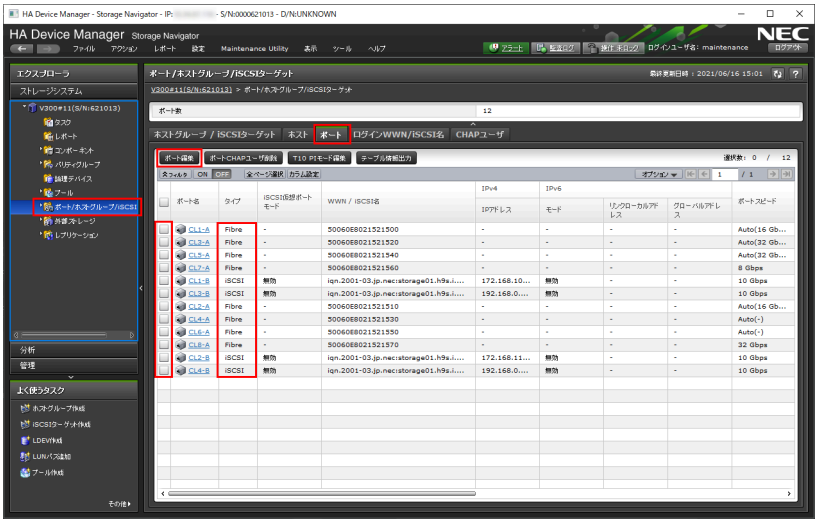
5. ［ポート編集］画面が表示されます。詳細は、『システム構築ガイド』の「ポート編集ウィザード」を参照してください。編集後、［完了］をクリックします。

6. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

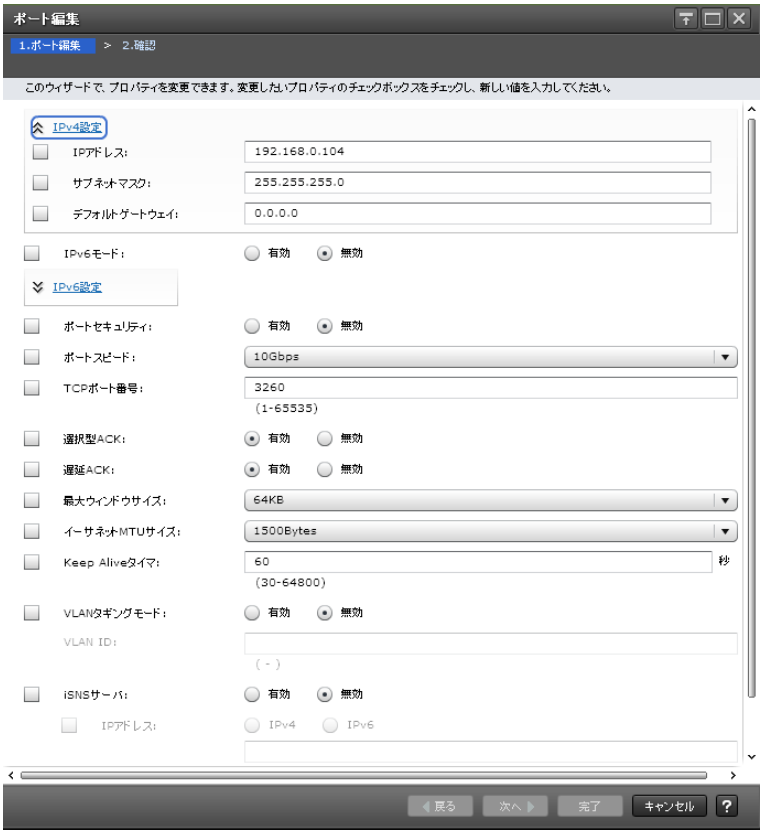
B.6.1.2 iSCSI ポートの設定（Storage Navigator）

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ポート］タブをクリックします。
3. 編集するポート（［タイプ］が iSCSI）を選択します。
4. ［ポート編集］をクリックします。



5. ［ポート編集］画面が表示されます。詳細は、『システム構築ガイド』の「ポート編集ウィザード」を参照してください。編集後、［完了］をクリックします。



6. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

B.7 ホストグループ/iSCSI ターゲットの編集の手順

ホストグループのホストモードとホストモードオプションを設定します。

LDEV を割り当てる LUN パスは、ホストグループ単位で定義します。ホストグループは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です。

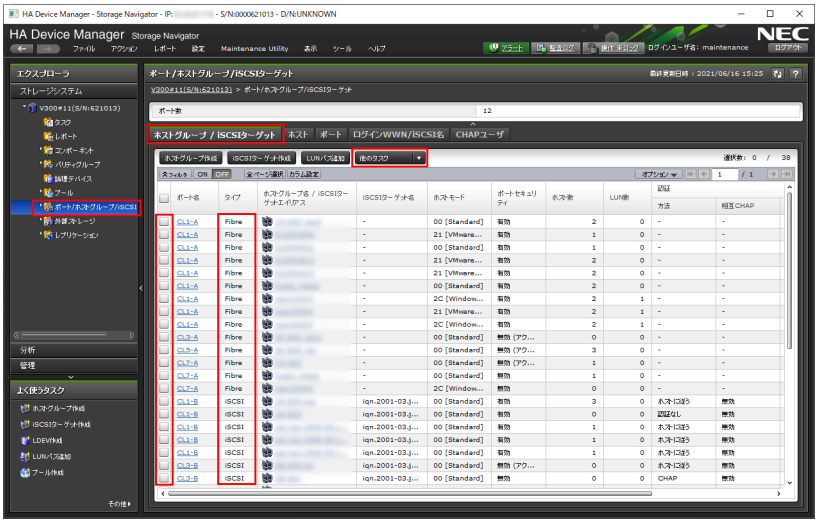
B.7.1 Storage Navigator からホストグループ/iSCSI ターゲットを編集する

ストレージシステムをホストサーバへ接続するインターフェースに Fibre Channel を使用している場合は「B.7.1.1 ホストグループの編集（Storage Navigator）（235 ページ）」を、iSCSI を使用している場合は「B.7.1.2 iSCSI ターゲットの編集（Storage Navigator）（236 ページ）」を参照し、ホストモードとホストモードオプションを設定します。

B.7.1.1 ホストグループの編集（Storage Navigator）

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ホストグループ］タブをクリックします。
3. 編集するホストグループ（［タイプ］が Fibre）を選択します。
4. ［他のタスク］－［ホストグループ編集］を選択します。



5. ［ホストグループ編集］画面が表示されます。詳細は、「B.7.2 ホストモード一覧（237 ページ）」および「B.7.3 ホストモードオプション一覧（239 ページ）」を参照してください。編集後、［完了］をクリックします。

6. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

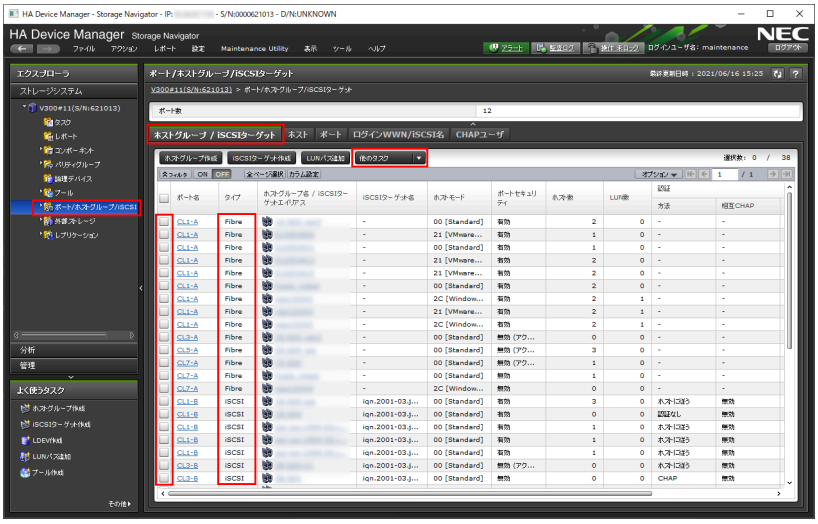
B.7.1.2 iSCSI ターゲットの編集（Storage Navigator）

iSCSI では、ホスト接続モード、論理デバイスの割り当て、LUN セキュリティ情報はポートではなくターゲットに設定されます。これにより、各ターゲットに基づきストレージシステムが接続されているホストを選択します。

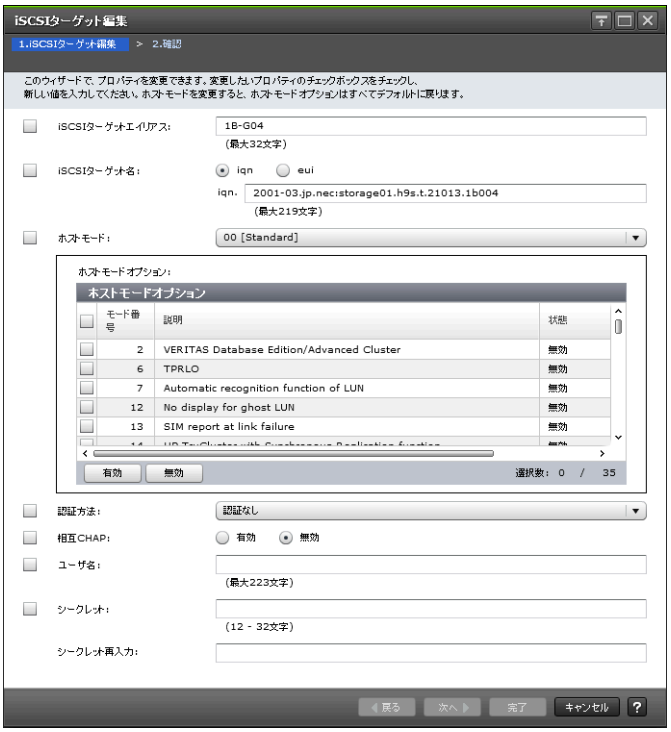
各 iSCSI ポートには初期構成として常に Target000 が存在します。

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ホストグループ］タブをクリックします。
3. 編集する iSCSI ターゲット（［タイプ］が iSCSI）を選択します。
4. ［他のタスク］－［iSCSI ターゲット編集］を選択します。



5. ［iSCSI ターゲット編集］画面が表示されます。詳細は、「B.7.2　ホストモード一覧（237 ページ）」および「B.7.3　ホストモードオプション一覧（239 ページ）」を参照してください。編集後、［完了］をクリックします。



6. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

B.7.2　ホストモード一覧

ホストモードを、ホストグループまたは iSCSI ターゲットに設定します。設定できるモードの一覧を次に示します。

一覧に記載のないホストモードが画面に表示される場合がありますが、使用しないでください。

ホストモード	どんな場合にこのホストモードを選択すればよいか
00 [Standard]	Red Hat Linux などのサーバホストをホストグループに登録する場合
21 [VMware Extension]	VMware のサーバホストをホストグループに登録する場合※1
2C [Windows Extension]	Windows のサーバホストをホストグループに登録する場合

注※1

次の 3 種類のサーバホストおよび VMware 上の複数の仮想ホストを 1 つのホストグループに統合することが可能です。

- VMware のサーバホスト：VMware 上で RDM（Raw Device Mapping）方式で LU を認識している Linux 系や Windows の仮想ホストや、VMware 上の VMFS 上で動作する Linux 系や Windows の仮想ホストも含まれます。
- Red Hat Linux などの Linux 系 OS のサーバホスト
- Windows のサーバホスト

これらのサーバホストを 1 つのホストグループに追加する場合は、次のホストモードおよびホストモードオプションを設定してください。

- ホストモード：21 [VMware Extension]
- ホストモードオプション：2、22、25、54、63、68、および 110

ただし、複数種類のサーバホストおよび VMware 上の複数種類の仮想ホストを 1 つのホストグループに統合する場合は、次の注意事項があります。

- Windows がサポートする Offloaded Data Transfer（ODX）機能は、Windows のサーバホストのみで使用可能です。VMware 上の Windows 仮想ホストでは使用できません。
- Windows がサポートする Thin Provisioning 機能を使用する場合は、Windows のサーバホストおよび VMware 上の複数種類の仮想ホストを 1 つのホストグループに統合できません。次の設定のホストグループに Windows のサーバホストまたは RDM を利用する Windows の仮想ホストのみを追加してください。
  - ホストモード：2C [Windows Extension]
  - ホストモードオプション：73
- Windows がサポートする Thin Provisioning 機能を使用しない場合は、複数種類のサーバホストおよび VMware 上の複数種類の仮想ホストを 1 つのホストグループに統合できます。ただし、ホストモードオプション 73 を設定しないでください。ホストモードオプション 73 を設定した場合、同一ホストグループに追加された Linux 系 OS のサーバホストおよび Linux 系 OS の仮想ホストの Thin Provisioning 機能が動作しません。

上記の制限事項を回避するには、VMware のサーバホストおよび VMware 上の仮想ホストの OS 種別ごとにホストグループを作成し、対応したホストモードを設定する必要があります。VMware 上の仮想ホストが RDM 方式で LU を認識している環境において、

VMware のサーバホストおよび VMware 上の複数の仮想ホストについてホストの OS 種別ごとにホストグループを分けるには、ホストグループ別に物理 FC HBA が必要になります。

B.7.3 ホストモードオプション一覧

ホストモードオプションを、ホストグループまたは iSCSI ターゲットに設定します。設定できるオプションの一覧を次に示します。

一覧に記載のないホストモードオプションが画面に表示される場合がありますが、使用しないでください。

No.	ホストモードオプション	ホストモードオプションの選択条件
2	VERITAS Database Edition/ Advanced Cluster	次の条件のどれかが満たされる場合 • Windows Server Failover Clustering（WSFC）を使用する場合 • Microsoft Failover Cluster（MSFC）を使用する場合 • 上記以外の構成で、Key 登録の無いパスからの Test Unit Ready に対する応答を Reservation Conflict から Good Status に変更する場合 補足事項 : PERSISTENT GROUP RESERVATION の Key 登録のないホストから TEST UNIT READY コマンドが発行されると、ストレージシステムはデフォルトで RESERVATION CONFLICT ステータスを応答します。しかし、ホストによっては GOOD ステータスを期待する場合があります。このホストモードオプションを有効にすると、ストレージシステムは TEST UNIT READY コマンドの応答を RESERVATION CONFLICT ステータスから GOOD ステータスに切り替えます。
6	TPRLO	次のすべての条件が満たされる場合 • ホストモードの「2C [Windows Extension]」を使用する • Broadcom（Emulex）社製のホストバスアダプタを使用する • ミニポートドライバを使用する • ホストバスアダプタのミニポートドライバに TPRLO=2 が設定されている 補足事項 : TPRLO に対して、ストレージシステムはデフォルトで PRLO を応答しますが、ホストによっては LOGO を期待する場合があります。このホストモードオプションを有効にすると、ストレージシステムは TPRLO の応答を PRLO から LOGO に切り替えます。
7	Automatic recognition function of LUN	次の条件が満たされる場合 • SCSI パス変更時にホストに UNIT ATTENTION を返却したい 補足事項 : ホストグループに LU を追加する際、デフォルトでは UNIT ATTENTION がホストに応答されませんが、ホストによっては UNIT ATTENTION 応答を期待する場合があります。このホストモードオプションを有効にすると、ストレージシステムは UNIT ATTENTION をホストに応答します。
13	SIM report at link failure※1	ポート間のリンク障害の検出数が一定のしきい値を超えたとき、SIM（Service Information Message）によってユーザに通知する場合 補足事項 : このホストモードオプションを使用する場合、Target ポートのホストグループ番号 0 に、このホストモードオプションを設定してください。
22	Veritas Cluster Server	次の条件のどれかが満たされる場合 • Veritas Cluster Server を使用する場合

No.	ホストモードオプション	ホストモードオプションの選択条件
		• SPC-4 に対応した OS やミドルウェアを使用する場合 • シングルサイトおよび、Active Mirror によるデュアルサイトの Clustered VMDK 構成を使用する場合 補足事項 : PERSISTENT GROUP RESERVATION の Key 登録をしていないホストから MODE SENSE コマンドが発行されると、ストレージシステムはデフォルトで RESERVATION CONFLICT ステータスを応答します。しかし、ホストによっては GOOD ステータスを期待する場合があります。このホストモードオプションを有効にすると、ストレージシステムは MODE SENSE コマンドの応答を RESERVATION CONFLICT ステータスから GOOD ステータスに切り替えます。
25	Support SPC-3 behavior on Persistent Reservation	次の条件のどれかが満たされる場合 • Windows Server Failover Clustering（WSFC）を使用する場合 • Microsoft Failover Cluster（MSFC）を使用する場合 • 上記以外の構成で、PERSISTENT RESERVE OUT（Service Action=REGISTER AND IGNORE EXISTING KEY）コマンドによって削除対象の登録済みキーがないときのステータス応答を Reservation Conflict から Good Status に変更する場合 補足事項 : ホストから PERSISTENT RESERVE OUT コマンド（Service Action = REGISTER AND IGNORE EXISTING KEY）が発行された際、削除対象の Key がストレージシステムに登録されていない場合、デフォルトでは RESERVATION CONFLICT ステータスをホストに応答します。しかし、ホストによっては GOOD ステータスを期待する場合があります。このホストモードオプションを有効にすると、ホストへの応答を RESERVATION CONFLICT ステータスから GOOD ステータスに切り替えます。
39	Change the nexus specified in the SCSI Target Reset	Target Reset を受領したときに次の範囲をホストグループごとに制御したい場合 • ジョブをリセットする範囲 • UA（Unit Attention）が設定される範囲 補足事項：ホストが、Target Reset のジョブのリセット範囲と UA 設定範囲を、リセットを発行したイニシエータのみではなく、ホストグループ内の全イニシエータを対象にすることを期待する場合に設定してください。
40	V-Vol expansion	次のすべての条件が満たされる場合 • ホストモードの「2C [Windows Extension]」を使用する場合 • 仮想ボリュームの容量を拡張したあと、拡張した仮想ボリュームの容量を自動的に認識させたい
51	Round Trip Set Up Option	ホスト I/O の応答時間を調節したい場合 例：Synchronous Replication ペア（または Active Mirror ペア）の正サイトのストレージシステムと副サイトのストレージシステムとの距離が長く（100km 程度）Point-to-point トポロジが使用されている場合
54	(VAAI) Support Option for the EXTENDED COPY command※3	VMware ESXi 6.5 以降の VAAI（vStorage APIs for Array Integration）機能を利用する場合 補足事項： • このホストモードオプションを設定すると、VMware ESXi 6.5 以降の VAAI (vStorage APIs for Array Integration) 機能がストレージシステムに発行する VENDOR SPECIFIC EXTENDED COPY コマンドを利用できるようになります。 • VMware ESXi 6.5 以降を接続する場合、このホストモードオプションとホストモードオプション 63 を組み合わせて使用してください。

No.	ホストモードオプション	ホストモードオプションの選択条件
60	LUN0 Change Guard	LUN0 の追加または削除を抑止したい場合
63	(VAAI) Support Option for vStorage APIs based on T10 standards※3	VMware ESXi 6.5 以降に接続し、T10 対応の VAAI 機能を利用する場合。 このオプションとホストモードオプション 54 を組み合わせて使用してください。
68	Support Page Reclamation for Linux※3	Linux のホストに接続している環境から Page Reclamation 機能を利用する場合。 補足事項：このホストモードオプションは、Linux 2.6.33 以降を接続した際に有効になります。
71	Change the Unit Attention for Blocked Pool-VOLs	プールボリューム閉塞時の UA（Unit Attention）の応答を NOT READY から MEDIUM ERROR に変更する場合
73	Support Option for WS2012 ※3	Windows Server 2012 以降の Windows OS ホストに接続している環境から、Windows Server 2012 以降が提供する Thin Provisioning 機能および Offloaded Data Transfer（ODX）機能を利用する場合。 補足事項：ホストモードオプション 73 とホストモードオプション 110 の両方が設定されている場合、ホストモードオプション 73 が優先されます。
78	The non-preferred path option	次のすべての条件が満たされる場合 • データセンタを接続した構成（Metro 構成）で Active Mirror を使用している。 • マルチパスソフトウェアとして HA Dynamic Link Manager を使用している。 • ホストグループが HA Dynamic Link Manager の非最適化パス上にある。 • HA Dynamic Link Manager の非最適化パスで I/O をさせずに、I/O の応答の性能低下が回避できる。 **⚠ 注意** 誤ったホストグループに、このホストモードオプションを設定すると、HA Dynamic Link Manager のロードバランシング機能が意図しない動作となり、性能問題を招くおそれがあります。
80	Multi Text OFF	MultiText 機能をサポートしていない OS のホストとストレージシステムを iSCSI で接続する場合。
81	NOP-In Suppress Mode	iSCSI によって接続されている環境では、センスコマンド（Inquiry、Test unit ready、Mode sense など）を実行して NOP-IN を送信して、上位レイヤーの Delayed Ack 機能の応答遅延を抑止します。しかし、NOP-IN の送信が不要なホストとストレージシステムを接続する場合、このオプションを選択してください。
82	Discovery CHAP Mode	iSCSI によって接続されている環境で、ディスカバリログイン時に CHAP 認証する場合。 例 : VMware のホストとストレージシステムを iSCSI で接続している環境で、ディスカバリログイン時に CHAP 認証する場合
83	Report iSCSI Full Portal List Mode	VMware のホストとストレージシステムを iSCSI によって接続している環境で冗長パスを構成し、[動的検出] タブに設定するディスカバリアドレス（IP アドレス）を 1 個にする場合。 補足事項： • このホストモードオプションを設定すると、Send Target 要求を受領した iSCSI Target と同じ iSCSI Target Name、かつ同じ Target 番号が対象として報告されます。ポータルリスト報告が必要な Target 情報については、Send Target 要求を受領したポート配下にある

No.	ホストモードオプション	ホストモードオプションの選択条件
		iSCSI Target の iSCSI Target Name、および Target 番号が一致していることを確認してください。 • 報告が必要なすべての Target に対して、このホストモードオプションを設定してください。
91	Disable I/O wait for OpenStack Option	OpenStack の I/O データパスとして利用されるホストグループ（ファイバチャネル接続時）または iSCSI ターゲット（iSCSI 接続時）を手動設定で作成する場合
94	Disable initiator function on port※5	次のホスト接続構成で運用する際に使用してください。 • ストレージシステムとの接続をサポートしている Broadcom（Emulex）社製の 16Gbps、32Gbps、または 64Gbps の Fibre Channel HBA と、ファイバチャネルのチャネルボードを直接接続して、SAN Boot システムを構築する場合。 • FC-AL で接続されているホストおよびストレージシステムを起動した後、またはすでに起動されているホストおよびストレージシステムを FC-AL で接続した後に、ボリュームが認識できない場合。 • 上記以外の接続構成でシステムを運用する際に設定の指定があった場合。※4 補足事項：ホストの構成によっては、本ホストモードオプションを設定しないと、ストレージシステムのファイバチャネルポートのイニシエータ機能が動作することにより、ホストがデバイスを認識しない場合があります。
96	Change the nexus specified in the SCSI Logical Unit Reset	LU Reset を受領したときに次の範囲をホストグループごとに制御したい場合 • ジョブをリセットする範囲 • UA（Unit Attention）が設定される範囲 補足事項：ホストが、LU Reset のジョブのリセット範囲と UA 設定範囲を、リセットを発行したイニシエータのみではなく、ホストグループ内の全イニシエータを対象にすることを期待する場合に設定します。
105	Task Set Full response in the event of I/O overload	次のすべての条件が満たされる場合 • ホストモードの「2C [Windows Extension]」を使用する場合 • ストレージシステムが I/O 過負荷のときに、ホスト側に Task Set Full を応答させたい場合
109	Change FLOGI TOV on port※5	次のホスト接続構成で運用する際に使用してください。 • ストレージシステムとの接続をサポートしている Broadcom（Emulex）社製の 16Gbps、32Gbps、または 64Gbps の Fibre Channel HBA と、ファイバチャネルのチャネルボードを直接接続して、SAN Boot システムを構築する場合。 • 上記以外の接続構成でシステムを運用する際に設定の指定があった場合。※4
110	ODX support for WS2012※3	Windows Server 2012 以降のホストに接続している環境から、Windows Server 2012 以降が提供する Offloaded Data Transfer（ODX）機能を利用する場合 補足事項：ホストモードオプション 73 とホストモードオプション 110 の両方が設定されている場合、ホストモードオプション 73 が優先されます。
113	iSCSI CHAP Authentication Log※2	CHAP 認証の認証結果を監査ログ（DKC）に出力したい場合 補足事項：このホストモードオプションを使用する場合、ホストグループ番号 0 に、このホストモードオプションを設定してください。

No.	ホストモードオプション	ホストモードオプションの選択条件
114	The automatic asynchronous reclamation on ESXi6.5 or later※3	VMware ESXi6.5 以降に接続し、VMFS（Virtual Machine File System）上のファイル削除に伴い自動実行されるゼロデータページ破棄機能を使用する場合。 このオプションとホストモードオプション 63 を組み合わせて使用してください。
122	Task Set Full response after reach QoS upper limit	Windows/Linux/VMware ホストに接続している環境で、QoS の上限値到達時に、ストレージシステム内部で I/O を滞留させずに、ホストに TASK SET FULL 応答を返したい場合

注※1

設定するように依頼があったときだけ設定してください。

注※2

このホストモードオプションの設定は、ポート単位で有効になります。設定対象のポートの iSCSI ターゲット 00 に、このホストモードオプションを設定してください。

注※3

このホストモードオプションを設定後、ホスト側で INQUIRY コマンドを再発行するような操作（サーバリブートなど）を実施してください。

注※4

適用対象の接続構成条件については、PP サポートサービスにお問い合わせください。また、このオプションを設定した場合、外部ストレージ接続ポートやリモートコピー接続ポートとして使用しないでください。

注※5

このホストモードオプションの設定は、ポート単位で有効になります。設定対象のポートのホストグループ 0 に、このホストモードオプションを設定してください。

メモ

Storage Advisor Embedded でサーバを管理している場合、サーバの OS タイプに対応するホストモードおよび OS タイプのオプションに対応するホストモードオプションがホストグループに自動で設定されます。それぞれの OS タイプに対応するホストモードおよびデフォルトで設定されるホストモードオプションを、次の表に示します。 ホストモードオプションの設定を編集する場合、対象サーバの OS タイプのオプションを変更してください。詳細については、『HA Storage Advisor Embedded ガイド』を参照してください。

サーバの OS タイプ	ホストモード	デフォルトで設定されるホストモードオプション（OS タイプのオプション）
Linux	00 [Standard]	2、22、25、68
VMware	21 [VMware Extension]	2、22、25、40、54、63、68、110

サーバの OS タイプ	ホストモード	デフォルトで設定されるホストモードオプション（OS タイプのオプション）
Windows	2C [Windows Extension]	2、22、25、40、110

B.8 初期構築作業完了後の確認

初期構築が終了したあと、正常に作業が完了していることを確認します。

初期構築作業が正しく完了すると、ホストからストレージシステムの LDEV が認識できます。また、Storage Navigator、Maintenance Utility から、設定した内容が管理 GUI に反映されます。

ホストからストレージシステムの LDEV が認識できなかったり、Storage Navigator、Maintenance Utility から設定した内容がそれぞれの管理 GUI に反映されていなかったりする場合は、初期構築作業が正常に完了していません。「第 5 章 トラブルシュート（101 ページ）」へ進み、不具合を解消してください。

問題がなければ運用の準備が整います。「第 4 章 ストレージシステム運用上の注意（96 ページ）」の内容を確認して理解したあと、『システム構築ガイド』を参照し、プログラムプロダクトを利用したストレージの運用を検討してください。

また、運用へ進む前に、次の項目も参考にしてください。

- 「付録 D. SVP による外部認証サーバとの連携（277 ページ）」
- 「付録 E. ドライブ管理（292 ページ）」
- 「付録 F. Fibre Channel ポートおよび iSCSI ポートの管理（304 ページ）」
- 「付録 G. SVP の管理と機能（314 ページ）」
- 「付録 H. ホスト接続の参考情報（394 ページ）」

付録 C.　SSL 通信の設定

管理 PC とストレージシステム、管理クライアントと SVP、および SVP とストレージシステムの通信をセキュアにするためには、SSL 通信を構築します。

C.1　SSL とは

Secure Sockets Layer（SSL）は、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す。SSL が有効になっている 2 つの装置は、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。どちらの装置も、ランダムに生成された対称鍵を利用して、転送するデータを暗号化します。

サーバ（SVP）を使用する場合、SVP と公開鍵と秘密鍵を結びつけるために、サーバ証明書を使用します。サーバ証明書によって、SVP は自分がサーバであることと鍵の所有者であることをクライアントに証明します。これによって SVP 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。サーバ証明書には次の 2 つの種類があります。

- 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 上で管理クライアントと SVP 間の通信が行われている場合は、この証明書でもセキュリティの向上を図れます。

- 認証局発行の証明書

  証明書発行要求を生成した後、信頼できる認証局に送付して署名してもらいます。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、信頼性が向上します。認証局の例としては Verisign 社があります。

メモ

- 秘密鍵と公開鍵とサーバ証明書の有効期限が切れていないことを確認してください。どれか 1 つでも有効期限が切れていると、ユーザはストレージシステム、または SVP に接続できなくなります。
- 証明機関から SSL サーバ証明書を発行する場合には数日かかります。

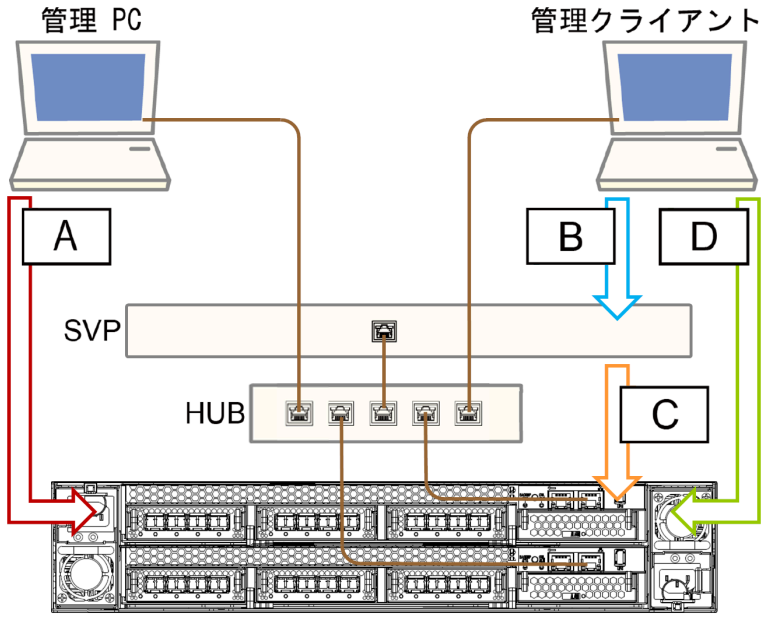
C.2　ストレージシステムの SSL 通信

ストレージシステムでは、次の図に示す記号 A～D の 4 つの接続経路で、SSL 通信を使用します。

SSL 通信で使用する暗号プロトコルは TLS バージョン 1.2 です。

SSL 通信で使用する、RSA 鍵交換の暗号スイートのデフォルト設定は有効です。

図 C-1　SSL 通信の接続経路



各管理モデルで使用する接続経路と、各経路の通信用途を示します。

管理モデル	記号	接続経路	通信用途
HA Storage Advisor Embedded を利用する	A	管理 PC とストレージシステム間	Maintenance Utility、HA Storage Advisor Embedded、および内蔵 CLI の操作と、REST API へのアクセス
Storage Navigator を利用する	B	管理クライアントと SVP 間	Storage Navigator の操作
	C	SVP とストレージ間	SVP とストレージシステムの情報交換
	D	管理クライアントとストレージシステム間	Maintenance Utility の操作

各管理モデルで使用する証明書、および証明書のアップロード先を示します。

管理モデル	記号	使用する証明書	証明書のアップロード先
HA Storage Advisor Embedded を利用する	A	Web サーバ接続用証明書※	ストレージシステム
Storage Navigator を利用する	B	管理クライアントと SVP 間の SSL 通信の署名付き証明書	SVP
	C	SVP 接続用証明書※	ストレージシステムと SVP
		Web サーバ接続用証明書※	ストレージシステムと SVP
	D	Web サーバ接続用証明書※	ストレージシステム

注※: SVP 接続用証明書と Web サーバ接続用証明書には同じ証明書を使用できます。

⚠ 注意

記号 C の通信では、SVP は中間者攻撃を防ぐため、ストレージシステムと SVP の証明書を照合して接続の妥当性を検証します。記号 C での証明書アップロードの注意事項を示します。正しく操作しなかった場合は、SVP が正常に動作しません。

- ストレージシステムと SVP それぞれに、同じ証明書をアップロードする必要があります。

- 1 台の SVP で複数ストレージシステムを管理する場合、各ストレージシステムにすべて同じ証明書をアップロードする必要があります。
- 先にストレージシステムに証明書をアップロードしてから、SVP に証明書をアップロードする必要があります。

各管理モデルで使用する証明書用の暗号スイートを示します。

管理モデル	記号	接続経路	暗号スイート
HA Storage Advisor Embedded を利用する	A	管理 PC とストレージシステム間	• iStorage V100, V300 の場合、次のいずれかの暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_256_GCM_SHA384 - TLS_RSA_WITH_AES_256_CBC_SHA256 - TLS_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA256 • iStorage V10e の場合、暗号スイートを Maintenance Utility で選択できます（「3.12.3 暗号化スイートの選択（90 ページ）」参照）。 - TLS_RSA_WITH_AES_128_CBC_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_RSA_WITH_AES_128_CBC_SHA と TLS_RSA_WITH_AES_128_CBC_SHA256 を無効にする TLS_RSA_WITH_AES_128_CBC_SHA の場合、次の暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 の場合、次の暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA と TLS_RSA_WITH_AES_128_CBC_SHA256 の両方を無効にするの場合、次の暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
Storage Navigator を利用する	B	管理クライアントと SVP 間	• iStorage V100, V300 の場合、次のいずれかの暗号スイートを使用できます。 - TLS_RSA_WITH_AES_256_GCM_SHA384 - TLS_RSA_WITH_AES_256_CBC_SHA256 - TLS_RSA_WITH_AES_256_CBC_SHA

管理モデル	記号	接続経路	暗号スイート
			- TLS_PSK_WITH_AES_256_CBC_SHA - TLS_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_PSK_WITH_AES_128_CBC_SHA • iStorage V10e、かつ RSA 鍵交換の暗号スイートが有効の場合（デフォルトは有効）、次のいずれかの暗号スイートを使用できます（有効/無効の切り替えは「C.26 RSA 鍵交換の暗号スイート（271 ページ）」参照）。 - TLS_RSA_WITH_AES_256_GCM_SHA384 - TLS_RSA_WITH_AES_256_CBC_SHA256 - TLS_RSA_WITH_AES_256_CBC_SHA - TLS_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • iStorage V10e、かつ RSA 鍵交換の暗号スイートが無効の場合（デフォルトは有効）、次のいずれかの暗号スイートを使用できます（有効/無効の設定方法は「C.26 RSA 鍵交換の暗号スイート（271 ページ）」を参照）。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • iStorage V10e の場合、暗号化スイートで使用する DHE 鍵の下限長（デフォルトは 1024 ビット）を変更できます（「C.27 DHE 鍵の下限長の設定（274 ページ）」を参照）。
	C	SVP とストレージシステム間	• iStorage V100, V300 の場合、次の暗号スイートを Maintenance Utility で選択できます（「3.12.3 暗号化スイートの選択（90 ページ）」参照）。 - TLS_RSA_WITH_AES_128_CBC_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA • iStorage V10e の場合、次の暗号スイートを Maintenance Utility で選択できます（「3.12.3 暗号化スイートの選択（90 ページ）」参照）。 - TLS_RSA_WITH_AES_128_CBC_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_RSA_WITH_AES_128_CBC_SHA および TLS_RSA_WITH_AES_128_CBC_SHA256 を無効にする なお、上記の選択にかかわらず、次の暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

管理モデル	記号	接続経路	暗号スイート
	D	管理クライアントとストレージシステム間	• iStorage V100, V300 の場合、次のいずれかの暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_256_GCM_SHA384 - TLS_RSA_WITH_AES_256_CBC_SHA256 - TLS_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA256 • iStorage V10e の場合、暗号スイートを Maintenance Utility で選択できます（「3.12.3 暗号化スイートの選択（90 ページ）」参照）。 - TLS_RSA_WITH_AES_128_CBC_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA - TLS_RSA_WITH_AES_128_CBC_SHA および TLS_RSA_WITH_AES_128_CBC_SHA256 を無効にする TLS_RSA_WITH_AES_128_CBC_SHA の場合、次の暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 の場合、次の暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA と TLS_RSA_WITH_AES_128_CBC_SHA256 の両方を無効にするの場合、次の暗号スイートを使用できます。 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

C.3 SSL 通信の設定の流れ

SSL 通信に必要な設定の流れを次に示します。

作業項目	操作方法、参照先	必須/任意
OpenSSL の入手	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。または SVP に格納された OpenSSL を使用することもできます。	必須

作業項目	操作方法、参照先	必須/任意
	SVP の OpenSSL の格納ディレクトリは、C:\Mapp\OSS\apache\bin\openssl です。"C:\Mapp"は、SVP ソフトウェアのデフォルトのインストールディレクトリです。インストール時の指定により異なる場合があります。	
設定開始前に知っておくこと	「C.4 SVP のサーバ証明書を更新するときの注意事項（251 ページ）」	必須
秘密鍵の作成	「C.5 秘密鍵を作成（251 ページ）」	必須
公開鍵の作成	「C.6 公開鍵を作成（252 ページ）」	必須
証明付き証明書の取得	• 自己署名付きの証明書の場合: 「C.7 署名付き証明書を取得（254 ページ）」 • 認証局発行の証明書の場合: 「C.8 署名付きの信頼できる証明書を取得（255 ページ）」	必須
証明書アップロードの前処理	• HA Storage Advisor Embedded を利用する管理モデルの場合 「C.15 SVP 接続用証明書と 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（261 ページ）」 • Storage Navigator を利用する管理モデルの場合 「C.9 SSL 証明書のパスフレーズを解除（255 ページ）」 「C.15 SVP 接続用証明書と 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（261 ページ）」	必須
証明書のアップロード	• HA Storage Advisor Embedded を利用する管理モデルの場合 「C.15 SVP 接続用証明書と 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（261 ページ）」 • Storage Navigator を利用する管理モデルの場合 「C.11 SVP と管理クライアント間の SSL 通信の署名付き証明書を SVP へアップロード（258 ページ）」 「C.15 SVP 接続用証明書と 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（261 ページ）」 「C.16 SVP 接続用証明書を SVP へアップロード（262 ページ）」 「C.18 Web サーバ接続用証明書を SVP へアップロード（263 ページ）」	必須
HTTP 通信のブロック、HSTS の有効化	Storage Navigator を利用する管理モデルの場合に、必要に応じて設定します。 •「C.21 SVP への HTTP 通信を拒否（266 ページ）」 •「C.23 HSTS を有効化する（267 ページ）」	任意
RSA 鍵交換の暗号スイートの無効化または有効化	• HA Storage Advisor Embedded を利用する管理モデルの場合 RSA 鍵交換の暗号スイートを無効化したい場合に設定します。 -「3.12.3 暗号化スイートの選択（90 ページ）」 RSA 鍵交換の暗号スイートを有効化したい場合に設定します。 -「3.12.3 暗号化スイートの選択（90 ページ）」 • Storage Navigator を利用する管理モデルの場合 RSA 鍵交換の暗号スイートを無効化したい場合に設定します。 -「C.26 RSA 鍵交換の暗号スイート（271 ページ）」 -「C.26.1 SVP の RSA 鍵交換の暗号スイートを無効化する（272 ページ）」 -「3.12.3 暗号化スイートの選択（90 ページ）」 RSA 鍵交換の暗号スイートを有効化したい場合に設定します。 -「C.26 RSA 鍵交換の暗号スイート（271 ページ）」 -「C.26.2 SVP の RSA 鍵交換の暗号スイートを有効化する（273 ページ）」	任意

作業項目	操作方法、参照先	必須/任意
	-「3.12.3 暗号化スイートの選択（90 ページ）」	
DHE 鍵の下限長の設定	「C.27 DHE 鍵の下限長の設定（274 ページ）」	任意
トラブルシュート	「C.25 セキュリティ警告が表示されたときの対処方法（269 ページ）」	―

C.4 SVP のサーバ証明書を更新するときの注意事項

SVP のサーバ証明書を更新するときの注意事項を次に示します。

- 証明書を更新している間は、Storage Navigator で実行中および実行予定のタスクは実行されません。
- RMI 通信の証明書の更新は非同期（約 2 分以内）に実行されます。
- SSL 証明書の更新はシステムに大きな影響を与えます。SVP 故障の原因となることがあるため、設定する証明書と秘密鍵の整合性を十分にご確認ください。
- ご使用の環境によっては、証明書の更新が完了したあとの SVP の再起動に時間がかかることがあります。再起動が完了しても［電子証明書の更新］の更新完了画面は表示されず、Internal Server Error となりますが、証明書の更新は完了しています。

C.5 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。

   または SVP の OpenSSL を使用します。この場合インストールは不要です。SVP の OpenSSL の格納先ディレクトリは C:\Mapp\OSS\apache\bin\openssl です。

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

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. 次に示すコマンドを実行し、OpenSSL のバージョンを確認します。
   - OpenSSL をインストールした場合：
     `C:\openssl\bin\openssl version`
   - SVP の OpenSSL を使用する場合：
     `C:\Mapp\OSS\apache\bin\openssl version`
5. 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。
   - OpenSSL3.0.0 未満の場合
     - OpenSSL をインストールした場合：

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

     - SVP の OpenSSL を使用する場合：

       ```
       C:\key>c:\Mapp\OSS\apache\bin\openssl genrsa -out server.key 2
       048
       ```

   - OpenSSL3.0.0 以降の場合
     - OpenSSL をインストールした場合：

       ```
       C:\key>c:\openssl\bin\openssl genrsa -out server.key -traditio
       nal 2048
       ```

     - SVP の OpenSSL を使用する場合：

       ```
       C:\key>c:\Mapp\OSS\apache\bin\openssl genrsa -out server.key
       -traditional 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。

C.6 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 をインストールした場合：C:\key>c:\openssl\bin\openssl req -sha256 -new -key server.key -config c:\openssl\bin\openssl.cnf -out server.csr

   SVP の OpenSSL を使用する場合：C:\key>c:\Mapp\OSS\apache\bin\openssl req -sha256 -new -key server.key -config c:\Mapp\OSS\apache\conf\openssl.cnf -out server.csr

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

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。

公開鍵として、server.csr ファイルが C:\key フォルダに作成されます。

⚠ 注意

- セキュリティ上の問題が回避するため、ハッシュアルゴリズムに MD5 や SHA-1 を使用せず、SHA-256 を使用してください。
- SVP の OpenSSL を使用する場合、c:\Mapp\OSS\apache\conf\openssl.cnf の内容を変更しないでください。

2. 対話形式で、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： NEC）。
   - Organization Unit Name (eg, section)[]：例えば部署名を入力します（例：Support Group）。
   - 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 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。入力は任意です（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

```
......++++++
..++++++
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 incorporat
ed 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]:NEC
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 []:
```

C.7 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、SVP 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 -out server.crt
```

SVP の OpenSSL を使用する場合：
```
C:\key>c:\Mapp\OSS\apache\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。

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。

C.8 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。

C.9 SSL 証明書のパスフレーズを解除

パスフレーズが設定された SSL 証明書は、SVP にアップロードできません。SVP に SSL 証明書をアップロードする前に、SSL 証明書のパスフレーズを解除してください。

パスフレーズが設定されているかどうかを確認して、パスフレーズを解除する手順を次に示します。

前提条件

- 秘密鍵（server.key ファイル）が作成済みであること。
- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. コマンドを実行します。

⚠注意

このコマンドを実行すると鍵ファイルが上書きされます。そのため、次のどちらかを実施することを推奨します。

- 事前に鍵ファイルをバックアップする。
- 出力する鍵ファイルのディレクトリを、入力用の鍵ファイルの格納ディレクトリと別にする。

パスフレーズの確認コマンド

OpenSSL をインストールした場合：C:\key>c:\openssl\bin\openssl rsa -in ［鍵ファイル入力先］ -out ［鍵ファイル出力先］

SVP の OpenSSL を使用する場合：C:\key>c:\Mapp\OSS\apache\bin\openssl rsa -in［鍵ファイル入力先］ -out ［鍵ファイル出力先］

［］内：引数

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

パスフレーズが設定されている場合の出力例

パスフレーズ確認コマンドに対して、パスフレーズの入力を要求されます。設定されているパスフレーズを入力し、パスフレーズを解除してください。

```
C:\key>c:\openssl\bin\openssl rsa -in server.key -out server.key
```

Enter pass phrase for server.key:パスフレーズを入力します

Writing RSA key

パスフレーズが設定されていない場合の出力例

パスフレーズ確認コマンドに対して、パスフレーズの入力を要求されなければ、SSL 証明書は、SVP にアップロードできます。

```
C:\key>c:\openssl\bin\openssl rsa -in server.key -out server.key
```

Writing RSA key

3. パスフレーズが解除されていることを確認し、コマンドプロンプトを閉じます。

C.10 SSL 証明書を PKCS#12 形式に変換

作成した秘密鍵と SSL 証明書を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 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 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 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 証明書ファイルを出力します。

前提条件

- 秘密鍵と SSL 証明書を同じフォルダに格納していること。
- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で 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

   SVP の OpenSSL を使用する場合：C:\key>c:\Mapp\OSS\apache\bin\openssl pkcs12 -export -in client.crt -inkey client.key -out client.p12

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

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 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 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 証明書です。
5. コマンドプロンプトを閉じます。

C.11 SVP と管理クライアント間の SSL 通信の署名付き証明書を SVP へアップロード

SVP と管理クライアント間の SSL 通信に任意の証明書を利用するには、秘密鍵と署名付き公開鍵証明書を SVP へアップロードします。証明書更新ツールを使って証明書をアップロードする手順を次に示します。

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される「基本制限(BasicConstraints)」「キー使用法(KeyUsage)」「サブジェクトキー識別子(Subject Key Identifier)」「主体者別名(SubjectAltName)」をサポートしています。

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）と署名付き公開鍵証明書（server.crt ファイル）の形式が「X509PEM 形式」であること。「X509DER 形式」の証明書は使用できません。
- 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で構成された、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 5 階層以下であること
- アップロードする証明書の公開鍵暗号方式は、RSA であること。
- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappApacheCrtUpdate.bat ［証明書ファイルの（絶対パス）］ ［秘密鍵ファイルの（絶対パス）］
   ```

[] 内：引数

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

⚠ 注意

ストレージ管理ソフトウェアを更新した場合、秘密鍵と署名付き公開鍵証明書がデフォルトに戻る場合があります。

デフォルトに戻った場合は、再度、秘密鍵と署名付き公開鍵証明書を SVP へアップロードしてください。

C.12 SVP と管理クライアント間の SSL 通信の証明書をデフォルトに変更

前提条件

すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet

MappApacheCrtInit.bat
```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

C.13 SVP と管理クライアント間の SSL 通信の証明書の確認（Microsoft Edge）

前提条件

- SVP が起動していること。
- Storage Device Launcher がインストールされていること（インストール方法は、『HA Device Manager - Storage Navigator ユーザガイド』を参照）。

操作手順

1. 管理クライアントの Microsoft Edge を起動し、SVP の IP アドレスを入力します。

   https://［SVP の IP アドレス］

   ［Storage Device List］が起動し、［Storage Navigator］画面が表示されます。

   メモ

   SVP で使用する HTTPS サービスのポート番号を初期値［443］から変更している場合、URL として下記を入力します。

   https://［SVP の IP アドレス］:［HTTPS サービスのポート番号］

2. Microsoft Edge の画面内で URL の左側にある［サイト情報の表示］アイコンをクリックし、［接続がセキュリティで保護されています］または［このサイトへの接続は安全ではありません］を選択します。
3. ［接続がセキュリティで保護されています］画面または［このサイトへの接続は安全ではありません］画面の右上にある［証明書を表示する］アイコンをクリックします。

   次の場合は、デフォルトの証明書が使用されています。

   - ［全般］タブに次の表示がある。

     発行先：www.example.com

     発行者：www.example.com

有効期限 : YYYY/MM/DD から YYYY/MM/DD（有効期限は SVP ソフトウェアのバージョンによって変わります）

C.14 SVP と管理クライアント間の SSL 通信の証明書の確認（Google Chrome）

前提条件

SVP が起動していること。

操作手順

1. 管理クライアントの Google Chrome を起動し、SVP の IP アドレスを入力します。

   https://［SVP の IP アドレス］

   ［Storage Device List］画面または［Storage Navigator］画面が表示されます。

   メモ

   SVP で使用する HTTPS サービスのポート番号を初期値［443］から変更している場合、URL として［SVP の IP アドレス］:［HTTPS サービスのポート番号］を入力します。

   https://［SVP の IP アドレス］:［HTTPS サービスのポート番号］

2. Google Chrome の画面内で右クリックして［検証(I)］－［Security］タブを選択します。

   ［Security Overview］が表示されます。

3. ［View Certificate］をクリックします。

   次の場合は、デフォルトの証明書が使用されています。

   - ［全般］タブに次の表示がある。

     発行先：www.example.com

     発行者：www.example.com

     有効期限 : YYYY/MM/DD から YYYY/MM/DD（有効期限は SVP ソフトウェアのバージョンによって変わります）

C.15 SVP 接続用証明書と 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

管理 PC とストレージシステム、および SVP とストレージシステムの SSL 通信に使用する SVP 接続用証明書と 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。

詳細は「3.12.4 証明書ファイルの更新（91 ページ）」を参照してください。

C.16 SVP 接続用証明書を SVP へアップロード

ストレージシステムと SVP 間の SSL 通信に任意の証明書を利用するには、署名付き公開鍵証明書を SVP へアップロードします。

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される「基本制限(BasicConstraints)」「キー使用法(KeyUsage)」「サブジェクトキー識別子(Subject Key Identifier)」をサポートしています。

前提条件

- Maintenance Utility からストレージシステムの秘密鍵と署名付き公開鍵証明書を更新しておくこと。
- 署名付き公開鍵証明書（server.crt ファイル）の形式が「X509PEM 形式」であること。
- 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（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 5 階層以下であること。
- アップロードする証明書の公開鍵暗号方式は、RSA であること。
- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappL7SwitchGumSslCrtUpdate.bat ［証明書ファイルの（絶対パス)］
   ```

   [] 内：引数

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。

4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

C.17 SVP 接続用証明書をデフォルトに変更

前提条件

- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappL7SwitchGumSslCrtInit.bat
   ```

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

C.18 Web サーバ接続用証明書を SVP へアップロード

SVP にインストールされた Storage Navigator をクライアントとして、ストレージシステムのコントローラをサーバとして SSL 通信を行います。SSL 通信を利用するには署名付き公開鍵証明書を SVP へアップロードします。

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される「基本制限(BasicConstraints)」「キー使用法(KeyUsage)」「サブジェクトキー識別子(Subject Key Identifier)」をサポートしています。

アップロードした証明書が機能するか確認する場合は「C.19 SVP へアップロードした Web サーバ接続用証明書の確認（265 ページ）」を実施してください。

前提条件

- Maintenance Utility からストレージシステムの Web サーバ用秘密鍵と署名付き公開鍵証明書を更新しておくこと。
- 秘密鍵（server.key ファイル）と署名付き公開鍵証明書（server.crt ファイル）の形式が「X509PEM 形式」、または「X509DER 形式」であること。
- 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（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 5 階層以下であること。
- アップロードする証明書の公開鍵暗号方式は、RSA であること。
- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappSn2GumSslCrtUpdate.bat ［証明書ファイルの（絶対パス)］
   ```

   [] 内：引数

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。
3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

C.19 SVP へアップロードした Web サーバ接続用証明書の確認

操作手順

1. Storage Navigator にログインします。
2. Storage Navigator メイン画面の［Maintenance Utility］－［ハードウェア］－［その他ハードウェア保守］をクリックします。
3. Maintenance Utility 画面が表示されるか確認してください。

   表示された場合は Web サーバ接続用証明書が機能しています。

   エラーメッセージ［20122 207001（E）］が表示された場合は、SVP とストレージシステムにアップロードした証明書に問題がある可能性があります。以下の操作を行ってください。

   a. 証明書が「付録 C. SSL 通信の設定（245 ページ）」に記載されている条件を満たせているか確認してください。
   b. 満たせない場合は、条件を満たす証明書を作成してください。
   c. 「C.15 SVP 接続用証明書と 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（261 ページ）」を再度実施してください。
   d. 「C.18 Web サーバ接続用証明書を SVP へアップロード（263 ページ） 」を再度実施してください。

   エラーメッセージ［20122 207001（E）］が表示される要因が上記以外の場合は、『Storage Navigator メッセージガイド』を参照してください。

C.20 Web サーバ接続用証明書をデフォルトに変更

前提条件

- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappSn2GumSslCrtInit.bat
   ```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

C.21 SVP への HTTP 通信を拒否

HTTP 通信ポートの外部アクセスをブロックできます。この設定は任意です。

前提条件

- 管理クライアントから SVP にリモートデスクトップ接続を実施済みであること。
- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet

MappHttpBlock.bat
```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

C.22 SVP への HTTP 通信のブロックを解除

HTTP 通信ポートのポートブロックを解除します。この設定は任意です。

前提条件

- 管理クライアントから SVP にリモートデスクトップ接続を実施済みであること。
- すべてのユーザが Storage Navigator をログアウトしていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappHttpRelease.bat
   ```

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

C.23 HSTS を有効化する

HSTS を有効化できます。この設定は任意です。

メモ

HSTS（HTTP Strict Transport Security）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。

⚠ 注意

HSTS を有効にした場合、HTTP で Storage Navigator に接続ができない場合があります。HTTP で接続できない場合は、HTTPS で接続してください。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappHstsEnable.bat
```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 画面に「Press any key to continue…」が表示されます。Enter キーを押してください。
4. HSTS が有効化されたか確認するため、次のコマンドを実行します。

```
MappHstsState.bat
```

「hsts=on」のメッセージが表示され場合、HSTS は有効化されています。Enter キーを押してください。

「hsts=off」のメッセージが表示され場合、HSTS は有効化されていません。Enter キーを押して、操作手順 2.からやり直してください。

「指定されたファイルが見つかりません。」のメッセージが表示され場合、HSTS の設定処理が失敗しています。Enter キーを押して、操作手順 2.からやり直してください。

5. コマンドプロンプトを閉じます。

C.24 HSTS を無効化する

HSTS を無効化します。この設定は任意です。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappHstsDisable.bat
```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 画面に「Press any key to continue…」が表示されます。Enter キーを押してください。
4. HSTS が無効化されたか確認するため、次のコマンドを実行します。

```
MappHstsState.bat
```

「hsts=off」のメッセージが表示され場合、HSTS は無効化されています。Enter キーを押してください。

「hsts=on」のメッセージが表示され場合、HSTS は無効化されていません。Enter キーを押して、操作手順 2.からやり直してください。

「指定されたファイルが見つかりません。」のメッセージが表示され場合、HSTS の設定処理が失敗しています。Enter キーを押して、操作手順 2.からやり直してください。

5. コマンドプロンプトを閉じます。

C.25 セキュリティ警告が表示されたときの対処方法

SSL 通信の設定操作中に、次のような警告が表示されたときの対処方法を示します。

このような警告メッセージが表示された場合は、次の操作をしてください。

＜ Microsoft Edge の場合＞

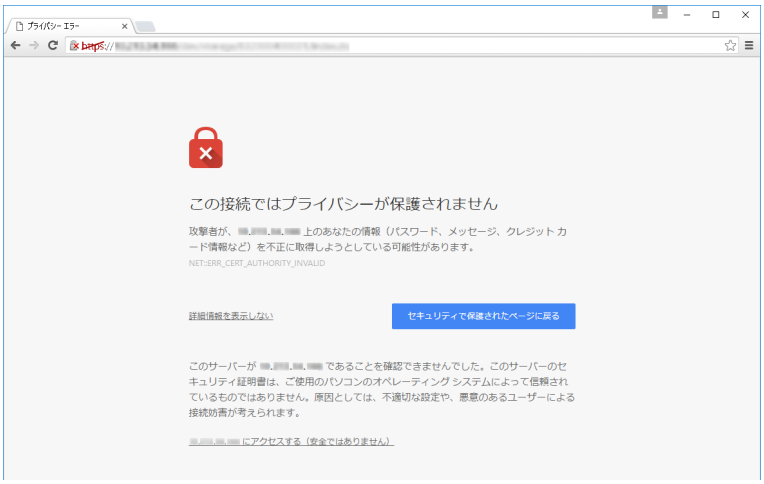
［詳細設定］－［<IP アドレスまたはホスト名>に進む（安全ではありません）］をクリックしてください。

Microsoft Edge の場合の警告表示例（Web ブラウザのバージョンにより表示が異なる場合があります。）

＜ Google Chrome の場合＞

［詳細設定］－［<IP アドレス>にアクセスする（安全ではありません）］をクリックしてください。

Google Chrome の場合の警告表示例（Web ブラウザのバージョンにより表示が異なる場合があります。）



この警告メッセージは、SSL 対応に設定された Storage Navigator に接続したとき、セキュリティ証明書が信頼された証明機関から発行されたものではない場合に表示されます。また、URL に指定した IP アドレスまたはホスト名が、セキュリティ証明書に記載されている CN（Common Name）と一致していない場合にも表示されます。

ストレージ管理ソフトウェア更新後からこの警告メッセージが表示されるようになった場合、SSL 証明書がデフォルトに戻っています。SSL 証明書を確認して、デフォルトに戻っていた場合は、「G.2.1.1 SSL 通信の署名付き証明書について（318 ページ）」を参照して、元の SSL 証明書に差し替えてください。

C.26 RSA 鍵交換の暗号スイート

鍵交換の方式が、RSA 鍵交換の暗号スイートを使用していない場合、RSA 鍵交換の暗号スイートを無効化できます。なお、iStorage V100, V300 の場合、RSA 鍵交換の暗号スイートを無効化する機能は未サポートです。※

注※

画面に表示される転送プロトコルは、モデルやファームウェアバージョンによって異なります。

詳細は「N.1 モデルやファームウェアバージョンによる転送プロトコルの表示の差異（432 ページ）」を参照してください。

操作手順

SVP の設定手順は次の項を参照。

「C.26.1 SVP の RSA 鍵交換の暗号スイートを無効化する（272 ページ）」

「C.26.2 SVP の RSA 鍵交換の暗号スイートを有効化する（273 ページ）」

GUM の設定手順は次の項を参照。

「3.12.3 暗号化スイートの選択（90 ページ）」

⚠ 注意

- RSA 鍵交換の暗号スイートを無効化する場合、または有効化に戻す場合、SVP と GUM の両方に対して、無効化もしくは有効化を設定する必要があります。次に示す操作手順を参照してください。
  - SVP に無効化を設定：「C.26.1 SVP の RSA 鍵交換の暗号スイートを無効化する（272 ページ）」
  - SVP に有効化を設定：「C.26.2 SVP の RSA 鍵交換の暗号スイートを有効化する（273 ページ）」
  - GUM に有効化/無効化を設定：「3.12.3 暗号化スイートの選択（90 ページ）」
- Maintenance Utility で次のどちらかの暗号スイートを指定した場合、GUM の RSA 鍵交換の暗号スイートは、自動で有効化されます。また、どちらの暗号スイートも指定しない場合、GUM の RSA 鍵交換の暗号スイートは、自動で無効化されます。
  - TLS_RSA_WITH_AES_128_CBC_SHA256
  - TLS_RSA_WITH_AES_128_CBC_SHA
- RSA 鍵交換の暗号スイートを無効化した場合、次の暗号スイートを使用できます。
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

管理クライアントや各種サーバが上記の暗号スイートをサポートしていない場合、SVP と管理クライアント、SVP と各種サーバとの通信できなくなるためご注意ください。

- 監査ログを Syslog サーバへ TLS で転送する場合、およびアラート通知を Syslog サーバへ TLS で送付する場合、Syslog サーバ側で次の暗号スイートを使用できるように設定してください。
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- 暗号スイートを無効化した結果、SVP とストレージシステム間の通信ができなくなった場合、ダンプファイルを採取して保守員へ送付してください（「5.11 ダンプファイルの採取方法（163 ページ）」を参照）。その後、暗号スイートを有効化に戻してください（「C.26.2 SVP の RSA 鍵交換の暗号スイートを有効化する（273 ページ）」を参照）。

C.26.1 SVP の RSA 鍵交換の暗号スイートを無効化する

RSA 鍵交換の暗号スイートを無効に設定します。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappRSAKeyExchangeDisable.bat
```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

メモ

- コマンドの実行時間は 5 分程度です。コマンドプロンプトにメッセージが表示されるまで、画面を閉じないでください。
- コマンドの実行により、Storage Device List に登録されているストレージシステムのサービスが再起動されます。再起動は装置アイコンの［Starting Service］が "Auto" の状態のストレージシステムが対象となります。"Manual" の状態のストレージシステムのサービスが起動した状態でコマンドを実行した場合、サービスは停止した状態になります。サービスを開始してください。また、"Auto" の状態のストレージシステムのサービスが停止した状態でコマンドを実行した場合、サービスは開始状態になります。

なお、再起動中に“21041-006005”のメッセージが表示されることがあります。[閉じる]を押してサービスの起動をお待ちください。

3. 画面に「Press any key to continue…」が表示されます。Enter キーを押してください。
4. RSA 鍵交換の暗号スイートが無効化されたか確認します。

```
MappRSAKeyExchangeState.bat
```

「RSAKeyExchangeStatus=Disable」のメッセージが表示された場合、RSA 鍵交換の暗号スイートは無効化されています。Enter キーを押してください。

「RSAKeyExchangeStatus=Enable」のメッセージが表示された場合、RSA 鍵交換の暗号スイートは無効化されていません。Enter キーを押して、操作手順 2.からやり直してください。

5. コマンドプロンプトを閉じます。

⚠ 注意

SVP の RSA 鍵交換の暗号スイートを無効化した場合、必ず GUM の鍵交換の暗号スイートも未使用に設定してください（「3.12.3 暗号化スイートの選択（90 ページ）」で「TLS_RSA_WITH_AES_128_CBC_SHA および TLS_RSA_WITH_AES_128_CBC_SHA256 を無効にする」を選択）。

C.26.2 SVP の RSA 鍵交換の暗号スイートを有効化する

RSA 鍵交換の暗号スイートを有効に設定します。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappRSAKeyExchangeEnable.bat
```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

メモ

- コマンドの実行時間は 5 分程度です。コマンドプロンプトにメッセージが表示されるまで、画面を閉じないでください。
- コマンドの実行により、Storage Device List に登録されているストレージシステムのサービスが再起動されます。再起動は装置アイコンの［Starting Service］が "Auto" の状態のストレージシステムが対象となります。"Manual" の状態のストレージシステムのサービスが起動した状態でコマンドを実行した場合、サービスは停止した状態になります。サービスを開始してください。また、"Auto" の状態のストレージシステムのサービスが停止した状態でコマンドを実行した場合、サービスは開始状態になります。

  なお、再起動中に“21041-006005”のメッセージが表示されることがあります。［閉じる］を押してサービスの起動をお待ちください。

3. 画面に「Press any key to continue…」が表示されます。Enter キーを押してください。
4. RSA 鍵交換の暗号スイートが有効化されたか確認します。

   ```
   MappRSAKeyExchangeState.bat
   ```

   「RSAKeyExchangeStatus=Enable」のメッセージが表示された場合、RSA 鍵交換の暗号スイートは有効化されています。Enter キーを押してください。

   「RSAKeyExchangeStatus=Disable」のメッセージが表示された場合、RSA 鍵交換の暗号スイートは有効化されていません。Enter キーを押して、操作手順 2.からやり直してください。
5. コマンドプロンプトを閉じます。

⚠ 注意

SVP の RSA 鍵交換の暗号スイートを有効化した場合、必ず GUM の鍵交換の暗号スイートも選択してください（「3.12.3 暗号化スイートの選択（90 ページ）」で「TLS_RSA_WITH_AES_128_CBC_SHA256」または「TLS_RSA_WITH_AES_128_CBC_SHA」のどちらかを選択）。

C.27 DHE 鍵の下限長の設定

暗号化スイートで使用する DHE 鍵の下限長（デフォルトは 1024 ビット）を変更します。

前提条件

- iStorage V10e の Storage Device List が必要です。

  iStorage V100, V300 の Storage Device List はサポートしていません。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   なお、現在の設定値を確認したい場合は、コマンドを実行せずに、操作手順 4. に進んでください。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

   DHE 鍵の下限長を 1024 ビットから 2048 ビットに変更する場合

   ```
   MappSetDheMin2048.bat
   ```

   DHE 鍵の下限長を 2048 ビットから 1024 ビットに変更する場合

   ```
   MappSetDheMin1024.bat
   ```

3. コマンドが正常に終了すると、コマンドプロンプトに次のメッセージが表示されます。

   ```
   RESULT: SUCCESS
   The setting is applied successfully.
   To make this setting effective, restart SVP.
   ```

   メモ

   コマンドプロンプトにメッセージが表示されるまで、画面を閉じないでください。

4. DHE 鍵の下限長が変更されたことを確認します。

   ```
   MappDheMinStatus.bat
   ```

   - 1024 ビットから 2048 ビットに変更された場合：「DHE Minimum Key Length = 2048 bits」と表示されます。
   - 2048 ビットから 1024 ビットに変更された場合：「DHE Minimum Key Length = 1024 bits」と表示されます。

   メモ

   変更されていない場合、または「DHE Minimum Key Length = Unknown」と表示された場合は、Enter キーを押して、操作手順 2.からやり直してください。

5. Enter キーを押してください。
6. コマンドプロンプトを閉じます。
7. DHE 鍵の下限長を変更した場合は、SVP を再起動してください（「G.1.3 SVP を再起動する（315 ページ）」参照）。

付録 D.　SVP による外部認証サーバとの連携

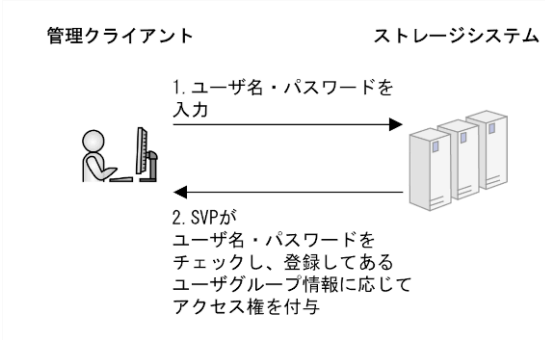
SVP を外部認証サーバと連携させるための設定方法について説明します。

D.1　外部サーバとの連携設定の手順

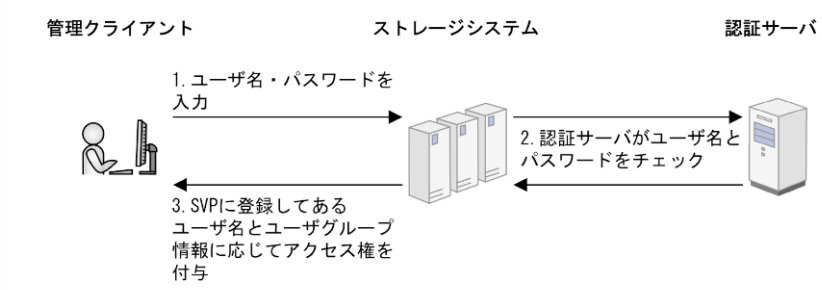
ユーザ認証を行う認証サーバと、ユーザ名に応じてユーザグループを通知する認可サーバに接続するための設定をします。

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。

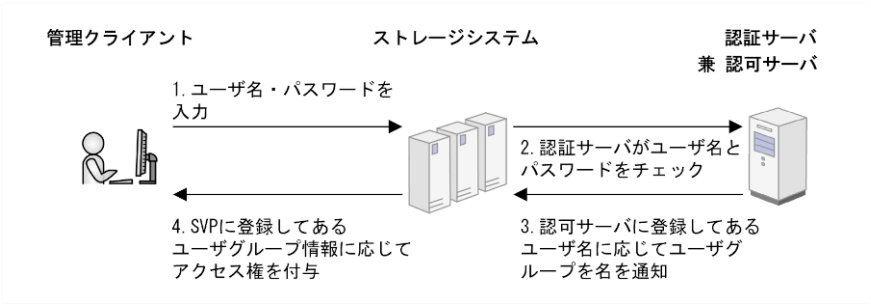


認証サーバを使用する場合のユーザ認証の流れを次の図に示します。



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。

認証サーバと認可サーバを併用する場合のユーザ認証の流れを次の図に示します。



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。

SVP の外部認証機能は、Storage Device List に登録されているすべてのストレージシステムに対して同時に機能します。このため Storage Device List に登録されているストレージシステムを個別に、SVP の外部認証と Maintenance Utility の外部認証を切り替えることはできません。

構成と使用する認証サーバによって、外部認証の設定手段が異なります。

構成	認証サーバ	Maintenance Utility	SVP の外部認証設定
SVP を使用する管理モデル	LDAP	×※	○
	Kerberos	×	○
	RADIUS	×	○
SVP を使用しない管理モデル	LDAP	○	×
	Kerberos	×	×
	RADIUS	×	×

凡例

○：設定可能、×：設定不可

注※

SVP を使用する管理モデルでは、運用上の制約として Maintenance Utility で設定しないでください。

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。
- ストレージシステムの管理を、SVP を使用しない管理モデルから、SVP を使用する管理モデルへ変更する場合は、Maintenance Utility の外部認証機能を無効にしたのちに、当該のストレージシステムを SVP の Storage Device List へ登録してください（無効にする方法は「3.8.3 無効化（83 ページ）」を参照）。

- ストレージシステムの管理を、SVP を使用する管理モデルから、SVP を使用しない管理モデルへ変更する場合は、SVP の Storage Device List からストレージシステムを削除したのちに、Maintenance Utility の外部認証機能を設定してください（設定方法は「3.8.2 LDAP の設定 (82 ページ)」を参照）。
- 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。
- SVP と外部認証サーバの間にロードバランサは構築できません。
- ユーザアカウントを Storage Navigator 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、「3.2.4 ユーザグループ (36 ページ)」を参照してください。ユーザアカウントを Storage Navigator 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 Storage Navigator 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。

D.1.1 認証サーバの要件

使用する認証サーバが、次の条件を満たしていることを確認してください。

- 認証サーバのプロトコル
- LDAP サーバの設定に使用できる証明書ファイルの形式
- Kerberos サーバの暗号タイプ
- 接続できる認証サーバ
- サーバ検索
- 暗号通信

D.1.1.1 認証サーバのプロトコル

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。サポートされている認証形式は次のとおりです。

LDAP の場合

- LDAPv3 Simple bind 認証

RADIUS の場合

- RFC2865 準拠 RADIUS
  - PAP 認証

- CHAP 認証

Kerberos の場合

- Kerberos v5

D.1.1.2 LDAP サーバの設定に使用できる証明書ファイルの形式

LDAP サーバの設定に使用できる証明書ファイルの形式は次のとおりです。

- X509 DER 形式※
- X509 PEM 形式※

注※

X.509 証明書の拡張プロファイルのフィールドは、RFC5280 に規定される、次のフィールドがサポートされます。

- 基本制限 (BasicConstraints)
- キー使用法(KeyUsage)
- サブジェクトキー識別子(Subject Key Identifier)

また、iStorage V100, V300 のファームウェアバージョン 93-06-23-XX/XX 以降、および iStorage V10e では、次のフィールドもサポートされます。

- 機関キー識別子(Authority Key Identifier)
- 証明書ポリシー(Certificate Policies)
- サブジェクト代替名(Subject Alternative Name)
- 名前の制限(Name Constraints)
- ポリシーの制限(Policy Constraints)
- 拡張キー使用法(Extended Key Usage)
- ポリシー禁止(Inhibit anyPolicy)

上記以外のフィールドを使用しないでください。

D.1.1.3 Kerberos サーバの暗号タイプ

Kerberos サーバでは、次のどれかの暗号タイプを使用できるようにしてください。

Windows の場合

- AES128-CTS-HMAC-SHA1-96
- RC4-HMAC

- DES3-CBC-SHA1

D.1.1.4 接続できる認証サーバ

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。

D.1.1.5 サーバ検索

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

D.1.1.6 暗号通信

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を行ったうえ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。

D.1.2 認証サーバに接続するための設定をする

認証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。

設定を行ったにもかかわらず、認証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可能性があります。サーバの管理者およびネットワークの管理者に問い合わせてください。

設定完了後、認証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。

前提条件

- 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問い合わせてください。

操作手順

1. コンフィグファイルを作成します。使用するプロトコルによって設定する項目が異なります（「D.1.3 コンフィグファイルの作成（283 ページ）」参照）。
2. SVP へログインし、次のファイルを参照可能な場所に格納します。
   - 証明書（セキュアな通信を行う場合）
   - コンフィグファイル
3. SVP で 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ツールが存在するディレクトリに移動し、次に示すコマンドにコンフィグファイルパス（例 C:\auth\auth.properties）と証明書ファイルパス（例 C:\auth\auth.cer）を指定して実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappSetExAuthConf "C:\auth\auth.properties" "C:\auth\auth.cer"
   ```

   ヒント

   - C:\Mapp : ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

     「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。
   - 指定した証明書ファイルは、副サーバに対しても使用されます。

5. 認証サーバが使用できることを確認したのち、認証サーバへの接続設定をバックアップします（バックアップの詳細は「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」参照）。
6. 操作手順 4. で指定したファイルを削除するためのメッセージが表示されます。

   ```
   Do you want to delete files("C:\auth\auth.properties" "C:\auth\auth.cer")?
   ```

   削除する場合は“y”を指定してください。

   “n”を指定すると、ファイルは削除されません。

   手動で削除してください。

D.1.3 コンフィグファイルの作成

使用する認証サーバのプロトコルにあわせて、コンフィグファイルを作成します。コンフィグファイルは、認証サーバへの接続設定時に必要です（「D.1.2 認証サーバに接続するための設定をする（281 ページ）」参照）。

D.1.3.1 LDAP 用コンフィグファイルの作成

認証サーバとして LDAP サーバを使用するには、テキストエディタでコンフィグファイルを作成し、認証サーバの情報を次の形式で定義します。ファイル名および拡張子は任意です。

メモ

コンフィグファイルは、UTF-8 エンコーディングで保存してください。

形式

```
#コメント
auth.server.type=ldap
auth.server.name=<サーバ識別名>
auth.group.mapping=<値>
auth.ldap.<サーバ識別名>.<属性>=<値>
```

例

```
auth.server.type=ldap
auth.server.name=PrimaryServer
auth.group.mapping=true
auth.ldap.PrimaryServer.protocol=ldaps
auth.ldap.PrimaryServer.host=ldaphost.domain.local
auth.ldap.PrimaryServer.port=636
auth.ldap.PrimaryServer.timeout=3
auth.ldap.PrimaryServer.attr=sAMAccountName
auth.ldap.PrimaryServer.searchdn=CN=sample1,CN=Users,DC=domain,DC=local
auth.ldap.PrimaryServer.searchpw=password
auth.ldap.PrimaryServer.basedn=CN=Users,DC=domain,DC=local
auth.ldap.PrimaryServer.retry.interval=1
auth.ldap.PrimaryServer.retry.times=3
auth.ldap.PrimaryServer.domain.name=EXAMPLE.COM
```

表 D-1 LDAP 用設定項目

属性	説明	省略可否	デフォルト値
auth.server.type	認証サーバの種別。ldap を指定してください。	必須	なし
auth.server.name	認証サーバの識別名。正・副 2 台の認証サーバを登録する場合は、コンマ（,）で区切ってください。正・副あわせて 64 バイト以下で指定します。 次の記号を除く ASCII コードを使用できます。 \ / : , ; * ? " < > | $ % & ' ~	必須	なし

属性	説明	省略可否	デフォルト値
	これより以下の項目では、ここで設定した値を<サーバ識別名>と言います。		
auth.group.mapping	認可サーバと連携するかどうかを設定します。 • true：連携する • false：連携しない	省略可	false
auth.ldap.<サーバ識別名>.protocol	使用する LDAP プロトコル。 ldaps（LDAP over SSL/TLS を用いた認証）を指定してください。 starttls（StartTLS を用いた認証）は指定できません。	必須	なし
auth.ldap.<サーバ識別名>.host	LDAP サーバのホスト名、IPv4 アドレス、または IPv6 アドレス。 IPv6 アドレスは[]で囲んで指定してください。 IPv6 アドレスとして、次の IP ドレスは指定できません。 • 無効値： [::] • ループバックアドレス： [::1] • マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF] • IPv4 射影アドレス： [::FFFF:(IPv4)] • リンクローカルアドレス： [FE80::] • グローバルユニキャストアドレス： [2001::] • グローバルユニキャストアドレス： [2002::] プロトコルとして StartTLS を使用する場合、ホスト名を指定します。 この値を設定した場合、 auth.ldap.<サーバ識別名>.dns_lookup の設定は無視されます。	auth.ldap.<サーバ識別名>.dns_lookup に true を指定した場合は省略可	なし
auth.ldap.<サーバ識別名>.port	LDAP サーバのポート番号。1～65535 の範囲で指定します。範囲外の値が指定された場合はデフォルト値を使用します。	省略可	389
auth.ldap.<サーバ識別名>.timeout	LDAP サーバとの接続タイムアウトを検出するまでの時間。1～30 の範囲で指定します。単位は秒です。	省略可	10
auth.ldap.<サーバ識別名>.attr	ユーザを確定する属性名（ユーザ ID など）。 • 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 • フラットモデルの場合 ユーザエントリの RDN の属性名 Active Directory では sAMAccountName が使用されます。	必須	なし
auth.ldap.<サーバ識別名>.searchdn	検索用ユーザの DN。省略した場合、[attr 値]=[ログイン ID],[basedn 値]で表される DN にバインド認証を行います。※	必須	なし
auth.ldap.<サーバ識別名>.searchpw	検索用ユーザのパスワード。LDAP サーバに登録しているパスワードと同じ値を指定してください。	必須	なし
auth.ldap.<サーバ識別名>.basedn	認証するユーザを検索する際に基点となる DN（BaseDN）※。 • 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	必須	なし

属性	説明	省略可否	デフォルト値
	• 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		
auth.ldap.<サーバ識別名>.retry.interval	LDAP サーバの通信に失敗した場合のリトライ間隔。 1～5 の範囲で指定します。単位は秒です。	省略可	1
auth.ldap.<サーバ識別名>.retry.times	LDAP サーバの通信に失敗した場合のリトライ回数。 0～3 の範囲で指定します。0 を指定するとリトライしません。	省略可	3
auth.ldap.<サーバ識別名>.domain.name	LDAP サーバが管理するドメインの名称。	必須	なし
auth.ldap.<サーバ識別名>.dns_lookup	DNS サーバの SRV レコードに登録してある情報を使用して LDAP サーバを検索するかどうかを設定します。 false（ホスト名やポート番号で検索）を指定してください。 true（DNS サーバの SRV レコードに登録してある情報で検索）は指定できません。	省略可	false

注※

属性値に記号（+ ; , < = >など）を入力する場合、記号の前に円記号（\）を入力してしてください。記号を複数入力する場合、1 文字ごとに円記号（\）を入力してください。

例えば、searchdn に指定した値が「abc++」の場合は、次のように入力して「+」を入力してください。

abc\+\+

ただし、\、/、または"を入力するときは、円記号（\）のあとにそれぞれの記号の ASCII コードを 16 進数で入力してください。

- 「\」は、「\5c」と入力します。
- 「/」は、「\2f」と入力します。
- 「"」は、「\22」と入力します。

例えば、searchdn に指定した値が「abc\」の場合は、次のように入力してください。

abc\5c

D.1.3.2 RADIUS 用コンフィグファイルの作成

認証サーバとして RADIUS サーバを使用するには、テキストエディタでコンフィグファイルを作成し、認証サーバの情報を次の形式で定義します。ファイル名および拡張子は任意です。

メモ

コンフィグファイルは、UTF-8 エンコーディングで記述してください。

形式

```
#コメント
auth.server.type=radius
auth.server.name=<サーバ識別名>
auth.group.mapping=<値>
auth.radius.<サーバ識別名>.<属性>=<値>
auth.group.<ドメイン名>.<属性>=<値>
```

例

```
auth.server.type=radius
auth.server.name=PrimaryServer
auth.group.mapping=true
auth.radius.PrimaryServer.protocol=PAP
auth.radius.PrimaryServer.host=example.com
auth.radius.PrimaryServer.port=1812
auth.radius.PrimaryServer.timeout=3
auth.radius.PrimaryServer.secret=secretword
auth.radius.PrimaryServer.retry.times=3
auth.radius.PrimaryServer.domain.name=radius.example.com
auth.group.radius.example.com.protocol=ldaps
auth.group.radius.example.com.host=xxx.xxx.xxx.xxx
auth.group.radius.example.com.port=636
auth.group.radius.example.com.searchdn=CN=sample1,CN=Users,DC=domain,DC=loc
al
auth.group.radius.example.com.searchpw=password
auth.group.radius.example.com.basedn=CN=Users,DC=domain,DC=local
```

表 D-2　RADIUS 用設定項目（認証サーバ分）

属性	説明	省略可否	デフォルト値
auth.server.type	認証サーバの種別。radius を指定してください。	必須	なし
auth.server.name	サーバの識別名。正・副 2 台の認証サーバを登録する場合は、コンマ（,）で区切ってください。正・副あわせて 64 バイト以下で指定します。 次の記号を除く ASCII コードを使用できます。 \ / : , ; * ? " < > | $ % & ' ~ これより以下の項目では、ここで設定した値を<サーバ識別名>と言います。	必須	なし
auth.group.mapping	認可サーバと連携するかどうかを設定します。 • true：連携する • false：連携しない	省略可	false
auth.radius.<サーバ識別名>.protocol	使用する RADIUS プロトコル。 • PAP：ユーザ ID とパスワードを平文で送る方式 • CHAP：パスワードを暗号化して送る方式	必須	なし
auth.radius.<サーバ識別名>.host	RADIUS サーバのホスト名、IPv4 アドレス、または IPv6 アドレス。 IPv6 アドレスは[]で囲んで指定してください。 IPv6 アドレスとして、次の IP ドレスは指定できません。	必須※1	なし

属性	説明	省略可否	デフォルト値
	• 無効値： [::] • ループバックアドレス： [::1] • マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF] • IPv4 射影アドレス： [::FFFF:(IPv4)] • リンクローカルアドレス： [FE80::] • グローバルユニキャストアドレス： [2001::] • グローバルユニキャストアドレス： [2002::]		
auth.radius.<サーバ識別名>.port	RADIUS サーバのポート番号。1～65535 の範囲で指定します。	省略可※2	1812
auth.radius.<サーバ識別名>.timeout	RADIUS サーバとの接続タイムアウトを検出するまでの時間。1～30 の範囲で指定します。単位は秒です。	省略可※2	10
auth.radius.<サーバ識別名>.secret	PAP または CHAP 認証で使用する RADIUS シークレット（共有鍵）。	必須	なし
auth.radius.<サーバ識別名>.retry.times	RADIUS サーバの通信に失敗した場合のリトライ回数。0～3 の範囲で指定します。0 を指定するとリトライしません。	省略可※2	3

注※1

外部認可で DNS 照会する場合、設定が不要になります。

注※2

指定可能な値以外を指定した場合は、デフォルト値が設定されます。

表 D-3　RADIUS 用設定項目（認可サーバ分）

属性	説明	省略可否	デフォルト値
auth.radius.<サーバ識別名>.domain.name	LDAP サーバが管理するドメインの名称を指定します。 これより以下の項目では、ここで設定した値を<ドメイン名>といいます。	外部認可サーバ連携時必須	なし
auth.radius.<サーバ識別名>.dns_lookup	LDAP ディレクトリサーバの情報を DNS サーバに照会するかどうかを設定します。 false（ホスト名やポート番号で検索）を指定してください。 true（DNS サーバの SRV レコードに登録してある情報で検索）は指定できません。	省略可	false
auth.group.<ドメイン名>.protocol	LDAP ディレクトリサーバ接続のプロトコルです。 ldaps（LDAP over SSL/TLS を用いた認証）を指定してください。 starttls（StartTLS を用いた認証）は指定できません。	必須	なし
auth.group.<ドメイン名>.host	LDAP ディレクトリサーバのホスト名または IP アドレスを指定します。 ホスト名を指定する場合、IP アドレスへの名前解決ができることを事前に確認してください。 IPv6 アドレスは[]で囲んで指定してください。 IPv6 アドレスとして、次の IP ドレスは指定できません。	省略可※1	なし

属性	説明	省略可否	デフォルト値
	• 無効値： [::] • ループバックアドレス： [::1] • マルチキャストアドレス： [FF00:: ～ FDFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF] • IPv4 射影アドレス： [::FFFF:(IPv4)] • リンクローカルアドレス： [FE80::] • グローバルユニキャストアドレス： [2001::] • グローバルユニキャストアドレス： [2002::]		
auth.group.<ドメイン名>.port	LDAP ディレクトリサーバのポート番号です。1～65535 の範囲で指定します。	省略可※2	389
auth.group.<ドメイン名>.searchdn	LDAP ディレクトリサーバとの認証に必要な検索ユーザ DN を指定します。	必須	なし
auth.group.<ドメイン名>.searchpw	LDAP ディレクトリサーバとの認証に必要な検索ユーザのパスワードを指定します。	必須	なし
auth.group.<ドメイン名>.basedn	LDAP ディレクトリサーバの情報を検索する際に、起点となるエントリーの DN（BaseDN）。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。 例えば、次の文字が DN に含まれる場合は，1 文字ごとに円記号（\）でエスケープする必要があります。 空白文字 # + ; , < = > \ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため、BaseDN にエスケープが必要な文字が含まれる場合は、正しくエスケープしてください。 省略した場合は、Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。	省略可	abbr
auth.group.<ドメイン名>.timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間を設定します。0～30 の範囲で指定します。	省略可※2	10
auth.radius.<ドメイン名>.retry.interval	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となる秒数を設定します。1～5 の範囲で指定します。	省略可※2	1
auth.radius.<ドメイン名>.retry.times	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設定します。0～3 の範囲で指定します。	省略可※2	3

注※1

「auth.radius.<サーバ識別名>.dns_lookup」に「true」を指定した場合に省略できます。

注※2

指定可能な値以外を指定した場合は、デフォルト値が設定されます。

D.1.3.3 Kerberos 用コンフィグファイルの作成

認証サーバとして Kerberos サーバを使用するには、テキストエディタでコンフィグファイルを作成し、認証サーバの情報を次の形式で定義します。ファイル名および拡張子は任意です。

メモ

コンフィグファイルは、UTF-8 エンコーディングで記述してください。

形式

```
#コメント
auth.server.type=kerberos
auth.group.mapping=<値>
auth.kerberos.<属性>=<値>
auth.group.<レルム名>.<属性>=<値>
```

例

```
auth.server.type=kerberos
auth.group.mapping=true
auth.kerberos.default_realm=example.com
auth.kerberos.dns_lookup_kdc=true
auth.kerberos.clockskew=300
auth.kerberos.timeout=10
auth.group.example.com.protocol=ldaps
auth.group.example.com.port=636
auth.group.example.com.searchdn=CN=sample1,CN=Users,DC=domain,DC=local
auth.group.example.com.searchpw=password
auth.group.example.com.basedn=CN=Users,DC=domain,DC=local
```

表 D-4　Kerberos 用設定項目（認証サーバ分）

属性	説明	省略可否	デフォルト値
auth.server.type	認証サーバの種別。kerberos を指定してください。	必須	なし
auth.group.mapping	認可サーバと連携するかどうかを設定します。 • true：連携する • false：連携しない	省略可	false
auth.kerberos.default_realm	デフォルトのレルム名。	必須	なし
auth.kerberos.dns_lookup_kdc	DNS サーバの SRV レコードに登録してある情報を使用して Kerberos サーバを検索するかどうかを設定します。 false（ホスト名やポート番号で検索）を指定してください。 true（DNS サーバの SRV レコードに登録してある情報で検索）は指定できません。	省略可	false
auth.kerberos.clockskew	SVP と Kerberos サーバ間の時刻差の許容範囲。0～300 の範囲で指定します。	省略可※1	300
auth.kerberos.timeout	Kerberos サーバとの接続タイムアウトを検出するまでの時間。1～30 の範囲で指定します。単位は秒です。	省略可※1	10
auth.kerberos.realm_name	レルム識別名。レルムごとに Kerberos サーバの情報を区別するための任意の名称。重複登録はできません。複数登録する場合は、コンマ（,）で区切ってください。	省略可※2	なし

属性	説明	省略可否	デフォルト値
	これより以下の項目では、ここで設定した値を<レルム識別名>と言います。		
auth.kerberos.<レルム識別名>.realm	Kerberos サーバに設定してあるレルム名	省略可※2	なし
auth.kerberos.<レルム識別名>.kdc	Kerberos サーバのホスト名または IPv4 アドレス、およびポート番号。 「<ホスト名または IP アドレス>[:ポート番号]」の形式で指定してください。	省略可※2	なし

注※1

指定可能な値以外を指定した場合は、デフォルト値が設定されます。

注※2

「auth.kerberos.dns_lookup_kdc」で「true」を指定した場合に省略できます。

表 D-5 Kerberos 用設定項目（認可サーバ分）

属性	説明	省略可否	デフォルト値
auth.group.<レルム識別名>.protocol	LDAP ディレクトリサーバ接続のプロトコルです。 ldaps（LDAP over SSL/TLS を用いた認証）を指定してください。 starttls（StartTLS を用いた認証）は指定できません。	必須	なし
auth.group.<レルム識別名>.port	LDAP ディレクトリサーバのポート番号です。1～65535 の範囲で指定します。	省略可※1	389
auth.group.<レルム識別名>.searchdn	LDAP ディレクトリサーバとの認証に必要な検索ユーザ DN を指定します。 DN は RFC4514 の規約に従って指定してください。例えば、次の文字が DN に含まれる場合は、1 文字ごとに円記号（\）でエスケープする必要があります。 空白文字 # + ; , < = > \ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため，BaseDN にエスケープが必要な文字が含まれる場合は，正しくエスケープしてください。	必須	なし
auth.group.<レルム識別名>.searchpw	LDAP ディレクトリサーバとの認証に必要な検索ユーザのパスワードを指定します。	必須	なし
auth.group.<レルム識別名>. timeout	LDAP ディレクトリサーバと接続するときの接続待ち時間を設定します。0～30 の範囲で指定します。	省略可※1	10
auth.group.<レルム識別名>.retry.interval	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となる秒数を設定します。1～5 の範囲で指定します。	省略可※1	1
uth.group.<レルム識別名>.retry.times	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設定します。0～3 の範囲で指定します。	省略可※1	3
auth.group.<外部認可サーバ>>.basedn	LDAP ディレクトリサーバの情報を検索する際に，起点となるエントリーの DN（BaseDN）。この DN より下の階層のユーザーエントリーが認可の対象となります。検索対象のユーザーエントリーをすべて含む階層の DN を指定してください。	省略可※1	abbr

属性	説明	省略可否	デフォルト値
	DN は RFC4514 の規約に従って指定してください。例えば，次の文字が DN に含まれる場合は，1 文字ごとに円記号（\）でエスケープする必要があります。 空白文字 # + ; , < = > \ 指定した値は LDAP ディレクトリサーバにそのまま渡されるため，BaseDN にエスケープが必要な文字が含まれる場合は，正しくエスケープしてください。 省略した場合は，Active Directory の defaultNamingContext 属性に指定されている値が BaseDN と見なされます。		

注※1

指定可能な値以外を指定した場合は、デフォルト値が設定されます。

付録 E.　ドライブ管理

スペアドライブの割り当てと解除や、パリティグループ、LDEV の作成などを、Storage Navigator から行う方法を説明します。

DP（Dynamic Provisioning）プールの作成方法は、『システム構築ガイド』を参照してください。

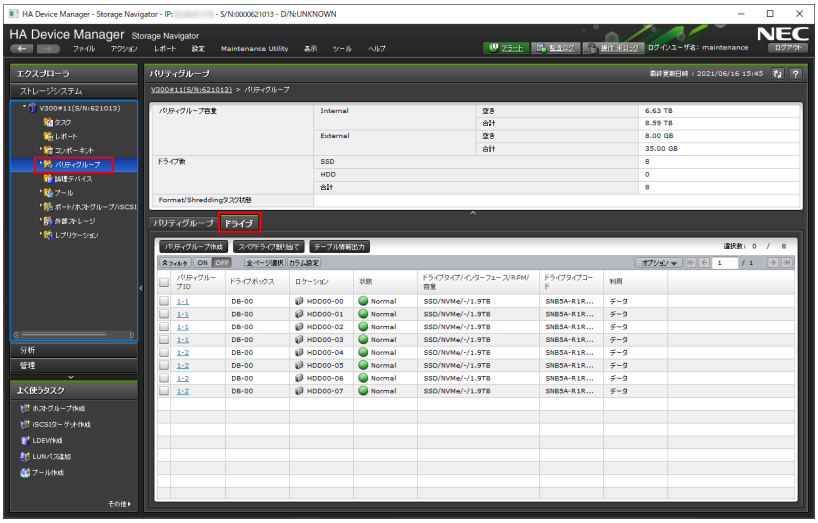
E.1　ドライブ管理（Storage Navigator 編）

Storage Navigator からスペアドライブの割り当てや、パリティグループ、LDEV の作成、LUN パスの割り当てをする手順を説明します。また、タスクの状態を確認する方法も説明します。

E.1.1　スペアドライブの割り当てと削除

操作手順

1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［パリティグループ］を選択し、表示します。
2. ［ドライブ］タブをクリックします。



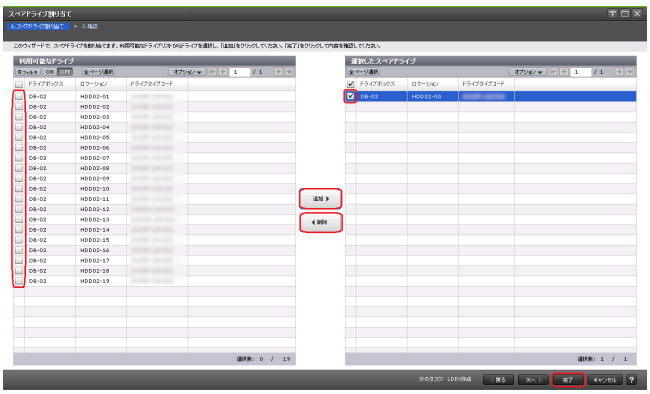
3. ［スペアドライブ割当て］をクリックします。
4. ［スペアドライブ割り当て］画面が表示されます。
   - 割り当てる場合：

     ［利用可能なドライブ］リストからドライブを選択し、［追加］をクリックします。［選択したスペアドライブ］に追加されます。［完了］をクリックします。

   - 削除する場合：

［選択したスペアドライブ］リストからドライブを選択し、［削除］をクリックします。［利用可能なドライブ］に追加されます。［完了］をクリックします。

削除されたスペアドライブはストレージシステムで空き領域として使えるようになります。

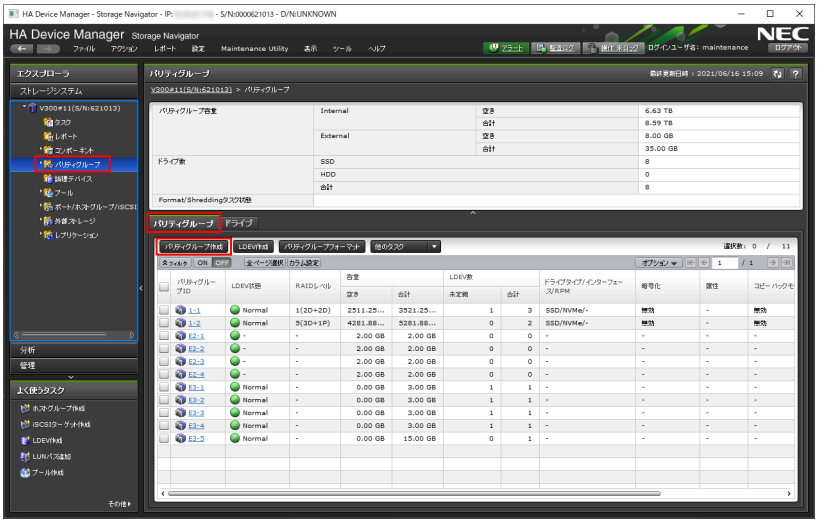


5. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

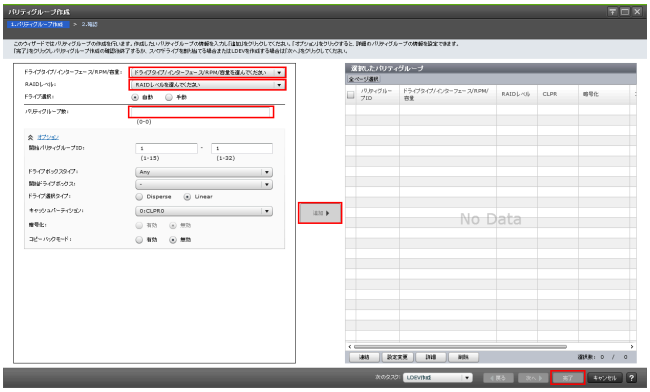
E.1.2 パリティグループの作成

操作手順

1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［パリティグループ］を選択します。
2. ［パリティグループ］タブの［パリティグループ作成］をクリックします。



3. ［ドライブタイプ/インターフェース/RPM/容量］と［RAID レベル］と［パリティグループ数］で作成したいパリティグループ数を入力し［追加］をクリックします。［完了］をクリックします。



4. 確認画面が表示されます。内容を確認し、タスク名を指定後、[適用]をクリックします。

E.1.3 パリティグループの削除

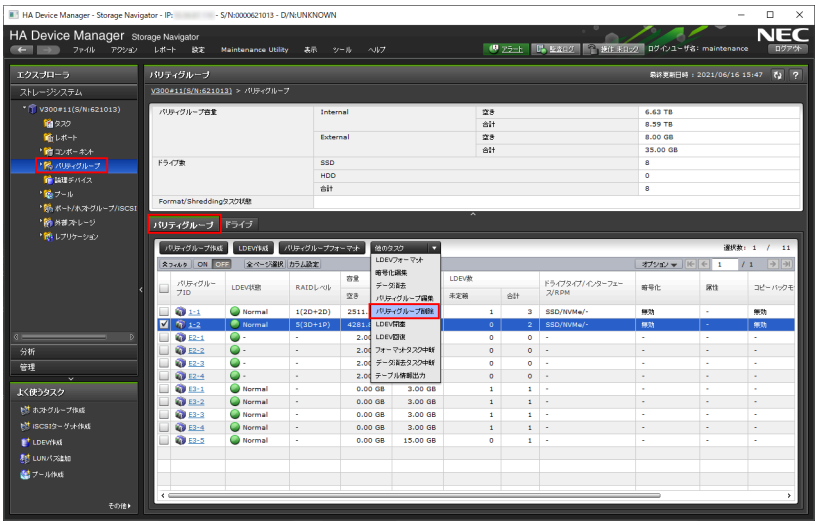
指定したパリティグループ内に論理デバイスが定義されている場合でもパリティグループの削除ができます。

⚠注意

この操作を実行すると論理デバイスが削除されるため、ユーザデータを消失します。必要に応じてユーザデータをバックアップしてから作業を進めてください。

操作手順

1. Storage Navigator メイン画面の[ストレージシステム]ツリーから[パリティグループ]を選択します。
2. [パリティグループ]タブをクリックします。
3. 削除するパリティグループをチェックし、[他のタスク]－[パリティグループ削除]を選択します。

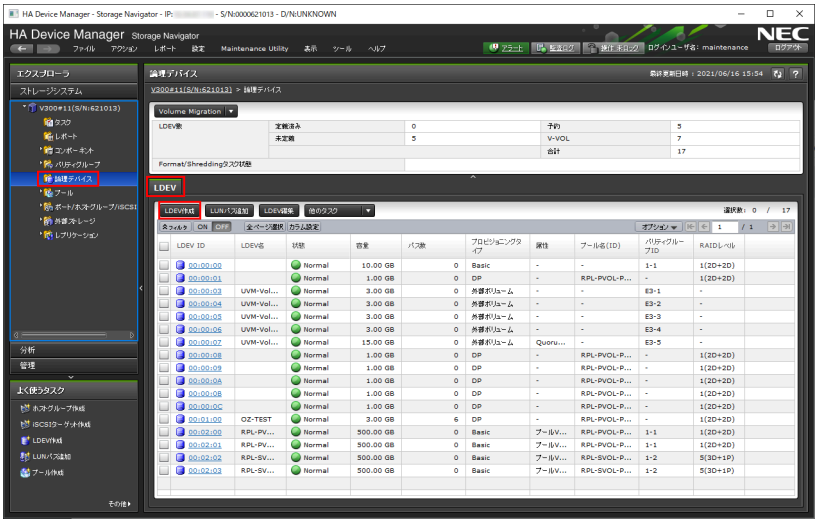


4. 確認画面が表示されます。内容を確認し、タスク名を指定後、[適用]をクリックします。

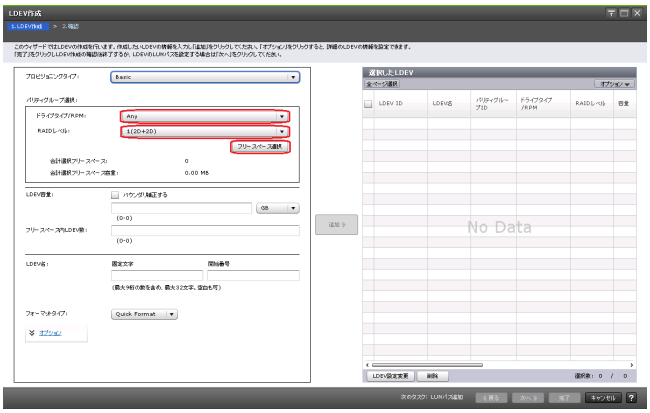
E.1.4 LDEV の作成

操作手順

1. Storage Navigator メイン画面の[ストレージシステム]ツリーから[論理デバイス]を選択します。
2. [LDEV]タブの[LDEV 作成]をクリックします。



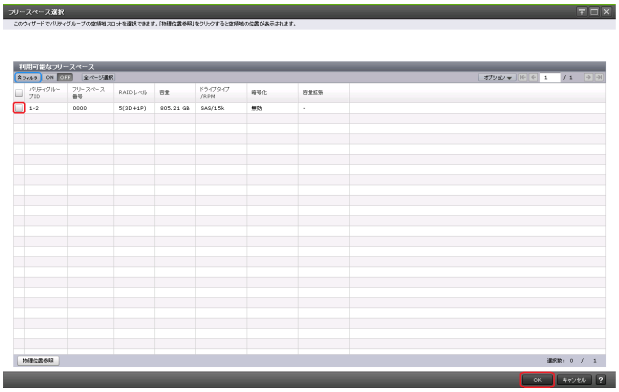
3. [ドライブタイプ/インターフェース/RPM/容量]と[RAID レベル]を選択して[フリースペース選択]をクリックします。



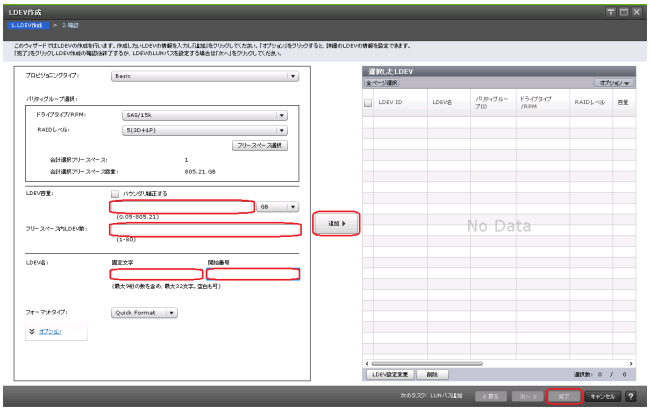
ヒント

[オプション]をクリックすると、LDEV の詳細情報を設定できます。

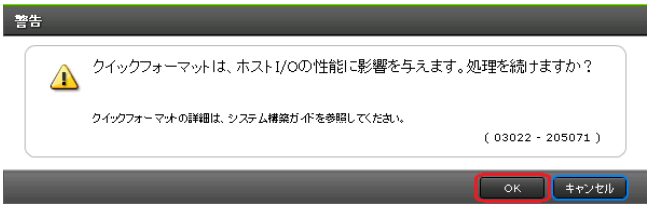
4. [利用可能なフリースペース]から LDEV を作成するパリティグループを選択して[OK]をクリックします。



5. ［LDEV 容量］、［フリースペース内 LDEV 数］、［LDEV 名］の［固定文字］、および［LDEV 名］の［開始番号］を入力して［追加］をクリックします。［選択した LDEV］を確認して［次へ］をクリックします。なお、入力した［開始番号］が使用済の場合は、入力した番号以降で使用可能な番号が小さい順に割り当てられます。



6. クイックフォーマットに関する警告メッセージが表示されます。［OK］をクリックします。



7. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

メモ

ここで［次へ］を選択して LUN パスを設定した場合、作成した LDEV を使ってプールを作成できなくなります。

プールを作成する場合、『システム構築ガイド』の「Dynamic Provisioning のプールを作成する（プールボリュームを自動で選択する場合）」を参照してください。

E.1.5 LDEV を LUN パスに割り当て

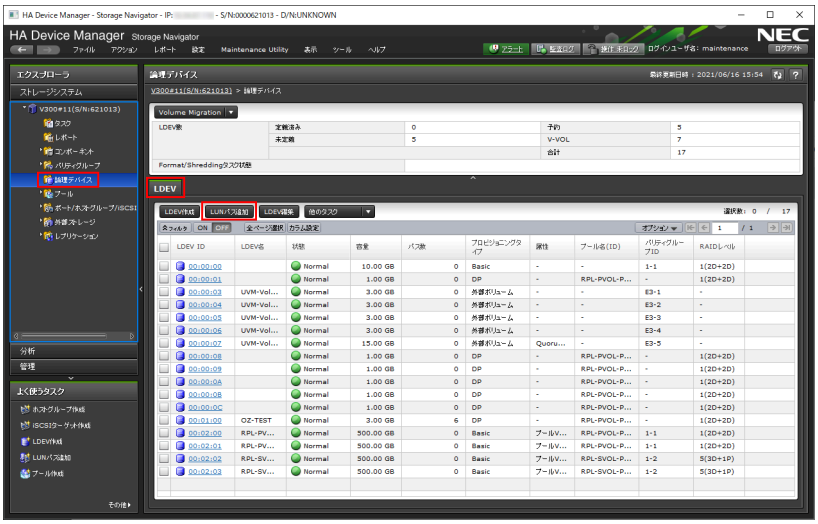
ホストで、設定した構成で論理デバイスが使えるように、論理デバイスにポート ID とホストグループ/iSCSI Target をマッピング設定します。マッピング設定は、I/O 実行中に既存のマッピング設定で変更することができます。

メモ

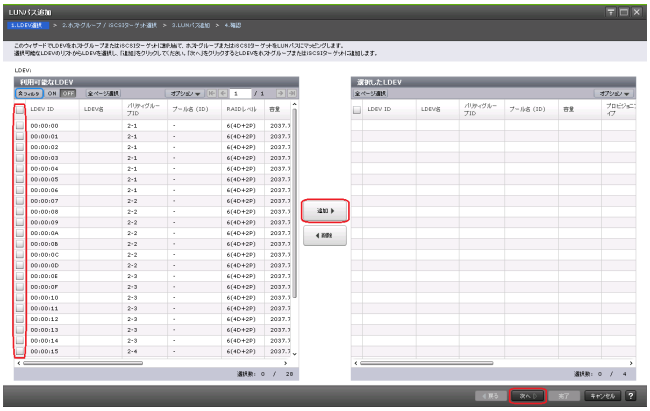
ストレージシステムとホスト間での Fibre Channel インターフェース接続時、ホストによって論理デバイス 0 がストレージシステムに作成されていないと、ストレージシステムの論理デバイスが認識されないことがあります。その場合は、論理デバイス 0 を作成するか、論理デバイスをホストグループ 0 にマッピングしてください。

操作手順

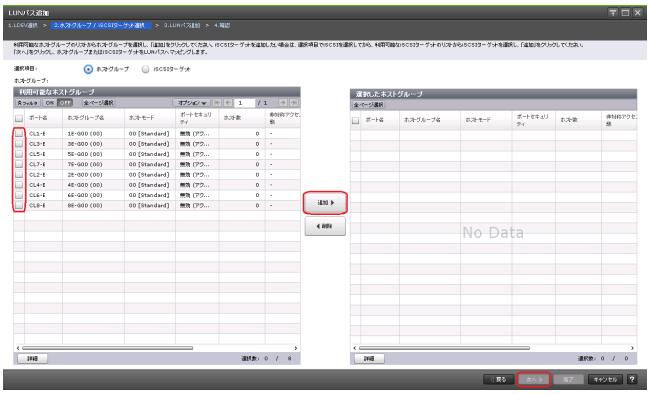
1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［論理デバイス］を選択します。



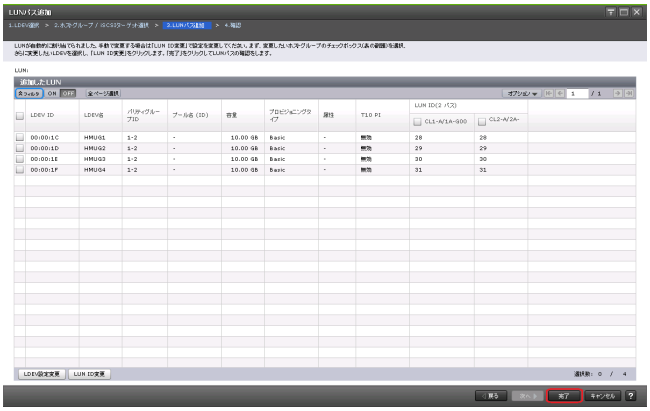
2. ［LDEV］タブの［LUN パス追加］をクリックします。
3. ［LDEV 選択］画面が表示されます。［利用可能な LDEV］リストから LDEV を選択し、［追加］をクリックします。［選択した LDEV］に追加されます。ホストグループを選択するために［次へ］をクリックします。



4. ［ホストグループ/iSCSI ターゲット選択］画面が表示されます。追加したいホストグループ、または iSCSI ターゲットを選択し、［追加］をクリックします。LUN パスを追加するために［次へ］をクリックします。



5. ［LUN パス追加］画面が表示されます。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。内容を確認し、タスク名を指定後、［適用］をクリックします。

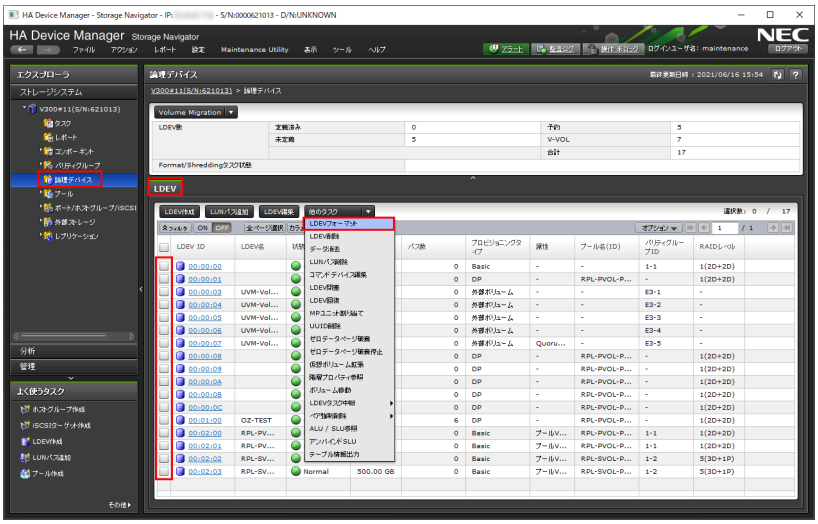
E.1.6 LDEV のフォーマット

⚠ 注意

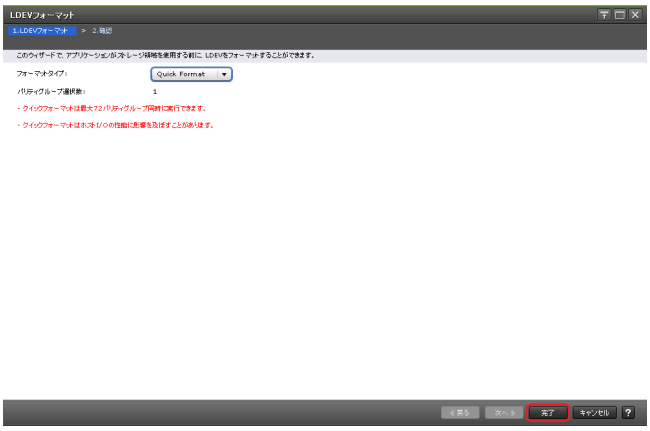
この操作を実行するとユーザデータを消失します。必要に応じてユーザデータをバックアップしてから作業を進めてください。

操作手順

1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［論理デバイス］を選択します。
2. ［LDEV］タブを表示します。フォーマットしたい論理デバイスをチェックします。
3. ［他のタスク］－［LDEV フォーマット］をクリックします。



4. ［フォーマットタイプ］を指定し、［完了］をクリックします。



5. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。指定した論理デバイスがフォーマットされます。この時点で、この論理デバイスはホストから認識可能になります。

6. フォーマットが開始されると、バックグラウンドで実行している論理デバイスフォーマットの進捗状況が論理デバイスの［状態］に表示されます。ストレージシステムの状態を最新の情報で取得し、パーセンテージを更新するために［更新］ボタンをクリックしてください。

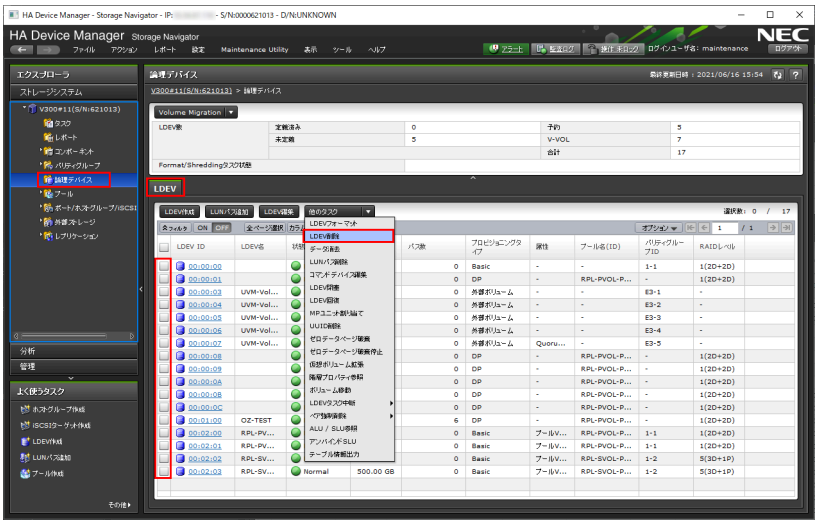
E.1.7 LDEV の削除

⚠注意

この操作を実行すると論理デバイスが削除されるため、ユーザデータを消失します。必要に応じてユーザデータをバックアップしてから作業を進めてください。

操作手順

1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［論理デバイス］を選択します。
2. ［LDEV］タブを表示します。
3. 削除したい論理デバイスをチェックします。［他のタスク］－［LDEV 削除］をクリックします。

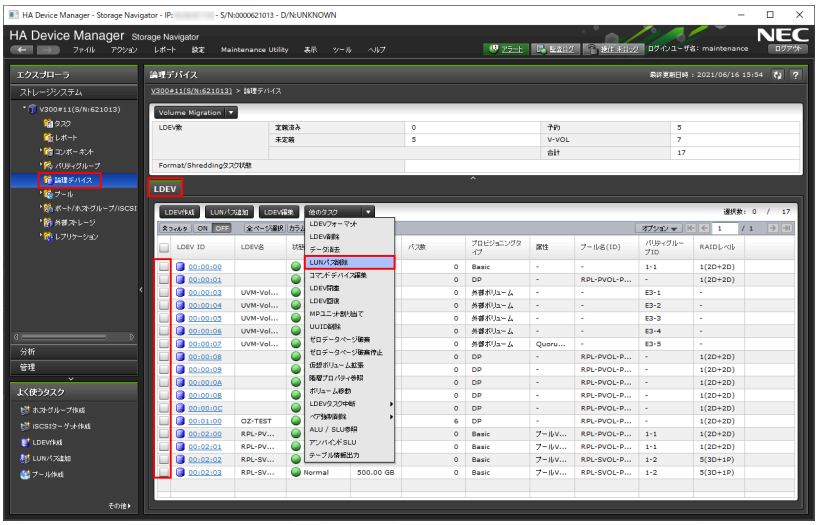


4. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。
5. 削除してもよいかを尋ねるメッセージが表示されます。［OK］をクリックします。

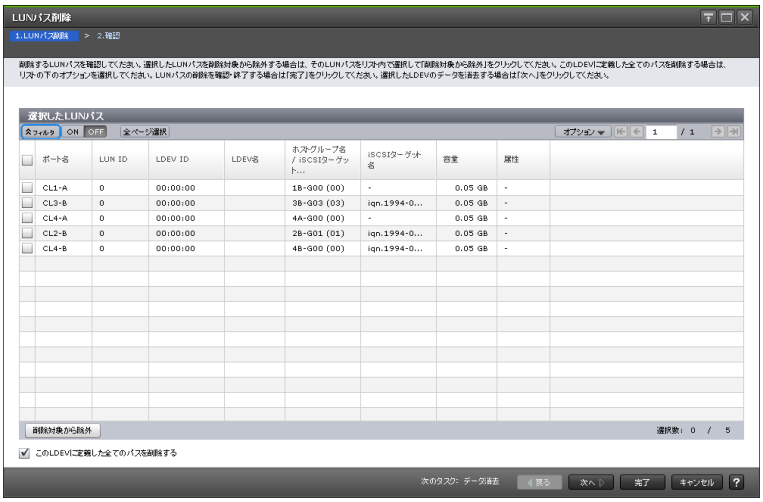
E.1.8 LDEV からの LUN パス削除

操作手順

1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［論理デバイス］を選択します。
2. ［LDEV］タブを表示します。
3. LUN パスを削除したい LDEV をチェックします。［他のタスク］－［LUN パス削除］をクリックします。



4. ［選択した LUN パス］に削除する LUN パスが表示されていることを確認します。［次へ］をクリックします。

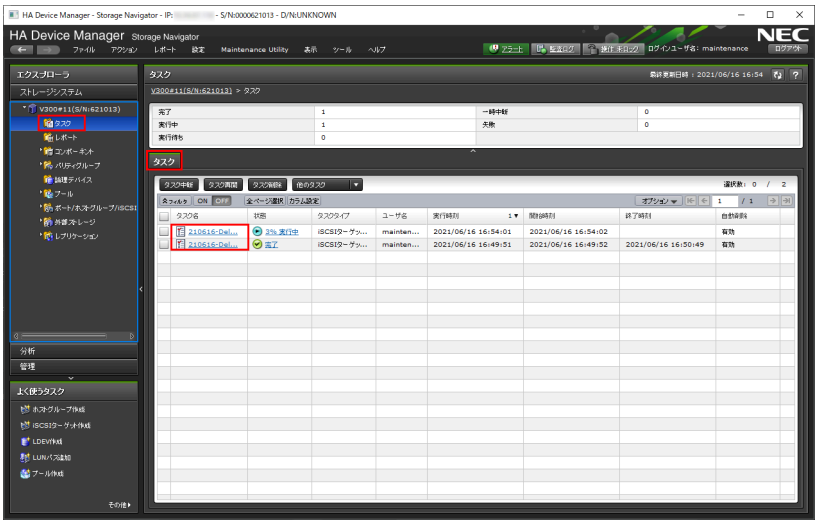


5. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。
6. 削除してもよいかを尋ねるメッセージが表示されます。［OK］をクリックします。

E.1.9 タスクの状態確認

操作手順

1. Storage Navigator メイン画面の［ストレージシステム］ツリーから［タスク］を選択します。
2. ［タスク］タブを表示します。



ストレージシステムに対するタスクの一覧が表示されます。

表示される最大のタスク件数は、完了/失敗が 256 件、実行中/実行待ち/一時中断が 128 件、合わせて 384 件です。

サマリ

項目	説明
完了	完了したタスクの数が表示されます。
実行中	実行中のタスクの数が表示されます。
実行待ち	実行待ちのタスクの数が表示されます。
一時中断	一時中断したタスクの数が表示されます。
失敗	エラーが発生したタスクの数が表示されます。

［タスク］タブ

項目	説明
タスク名	タスク実行時にユーザが入力したタスク名。タスクを実行したユーザがクリックすると、そのタスクの詳細が表示されます。
状態	タスクの状態。タスクを実行したユーザがクリックすると、タスクの状態やエラーの詳細が表示されます。 • ［完了］または［完了(開始指示)］：タスクが正常終了したことを示します。 • ［実行中］：タスクが実行中であることを示します。

項目	説明
	• ［実行待ち］：タスクが実行待ちであることを示します。 • ［一時中断］：タスクが一時中断していることを示します。 • ［失敗］：タスクが異常終了したことを示します。
タスクタイプ	タスクの一般的な名称が表示されます。
ユーザ名	タスクを実行したユーザ名が表示されます。
実行時刻	タスクが受け付けられた日時（24 時間表記）が表示されます。
開始時刻	タスクの実行が開始された日時（24 時間表記）が表示されます。 空白は、タスクが開始されていないことを示します。
終了時刻	タスクが終了した日時（24 時間表記）が表示されます。 空白は、タスクが終了していないことを示します。
自動削除	• ［有効］：タスクが完了し画面の表示件数に達すると、自動的に削除されるタスクであることを示します。 • ［無効］：ユーザが削除するまで、タスクが画面に表示されます。 状態が失敗のタスクは、自動削除が無効になります。
［タスク中断］ボタン	選択したタスクを一時中断し、順番が来ても実行されないようにします。実行待ちのタスクだけ一時中断できます。
［タスク再開］ボタン	選択したタスクを実行待ちの状態に戻します。
［タスク削除］ボタン	選択したタスクを画面から削除します。 • 実行待ちのタスクを削除すると、タスクはキャンセルされます。 • エラーが発生したタスクや中断したタスクを画面から削除できます。 • 自動削除を有効にした場合、画面の表示最大件数に達しているときに、新たなタスクを実行すると、古いタスクから順に自動的に削除されます。 • 実行中のタスクは削除できません。
［タスク自動削除無効］※	選択したタスクが完了したあと、自動的に削除されないように設定します。
［タスク自動削除有効］※	選択したタスクが完了し画面の表示最大件数に達すると、古い順に自動的に削除されるように設定します。
［テーブル情報出力］※	テーブル情報を出力させる画面が表示されます。

注※

［他のタスク］をクリックすると表示されます。

3. 該当するタスクの情報を確認します。

タスク名のリンクをクリックすると、詳細な情報を確認できます。

付録 F.　Fibre Channel ポートおよび iSCSI ポートの管理

ホストへ接続する Fibre Channel ポートと iSCSI ポートの設定や、ホストグループ/iSCSI ターゲットの削除などを、Storage Navigator から行う方法を説明します。

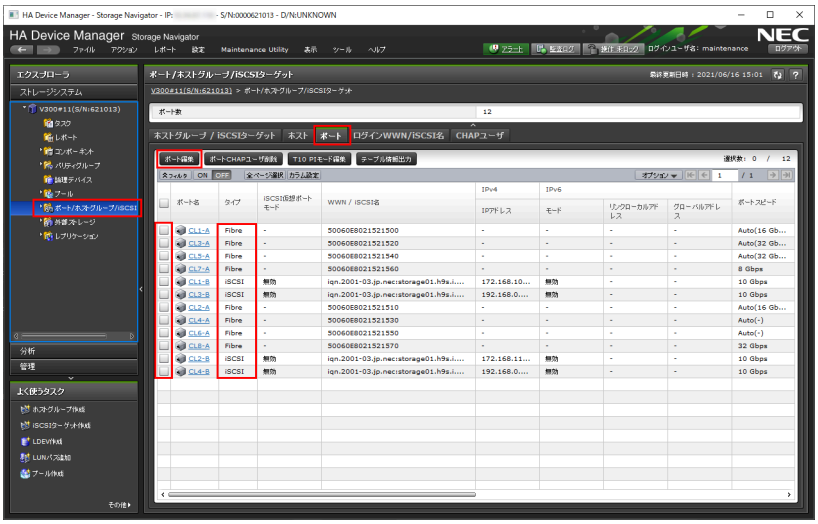
F.1　Fibre Channel ポートおよび iSCSI ポートの管理（Storage Navigator 編）

Storage Navigator から Fibre Channel ポートと iSCSI ポートの設定変更や、ホストグループ/iSCSI ターゲットを削除する手順を説明します。また、iSCSI ポートでの CHAP 認証の設定方法も説明します。

F.1.1　Fibre Channel ポートの設定変更

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ポート］タブをクリックします。
3. 編集するポート（［タイプ］が Fibre）を選択します。
4. ［ポート編集］をクリックします。



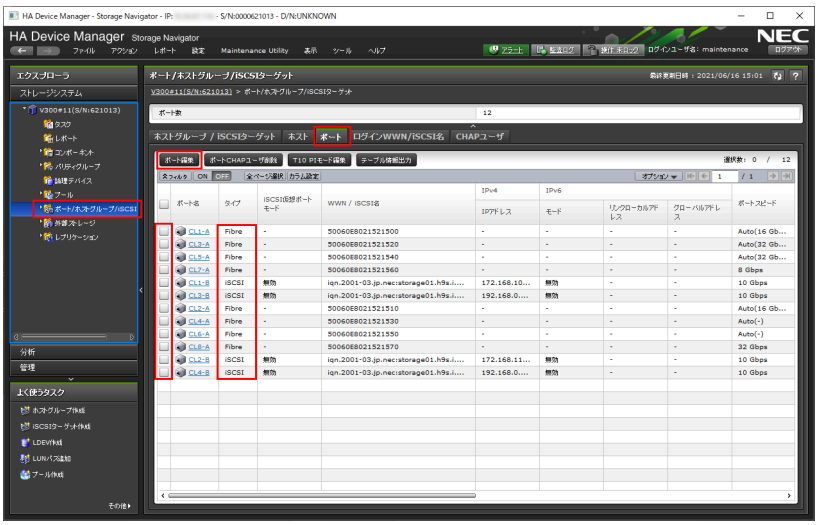
5. ［ポート編集］画面が表示されます。詳細は、『システム構築ガイド』の「ポート編集ウィザード」を参照してください。編集後、［完了］をクリックします。

6. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

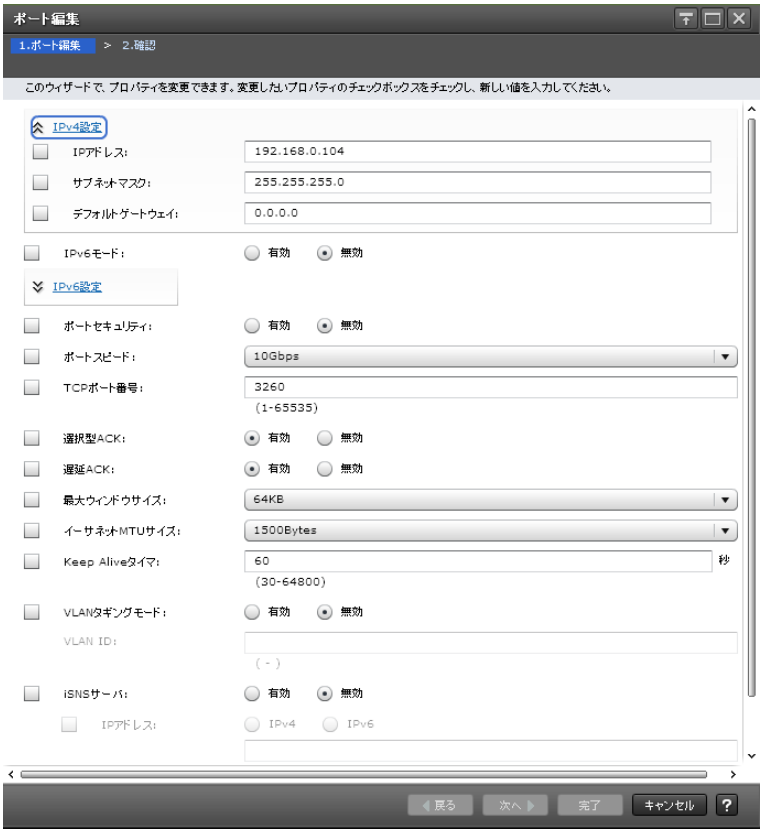
F.1.2　iSCSI ポートの設定変更

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ポート］タブをクリックします。
3. 編集するポート（［タイプ］が iSCSI）を選択します。
4. ［ポート編集］をクリックします。



5. ［ポート編集］画面が表示されます。詳細は、『システム構築ガイド』の「ポート編集ウィザード」を参照してください。編集後、［完了］をクリックします。

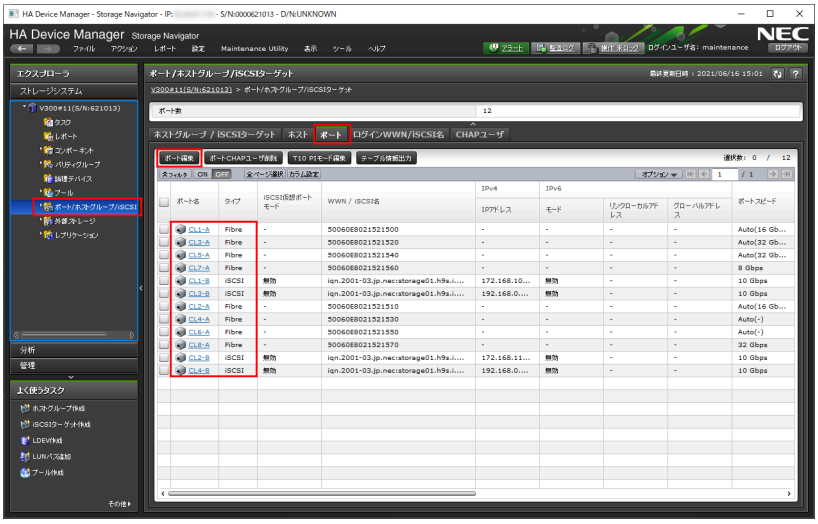


6. 確認画面が表示されます。内容を確認し、タスク名を指定後、[適用]をクリックします。

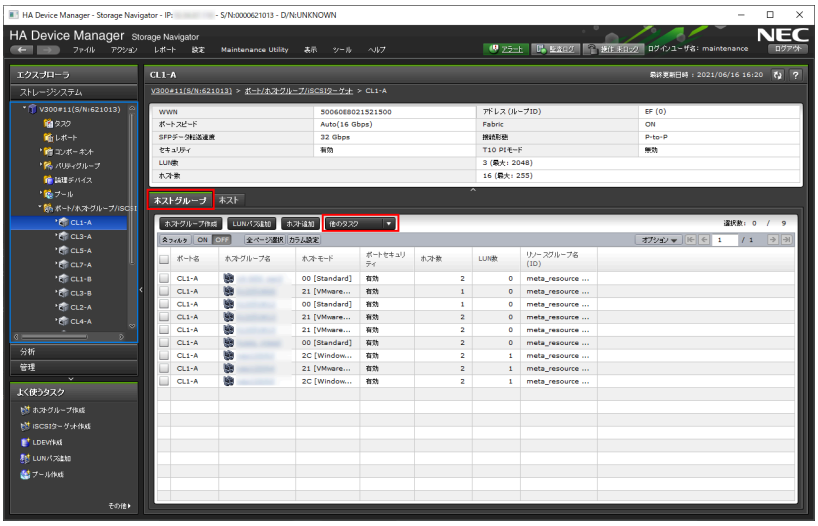
F.1.3 ホストグループの削除

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ポート］タブをクリックします。
3. 編集するポート（［タイプ］が Fibre）を選択します。



4. 選択したポートの画面が表示されます。
5. ［ホストグループ］タブをクリックします。
6. ホストグループを削除するポート名をチェックし、［他のタスク］－［ホストグループ削除］を選択します。



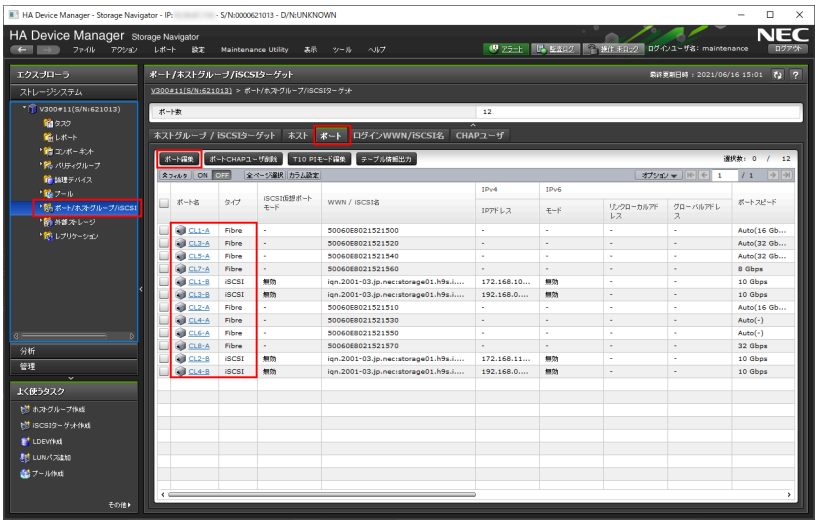
7. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。
8. 削除してもよいかを尋ねるメッセージが表示されます。［OK］をクリックします。

F.1.4 iSCSI ターゲットの削除

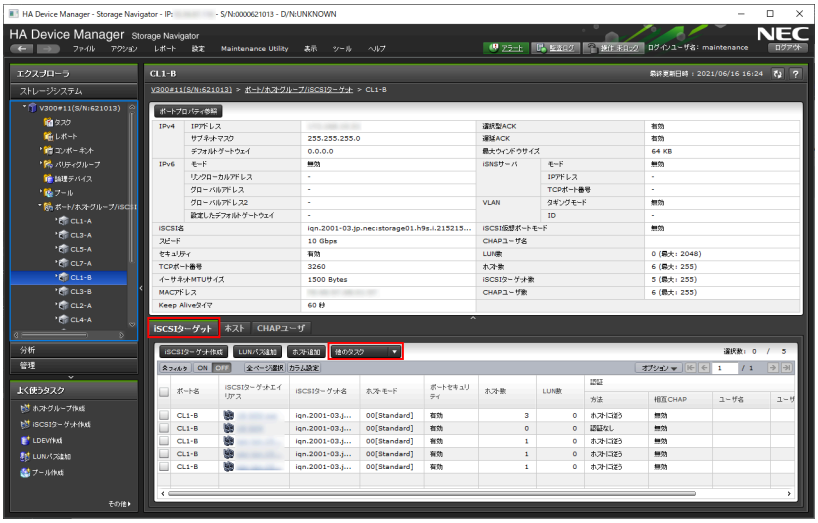
操作手順

1. Storage Navigator メイン画面の［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。
2. ［ポート］タブをクリックします。

3. 編集するポート（[タイプ] が iSCSI）を選択します。



4. 選択したポートの画面が表示されます。
5. [iSCSI ターゲット] タブをクリックします。
6. iSCSI ターゲットを削除するポート名をチェックし、[他のタスク] – [iSCSI ターゲット削除] を選択します。



7. 確認画面が表示されます。内容を確認し、タスク名を指定後、[適用] をクリックします。
8. 削除してもよいかを尋ねるメッセージが表示されます。[OK] をクリックします。

F.1.5 iSCSI ポートでの CHAP 認証の使用

CHAP（Challenge Handshake Authentication Protocol）は、ストレージシステム（target）がサーバの iSCSI Initiator を認証する iSCSI 認証方法（オプション）です。

2 種類の CHAP 認証があります。

- 単方向 CHAP

- 双方向 CHAP

単方向 CHAP では、ストレージシステムは CHAP シークレット経由でサーバの iSCSI Initiator より発行されたすべてのアクセス要求を認証します。

単方向 CHAP 認証を設定するときは、ストレージシステムで CHAP シークレットを入力し、サーバの各 iSCSI Initiator がストレージシステムにアクセスしようとするたびに、シークレットを送信するように構築します。

双方向 CHAP では、ストレージシステムと iSCSI Initiator は双方で認証します。双方向 CHAP を設定するときは、ストレージシステムがサーバに接続を確立するよう送信する必要がある CHAP シークレットを用いて iSCSI Initiator を構築します。双方向認証処理中、サーバとストレージシステムは接続が許可される前に相手側の認証を受けなければならない情報を送信し続けます。

CHAP はオプション機能なので、iSCSI を使うときに必ずしも必要ではありません。ただし、CHAP 認証の構築をしない場合、ストレージシステムと同じ IP ネットワークに接続されたどのサーバからでも、ストレージシステムへの読み書きができるので注意してください。

メモ

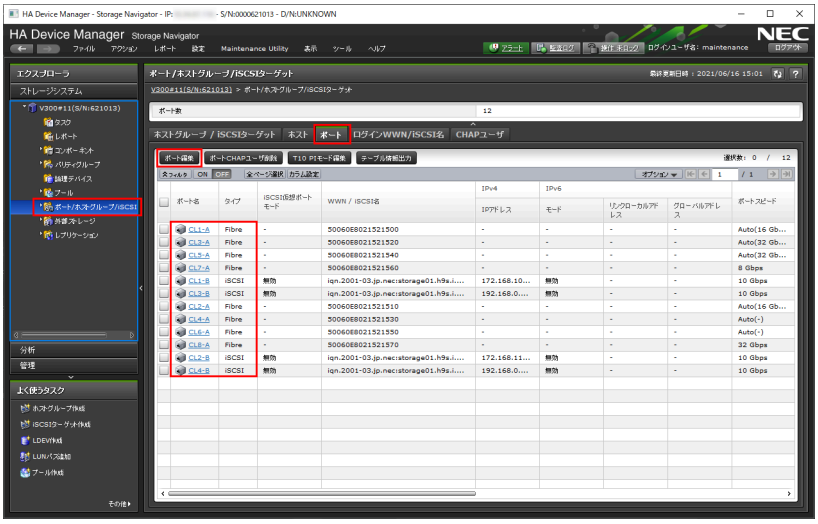
ストレージシステムで CHAP 認証を有効にするには、iSCSI Initiator を用いてサーバを構築してください。ホストに接続している HBA を交換するときは、CHAP の iSCSI Name 設定を変更してください。MTU サイズを変更する場合は、ストレージシステム側とスイッチ/ホスト側で設定を再設定してください。

F.1.5.1 単方向 CHAP 認証の構築

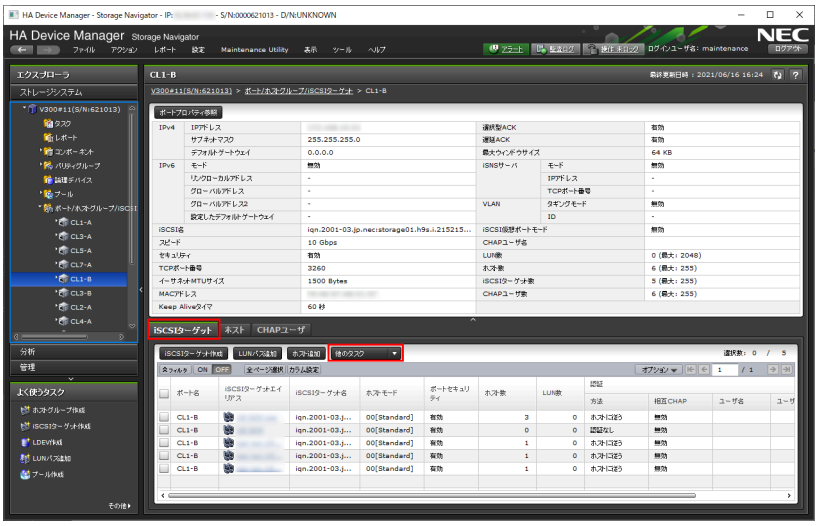
Initiator 認証のために、CHAP ユーザを作成しターゲットに割り当てます。

操作手順

1. Storage Navigator メイン画面の［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。
2. ［ポート］タブをクリックします。
3. CHAP ユーザを追加するポート（［タイプ］が iSCSI）を選択します。



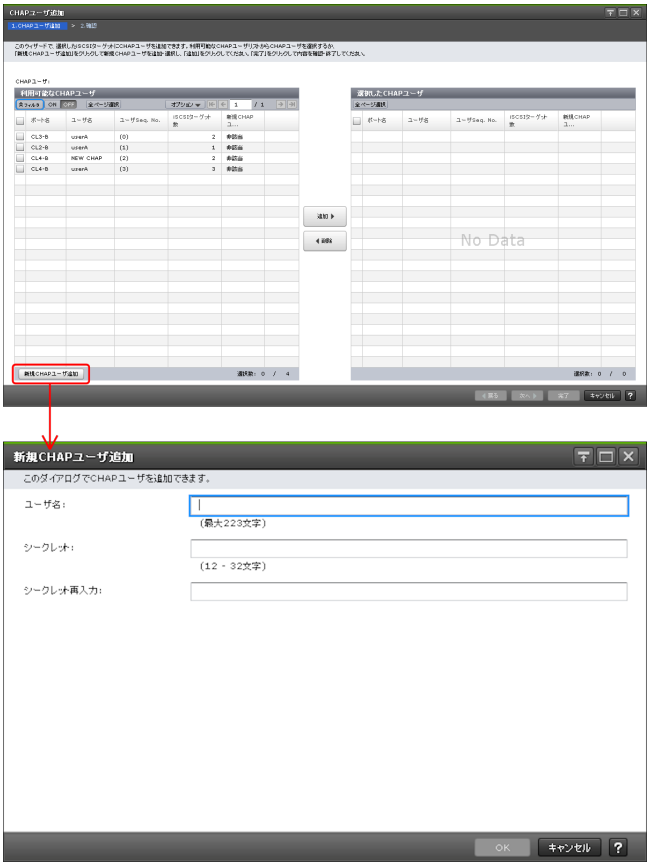
4. 選択したポートの画面が表示されます。
5. ［iSCSI ターゲット］タブをクリックします。
6. CHAP ユーザを追加するポート名を選択し、［他のタスク］－［CHAP ユーザ追加］を選択します。



7. ［利用可能な CHAP ユーザ］リストから CHAP ユーザを選択し、［追加］をクリックします。

   ［選択した CHAP ユーザ］に追加されます。［完了］をクリックします。

   新規に CHAP ユーザを作成する場合は、［新規 CHAP ユーザ追加］をクリックします。CHAP ユーザ情報を入力し、［OK］をクリックします。

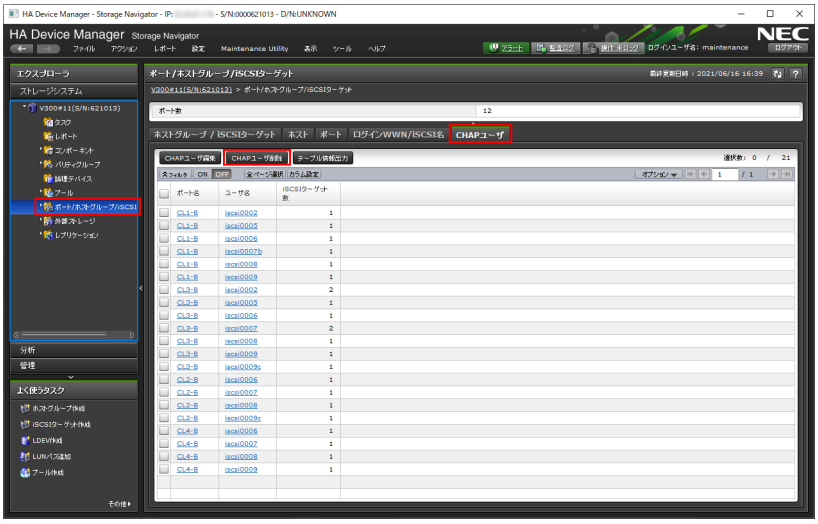


8. 確認画面が表示されます。内容を確認し、タスク名を指定後、[適用]をクリックします。

F.1.5.2 単方向 CHAP 認証のユーザ削除

操作手順

1. Storage Navigator メイン画面の[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。
2. [CHAP ユーザ]タブをクリックします。
3. 削除するポート名をチェックし、[CHAP ユーザ削除]をクリックします。



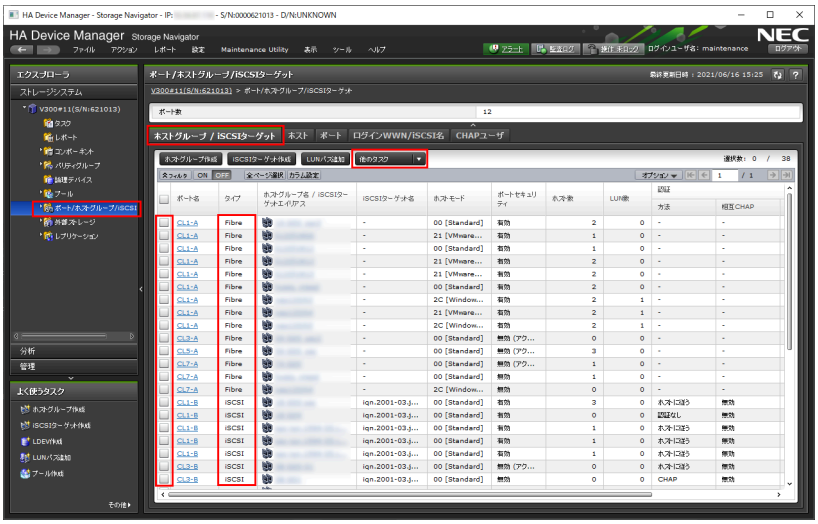
4. 確認画面が表示されます。内容を確認し、タスク名を指定後、[適用]をクリックします。
5. 削除してもよいかを尋ねるメッセージが表示されます。[OK]をクリックします。

F.1.5.3 単方向 CHAP 認証の設定変更

認証方法を設定するには iSCSI ターゲット編集画面で設定します。

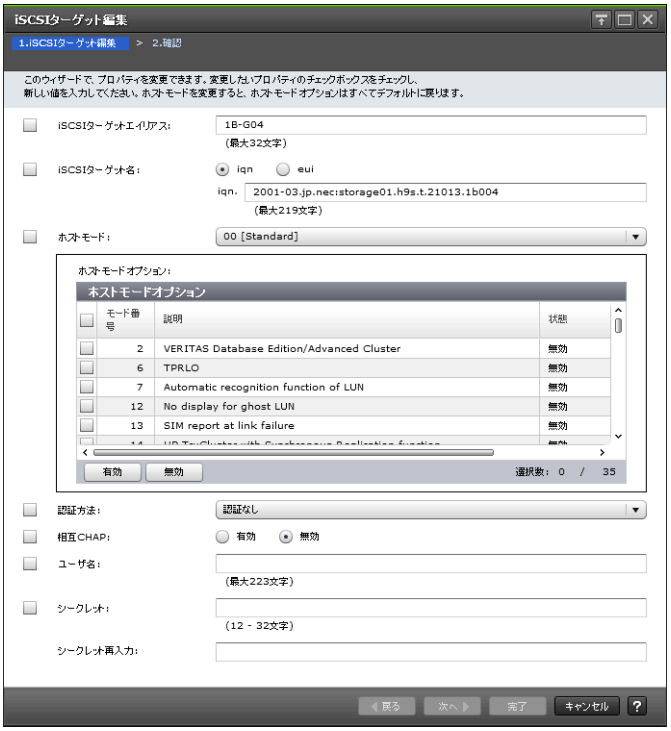
操作手順

1. Storage Navigator メイン画面の[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。
2. [ホストグループ]タブをクリックします。
3. CHAP 認証を変更するポート([タイプ]が iSCSI)を選択します。
4. [他のタスク]－[iSCSI ターゲット編集]を選択します。



5. ［iSCSI ターゲット編集］画面が表示されます。［認証方法］で［ホストに従う］、［CHAP］または［認証なし］を選択します。

   ［CHAP］を選択した場合、次の項目を設定します。



相互 CHAP	ユーザ名	シークレット	シークレット再入力
有効（双方向認証）	必須	必須	必須
無効（単方向認証）	任意	任意	任意

6. ［完了］をクリックします。
7. 確認画面が表示されます。内容を確認し、タスク名を指定後、［適用］をクリックします。

付録 G. SVP の管理と機能

SVP の電源の ON/OFF 手順と、SVP から利用できるストレージ管理機能とその実施手順を説明します。操作は主に Storage Device List を使用します。

G.1 SVP の管理

SVP の電源の ON/OFF 手順を説明します。

G.1.1 SVP の電源を ON する

SVP として使用している物理マシンまたは仮想マシンの電源を ON にしてください。

G.1.2 SVP の電源を OFF する

操作手順

1. SVP で 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。「`shutdown /s /f /t 0`」
3. コマンドプロンプトを閉じます。

メモ

ユーザガイド中で“再起動”を指示されている箇所については必ず「G.1.3 SVP を再起動する (315 ページ)」の手順を実施してください。OS ごとのシャットダウン方法の違いについては、次の注意を参照してください。

⚠ 注意

上記の操作手順以外の方法でシャットダウンすると、次回起動時に正常に SVP が起動しない場合があります。

上記の操作手順以外の方法でシャットダウンした場合は、SVP を再起動してください。次の設定により、上記の操作手順以外の方法でシャットダウンを行っても、次回起動時に正常に Storage Navigator が起動できるようになります。

コントロールパネル－［システムとセキュリティ］

－［電源オプション］－［スリープ解除時のパスワード保護］または［電源ボタンの動作を選択する］

－［システム設定］－［現在利用可能ではない設定を変更します］

－［シャットダウン設定］－［高速スタートアップを有効にする(推奨)］のチェックをはずす。

－［高速スタートアップを有効にする(推奨)］のチェックをはずす。

－［変更の保存］

この設定は Windows Update などで元に戻る場合があります。

G.1.3 SVP を再起動する

操作手順

1. SVP で 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。「`shutdown /r /f /t 0`」
3. コマンドプロンプトを閉じます。

   SVP が再起動します。

G.1.4 SVP への接続を解除する

操作手順

1. Windows の［スタート］メニューから、［電源］をクリックします。または［ログオフ］のオプションをクリックします。
2. 表示されたメニューから、［切断］をクリックします。

G.1.5 SVP のシステム日時とタイムゾーンを変更する

前提条件

- Storage Device List にストレージシステムが登録されていないこと
- Storage Device List にストレージシステムが登録済みの場合は、ストレージシステムのサービスが停止していること（停止手順は「G.2.6 ストレージシステム単位のサービスを停止（354 ページ）」を参照してください）

操作手順

1. 使用している SVP OS のマニュアルを参照して、日時とタイムゾーンを変更します。
2. タイムゾーンを変更した場合は、SVP を再起動して、バックグラウンドのサービスを再起動します。

SVP の再起動は、「G.1.3 SVP を再起動する（315 ページ）」を参照してください。再起動しないと変更が反映されません。SVP とストレージシステムのタイムゾーンが異なった状態が続き、障害の要因となります。

G.2 SVP の機能

SVP から行うソフトウェアとファームウェアの更新手順や、Storage Device List を使用したストレージ管理機能を説明します。また、SVP の障害時に備えて、SVP のバックアップとリストアを行う手順を説明します。

G.2.1 セットアッププログラムを使用したストレージ管理ソフトウェア、SVP ソフトウェア、ファームウェアの更新

メモ

- Windows エクスプローラー、あるいはコマンドプロンプトなどから、ストレージ管理ソフトウェア、SVP ソフトウェアがインストールされているフォルダおよびファイルが削除されると、更新処理が異常終了する場合があります。フォルダおよびファイルを削除する場合は、「G.2.10 ストレージ管理ソフトウェア、および SVP ソフトウェアの削除（アンインストール）（360 ページ）」に従って削除してください。
- 更新処理が異常終了した場合は、「5.4.1 ストレージ管理ソフトウェアおよび SVP ソフトウェア インストール時のトラブルシューティング（107 ページ）」を参照してください。

ストレージ管理ソフトウェア、SVP ソフトウェア、ストレージシステムのファームウェアを更新します。更新には新しいプログラムが入っている SVP ファームウェアメディア（メディア名称「装置添付ソフトウェア １／２」）を使用します。

所要時間はストレージ管理ソフトウェアの更新が 10 分程度、SVP ソフトウェアを更新する場合はストレージシステムあたり 10 分程度、ファームウェアを更新する場合はストレージシステムあたり 200 分程度です。

ヒント

SVP に登録されているストレージシステムの SVP ソフトウェアを更新する場合、Storage Device List から起動できます。ストレージ管理ソフトウェア、およびファームウェアの更新は Storage Device List から起動できません。Storage Device List による SVP ソフトウェアの更新の起動は、SVP ソフトウェアのバージョンと、ストレージ管理ソフトウェア、およびファームウェアのバージョンの対応を維持させるため、SVP ファームウェアメディアに格納されているファームウェアバージョン（XX-nn-mm-xx/yy）と、更新の対象となるストレージシステムの SVP 管理ソフトウェアのバージョン（XX-nn-mm-00/yy）の「XX,nn,mm,yy」が同じ場合のみ適用してください。

メモ

- 事前に SVP のソフトウェア設定情報をバックアップしてください（詳細は「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」を参照）。

- ファームウェアの更新中に「Web サーバとの間でタイムアウトエラーが発生しました。[33361-201301:00000-200000]」メッセージが表示されたら、前提条件、操作手順を再確認してください。

  前提条件、操作手順に問題が無い場合は、「サポート」へ連絡してください。

- ストレージ管理ソフトウェア以外のアプリケーションが使用するポート番号とストレージ管理ソフトウェアのアプリケーションが使用するポート番号が重複した場合、ストレージ管理ソフトウェア、および SVP ソフトウェアは正しく動作しません。SVP ソフトウェアを更新すると、ストレージ管理ソフトウェアが使用するポート番号が追加または変更されることがあります。

  追加または変更されるポート番号が、ストレージ管理ソフトウェア以外のアプリケーションで使用されていないか確認してください（「L.9 ポート番号を使用しているアプリケーションを確認する（423 ページ）」を参照）。

  SVP ソフトウェアのバージョンとポート番号の初期値の対応は、「L.1 SVP で使用するポート番号を変更する（411 ページ）」の表を参照してください。

  追加または変更されるポート番号が、ストレージ管理ソフトウェア、および SVP ソフトウェア以外のアプリケーションで使用されている場合は、次のどちらか対処を実施してください。

  - ストレージ管理ソフトウェア以外のアプリケーションが使用するポート番号を変更するか、ストレージ管理ソフトウェア以外のアプリケーションを無効にしてください。
  - ソフトウェアの更新後に、ストレージ管理ソフトウェアのポート番号を変更してください（「付録 L. SVP で使用するポート番号の変更・初期化（411 ページ）」参照）。

- SVP 上で次のプログラムを起動した状態でストレージ管理ソフトウェアを更新すると、エラーが発生し、[21443-200051] のメッセージが表示されます。その場合はプログラムを終了してから、再度ストレージ管理ソフトウェアを更新してください。

  プログラム名と終了方法を示します。

  - Storage Navigator のサブ画面：画面を閉じます。
  - Storage Navigator：画面を閉じます。

- RAID Manager をユーザスクリプトで使用しているときに、ストレージ管理ソフトウェアの更新を実行すると失敗します。RAID Manager の使用を終了した後、更新作業をやり直してください。

- RAID Manager をインストールしている環境では、ストレージ管理ソフトウェアのインストール時に、ストレージ管理ソフトウェア同梱の RAID Manager で更新ができます。ただし、ストレージ管理ソフトウェアをインストールする前に、すべての RAID Manager インスタンスコンポーネントとサービスを停止してください。

- RAID Manager のバージョンを 01-68-03/00 以降に変更すると、変更後の RAID Manager のバージョンが Windows の［コントロールパネル］－［プログラムと機能］に反映されます。ただし、変更の処理（RAID Manager のインストール）のトラブルなどにより、実際にインストールされた RAID Manager のバージョンが、コントロールパネルに反映されない場合があります（反映されていなくても、RAID Manager は正常に動作します）。このため、Windows の［コン

トロールパネル］－［プログラムと機能］に表示されるバージョンを確認し、インストールしたバージョンと異なる場合は『RAID Manager インストール・設定ガイド』のトラブルシュートを参照して、バージョン情報を修正してください。これにより、Windows のコントロールパネルでも、RAID Manager のバージョンを確認できます。

- RAID Manager のバージョンを 01-68-03/00 以降から、01-68-03/00 未満に変更すると、Windows の［コントロールパネル］－［プログラムと機能］には変更する前の RAID Manager のバージョンが表示され、バージョン情報が削除されない場合があります（削除されていなくても、RAID Manager は正常に動作します）。RAID Manager のバージョン情報が削除されていない場合は、『RAID Manager インストール・設定ガイド』に示すトラブルシュートを参照して、コントロールパネルに表示されるバージョン情報を削除してください。
- RAID Manager のバージョンは RAID Manager の raidqry -h コマンドで確認できます。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、リモートでソフトウェアとファームウェアの更新を行うこともできます。SVP に DVD ドライブが搭載されていない場合は、リモートデスクトップ接続して管理クライアントの DVD ドライブを使用します。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

⚠ 注意

- インストール先のドライブの空き容量を、20GB 以上確保してください。
- SVP ソフトウェアの更新後、ソフトウェア設定情報のバックアップファイルを取得し、保管してください（バックアップの方法は「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」を参照）。SVP ソフトウェアの設定情報をリストアする場合、リストアするバックアップファイルは、リストア先の SVP ソフトウェアと同じバージョンの SVP ソフトウェアで取得したバックアップファイルを使用してください（リストアの方法は「G.2.9.2 SVP のソフトウェア設定情報のリストア（359 ページ）」を参照）。異なるバージョンで取得したバックアップファイルをリストアする場合は、「G.2.9.2 SVP のソフトウェア設定情報のリストア（359 ページ）」の注意を参照ください。

G.2.1.1 SSL 通信の署名付き証明書について

ストレージ管理ソフトウェアを更新すると、SVP と管理クライアント間の SSL 通信の署名付き証明書が、デフォルトの証明書に戻ることがあります。

このため、SVP と管理クライアント間の SSL 通信の署名付き証明書をインストールしている場合は、以下の流れでソフトウェアを更新してください。

1. 証明書のインストールで使用した証明書ファイルがあることを確認します（確認結果は「G.2.1.3 SSL 通信の署名付き証明書の再インストール（331 ページ）」で使用）。

2. ストレージ管理ソフトウェアを更新します（「G.2.1.2 GUI による更新（319 ページ）」を参照）。
3. SSL 通信の署名付き証明書の状態を確認します（「G.2.1.3 SSL 通信の署名付き証明書の再インストール（331 ページ）」を参照）。
4. デフォルトの証明書に戻っている場合、証明書を再インストールします（「G.2.1.3 SSL 通信の署名付き証明書の再インストール（331 ページ）」を参照）。

G.2.1.2 GUI による更新

前提条件

- ストレージシステムの電源が ON になっていること。
- Windows のイベントビューアーが起動していないこと。
- ウィルス検出プログラムのサービスを停止していること。ウィルス検出プログラムが稼働している状態で実行すると、ソフトウェア更新のパフォーマンスが低下したり、正しく完了できない可能性があります。

操作手順

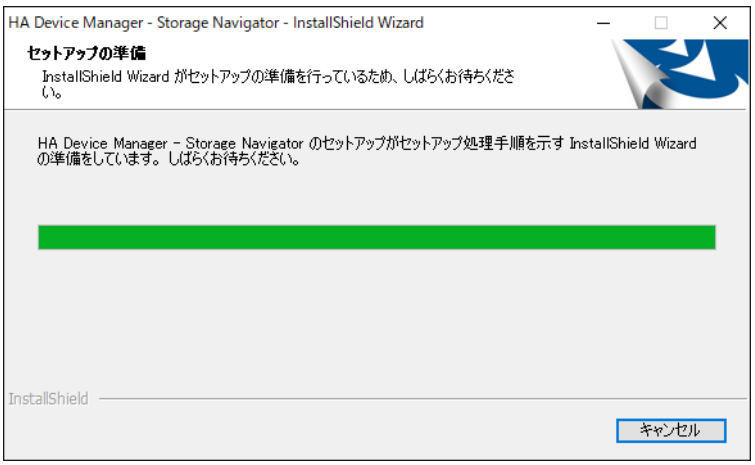
1. SVP ファームウェアメディアを、SVP の DVD ドライブに挿入します。

   メモ

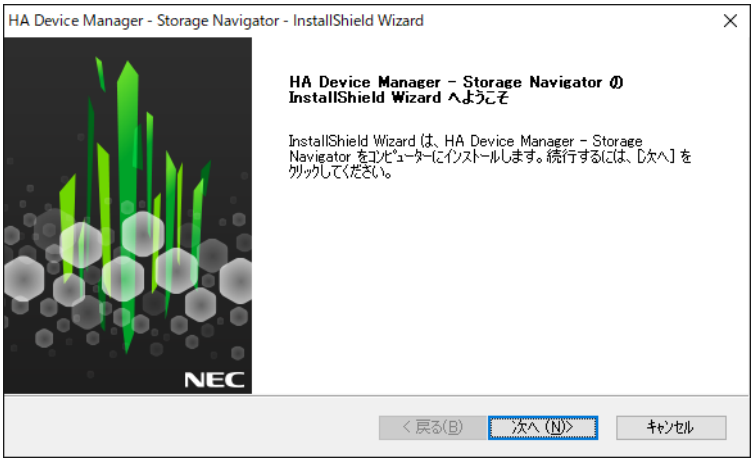
   SVP ファームウェアメディアを使用後、DVD ドライブからメディアを取り出して保管してください。

2. ドライブ直下の Setup.exe を右クリックし、［管理者として実行］をクリックします。

   インストール準備中画面が表示されます。準備が完了するまでお待ちください。



3. 準備が完了したら、Install Shield 画面が表示されます。［次へ］をクリックします。



4. OSS（Open Source Software）の使用許諾の確認画面が表示されます。

   ［使用許諾契約の全条項に同意します］を選択し、［次へ］をクリックします。

5. 既存の OSS のバージョンにより、インストールのスキップ、またはアップデートの確認メッセージが表示されるので、どちらの場合も［はい］をクリックします。

インストール済みの OSS のバージョンが SVP ファームウェアメディアからインストールするバージョンと同じ場合

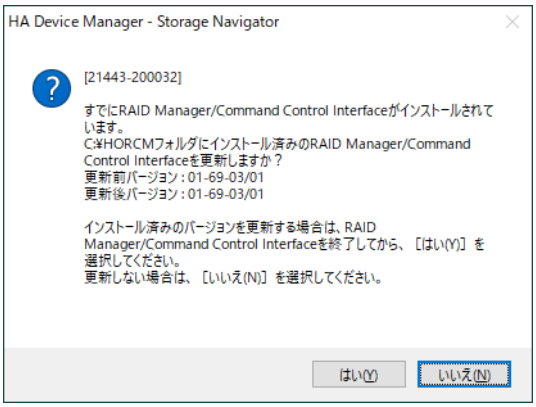
インストール済みの OSS のバージョンが SVP ファームウェアメディアからインストールするバージョンと一致していない場合

別途 RAID Manager をインストールしている場合は、ストレージ管理ソフトウェア同梱の RAID Manager での更新メッセージ“21443-200032” が表示されます。

RAID Manager をインストールしていない、またはインストールしたフォルダ(HORCM フォルダ)をリネームしている場合は表示されません。

更新する場合は、RAID Manager の使用を終了した後、［はい］ボタンをクリックしてください。［いいえ］ボタンをクリックすると RAID Manager のバージョンは維持されます。

複数の RAID Manager をインストールしている場合は、もっとも順番が前のドライブレターのドライブにインストールしている RAID Manager が更新対象となります。

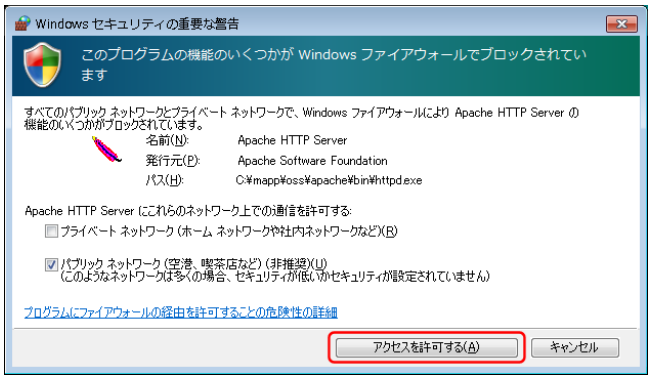


メッセージ画面に「注意」が表示されているときに［はい］ボタンをクリックすると、Windows の［コントロールパネル］－［プログラムと機能］には、すでにインストールされている RAID Manager のバージョンが表示され、変更後のバージョンは反映さ

れません。このため、ストレージ管理ソフトウェアのインストールが完了したら『RAID Manager インストール・設定ガイド』に示す RAID Manager のバージョン削除方法を参照して、コントロールパネルに表示されるバージョン情報を削除してください。

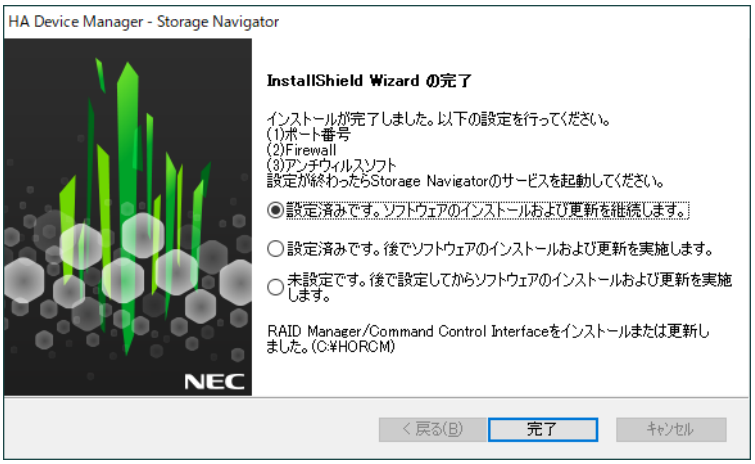
メモ

セキュリティ警告の画面が表示される場合は、[アクセスを許可する] をクリックしてください。



6. 完了メッセージが表示されます。

[設定済みです。ソフトウェアのインストールおよび更新を継続します。] を選択し、[完了] をクリックします。

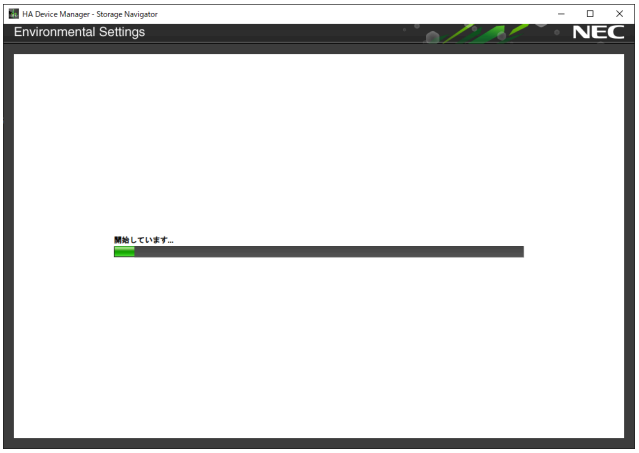


ストレージ管理ソフトウェアの更新が完了すると、Environmental Settings ツールが起動します。

メモ

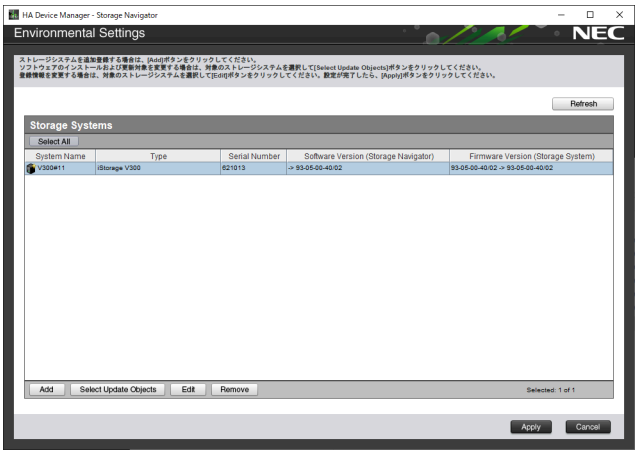
[設定済みです。後でソフトウェアのインストールおよび更新を実施します。] は選択しないでください。Environmental Settings ツールが起動しません。

更新準備中画面が表示されます。準備が完了するまで待ってください。



7. ストレージシステムの一覧画面が表示されます。

   更新したいストレージシステムを選択して［Select Update Objects］をクリックします。

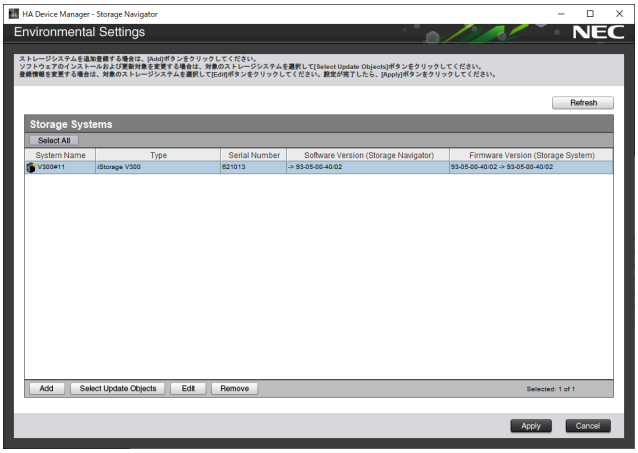


8. ［Select Update Objects］画面が表示されます。SVP ソフトウェアの更新を実施する場合は［Software (Storage Navigator)］をチェックし、更新を実施しない場合はチェックを外します。ファームウェアの更新を実施する場合は［Firmware (Storage System)］をチェックし、更新を実施しない場合はチェックを外します。選択が終わったら［Apply］をクリックします。

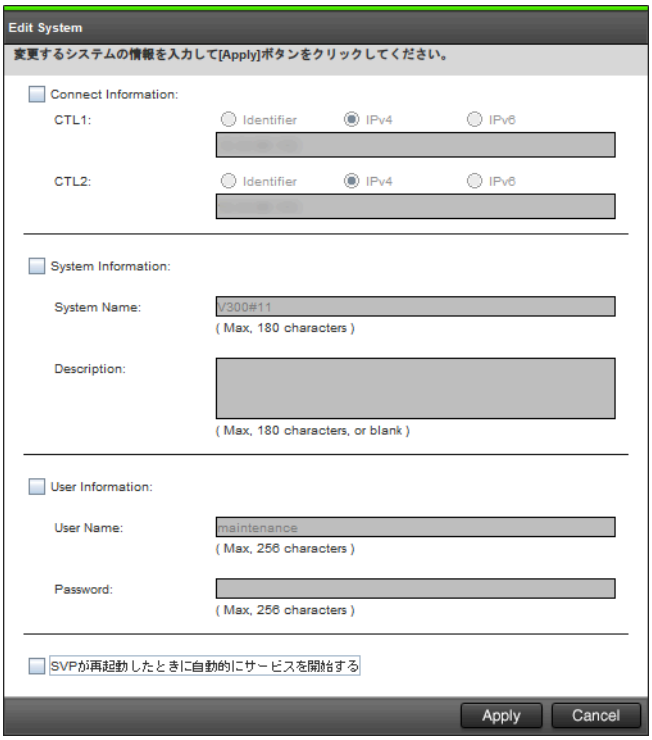
9. ［Apply］をクリックすると、［Environmental Settings］画面に戻ります。

   ファームウェアを更新する場合は、以下の操作を実施してください。

   a. 対象ストレージシステムを選択し、［Edit］をクリックします。

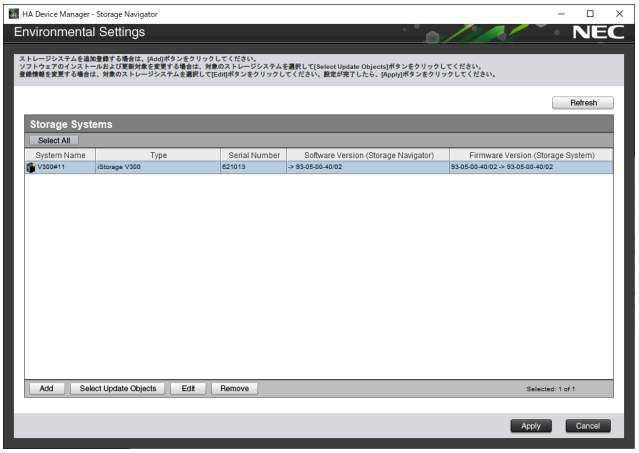


b. ［SVP が再起動したときに自動的にサービスを開始する］のチェックボックスでチェックが外れていることを確認します。チェックされている場合は、チェックを外します。



c. 確認および入力が完了したら、［Apply］をクリックします。

10. 手順 7～9 を繰り返して、すべてのストレージシステムに対して更新を実施するかを選択したら、対象ストレージシステムの一覧画面で［Apply］をクリックします。



11. ［Update software and firmware］画面が表示されます。［Confirm］をクリックします。

更新実行画面が表示され、ストレージシステムのソフトウェア更新が自動で開始されます。

［Software (Storage Navigator)］列ではソフトウェア更新の状態が確認できます。

メモ

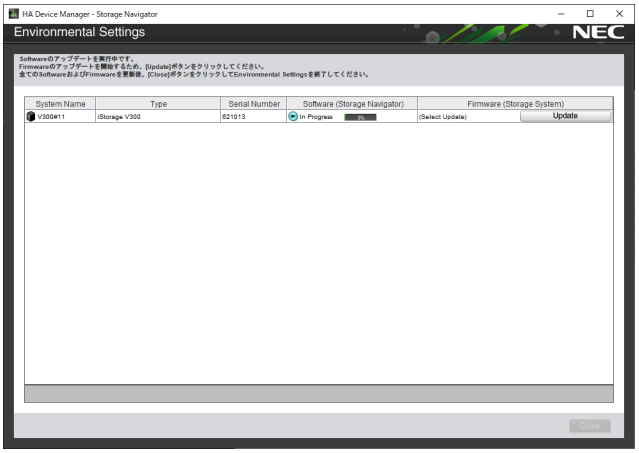
アプリケーションの実行中に、アプリケーションを強制終了する操作（PC シャットダウンなど） をしないでください。このような操作をした場合は、Maintenance Utility へのログイン時にメッセージ ［32061-208063］ が表示されることがあります。

この状態に陥ったと思われる場合は、以下の対処方法を実施してください。

a. 新しく開いた Maintenance Utility 画面で、［ファームウェア更新］画面を開きます。

b. ［ファームウェア更新設定］画面が表示されることを確認します（ファームウェア更新の進捗画面が表示された場合は、ファームウェア更新が動作中ですので 終了するまでお待ちください)。

c. システムロック強制解除を実行します（「3.12.5 システムロックの強制解除（92 ページ)」参照)。

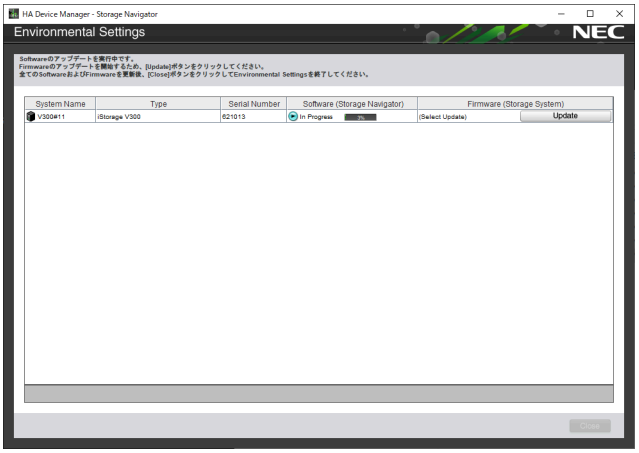


ソフトウェア更新の状態は、次の状態があります。

状態	内容
Waiting	ソフトウェアの更新を実施していません。 ソフトウェアの更新は 1 台ずつ実行されます。すでに別のストレージシステムのソフトウェア更新が実行されている場合は、他のストレージシステムはこの状態になります。
In Progress	ソフトウェアの更新が実行中です。
Completed	ソフトウェアの更新が完了しています。
Failed	ソフトウェアの更新に失敗しました。 ストレージシステムを追加した場合は、追加が完了していない場合があります。クリックしてメッセージに従ってください。
(Not Update)	ソフトウェア更新対象に選択されていません。 ストレージシステムを追加した場合は、この状態になることはありません。

12. ストレージシステムにアクセスしてファームウェア更新を実施します。

    ファームウェア更新を実施するためには、［Firmware (Storage System)］列の［Update］をクリックします。ファームウェア更新は、ソフトウェア更新の実行中に実施できます。



ヒント

手順 8 で［Firmware (Storage System)］のチェックを外した場合、手順 12 から手順 16 は必要ありません。

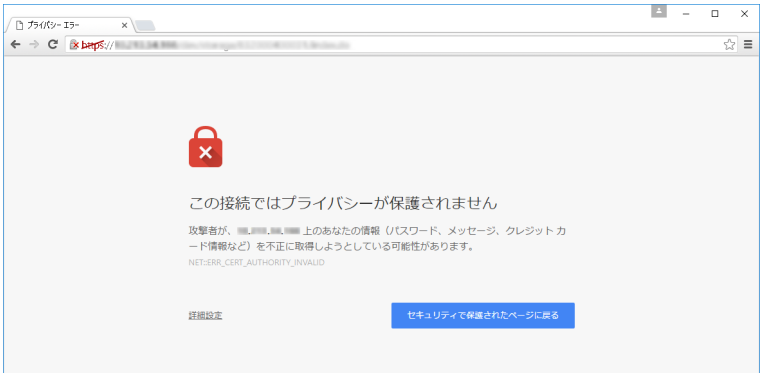
メモ

＜ Microsoft Edge の場合＞

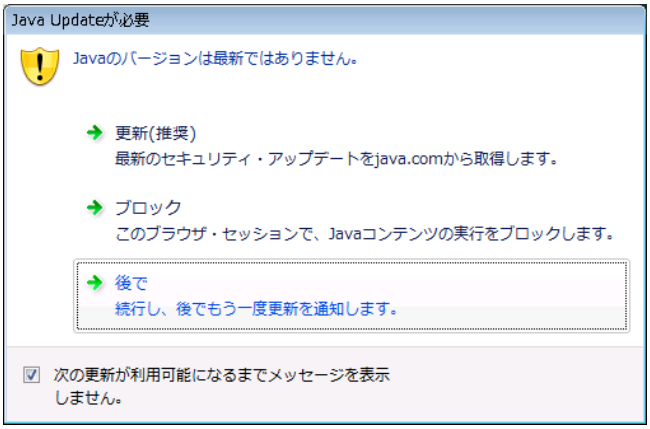
セキュリティ警告の［接続がプライベートではありません］画面が表示される場合は、［詳細設定］－［<IP アドレスまたはホスト名>に進む（安全ではありません）］をクリックしてください。

＜ Google Chrome の場合＞

プライバシーエラーの［この接続ではプライバシーが保護されていません］画面が表示される場合は、［詳細設定］－［<IP アドレス>にアクセスする（安全ではありません）］をクリックしてください。



13. ［Java Update Needed］画面が表示されます。［後で］をクリックします。



14. JAVA が起動します。

メモ

アプリケーションの実行中に、ファームウェア画面を開いた元の Maintenance Utility をログアウトまたはアプリケーションを強制終了する操作（PC シャットダウンなど）をしないでください。このような操作をした場合は、次回ログイン時 にメッセージ［32061-208063］が表示されることがあります。

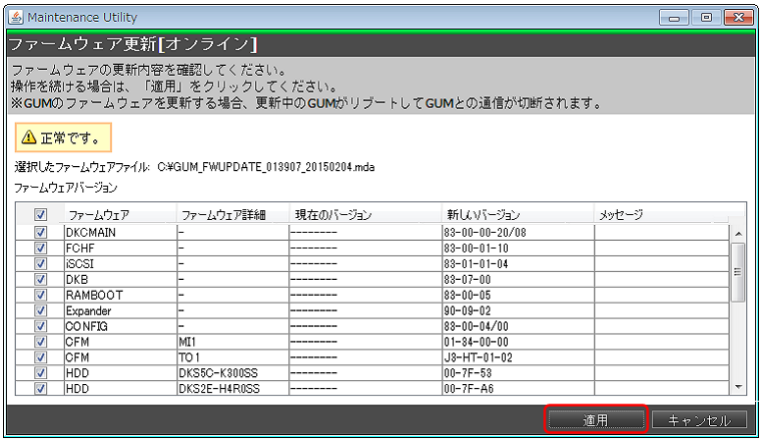
この状態に陥ったと思われる場合は、以下の対処方法を実施してください。

a. 新しく開いた Maintenance Utility 画面で、［ファームウェア更新］画面を開きます。

b. ［ファームウェア更新設定］画面が表示されることを確認します（ファームウェア更新の進捗画面が表示された場合は、ファームウェア更新が動作中ですので終了するまでお待ちください）。

c. システムロック強制解除を実行します（「3.12.5 システムロックの強制解除（92 ページ）」参照）。

15. ファームウェア更新画面が表示されるので、［適用］をクリックします。

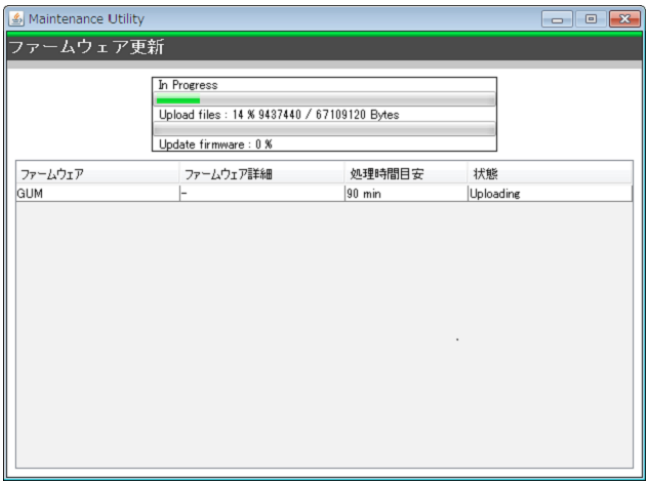


メモ

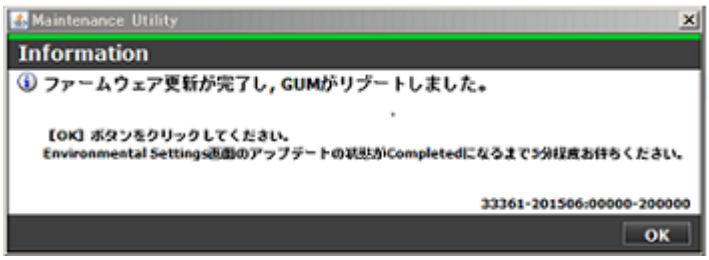
この画面で［キャンセル］をクリックした場合は、ファームウェア更新が完了しません。

ソフトウェア更新完了後にツールを終了し、再度ファームウェア更新を実行してください。

ファームウェア更新の進捗が表示されます。

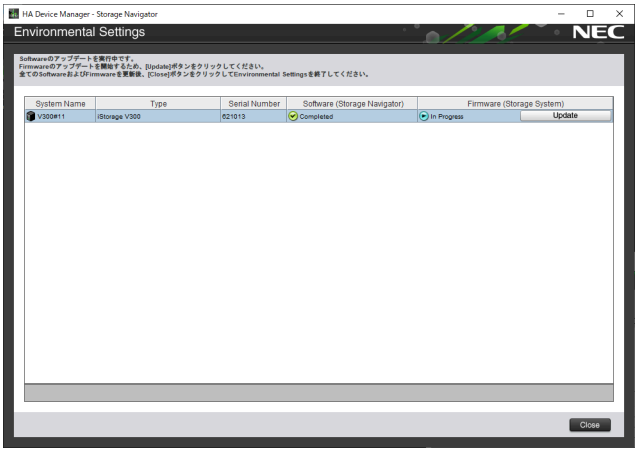


16. メッセージに対して［OK］ボタンをクリックします。
17. 進捗率画面の［×］ボタンをクリックします。
18. GUM のリブートが完了し、Environmental Settings 画面のアップデート状態が Completed になるまで、約 5 分程度待ってください。



19. ［Firmware (Storage System)］列で、ファームウェア更新の状態を確認します。

    ファームウェアの更新が完了するまで待ってください。

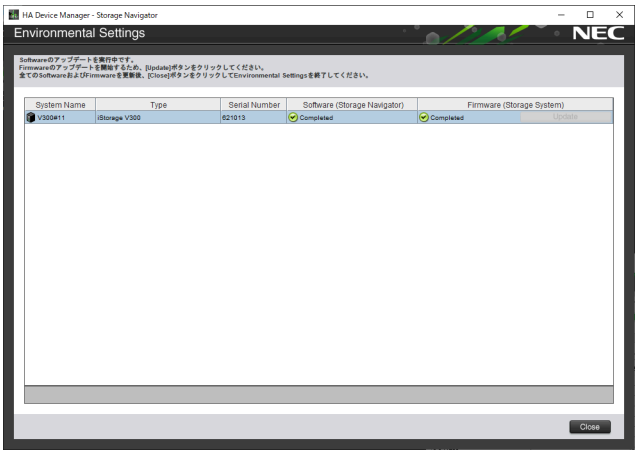


ファームウェア更新の状態は、次の状態があります。

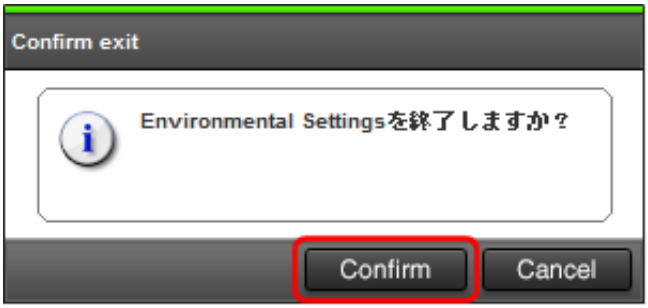
項目	内容
(Select Update)	ファームウェア更新画面の起動待ちです。

項目	内容
	［Update］をクリックしてファームウェア更新画面を表示してください。
In Progress	ファームウェア更新画面の起動後、ファームウェア更新が完了していません。 ファームウェア更新をキャンセルした場合でもこの状態になります。
Completed	ファームウェアの更新が完了しています。
Failed	ファームウェアの更新に失敗しました。 ［Update］をクリックしてファームウェア更新画面を表示してエラー内容を確認してください。
Communication Timeout	ファームウェアの更新が時間内（200 分）に完了したことを確認できていません。 ファームウェア更新画面から状態を確認してください。
(Not Update)	ファームウェア更新対象に選択されていません。

20. ソフトウェアおよびファームウェアの更新状態が［Completed］であることを確認し、［Close］をクリックします。



21. ［Confirm］をクリックして、ツールを終了します。



22. ［Storage Device List］画面で、ストレージシステムの［Start Service］をクリックしてサー ビスを開始します。

23. 手順 9 で［SVP が再起動したときに自動的にサービスを開始する］の設定を変更した場合は、元の設定に戻してください。

    方法は、「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。

メモ

ファームウェアの更新後に HA Storage Advisor Embedded をご使用する場合は、HA Storage Advisor Embedded を起動するブラウザのキャッシュをクリアしてください。

G.2.1.3 SSL 通信の署名付き証明書の再インストール

SSL 通信の署名付き証明書の状態を確認して、デフォルトの証明書に戻った場合は、証明書を再インストールします。

操作手順

1. SSL 通信の署名付き証明書の状態を確認します（「C.13 SVP と管理クライアント間の SSL 通信の証明書の確認（Microsoft Edge）（260 ページ）」または「C.14 SVP と管理クライアント間の SSL 通信の証明書の確認（Google Chrome）（261 ページ）」を参照）。
2. SSL 通信の署名付き証明書が、デフォルトの証明書に戻っていた場合、証明書を再インストールします。

   なお、証明書ファイルを再作成する場合は、「C.8 署名付きの信頼できる証明書を取得（255 ページ）」から「C.11 SVP と管理クライアント間の SSL 通信の署名付き証明書を SVP へアップロード（258 ページ）」を参照してください。

G.2.2 SVP の IP アドレスを変更

SVP の IP アドレスを変更した場合、Storage Device List に登録した IP アドレスを変更する必要があります。Windows の機能を使用して SVP の IP アドレスを変更したあと、以下の手順を実施してください。

なお、管理 LAN に接続している LAN ポートの IP アドレス（Storage Device List に表示されている IP アドレス）以外の LAN ポートの IP アドレスを変更した場合も、本項の操作を行ってください。ただし、操作手順 3.で IP アドレスを入力しなおす必要はありません。操作手順 4.に進み、［Apply］をクリックしてください。

前提条件

- ストレージシステムを Storage Device List に登録していないこと、または登録済みの場合はストレージシステムのサービスを停止していること。

メモ

ストレージシステム単位のサービスを停止する場合は、「G.2.6 ストレージシステム単位のサービスを停止（354 ページ）」を参照してください。

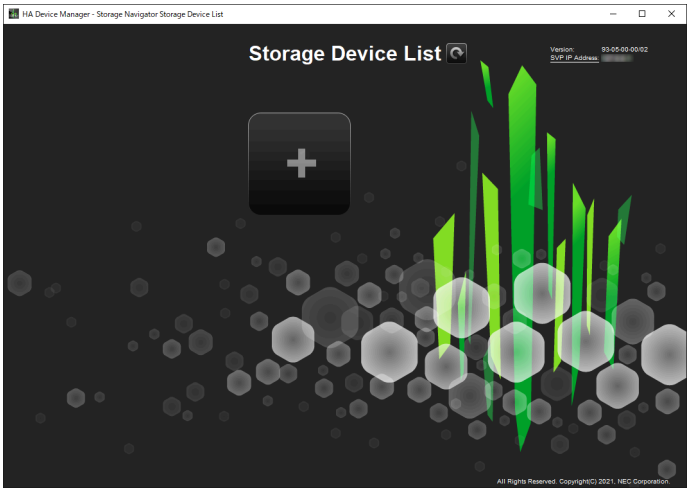
操作手順

1. Windows の［スタート］メニューから、［HA Device Manager - Storage Navigator］－［Storage Device List］を右クリックし、［管理者として実行］をクリックします。［管理者として実行］が表示されない場合は、［詳細］または［その他］－［ファイルの場所を開く］をクリックします。開かれたエクスプローラーにあるファイルを右クリックし、［管理者として実行］をクリックします。

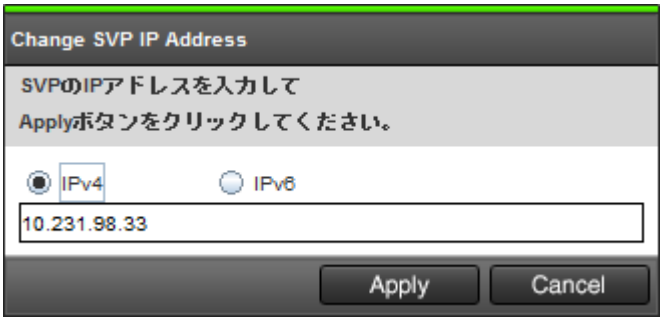
   ヒント

   SVP デスクトップ上の［Open StorageDeviceList］アイコンを右クリックして、［管理者として実行］を選択することでも Storage Device List を起動できます。

2. ［Storage Device List］画面が表示されます。右上の SVP IP Address のテキストリンクをクリックします。



3. ［Change SVP IP Address］画面が表示されます。



4. 変更後の IP アドレスを入力し［Apply］をクリックします。

   メモ

   ストレージシステムの各 CTL や管理クライアントと SVP を直結している場合は、ブリッジ接続時に設定した IP アドレスを入力してください。

5. ［Storage Device List］画面右上の［SVP IP Address］横に、変更後の IP アドレスが表示されていることを確認してください。

G.2.3 SVP へのストレージシステム追加登録

既存の SVP に管理対象のストレージシステムを追加したい場合は、ストレージシステムの追加登録が必要です。

⚠注意

- iStorage V100, V300 の場合、Storage Device List に、ストレージシステムを 1 台だけ登録できます。この Storage Device List に、別のストレージシステムを登録できません。また別の装置を管理している SVP の Storage Device List への移動もできません。
- インストール先のドライブの空き容量を、20GB 以上確保してください。
- 1 台の SVP から同時に起動できるストレージシステムの台数は、SVP のハードウェアに依存します。「1.6.2.1 SVP のハードウェア条件（19 ページ）」に示す SVP のハードウェア条件を参照して、同時に起動できるストレージシステムの台数を確認してください。
- ストレージシステムを起動すると、SVP 内で動作するプロセスに応じて、デスクトップヒープの消費量が増加します。「A.8 デスクトップヒープの指定値を変更する（206 ページ）」を参照してデスクトップヒープとして使用するメモリ領域を確保してください。

- 追加するストレージシステムのファームウェアバージョン（XX-nn-mm-xx/yy）と登録済みのストレージシステムのファームウェアバージョン（XX-nn-mm-xx/yy）の「XX,nn,mm,yy」が異なる場合

  SVP ファームウェアメディアを使用してセットアッププログラムを起動し、ストレージシステムを追加する。（SVP ソフトウェアのインストールが必要です。）

  設定方法は、「G.2.3.1 セットアッププログラムによるストレージシステム追加登録（334 ページ）」を参照してください。

- 追加するストレージシステムのファームウェアバージョン（XX-nn-mm-xx/yy）と登録済みのストレージシステムのファームウェアバージョン（XX-nn-mm-xx/yy）の「XX,nn,mm,yy」が同じ場合

  Storage Device List でストレージシステムを追加する。（SVP にインストール済みの SVP ソフトウェアが利用できます。）

  設定方法は、「G.2.3.2 Storage Device List によるストレージシステム追加登録（345 ページ）」を参照してください。

メモ

ファームウェアのバージョンは次に表示されます。

- 追加するストレージシステムのファームウェアバージョン

  Maintenance Utility の［管理］－［ファームウェア］を選択して表示する画面の［DKCMAIN］

- 登録済みのストレージシステムのファームウェアバージョン

  Storage Navigator のエクスプローラでストレージシステムを選択して表示する画面［ストレージシステム情報編集］の［ソフトウェアバージョン］の［Main］

G.2.3.1 セットアッププログラムによるストレージシステム追加登録

セットアッププログラムを使用して、SVP にストレージシステムを追加登録します。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、ストレージシステムの追加を行うこともできます。SVP に DVD ドライブが搭載されていない場合は、リモートデスクトップ接続して管理クライアントの DVD ドライブを使用します。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

前提条件

- ストレージシステムの電源が ON になっていること。
- ウィルス検出プログラムのサービスを停止していること。ウィルス検出プログラムが稼働している状態で実行すると、ストレージシステム追加登録のパフォーマンスが低下したり、正しく完了できない可能性があります。

操作手順

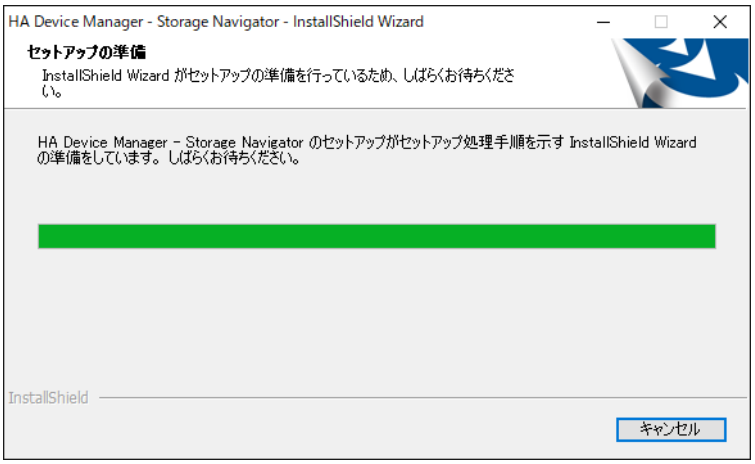
1. SVP ファームウェアメディアを、SVP の DVD ドライブに挿入します。

   メモ

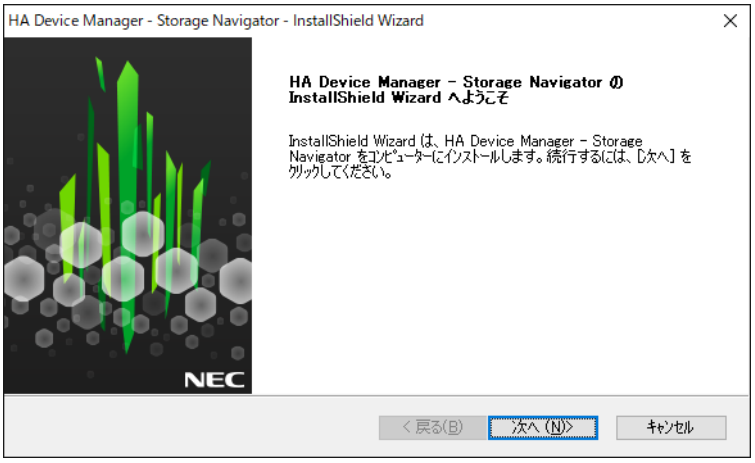
   SVP ファームウェアメディアを使用後、DVD ドライブからメディアを取り出して保管してください。

2. ドライブ直下の Setup.exe を右クリックし、[管理者として実行] をクリックします。

   インストール準備中画面が表示されます。準備が完了するまでお待ちください。



3. 準備が完了したら、Install Shield 画面が表示されます。[次へ] をクリックします。



4. OSS（Open Source Software）の使用許諾の確認画面が表示されます。

   ［使用許諾契約の全条項に同意します］を選択し、［次へ］をクリックします。

5. 既存の OSS のバージョンにより、インストールのスキップ、またはアップデートの確認メッセージが表示されるので、どちらの場合も［はい］をクリックします。

インストール済みの OSS のバージョンが SVP ファームウェアメディアからインストールするバージョンと同じ場合

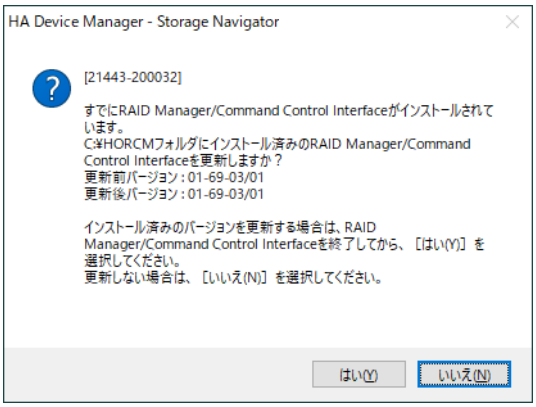
インストール済みの OSS のバージョンが SVP ファームウェアメディアからインストールするバージョンと一致していない場合

別途 RAID Manager をインストールしている場合は、ストレージ管理ソフトウェア同梱の RAID Manager での更新メッセージ“21443-200032” が表示されます。

RAID Manager をインストールしていない、またはインストールしたフォルダ(HORCM フォルダ)をリネームしている場合は表示されません。

更新する場合は、RAID Manager の使用を終了した後、［はい］ボタンをクリックしてください。［いいえ］ボタンをクリックすると RAID Manager のバージョンは維持されます。

複数の RAID Manager をインストールしている場合は、もっとも順番が前のドライブレターのドライブにインストールしている RAID Manager が更新対象となります。

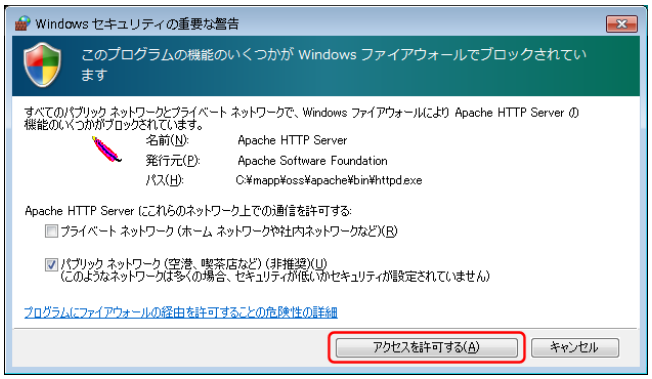


メッセージ画面に「注意」が表示されているときに［はい］ボタンをクリックすると、Windows の［コントロールパネル］－［プログラムと機能］には、すでにインストールされている RAID Manager のバージョンが表示され、変更後のバージョンは反映さ

れません。このため、ストレージ管理ソフトウェアのインストールが完了したら『RAID Manager インストール・設定ガイド』に示す RAID Manager のバージョン削除方法を参照して、コントロールパネルに表示されるバージョン情報を削除してください。

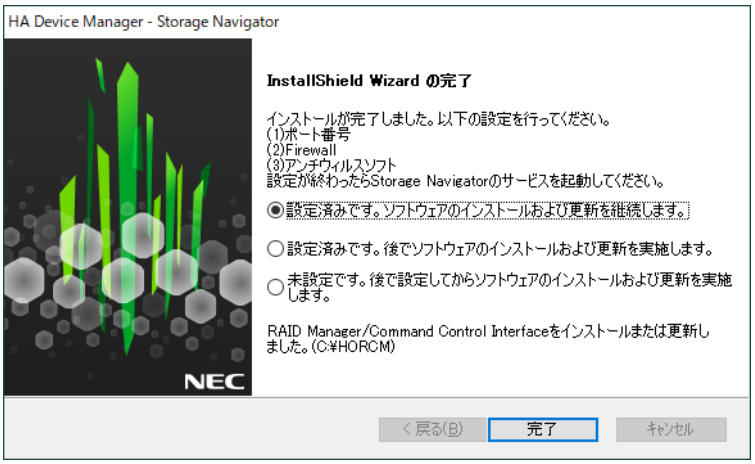
メモ

セキュリティ警告の画面が表示される場合は、［アクセスを許可する］をクリックしてください。



6. 完了メッセージが表示されます。

［設定済みです。ソフトウェアのインストールおよび更新を継続します。］を選択し、［完了］をクリックします。

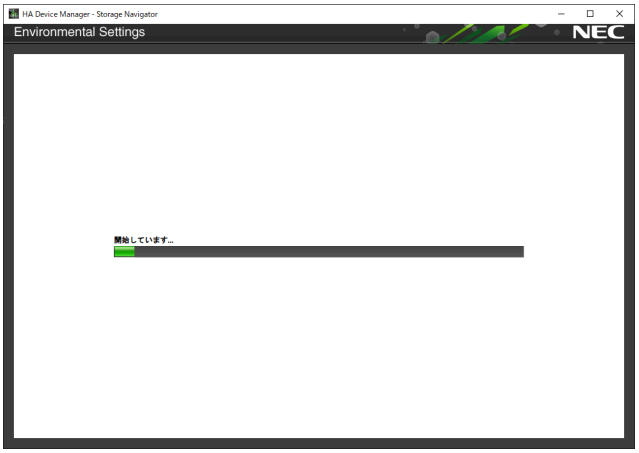


ストレージ管理ソフトウェアの更新が完了すると、Environmental Settings ツールが起動します。

メモ

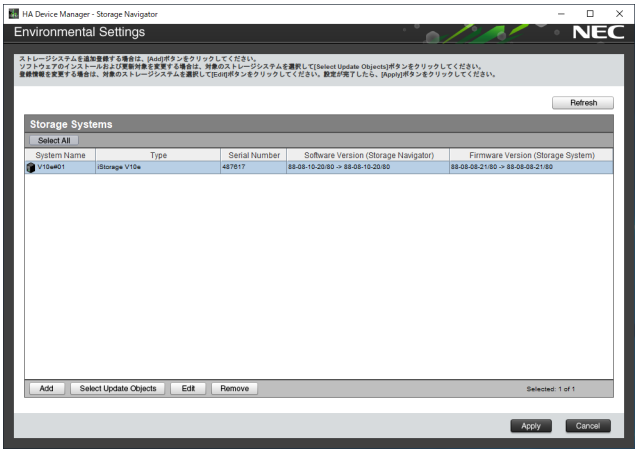
［設定済みです。後でソフトウェアのインストールおよび更新を実施します。］は選択しないでください。Environmental Settings ツールが起動しません。

更新準備中画面が表示されます。準備が完了するまで待ってください。



7. ［Environmental Settings］の画面に表示される登録済のストレージシステムに対して、SVP ソフトウェアとファームウェアのアップデートを回避する設定を行います。

   ［Environmental Settings］から登録済のストレージシステムを選択し、［Select Update Objects］をクリックします。



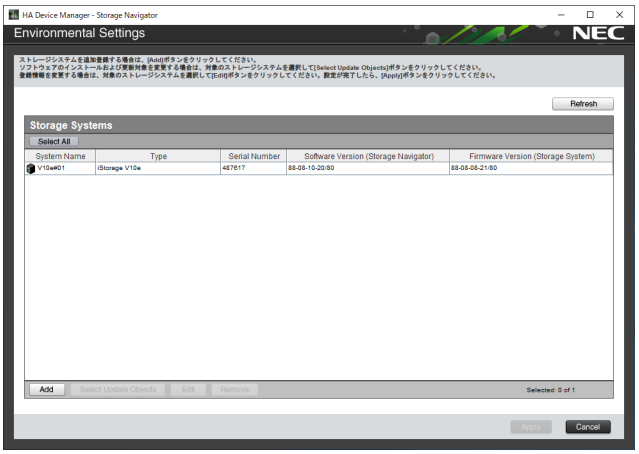
8. ［Select Update Objects］画面が表示されます。［Software(Storage Navigator)］と［Firmware(Storage System)］※双方のチェックを外します。

注※

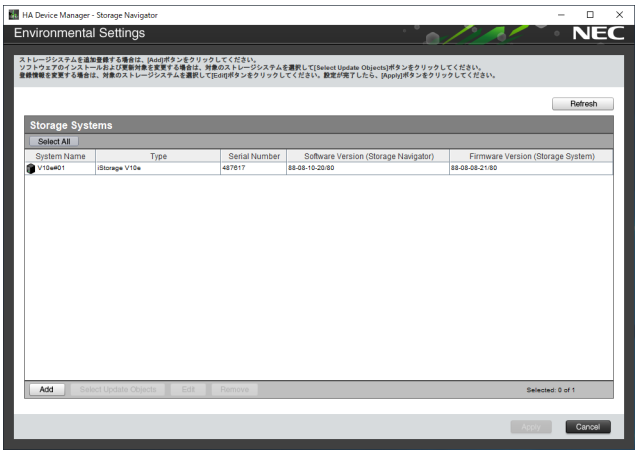
［Firmware （Storage System)］のチェックが最初から外れている場合があります。その場合はそのまま、［Apply］をクリックします。

9. ［Apply］をクリックして、［Environmental Settings］画面に戻ります。

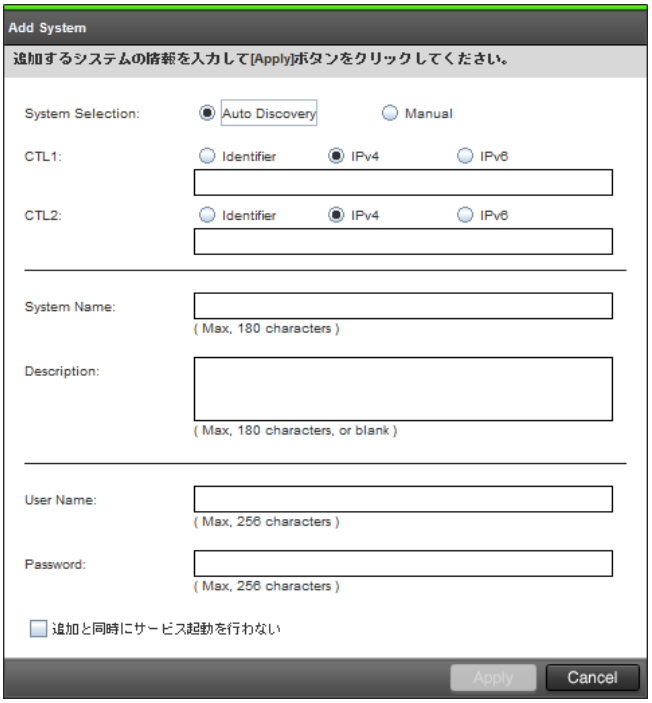
10. 登録済のすべてのストレージシステムに対して、手順 7～9 を行ってください。



11. ［Add］をクリックします。



12. ［Add System］画面が表示されます。次に従い各設定項目を入力して、［Apply］をクリックします。



項目	内容
System Selection	ストレージシステム情報の入力方法を選択します。 • ［Auto Discovery］(デフォルト選択) : ストレージシステム情報を自動で取得します。 • ［Manual］※1 : ストレージシステム情報を手動で設定します。
CTL1,CTL2	Maintenance Utility のネットワーク画面の CTL1 と CTL2 の IP アドレスを指定します。IP アドレスの代わりに DNS サーバに登録したホスト名でも指定できます。 ホスト名で指定する場合は、[Identifier]を選択し、DNS サーバに登録したホスト名を入力してください。なお、CTL1 と CTL2 に同じホスト名を指定できません。 SVP の Windows に対する設定も必要です。［コントロールパネル］から DNS サフィックスを追加する画面を表示して、CTL1、CTL2 に設定するホストのドメイン名を追加してください (「G.2.21 DNS サフィックスの設定 (393 ページ)」参照)。
System Name	ストレージシステムの表示名を設定します。 入力できる文字数は、半角文字で 180 文字までです。 使用可能文字：半角英数字と記号 (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~) 半角の空白は使用できません。
Description	ストレージシステムの説明を設定します。Description は、任意の項目です。 入力できる文字数は、半角文字で 180 文字までです。

項目	内容
User Name	ストレージシステムのユーザ名を入力します。 使用可能文字：半角英数字と記号（# $ % & ' * + - . / = ? @ ^ _ ` { | } ~）
Password	ストレージシステムのパスワードを入力します。
追加と同時にサービス起動を行わない※2※3	ストレージシステムを追加するのと同時にサービス起動するかを選択します。 （デフォルトはチェックなし）

注※1

保守員が手動で設定します。

ユーザは［Manual］を選択して設定しないでください。

注※2

複数台のストレージシステムを登録する場合は、このチェックボックスにチェックを入れて、追加と同時にサービスが開始されないように設定することを推奨します。

SVP の再起動時にストレージシステムのサービスを自動で開始させるための設定は、「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。

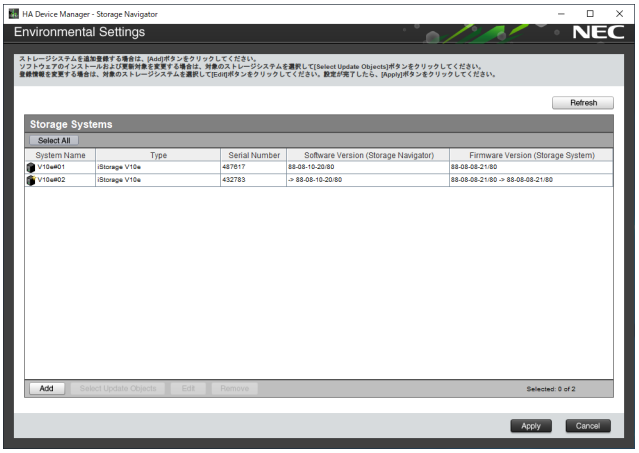
注※3

「G.2.3.2 Storage Device List によるストレージシステム追加登録（345 ページ）」と異なり、このチェックボックスをチェックすると、Storage Device List から起動される［Edit System］画面の［SVP 再起動時に自動でサービスを開始する］は、チェックが外れた状態で登録されます。

（デフォルトでは、チェックが入っています。詳細は、「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。）

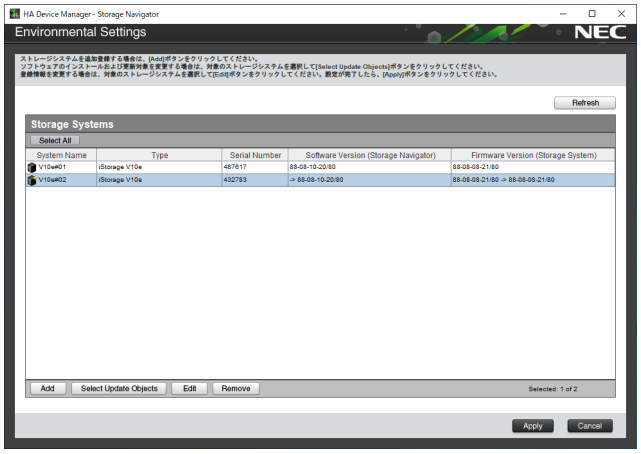
なお、ストレージシステムのサービスが起動されないと、エクスポートツール（ExportTool）は使用できません。

13. ［Environmental Settings］画面に入力したストレージシステムが追加されます。

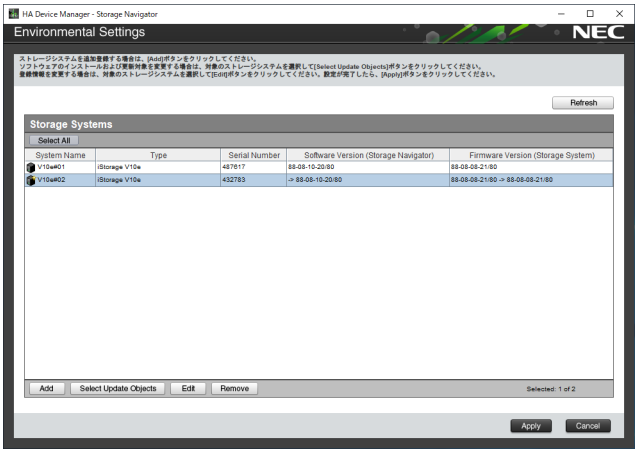


ヒント

間違ったストレージシステムを追加してしまった場合は、削除したいストレージシステムを選択して［Remove］をクリックしてください。



14. ［Environmental Settings］画面から、追加したストレージシステムを選択し、［Select Update Objects］をクリックします。



15. ［Select Update Objects］画面が表示されます。

［Firmware （Storage System)］※のチェックを外し、［Apply］をクリックします。

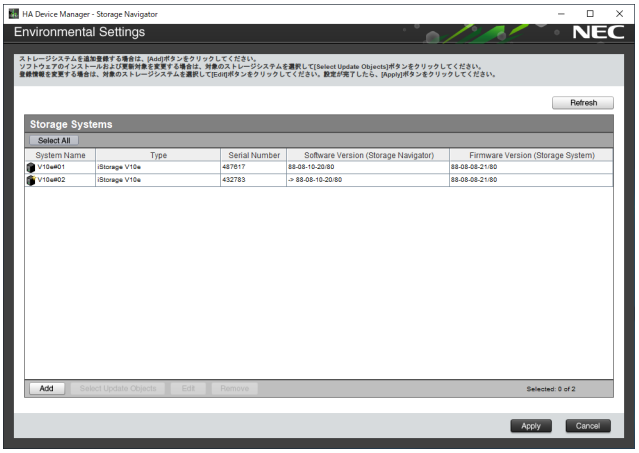
注※

［Firmware （Storage System)］のチェックが最初から外れている場合があります。その場合はそのまま、［Apply］をクリックします。

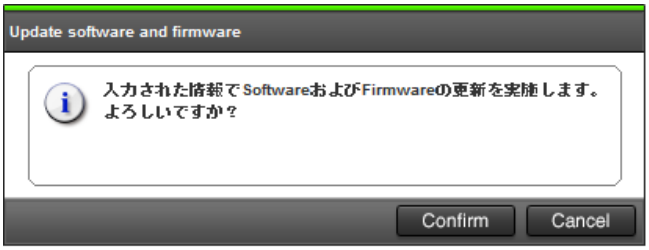
ヒント

登録するストレージシステムは自動的に［Software （Storage Navigator)］がチェックされ、変更できません。

16. 複数のストレージシステムを追加する場合は、手順 11～15 を繰り返してください。
17. ［Environmental Settings］画面の［Apply］をクリックします。

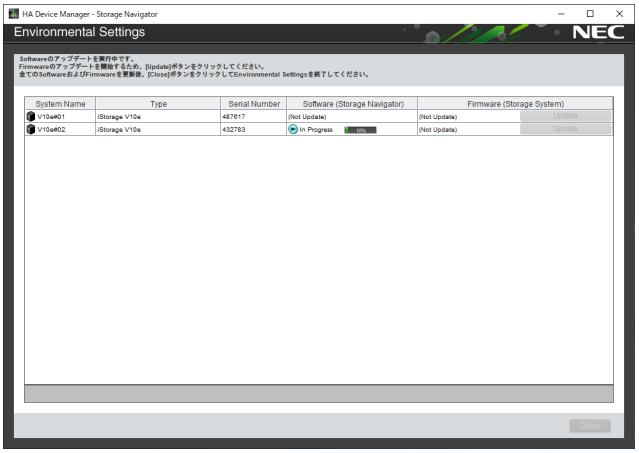


18. ［Update software and firmware］画面が表示されるので、［Confirm］をクリックします。



更新実行画面が表示され、ソフトウェアの更新が自動で開始されます。

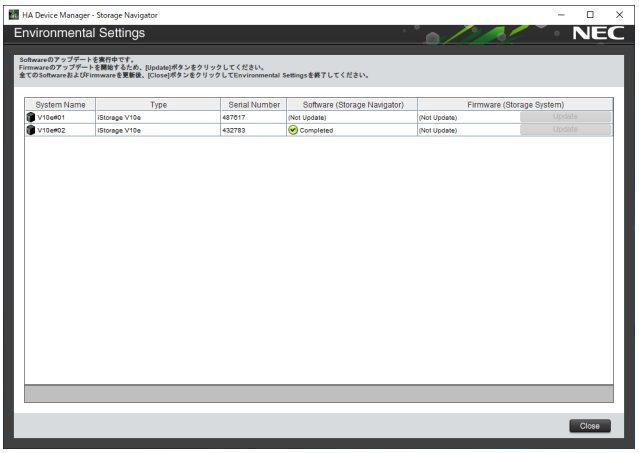
［Software （Storage Navigator)］列で、ソフトウェアの更新の状態が確認できます。



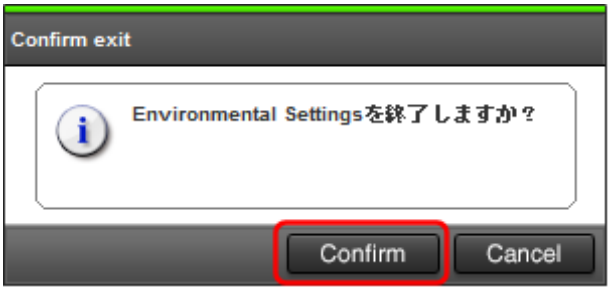
ソフトウェアの更新の状態は、以下の状態があります。

状態	内容
Waiting	ソフトウェアの更新を実施していません。 ソフトウェアの更新は 1 台ずつ実行されます。すでに別のストレージシステムのソフトウェアの更新が実行されている場合は、他のストレージシステムはこの状態になります。
In Progress	ソフトウェアの更新を実行中です。
Completed	ソフトウェアの更新が完了しています。
Failed	ソフトウェアの更新に失敗しました。 ストレージシステムを追加した場合は、追加が完了していない場合があります。クリックしてメッセージに従ってください。
(Not Update)	ソフトウェアの更新対象に選択されていません。 ストレージシステムを追加した場合は、この状態になることはありません。

19. ソフトウェアの更新状態が［Completed］であることを確認し、［Close］をクリックします。



20. ［Confirm］をクリックして、ツールを終了します。



21. 複数台のストレージシステムのサービスを同時に開始する場合は、「A.8 デスクトッププヒープの指定値を変更する（206 ページ）」を参照して指定値を変更します。

G.2.3.2 Storage Device List によるストレージシステム追加登録

Storage Device List を使用して SVP にストレージシステムを登録します。

⚠ 注意

次の条件の場合は、「G.2.3.1 セットアッププログラムによるストレージシステム追加登録（334 ページ）」に従ってください。次の条件の場合に、Storage Device List を使用して、SVP にストレージシステムを追加登録すると、ストレージシステムが正しく動作しないことがあります。

- 追加登録するストレージシステムのファームウェア※1 が、SVP に登録済のストレージシステムのファームウェア※2 のバージョンより新しい場合

注※1

追加登録するストレージシステムのファームウェアバージョンは、Maintenance Utility の［管理］－［ファームウェア］を選択して表示する画面の［DKCMAIN］で確認できます。

注※2

SVP に登録済のストレージシステムのファームウェアバージョンは、Storage Navigator のエクスプローラでストレージシステムを選択して表示する画面［ストレージシステム情報編集］の［ソフトウェアバージョン］の［Main］で確認できます。

メモ

ストレージ管理ソフトウェア、および SVP ソフトウェアの更新が完了していない状態で、この手順を使用してストレージシステムを登録すると、ストレージシステムが正常に動作しない場合があります。

この手順実施前に必ず「G.2.1 セットアッププログラムを使用したストレージ管理ソフトウェア、SVP ソフトウェア、ファームウェアの更新（316 ページ）」の手順でストレージ管理ソフトウェアの更新を実行してください。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、ストレージシステムの登録を行うこともできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

前提条件

- 登録するストレージシステムの電源が ON になっていること。

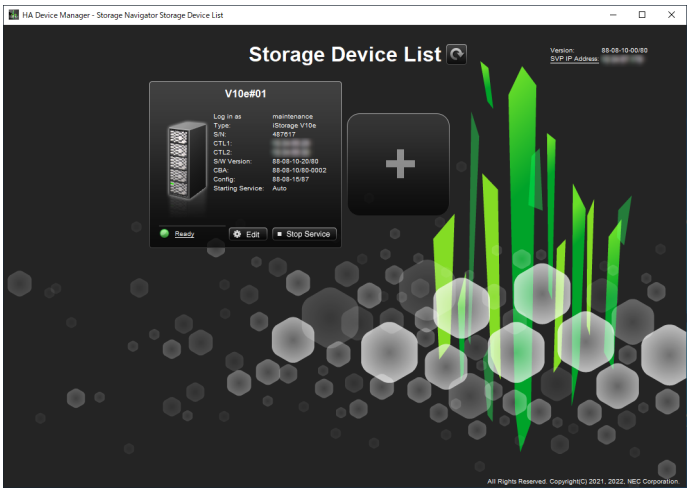
操作手順

1. SVP の Windows の［スタート］メニューから、［HA Device Manager - Storage Navigator］－［Storage Device List］を右クリックし、［管理者として実行］をクリックします。

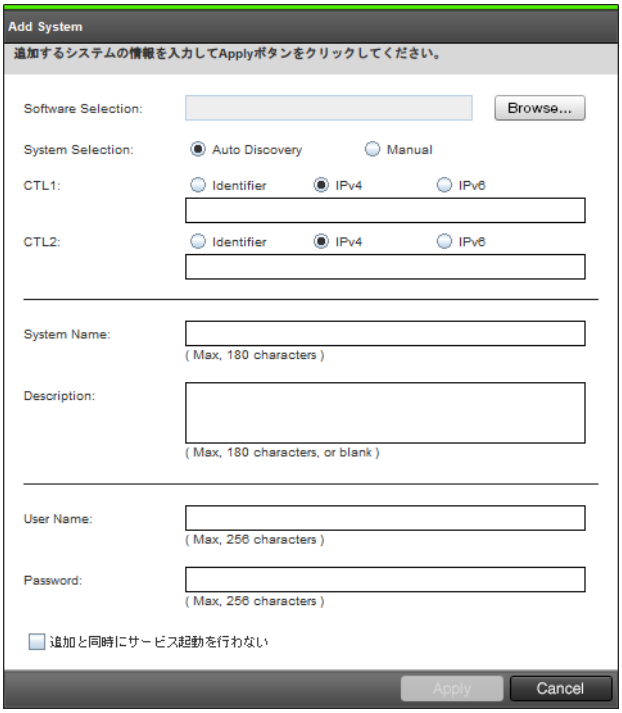
   ### ヒント

   SVP デスクトップ上の［Open StorageDeviceList］アイコンを右クリックして、［管理者として実行］を選択することでも Storage Device List を起動できます。

2. ［Storage Device List］画面が表示されます。［＋］ボタンをクリックします。



3. ［Add System］画面が表示されます。次の表に従い各設定項目を入力して、［Apply］をクリックします。



項目	内容
Software Selection	[Browse] をクリックして、SVP ファームウェアメディアの内容をコピーしたインストール作業用フォルダ内の `software\productname.inf` を指定し、インストール情報を取得します。
System Selection	ストレージシステム情報の入力方法を選択します。 • [Auto Discovery] (デフォルト選択) : ストレージシステム情報を自動で取得します。 • [Manual] ※1 : ストレージシステム情報を手動で設定します。
CTL1,CTL2	Maintenance Utility のネットワーク画面の CTL1 と CTL2 の IP アドレスを指定します。IP アドレスの代わりに DNS サーバに登録したホスト名でも指定できます。 ホスト名で指定する場合は、[Identifier]を選択し、DNS サーバに登録したホスト名を入力してください。なお、CTL1 と CTL2 に同じホスト名を指定できません。 SVP の Windows に対する設定も必要です。[コントロールパネル] から DNS サフィックスを追加する画面を表示して、CTL1、CTL2 に設定するホストのドメイン名を追加してください (「G.2.21 DNS サフィックスの設定 (393 ページ)」参照)。
System Name	ストレージシステムの表示名を設定します。 入力できる文字数は、半角文字で 180 文字までです。 使用可能文字 : 半角英数字と記号 (# $ % & ' * + - . / = ? @ ^ _ ` { | } ~) 半角の空白は使用できません。

項目	内容
Description	ストレージシステムの説明を設定します。 Description は、任意の項目です。 入力できる文字数は、半角文字で 180 文字までです。
User Name	ストレージシステムのユーザ名を入力します。 使用可能文字：半角英数字と記号（# $ % & ' * + - . / = ? @ ^ _ ` { | } ~）
Password	ストレージシステムのパスワードを入力します。
追加と同時にサービス起動を行わない※2※3	ストレージシステムを追加するのと同時にサービス起動するかを選択します。 （デフォルトはチェックなし）

注※1

保守員が手動で設定します。

ユーザは［Manual］を選択して設定しないでください。

注※2

複数台のストレージシステムを登録する場合は、このチェックボックスにチェックを入れて、追加と同時にサービスが開始されないように設定することを推奨します。

SVP の再起動時にストレージシステムのサービスを自動で開始させるための設定は、「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。

注※3

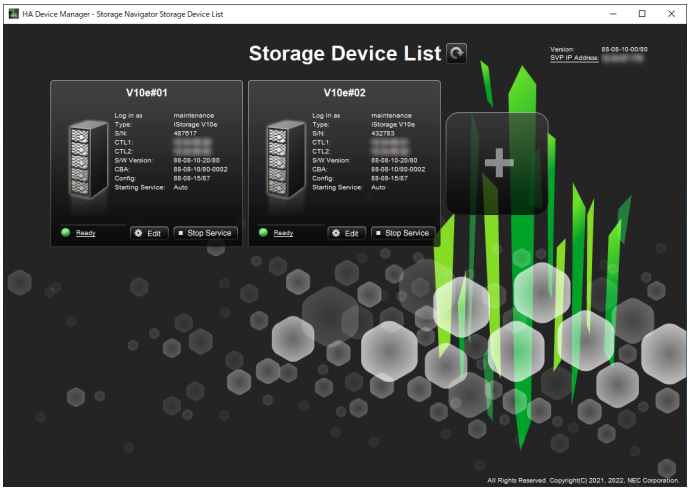
「G.2.3.1 セットアッププログラムによるストレージシステム追加登録（334 ページ）」と異なり、このチェックボックスをチェックしても、Storage Device List から起動される［Edit System］画面の［SVP 再起動時に自動でサービスを開始する］のチェックに影響を与えません。

（デフォルトでは、チェックが入っていますが、他のストレージシステムのバージョンや設定状態によって消えている場合もあります。詳細は、「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」を参照してください。）

なお、ストレージシステムのサービスが起動されないと、エクスポートツール（ExportTool）は使用できません。

4. 確認画面が表示されます。［Close］をクリックします。

登録されたストレージシステムが Storage Device List に表示されます。



ヒント

登録したストレージシステムを操作する場合は、「G.2.7 ストレージシステム単位のサービスの開始（354 ページ）」を実施してください。

G.2.4 Storage Device List を使用した SVP ソフトウェアの更新

SVP に登録されているストレージシステムの SVP ソフトウェアを更新する場合、Storage Device List から起動できます。

SVP ソフトウェアの更新は、新しいプログラムが入っている SVP ファームウェアメディア（メディア名称「装置添付ソフトウェア 1／2」）を使用します。SVP ソフトウェアの更新は、ストレージシステムのサービスを停止してから行います。

なお、ストレージ管理ソフトウェア、およびファームウェアの更新は Storage Device List から起動できません。Storage Device List による SVP ソフトウェアの更新の起動は、SVP ソフトウェアのバージョンと、ストレージ管理ソフトウェア、およびファームウェアのバージョンの対応を維持させるため、SVP ファームウェアメディアに格納されているファームウェアバージョン（XX-nn-mm-xx/yy）と、更新の対象となるストレージシステムの SVP 管理ソフトウェアのバージョン（XX-nn-mm-00/yy）の「XX,nn,mm,yy」が同じ場合のみ適用してください。

メモ

- 事前に SVP のソフトウェア設定情報をバックアップしてください（詳細は「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」を参照）。
- ストレージ管理ソフトウェアの更新が完了していない状態で、この手順を使用してストレージシステムを登録すると、ストレージシステムが正常に動作しない場合があります。
- この手順実施前に必ず「G.2.1 セットアッププログラムを使用したストレージ管理ソフトウェア、SVP ソフトウェア、ファームウェアの更新（316 ページ）」の手順でストレージ管理ソフトウェアの更新を実行してください。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、リモートで SVP ソフトウェアの更新を行うこともできます。SVP に DVD ドライブが搭載されていない場合は、リモートデスクトップ接続して管理クライアントの DVD ドライブを使用します。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

前提条件

- Windows のイベントビューアーが起動していないこと。

操作手順

1. SVP ファームウェアメディアを、SVP の DVD ドライブに挿入します。

   ### メモ

   SVP ファームウェアメディアを使用後、DVD ドライブからメディアを取り出して保管してください。

2. Windows の［スタート］メニューから、［HA Device Manager - Storage Navigator］－［Storage Device List］を右クリックし、［管理者として実行］をクリックします。［管理者として実行］が表示されない場合は、［詳細］または［その他］－［ファイルの場所を開く］をクリックします。開かれたエクスプローラーにあるファイルを右クリックし、［管理者として実行］をクリックします。

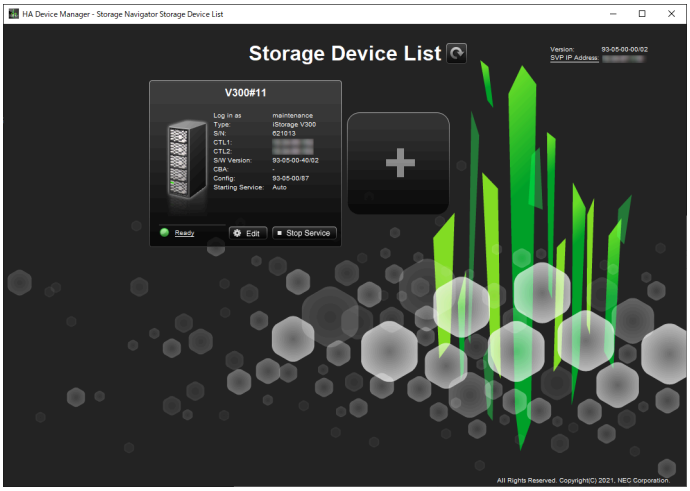
   ［Storage Device List］画面が表示されます。

   現在のソフトウェアバージョンを確認します。

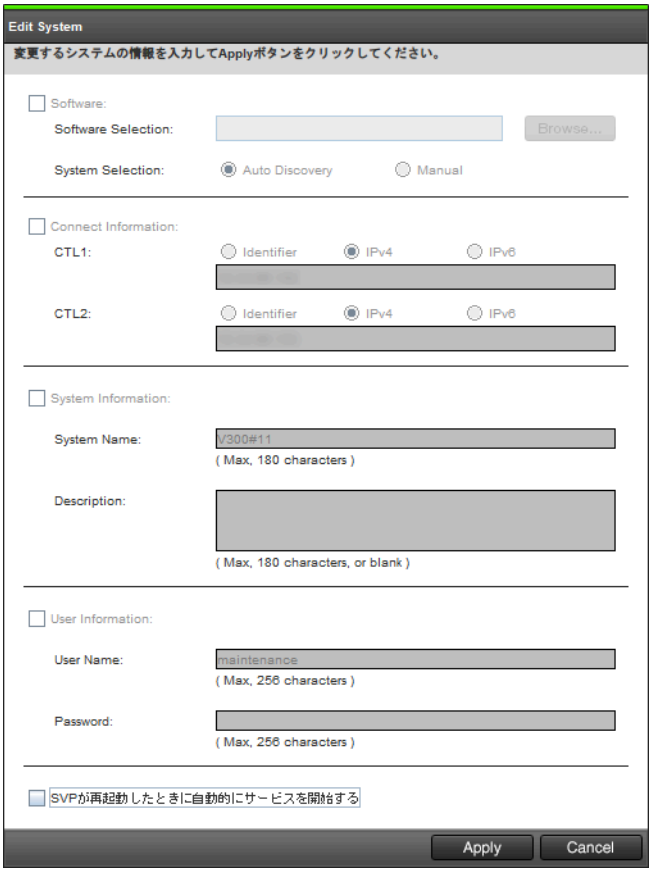
   ### ヒント

   SVP デスクトップ上の［Open StorageDeviceList］アイコンを右クリックして、［管理者として実行］を選択することでも Storage Device List を起動できます。

3. ストレージシステムのサービスを停止します（参照：「G.2.6 ストレージシステム単位のサービスを停止（354 ページ）」）。
4. ［Edit］をクリックします。



［Edit System］画面が表示されます。



5. ［Software］をチェックし、ソフトウェアのロケーションを指定します。

   ［Software Selection］で［Browse］をクリックします。

   インストール作業用フォルダの“Software\productname.inf”を指定します。

   メモ

   ［System Selection］の［Manual］を選択して設定しないでください。

6. ［Apply］をクリックします。

G.2.5 Storage Device List からストレージシステム情報を変更

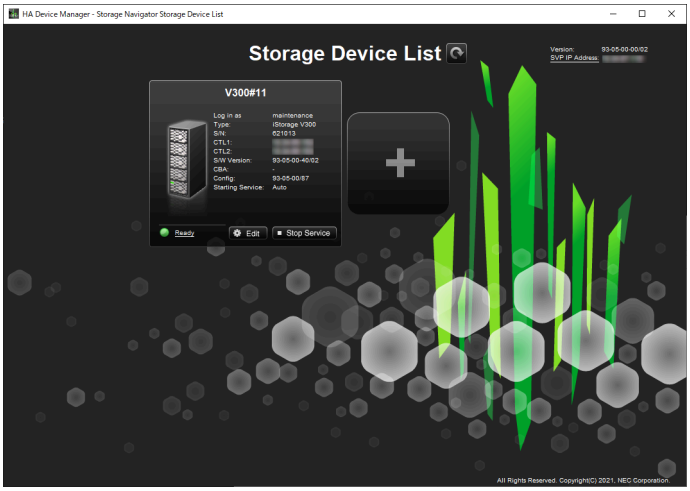
お客様の環境に合わせて変更してください。

前提条件

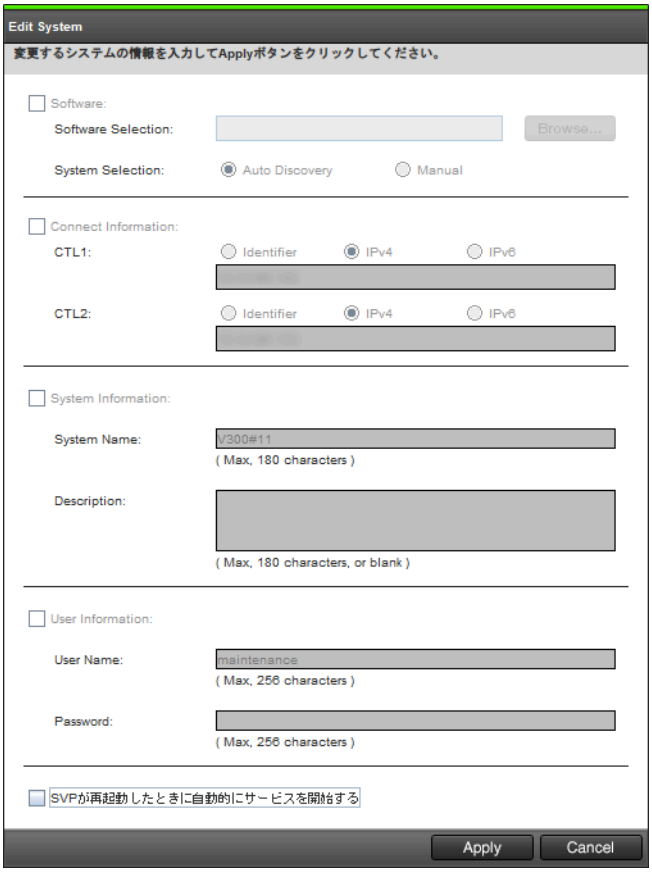
- Windows のイベントビューアーが起動していないこと。
- Storage Navigator のサービスが停止していること。

操作手順

1. ［Storage Device List］画面で、編集するストレージシステムの［Edit］をクリックします。



［Edit System］画面が表示されます。



2. 変更事項を入力し、［Apply］をクリックします。

メモ

- ［Software］を変更する場合は、［System Selection］の［Manual］を選択して設定しないでください。
- SVP の再起動時にストレージシステムのサービスを自動で開始させる場合は、［SVP が再起動したときに自動的にサービスを開始する］をチェックしてください。
- ［CTL1］と［CTL2］には、Maintenance Utility のネットワーク画面の CTL1 と CTL2 の IP アドレスを指定します。IP アドレスの代わりに DNS サーバに登録したホスト名でも指定できます。Storage Navigator のサービスを起動する前に、DNS サーバへ「A.4.1 ストレージシステムと SVP の IP アドレスを設定する（182 ページ）」で設定した IP アドレスと、ホスト名を登録してください。ホスト名で指定する場合は、[Identifier]を選択し、DNS サーバに登録したホスト名を入力してください。なお、CTL1 と CTL2 に同じホスト名を指定できません。

  ストレージシステムを、ホスト名で登録している場合、SVP の Windows に設定が必要です。DNS サフィックスに、CTL1、CTL2 に設定しているホストのドメイン名を追加してください（「G.2.21 DNS サフィックスの設定（393 ページ）」を参照）。

  DNS サーバに登録済の CTL1 と CTL2 の IP アドレスを変更した場合は、DNS サーバの設定変更後に、SVP のコマンドプロンプトで「ipconfig /flushdns」コマンドを実行して

ください。このコマンドを実行しない場合、SVP の DNS キャッシュが最大 1 時間クリアされないため、SVP からストレージシステムに接続できません。

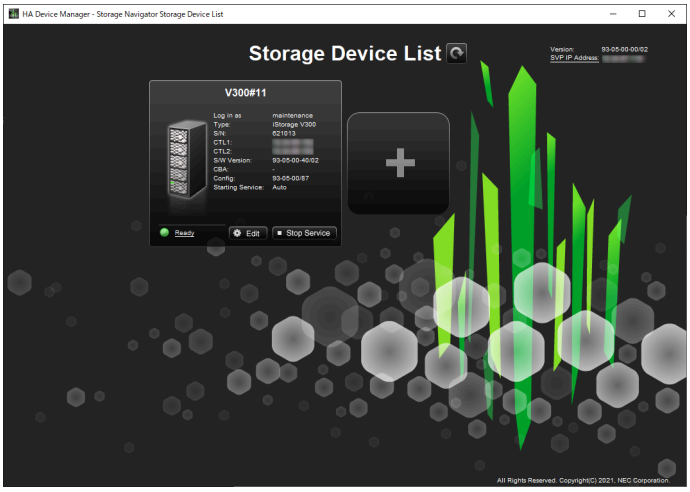
G.2.6 ストレージシステム単位のサービスを停止

次の場合は、Storage Device List でサービス状態が［Ready］のストレージシステムをすべて停止する必要があります。

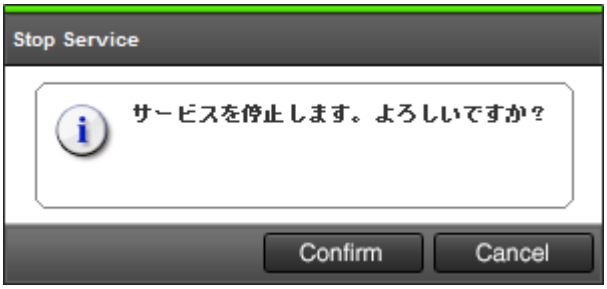
- SVP のソフトウェアを更新する。
- SVP のソフトウェア設定情報をバックアップする。
- SVP のソフトウェア設定情報をリストアする。

操作手順

1. ［Storage Device List］画面で、サービスを停止するストレージシステムの［Stop Service］をクリックします。



2. ［Confirm］をクリックします。



G.2.7 ストレージシステム単位のサービスの開始

［Storage Device List］画面で、目的のストレージシステムの［Start Service］をクリックして、サービスを開始します。サービス状態が［Ready］になることを確認してください。

複数台のストレージシステムのサービスを、同時に開始できます。

詳細は、「4.2 ストレージシステムのサービスを開始できる台数（96 ページ）」を参照してください。

G.2.8 Storage Device List からストレージシステムの削除

登録したストレージシステムを削除するには、ストレージシステムのサービスを停止してから行います。

前提条件

- Windows のイベントビューアーが起動していないこと。
- 削除するストレージシステムの装置識別番号と同じ名称のフォルダ、およびその配下のフォルダやファイルに対して、フォルダを開く、ファイルを開く、コマンドプロンプトのカレントディレクトリを移動するなどの操作をしていないこと。

操作手順

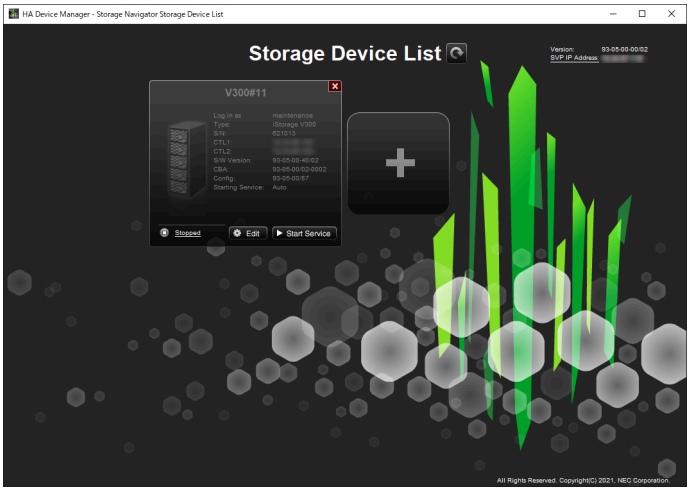
1. Windows の［スタート］メニューから、［HA Device Manager - Storage Navigator］－［Storage Device List］を右クリックし、［管理者として実行］をクリックします。［管理者として実行］が表示されない場合は、［詳細］または［その他］－［ファイルの場所を開く］をクリックします。開かれたエクスプローラーにあるファイルを右クリックし、［管理者として実行］をクリックします。

   ［Storage Device List］画面が表示されます。

   ヒント

   SVP デスクトップ上の［Open StorageDeviceList］アイコンを右クリックして、［管理者として実行］を選択することでも Storage Device List を起動できます。

2. ストレージシステムのサービスを停止します（参照：「G.2.6 ストレージシステム単位のサービスを停止（354 ページ）」）。
3. 削除するストレージシステムの［×］をクリックします。



G.2.9 SVP のソフトウェア設定情報のバックアップとリストア

SVP の障害に備えて、SVP にインストールされているソフトウェアの各種設定情報をバックアップしてください。障害復旧後の SVP、あるいは代替えの SVP にリストアすることで、元の設定に復元できます。

G.2.9.1 SVP のソフトウェア設定情報のバックアップ

SVP のバックアップを作成しておくことにより、SVP の故障時に、新しい SVP にバックアップした設定をリストアすることができます（「G.2.9.2 SVP のソフトウェア設定情報のリストア（359 ページ）」参照）。

⚠ 注意

- 初期設定作業で、「A.8 デスクトップヒープの指定値を変更する（206 ページ）」を実施していた場合、リストア後に、初期設定作業時に指定した値で「A.8 デスクトップヒープの指定値を変更する（206 ページ）」を再実施してください。
- Storage Navigator のタスク一覧画面の更新間隔は、ログイン中のユーザーに有効である為、バックアップ対象ではありません。『HA Device Manager - Storage Navigator ユーザガイド』の「[タスク] 画面の自動更新間隔を設定する」を参照してください。

⚠ 注意

以下の表に示す情報はバックアップ対象外です。必要に応じて、対応欄に示す方法で保管または再登録を実施してください。

	内容	対応
1	管理サーバ（SVP）に登録したストレージシステム情報	「A.7 管理サーバ（SVP）にストレージシステムを登録する（199 ページ）」を参照して再度登録ください。
2	ストレージシステムの構成レポート	『HA Device Manager - Storage Navigator ユーザガイド』を参照して適宜ダウンロードして保管ください。

	内容	対応
3	「SVP 接続」用証明書および「Web サーバ」接続用証明書	「C.16 SVP 接続用証明書を SVP へアップロード（262 ページ）」と「C.18 Web サーバ接続用証明書を SVP へアップロード（263 ページ）」を参照して再度アップロードください。
4	SVP への HTTP 通信を拒否する設定※1	「C.21 SVP への HTTP 通信を拒否（266 ページ）」を参照して再度設定ください。
5	HSTS の設定	「C.23 HSTS を有効化する（267 ページ）」を参照して再度設定ください。
6	デスクトップヒープの指定値	「A.8 デスクトップヒープの指定値を変更する（206 ページ）」を参照して再度設定ください。
7	Storage Navigator のタスク一覧画面の更新間隔	『HA Device Manager - Storage Navigator ユーザガイド』を参照して再度設定ください。
8	Log Dump の自動採取機能で採取したダンプ	「G.2.15.1 Log Dump 自動採取機能の仕様（368 ページ）」を参照して適宜ダンプを保管ください。
9	SVP に保存された監査ログ	「J.1 SVP に保存された監査ログをエクスポートする（407 ページ）」を参照して適宜エクスポートして保管ください。
10	RAID Manager の設定情報	『RAID Manager インストール・設定ガイド』を参照して適宜構成定義ファイルを保管ください。
11	Performance Monitor のモニタリングデータ	『Performance Manager (Performance Monitor, Server Priority Manager, QoS) ユーザガイド』を参照して適宜モニタリングデータを保管ください。

注※1

iStorage V100, V300 の SVP ソフトウェアでは、バックアップ/リストアされます。

バックアップ/リストアされる情報

- Storage Navigator が内部的に使用する設定情報
- 認証サーバへの接続設定
- 管理クライアント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
- Storage Navigator のユーザごとの画面表示（テーブル幅）の設定
- Storage Navigator のログイン画面の警告文
- Storage Navigator のタスクの自動削除設定情報
- Storage Navigator のタスク
- SVP-管理クライアント間の SSL 通信に関する情報（証明書情報など）
- SVP で使用するポート番号
- RSA 鍵交換設定
- SVP への HTTP 通信を拒否する設定※1
- DHE 鍵の下限長設定※2

注※1

iStorage V100, V300 の SVP ソフトウェアでは、バックアップ/リストアされます。

注※2

iStorage V10e の SVP ソフトウェアでは、バックアップ/リストアされます。

前提条件

- 操作の対象となる SVP に登録されているすべてのストレージシステムのサービスが停止していること（「G.2.6 ストレージシステム単位のサービスを停止（354 ページ）」参照）。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappBackup.bat ［バックアップファイルの格納先パス（絶対パス指定）\ファイル名］
   ```

   ［］内：引数

   SVP ソフトウェアの設定情報をリストアする場合、リストアするバックアップファイルは、リストア先の SVP ソフトウェアと同じバージョンの SVP ソフトウェアで取得したバックアップファイルを使用します。このためファイル名に、SVP ソフトウェアのバージョンの先頭 8 桁を指定することを推奨します。（SVP ソフトウェアのバージョンの確認方法は「G.2.4 Storage Device List を使用した SVP ソフトウェアの更新（349 ページ）」の操作手順 2.を参照）。

   引数を指定した場合は、拡張子 tgz ファイルが指定したパスに指定したファイル名で作成されます。

   引数を指定しない場合は、“C:\Mapp\wk\Supervisor\MappIniset”下にファイル名 Logs[YYYYMMDDhhmmss].tgz のバックアップファイルを作成します。バックアップファイル名の“YYYYMMDDhhmmss”は、作成年月日と時間を示します。

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. バックアップの実行確認メッセージが表示されます。

   処理を続行する場合、[y] を入力してから Enter キーを押してください。処理を取り消す場合、[n] を入力してから Enter キーを押してください。

   実行確認メッセージの内容については、「G.2.9.2 SVP のソフトウェア設定情報のリストア（359 ページ）」の注意を参照してください。

4. バックアップ完了メッセージが表示されます。
5. 任意のキーを入力し、メッセージを終了させ、コマンドプロンプトを閉じます。
6. 作成したバックアップファイルを、ほかの PC や USB メモリなどの外部記憶装置に保存します。バックアップファイルの内容は編集しないでください。

G.2.9.2 SVP のソフトウェア設定情報のリストア

SVP の故障時など SVP を交換する場合に、「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」で作成したバックアップを使用して新しい SVP に各種設定情報をリストアすることができます。

⚠ 注意

SVP ソフトウェアの設定情報をリストアする場合、リストアするバックアップファイルは、リストア先の SVP ソフトウェアと同じバージョンの SVP ソフトウェアで取得したバックアップファイルを使用してください。

前提条件

- バックアップを取得した SVP に登録していたストレージシステムを、新しい SVP に登録していること（「A.7 管理サーバ（SVP）にストレージシステムを登録する（199 ページ）」参照）。
- 操作の対象となる SVP に登録されているすべてのストレージシステムのサービスが停止していること（「G.2.6 ストレージシステム単位のサービスを停止（354 ページ）」参照）。

操作手順

1. バックアップファイルを SVP の任意のフォルダにコピーします。
2. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
3. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappRestore.bat ［バックアップファイルの格納先パス（絶対パス指定）\ファイル名］
   ```

[] 内：引数

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

4. リストア完了メッセージが表示されます。
5. 任意のキーを入力しメッセージを終了させ、コマンドプロンプトを閉じます。
6. Storage Device List に登録されている各ストレージシステムに対して、ポート番号を再割り振りします（「L.4 自動割り振りされたポート番号を再割り振りする（416 ページ）」を参照）。
7. SVP の起動時にサービスを自動で起動させたいストレージがある場合は、当該ストレージに対してサービスの自動起動を設定します（「G.2.5 Storage Device List からストレージシステム情報を変更（352 ページ）」参照）。
8. SVP を再起動します（「G.1.3 SVP を再起動する（315 ページ）」参照）。

G.2.10 ストレージ管理ソフトウェア、および SVP ソフトウェアの削除（アンインストール）

メモ

- ストレージ管理ソフトウェア、および SVP ソフトウェアを削除する場合は、本マニュアルに記載された手順に従ってください。

  事前に SVP のソフトウェア設定情報をバックアップしてください（詳細は「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」を参照）。

  Windows エクスプローラー、あるいはコマンドプロンプトなどから直接フォルダおよびファイルの削除はしないでください。

  誤って削除してしまった場合の対処方法は、「5.4.1 ストレージ管理ソフトウェアおよび SVP ソフトウェア インストール時のトラブルシューティング（107 ページ）」を参照してください。
- ストレージ管理ソフトウェア、および SVP ソフトウェアを削除（アンインストール）する前に、必ず、以下の状態であることを確認してください。
  - インストール先フォルダ、およびサブフォルダをエクスプローラーで開いていないこと
  - インストール先フォルダ、およびサブフォルダ配下のファイルをアプリケーションで開いていないこと
  - インストール先フォルダ、およびサブフォルダをカレントディレクトリとして、コマンドプロンプトを開いていないこと

デフォルトのインストール先フォルダは「C:\Mapp」です。フォルダおよびファイルを開いている状態で削除（アンインストール）するとエラー（21443-200017）が発生することがあります。このエラーが発生したあとにフォルダおよびファイルを閉じても、削除（アンインストール）が失敗します。対処方法は、「5.4.1 ストレージ管理ソフトウェアおよび SVP ソフトウェア インストール時のトラブルシューティング（107 ページ）」を参照してください。

- ストレージ管理ソフトウェアを削除する前に、「L.5 自動割り振りされたポート番号を初期化する（417 ページ）」を実行してください。
- ストレージ管理ソフトウェアを削除後に、不要なファイアウォールの受信の規則を削除してください。

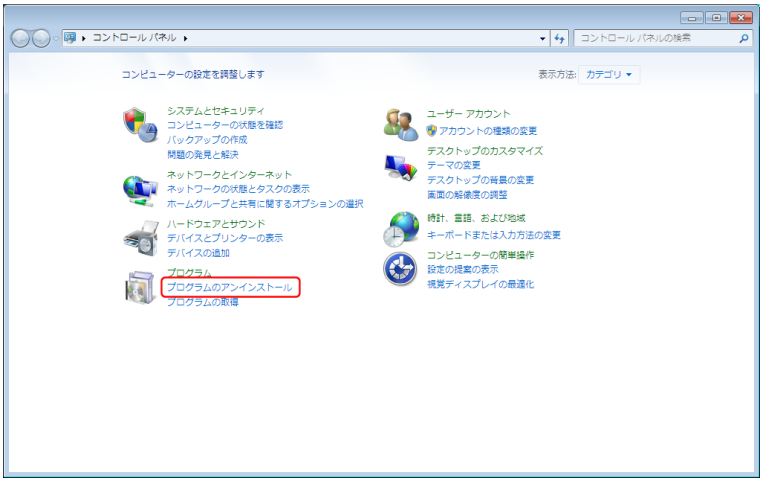
  Windows のスタートメニューより、［コントロールパネル］－［システムとセキュリティ］－［Windows ファイアウォール］－［詳細設定］－［受信の規則］
- RAID Manager の操作を行ったコマンドプロンプトを閉じてから、ストレージ管理ソフトウェアを削除してください。コマンドプロンプトを閉じていない場合は、削除が失敗します。
- ストレージ管理ソフトウェアに同梱された RAID Manager 以外の RAID Manager をインストールしている場合は、ストレージ管理ソフトウェアを削除しても RAID Manager は削除されません。
- ストレージ管理ソフトウェアと異なるドライブレターのドライブに RAID Manager をインストールすると、ストレージ管理ソフトウェアをインストールしていたドライブの直下に HORCM フォルダが残る場合があります。Windows エクスプローラーを使用して、手動で削除してください。

前提条件

- Windows のイベントビューアーが起動していないこと。
- RAID Manager を起動していないこと。
- RAID Manager の操作を行ったコマンドプロンプトを閉じていること。

操作手順

1. Windows の［スタート］メニューから、［コントロールパネル］をクリックします。
2. ［プログラムのアンインストール］アイコンをクリックします。



3. ストレージ管理ソフトウェアを選択し、[アンインストール] をクリックします。アンインストール実行時に Windows のユーザーアカウント制御（UAC）画面が表示された場合は、[続行] または [はい] をクリックしてください。

   アンインストール準備中の画面が表示されます。

   ストレージ管理ソフトウェア、および SVP ソフトウェアに同梱された RAID Manager 以外の RAID Manager をインストールしていなければ、ストレージ管理ソフトウェア、および SVP ソフトウェア同梱の RAID Manager の削除メッセージが表示されます。RAID Manager のフォルダにお客様が作成したスクリプトがある場合は、別のフォルダに退避した後、[Yes] をクリックしてください。

4. ストレージ管理ソフトウェア、および SVP ソフトウェアを完全に削除するかどうか、確認画面が表示されます。[はい] をクリックします。

5. システム情報のダンプ採取確認画面が表示されます。

   - すでにダンプ採取済みの場合は、[OK] をクリックしてください。
   - ダンプ採取していない場合は、ダンプの採取をしてから [OK] をクリックしてください。（「5.11.1 ダンプツールを使用した採取（163 ページ）」参照）

6. アンインストールの完了画面が表示されます。[完了] をクリックします。

G.2.11 OSS のバージョン確認

SVP が使用している Apache、OpenSSL、Jetty、Java または JRE、Perl のバージョンを確認することができます。

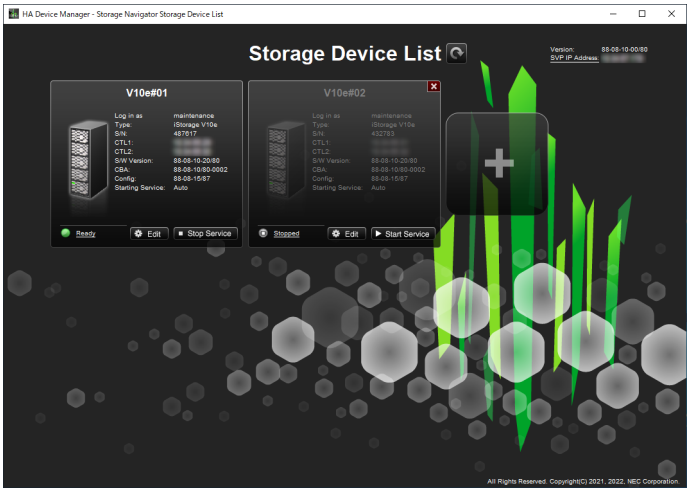
SVP が使用している OSS のバージョンを確認する場合は、“<SVP のインストール先のディレクトリ>\OSS\OSS_Version.txt”のテキストを参照してください。

G.2.12 ストレージシステムの切り替え

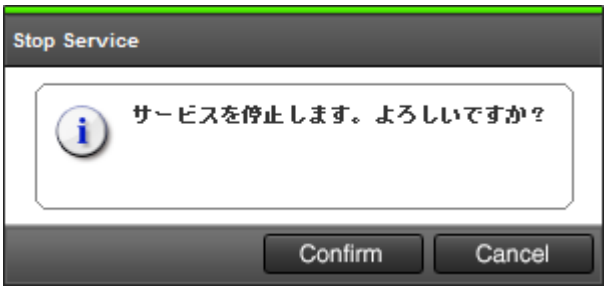
ストレージシステムのサービスを同時に開始できない場合は、ストレージシシステムを切り替えてください。

操作手順

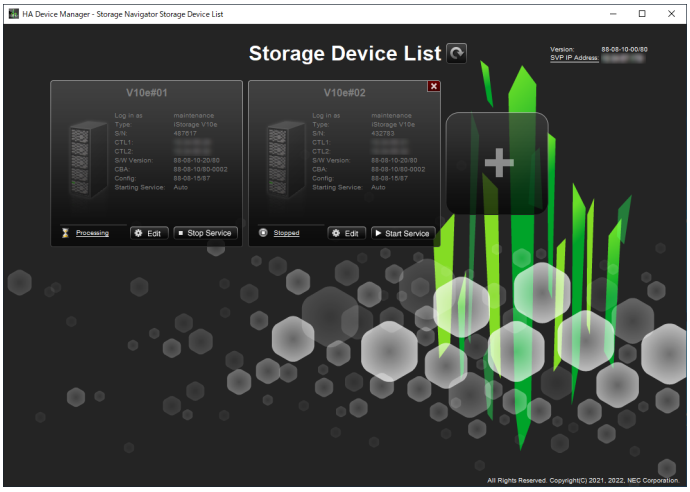
1. ［Storage Device List］画面の既にサービスが起動しているストレージの［Stop Service］をクリックします（起動しているストレージが存在しない場合はこの操作をスキップして手順 4 以降を実行します）。



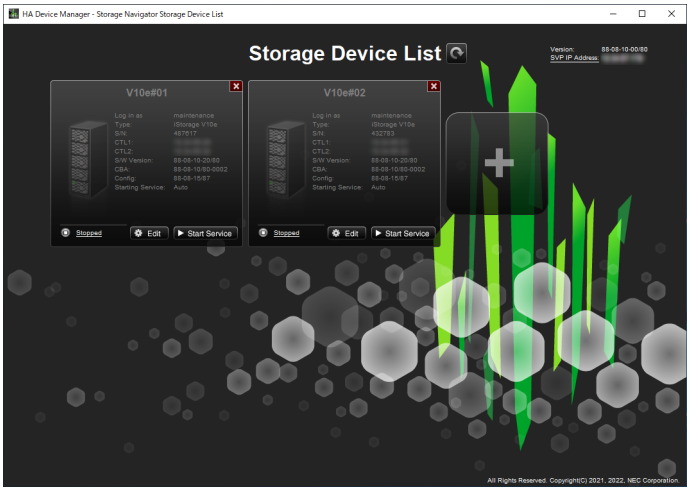
2. 確認メッセージが表示されます。［Confirm］をクリックします。



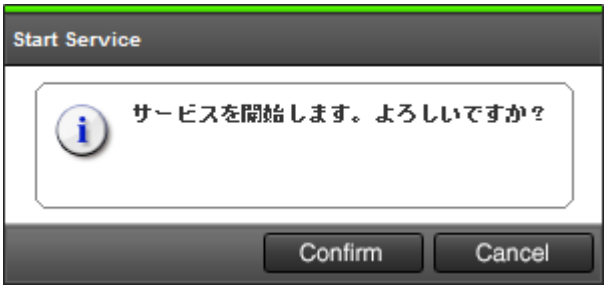
3. ストレージシステムのサービス状態が［Stopped］になるまで［Processing］が表示されます。



4. ［Storage Device List］画面の操作したいストレージシステムの［Start Service］をクリックします。

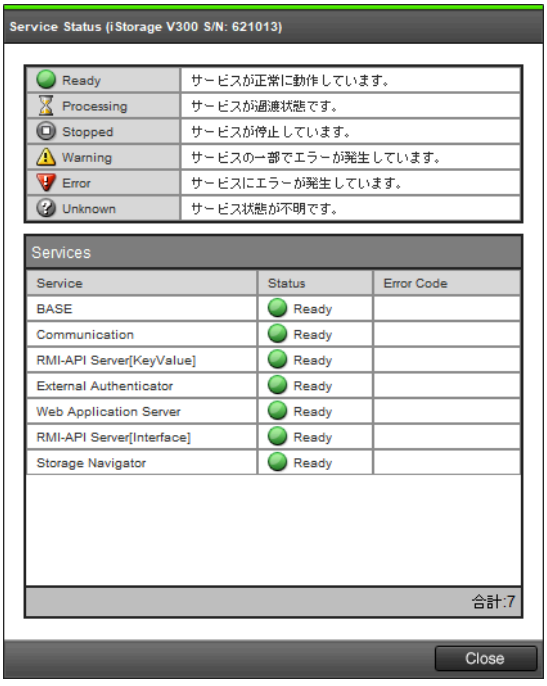


5. 確認メッセージが表示されます。［Confirm］をクリックします。



G.2.13 サービス状態一覧

装置サービスのモジュール毎の状態一覧を表示します。



項目	内容
状態一覧	各サービスモジュールが取りうる状態一覧を表示します。

項目	内容
Services	各サービスモジュールの状態一覧を表示します。 状態が Warning、Error の場合は、状態のエラーコードが表示されます。 エラーコードをクリックするとエラーメッセージが表示され、トラブルシュートが表示されます。

メモ

エラーメッセージにマニュアルを参照する旨、表示されている場合、「5.4.2 Storage Device List 操作時のトラブルシューティング（111 ページ）」を参照してください。

G.2.14 ストレージシステムの登録先 SVP を変更

ストレージシステムの登録を、すでに登録している SVP から、別の SVP に移行する場合の手順を示します。

メモ

- 1 台のストレージシステムを、同時に複数の SVP に登録できません。
- Apache 証明書とポート番号の設定は、最後にリストアした設定になります。設定内容を確認し、必要であれば設定を変更してください。

⚠ 注意

- ストレージシステムを起動すると、SVP 内で動作するプロセスに応じて、デスクトップヒープの消費量が増加します。「A.8 デスクトップヒープの指定値を変更する（206 ページ）」を参照してデスクトップヒープとして使用するメモリ領域を確保してください。

G.2.14.1 移行元 SVP の作業をする

操作手順

1. 移行の対象となるすべてのストレージシステムのサービスを停止してください。

   サービスを停止しないと、移行先の SVP から Storage Navigator が起動しません。
2. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
3. 移行作業を実施する前に、カレントディレクトリをツールが存在するディレクトリに移動し、次に示すコマンドを実行してください。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappBackup.bat
   ```

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

バックアップされる情報の詳細は、「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」を参照してください。

4. 「続行するためには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. バックアップファイル（LogsYYYYMMDDhhmmss.tgz）が生成されていることを確認してください。
6. コマンドプロンプトを閉じます。

   移行作業後、移行先の SVP の動作に問題がなければ、移行したストレージシステムを削除してください。

G.2.14.2 移行先 SVP の作業をする

操作手順

1. 移行先の SVP に必要なソフトウェアをインストールします（「A.6 管理サーバ（SVP）に必要なソフトウェアをインストールする（191 ページ）」を参照）。
2. 移行先の SVP に移行対象のストレージシステムをすべて登録します（「A.7 管理サーバ（SVP）にストレージシステムを登録する（199 ページ）」を参照）。
3. 移行先の SVP でストレージシステムのサービスが起動している場合は、サービスを停止します（「G.2.6 ストレージシステム単位のサービスを停止（354 ページ）」を参照）。
4. 移行元で生成されたバックアップファイル（LogsYYYYMMDDhhmmss.tgz）を移行先の SVP のツールのあるフォルダにすべてコピーします。
5. 移行先の SVP で Windows のコマンドプロンプトを管理者権限で起動します。
6. カレントディレクトリをツールが存在するディレクトリに移動し、次に示すコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   mapprestore.bat LogsYYYYMMDDhhmmss.tgz
   ```

メモ

一回のコマンドごとの SVP の再起動の手順は Skip してください。

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

リストアされる情報の詳細は、「G.2.9.1 SVP のソフトウェア設定情報のバックアップ（356 ページ）」を参照してください。また、リストア手順については、「G.2.9.2 SVP のソフトウェア設定情報のリストア（359 ページ）」も参照してください。

7. 「続行するためには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
8. 移行する SVP のバックアップファイルの数だけ、手順 4～手順 5 を実行してください。
9. コマンドプロンプトを閉じます。
10. Storage Device List に登録されている各ストレージシステムに対して、ポート番号を再割り振りします（「L.4 自動割り振りされたポート番号を再割り振りする（416 ページ）」を参照）。
11. SVP を再起動してください。

G.2.15 Log Dump の自動採取

Log Dump 自動採取機能により、特定の障害情報（SIM）の発生と同時に自動でログのダンプを採取できます。これにより装置に障害が発生した際に迅速な対応ができます。

メモ

障害検出時に自動採取されたダンプファイル（以下、Log Dump）を保守員に送付いただくことで、復旧プランの早期提示、復旧作業の早期着手に役立ちます。

前提条件

- Log Dump に必要なドライブの空き容量

  SVP ソフトウェアのインストール先ドライブに、ダンプファイル 2 世代分の格納領域として次の空き容量が必要です。

  - iStorage V100, V300 の場合：50GB
  - iStorage V10e の場合：40GB

⚠ 注意

本機能の対象は、Storage Device List に登録された装置のうち 1 台のみです。対象を別の装置に切り替えた場合には、別途、上記の容量が必要になります。

G.2.15.1 Log Dump 自動採取機能の仕様

Log Dump 自動採取機能の主な仕様を示します。

表 G-1 Log Dump 自動採取機能の主な仕様

項目	説明
Log Dump の採取対象の SIM コード	デフォルトでは、エラーレベルが Moderate、Serious、または Acute で、保守員通報される SIM コードが設定されています。 特定の SIM コードを Log Dump の採取対象として追加、または削除できます。詳細は、『SIM リファレンス』を参照してください。
採取される Log Dump の種別	Rapid、Normal、Detail のダンプが順番に採取されます。
Log Dump 自動採取の対象となるストレージシステム	Storage Device List に登録された、サービスが稼働しているストレージシステムのうち 1 台のみ、本機能を有効にできます。
Log Dump 自動採取機能の有効化	操作画面「Log Dump Ex Tool 画面」で本機能を有効にする必要があります。「G.2.15.2 Log Dump 自動採取機能を利用するための準備（369 ページ）」を参照してください。
Log Dump 自動採取機能の停止・再開	SVP の Storage Device List で、Log Dump 自動採取機能を有効化した装置のサービスを停止、開始することによって、Log Dump 自動採取機能が停止、再開されます。詳細は「G.2.15.6 Log Dump 自動採取機能を停止する（372 ページ）」と「G.2.15.7 Log Dump 自動採取機能を再開する（373 ページ）」を参照してください。
操作画面	Log Dump Ex Tool 画面で次の操作を実行できます。詳細は、「G.2.16 Log Dump Ex Tool 画面の操作（373 ページ） 」を参照してください。 • Log Dump の採取対象となる SIM の追加・削除・除外・除外解除 （1）Log Dump の採取対象に SIM コードを追加する （2）Log Dump の採取対象から SIM コードを削除する （3）Log Dump の採取対象から SIM コードを除外する （4）Log Dump の除外対象から SIM コードの除外設定を解除する • Log Dump のコピー （5）Log Dump をコピーする • Log Dump 採取の中止 （6）Log Dump の採取中に採取処理を中止する Log Dump Ex Tool 画面で発生するメッセージは、「G.2.19 Log Dump Ex Tool が表示するメッセージ（389 ページ）」を参照してください。
Log Dump 採取中の操作画面	Log Dump の採取が始まると、Log Dump Ex Tool 画面が表示されます。Log Dump の採取が完了すると、Log Dump Ex Tool 画面が最小化されます。
Log Dump の格納ディレクトリ	C:\Mapp\wk\[装置識別番号]\dkc200\others\logdumpex • "C:\Mapp"は、SVP ソフトウェアのデフォルトのインストールディレクトリです。インストール時の指定により異なる場合があります。 • 装置識別番号の下 6 桁が、装置製番を示します。 • 直近に発生した Log Dump の採取対象 SIM 2 つ分（2 世代分）の Log Dump が、ストレージシステムごとに保持されます。
Log Dump の名称	装置製番_hdcpyyyymmddhhmm-xxxx-種別.tgz yyyymmddhhmm は Log Dump を出力した時刻です。このため、Rapid、Normal、Detail で異なります。 例： 装置製番 600001 の装置で、SIM=2130 により Log Dump が採取された場合 • Rapid： 600001_hdcp201803280339-2130-Rapid.tgz

項目	説明
	• Normal： 600001_hdcp201803280409-2130-Normal.tgz • Detail： 600001_hdcp201803280418-2130-Detail.tgz
Log Dump 採取のイベント通知	以下のイベントが発生すると、SVP の Windows イベントログが出力されます。これらのイベントは ALIVE 通報されます。詳細は「G.2.18 Log Dump の採取処理で発生するイベントと対処方法（388 ページ）」を参照してください。 • イベント ID：19 Log Dump の採取開始 • イベント ID：20 Log Dump の採取正常終了 • イベント ID：21 Log Dump の採取異常終了 • イベント ID：22 Log Dump の採取中止完了 イベントログの参照方法は、「B.4.1 Windows イベントログでストレージシステムの障害情報を監視する（223 ページ）」を参照してください。
Log Dump の採取が実行されない条件	以下の場合は、Log Dump の採取が実行されません。 • ストレージ管理ソフトウェアのインストール先ドライブの空き容量不足 - iStorage V100, V300 の場合：25GB 未満 - iStorage V10e の場合：20GB 未満 空き容量が不足していると、空き容量を増やすことを指示するメッセージ［LOG3977E］が SVP 画面に表示されます。 • 保守操作中 • 自動ダンプ採取対象の SIM が発行された装置に対して、SVP でダンプツール（バッチファイル）を実行中 • Log Dump の採取中に、Log Dump の採取対象の SIM が発生した場合
Log Dump の採取が中止される条件	Log Dump の採取中に SVP をリブートした場合は、Log Dump の採取が中止されます。

G.2.15.2 Log Dump 自動採取機能を利用するための準備

ストレージシステムのサービスを起動する

Log Dump 自動採取機能を利用するには、Log Dump 自動採取機能を有効化したいストレージシステムのサービスが起動されている必要があります。

Storage Device List の画面で、Log Dump 自動採取機能を有効化したいストレージシステムのアイコン左下のステータスが"Stopped"の場合は、［Start Service］ボタンをクリックしてください。サービスが起動すると、ステータスが"Ready"に変わります。

G.2.15.3 Log Dump Ex Tool 画面を起動する

Log Dump 自動採取機能の設定は、Log Dump Ex Tool 画面で行います。SVP でバッチファイルを実行すると Log Dump Ex Tool 画面が起動します。

操作手順

1. Storage Device List の画面で、Log Dump 自動採取機能を有効化したいストレージシステムのサービスが起動されていることを確認してください。

2. コマンドプロンプトを管理者権限で起動します。
3. カレントディレクトリを移動します。

   CD /D C:\Mapp\wk\[装置識別番号]\dkc200\mp\pc\

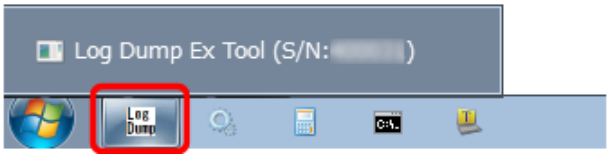
   メモ

   - "C:\Mapp"は、SVP ソフトウェアのデフォルトのインストールディレクトリです。インストール時の指定により異なる場合があります。
   - 装置識別番号の下 6 桁が、装置製番を示します。

4. 画面起動用バッチファイルを実行します。

   Start_LogDumpTool.bat

   バッチファイルの実行が完了すると、タスクバーに Log Dump Ex Tool 画面のアイコンが表示されます。

   メモ

   バッチファイルがインストールされているフォルダにある他のファイルを誤って操作しないように注意してください。

5. コマンドプロンプトを閉じます。

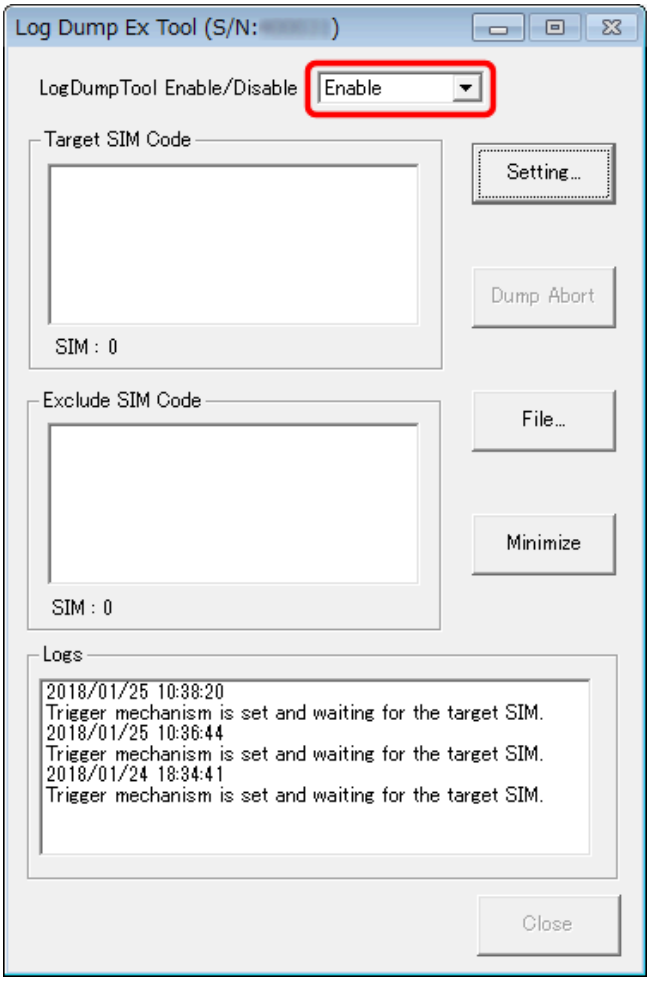
   バッチファイルは終了しませんので、画面右上の［×］ボタンをクリックしてコマンドプロンプトを閉じてください。

G.2.15.4 Log Dump 自動採取機能を有効にする

Log Dump 自動採取機能を有効にすると、特定の SIM が発生した際に Log Dump が自動で採取されます。

操作手順

1. タスクバー上のアイコンを選択し、Log Dump Ex Tool 画面を表示します。
2. ［Log Dump Tool Enable/Disable］を Enable に設定します。



3. 確認メッセージが表示されるので、［OK］ボタンをクリックします。
4. ［Minimize］ボタンをクリックします。

   Log Dump Ex Tool 画面がタスクバーにアイコンとして表示されます。この状態で運用してください。

G.2.15.5 Log Dump 自動採取機能の対象ストレージシステムを変更する

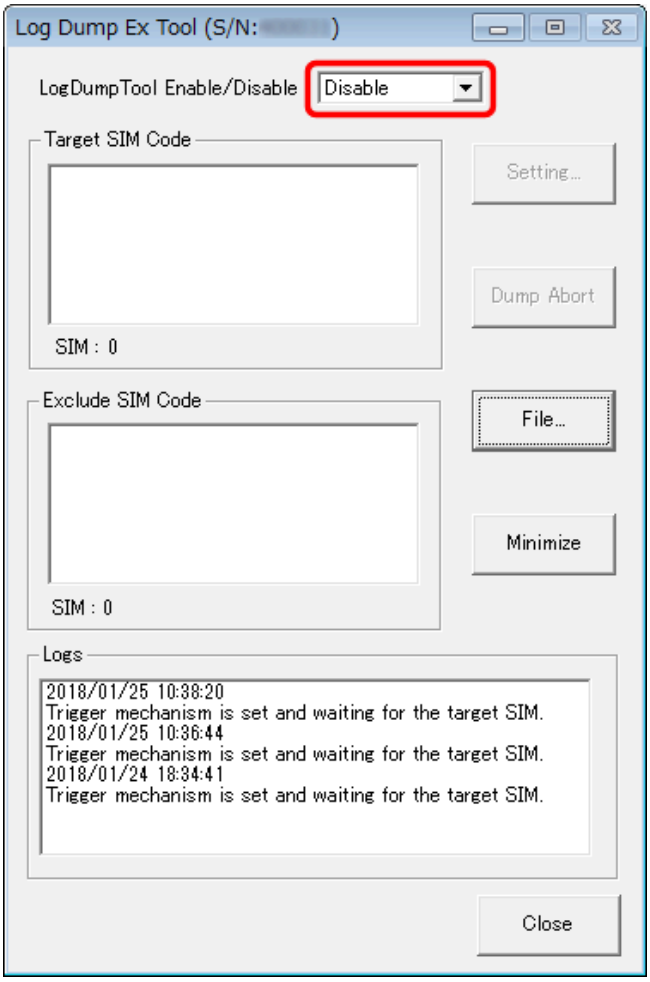
Log Dump 自動採取機能を有効化できるストレージシステムは、Storage Device List に登録された、サービスが稼働しているストレージシステムです。

操作手順

1. Log Dump 自動採取機能の無効化

   （1） タスクバー上のアイコンを選択し、Log Dump Ex Tool 画面を表示します。

   （2）［Log Dump Tool Enable/Disable］を Disable に設定します。



(3) 確認メッセージが表示されるので、[OK] ボタンをクリックします。

(4) [Close] ボタンをクリックして画面を閉じます。

2. 別の装置の Log Dump 自動採取機能の有効化

「G.2.15.3 Log Dump Ex Tool 画面を起動する (369 ページ)」と「G.2.15.4 Log Dump 自動採取機能を有効にする (370 ページ)」を参照して、Log Dump 自動採取機能を有効化します。

G.2.15.6 Log Dump 自動採取機能を停止する

前提条件

SVP の Storage Device List で、Log Dump 自動採取機能を有効化した装置のサービスを停止することで、Log Dump 自動採取機能も連動して停止します。

操作手順

1. SVP の Storage Device List で、Log Dump 自動採取機能を有効化した装置のサービスを停止します。詳細は「G.2.6 ストレージシステム単位のサービスを停止 (354 ページ)」を参照してください。
2. Log Dump Ex Tool 画面が自動で閉じられます。SVP のタスクバーに、Log Dump Ex Tool 画面のアイコンが表示されていないことを確認してください。

⚠ 注意

Log Dump Ex Tool 画面が自動で閉じられないことがあります。Log Dump Ex Tool 画面のアイコンが表示されている場合、次の手順で Log Dump Ex Tool 画面が閉じてください。Log Dump Ex Tool 画面のアイコンが残ったままで、装置のサービスを再開しても、Log Dump 自動採取機能が動作しません。

a. タスクバーにある Log Dump Tool Ex のアイコンを右クリックします。
b. コンテキストメニューから、［ウィンドウを閉じる］を選択します。

G.2.15.7 Log Dump 自動採取機能を再開する

前提条件

SVP の Storage Device List で、Log Dump 自動採取機能を有効化した装置のサービスを再開することで、Log Dump 自動採取機能も連動して再開します。

操作手順

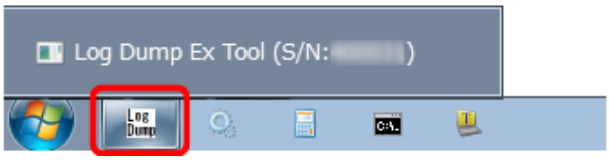
1. SVP の Storage Device List で、Log Dump 自動採取機能を有効化した装置のサービスを開始します。詳細は「G.2.7 ストレージシステム単位のサービスの開始 (354 ページ)」を参照してください。
2. Log Dump Ex Tool 画面を起動します。詳細は「G.2.15.3 Log Dump Ex Tool 画面を起動する (369 ページ)」の「Log Dump Ex Tool 画面を起動する」を参照してください。

G.2.16 Log Dump Ex Tool 画面の操作

G.2.16.1 Log Dump の採取対象に SIM コードを追加する

操作手順

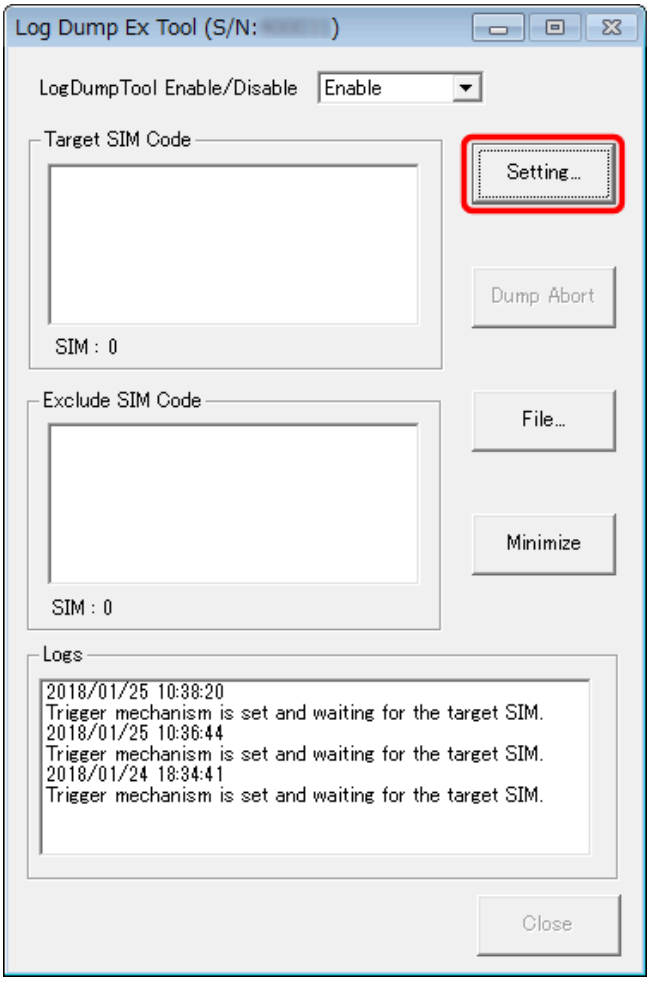
1. タスクバー上のアイコンを選択し、Log Dump Ex Tool 画面を表示します。



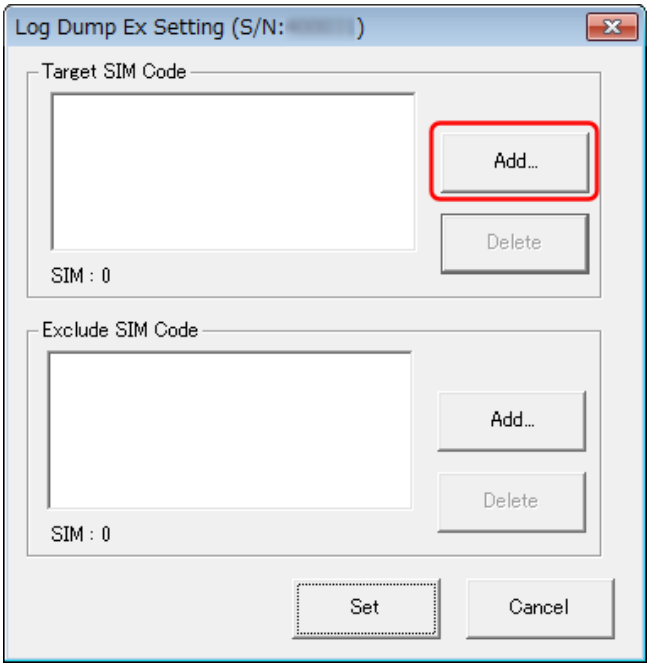
メモ

タスクバーにアイコンがない場合は、Log Dump Ex Tool 画面が未起動状態です。
「G.2.15.3 Log Dump Ex Tool 画面を起動する（369 ページ）」を参照して、Log Dump Ex Tool 画面を起動してください。

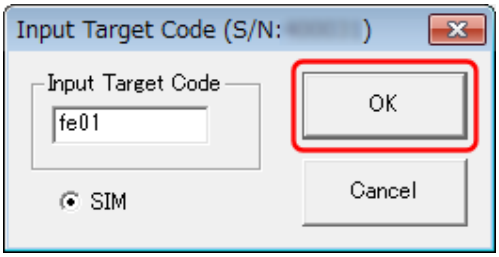
2. Log Dump Ex Tool 画面で、［Setting...］ボタンをクリックします。



3. Log Dump Ex Setting 画面が表示されたら、［Target SIM Code］の枠内にある［Add...］ボタンをクリックします。

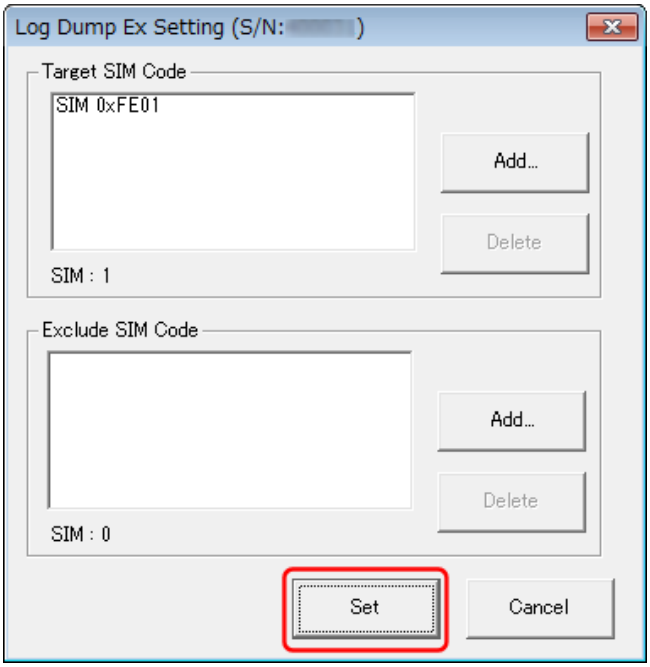


4. Input Target Code 画面が表示されます。［Input Target Code］欄に Log Dump の採取対象にする SIM コードの上 4 桁を入力し、［OK］ボタンをクリックします。



   - Log Dump の採取対象にする SIM コードが複数ある場合は、手順 3、4 を繰り返してください。
   - SIM コード 4 桁目が可変値の場合は、上 3 桁の固定値部分に 0～9、a～f を付加した SIM コードをすべて登録してください。

5. SIM コードの入力が完了したら、［Set］ボタンをクリックします。

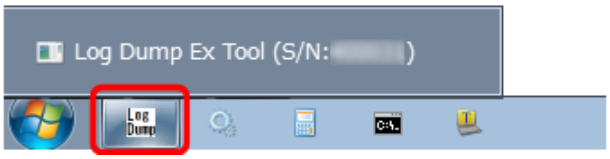


6. Log Dump Ex Tool 画面で、[Minimize] ボタンをクリックします。

G.2.16.2 Log Dump の採取対象から SIM コードを削除する

操作手順

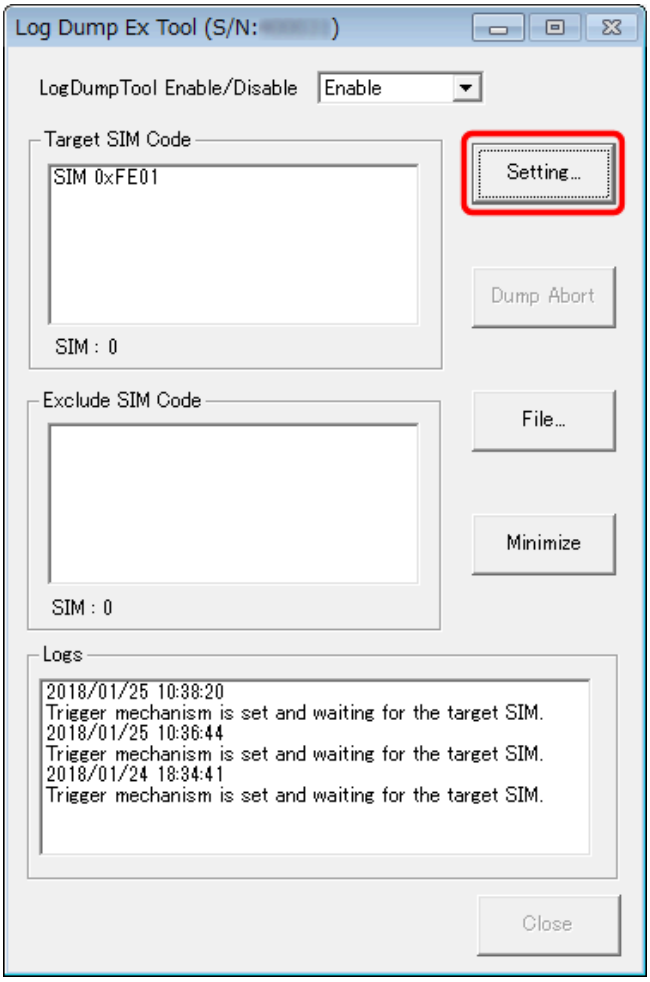
1. タスクバー上のアイコンを選択し、Log Dump Ex Tool 画面を表示します。



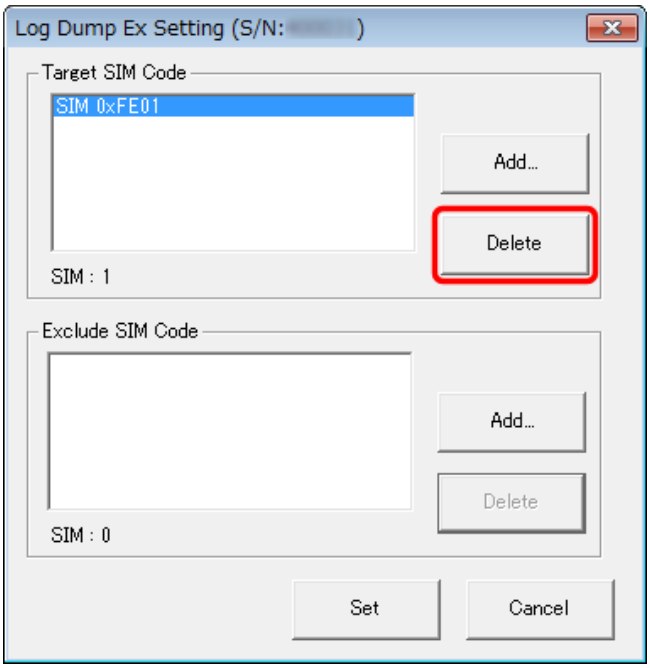
メモ

タスクバーにアイコンがない場合は、Log Dump Ex Tool 画面が未起動状態です。
「G.2.15.3 Log Dump Ex Tool 画面を起動する (369 ページ)」を参照して、Log Dump Ex Tool 画面を起動してください。

2. Log Dump Ex Tool 画面で、[Setting...] ボタンをクリックします。

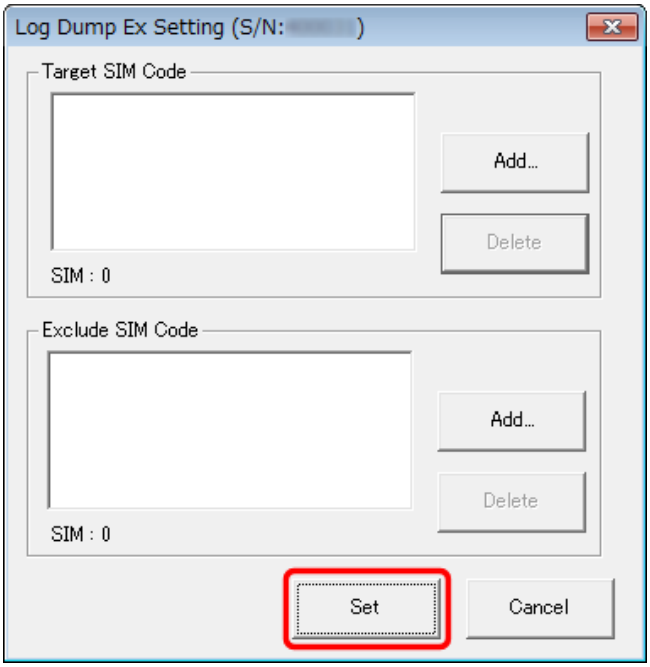


3. Log Dump Ex Setting 画面が表示されます。［Target SIM Code］の枠内にあるリストから、Log Dump の採取対象から削除する SIM コードを選択し、［Target SIM Code］の枠内にある［Delete］ボタンをクリックします。



- Log Dump の採取対象から削除する SIM コードが複数ある場合は、本手順を繰り返してください。

4. SIM コードの削除が完了したら、［Set］ボタンをクリックします。

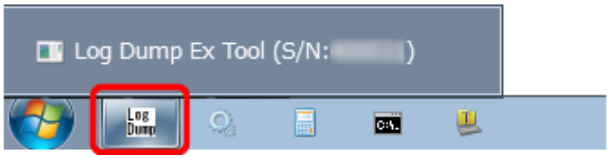


5. Log Dump Ex Tool 画面で、［Minimize］ボタンをクリックします。

G.2.16.3 Log Dump の採取対象から SIM コードを除外する

操作手順

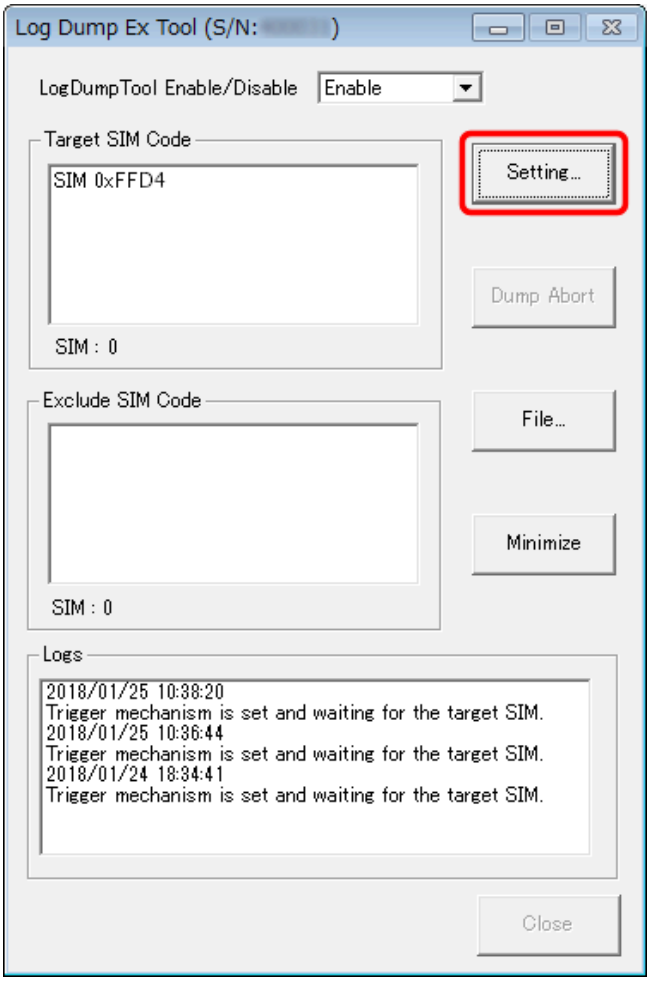
1. タスクバー上のアイコンを選択し、Log Dump Ex Tool 画面を表示します。



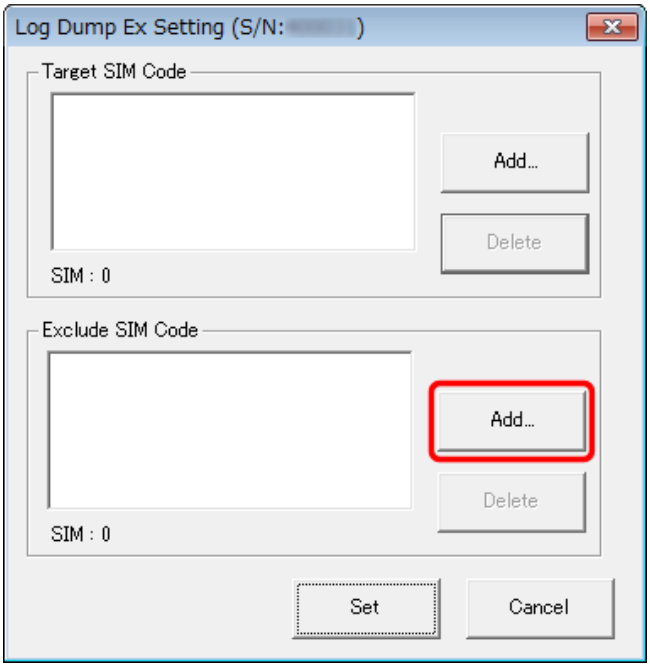
メモ

タスクバーにアイコンがない場合は、Log Dump Ex Tool 画面が未起動状態です。
「G.2.15.3 Log Dump Ex Tool 画面を起動する（369 ページ）」を参照して、Log Dump Ex Tool 画面を起動してください。

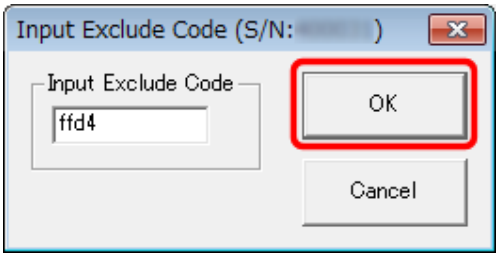
2. Log Dump Ex Tool 画面で、［Setting...］ボタンをクリックします。



3. Log Dump Ex Setting 画面が表示されたら、［Exclude SIM Code］の枠内にある［Add...］ボタンをクリックします。

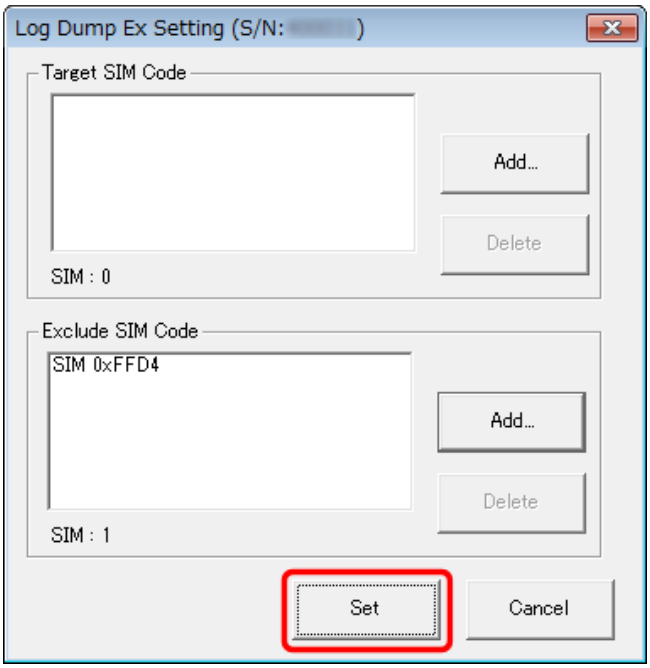


4. Input Exclude Code 画面が表示されます。[Input Exclude Code] 欄に Log Dump の採取対象から除外する SIM コードの上 4 桁を入力し、[OK] ボタンをクリックします。



- Log Dump の採取対象から除外する SIM コードが複数ある場合は、手順 3、4 を繰り返してください。
- SIM コード 4 桁目が可変値の場合は、上 3 桁の固定値部分に 0～9、a～f を付加した SIM コードをすべて登録してください。

5. SIM コードの入力が完了したら、[Set] ボタンをクリックします。

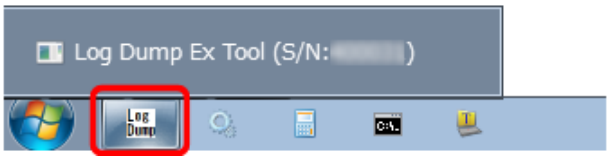


6. Log Dump Ex Tool 画面で、[Minimize] ボタンをクリックします。

G.2.16.4 Log Dump の除外対象から SIM コードの除外設定を解除する

操作手順

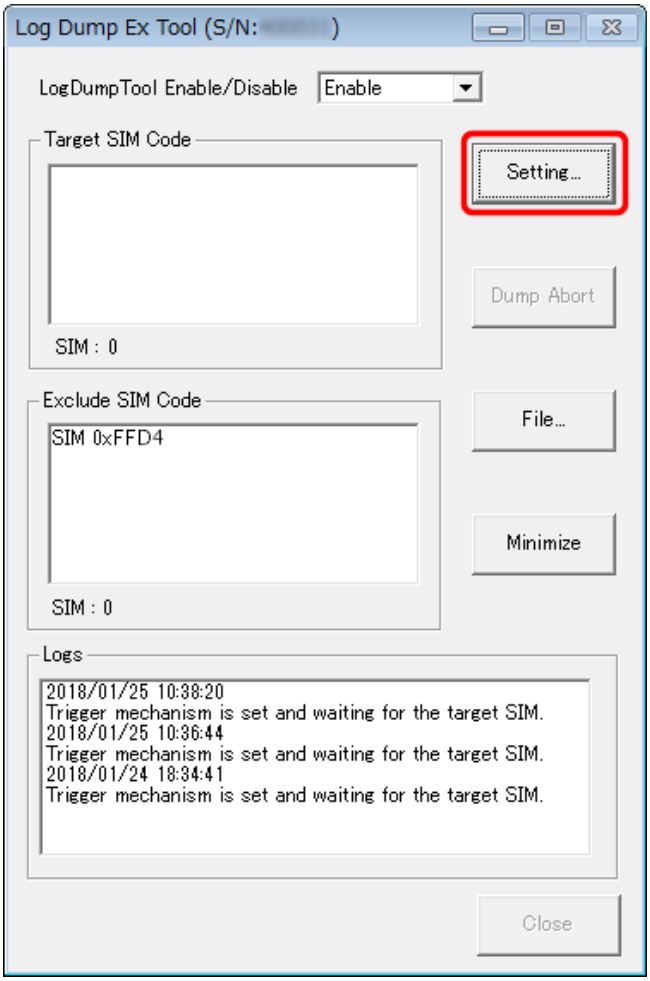
1. タスクバー上のアイコンを選択し、Log Dump Ex Tool 画面を表示します。



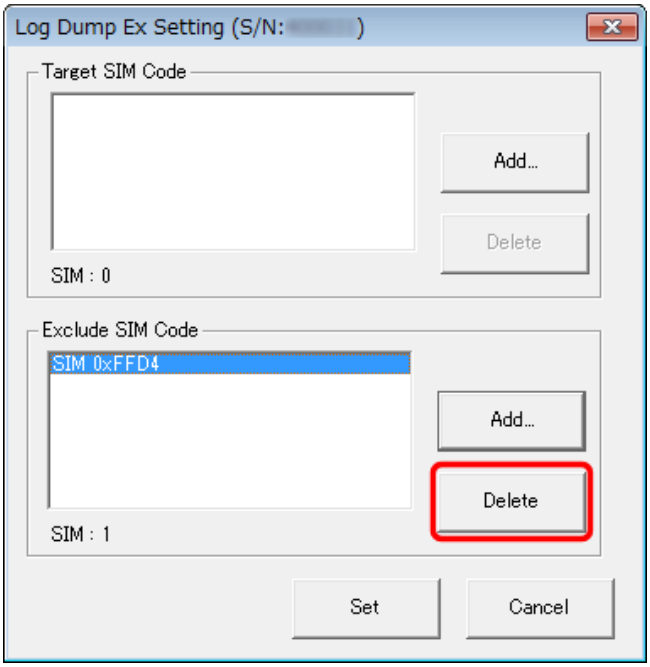
メモ

タスクバーにアイコンがない場合は、Log Dump Ex Tool 画面が未起動状態です。
「G.2.15.3 Log Dump Ex Tool 画面を起動する（369 ページ）」を参照して、Log Dump Ex Tool 画面を起動してください。

2. Log Dump Ex Tool 画面で、［Setting...］ボタンをクリックします。

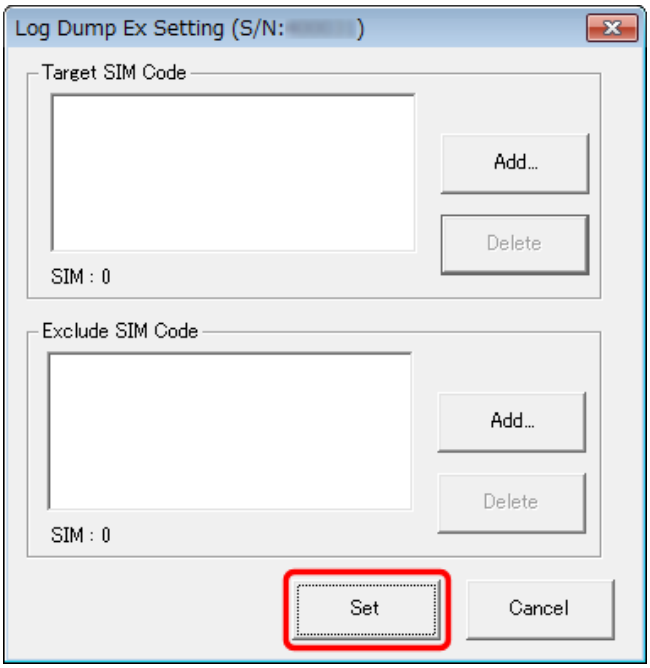


3. Log Dump Ex Setting 画面が表示されたら、［Exclude SIM Code］の枠内にあるリストから、Log Dump の除外対象を解除する SIM コードを選択し、［Exclude SIM Code］の枠内にある［Delete］ボタンをクリックします。



- Log Dump の除外対象を解除する SIM コードが複数ある場合は、本手順を繰り返してください。

4. SIM コードの解除が完了したら、［Set］ボタンをクリックします。

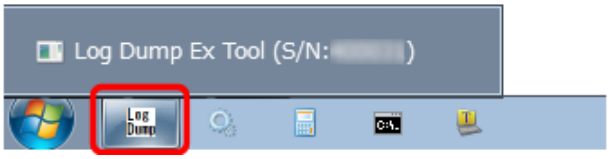


5. Log Dump Ex Tool 画面で、［Minimize］ボタンをクリックします。

G.2.16.5 Log Dump をコピーする

操作手順

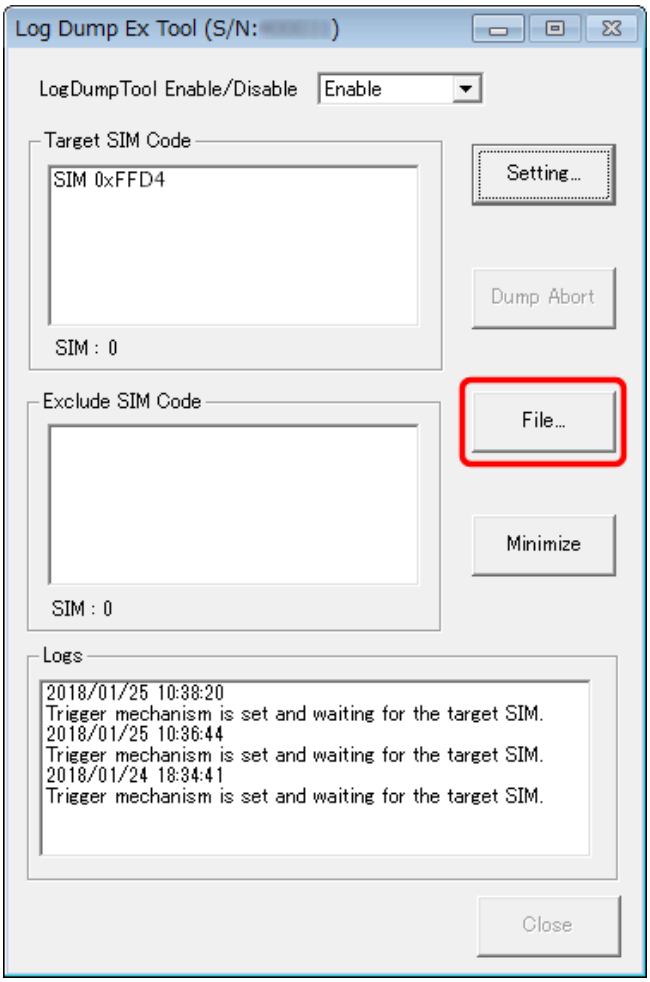
1. タスクバー上のアイコンを選択し、Log Dump Ex Tool 画面を表示します。



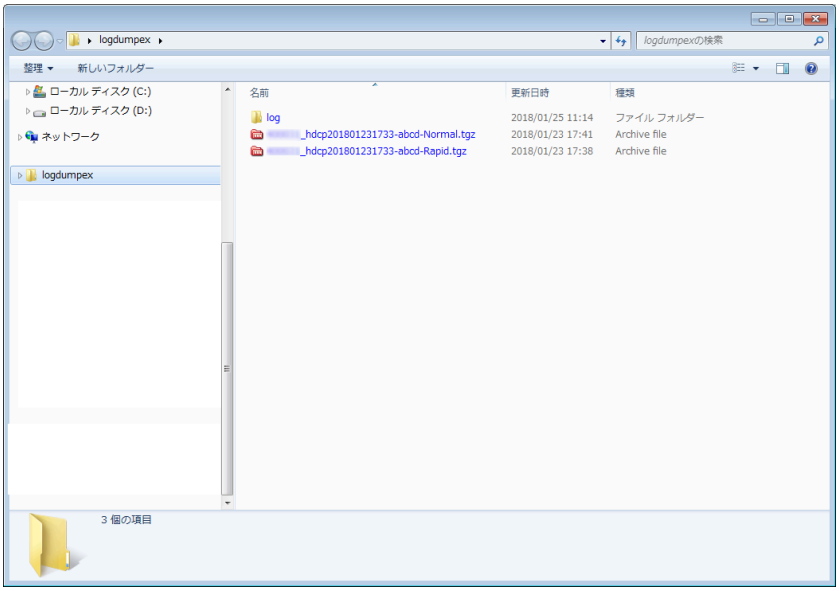
メモ

タスクバーにアイコンがない場合は、Log Dump Ex Tool 画面が未起動状態です。
「G.2.15.3 Log Dump Ex Tool 画面を起動する（369 ページ）」を参照して、Log Dump Ex Tool 画面を起動してください。

2. Log Dump Ex Tool 画面で、［File...］ボタンをクリックします。



3. エクスプローラーが起動され、Log Dump が格納されているフォルダが表示されます。必要な Log Dump をコピーします。



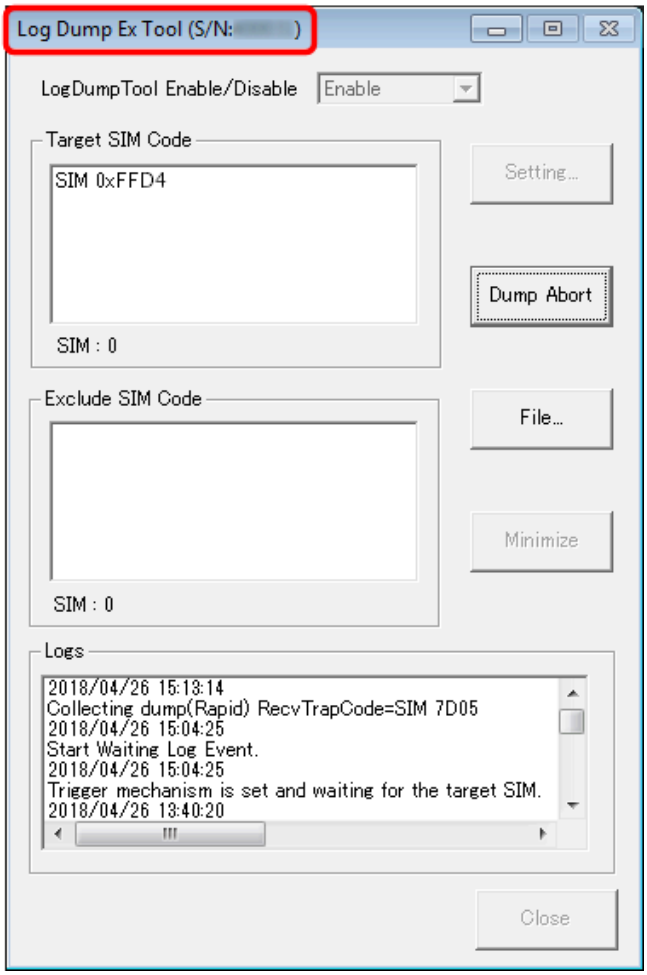
4. Log Dump Ex Tool 画面で、［Minimize］ボタンをクリックします。

G.2.16.6 Log Dump の採取中に採取処理を中止する

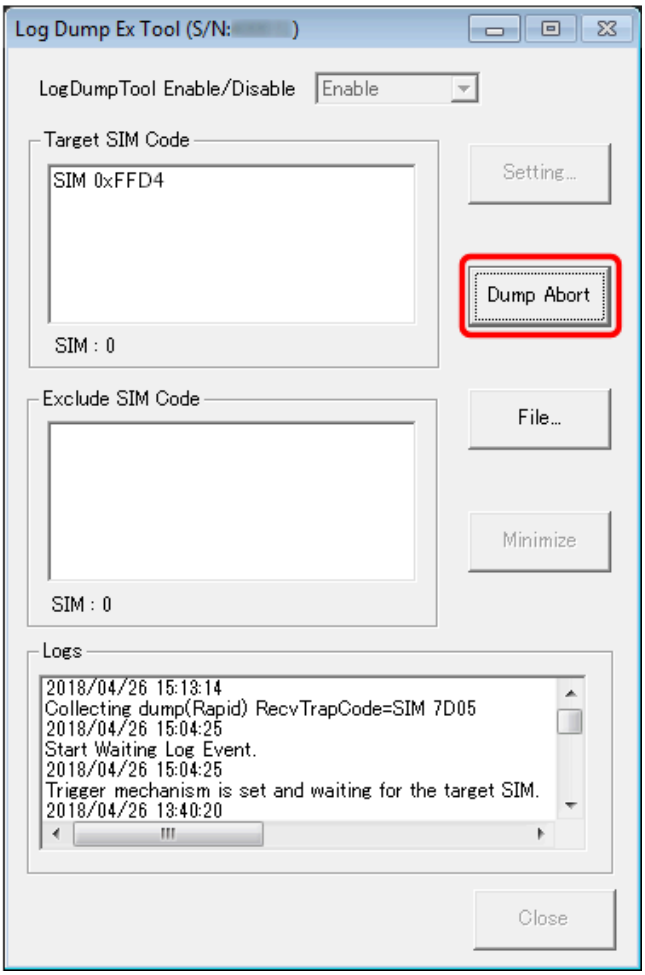
Log Dump の採取中に障害の原因が判明した場合など、Log Dump が不要になった場合は、採取を中止できます。

操作手順

1. Log Dump の採取中は、Log Dump Ex Tool 画面が表示されています。タイトルバーの装置製番を見て、Log Dump の採取を中止する装置であることを確認します。



2. Log Dump Ex Tool 画面で、［Dump Abort］ボタンをクリックします。



3. Log Dump Ex Tool 画面で、［Minimize］ボタンをクリックします。

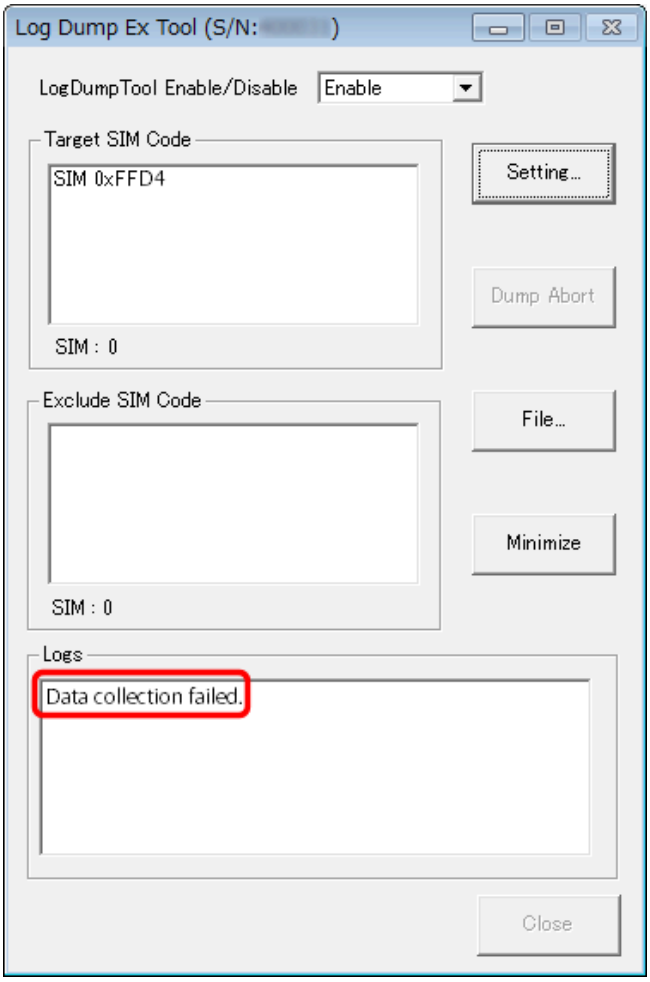
G.2.17 Log Dump の採取が失敗した場合の対応

Log Dump の採取中に保守員が保守作業を始めると、採取の処理が失敗する場合があります。また予期せぬエラーにより失敗する場合もあります。

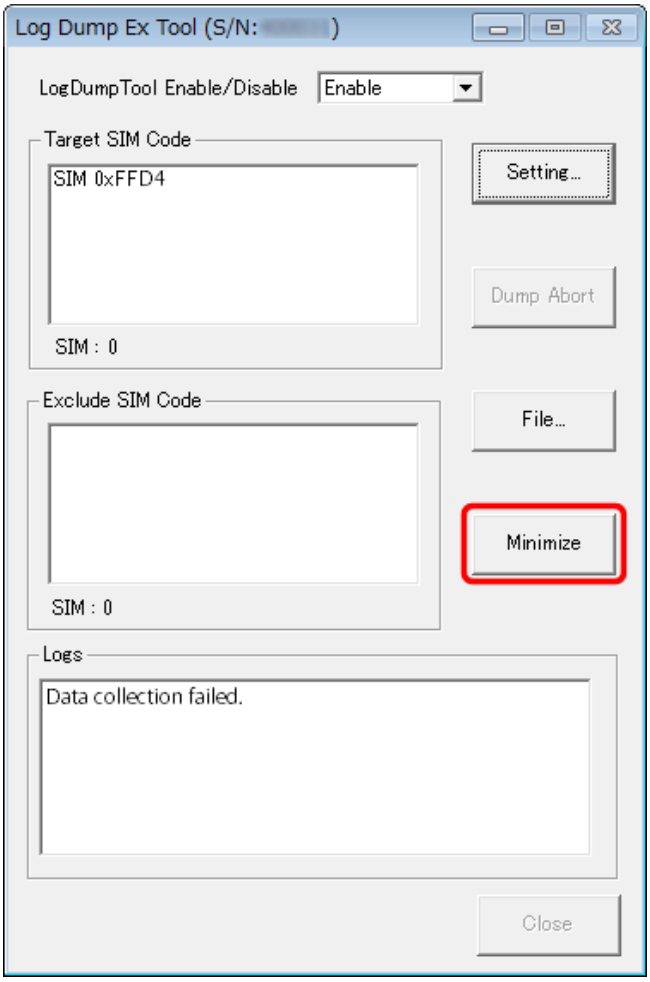
Log Dump の採取が失敗した場合は、保守員に連絡してください。

操作手順

1. Log Dump の採取が失敗すると Log Dump Ex Tool 画面の［Logs］に［Data collection failed.］と表示されます。



2. Log Dump Ex Tool 画面で、［Minimize］ボタンをクリックします。



G.2.18 Log Dump の採取処理で発生するイベントと対処方法

Log Dump の採取処理のプロセスを示すイベント ID と主な内容を示します。対処が必要なイベント ID が表示された場合は、下表を参照して対処してください。

表 G-2 Log Dump の採取処理で発生するイベントと対処方法

イベント ID	レベル	項目	内容
19	情報	概要	Log Dump の採取が開始された
		Detail 表示	Dump collection starts
		対処方法	なし
20	情報	概要	Log Dump の採取が正常終了した
		Detail 表示	Dump collection ends normally
		対処方法	なし
21	エラー	概要	Log Dump の採取が異常終了した
		Detail 表示	Dump collection ends abnormally
		対処方法	SVP のドライブの空き容量が不足しているか、Log Dump の採取中に保守作業が実施された可能性があります。

イベント ID	レベル	項目	内容
			SVP ソフトウェアのインストール先ドライブに、ダンプファイル 1 世代分の格納領域として、25GB 以上）の空き容量を確保してください。 保守作業中に本イベントが発生した場合は、対処は不要です。その他の場合は、保守員に連絡してください。
22	情報	概要	Log Dump の採取が中止された
		Detail 表示	Cancellation of the dump collection completed
		対処方法	なし

G.2.19 Log Dump Ex Tool が表示するメッセージ

Log Dump Ex Tool が表示するメッセージと対処方法を示します。

表 G-3 Log Dump Ex Tool が表示するメッセージと対処方法

メッセージコード	項目	内容
LOG3977E	メッセージ	HDD 空き容量が（空き容量）GB 未満となっています。HDD 空き容量を確保してから操作を行ってください。
	内容	HDD の空き容量が不足しています。
	対処方法	HDD の容量を確保して、操作してください。
LOG3978E	メッセージ	Autodump の起動に失敗しました。
	内容	Autodump の起動に失敗しました。
	対処方法	保守員に連絡してください。
LOG3981E	メッセージ	このコードはすでに設定されています。
	内容	すでに設定されている SIM コードが入力されました。
	対処方法	新たな SIM コードを設定したい場合は、再度入力してください。
LOG3982E	メッセージ	入力されたコードは正しくありません。
	内容	Log Dump Ex Tool に設定できない SIM コードが入力されました。
	対処方法	SIM コードを確認して、再度入力してください。
LOG4643i	メッセージ	設定の変更を確定してもよろしいですか？
	内容	確認メッセージです。
	対処方法	確定する場合は［OK］ボタンをクリックしてください。
LOG4644W	メッセージ	すでに他の装置（S/N：装置名）の自動 LogDump 採取機能の設定が「Enable」となっています。 現在の装置を「Enable」に設定する場合は、他の装置（S/N：装置名）の自動 LogDump 採取機能を「Disable」に設定してください。その後、現在の装置の設定変更を行ってください。
	内容	他の装置の自動 LogDump 採取機能の設定が「Enable」に設定されている場合に表示されるメッセージです。
	対処方法	現在の装置を「Enable」に設定する場合は、他の装置（S/N：装置名）の自動 LogDump 採取機能を「Disable」に設定してください。

G.2.20 Jetty の定期リブート

Jetty を定期的にリブートすると、Storage Navigator の起動が安定します。指定した間隔の時刻に Jetty がリブートされるため、Java プログラムのメモリが解放され、Storage Navigator の起動に必要なメモリを安全に確保できます。

メモ

SVP が下記の場合、Jetty の定期リブートの時刻でもリブートされず、翌日の同じ時刻に繰り越されます。

- Storage Navigator を停止している場合
- Storage Navigator のサブ画面が Modify モードの場合
- Web Console Launcher を設定、操作している場合
- RAID Manager を使用してストレージシステムを操作している場合

G.2.20.1 Jetty 定期リブートの設定

定期リブートの時刻と間隔を設定します。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールがインストールされているディレクトリに移動します。

   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。
3. バッチファイル（MappJettyRebootSetting.bat ［装置製番］ ［"Enable"］ ［実行間隔］ ［時］ ［分］）を実行します。

項目	内容
装置製番	装置製番 Storage Device List に表示されている装置製番（S/N）を指定します。 例えば、"S/N: 600102"と表示されている場合は、600102 を指定してください。
"Enable"	"Enable"固定
リブートする間隔	1 回/日：Daily

項目	内容
	1 回/週：曜日を指定（Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday）
時	24 時間表記、2 桁で指定（00～23）
分	2 桁で指定（00～59）

4. 完了メッセージを確認します。
5. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
6. コマンドプロンプトを閉じます。

⚠ 注意

- Jetty がリブートされると、Storage Navigator のユーザーセッションが切断されます。
- Jetty のリブート中は、SVP を再起動しないでください。リブートは 5 分ほどかかります。
- Jetty をリブートする時間は、深夜など、管理インターフェースで装置を操作しない時間帯に設定してください。

G.2.20.2 Jetty 定期リブートの解除

定期リブートを解除します。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールがインストールされているディレクトリに移動します。

   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。
3. バッチファイル（MappJettyRebootSetting.bat ［装置製番］ ["Disable"]）を実行します。
4. 完了メッセージを確認します。
5. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
6. コマンドプロンプトを閉じます。

G.2.20.3 Jetty 定期リブートの設定内容の参照

定期リブートの設定内容を参照します。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールがインストールされているディレクトリに移動します。

   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. バッチファイル（MappJettyRebootRefer.bat ［装置製番］）を実行します。

   バッチファイルを実行すると、次に示す設定内容が表示されます。

項目	内容
SerialNumber	装置製番
Setting	有効/無効 • Enable：有効 • Disable：無効
Dayofweek	リブートする間隔 • Daily：1 回/日 • Sunday、Monday、Tuesday、Wednesday、Thursday、Friday、Saturday：週に 1 回、リブートする曜日
Time	リブートする時刻
RebootPass	リブート予約の有効/無効 • 1：「G.2.20.1 Jetty 定期リブートの設定（390 ページ）」の「メモ」に示す要因により、リブートが翌日に繰り越されている状態 • 0：リブートが翌日に繰り越されていない状態

4. 完了メッセージを確認します。
5. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
6. コマンドプロンプトを閉じます。

G.2.21 DNS サフィックスの設定

SVP を使用して、管理 LAN にストレージシステムをホスト名で接続する場合、SVP の Windows に、DNS サフィックスを設定する必要があります。

操作手順

1. ［コントロールパネル］から［ネットワークと共有センター］を開いてください。
2. ［イーサネット］をクリックしてください。
3. ［イーサネットの状態］が表示されます。

   ［プロパティ］ボタンをクリックしてください。
4. ［イーサネットのプロパティ］が開きます。

   一覧の中の［インターネット プロトコルバージョン 4 (TCP/IPv4)］を選択して、［プロパティ］ボタンをクリックしてください。
5. ［全般] タブから［詳細設定] ボタンをクリックしてください。
6. ［TCP/IP 詳細設定］を開いた後、［DNS］タブをクリックしてください。
7. ［以下の DNS サフィックスを順に追加する］のラジオボタンを選択し、［追加］ボタンから DNS サフィックスを追加してください。

付録 H.　ホスト接続の参考情報

ホストをストレージシステムに接続するときに参考となる情報を説明します。

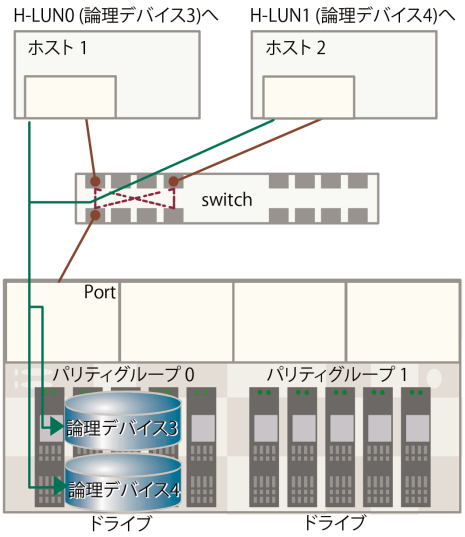
H.1　Fibre Channel ホスト

Fibre Channel ホストをストレージシステムに接続するときの参考情報です。

H.1.1　複数ホストでの構築

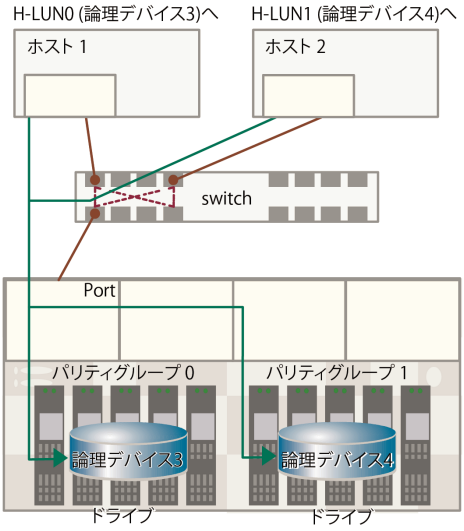
複数のホストを 1 台のストレージシステムに接続したとき、それぞれのホストに割り当てられた論理デバイスが同じパリティグループに存在すると、同じドライブへのアクセスが発生します。このときドライブへのアクセスが競合し、性能が劣化する可能性があります。

同一パリティグループの場合



この競合を回避するために、同時に稼働させるホストに割り当てる論理デバイスを別のパリティグループに分けて設定してください。作成できるパリティグループの数は、搭載するドライブ数と作成するパリティグループの RAID レベルで決まります。

異なるパリティグループの場合



H.1.2　ゾーニング

SAN 環境のホストは、ゾーンごとにグループ化できます。ゾーンごとに構築した SAN 環境では、ゾーン外のホストからゾーン内のホストを見ることができなくなります。また、各ゾーン内の SAN トラフィックはほかのゾーンに影響しません。

複数の SAN 環境を使う場合は、SAN スイッチを用いてゾーニングします。ゾーニングごとに、必要なセキュリティと SAN 環境のアクセス権を定義し構築します。

ゾーニングでは、サーバ間の共有デバイスが競合せずに論理デバイスにアクセスできるよう定義します。通常、ゾーンはストレージ論理デバイスの共有グループにアクセスするサーバグループごとに作成されます。

OS によるゾーニング

SAN 環境で、Windows、VMware、Red Hat Linux のような OS が稼働する異なるサーバからのアクセスが続く場合、サーバは OS ごとにグループ化し、SAN 環境ゾーンをサーバのグループごとに定義します。これにより、サーバのほかのグループまたはほかのクラスから、論理デバイスのアクセスを防御します。

バックアップ

ゾーンはバックアップ用の共通サーバにアクセスできます。SAN は、バックアップ、回復処理用サーバも兼ねているので、これらのバックアップサーバにアクセスできるようにしなければいけません。バックアップサーバが特定のホストでバックアップ、回復処理できるように SAN 環境ゾーンを構築します。

セキュリティ

ゾーニングはセキュリティを提供します。試験用に定義されたゾーンは、SAN 環境内で個別に管理でき、本稼働用ゾーン内で作動している作業に影響しません。

マルチストレージシステム

ゾーンは複数のストレージシステムを使いやすくします。個々のゾーンを使うことにより、各ストレージシステムは、サーバ間でアクセス競合せず、個別に管理できます。

H.1.3 ホスト側に設定するコマンド多重数

ホスト側に設定するコマンド多重数については、ストレージシステムごとに適切な値を設定してください。また、コマンド多重数は、プラットフォームごとに対象単位、設定単位が異なりますので、OS や HBA などのマニュアルで事前に確認してください。

設定に当たってのガイダンスは次のとおりです。

- コマンド多重数が小さい場合は、I/O が多重で発行されず、I/O 性能が低下する可能性があります（多重数が 4 以下の場合）。
- ストレージシステムは、コマンド多重限界数を超えた状態でコマンドを受領すると Queue Full ステータスを報告します。使用する論理デバイス数が多く、多重数に大きな値が設定されているときに Queue Full が発生する可能性がありますので、ご使用の環境に合わせて適切な多重数を設定してください。下記の表を参照してください。
- 新規導入時だけでなく、ドライブの増設時も、コマンド多重数の設定を忘れずに実施してください。

表 H-1 コマンドの多重数

項目	仕様
コマンド多重数	論理デバイス当り最大 32 です。 ポート当り最大 1024 です。

H.1.4 デバイスタイムアウト値の推奨値

ストレージシステムの論理デバイスに対するデバイスタイムアウト値は、60 秒以上に設定してください。

デバイスタイムアウト値が短いと、SCSI コマンドのタイムアウトが発生し、I/O 性能が低下します。

H.2 iSCSI ホスト

iSCSI ホストをストレージシステムに接続するときの参考情報です。

H.2.1 iSCSI の概要

iSCSI インターフェース（以下、iSCSI I/F）は、ホストとの通信に iSCSI を利用できます。特徴は次のとおりです。

- ギガビットイーサネットで構築した IP ネットワークを利用して通信します。
- LUN Manager を利用することで、iSCSI ポートの配下に複数個の iSCSI ターゲット（以下、単にターゲット）を定義できます。ターゲットごとに LU マッピングとホスト接続モードを設定するため、ホストごとに別々のターゲット（すなわち論理的なボリューム）へアクセスすることが可能になり、ボリューム構成やアクセス認証が柔軟に設定可能になります。
- CHAP によるホスト認証および双方向認証を設定して、ホスト（またはホストのユーザ）からの不用意なアクセスを防止することが可能です。LUN Manager を併用すれば複数のターゲットごとにこれらの認証を設定できます。
- iSCSI ポートに仮想ポートモードを適用すると、1 個のポートに 16 個の仮想ポートを追加できます。VLAN によりネットワークを分割して、複数のセグメントでストレージシステムを使用する場合、仮想ポートを使用することで、ポートおよびネットワークリソースを効率的に使用できます。

H.2.2 iSCSI I/F の仕様

表 H-2 iSCSI I/F 仕様

プロトコル層	項目	仕様
全般	iSCSI ターゲット機能	サポート
	iSCSI イニシエータ機能	サポート
	パス切替	Windows：HDLM、Microsoft DSM/MPIO を使用可能 Linux：HDLM、Device Mapper Multipath を使用可能 VMware：HDLM、Native MultiPath を使用可能
	接続ホスト（コネクション）数	127 コネクション/Port 接続数が多くなると iSCSI Port への負荷が増大するため、127 コネクション/Port 以下での接続を推奨します。
物理層、MAC 層	リンク	10Gbps（Optic）：10Gbps SFP+ 10Gbps（Copper）：10Gbps/1Gbps
	転送速度	10Gbps（Optic）：10Gbps 10Gbps（Copper）：10Gbps/1Gbps
	コネクタ形状	10Gbps（Optic）：LC 10Gbps（Copper）：RJ-45
	ケーブル	10Gbps（Optic）：マルチモードファイバケーブル（OM2/OM3） 10Gbps（Copper）： • 転送速度が 10Gbps の場合は、カテゴリ 6a 以上の LAN ケーブル

プロトコル層	項目	仕様
		• 転送速度が 1Gbps の場合は、カテゴリ 5e/6a 以上の LAN ケーブル
	ネットワークスイッチ	L2 スイッチ、L3 スイッチ 10Gbps（Optic）: IEEE 802.3ae（10Gbps SFP+）準拠 10Gbps（Copper）: • IEEE 802.3an （10GBASE-T）準拠 • IEEE 802.3ab （1000BASE-T）準拠
	スイッチのカスケード	最大 5 段 カスケード段数が増加すると、ホスト I/O の遅延が多くなるため、必要最小限の段数での利用を推奨します。
	MAC アドレス	ポートごと（固定値） 出荷時に World Wide Unique な値を設定しています。変更できません。
	最大通信データ長（MTU）	1500/4500/9000 Byte （イーサネットフレーム）
	ジャンボフレーム	サポート
	リンクアグリゲーション	未サポート
	VLAN	サポート 1～4094 の範囲で設定可能（スイッチのポート VLAN も利用可能）
TCP/IP	IPv4	サポート
	IPv6	サポート
	サブネットマスク	サポート
	ゲートウェイ	サポート
	DHCP	未サポート
	DNS	未サポート
	Ping 送受信	サポート
	IPsec※1	未サポート
	TCP ポート番号	3260（デフォルト） 1～65535 の範囲で変更可能ですが、次の内容に注意してください。 (1) アクセスするホストの設定も変更してください。 (2) 変更後の番号が、経路上のスイッチなどでフィルタリングにより無効化されていないか確認してください。
	Fragment	未サポート
	Window Scale	サポート Window Size 64KB（デフォルト）/128KB/256KB/512KB/1MB
iSCSI	iSCSI Name	iqn※2、eui※3 の両形式をサポート ターゲット設定時に World Wide Unique な iqn 値が自動的に設定されますが、変更もできます。
	Error Recovery Level	レベル 0

プロトコル層	項目	仕様
		ホストのリトライによって障害回復します。レベル 1、2 は未サポート。
	Header digest, Data digest	サポート iSCSI 通信のヘッダ、データ情報をエラーから保護します。iSCSI ポートはホスト側の設定にあわせてこの機能を使用しますが、使用時は性能が低下します（ホストの能力や通信内容によって低下率は変わります）。
	CHAP	サポート ストレージにとって、CHAP に登録したホストからのログインであることを認証します※4。
	Mutual CHAP	サポート （Linux ホストとの接続では未サポート） ホストにとって、CHAP に登録したストレージへのログインであることを認証します。双方向認証または two-way authentication と呼ばれることがあります。
	CHAP User 登録数	最大 256 ユーザ/iSCSI ポート
	iSNS	サポート iSNS（ネームサービス）を利用すれば各ターゲットの IP アドレスを直接知らずともディスカバリできます。

注※1

IP Security。IP パケットの認証と暗号化技術です。

注※2

iqn: iSCSI Qualified Name の意。IP ドメインを使用し、タイプ識別子「iqn.」、ドメイン取得日、ドメイン名、ドメイン取得者が付けた文字列から構成されます。

（例） iqn.2001-03.jp.nec:storage01.d7m.t.10020.1b000.Tar

注※3

eui: 64 ビット Extended Unique Identifier の意。IEEE EUI-64 Format は、タイプ識別子「eui.」とアスキーコード化された 16 進数の EUI-64 識別子から構成されます。

（例） eui.0123456789ABCDEF

注※4

iSCSI の規格では CHAP 動作は、実際にイニシエータからターゲットにログインするログインセッションと、接続可能なイニシエータを検索するディスカバリセッションで実施可能とされています。どちらもサポートしています。

H.2.3 iSCSI 規格

ストレージシステムを構成するためには、次の規格に準拠したスイッチを使用してください。

- IEEE 802.1D STP
- IEEE 802.1w RSTP
- IEEE 802.3 CSMA/CD
- IEEE 802.3u Fast Ethernet
- IEEE 802.3z 1000BASE-X
- IEEE 802.1Q Virtual LANs
- IEEE 802.3ad Dynamic LACP
- IEEE 802.3ae 10 Gigabit Ethernet
- RFC 768 UDP
- RFC 783 TFTP
- RFC 791 IP
- RFC 793 TCP
- RFC 1157 SNMP v1
- RFC 1213 MIB II
- RFC 1757 RMON
- RFC 1901 SNMP v2

H.2.4 注意事項

iSCSI では安価に多数のホストとストレージシステムを接続して IP-SAN を構成することができますが、それによりネットワークやストレージシステムの負荷も増大します。IP-SAN は、ネットワーク／iSCSI ポート／ストレージシステムのコントローラ／ドライブの特定箇所に負荷が集中しないようにシステム構成を設計する必要があります。IP-SAN を設計する場合の注意事項は次のとおりです。

- 通常、LAN はイーサネットの帯域の数分の一を消費して通信するよう設計・構築されるのに対し、iSCSI による通信は利用可能なイーサネットの帯域のほとんどすべてを消費します。IP-SAN と業務用ネットワーク（LAN）を混在すると、構築コストは低く済みますが、次についての注意が必要です。
  - 業務用ネットワークの通信を iSCSI が阻害します。
  - iSCSI の通信と業務用ネットワークの通信が衝突してパケットロスが発生し、iSCSI の転送性能が低下すると、互いに悪影響を与える場合があります。IP-SAN と業務用ネットワークは、別々のネットワークとして構築する必要があるか、帯域設計を確認してください。
- IP-SAN では、ネットワークのパケットロスが発生すると、TCP の輻輳制御のため iSCSI の転送性能が大きく低下します。パケットロスや輻輳制御は、ネットワークの性質上不

可避ですが、IP-SAN 構築ではパケットロスによる影響を少なくできるように、セグメントを分けるなど、ネットワークの構築を確認してください。

- iSCSI の性能（単位時間あたりの実効データ転送量、応答時間など）は、ホストからのアクセスの条件に大きく影響を受けます。また、多数のイニシエータを限られたリソース（ストレージシステムの単一の iSCSI ポートや単一のコントローラなど）へ接続した場合、各ホストからみた性能は低下します。
- ネットワーク機器は Fibre Channel の機器と比べ低価格のため、IP-SAN も安価に構築できますが、個々の機器の性質/品質にシステムの信頼性が依存することになります。機器の選定には注意してください。
- CHAP 認証で iSCSI User Name や Secret を設定するときは、指定に誤りがないか確認してください。誤った設定をすると、次の理由でシステムの正常な運用ができなくなります。
  - ログイン許可されているはずのイニシエータ（ユーザ）がログインできない
  - ログイン許可されていないはずのイニシエータ（ユーザ）がログインできる
- CHAP 認証を使用している環境で、接続しているホストの HBA を交換した場合は、CHAP 認証の設定を変更する必要があります。HBA を交換したあとは、必ず CHAP 認証の設定を変更してください。

  NIC を使用する場合は、NIC を交換しても iSCSI ソフトウェアイニシエータの設定が変わらないので、CHAP 認証の設定の変更は不要です。
- MTU サイズを Default から変更する場合には、ストレージシステムのポートの設定／スイッチ／ホストのすべての機器の変更が必要です。
- CNA を使用する場合は、設定モードで iSCSI Function と NIC Function が存在しますが、NIC Function のみサポートしています。
- Ping 送受信

  iSCSI ポートから unreachable なアドレス※への Ping 送信テストを行うと、I/O 処理に遅延やタイムアウトを起こします。Ping テストはホスト I/O 処理を行っていない状態での実施を強く推奨します。また、複数 iSCSI Port から同時に Ping テストは実施しないでください。

  注※

  Unreachable なアドレスとは、Ping 送信元のポートから物理的・論理的に到達不能な（接続されていない）アドレスを示します。応答が得られないため Ping テストの結果はタイムアウトします。
- スイッチ

  ネットワークスイッチの物理ポートのうち、ホストおよびストレージシステムの iSCSI ポートと直接接続するポートに関して、Spanning Tree が有効の場合、通信が阻害される

可能性があります。Spanning Tree プロトコル機能を OFF にしてください（確認・設定方法は使用するスイッチのマニュアルを参照してください)。

- iSCSI ポートに接続しているスイッチのポートでは、フローコントロール設定を有効にすることを推奨します。フローコントロール設定が無効の場合、iSCSI でのパケットロスが発生しやすくなり、TCP の輻輳制御のため、iSCSI の転送性能低下または応答時間遅延につながる可能性があります。フローコントロール設定を有効にすると、iSCSI の転送性能低下または応答時間遅延が改善される可能性があります。

  ネットワーク全体に影響があるため、事前にシステム構成を検証して最適なフローコントロール設定を確認してください。フローコントロールの設定方法は使用するスイッチのマニュアルを参照してください。

- iSCSI Port 設定

  ホスト接続の状態で iSCSI Port の設定変更を実施する際、一時的に接続が切れホストから再接続が行われます。iSCSI Port 設定変更後 1 分以上時間をあけて、ホストから再接続されたことを確認してください。

- iSCSI Port の IPv6 が有効設定のときは、IPv6 グローバルアドレスを自動に設定すると、IPv6 ルータからプレフィックスを取得してアドレスを決定する動作を行います。

  IPv6 ルータがネットワークに存在しないと、アドレスの決定ができないので、iSCSI 接続に遅延が生じる場合があります。

  iSCSI Port の IPv6 が有効設定のときは、IPv6 ルータが同一ネットワーク上に接続されていることを確認して、IPv6 グローバルアドレスを自動に設定してください。

H.2.5 OS に依存する注意事項

各ホスト共通の注意事項

- iSCSI software initiator と NIC で iSCSI プロトコルの通信をする場合は、iSCSI HBA/CNA を用いる場合と比べ、ホストの CPU 負荷が増大するため、他のアプリケーションの動作が遅くなる可能性があります。
- ホストの iSCSI Digest 設定を有効にすることで、iSCSI Data Digest および iSCSI Header Digest（CRC/Checksum）を使用できます。これらを使用時は通信路上のデータの信頼性が向上しますが、性能が低下します（低下の割合はホストやネットワークなどの環境に依存します。一般的には転送性能が 10%程度低下します。ネットワーク上でのデータ保証強化のため、すべての iSCSI 構成において iSCSI Header Digest および iSCSI Data Digest の使用を推奨します)。
- ホストの NIC は、必ずしもギガビットイーサネットをサポートしていなくても iSCSI プロトコルで通信できますが、性能が低下する場合があります（IP-SAN の構成に依存します)。

- iSCSI 接続構成でホスト側の遅延 Ack が有効設定の場合、ホスト I/O 遅延が発生し、性能に大きな影響を与える可能性があります。このホスト I/O 遅延を回避するためには、遅延 Ack を無効設定に変更する必要があります。

Windows ホスト

- Windows OS がストレス無く動作する処理能力のサーバを利用してください。
- designed for Windows ロゴを取得している iSCSI HBA/CNA または NIC の使用を推奨します。NIC で iSCSI 通信をする場合、iSCSI software initiator はバージョン 2.00 以降をサポートしています。2.00 未満のバージョンでは動作保証外です。
- 利用していないアプリケーションや OS のサービスは停止することを推奨します。これにより不要な通信や負荷を軽減します。
- Windows の場合、LAN ネットワーク内のストレージシステムに設定する iSCSI ターゲット名は全て異なる名前にしてください。複数の物理ポートで同じ iSCSI ターゲット名を設定する必要がある場合は、物理ポート毎にアクセスする iSCSI software initiator を変更してください。

Linux ホスト

- Linux の場合、ホストおよび iSCSI ポートの設定共に双方向 CHAP を ON にしないでください。

H.2.6 iSCSI に関するトラブルシューティング

次に示す 1 つ、もしくは複数の項目が、ホストとストレージシステムが通信できない原因と考えられます。各項目の妥当性を確認し、問題がある場合は対処してください。

表 H-3 確認項目一覧表

項番	確認項目
1	ホストの LAN ポートのリンク状態は正常ですか?
2	ストレージシステムとホスト間のネットワーク周辺機器（スイッチ、ルータや NIC など）の電源状態。機器の電源が OFF だった場合、その電源を ON にしてください。
3	ホストとストレージシステム間のすべての LAN ケーブルが両端共コネクタに接続してありますか？ LAN ケーブルが緩んで接続されていた場合、しっかりと接続し直してください。
4	ストレージシステムに接続している HBA、スイッチまたは NIC のポート転送速度がストレージシステムの転送速度と一致していますか？ ストレージシステムとお客様が準備した機器で一致させてください。
5	VLAN の設定を確認してください。
6	ファイアウォールの設定を確認してください。
7	L3 スイッチやルータの設定を確認してください。
8	ホストの iSCSI ドライバの設定を確認してください。

項番	確認項目
9	ストレージシステムのポートに対して、ホストの IPsec が OFF ですか？ ホストの IPsec の設定は、ストレージシステムのポートに対して OFF である必要があります。
10	ストレージシステムとホストそれぞれの IP アドレス、サブネットマスク、デフォルトゲートウェイや MTU 値の設定がネットワークに適合していますか？ MTU 値は、ストレージシステムに接続されている LAN ネットワーク環境のすべての機器（ホスト、スイッチなど）でストレージシステム iSCSI Port に設定した MTU 値以上の値に設定する必要があります。 IPv6 アドレスで接続している場合、IPv6 アドレス、サブネットマスク、デフォルトゲートウェイや MTU 値の設定がネットワークに適合していますか？ IPv6 アドレスのアドレスステータス（下記の表を参照）でアドレスの状態を確認してください。
11	ホストが iSCSI ドライバを認識できていますか？
12	ホストから Target に誤った IP アドレスと iSCSI Name でログインしていませんか？
13	ホストにストレージシステムの TCP ポート番号が正しく設定してありますか？
14	ホストから「ディスカバリ」と「ログイン」を実施していますか？
15	iSNS サーバを使用している場合、ホストやストレージシステムに iSNS サーバの IP アドレスが正しく設定できていますか？
16	iSNS サーバを使用している場合、iSNS サーバが新規に iSCSI 機器の情報（IP アドレスや iSCSI Name など）を登録できる状態にありますか？
17	CHAP 認証の Initiator 認証を使用している場合、ストレージシステムのポートに Initiator の CHAP User が登録してありますか？ 登録されていない場合、Initiator の CHAP User を新規登録してください。
18	CHAP 認証の Initiator 認証を使用している場合、ストレージシステム側の Initiator の CHAP User に Target の Target 名（例：[000：T000]）が登録してありますか？ 登録されていない場合、Initiator の CHAP User に Target の Target 名を割り当ててください。
19	CHAP 認証の双方向認証を使用している場合、Target の User Name と Secret をホストに正しく設定できていますか？
20	LUN セキュリティを使用している場合、ストレージシステムの Target に割り当てている Initiator の iSCSI Name のリストに、接続する Initiator の iSCSI Name がありますか？ リストにない場合、接続する Initiator の iSCSI Name を Target に割り当ててください。

次の確認項目について対策を実施し、障害が回復することを確認してください。

表 H-4　iSCSI IPv6 接続障害対策表

確認項目		対策
接続する iSCSI Port の IPv6 アドレス、デフォルトゲートウェイアドレスは正しい値が設定されていますか？		iSCSI Port の IPv6 アドレス、デフォルトゲートウェイは、自動生成されます。手動で設定する場合は、お客様の環境に合わせた適切な値を設定してください。
iSCSI Port IPv6 アドレスのアドレスステータス表示	確認中	IPv6 アドレスが、接続ネットワーク内の他のホストとアドレスが重複していないか確認中の状態です。有効に遷移されることを確認してください。
	有効	iSCSI Port の IPv6 アドレスが、重複せず正しく設定されており、アドレスが正常な状態です。

確認項目		対策
	無効	iSCSI Port がリンクダウンしている状態です。 iSCSI Port の IPv6 アドレスを使用する場合は、正しくケーブルが接続されていることを確認してください。
	重複	iSCSI Port の IPv6 アドレスが、接続ネットワーク内の他のホストとアドレスが重複している状態です。重複しない任意の IPv6 アドレスを手動で設定してください。
	未確定	iSCSI Port の IPv6 アドレスが、同一 iSCSI Port 内でアドレス重複している状態です。 iSCSI Port の IPv6 アドレスには、iSCSI Port 内で重複しない任意の IPv6 アドレスを手動で設定してください。
MTU サイズは正しい値が設定されていますか？		IPv6 Link MTU サイズは、ネットワーク上の MTU サイズカレント値を示します。 ストレージシステム iSCSI Port に設定した MTU サイズと Link MTU サイズが異なる場合、ホスト、ルータまたはスイッチの MTU サイズ値がストレージシステムと異なっています。 MTU サイズがストレージシステム iSCSI Port に設定した MTU 値以上の値になるように設定してください。
IPv6 アドレスでのリモートパス設定では、正しく IPv6 アドレスが設定されていますか？		IPv6 アドレスを有効にする必要があります。 リモートパス設定するローカル、およびリモート両方の iSCSI Port において IPv6 アドレスを有効に設定してください。
サーバ内の IPv6 グローバルアドレスは、正しいプレフィックスが設定されていますか？		サーバ内の複数のインターフェースに IPv6 グローバルアドレスを設定する場合、それぞれのインターフェースには異なるプレフィックスを持つ IPv6 アドレスを設定する必要があります。

H.2.7 デバイスタイムアウト値の推奨値

ストレージシステムの論理デバイスに対するデバイスタイムアウト値は、60 秒以上に設定してください。

デバイスタイムアウト値が短いと、コマンドのタイムアウトが発生し、I/O 性能が低下します。

付録 I. ファイアウォール使用環境で必要な設定

ファイアウォールのポリシー・ルールを作成する場合に必要となる、ストレージシステムで使用するポート情報を説明します。

I.1 ファイアウォールの概要

ファイアウォールの主な目的は、ネットワークへの不正侵入による接続攻撃をブロックすることです。ファイアウォールを使用する環境内でストレージシステムを使う場合、ストレージシステムのアウトバウンド接続をするときは、ファイアウォールを遮断する必要があります。

ストレージシステムの着信指示ポートは一時的なポートであり、システムは、ほかの TCP アプリケーションで使われていない利用可能なファーストオープンポートをランダムに選択します。ストレージシステムからのアウトバウンド接続を許可するためには、ファイアウォールを無効にするか、もしくは送信元ファイアウォールルール（ポート元ルールではなく）を作成、または変更しなければなりません。それにより、ストレージシステムの着信アイテムがファイアウォールを遮断することを許可されます。

セキュリティ対策ソフトウェアにファイアウォール機能をサポートしている製品があります。ファイアウォール機能をサポートしているセキュリティ対策ソフトウェアを導入する場合は、必要なポートが利用できるように設定してください。

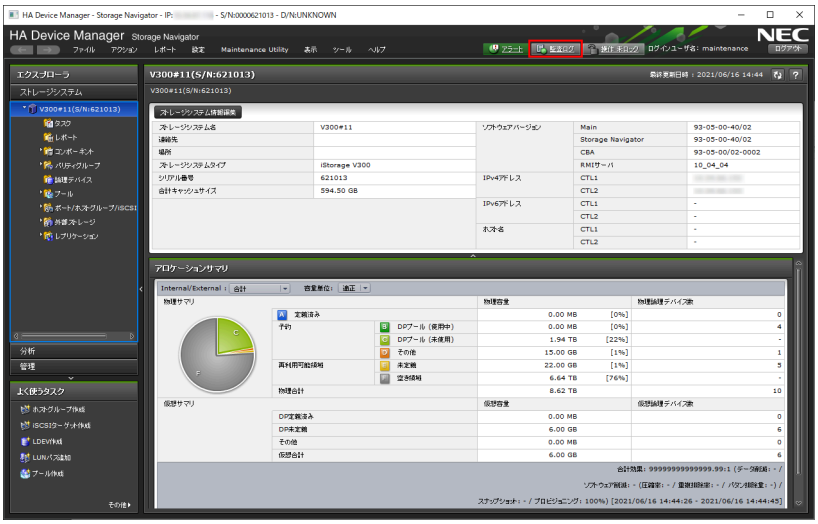
付録 J. SVP に保存された監査ログのエクスポート

Storage Navigator から監査ログをエクスポートする手順を説明します。

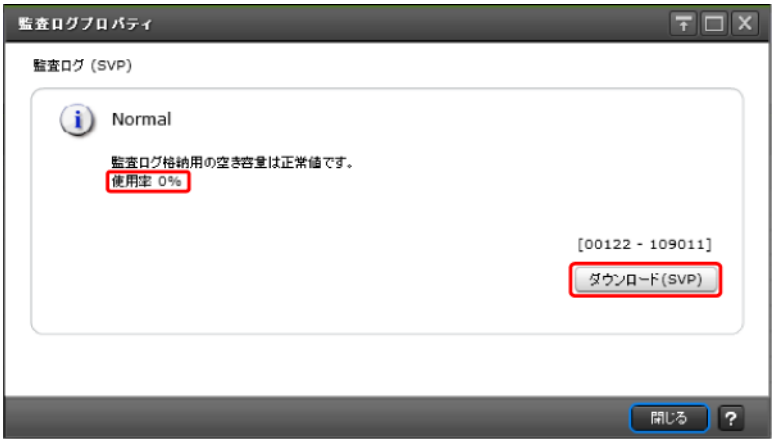
J.1 SVP に保存された監査ログをエクスポートする

操作手順

1. Storage Navigator メイン画面のメニューバー（右上）の［監査ログ］をクリックします。なお、メニューバーに表示されるアイコンは監査ログファイルの蓄積状態を示しています。
   - ：しきい値以下です。
   - ：しきい値に達しましたが、監査ログはまだ保存されています。
   - ：ファイルが満杯になったため、監査ログが上書きされ一部のデータが失われました。



2. ［監査ログプロパティ］画面が表示されます。



項目	内容
使用率	未転送の監査ログの保存容量が、最大保存容量に対してどのくらいかを示します。
ダウンロード（SVP）	次の監査ログをエクスポートします。 • 管理クライアントで設定した操作 • 格納データ暗号化用の暗号化鍵に関する操作のログ • リモートメンテナンス API の実行ログ

3. ［ダウンロード (SVP)］をクリックします。［ダウンロード (SVP)］は Storage Navigator で操作したログをエクスポートすることを示します。

   準備完了のメッセージが表示されます。

4. ［OK］をクリックします。

   エクスポート先を指定する画面が表示されます。

5. エクスポート先とファイル名を指定して［保存］をクリックします。

6. ［閉じる］をクリックします。

付録 K.　管理クライアントから SVP への接続方法

SVP は、管理クライアントからリモートデスクトップ接続して操作することができます。その接続手順を説明します。

K.1　管理クライアントから SVP にリモートデスクトップ接続する

⚠ 注意

リモートデスクトップセッションホストを使用した接続はできません。

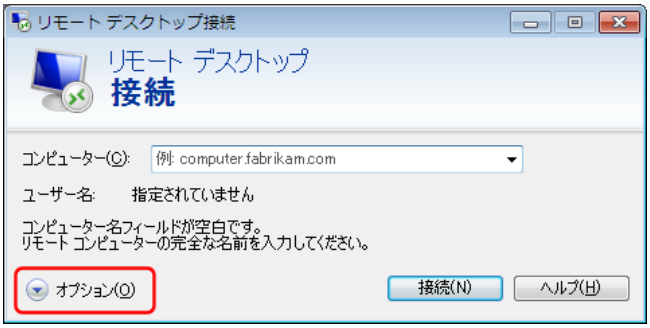
前提条件

- 管理クライアントと SVP が LAN 接続されていること。
- 管理クライアントと SVP の IP アドレスが設定されていること。
- SVP に登録されているユーザアカウントとパスワードを用意していること。

操作手順

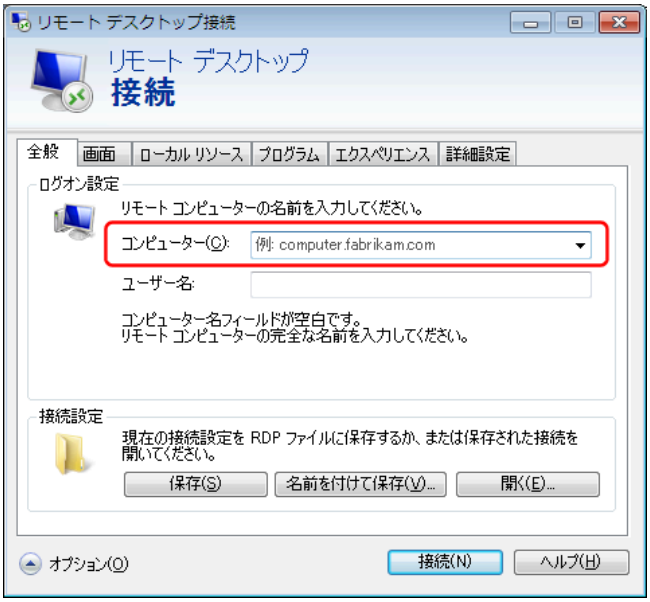
1. スタートメニューから、［すべてのプログラム］（Windows 10 の場合は、「すべてのアプリ」）－［アクセサリ］－［リモートデスクトップ接続］を選択します。Windows 11 の場合は、［すべてのアプリ］－［Windows ツール］ －［リモートデスクトップ接続］を選択します。
2. ［リモートデスクトップ接続］ダイアログが表示されます。

   接続する前にログインの設定を行うため、［オプション］をクリックします。



3. ［コンピューター］欄に、SVP の IP アドレスを入力します。

   また、［ユーザー名］欄に、SVP に登録してあるアカウント名を入力します。



4. ［接続］をクリックします。

メモ

手順 4 のあとに、リモートコンピュータの ID を識別できないが、接続するかどうかを尋ねる警告メッセージが表示された場合、［はい］をクリックしてください。

5. パスワードを入力して SVP に接続します。

お客様で用意しているパスワードを入力してください。

不明な場合は、SVP の管理者（システム管理者）に確認してください。

ログイン先の画面が表示されることを確認してください。

付録 L. SVP で使用するポート番号の変更・初期化

SVP で使用するポート番号を任意のポート番号に変更できます。 また、ポート番号の初期化を行うことで設定を初期状態に戻せます。

他のアプリケーションと SVP が使用するポート番号が重複する場合のみ、この作業を実施してください。 また、ポート番号の変更（または初期化）に伴う影響について、事前に確認してください。

自動割り振りされるポート番号を特定の範囲のポート番号に変更したい場合、「L.6 自動割り振りされるポート番号の範囲を変更する（419 ページ）」を実施後、「L.4 自動割り振りされたポート番号を再割り振りする（416 ページ）」を実施してください。

自動割り振りされるポート番号を特定の範囲のポート番号に初期化したい場合、「L.7 自動割り振りされるポート番号の範囲を初期化する（421 ページ）」を実施後、「L.4 自動割り振りされたポート番号を再割り振りする（416 ページ）」を実施してください。

L.1 SVP で使用するポート番号を変更する

SVP で使用するポート番号を任意のポート番号に変更します。変更に伴い、SVP が使用するサービスは再起動されます。

自動割り振りの設定を変更したい場合は、「L.4 自動割り振りされたポート番号を再割り振りする（416 ページ）」以降を参照してください。

ヒント

- SVP ソフトウェアが、ポート番号の変更をサポートしていないバージョンの場合、ポート番号の変更操作がエラーとなります。 登録したストレージシステムの SVP ソフトウェアを更新してください（「G.2.4 Storage Device List を使用した SVP ソフトウェアの更新（349 ページ）」参照）。
- 管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法（409 ページ）」を参照してください。

前提条件

- Storage Navigator をログアウトしていること。
- Storage Device List の画面が閉じていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
```

```
MappSetPortEdit.bat ［ポート番号キー名］ ［ポート番号］
```

［］内：引数

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

「ポート番号キー名」と「ポート番号の初期値」は次のとおりです。

ポート番号キー名	プロトコル	TCP/UDP	ポート番号の初期値	ポート番号変更可否
MAPPWebServer	HTTP	TCP	80	可
MAPPWebServerHttps	HTTPS	TCP	443	可
RMIClassLoader	RMI	TCP	51099	可
RMIClassLoaderHttps	RMI(SSL)	TCP	5443	可
RMIIFRegist	RMI	TCP	1099	可
PreRMIServer※1	RMI	TCP	自動割り振り	可
DKCManPrivate	RMI	TCP	11099	可
SLP	SLP	TCP、UDP	427	可
CommonJettyStart	HTTP	TCP	8080	可
CommonJettyStop	HTTP	TCP	8210	可
RestAPIServerStart	HTTP	TCP	9080	可
RestAPIServerStop	HTTP	TCP	9210	可
RestAPIClientStart※2	RAID Manager 独自プロトコル	UDP	36000	可
RestAPIClientEnd※2	RAID Manager 独自プロトコル	UDP	37000	可
RestAPIInitiatorStart※3、※4	RAID Manager 独自プロトコル	UDP	35049	可
RestAPIInitiatorEnd※3、※4	RAID Manager 独自プロトコル	UDP	36048	可
DeviceJettyStart※1	HTTP	TCP	自動割り振り	可
DeviceJettyStop※1	HTTP	TCP	自動割り振り	可

注※1

ストレージシステムごとに割り振られます。

注※2

指定した範囲（36000～37000）で処理に必要なポート番号のみが随時、採番され、使用されます。

注※3

RestAPIInitiatorStart のポート番号と、RestAPIInitiatorEnd のポート番号で指定した範囲（初期値は 35049～36048）で、処理に必要なポート番号が割り当てられます。

注※4

対応 SVP ソフトウェアバージョン

- iStorage V100, V300 の場合：93-06-81-XX/XX 以降
- iStorage V10e の場合：全バージョン

メモ

- ポート番号の有効範囲は「1～65535」です。他サービスで使用中のポート番号と競合しないように設定してください。
- 1～1023 のポート番号は他アプリケーションで予約済みのポート番号のため、推奨しません。1～1023 の番号に変更して問題が起きた場合は、1024 以降のポート番号に変更してください。ただし、1024 以降でも、2049、4045、および 6000 のポート番号は、MAPPWebServer と MAPPWebServerHttps に使用できません。
- コマンド入力パラメータ「[ポート番号キー名] [ポート番号]」は、複数指定できます。

  （例）`MappSetPortEdit.bat MAPPWebServer 81 MAPPWebServerHttps 444`
- SVP で使用するポート番号は、「L.8 SVP で使用されるポート番号の参照（422 ページ）」に記載された手順で確認してください。
- サービス再起動メッセージに続けて、完了メッセージが表示されます。
- ［ポート番号キー名］のみ、大文字・小文字の区別が必要です。

3. サービス再起動メッセージに続けて、完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. 「L.8 SVP で使用されるポート番号の参照（422 ページ）」を参照して変更内容を確認します。

メモ

間違えて設定した場合は、再度手順 1 から設定してください。

6. コマンドプロンプトを閉じます。

L.2 SVP で使用するポート番号を初期化する

SVP で使用するポート番号の設定を初期状態に戻します。初期化に伴い、SVP が使用するサービスは再起動されます。

自動割り振りされたポート番号を初期化する場合は、「L.5 自動割り振りされたポート番号を初期化する（417 ページ）」を参照してください。ポート番号の初期値は、「L.1 SVP で使用するポート番号を変更する（411 ページ）」の表を参照してください。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法 (409 ページ)」を参照してください。

前提条件

- Storage Navigator をログアウトしていること。
- Storage Device List の画面が閉じていること。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappSetPortInit.bat
   ```

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 初期化の実行確認メッセージが表示されます。

   処理を続行する場合、[y] を入力してから Enter キーを押してください。処理を取り消す場合、[n] を入力してから Enter キーを押してください。

4. サービス再起動メッセージに続けて、完了メッセージが表示されます。
5. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
6. コマンドプロンプトを閉じます。

L.3 SVP で使用するポート番号変更時の影響

SVP と接続するクライアント側で SVP が使用するポートに対して、TCP/IP のポートを使用できるようにファイアウォール設定をしている場合、SVP の変更後ポートに合わせて設定してください（変更前のポートはファイアウォールの開放設定を閉じてください）。

各ポート番号の影響は次のとおりです。

ポート番号キー名	影響内容	変更方法の記載マニュアル
MAPPWebServer MAPPWebServerHttps	Storage Navigator にログインする URL 指定時に、ポート番号を指定する必要があります。	本マニュアルの「A.9.1 Storage Navigator にログインする（208 ページ）」
RMIClassLoader	エクスポートツール(ExportTool) コマンド実行時、java コマンドの el.dlport オペランドで指定するポート番号に、エクスポートツールをダウンロードするときに使用するポート番号を指定します。	『Performance Manager (Performance Monitor, Server Priority Manager, QoS) ユーザガイド』
RMIClassLoaderHttps	構成レポート取得／階層再配置ログ作成プログラム（raidinf コマンド） • Storage Navigator に raidinf コマンドでログイン時、SVP の IP アドレス(またはホスト名)に加えて、<SVP の変更ポート>を指定する。	『HA Device Manager - Storage Navigator ユーザガイド』の「付録」
RMIIFRegist	エクスポートツール(Export Tool) • コマンド実行時、「ip サブコマンド」にて SVP の IP アドレスに加えて、<SVP の変更ポート>を指定する。	『Performance Manager (Performance Monitor, Server Priority Manager, QoS) ユーザガイド』
PreRMIServer	影響なし	－
DKCManPrivate	影響なし	－
CommonJettyStart	影響なし	－
CommonJettyStop	影響なし	－
RestAPIServerStart	影響なし	－
RestAPIServerStop	影響なし	－
RestAPIClientStart	影響なし	－

ポート番号キー名	影響内容	変更方法の記載マニュアル
RestAPIClientEnd	影響なし	―
RestAPIInitiatorStart	影響なし	―
RestAPIInitiatorEnd	影響なし	―
DeviceJettyStart	影響なし	―
DeviceJettyStop	影響なし	―

L.4 自動割り振りされたポート番号を再割り振りする

ストレージシステムごとに自動的に割り振りされたポート番号を再度割り振りできます。

ストレージシステムに割り振られたポート番号が、他のアプリケーションで使用された場合は、そのポートに対して再割り振りされます。

メモ

- 再割り振りするストレージシステムのサービスを停止してから再割り振りを実行してください。

  停止せずに実行した場合は、Storage Device List 画面で対象のストレージシステムのサービスを停止してから、サービスを開始してください。
- ストレージシステムのサービス開始時に割り振りされる DeviceJettyStart と DeviceJettyStop のポートは、再割り振りされません。
- ポートを使用している機能を無効化した場合は、割り振りされているポート番号を削除します。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法 (409 ページ)」を参照してください。

操作手順

1. 再割り振りするストレージシステムの Storage Navigator をログアウトします。
2. 再割り振りするストレージシステムのサービスを停止します。
3. SVP で Windows のコマンドプロンプトを管理者権限で起動します。

4. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappPortManageRenum.bat ［シリアル番号］（任意）
   ```

   ［］内：引数

   ［シリアル番号］を省略した場合、Storage Device List に登録したストレージシステムに対して実行されます。

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

5. 再割り振りの実行確認メッセージが表示されます。

   処理を続行する場合、［y］を入力してから Enter キーを押してください。

   処理を取り消す場合、［n］を入力してから Enter キーを押してください。

6. 完了メッセージが表示されます。
7. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
8. コマンドプロンプトを閉じます。
9. 再割り振りしたストレージシステムのサービスを開始します。

L.5 自動割り振りされたポート番号を初期化する

ストレージシステムごとに自動的に割り振りされたポート番号を初期化できます。

メモ

- Storage Device List のステータスが［Ready］のストレージシステムをすべてサービス停止してから初期化を実行してください。
- 自動割り振りされたポート番号の初期値は、「L.1 SVP で使用するポート番号を変更する（411 ページ）」の表を参照してください。
- 停止せずに初期化を実行した場合は、そのストレージシステムに対して、「L.4 自動割り振りされたポート番号を再割り振りする（416 ページ）」を実行してください。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法 (409 ページ)」を参照してください。

操作手順

1. Storage Navigator をログアウトします。
2. Storage Device List のステータスが［Ready］のストレージシステムをすべてサービス停止します。
3. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
4. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappPortManageInit.bat
   ```

   ### ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

5. 初期化の実行確認メッセージが表示されます。

   処理を続行する場合、［y］を入力してから Enter キーを押してください。

   処理を取り消す場合、［n］を入力してから Enter キーを押してください。
6. 完了メッセージが表示されます。
7. 「続行するには何かキーを押してください . . .」のメッセージが表示されます。任意のキーを入力します。
8. 再割り振りを実行します。

   ```
   MappPortManageRenum.bat ［シリアル番号］（任意）
   ```

   ［］内：引数

   ［シリアル番号］を省略した場合、Storage Device List に登録したストレージシステムに対して実行されます。

   ### ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

9. 再割り振りの実行確認メッセージが表示されます。

   処理を続行する場合、[y] を入力してから Enter キーを押してください。

   処理を取り消す場合、[n] を入力してから Enter キーを押してください。

10. 完了メッセージが表示されます。
11. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
12. 手順 8～手順 11 を実行して、登録しているすべてのストレージシステムに対してポート番号の再割り振りを実行します。
13. コマンドプロンプトを閉じます。
14. 操作するストレージシステムのサービスを開始します。

L.6 自動割り振りされるポート番号の範囲を変更する

ストレージシステムごとに自動的に割り振りされるポート番号の範囲を変更できます。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法 (409 ページ)」を参照してください。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet
   ```

   ```
   MappPortRangeSet.bat ［ポート番号キー名］ ［ポート番号範囲］
   ```

   [] 内：引数

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

変更できる「ポート番号キー名」と「ポート番号範囲の初期値」は次のとおりです。

0 番ポートは、本コマンドの設定に関係なく、割り振りされません。

ポート番号キー名	ポート番号範囲の初期値	ポート割り振りのタイミング
PreRMIServer	51100～51355	Storage Device List にストレージシステムを登録した時点
DeviceJettyStart	48081～48336	ストレージシステムのサービスを開始した時点※1
DeviceJettyStop	48411～48666	
available※2	49152～65535	
unavailable※3	1～1023	

注※1

ストレージシステムのサービス開始により割り振られたポートは、サービスが停止すると解除されます。

注※2

PreRMIServer、DeviceJettyStart、および DeviceJettyStop で指定したポート番号の範囲が、すべて使われている場合は、available で指定したポート番号の範囲から割り振られます。

注※3

自動割り振りで使用されたくないポート番号の範囲を指定します。

メモ

- ポート番号範囲の有効範囲は「1～65535」です。他サービスで使用中のポート番号と競合しないように 設定してください。
- Windows の Ephemeral Ports（49152～65535）を使用すると競合する可能性があります。

  競合が発生した場合は、このポート番号範囲を除外して範囲の変更をしてください。
- 「1～1023」のポート番号は、他のアプリケーションで予約済みのポート番号です。

  unavailable の設定 値から「1～1023」を除外すると、正常に動作しなくなる場合があります。
- ポート番号範囲を変更する場合、少なくとも Storage Device List に登録したストレージシステムの台数分が含まれる範囲を指定してください。
- 有効範囲で使用可能な文字列は、次の通りです。"数字" "," "-" "rm"

  ポート番号範囲が連続する場合、「-」でつないでください。

  （例）PreRMIServer のポート番号 51200 から 55000 を指定したい場合

  MappPortRangeSet.bat PreRMIServer 51200-55000

ポート番号範囲が不連続な場合、「,」でつないでください。

（例）PreRMIServer のポート番号 51200 と 55000 を指定したい場合

MappPortRangeSet.bat PreRMIServer 51200,55000

ポート番号範囲が 1 つの場合も、「-」または「,」でつないでください。

（例）PreRMIServer のポート番号 51200 を指定したい場合

MappPortRangeSet.bat PreRMIServer 51200-51200

MappPortRangeSet.bat PreRMIServer 51200,51200

"rm"はポート番号キー名単位に設定を削除します。

（例）PreRMIServer rm

- コマンド入力パラメータ「[ポート番号キー名] [ポート番号範囲]」は、複数指定できます。

  [] 内：引数

  （例）MappPortRangeSet.bat PreRMIServer 51200-55000 DeviceJettyStart 48181-48336,8000

- unavailable に設定されたポート番号範囲は、他のキーの有効範囲であっても、使用できません。

  （例）PreRMIServer 51100-51355 unavailable 51100-51200 のように設定した場合、PreRMIServer で割り振りされるポート番号範囲は、51201-51355 になります。

3. 完了メッセージが表示されます。
4. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
5. コマンドプロンプトを閉じます。

上記の操作を実施後、「L.4 自動割り振りされたポート番号を再割り振りする (416 ページ)」を実施してください。自動割り振りされるポート番号の範囲を変更しただけでは、ポート番号は変更されません。

L.7 自動割り振りされるポート番号の範囲を初期化する

ストレージシステムごとに自動的に割り振りされるポート番号の範囲を初期化できます。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法 (409 ページ)」を参照してください。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

   ```
   cd /d C:\Mapp\wk\Supervisor\MappIniSet

   MappPortRangeInit.bat
   ```

   ヒント

   C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

   「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. 初期化の実行確認メッセージが表示されます。

   処理を続行する場合、[y] を入力してから Enter キーを押してください。

   処理を取り消す場合、[n] を入力してから Enter キーを押してください。
4. 完了メッセージが表示されます。
5. 「続行するには何かキーを押してください...」のメッセージが表示されます。任意のキーを入力します。
6. コマンドプロンプトを閉じます。

上記の操作を実施後、「L.4 自動割り振りされたポート番号を再割り振りする (416 ページ)」を実施してください。

L.8 SVP で使用されるポート番号の参照

SVP で使用されるポート番号を参照できます。

ヒント

管理クライアントから SVP にリモートデスクトップ接続して、SVP を操作することもできます。リモートデスクトップ接続を行う場合は、「付録 K. 管理クライアントから SVP への接続方法 (409 ページ)」を参照してください。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. カレントディレクトリをツールが存在するディレクトリに移動し、次のコマンドを実行します。

```
cd /d C:\Mapp\wk\Supervisor\MappIniSet
MappPortRefer.bat ［シリアル番号］（任意）
```

［］内：引数

［シリアル番号］を省略した場合、Storage Device List に登録したストレージシステムすべての情報が表示されます。

ヒント

C:\Mapp：ストレージ管理ソフトウェア、および SVP ソフトウェアのインストールディレクトリを示します。

「C:\Mapp」以外をインストールディレクトリに指定した場合は、「C:\Mapp」を、指定のインストールディレクトリに置き換えてください。

3. SVP で使用されるポート番号の情報が表示されます。

   番号が割り振られていないポートは、［Not Defined］が表示されます。

4. 完了メッセージが表示されます。
5. 「続行するには何かキーを押してください...」 のメッセージが表示されます。任意のキーを入力します。
6. コマンドプロンプトを閉じます。

L.9 ポート番号を使用しているアプリケーションを確認する

どのポート番号が、どのアプリケーションで使用されているを確認できます。

操作手順

1. SVP で Windows のコマンドプロンプトを管理者権限で起動します。
2. netstat コマンドを使用して、ポート番号を使用しているプロセス ID を特定してください。

ヒント

Storage Device List で、ストレージシステムのサービスを停止してから netstat コマンドを実行すると、ストレージ管理ソフトウェア、および SVP ソフトウェア以外のアプリケーションが使用しているポート番号だけが出力されます。

［例］

```
>netstat -ano

  プロトコル  ローカル アドレス          外部アドレス        状態           PID
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING       2184
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       988
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:623            0.0.0.0:0              LISTENING       2624
  TCP    0.0.0.0:1099           0.0.0.0:0              LISTENING       1548
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1620
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       5216
  TCP    0.0.0.0:11099          0.0.0.0:0              LISTENING       5388
  TCP    0.0.0.0:16992          0.0.0.0:0              LISTENING       2624
```

コマンドの実行結果から、ポート番号 8080 を使用しているプロセス ID（5216）が特定できます。

ストレージ管理ソフトウェア、および SVP ソフトウェアが使用するポートを以下に示します。

ポート番号キー名	プロトコル	TCP/UDP	ポート番号の初期値	ポート番号変更可否
MAPPWebServer	HTTP	TCP	80	可
MAPPWebServerHttps	HTTPS	TCP	443	可
RMIClassLoader	RMI	TCP	51099	可
RMIClassLoaderHttps	RMI(SSL)	TCP	5443	可
RMIIFRegist	RMI	TCP	1099	可
PreRMIServer	RMI	TCP	自動割り振り	可
DKCManPrivate	RMI	TCP	11099	可
SLP	SLP	TCP、UDP	427	可
CommonJettyStart	HTTP	TCP	8080	可
CommonJettyStop	HTTP	TCP	8210	可
RestAPIServerStart	HTTP	TCP	9080	可
RestAPIServerStop	HTTP	TCP	9210	可
RestAPIClientStart	RAID Manager 独自プロトコル	UDP	36000	可
RestAPIClientEnd	RAID Manager 独自プロトコル	UDP	37000	可
RestAPIInitiatorStart※	RAID Manager 独自プロトコル	UDP	35049	可
RestAPIInitiatorEnd※	RAID Manager 独自プロトコル	UDP	36048	可
DeviceJettyStart	HTTP	TCP	自動割り振り	可
DeviceJettyStop	HTTP	TCP	自動割り振り	可

注※

対応 SVP ソフトウェアバージョン

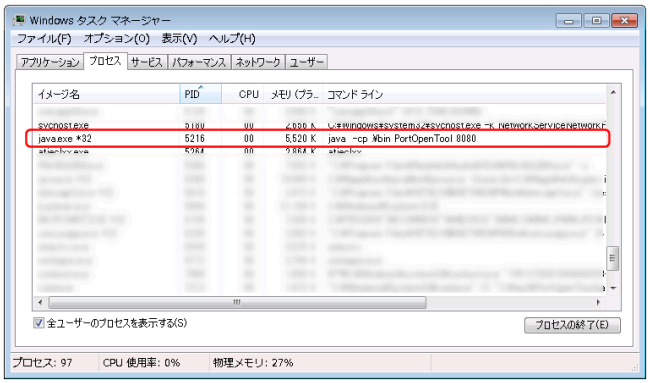
- iStorage V100, V300 の場合：93-06-81-XX/XX 以降
- iStorage V10e の場合：全バージョン

3. タスクマネージャを起動して、手順 2 で特定したプロセス ID のアプリケーションを特定してください。

   タスクマネージャの［詳細］タブで、列の部分を右クリックし、［列の選択］からコマンドラインを選択してください。

   ［例］

   プロセス ID（5216）が java.exe のアプリケーションの場合



   java.exe の場合は、コマンドラインも参照することで、アプリケーションを特定することができます。

付録 M.　障害通知メール、Syslog メッセージ、SNMP メッセージの内容

障害通知メール、Syslog メッセージ、および SNMP メッセージの内容について説明します。

M.1　障害通知メールの内容

ストレージシステムからメールサーバに送付される障害通知メールの内容を示します。

障害通知メールの例

```
StorageSystemName Report
////////////////////////////////
//e-Mail Report
////////////////////////////////
Date : 20/04/2018
Time : 00:20:00
Machine : StorageSystemName(Serial# 64019)
RefCode : 7fffff
Detail: This is Test Report.
```

障害通知メールの各項目について次の表で説明します。

構成要素	例の項目	内容
メールタイトル	StorageSystemName Report	（ストレージシステムの装置名）＋ Report
付加情報	//////////////////////////////// //e-Mail Report ////////////////////////////////	「3.3.1　メール通知の設定（61 ページ）」で設定した内容 未設定の場合は何も表示されません。
日付	Date : 20/04/2018	障害が発生した日付
時刻	Time : 00:20:00	障害が発生した時刻
ハードウェア識別情報	Machine : StorageSystemName(Serial# 64019)	「3.3.1　メール通知の設定（61 ページ）」で設定したストレージシステム名"+"(Serial#"+"シリアル番号)"
障害コード	RefCode : 7fffff	アラート画面に表示される SIM リファレンスコード
障害情報	Detail: This is Test Report.	保守作業に必要な不良個所の情報 最大 8 件の不良個所の情報が表示されます。 1 件の不良個所の情報には、[アクションコード]、[想定障害部品]、および［ロケーション］の項目が含まれます。

M.2　Syslog メッセージの内容

ストレージシステムから syslog サーバに送付されるメッセージの内容を示します。

メモ

アラート通知の Syslog メッセージと、監査ログの Syslog メッセージでは内容が異なります。

本節では、アラート通知の Syslog メッセージの内容を示します。監査ログの Syslog メッセージの内容は、『監査ログ リファレンスガイド』を参照してください。

メッセージの書式は RFC3164 準拠と RFC5424 準拠の 2 種類があり、Maintenance Utility で選択します。

書式の選択については、「3.3.3 アラート通知を蓄積するための Syslog の設定（63 ページ）」および「3.7.1 監査ログを蓄積するための Syslog の設定（76 ページ）」を参照してください。

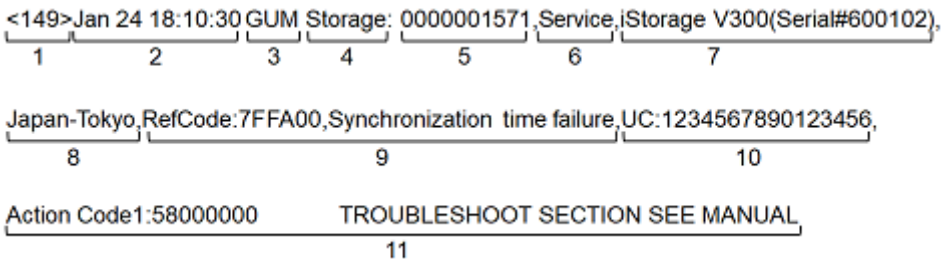


図 M-1 RFC3164 に準拠した syslog メッセージのフォーマット

表 M-1 RFC3164 に準拠した syslog メッセージの内容

項番	項目	説明
1	プライオリティ	括弧（<>）内にプライオリティ値が出力されます。 プライオリティ値 = 8× Facility + Severity Facility は 18 (固定)です。 Severity はログ情報の種類によって、次の値を示します。 • 3：Error（異常終了）の場合 • 4：Warning（部分的な異常終了、または操作が途中でキャンセルされた）の場合 • 5：Notice（通知）の場合 例えば、Severity が Error の場合、プライオリティ値は<147>が出力されます。
2	日付・時刻※	日付と時刻が、「MMM DD HH:MM:SS」の形式で出力されます（MMM：月、DD：日、HH：時、MM：分、SS：秒）。 月の出力形式「MMM」は英語の省略形（Jan～Dec）が出力されます。 日付の出力形式「DD」で、1 桁の日付のときは、空白の次に日付が出力されます。例えば、1 日のときは、「 1」と出力されます。
3	検出場所	「GUM」固定です。
4	プログラム名	「Storage」固定です。
5	メッセージ識別情報	“0000000000”から“4294967295”までの通し番号が出力されます。
6	事象の種別	下記に示す事象のカテゴリ名が出力されます。事象のカテゴリは Severity と対応しています。 • Acute Severity は 3（Error）です。 • Serious

項番	項目	説明
		Severity は 3（Error）です。 • Moderate Severity は 4（Warning）です。 • Service Severity は 5（Notice）です。
7	ハードウェア識別情報	装置モデル名称と、シリアル番号が出力されます。
8	付随情報	Maintenance Utility の［Syslog］タブで設定したロケーション識別情報が出力されます。
9	詳細情報	アラート画面に表示される SIM リファレンスコードと、障害情報が出力されます。
10	ユーザーシステムコード	Maintenance Utility の ALIVE 設定で設定したユーザーシステムコードが出力されます。 桁数は先頭 16 文字までで、ユーザーシステムコードが 16 文字未満の場合は 16 文字分まで半角空白が出力されます。 ALIVE 設定は保守員のみ設定可能です。
11	アクションコード	アラート詳細画面のアクションコード、想定障害部品、ロケーションが最大 8 個まで出力されます。 アクションコードが複数ある場合、以下の通り "|" 区切りで複数出力されます。 `Action Code1:58000000 TROUBLESHOOT SECTION SEE MANUAL |Action Code2:40700100 DKC PS(AC) DKCPS2 |Action Code3:40812100 CTL(Not Encryption) CTL2 |Action Code4:40812000 CTL(Not Encryption) CTL1` Maintenance Utility よりテスト送信を実施した場合、アクションコードは出力されません。

注※

ログに出力される日付と時刻は、SVP に設定された日付と時刻です。ストレージシステム内で SVP 障害や LAN 障害などが発生したときは、日付と時刻が 1970/01/01 からの積算時間になることがあります。

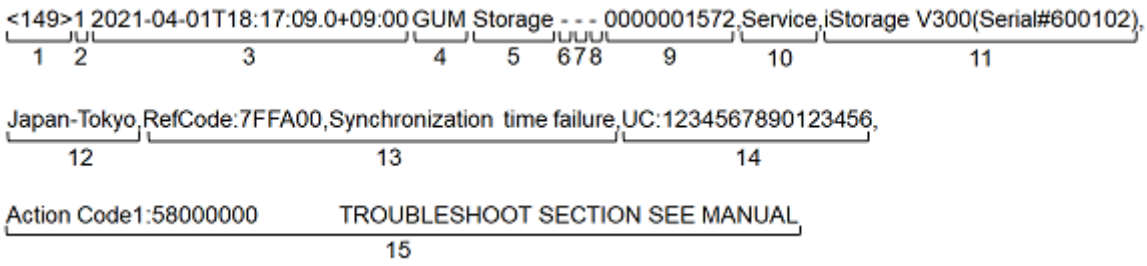


図 M-2 RFC5424 に準拠した syslog メッセージのフォーマット

表 M-2 RFC5424 に準拠した syslog メッセージの内容

項番	項目	説明
1	プライオリティ	括弧（<>）内にプライオリティ値が出力されます。 プライオリティ値 = 8× Facility + Severity

項番	項目	説明
		Facility は 18 (固定)です。 Severity はログ情報の種類によって、次の値を示します。 • 3：Error（異常終了）の場合 • 4：Warning（部分的な異常終了、または操作が途中でキャンセルされた）の場合 • 5：Notice（正常終了）の場合 例えば、Severity が Error の場合、プライオリティ値は<147>が出力されます。
2	バージョン	「1」固定です。
3	日付・時刻※	日付、時刻、および UTC（協定世界時）との時差が、「YYYY-MM-DDThh:mm:ss.s±hh:mm」の形式で出力されます（YYYY：年、MM：月、DD：日、hh：時、mm：分、ss.s：秒、hh：時差の時間、mm：時差の分）。 ただし、UTC との時差がないときは、「±hh:mm」の出力形式の代わりに「Z」の文字が出力されます。例えば、「2018-12-26T23:06:58.0Z」のように出力されます。 秒の出力形式「ss.s」は、小数点第 1 位まで出力されることを示します。
4	検出場所	「GUM」固定です。
5	プログラム名	「Storage」固定です。
6	プロセス名	「-」固定です。
7	メッセージ ID	「-」固定です。
8	構造化データ	「-」固定です。
9	メッセージ識別情報	“0000000000”から“4294967295”までの通し番号が出力されます。
10	事象の種別	下記に示す事象のカテゴリ名が出力されます。事象のカテゴリは Severity と対応しています。 • Acute Severity は 3 です。 • Serious Severity は 3 です。 • Moderate Severity は 4 です。 • Service Severity は 5 です。
11	ハードウェア識別情報	装置モデル名称と、シリアル番号が出力されます。
12	付随情報	Maintenance Utility の［Syslog］タブで設定したロケーション識別情報が出力されます。
13	詳細情報	アラート画面に表示される SIM リファレンスコードと、障害情報が出力されます。
14	ユーザーシステムコード	Maintenance Utility の ALIVE 設定で設定したユーザーシステムコードが出力されます。 桁数は先頭 16 文字までで、ユーザーシステムコードが 16 文字未満の場合は 16 文字分まで半角空白が出力されます。 ALIVE 設定は保守員のみ設定可能です。
15	アクションコード	アラート詳細画面のアクションコード、想定障害部品、ロケーションが最大 8 個まで出力されます。 アクションコードが複数ある場合、以下の通り "|" 区切りで複数出力されます。

項番	項目	説明
		Action Code1:58000000　TROUBLESHOOT SECTION SEE MANUAL　|Action Code2:40700100　DKC PS(AC)　DKCPS2　|Action Code3:40812100　CTL(Not Encryption)　CTL2　|Action Code4:40812000　CTL(Not Encryption)　CTL1 Maintenance Utility よりテスト送信を実施した場合、アクションコードは出力されません。

注※

ログに出力される日付と時刻は、SVP に設定された日付と時刻です。ストレージシステム内で SVP 障害や LAN 障害などが発生したときは、日付と時刻が 1970/01/01 からの積算時間になることがあります。

M.3　SNMP メッセージの内容

ストレージシステムから SNMP エージェントに送付される SNMP メッセージの内容を示します。

SNMP エージェントがサポートするトラップ種別は、『SNMP Agent ユーザガイド』を参照してください。

SNMP の表示例（使用するクライアント側のアプリケーションによって異なります）

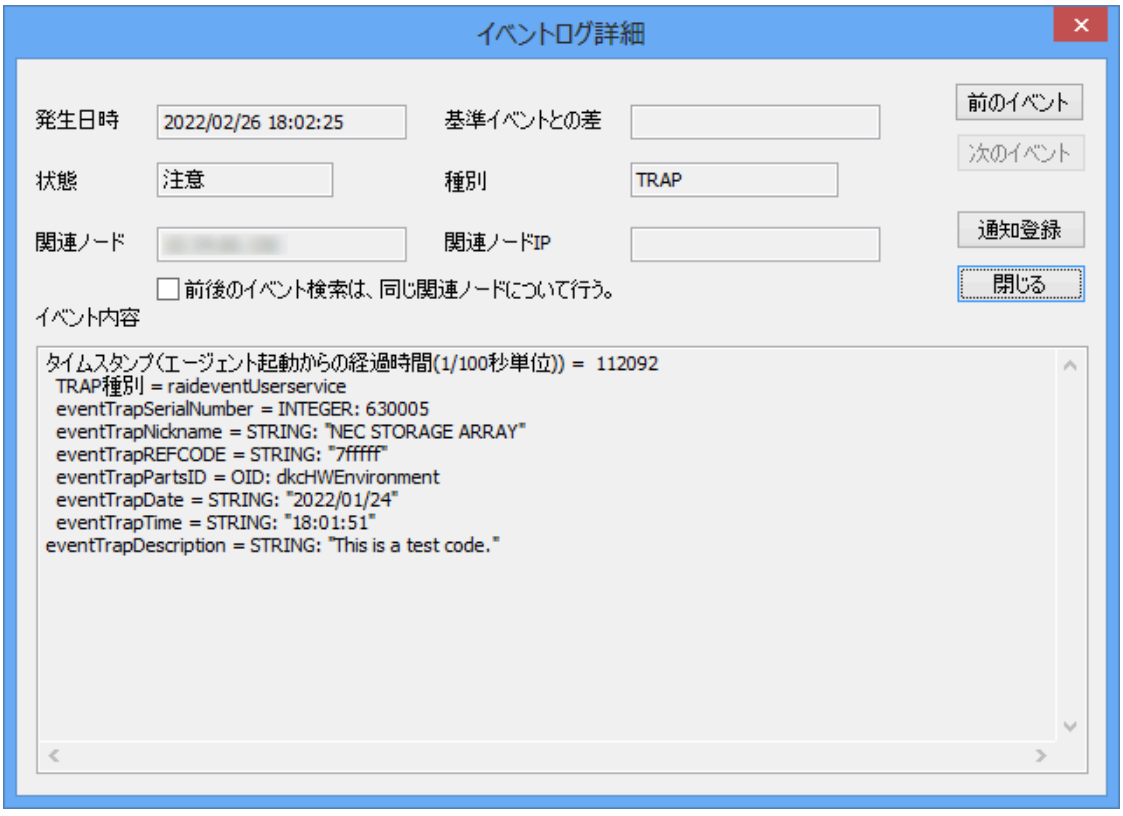


図 M-3　SNMP の表示例

イベント内容について次の表で説明します。

構成要素	例	内容
TRAP 種別	raideventUserservice	障害レベル
eventTrapSerialNumber	630005	装置製品番号
eventTrapNickname	NEC STORAGE ARRAY	製品名
eventTrapREFCODE	7fffff	アラート画面に表示される SIM リファレンスコード
eventTrapPartsID	dkcHWEnvironment	障害の部位
eventTrapDate	2022/01/24	SNMPAgent が受信した日付
eventTrapTime	18:01:51	SNMPAgent が受信した時間
eventTrapDescription	"This is a test code."	保守作業に必要な不良個所の情報

付録 N.　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。

N.1　モデルやファームウェアバージョンによる転送プロトコルの表示の差異

モデルやファームウェアバージョンによって設定項目や表示項目に示される表示内容が異なります。このマニュアルでは、iStorage V100, V300 の最新ファームウェアバージョンで示される表示内容を使って説明しています。

設定項目/表示項目	iStorage V100, V300		iStorage V10e	
	93-06-41-XX 以降	93-06-41-XX 未満	88-08-11-XX/XX 以降	88-08-11-XX/XX 未満
転送プロトコル	• TLS/RFC5424 • UDP/RFC3164	• TLS1.2/RFC5424 • UDP/RFC3164	• TLS/RFC5424 • UDP/RFC3164	• TLS1.2/RFC5424 • UDP/RFC3164

用語集

bps (bits per second)

データ転送速度の標準規格です。

CHAP (Challenge Handshake Authentication Protocol)

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

CNA

Converged Netwark Adapter

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。

CTL

Controller のことです。

DHCPv4

各クライアントが起動したときに、サーバが自動的に IPv4 アドレスを割り当てるクライアント/サーバ型のプロトコルのことです。

EIA

米国電子工業会のことを示します。単位として使用している場合、1 EIA=44.45 mm 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。

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。

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。

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)

ホストコンピュータのバスと、2 つのチャネル間の情報転送を管理するファイバチャネルループとの間に位置する I/O アダプタ。

ホストプロセッサの性能に対する影響を最小限にするために、ホストバスアダプタは、多くの低レベルのインターフェース機能を自動的に行う、またはプロセッサの関与を最小にします。

Initiator (iSCSI initiator)

サーバとストレージシステム間の通信を制御するサーバにインストールされている iSCSI 特有のソフトウェア。

Internet Explorer

Windows Internet Explorer

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。

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

LAN ボード

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

LDEV (logical device)

ストレージシステムに作成されるボリューム。

LRU

キャッシュメモリのデータ領域を開放する必要がある場合、すでにあるキャッシュメモリ上のデータをドライブに書き出すときに、最も長い時間使用していないデータを選択するアルゴリズムです。

NIC

Network Interface Card

Point to Point

2 点を接続して通信するトポロジ。

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。

SAS ケーブル

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

SNMP

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。

Storage Device List

ストレージシステムを管理するために使用されるアプリケーション。

Storage Navigator のコンポーネントの一つです。

Storage Navigator

ストレージシステムのストレージ機能を構成および管理するために使用されるマルチ機能のスケーラブルストレージ管理アプリケーション。

Storage Navigator は HA Device Manager のコンポーネントの 1 つです。

このマニュアルでは、HA Device Manager - Storage Navigator のことを「Storage Navigator」と呼びます。

SVP (SuperVisor PC)

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

UEFI

Unified Extensible Firmware Interface

UPS

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。

Windows

Microsoft Windows Operating System

WINS

Windows Internet Name Service

仮想ボリューム

実体を持たない、仮想的なボリュームです。Dynamic Provisioning、Dynamic Tiering、または Realtime Tiering で使用する仮想ボリュームを DP-VOL とも呼びます。

管理クライアント

SVP を操作するためのコンピュータです。

キャッシュ(キャッシュメモリ)

キャッシュメモリ(Cache Memory)とは、コントローラボードに搭載されるキャッシュメモリです。

メモリには、読み書きしたデータを一時的に保存し、ハードディスクより処理速度の早いメモリからデータを読み書きすることで、データ処理時間を短縮します。

クラスタ

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

スペアドライブ

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

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。

チャネルボード

コントローラシャーシに搭載され、ホストとのインターフェース機能を有します。

ディスクボード

コントローラシャーシに搭載され、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。

ドライブボックス

コントローラシャーシに接続される、ドライブを搭載するための筐体です。

パリティグループ

１つ以上のボリュームをまとめることのできる一連のディスクです。

パリティドライブ

RAID5 を構成するときに、1 つの RAID グループの中で 1 台のドライブがパリティドライブとなり、残りのドライブがデータドライブとなります。パリティドライブには複数台のデータドライブのデータから計算されたデータが記憶されます。これにより 1 つの RAID グループ内で 1 台のドライブが故障した場合でも、パリティドライブから再計算することでデータを損なわずにストレージシステムを使用できます。

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

ファームウェア

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

フラッシュメモリ

情報の書き換えが可能な ROM のことです。

EEPROM(Electrically Erasable and Programmable ROM)の一種です。電源の供給がなくても記憶内容を保持できるので、外部記憶装置などに多く利用されています。

ペア

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

ペア状態

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

ラック

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

リモートパス

ローカルストレージシステムとリモートストレージシステム上の同じポートに接続するルート。2 つのリモートパスは各ストレージシステム用に設定される必要があります（ストレージシステムに搭載された 2 台のコントローラボードごとに 1 パス）。

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。

索引

C

CHAP 認証.....308

F

Fibre Channel
　マッピング情報の設定..... 297

I

iSCSI
　概要..... 397
　規格..... 399
　トラブルシューティング..... 403

P

Port
　ポート..... 232,233,304,305

S

SNMP エージェントの設定.....66
Storage Navigator
　トラブルシューティング..... 101
　ログイン..... 208

あ

アラート通知を蓄積するための Syslog サーバへのテストメッセージの送信..... 64
アラート通知を蓄積するための Syslog の設定... 63

か

監査ログ管理者（参照・編集）.....35
監査ログ管理者（参照）.....35
規格
　iSCSI.....399
構築
　スペアドライブの増設..... 292
　パリティグループの削除..... 294
　ポート..... 232,233,304,305
　論理デバイスの削除..... 300

さ

削除
　パリティグループ..... 294
　論理デバイス..... 300
作成
　パリティグループの作成..... 293
システム日時の更新.....75
障害通知メールの内容.....426
証明書.....269
ストレージ管理者（参照）.....34
ストレージ管理者（システムリソース管理）34
ストレージ管理者（初期設定）.....34
ストレージ管理者（パフォーマンス管理）....35
ストレージ管理者（プロビジョニング）.....35
ストレージ管理者(リモートバックアップ管理) 35
ストレージ管理者(ローカルバックアップ管理) 35
ストレージシステムの情報編集.....218
スペアドライブ
　割り当て..... 292
セキュリティ管理者（参照・編集）.....35
セキュリティ管理者（参照）.....35

た

単方向
　構築..... 309
　削除..... 311
　変更..... 312
テスト SNMP トラップの送信.....66
テストメールの送信.....61
トラブルシューティング
　iSCSI.....403
　Storage Navigator..... 101

な

日時設定の変更.....73

ネットワーク拒否設定の変更.....73
ネットワーク設定の変更.....71

は

パリティグループ
　削除..... 294
パリティグループの削除.....294
パリティグループの作成.....293
ファイアウォール.....406
保守（ベンダ専用）.....36
保守（ユーザ）.....36
ホストモード一覧.....237
ホストモードオプション一覧.....239

ま

マッピングポート
　Fibre Channel.....297
メール通知の設定.....61

や

容量
　論理デバイス..... 295

ら

ログイン
　Storage Navigator..... 208
論理デバイス
　削除..... 300

わ

割り当て
　スペアドライブ..... 292

iStorage V10e/V100/V300
システム管理者ガイド

IV-UG-002-003-12

2025 年 10 月 第 12 版 発行

日本電気株式会社

© NEC Corporation 2021-2025