

システム管理者ガイド

Hitachi Virtual Storage Platform One Block 85

4051-1J-U50-00

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

著作権

All Rights Reserved, Copyright (C) 2026, Hitachi, Ltd.

免責事項

このマニュアルの内容の一部または全部を無断で複製することはできません。

このマニュアルの内容については、将来予告なしに変更することがあります。

このマニュアルに基づいてソフトウェアを操作した結果、たとえ当該ソフトウェアがインストールされているお客様所有のコンピュータに何らかの障害が発生しても、当社は一切責任を負いかねますので、あらかじめご了承ください。このマニュアルの当該ソフトウェアご購入後のサポートサービスに関する詳細は、弊社営業担当にお問い合わせください。

商標類

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

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

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。

IBM, HACMP 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。

Microsoft は、マイクロソフト 企業グループの商標です。

Oracle®, Java 及び MySQL は、Oracle, その子会社及び関連会社の米国およびその他の国における登録商標です。

UNIX は、The Open Group の米国ならびに他の国における登録商標です。

Veritas および Veritas ロゴは、米国およびその他の国における Veritas Technologies LLC またはその関連会社の登録商標です。

その他記載の会社名、製品名などは、それぞれの会社の商標もしくは登録商標です。

輸出時の注意

本製品を輸出される場合には、外国為替及び外国貿易法の規制並びに米国輸出管理規則など外国の輸出関連法規をご確認の上、必要な手続きをお取りください。

なお、不明な場合は、弊社担当営業にお問い合わせください。

発行

2026 年 1 月 (4051-1J-U50-00)

目次

はじめに.....	11
マニュアルの概要.....	12
マニュアルの目的.....	12
対象読者.....	12
マニュアルの位置づけ.....	12
マニュアルの読み方.....	12
マニュアルの構成.....	12
マニュアルの参照と適合プログラムバージョン.....	13
マニュアルで用いる表記.....	13
マニュアルに掲載している画面図.....	14
操作方法.....	14
サポート.....	14
プログラムプロダクト TrueCopy について.....	14
REST API の管理ツールについて.....	14
発行履歴.....	15
 1.概要.....	17
1.1 システム構成.....	18
1.2 ストレージシステムの機能と管理ツール.....	19
1.3 マニュアル体系.....	22
1.4 VSP One Block Administrator を利用して管理する構成.....	23
1.4.1 構成概要.....	24
1.4.2 管理ツールの操作端末の要件.....	25
1.4.3 利用例.....	27
1.4.4 ストレージシステムへアクセスするための IP アドレス.....	27
1.4.5 各ツールのログイン方法.....	28
1.4.6 VSP One Block Administrator 利用の構成の注意事項.....	29
1.4.7 VSP One Block Administrator でソフトウェアを利用する場合の注意事項.....	30
1.4.8 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.....	31
(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.....	31
(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.....	32
 2.初期設定作業を実施するための前提条件.....	35
2.1 初期設定作業を実施するための前提条件.....	36

3.ユーザネットワーク接続と日時設定.....	37
3.1 ユーザネットワーク接続と日時設定の流れ.....	38
3.2 ユーザネットワーク（管理 LAN）に接続するための前作業.....	38
3.2.1 管理ツールの操作端末をストレージシステムに一時的に接続する.....	38
3.2.2 maintenance utility に保守用アカウントでログインする.....	39
3.2.3 保守用アカウントのパスワードを変更する.....	40
3.2.4 ストレージシステムの管理ポートのネットワーク情報を設定する.....	40
3.3 ユーザネットワーク（管理 LAN）への接続.....	41
3.3.1 管理ツールの操作端末とストレージシステムを管理 LAN に接続する.....	41
3.3.2 管理 LAN から VSP One Block Administrator にログインする.....	42
3.3.3 管理 LAN の暗号化通信を設定する.....	42
3.4 ストレージシステムの日時を設定する.....	43
3.4.1 ストレージシステムの日時を設定する（NTP サーバを使用する場合）.....	43
3.4.2 ストレージシステムの日時を設定する（NTP サーバを使用しない場合）.....	44
4.ユーザアカウント作成.....	45
4.1 ユーザアカウント作成の流れ.....	46
4.2 ユーザアカウントを作成する.....	47
4.3 LDAP サーバを使用した外部認証および認可を設定する.....	48
5.ストレージシステムで使用する機能設定.....	51
5.1 ストレージシステムで使用する機能設定の流れ.....	52
5.2 プログラムプロダクトのライセンスを登録する.....	53
5.3 ストレージシステム情報を編集する.....	53
5.4 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する.....	54
5.5 アラート通知手段を設定する.....	55
5.5.1 アラートがメールで通知されるようにする.....	57
5.5.2 アラート通知メールをテスト送信する.....	57
5.5.3 アラートが Syslog サーバに転送されるようにする.....	58
5.5.4 Syslog サーバにテストメッセージを送信する.....	59
5.5.5 アラートが SNMP トラップ送信されるようにする（SNMP v1、または v2c の場合）.....	60
5.5.6 アラートが SNMP トラップ送信されるようにする（SNMP v3 の場合）.....	61
5.5.7 SNMP エンジン ID を SNMP マネージャに登録する（SNMP v3 の場合）.....	62
5.5.8 SNMP マネージャへトラップをテスト送信する.....	63
5.6 監査ログが Syslog サーバに転送されるようにする.....	63
5.6.1 監査ログの Syslog サーバへの転送を設定する.....	64
5.6.2 Syslog サーバに監査ログのテストメッセージを送信する.....	65
5.7 データ暗号化の環境を構築する.....	66
5.7.1 暗号化環境を有効化する.....	67
(1) VSP One Block Administrator での操作手順（暗号化環境を有効化する）.....	67
(2) 詳細 API での操作手順（暗号化環境を有効化する）.....	67
5.7.2 暗号化鍵をバックアップする.....	68
(1) VSP One Block Administrator での操作手順（暗号化鍵をバックアップする）.....	68
(2) 詳細 API での操作手順（暗号化鍵をバックアップする）.....	69
5.8 コモンクライテリア認証に準拠する設定を実施する.....	70

6.トラブルシューティング.....	73
6.1 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.....	74
6.2 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.....	74
6.3 トラブルシューティング作業前の確認.....	76
6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法	77
6.5 maintenance utility の内部アラート詳細の確認手順.....	82
6.6 maintenance utility の FRU (Field Replacement Unit) に関するアラートの確認手順.....	82
6.7 管理 GUI を起動する際にトラブルが発生した場合の対処方法	85
6.8 障害通知を受け取った場合の対処方法.....	86
6.9 ホスト (サーバ) がストレージシステムを認識できない場合の対処方法.....	86
6.10 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.....	89
付録 A ポート情報.....	91
A.1 各管理ツールが利用するポート情報.....	92
付録 B 管理ツールの起動および終了.....	93
B.1 管理ツールの起動方法.....	94
B.1.1 VSP One Block Administrator の起動.....	94
B.1.2 VSP One Block Administrator 経由での maintenance utility の起動.....	95
B.1.3 AMC の IP アドレス指定による maintenance utility の起動.....	95
B.1.4 VSP One Block Administrator 経由での内蔵 CLI の起動.....	96
B.1.5 SSH 接続による内蔵 CLI の起動.....	96
B.2 管理ツールの終了方法.....	97
B.2.1 VSP One Block Administrator の終了.....	97
B.2.2 VSP One Block Administrator 経由で起動した maintenance utility の終了.....	97
B.2.3 AMC の IP アドレス指定で起動した maintenance utility の終了.....	98
B.2.4 VSP One Block Administrator 経由で起動した内蔵 CLI の終了.....	98
B.2.5 内蔵 CLI の終了.....	99
付録 C maintenance utility の画面説明.....	101
C.1 基本フレームワーク	102
C.2 ヘッダエリア.....	102
C.3 ナビゲーションエリア.....	104
C.4 アプリケーションエリア	105
付録 D maintenance utility の機能.....	107
D.1 ファームウェア	108
D.1.1 ファームウェアバージョンの確認.....	108
D.1.2 ファームウェアの更新.....	108
D.2 ユーザ管理.....	108
D.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.....	108
D.2.2 ロール.....	108
D.2.3 リソースグループ	110
D.2.4 ユーザグループ.....	110
D.2.5 管理ツールとビルトイングループ.....	111
D.2.6 ユーザグループを作成する場合の参考情報.....	112

(1) maintenance utility の操作に必要なロール	112
(2) VSP One Block Administrator の操作に必要なロール	113
(3) 内蔵 CLI の操作に必要なロール	113
(4) RAID Manager の操作に必要なロール	113
(5) エクスポートツール 2 の操作に必要なロール	113
D.2.7 ユーザ名とパスワードの文字数と使用可能文字	114
D.2.8 ユーザアカウントポリシーの設定	115
(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	116
(2) ユーザアカウントのパスワードポリシー設定	117
(3) メールサーバの設定	119
(4) テストメールの送信	120
(5) ユーザ個別のパスワードポリシーの適用	121
(6) ユーザ個別のメールアドレスの設定	122
(7) ユーザアカウント状態の確認	123
(8) アカウントロックの解除	123
(9) アカウントの有効化	124
D.2.9 ユーザアカウントの作成	124
D.2.10 パスワードの変更	126
D.2.11 ユーザアカウントの無効化	127
D.2.12 ユーザアカウントの削除	127
D.2.13 ユーザアカウントのバックアップ	128
D.2.14 ユーザアカウントのリストア	128
D.3 アラート通知	128
D.3.1 メール通知の設定	129
D.3.2 テストメールの送信	130
D.3.3 アラート通知を蓄積するための Syslog の設定	132
D.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	134
D.3.5 SNMP エージェントの設定	135
D.3.6 テスト SNMP トラップの送信	135
D.3.7 SNMP エンジン ID を確認する	136
D.4 ライセンス	136
D.4.1 ライセンスキーの参照	137
D.4.2 ライセンスキーの追加	138
D.4.3 ライセンスキーの有効化	138
D.4.4 ライセンスキーの無効化	139
D.4.5 ライセンスキーのアンインストール	139
D.4.6 ライセンスの状態を更新	140
D.5 ネットワーク設定	140
D.5.1 ネットワーク設定の変更	140
D.5.2 ネットワーク拒否設定の変更	142
D.6 日時設定	142
D.6.1 日時設定の変更	142
D.6.2 システム日時の更新	144
D.7 監査ログ	144
D.7.1 監査ログを蓄積するための Syslog の設定	144
D.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	147
D.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	147
D.8 外部認証	149
D.8.1 LDAP ディレクトリサーバの要件	150
D.8.2 LDAP の設定	150
D.8.3 無効化	153

D.9 初期設定.....	153
D.9.1 初期設定ウィザードによる設定変更.....	153
D.10 電源管理.....	154
D.10.1 ストレージシステムの電源 ON.....	154
D.10.2 ストレージシステムの電源 OFF.....	155
D.10.3 UPS のモード編集.....	155
D.11 システム管理.....	155
D.11.1 パスワードの変更.....	155
D.11.2 ログインメッセージの編集.....	156
D.11.3 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.....	156
D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する.....	157
D.11.5 システムロックの強制解除.....	160
D.11.6 ESM の状態確認.....	161
D.11.7 ESM のリブート.....	161
D.11.8 ESM の手動フェールオーバー.....	162
D.11.9 システムダンプのダウンロード.....	162
D.11.10 スモールシステムダンプのダウンロード.....	164
D.11.11 構成情報バックアップのダウンロード.....	164
D.11.12 ボリューム状態の参照.....	164
D.11.13 セッションタイムアウト時間の編集.....	164
D.11.14 コモンクライテリア認証に準拠する設定を実施する.....	165
D.11.15 TLS セキュリティ設定を管理する.....	166
D.12 アラートの表示.....	167
D.12.1 アラート表示.....	167
D.12.2 FRU に関するアラート表示.....	168
D.13 SIM のコンプリート.....	168
付録 E ストレージシステムの障害情報の通知手段.....	169
E.1 ストレージシステムの障害情報の通知手段.....	170
E.1.1 Syslog の転送プロトコル (TLS/RFC5424) の要件.....	170
E.1.2 クライアント証明書の取得 (Syslog プロトコルを使用する場合)	171
E.1.3 テストメールの例.....	171
付録 F ストレージシステム運用上の注意.....	173
F.1 ストレージシステムに対してネットワーク監視 (Ping 応答またはリンクアップ/リンクダウンによる監視) をする場合.....	174
F.2 SSD 電源オフ時間の注意.....	174
付録 G SSL/TLS 通信の設定.....	175
G.1 SSL/TLS とは.....	176
G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信.....	176
G.2.1 証明書のアップロード時に実施する証明書検証項目.....	179
G.2.2 外部サーバとの通信時に実施する証明書検証項目.....	180
G.3 ストレージシステムと管理ツールの操作端末間の SSL/TLS 通信.....	180
G.4 SSL/TLS 通信の設定の流れ.....	183
G.5 秘密鍵を作成.....	184
G.6 公開鍵を作成.....	184
G.7 署名付き証明書を取得.....	185

G.8 署名付きの信頼できる証明書を取得.....	186
G.9 CSR 作成および自己署名証明書作成.....	186
G.10 SSL/TLS 証明書を PKCS#12 形式に変換.....	186
G.11 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.....	187
G.12 詳細 API サーバ間の SSL 通信用の証明書を詳細 API サーバへアップロード.....	187
G.12.1 詳細 API での操作手順.....	187
G.13 TLS セキュリティ設定を管理する.....	188
G.13.1 SSL/TLS 通信のセキュリティ設定項目.....	188
G.13.2 SSL/TLS 通信のセキュリティ設定を変更する.....	189
G.13.3 SSL/TLS 通信のセキュリティ設定を初期化する.....	189
G.14 セキュリティ警告が表示されたときの対処方法.....	190
付録 H ホスト接続の参考情報.....	193
H.1 Fibre Channel ホスト.....	194
H.1.1 複数ホストでの構築.....	194
H.1.2 ゾーニング.....	195
H.1.3 ホスト側に設定するコマンド多重数.....	195
H.1.4 デバイスタイムアウト値の推奨値.....	196
H.2 iSCSI、NVMe/TCP ホスト.....	196
H.2.1 iSCSI、NVMe/TCP の概要.....	196
H.2.2 iSCSI、NVMe/TCP I/F の仕様.....	196
H.2.3 Ethernet (iSCSI、NVMe/TCP) 規格.....	199
H.2.4 注意事項.....	200
H.2.5 OS に依存する注意事項.....	202
H.2.6 Ethernet に関するトラブルシューティング.....	202
H.2.7 Ethernet 25Gbps チャンネルボード使用時の注意事項.....	205
(1) ホストとストレージシステムの接続構成に関する注意事項.....	205
(2) ホスト OS とマルチパスソフトウェアに関する注意事項.....	206
(3) Windows Server 2019/2022 (Microsoft DSM/MPIO または Hitachi Dynamic Link Manager) のパラメータ設定の例.....	206
(4) Red Hat Enterprise Linux (Device Mapper Multipath) のパラメータ設定の例.....	207
(5) Red Hat Enterprise Linux (Hitachi Dynamic Link Manager) のパラメータ設定の例.....	208
(6) SUSE Linux (Device Mapper Multipath または Hitachi Dynamic Link Manager) のパラメータ設定の例.....	208
(7) Ethernet 25Gbps チャンネルボードのポートに関する注意事項.....	208
H.2.8 Ethernet 100Gbps チャンネルボードを使用する場合の注意事項.....	209
(1) 接続可能なホスト.....	209
(2) ホストとストレージシステムの接続構成に関する注意事項.....	209
H.2.9 デバイスタイムアウト値の推奨値.....	210
付録 I ASSIST の構成.....	211
I.1 ASSIST の構成.....	212
付録 J 障害通知メール、Syslog メッセージ、SNMP メッセージの内容.....	213
J.1 障害通知メールの内容.....	214
J.2 Syslog メッセージの内容.....	214
J.3 SNMP メッセージの内容.....	217

付録 K ロケーションの対応表.....	219
K.1 MP#とロケーションの対応.....	220
用語解説.....	225



はじめに

このマニュアルは Hitachi Virtual Storage Platform One Block 85（以下、B85 と略します）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。

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
- マニュアルの読み方
- サポート
- プログラムプロダクト TrueCopy について
- REST API の管理ツールについて
- 発行履歴

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

このマニュアルの目的について説明します。

- ・ ストレージシステムの導入作業として、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。
- ・ 初期構築作業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。
- ・ 初期構築したストレージシステムを運用、保守する際に必要な操作手順、機能を解説しているユーザガイドを示すことで、構築したいシステムの管理、設定をできるようにすること。

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最初に読んでいただくマニュアルです。

マニュアルに示す手順に従って、初期構築を完了させます。

初期構築後、運用・保守をするときに必要なユーザガイドをこのマニュアルで確認します。

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	記載している章と内容
1 概要	本ストレージシステムの管理手法と、必要な物品、注意事項を記載しています。
2 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構築における考慮事項と、作業の流れを記載しています。
3 ユーザネットワーク接続と日時設定	初期構築作業の手順を記載しています。
4 ユーザアカウント作成	初期構築作業の手順を記載しています。
5 ストレージシステムで使用する機能設定	初期構築作業の手順を記載しています。

章	記載している章と内容
6 トラブルシュート	初期構築作業で、管理 GUI（VSP One Block Administrator、maintenance utility）および内蔵 CLI の起動あるいは操作時にトラブルが発生した場合の対処について記載しています。
付録 A. ポート情報	各管理ツールの通信ポート番号を記載しています。
付録 B. 管理ツールの起動および終了	管理 GUI（VSP One Block Administrator、maintenance utility）および内蔵 CLI の起動起動および終了について記載しています。
付録 C. maintenance utility の画面説明	maintenance utility の画面構成について記載しています。
付録 D. maintenance utility の機能	maintenance utility のメニューについて記載しています。
付録 E. ストレージシステムの障害情報の通知手段	ストレージシステムの障害情報の通知設定について記載しています。
付録 F. 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記載しています。
付録 G. SSL/TLS 通信の設定	通信のセキュリティをより高めるための SSL/TLS 通信の設定について記載しています。
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の参考情報について記載しています。
付録 I. ASSIST の構成	ASSIST（遠隔保守支援システム）の構成について記載しています。
付録 J. 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記載しています。
付録 K. ロケーションの対応表	MP#および Port とロケーションの対応表を記載しています。
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。

マニュアルの参照と適合プログラムバージョン

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

- A0-05-21-XX

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。1Cyl（シリンダ）を KB に換算した値は、960KB 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。

シンボル	内容	説明
	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。

シンボル	内容	説明
	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。

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。

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

プログラムプロダクト TrueCopy について

DKCMAIN プログラムバージョン A0-05-21-XX/XX 以前では、TrueCopy は未サポートです。

REST API の管理ツールについて

Virtual Storage Platform One Block 80 が提供する REST API の管理ツールには、次の 2 種類があります。それぞれの特徴や使い分けなどの詳細は『VSP Block Storage REST API リファレンスガイド』を参照してください。

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

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

発行履歴

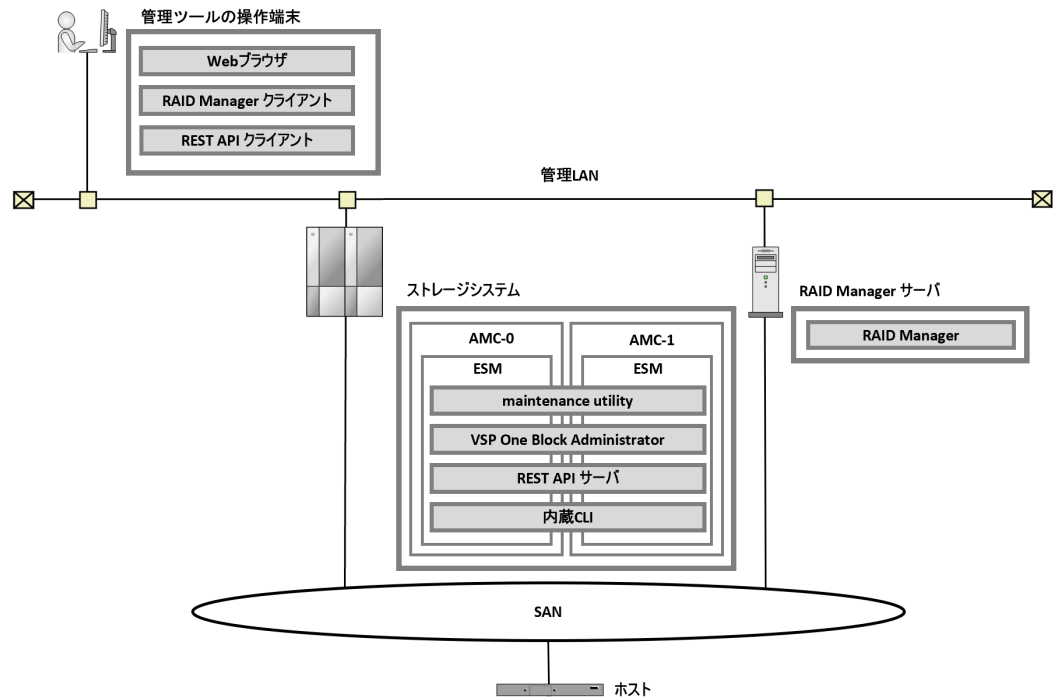
マニュアル資料番号	発行年月	変更内容
4051-1J-U50-00	2026 年 1 月	新規 適合 DKCMAIN プログラムバージョン : A0-05-21-XX

概要

- 1.1 システム構成
- 1.2 ストレージシステムの機能と管理ツール
- 1.3 マニュアル体系
- 1.4 VSP One Block Administrator を利用して管理する構成

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。



管理ツールの操作端末

各管理ツールにアクセスするための PC です。

- 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。

ストレージシステム

本ストレージシステムです。

- AMC-0、AMC-1
ストレージシステムと外部を接続するハードウェア（以下、AMC）です。
- ESM (Embedded Storage Manager)
ストレージシステムの基本的な管理機能を持つソフトウェアです。AMC-0 と AMC-1 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。VSP One Block Administrator から画面を開けます。
- VSP One Block Administrator
ストレージシステムの構成やリソースを操作するシンプルな GUI の管理ツールです。

- 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管理ツール

ストレージシステムの主な機能と管理ツール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	管理ツール			
		G U I	A P I	内 蔵 C L I	R M
Dynamic Provisioning	ボリューム容量の仮想化	○	○	○	○
Adaptive Data Reduction	格納データの圧縮と重複データ排除による容量削減	○	○	○	○
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	—	—	—	○
Quality of Service (QoS)	ボリューム単位、または QoS グループ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	△※1	△※2	○	○
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	—	○※8	○	○※8
SNMP Agent, SNMP Manager	SNMP によるストレージ監視	○	○	—	—

ストレージシステムの 機能	機能の概要	管理ツール			
		G U I	A P I	内 蔵 C L I	R M
Audit Log	監査ログの設定	○	○	—	—
Encryption License Key	ドライブ内データの暗号化	△※4	○	△※5	△※5
Universal Volume Manager	他のストレージ内ボリュームの利用	△※6、※8	○※8	○※8	○※8
ShadowImage ShadowImage for Mainframe※12	同一ストレージ内でのボリュームコピー	△※9、※10、※11	△※8	○	○※8
Thin Image Advanced	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	○	○	○	○
TrueCopy for Mainframe※12	遠隔拠点間のボリュームコピー（短距離での同期コピー）	—	—	○※8	○※8
Universal Replicator Universal Replicator for Mainframe※12	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）	—	△※8	○※8	○※8
global-active device	ボリュームミラーリングによるデータ二重化	—	○※8	○※8	○※8
Dynamic Carbon Reduction	消費電力を抑え CO ₂ 削減に寄与する環境配慮機能	—	—	○	○

凡例

- GUI : VSP One Block Administrator
- API : REST API
- RM : RAID Manager
- ○ : 対応、△ : 一部対応、— : 非対応

注※1

ボリューム単位 of QoS のみサポート

注※2

ボリューム単位 of QoS をサポート、QoS グループは上限値のみサポート

注※3

外部ボリュームの移動のみサポート

注※4

GUI で実行可能な暗号化操作については、『VSP One Block Administrator ユーザガイド』を参照

注※5

暗号有効のパリティグループ作成のみサポート

注※6

外部ストレージシステムのボリュームのマッピングのみサポート

注※7

global-active device を利用するための環境構築のみサポート

注※8

データ移行時に使用できる管理ツールは、次の表のように要件によって異なります。
また、次の使用を検討している場合は、「[サポート](#)」のお問い合わせ先に連絡ください。

- ・ #5～#12 の要件、#15～#16 の要件のどれかで、RAID Manager を使用してデータ移行を実施する場合。
- ・ #6、#8、#10、#12、#15、または#16 の要件で、詳細 API を使用してデータ移行を実施する場合。

#6、または#8 の要件で、VSP One Block Administrator を使用してデータ移行を実施する場合、Universal Volume Manager で移行先ストレージにボリュームをマッピングしてから、Volume Migration によるデータコピーが完了するまで、データ移行先のボリュームに対してサーバから I/O 発行ができません。この期間はサーバの業務停止が必要です。サーバから I/O 発行ができない期間の詳細については、『VSP One Block Administrator ユーザガイド』を参照してください。

サーバの業務停止時間を最小化したい場合は、RAID Manager を使用したデータ移行をご検討ください。RAID Manager を使用した場合は、Universal Volume Manager によるボリュームのマッピング後、Volume Migration によるデータ移行中でもデータ移行先のボリュームに対してサーバから I/O 発行ができます。

No	要件			サポート状況	利用するプログラム プロダクト	VSP One Block Administ rator	シンプル API	詳細 API	RAID Manager
	データ移行時の状態	移行元ストレージ	移行元ボリュームの容量						
1	無停止（オンライン）	日立	4TB 超	サポート	global-active device	×	×	○	○
2	無停止（オンライン）	日立	4TB 以下	サポート	global-active device	×	×	○	○
3	無停止（オンライン）	日立以外	4TB 超	未サポート	—	×	×	×	×
4	無停止（オンライン）	日立以外	4TB 以下	未サポート	—	×	×	×	×
5	停止（オフライン）	日立	4TB 超	サポート	Volume Migration、 Universal Volume Manager	×	×	×	○
6	停止（オフライン）	日立	4TB 以下	サポート	Volume Migration、 Universal Volume Manager	—	×	○	○
7	停止（オフライン）	日立以外	4TB 超	サポート	Volume Migration、 Universal Volume Manager	×	×	×	○
8	停止（オフライン）	日立以外	4TB 以下	サポート	Volume Migration、 Universal Volume Manager	—	×	○	○

No	要件			サポート 状況	利用するプログラ ムプロダクト	VSP One Block Administ rator	シンプル API	詳細 API	RAID Manager
	データ移 行時の状 態	移行元ス トレージ	移行元ボ リューム の容量						
9	停止（オフ ライン）	日立	4TB 超	サポー ト	ShadowImage、 Universal Volume Manager	×	×	×	○
10	停止（オフ ライン）	日立	4TB 以下	サポー ト	ShadowImage、 Universal Volume Manager	×	×	○	○
11	停止（オフ ライン）	日立以外	4TB 超	サポー ト	ShadowImage、 Universal Volume Manager	×	×	×	○
12	停止（オフ ライン）	日立以外	4TB 以下	サポー ト	ShadowImage、 Universal Volume Manager	×	×	○	○
15	停止（オフ ライン）	日立	4TB 超	サポー ト	Universal Replicator	×	×	○	○
16	停止（オフ ライン）	日立	4TB 以下	サポー ト	Universal Replicator	×	×	○	○

注※9

ShadowImage for Mainframe では使用できません。

注※10

GUI で実行可能な ShadowImage 操作については、『VSP One Block Administrator ユーザガイド』を参照

注※11

内部ボリュームのみサポート

注※12

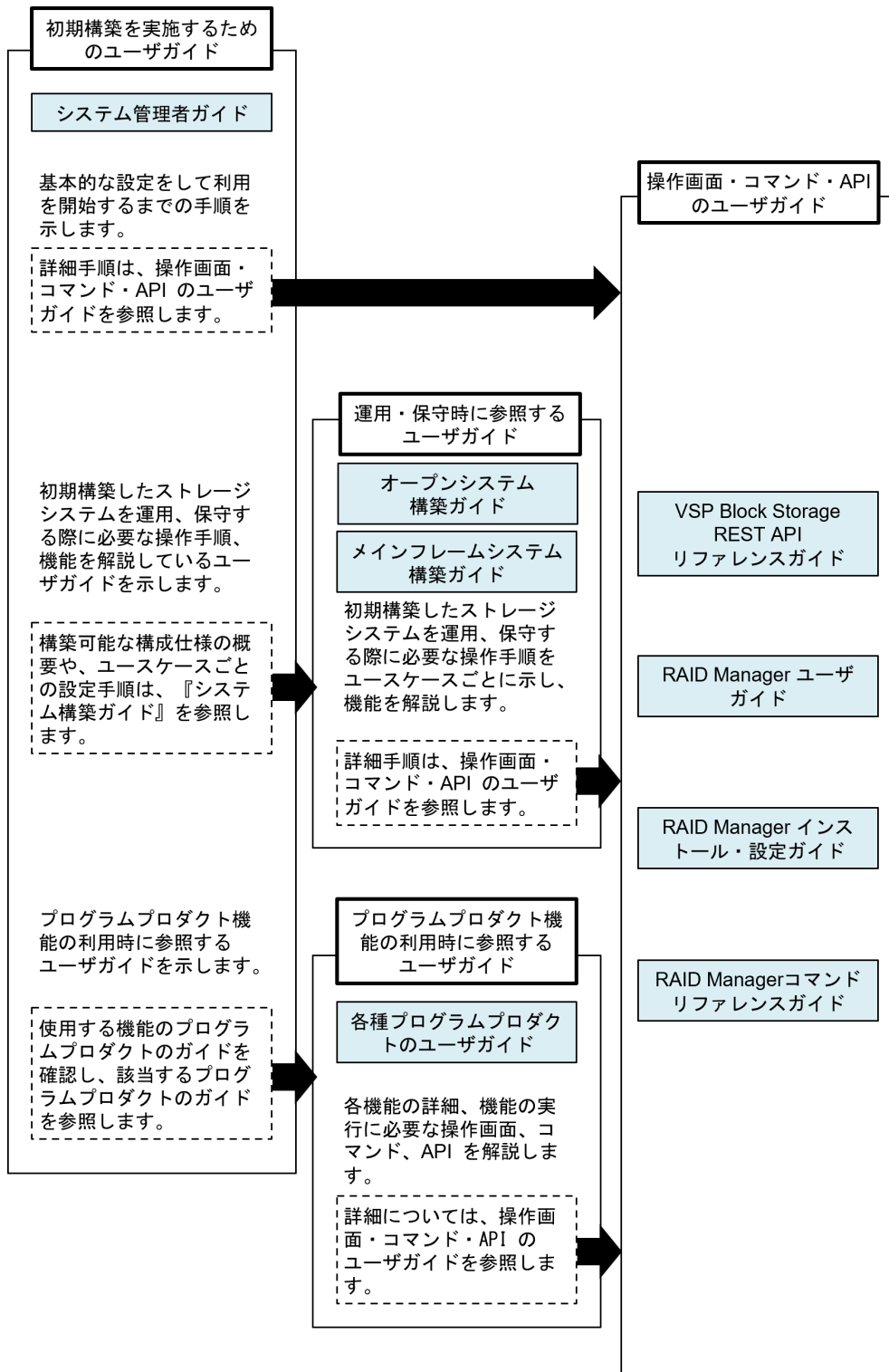
「for Mainframe」は、IBM 社のメインフレームコンピュータから、本ストレージシステムを操作する際に必要となる、ストレージシステム側の機能を示しています。IBM 社のメインフレームコンピュータに関する機能の詳細は、IBM 社の出版物を参照してください。ストレージシステム側の機能の詳細は、次に示すマニュアルを参照してください。

- ・ メインフレームシステム構築ガイド
- ・ ShadowImage for Mainframe ユーザガイド
- ・ TrueCopy for Mainframe ユーザガイド
- ・ Universal Replicator for Mainframe ユーザガイド

1.3 マニュアル体系

システム管理者ガイドは、ストレージシステムの導入時に最初に読んでいただくマニュアルです。マニュアルに示す手順に従って初期構築を完了させます。

ストレージシステムの初期構築、運用、保守にあたっては、あわせて以下のマニュアルを参照してください。



1.4 VSP One Block Administrator を利用して管理する構成

1.4.1 構成概要

ストレージシステムの管理ポート 2 ポートを LAN に接続して利用します。管理ツールの操作端末をその LAN に接続してください。

図 1 VSP One Block Administrator 利用の構成

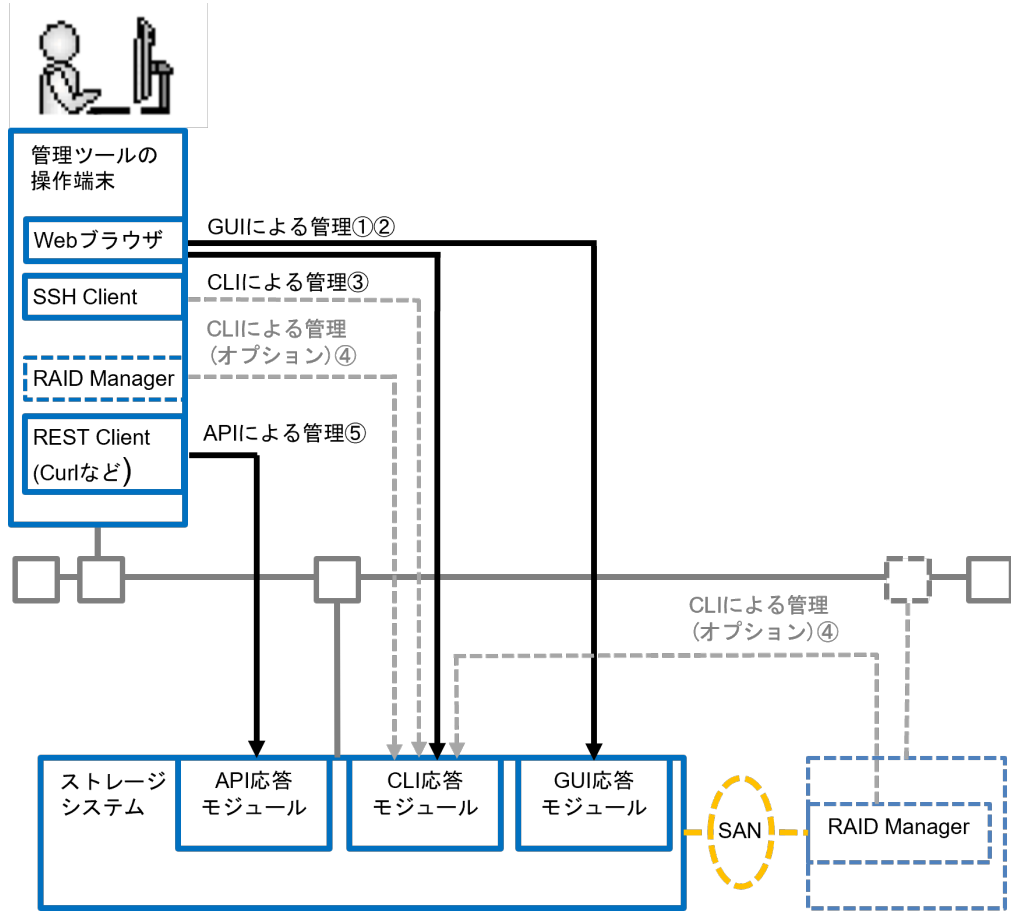


表 1 VSP One Block Administrator 利用の場合の管理インターフェース

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			VSP One Block Administrator	構成設定操作
3			内蔵 CLI ^{※1}	構成設定操作
4	CLI	外部サーバ ^{※2}	RAID Manager ^{※3}	- 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	詳細 API	- 構成設定操作 - レプリケーション操作^{※4}

注※1

内蔵 CLI は、2 種類の起動方法があります。

- VSP One Block Administrator のコマンドコンソールから起動する
- SSH ターミナルソフトウェアから起動する

内蔵 CLI では、RAID Manager の raidcom で始まるコマンドが使用できます。

すべての機能を使用したい場合は、RAID Manager を外部サーバにインストールして使用する必要があります。

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

RAID Manager コマンドを実行する方式には、In-Band 方式と Out-of-Band 方式があります。詳細は『RAID Manager ユーザガイド』を参照してください。

注※4

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

1.4.2 管理ツールの操作端末の要件

1 台の PC で VSP One Block Administrator、maintenance utility、内蔵 CLI を利用する場合、下記が条件となります。

管理ツールの操作端末のハードウェア条件

項目	仕様
プロセッサ (CPU)	• Windows 11、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 2025 以外 Intel Core i3 1.5GHz (2core) 相当以上※ 推奨: Intel Core i3 1.5GHz (4core) 相当以上 その他の仕様については、各 OS の仕様に従います。
メモリ (RAM)	• Windows 11 8GB 以上 推奨: 16GB 以上 • Windows 11 以外 4GB 以上 推奨: 8GB 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

項目	仕様
ネットワークアダプタ	1Gbps イーサネット

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。

管理ツールの操作端末のソフトウェア条件を示します。

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。

管理ツールの操作端末のソフトウェア条件

OS	アーキテクチャ	ブラウザ
Windows Server 2025	64	Microsoft Edge ^{※1} 、/Google Chrome ^{※2}
Windows Server 2022	64	Microsoft Edge ^{※1} 、/Google Chrome ^{※2}
Windows Server 2019	64	Microsoft Edge ^{※1} 、
Windows Server 2016	64	Microsoft Edge ^{※1} 、/Google Chrome ^{※2}
Windows 11	64	Microsoft Edge ^{※1} 、/Google Chrome ^{※2}
RHEL 7.4	64	Mozilla Firefox ^{※3}
RHEL 7.5	64	Mozilla Firefox ^{※3}

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。

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

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※3

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。



メモ

- 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。

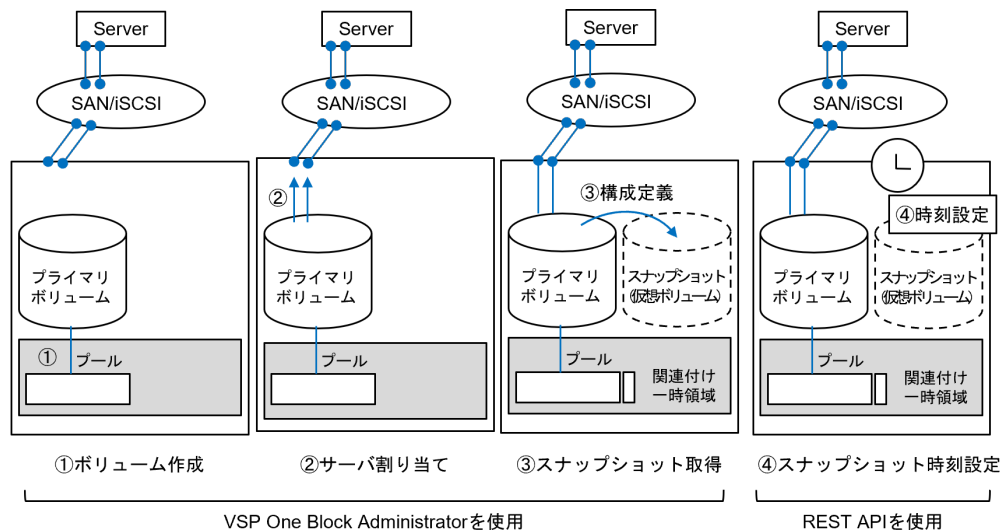
- Google Chrome は、RHEL 7.4 および RHEL 7.5 をサポートしていません。RHEL 7.4 および RHEL 7.5 では、Mozilla Firefox を使用してください。

1.4.3 利用例

VSP One Block Administrator 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

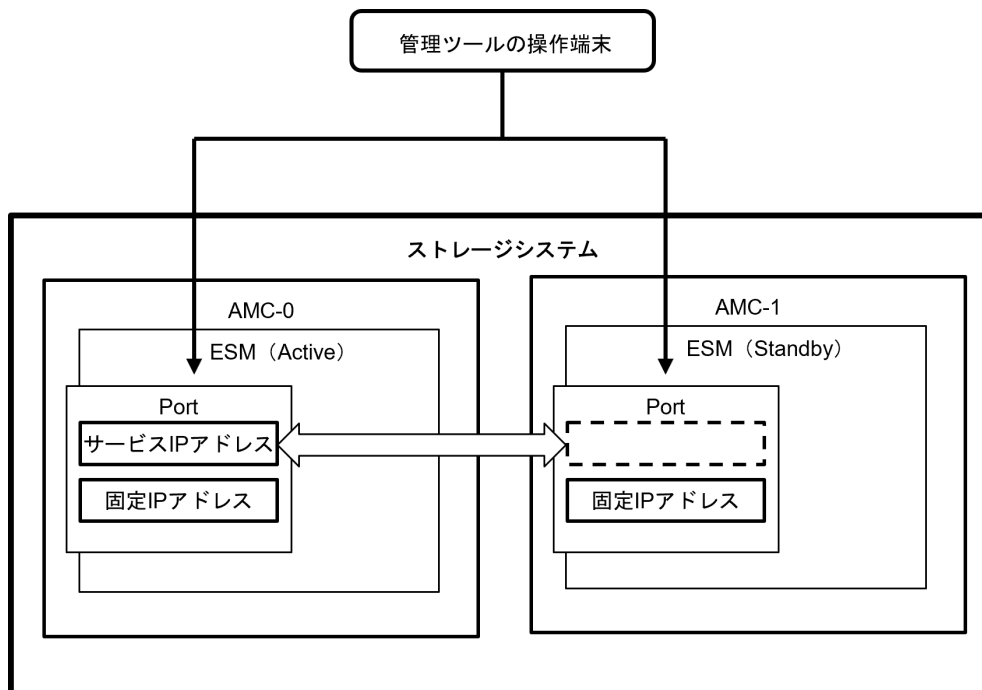
各管理ツールを下記のステップで利用することにより、上記ストレージ要件の構成を適切に設定できます。

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、『VSP One Block Administrator ユーザガイド』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。

- 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
- プライマリボリュームをサーバに割り当て
- スナップショットの取得
- 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

1.4.4 ストレージシステムへアクセスするための IP アドレス

AMC-0 と AMC-1 の ESM は Active-Standby 構成でクラスタ定義されています。ストレージシステムでは以下の 2 種類の IP アドレスを提供します。



- 固定 IP アドレス
AMC-0 と AMC-1 のそれぞれの ESM に割り当てられている IP アドレスです。AMC を指定してストレージシステムに接続する場合、固定 IP アドレスを使用します。
- サービス IP アドレス
クラスタに割り当てられている IP アドレスです。Active-Standby 構成のクラスタ内で Active となっている AMC に割り当てられます。Active AMC に障害が発生した場合、サービス IP アドレスは Standby AMC に引き継がれます。AMC の状態を意識せずにストレージシステムに接続する場合、サービス IP アドレスを使用します。

ストレージシステムおよび各種外部サーバ間のファイアウォールに設定する IP アドレスは、固定 IP アドレスとサービス IP アドレスを指定してください。

以降で「ESM の IP アドレス」または「AMC の IP アドレス」と記載されている場合は、固定 IP アドレスのことを指します。

1.4.5 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、VSP One Block Administrator、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、「[D.2 ユーザ管理](#)」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、サービス IP アドレスを使用して下記のように入力してください。または、AMC-0 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。AMC-0 に障害が発生してエラーとなる場合は、AMC-1 管理ポートの IP アドレスを使用してください。 https://(IP アドレス)/MaintenanceUtility/ または http://(IP アドレス)/MaintenanceUtility/ ただし、TCP ポート (HTTP) (TCP:80) を有効にするためには、「3.3.3 管理 LAN の暗号化通信を設定する」を参照してください。
VSP One Block Administrator	ブラウザのウィンドウに、サービス IP アドレスを使用して下記のように入力してください。または、ESM クラスタロールが Active 状態である AMC 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。 https://(IP アドレス)/ または http://(IP アドレス)/ ただし、TCP ポート (HTTP) (TCP:80) を有効にするためには、「3.3.3 管理 LAN の暗号化通信を設定する」を参照してください。
内蔵 CLI	内蔵 CLI にログインするには次の方法があります。 • VSP One Block Administrator にログインして、コマンドコンソールを起動して内蔵 CLI にログインしてください。 詳細は、「B.1.4 VSP One Block Administrator 経由での内蔵 CLI の起動」を参照してください。 内蔵 CLI へのログインはこちらの手順を推奨します。 • SSH ターミナルソフトウェアから、サービス IP アドレスを使用してログインしてください。または、AMC-0 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。AMC-0 に障害が発生してエラーとなる場合は、AMC-1 管理ポートの IP アドレスを使用してください。 詳細は、「B.1.5 SSH 接続による内蔵 CLI の起動」を参照してください。 なお、TCP ポート番号は 20522 を指定してください。 TCP ポート (SSH) (TCP:20522) を有効にするためには、「3.3.3 管理 LAN の暗号化通信を設定する」を参照してください。
RAID Manager	アプリケーションを起動する際にストレージシステム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。

1.4.6 VSP One Block Administrator 利用の構成の注意事項

NVMe/TCP を使用しない構成で利用してください

NVMe/TCP に関するプロビジョニング操作は、VSP One Block Administrator から実施できません。RAID Manager を使用してください。RAID Manager によるプロビジョニング操作についての詳細は、『RAID Manager コマンドリファレンス』を参照してください。

コピー系の機能の操作とトラブルシューティング

Thin Image Advanced と ShadowImage は、VSP One Block Administrator 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、VSP One Block Administrator 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 を利用してください。

- TrueCopy
- Universal Replicator
- global-active device

1.4.7 VSP One Block Administrator でソフトウェアを利用する場合の注意事項

VSP One Block Administrator 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 VSP One Block Administrator で操作できない項目を利用したい場合は、RAID Manager または詳細 API で実施してください。

表 2 VSP One Block Administrator 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
Adaptive Data Reduction	VSP One Block Administrator で利用できます。詳細な管理は RAID Manager を利用してください。
Hitachi LUN Manager Software	VSP One Block Administrator ではサーバモデルを使用して利用できます。従来のストレージと同様な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 VSP One Block Administrator 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 を利用してください。
Hitachi Dynamic Provisioning Software	VSP One Block Administrator 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。
Thin Image Advanced	VSP One Block Administrator 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。VSP One Block Administrator で構成定義したオブジェクトも扱えます。
Hitachi SNMP Agent Software	maintenance utility を利用してください。VSP One Block Administrator 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。
Hitachi Data Retention Utility	RAID Manager を利用してください。VSP One Block Administrator で構成定義するオブジェクトも扱えます。
Hitachi ShadowImage Software	VSP One Block Administrator で利用できます。詳細な管理は RAID Manager を利用してください。
Hitachi TrueCopy Software	RAID Manager を利用してください。VSP One Block Administrator で構成定義したオブジェクトも扱えます。
Hitachi Universal Replicator Software	RAID Manager を利用してください。VSP One Block Administrator で構成定義したオブジェクトも扱えます。
Remote Replication Extended	RAID Manager を利用してください。VSP One Block Administrator で構成定義したオブジェクトも扱えます。
Hitachi Open Volume Management Software	VSP One Block Administrator で利用できます。詳細な管理は RAID Manager を利用してください。
Hitachi Universal Volume Manager Software	VSP One Block Administrator で、外部ストレージシステムのボリュームをローカルストレージシステムのボリュームとしてマッピングできます。4TB 以上のボリュームのマッピングや、その他の操作の場合は RAID Manager を利用してください。

プログラムプロダクト	サポート状況
Hitachi Resource Partition Manager Software※ ¹	VSP One Block Administrator 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 を利用してください。
global-active device	RAID Manager を利用してください。
Encryption License Key	VSP One Block Administrator で利用できます。暗号化鍵生成や、鍵管理サーバに接続した暗号化鍵のバックアップやリストアなどをする場合は、詳細 API を利用してください。パリティグループ作成時に暗号化を有効にする場合は、RAID Manager を利用してください。

注※1

仮想ストレージマシンを利用する場合は、RAID Manager で設定・管理を行ってください。
VSP One Block Administrator 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。

1.4.8 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

VSP One Block Administrator 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 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) 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

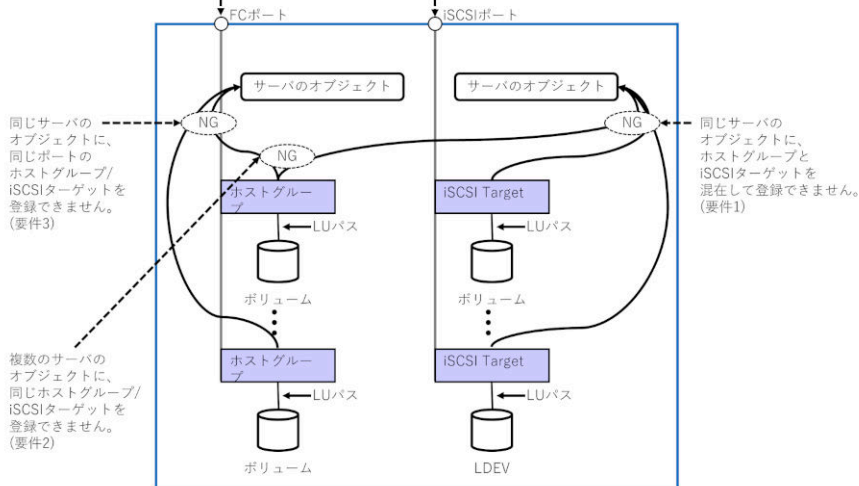
VSP One Block Administrator が管理しているサーバのオブジェクト（以下、サーバのオブジェクト）から、ホストグループ/iSCSI ターゲットを管理するためには、以下の要件を満たす必要があります。

表 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	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 4 を参照）
6	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。

No	要件
7	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。
8	動作モードが NVMe モードに設定されているポートのホストグループは、サーバのオブジェクトに登録できません。

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。
(要件4)



(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、そのホストモードおよ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。

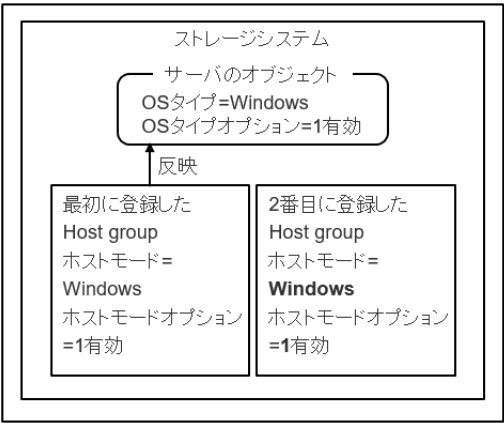
`raidcom add server` コマンドで作成したサーバのオブジェクトにホストグループ/iSCSI ターゲットを登録する場合、最初に登録したホストグループ/iSCSI ターゲットの、ホストモードおよびホストモードオプションが、サーバのオブジェクトの OS タイプおよび OS タイプオプションに反映されます。次に登録したホストグループ/iSCSI ターゲットの、ホストモードおよびホストモードオプションが、最初に登録したホストグループ/iSCSI ターゲットのホストモードおよびホストモードオプションと異なると、サーバのオブジェクトの OS タイプまたは、OS タイプオプションと、ホストグループ/iSCSI ターゲットのホストモードおよ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 タイプおよび 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およ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。

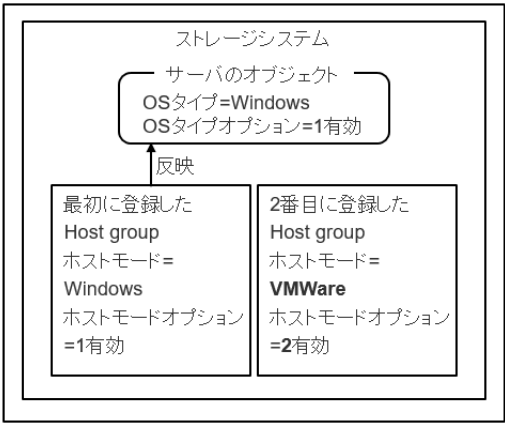
- VSP One Block Administrator で接続情報を追加すると、サーバのオブジェクトの OS タイプおよび OS タイプオプションと一致するホストグループおよびホストモードオプションが設定されたホストグループ/iSCSI ターゲットが、指定したポートに自動的に作成されます。
- VSP One Block Administrator で OS タイプまたは OS タイプオプションの設定を変更すると、サーバのオブジェクトに登録されたすべてのホストグループ/iSCSI ターゲットに変更内容

が反映されます。このためホストグループ/iSCSI ターゲットごとに異なるホストモードおよ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。

推奨構成



非推奨構成



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に必要な、前提条件を示します。

□ 2.1 初期設定作業を実施するための前提条件

2.1 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。
- 管理ツールの操作端末が要件を満たしていること。
管理ツールの操作端末の要件は、「[1.4.2 管理ツールの操作端末の要件](#)」を参照してください。
- 管理ツールの操作端末にロケールを設定していること。
管理ツールの操作端末のロケールも英語、または日本語のどちらかに設定してください。設定方法は使用している OS やブラウザのマニュアルを参照してください。
- 管理ツールの操作端末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を設定していること。
管理ツールの操作端末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、「[A.1 各管理ツールが利用するポート情報](#)」のポートを、管理ツールの操作端末とストレージシステムの間が存在するネットワーク環境に登録してください。
なお、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。
- 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。
- 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。

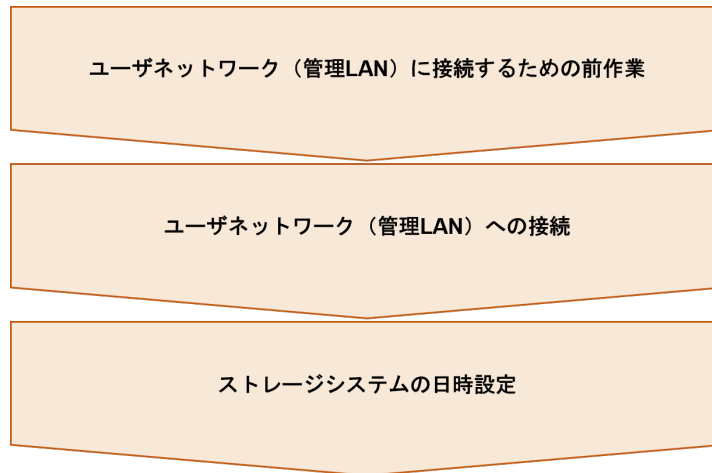
ユーザネットワーク接続と日時設定

ユーザネットワーク（管理 LAN）に接続できるようにするための設定手順、および、ストレージシステムの日時設定手順について説明します。

- 3.1 ユーザネットワーク接続と日時設定の流れ
- 3.2 ユーザネットワーク（管理 LAN）に接続するための前作業
- 3.3 ユーザネットワーク（管理 LAN）への接続
- 3.4 ストレージシステムの日時を設定する

3.1 ユーザネットワーク接続と日時設定の流れ

本章の設定作業の流れを以下のフローに示します。



これらの設定作業は、maintenance utility で実施します。maintenance utility の起動、終了については、「[B.1.2 VSP One Block Administrator 経由での maintenance utility の起動](#)」、「[B.1.3 AMC の IP アドレス指定による maintenance utility の起動](#)」、「[B.2.2 VSP One Block Administrator 経由で起動した maintenance utility の終了](#)」、「[B.2.3 AMC の IP アドレス指定で起動した maintenance utility の終了](#)」を参照してください。

maintenance utility の画面については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。ストレージシステムの日時設定は、REST API でも操作できます。REST API を使用する場合は、『VSP Block Storage REST API リファレンスガイド』を参照してください。

次の作業

[3.2.1 管理ツールの操作端末をストレージシステムに一時的に接続する](#)

3.2 ユーザネットワーク（管理 LAN）に接続するための前作業

3.2.1 管理ツールの操作端末をストレージシステムに一時的に接続する

ストレージシステムのネットワーク設定を実施するために、一時的に、管理ツールの操作端末をストレージシステムの管理ポートに LAN 接続します。接続後に、管理ツールの操作端末が管理ポートと通信できるように、管理ツールの操作端末に一時的な IP アドレスを設定します。

前提条件

- 要件を満たした管理ツールの操作端末を用意していること（管理ツールの操作端末については、「[1.4.2 管理ツールの操作端末の要件](#)」を参照してください）。
- LAN ケーブルを用意しておくこと。



メモ

- 管理ツールの操作端末と管理ポートの接続は、プロキシサーバを経由させないでください。

- 管理ツールの操作端末の arp テーブルに、管理ポートと同じ IP アドレスの別装置が記憶されている場合、該当する arp テーブルの IP アドレスを削除してください。
arp テーブルは、コマンドプロンプトで、arp -a を実行すると表示されます。コマンド arp -d を実行して削除対象の IP アドレスを削除してください。

操作手順

- 管理ツールの操作端末の電源を ON にします。



メモ

管理ツールの操作端末の電源ケーブルを使用する際は、以下について注意してください。

- 管理ツールの操作端末に適合した電圧のコンセントを使用してください。
- 電源ケーブルを接続してから、管理ツールの操作端末の電源を ON にしてください。

- 管理ツールの操作端末の LAN ポートと AMC-0 の管理ポートを LAN ケーブルで接続します。
- 管理ツールの操作端末がストレージシステムにアクセスできるように、管理ツールの操作端末の IP アドレスを設定します。

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。

なお、初期設定サービスを契約されている場合、お客様が指定した IP アドレスが設定されています。

- AMC-0 側ユーザ LAN ポート : 192.168.0.16
- AMC-1 側ユーザ LAN ポート : 192.168.0.17
- サブネットマスク : 255.255.255.0

管理ツールの操作端末の 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。

次の作業

[3.2.2 maintenance utility に保守用アカウントでログインする](#)

3.2.2 maintenance utility に保守用アカウントでログインする

ストレージシステムの保守用アカウントで maintenance utility にログインします。

maintenance utility の起動、終了については、「[B.1.2 VSP One Block Administrator 経由での maintenance utility の起動](#)」、「[B.1.3 AMC の IP アドレス指定による maintenance utility の起動](#)」、「[B.2.2 VSP One Block Administrator 経由で起動した maintenance utility の終了](#)」、「[B.2.3 AMC の IP アドレス指定で起動した maintenance utility の終了](#)」を参照してください。

maintenance utility の画面については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。

前提条件

- ファイアウォールを使用している場合は、次のポートを開放済みであること。
 - HTTP を使用する場合、80 番ポート。
 - HTTPS を使用する場合、443 番ポート。

操作手順

1. Web ブラウザを起動し、次の URL を入力します。

`http(s):// (AMC-0 の管理ポートの IP アドレス) /MaintenanceUtility`

2. 保守用アカウントユーザ名、初期パスワードを入力し、ログインします。

ユーザ名：maintenance

初期パスワード：raid-maintenance

maintenance utility が起動されます。

次の作業

[3.2.3 保守用アカウントのパスワードを変更する](#)

3.2.3 保守用アカウントのパスワードを変更する

保守用アカウントのパスワードを変更します。



メモ

保守用アカウント（ユーザ名：maintenance）は、保守員が保守作業を行う際に使用するアカウントです。必ず、変更後のパスワードを保守員に連絡してください。

操作手順

1. 保守用アカウントで maintenance utility にログインした状態で、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。
[パスワード変更] 画面が表示されます。
2. [パスワード変更] 画面で現在のパスワードと新しいパスワードを入力して、[完了] をクリックします。
3. パスワード変更を継続するかを確認する警告メッセージに対して、[OK] をクリックします。
4. 確認画面で設定内容を確認して、[適用] をクリックします。
5. 完了メッセージが表示されるので、[閉じる] をクリックします。

次の作業

[3.2.4 ストレージシステムの管理ポートのネットワーク情報を設定する](#)

3.2.4 ストレージシステムの管理ポートのネットワーク情報を設定する

ストレージシステムの AMC-0、AMC-1 の管理ポートを、管理 LAN のネットワーク設定に合うように IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバなどを設定します。

前提条件

- ・ 設定するネットワーク情報を確認しておくこと。

操作手順

1. maintenance utility の [管理] メニューから [ネットワーク設定] を選択します。
[ネットワーク設定] 画面が表示されます。
2. [ネットワーク設定] 画面で [ネットワーク設定] をクリックします。
ネットワーク情報を編集するための [ネットワーク設定] 画面が表示されます。
3. [ネットワーク設定] 画面で IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバなどを指定します。
4. [適用] ボタンをクリックします。

- 完了メッセージが表示されるので、[OK] をクリックします。

ESM が再起動され、ログイン画面が表示されます。



メモ

設定内容によっては、ESM が再起動されない場合があります。再起動されずに、[ネットワーク設定] 画面に戻った場合は、手順 8 に進んでください。

- 再度、保守用アカウントでログインします。
- [管理] メニューから [ネットワーク設定] を選択します。
[ネットワーク設定] 画面が表示されます。
- [ネットワーク設定] 画面で、ネットワーク情報が正しく設定されていることを確認します。

次の作業

[3.3 ユーザネットワーク（管理 LAN）への接続](#)

3.3 ユーザネットワーク（管理 LAN）への接続

3.3.1 管理ツールの操作端末とストレージシステムを管理 LAN に接続する

管理ツールの操作端末とストレージシステムの管理ポートを、管理 LAN に接続します。接続後に、管理ツールの操作端末に IP アドレスを設定します。

前提条件

- 管理ポートの IP アドレスを確認しておくこと。



メモ

- 管理ツールの操作端末と、ストレージシステムの管理ポートの接続は、プロキシサーバを経由させないでください。
- 管理ツールの操作端末の arp テーブルに、ストレージシステムの管理ポートと同じ IP アドレスの別装置が記憶されている場合、該当する arp テーブルの IP アドレスを削除してください。
arp テーブルは、コマンドプロンプトで、arp -a を実行すると表示されます。コマンド arp -d を実行して削除対象の IP アドレスを削除してください。

操作手順

- 管理ツールの操作端末、およびストレージシステムの管理ポートを、管理 LAN に接続します。
AMC-0 と AMC-1 の両方の管理ポートを接続してください。
- 管理ツールの操作端末の IP アドレスを、管理 LAN のネットワーク設定に合うように変更します。



メモ

管理ツールの操作端末に複数の LAN ポートを使用して、AMC-0 と AMC-1 の管理ポートに直接接続する場合は、管理ツールの操作端末の LAN ポートに、ブリッジ接続を設定してください。ブリッジ接続については、使用している OS のマニュアルを参照してください。

次の作業

[3.3.2 管理 LAN から VSP One Block Administrator にログインする](#)

3.3.2 管理 LAN から VSP One Block Administrator にログインする

管理ツールの操作端末を管理 LAN に接続した状態で、保守用アカウントで VSP One Block Administrator にログインできることを確認します。

前提条件

- 管理ポートのネットワーク情報の設定が完了していること。

操作手順

1. Web ブラウザを起動し、次の URL を入力します。

`http(s)://` (ESM クラスタロールが Active 状態である AMC の管理ポートの IP アドレス) /

2. 保守用アカウントのユーザ名、パスワードを入力し、ログインします。

VSP One Block Administrator が起動されます。



メモ

- ログインが失敗し、パスワードの変更が必要なメッセージが表示された場合は、maintenance utility でパスワードを変更してから再度 VSP One Block Administrator にログインしてください。
- ログインに 3 回続けて失敗すると、アカウントが 60 秒間ロックされます。ロックアウトポリシーが設定されている場合、その設定に従った挙動となります。詳細は「[D.2.8 ユーザアカウントポリシーの設定](#)」を参照してください。

3. ナビゲーションバーの  をクリックして [Maintenance Utility] を選択し、maintenance utility が起動されること確認します。
4. maintenance utility、VSP One Block Administrator からログアウトします。

次の作業

[3.3.3 管理 LAN の暗号化通信を設定する](#)

3.3.3 管理 LAN の暗号化通信を設定する

管理 LAN の暗号化通信を設定します。

前提条件

- 各通信ポートの設定内容を確認しておくこと。

操作手順

1. maintenance utility の [管理] メニューから [ネットワーク設定] を選択します。
[ネットワーク設定] 画面が表示されます。
2. [ネットワーク設定] 画面で [ネットワーク拒否設定] をクリックします。
[ネットワーク拒否設定] 画面が表示されます。
3. [ネットワーク拒否設定] 画面で暗号化通信を設定したあと、[適用] をクリックします。

項目	説明
TCP ポート(HTTP) (TCP:80)	管理ツールの操作端末とストレージシステム (VSP One Block Administrator、Maintenance Utility) の通信ポートです。 このポートを無効にすると、HTTPS 通信のみが有効になります。

項目	説明
UDP ポート (UDP:31001/31002)	ストレージシステムと RAID Manager ホストの平文通信ポートです。RAID Manager でストレージシステムを操作したい場合に有効にします。通信は暗号化されません。
UDP ポート(DTLS) (UDP:37001/37002)	現在、このポート使用するストレージ管理ソフトウェアはありません。
TCP ポート(SSH) (TCP:20522)	ストレージシステムと SSH クライアントの暗号通信ポートです。SSH 接続による内蔵 CLI でストレージシステムを操作したい場合に有効にします。通信は暗号化されます。

- 完了メッセージが表示されるので [閉じる] ボタンをクリックします。
ESM が再起動され、ログイン画面が表示されます。
- 再度、保守用アカウントでログインします。
- maintenance utility の [管理] メニューから [ネットワーク設定] を選択します。
[ネットワーク設定] 画面が表示されます。
- [ネットワーク設定] 画面で、暗号化通信の設定内容が正しいことを確認します。

次の作業

[3.4 ストレージシステムの日時を設定する](#)

3.4 ストレージシステムの日時を設定する

ストレージシステムの日時設定をします。

次の作業

- NTP サーバと時刻同期して設定する場合
[3.4.1 ストレージシステムの日時を設定する \(NTP サーバを使用する場合\)](#)
- NTP サーバと時刻同期しないで設定する場合
[3.4.2 ストレージシステムの日時を設定する \(NTP サーバを使用しない場合\)](#)

3.4.1 ストレージシステムの日時を設定する (NTP サーバを使用する場合)

ストレージシステムの日時を NTP サーバと同期させる手順を説明します。



メモ

- ストレージシステムの保守中、または保守員用の GUI から、他の設定を実行しているときに、日時を設定すると同期処理は翌日に実施されます。

前提条件

- 管理 LAN 上に NTP サーバを設置していること。
- ストレージシステムと NTP サーバ間にファイアウォールを使用している場合は、123 番のポートを開放済みであること。
- ストレージシステムの日時に適用する UTC タイムゾーンを確認しておくこと。

操作手順

- maintenance utility の [管理] メニューから [日時設定] を選択します。
[日時設定] 画面が表示されます。

2. [日時設定] 画面で、[設定] をクリックします。
ストレージシステムの日時を設定するための [日時設定] 画面が表示されます。
3. 以下の項目を設定します。
 - ・ [UTC タイムゾーン] を選択します。
 - ・ [NTP サーバを使用] の [はい] を選択します。
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] に IP アドレス、またはホスト名を入力します。
 - ・ [同期時刻] に NTP サーバと同期する時刻を指定します。
4. [適用] をクリックします。
5. 完了メッセージが表示されるので [閉じる] をクリックします。
設定内容を確認するための [日時設定] 画面が表示されます。
6. [日時設定] 画面の [更新] をクリックして、設定内容が正しいことを確認します。



メモ

時刻同期が失敗する場合は、NTP サーバの要因が考えられます。NTP サーバの IP アドレス、使用ポートが正しく設定されていることを確認してください。

次の作業

これで、ユーザネットワーク接続と日時設定は完了です。

3.4.2 ストレージシステムの日時を設定する（NTP サーバを使用しない場合）

ストレージシステムの日時を NTP サーバと同期させずに設定する手順を説明します。

前提条件

- ・ ストレージシステムの日時に適用する UTC タイムゾーンを確認しておくこと。

操作手順

1. maintenance utility の [管理] メニューから [日時設定] を選択します。
[日時設定] 画面が表示されます。
2. [日時設定] 画面上で、[設定] をクリックします。
ストレージシステムの日時を設定するための [日時設定] 画面が表示されます。
3. 以下の項目を設定します。
 - ・ [UTC タイムゾーン] で、ストレージシステムの日時に適用するタイムゾーンを選択します。
 - ・ [NTP サーバを使用] の [いいえ] を選択し、現在の日時を入力します。
4. [適用] をクリックします。
5. 完了メッセージが表示されるので [閉じる] をクリックします。
設定内容を確認するための [日時設定] 画面が表示されます。
6. [日時設定] 画面の [更新] をクリックして、日時設定内容が正しいことを確認します。

次の作業

これで、ユーザネットワーク接続と日時設定は完了です。

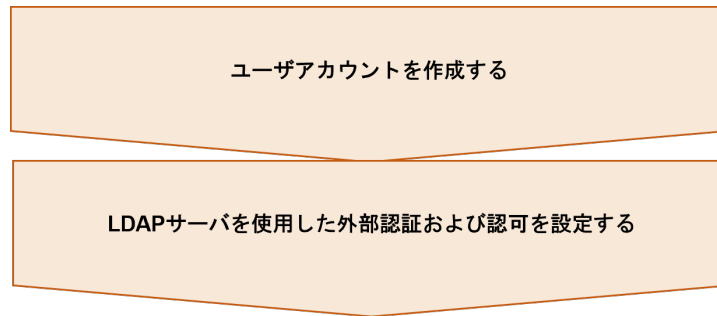
ユーザアカウント作成

管理ユーザアカウントを作成する手順について説明します。

- 4.1 ユーザアカウント作成の流れ
- 4.2 ユーザアカウントを作成する
- 4.3 LDAP サーバを使用した外部認証および認可を設定する

4.1 ユーザアカウント作成の流れ

本章の作業内容を以下のフローに示します。



管理ユーザアカウントの作成は、maintenance utility で実施します。

maintenance utility の起動、終了については、「[B.1.2 VSP One Block Administrator 経由での maintenance utility の起動](#)」、「[B.1.3 AMC の IP アドレス指定による maintenance utility の起動](#)」、「[B.2.2 VSP One Block Administrator 経由で起動した maintenance utility の終了](#)」、「[B.2.3 AMC の IP アドレス指定で起動した maintenance utility の終了](#)」を参照してください。

maintenance utility の画面については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。

ユーザアカウントの登録には、次の方法があります。

- ・ ストレージシステムのみアカウント登録する方法
- ・ 認証サーバの登録アカウントと連携する方法
認証サーバと連携すると、認証サーバが管理するパスワードで、管理ツールにログインできます。
さらに、認証サーバを認可サーバとして使用することもできます。この場合は、ユーザアカウントが属するユーザグループを認可サーバで管理します。

ユーザアカウントの登録方法によって必要な作業が異なります。以下の表に従い、作業を実施してください。

作業	ストレージシステムのみアカウント登録する場合	認証サーバの登録アカウントと連携する（認可サーバとして使用しない）場合	認証サーバの登録アカウントと連携する（認可サーバとして使用する）場合
ユーザアカウントを作成する	実施	実施	実施不要
LDAP サーバを使用した外部認証および認可を設定する	実施不要	実施	実施

ユーザアカウントの作成は、REST API でも操作できます。REST API を使用する場合は、『VSP Block Storage REST API リファレンスガイド』を参照してください。外部認証サーバとの連携設定は、maintenance utility で操作してください。

次の作業

- ・ ストレージシステムのみアカウント登録する場合

[4.2 ユーザアカウントを作成する](#)

- ・ 認証サーバの登録アカウントと連携する（認可サーバとして使用しない）場合
[4.2 ユーザアカウントを作成する](#)
- ・ 認証サーバの登録アカウントと連携する（認可サーバとして使用する）場合
[4.3 LDAP サーバを使用した外部認証および認可を設定する](#)

4.2 ユーザアカウントを作成する

新規にユーザアカウントを作成します。

認証サーバを認可サーバとして使用して登録アカウントと連携する場合、maintenance utility でのユーザアカウント作成は実施不要です。

前提条件

- ・ 作成するユーザ情報を確認しておくこと。

操作手順

1. maintenance utility の [管理] メニューから [ユーザ管理] を選択します。
[ユーザ管理] 画面が表示されます。
2. [ユーザ管理] 画面で [ユーザ作成] をクリックします。
ユーザを作成するための [ユーザ作成] 画面が表示されます。
3. 以下の項目を設定します。

項目	説明
ユーザ名	登録するユーザ名を入力します。 認証サーバと連携する場合は、認証サーバに登録済みのユーザ名を入力します。
アカウント状態	[有効] を選択します。
認証	・ ストレージシステムのみにアカウント登録する場合 [Local] を選択します。 ・ 認証サーバと連携する場合 [External] を選択します。
パスワード	ユーザアカウントのパスワードを入力します。 認証サーバと連携する場合は、入力不要です。
ユーザグループ	ユーザアカウントが属するユーザグループを選択します。

4. [完了] 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。[閉じる] をクリックします。
ユーザを複数作成する場合、作成するユーザ数だけ繰り返してください。
作成したユーザアカウントのユーザ名、パスワードで、VSP One Block Administrator にログインできることを確認してください。認証サーバと連携する場合、ログイン確認作業はスキップしてください。

次の作業

- ・ ストレージシステムのみにアカウント登録する場合
これで、ユーザアカウントの作成は完了です。

- ・ 認証サーバの登録アカウントと連携する（認可サーバとして使用しない）場合
[4.3 LDAP サーバを使用した外部認証および認可を設定する](#)

4.3 LDAP サーバを使用した外部認証および認可を設定する

認証サーバに LDAP サーバを使用した外部認証および認可を設定します。

前提条件

- ・ LDAP サーバの要件を確認しておくこと。
- ・ 要件を満たしている LDAP サーバが構築済みであること。
- ・ 管理 LAN 上に LDAP サーバを設置していること。
- ・ ルート証明書の証明書ファイルを用意しておくこと。
証明書の要件など詳細については、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照してください。
- ・ 外部認証設定に必要な情報を確認しておくこと。
- ・ ストレージシステムと LDAP サーバ間にファイアウォールを設置している場合は、通信に使用するポート番号を開放済みであること。



メモ

- ・ ストレージシステムにユーザアカウントが登録されていない場合、ユーザグループの割り当て（認可）は外部認証サーバでの設定が適用されます。
外部認証サーバで各ユーザアカウントのユーザグループを設定してください。設定の際、ストレージシステムに定義されているユーザグループと同じ名称のグループを外部認証サーバに定義してください。ビルトイングループの名称については、「[D.2 ユーザ管理](#)」を参照してください。
- ・ ストレージシステムにユーザアカウントが登録されている場合、認証の手段として外部認証を選択できますが、ユーザグループの割り当て（認可）は maintenance utility での設定が適用されます。
ユーザグループの割り当て（認可）を外部認証サーバに設定しても適用されません。

操作手順

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

項目	説明
証明書ファイル名	ルート証明書の証明書ファイルを指定します。[参照] ボタンをクリックし、証明書ファイルを指定してください。
DNS Lookup	外部認証・認可サーバの指定方法を選択します。 ・ [有効]: DNS サーバの SRV レコードで、外部認証・認可サーバを指定します。 ・ [無効]: ホスト名、または IP アドレスで、外部認証・認可サーバを指定します。
認証プロトコル	[DNS Lookup] で無効を選択した場合、LDAP プロトコルを選択します。次のプロトコルが選択できます。 ・ LDAP over SSL/TLS ・ STARTTLS

項目		説明
外部ユーザグループ連携		指定した LDAP ディレクトリサーバを認可サーバとしても使用するかを選択します。 ・ [有効]: 使用する ・ [無効]: 使用しない
プライマリサーバ		[DNS Lookup] で無効を選択した場合、[ホスト名] と [ポート番号] に LDAP ディレクトリサーバの情報を設定します。
	プライマリサーバ ホスト名	[DNS Lookup] で無効を選択した場合、LDAP ディレクトリサーバのホスト名、または IP アドレスを入力します。
	プライマリサーバ ポート番号	[DNS Lookup] で無効を選択した場合、LDAP ディレクトリサーバのポート番号を入力します。
	プライマリサーバ ドメイン名称	LDAP ディレクトリツリーのドメイン名称を入力します。
	プライマリサーバ ユーザ名属性	認証で使用するユーザ ID の値が定義されている属性名を入力します。 ・ 使用可能文字: 半角英数字と記号 (! # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~) ・ 階層モデルの場合: ユーザを特定できる値が格納されている属性名を設定します。 ・ フラットモデルの場合: ユーザエントリの RDN の属性名を設定します。
	プライマリサーバ タイムアウト	LDAP ディレクトリサーバとの接続タイムアウトを検出するまでの時間 (秒) を入力します。
	プライマリサーバ リトライ間隔	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔 (秒) を入力します。
	プライマリサーバ リトライ回数	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数を入力します。
	プライマリサーバ Base DN	認証するユーザを検索するときに基点となる DN を入力します。 ・ 使用可能文字: 半角英数字とすべての記号 ・ 階層モデルの場合: すべての検索対象のユーザを含む階層の DN を入力します。 ・ フラットモデルの場合: 検索対象のユーザより 1 つ上の階層の DN を入力します。 記号 (+ ; , < = > など) を入力する場合は、1 文字ごとに記号の直前に円記号 (¥) を入力してエスケープしてください。ただし、¥、/、" を入力するときは、次のとおり円記号 (¥) を入力したあとに ASCII コードを入力してください。 ・ 「¥」は、「¥5c」と入力します。 ・ 「/」は、「¥2f」と入力します。 ・ 「"」は、「¥22」と入力します。
	プライマリサーバ 検索用ユーザ DN	検索用ユーザの DN を入力します。 [プライマリサーバ・ユーザ名属性] に sAMAccountName を指定した場合、または [外部ユーザグループ連携] で有効を選択した場合にのみ、入力が必要です。 ・ 使用可能文字: 半角英数字とすべての記号 記号 (+ ; , < = > など) を入力する場合は、1 文字ごとに記号の直前に円記号 (¥) を入力してエスケープしてください。ただし、¥、/、" を入力するときは、次のとおり円記号 (¥) を入力したあとに ASCII コードを入力してください。 ・ 「¥」は、「¥5c」と入力します。

項目		説明
		「/」は、「¥2f」と入力します。 「"」は、「¥22」と入力します。
	プライマリサーバパスワード	検索用ユーザのパスワードを入力します。LDAP ディレクトリサーバに登録しているパスワードと同じ値を入力してください。 [プライマリサーバ・ユーザ名属性] に sAMAccountName を指定した場合、または [外部ユーザグループ連携] で有効を選択した場合にのみ、入力が必要です。 使用可能文字: 半角英数字と記号 (! # \$ % & ' () * + - . = @ ¥ ^ _ / : ; < > ? [] ` { } ~ " , とスペース)
	セカンダリサーバ	[DNS Lookup] で無効を選択した場合、LDAP ディレクトリサーバの代替サーバを使用するかを選択します。 [有効]: 代替サーバを使用する [無効]: 代替サーバを使用しない
	セカンダリサーバホスト名	[セカンダリサーバ] で有効を選択した場合、プライマリサーバと同様の設定項目を入力します。
	セカンダリサーバポート番号	[セカンダリサーバ] で有効を選択した場合、LDAP ディレクトリサーバの代替サーバのポート番号を入力します。
	テストユーザ名	[サーバ構成テスト] で使用するユーザ名を入力します。 使用可能文字: 半角英数字と記号 (! # \$ % & ' * + - . / = ? @ ^ _ ` { } ~)
	パスワード	[サーバ構成テスト] で使用するユーザのパスワードを入力します。 使用可能文字: 半角英数字と記号 (! # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~)

- 設定内容を確認して、[サーバ構成テスト] の [チェック] をクリックします。
- テストの結果を確認して、[適用] をクリックします。
- [外部認証] 画面で、設定内容が反映されていることを確認します。
- LDAP サーバに登録されているユーザアカウントのユーザ名、パスワードで、VSP One Block Administrator にログインできることを確認します。

外部認証を行うユーザアカウントが複数存在する場合は、外部認証を行うすべてのユーザアカウントでログインできることを確認してください。



メモ

認証サーバのみ使用 ([外部ユーザグループ連携] を無効) にした場合、サーバ構成のテストに成功しても、ストレージシステムに登録されていないユーザアカウントによるアクセスはできません。

認証・認可サーバの使用 ([外部ユーザグループ連携] を有効) でストレージシステムにアクセスできない場合は、LDAP サーバの設定を見直してください。

次の作業

これで、ユーザアカウントの作成は完了です。

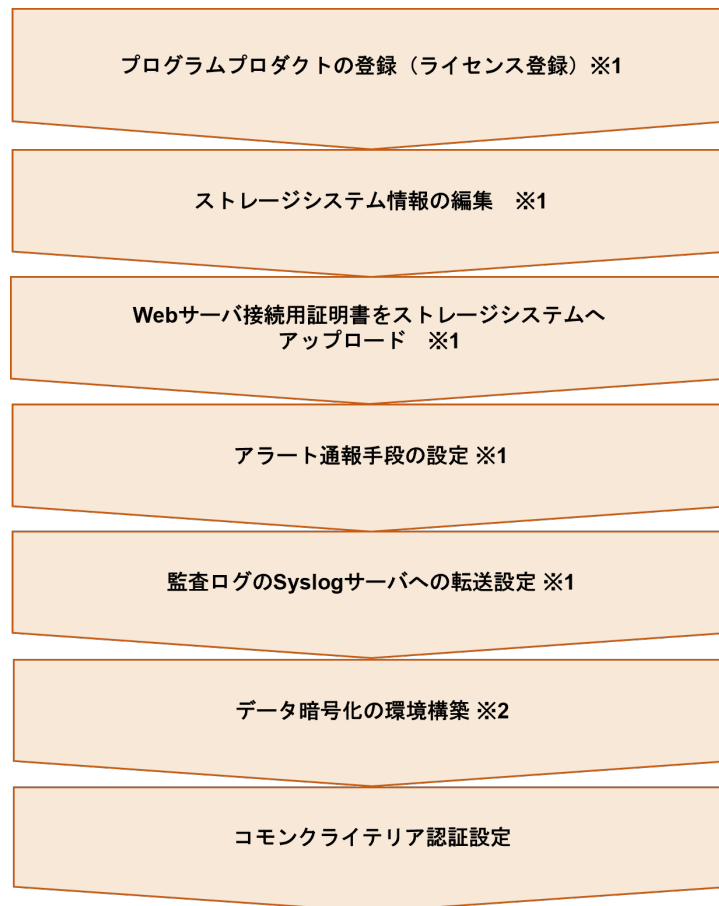
ストレージシステムで使用する機能設定

プログラムプロダクトのインストール、アラート通知手段の設定、データ暗号化の環境構築の手順について説明します。

- 5.1 ストレージシステムで使用する機能設定の流れ
- 5.2 プログラムプロダクトのライセンスを登録する
- 5.3 ストレージシステム情報を編集する
- 5.4 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する
- 5.5 アラート通知手段を設定する
- 5.6 監査ログが Syslog サーバに転送されるようにする
- 5.7 データ暗号化の環境を構築する
- 5.8 コモンクライテリア認証に準拠する設定を実施する

5.1 ストレージシステムで使用する機能設定の流れ

本章の設定作業の流れを以下のフローに示します。



注※1

これらの作業について、本マニュアルでは、maintenance utility による操作手順を記載しています。

maintenance utility の起動、終了については、「[B.1.2 VSP One Block Administrator 経由での maintenance utility の起動](#)」、「[B.1.3 AMC の IP アドレス指定による maintenance utility の起動](#)」、「[B.2.2 VSP One Block Administrator 経由で起動した maintenance utility の終了](#)」、「[B.2.3 AMC の IP アドレス指定で起動した maintenance utility の終了](#)」を参照してください。

maintenance utility の画面については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。これらの作業（アラート通知の Syslog サーバ転送を除く）は、REST API でも操作できます。REST API を使用する場合は、『VSP Block Storage REST API リファレンスガイド』を参照してください。

注※2

データ暗号化の環境構築は、詳細 API または VSP One Block Administrator で実施します。詳細 API の各 API の詳細については、『VSP Block Storage REST API リファレンスガイド』を参照してください。VSP One Block Administrator での操作の詳細については、『VSP One Block Administrator ユーザガイド』を参照してください。

次の作業

[5.2 プログラムプロダクトのライセンスを登録する](#)

5.2 プログラムプロダクトのライセンスを登録する

プログラムプロダクトのライセンスキーをインストールして、プログラムプロダクトを使用できるようにします。

前提条件

- プログラムプロダクト（ライセンスキーファイル）を用意しておくこと。

操作手順

1. maintenance utility の [管理] メニューから [ライセンス] を選択します。
[ライセンス] 画面が表示されます。
2. [ライセンス] 画面で [インストール] をクリックします。
[ライセンスキーインストール] 画面が表示されます。
3. 管理ツールの操作端末の DVD ドライブに、プログラムプロダクト（ライセンスキーファイル）を挿入します。
4. [ライセンスキーインストール] 画面で、[ライセンスキーファイル] を指定して、[適用] をクリックします。
 - ・ ライセンスキーファイルの拡張子は、.plk です。
 - ・ ライセンスキーコードを直接入力することもできます。
5. 完了メッセージが表示されるので、[OK] をクリックします。



メモ

インストールに失敗したプログラムプロダクトがあると、エラーメッセージ画面が表示されます。失敗の原因を表示するには、エラーメッセージ画面でプログラムプロダクトを選択して [詳細] をクリックします。

6. [ライセンス] 画面で、ライセンスが正常にインストールされたことを確認します。
7. プログラムプロダクト（ライセンスキーファイル）を取り出します。

次の作業

[5.3 ストレージシステム情報を編集する](#)

5.3 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 maintenance utility から編集します。

操作手順

1. maintenance utility のメイン画面の [システム情報設定] 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	説明
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。

項目	説明
	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。 先頭または末尾にスペースを入力することはできませんが、そのスペースは取り除かれて設定されます。 この項目を変更すると、maintenance utility の [ストレージシステム] 画面と、[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。 先頭または末尾にスペースを入力することはできませんが、そのスペースは取り除かれて設定されます。 この項目を変更すると、maintenance utility の [ストレージシステム] 画面と、[ストレージシステム] 画面の [SNMP] タブの [連絡先] も変更されます。 この項目の入力は任意です。
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。 先頭または末尾にスペースを入力することはできませんが、そのスペースは取り除かれて設定されます。 この項目を変更すると、maintenance utility の [ストレージシステム] 画面と、[アラート通知] 画面の [SNMP] タブの [場所] も変更されます。 この項目の入力は任意です。

3. 設定内容を確認し [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。

次の作業

[5.4 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する](#)

5.4 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する

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

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



注意

- アップロードする Web サーバ接続用証明書の要件については、「[G.3 ストレージシステムと管理ツールの操作端末間の SSL/TLS 通信](#)」を参照ください。
- ストレージシステムへアップロードする証明書ファイルは、次のいずれかの形式である必要があります。
 - PKCS#12 形式
 - PEM 形式
 - DER 形式

- PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合は、PKCS#12 形式に変換してください（「[G.10 SSL/TLS 証明書を PKCS#12 形式に変換](#)」を参照）。
- PEM 形式または DER 形式でアップロードする場合は、事前に秘密鍵と CSR（公開鍵）を作成してください（「[D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する](#)」を参照）。この際、[目的] に [Web Server] を選択してください。この CSR に基づいて署名された証明書を準備してください。
- 中間証明書が存在する場合は、中間証明書を含んだ証明書チェーンで構成された、署名付き公開鍵証明書を準備してください。

操作手順

1. maintenance utility の左下 [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。
2. 証明書ファイル更新画面が表示されます。
更新対象の証明書の左横のチェックボックスを選択してください。

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

3. アップロードする証明書ファイルの形式を選択します。

形式	説明
PKCS#12	サーバ証明書ファイルと秘密鍵ファイルを含む形式です。
PEM or DER	サーバ証明書ファイルのみの形式です。 [期待する Subject Key Identifier] 欄と、Subject Key Identifier 情報が一致する証明書ファイルをアップロードしてください。証明書ファイルの Subject Key Identifier 情報は、証明書の拡張属性に記載されています。[PEM or DER] を選択しても [期待する Subject Key Identifier] 欄に "-"（ハイフン）が表示される場合は、鍵情報の取得に失敗している可能性があります。3 分程度あけて、再度、「 D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する 」の手順に従って秘密鍵および CSR（公開鍵）の作成をしてください。

4. [ファイルを選択] ボタンをクリックして、アップロードする証明書ファイルを指定します。
手順 3 で PKCS#12 形式を選択した場合は、続けて PKCS#12 のパスワードを入力します。
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。

次の作業

[5.5 アラート通知手段を設定する](#)

5.5 アラート通知手段を設定する

ストレージシステムは、障害を検知すると、アラート（SIM : Service Information Message）を発行します。発行されたアラートは、管理ツールの画面に表示されますが、次に示す手段で通知できます。

- メール送信
- Syslog サーバへの転送
- SNMP トラップ送信

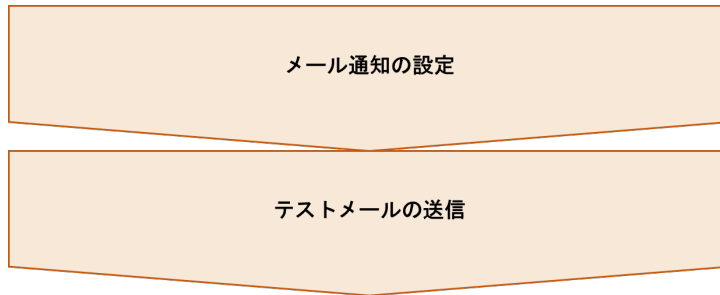
各アラート通知の設定の流れを示します。複数の手段を設定できます。



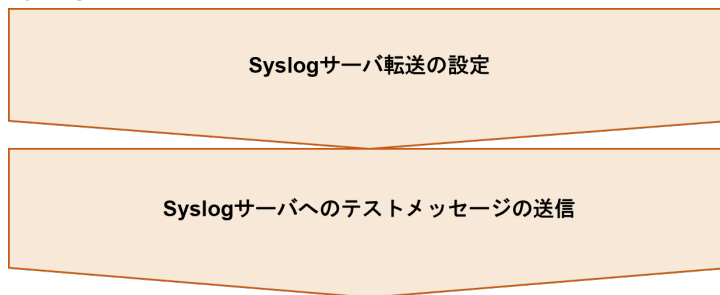
メモ

- アラートは各 AMC の管理ポートの固定 IP アドレスから管理 LAN を介して通知されます。AMC が障害により動作を停止している場合は正常な AMC の管理ポートの固定 IP アドレスから通知されます。このため各 AMC の管理ポートは必ず管理 LAN に接続してください。一方の AMC 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。
- アラートが発行された後、10 分間程度の間に ESM がリポートすると、発行日時とリファレンスコードが同一のアラートが複数回通知される場合があります。発行日時とリファレンスコードが同一のアラートが複数回通知された場合は、maintenance utility のアラート画面を確認し、表示されているアラートごとに対処を行ってください。対処方法については「[6.8 障害通知を受け取った場合の対処方法](#)」を参照してください。

メール通知の場合



Syslog サーバへの転送の場合



SNMP トラップ送信の場合



次の作業

- メール通知の場合
[5.5.1 アラートがメールで通知されるようにする](#)
- Syslog サーバへの転送の場合

[5.5.3 アラートが Syslog サーバに転送されるようにする](#)

- SNMP トラップ送信の場合

[5.5.5 アラートが SNMP トラップ送信されるようにする \(SNMP v1、または v2c の場合\)](#)

[5.5.6 アラートが SNMP トラップ送信されるようにする \(SNMP v3 の場合\)](#)

5.5.1 アラートがメールで通知されるようにする

ストレージシステムの障害発生時に、アラートが指定アドレスにメール送信されるようにします。

前提条件

- メール通知に必要な設定内容を確認しておくこと。

操作手順

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

設定項目	説明
Email 通知	[有効] を選択します。
メールアドレス (To)	[追加] をクリックして、アラート送信先のメールアドレスと属性 (To、Cc、Bcc) を入力します。
メールアドレス (From)	差出人として表示されるメールアドレスを入力します。
メールアドレス (Reply To)	返信先メールアドレスを入力します。入力は任意です。
通知する付加情報	メールの本文冒頭に記載される文章を入力します。
メールサーバ	SMTP サーバのホスト名、または IP アドレスを入力します。
SMTP 認証	SMTP 認証を使用するか選択します。 [有効] を選択した場合は、SMTP 認証に使用するアカウントとパスワードを入力します。

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

次の作業

[5.5.2 アラート通知メールをテスト送信する](#)

5.5.2 アラート通知メールをテスト送信する

アラートのメール通知の設定が完了したら、テストメールを送信します。

前提条件

- アラートのメール通知の設定が完了していること。
- 管理 LAN 上に通信可能な SMTP サーバを設置していること。

- ・ ストレージシステムと SMTP サーバ間にファイアウォールを設置している場合は、25 番のポートを開放済みであること。

操作手順

1. maintenance utility の [管理] メニューから [アラート通知] を選択します。
[アラート通知] 画面が表示されます。
2. [Email] タブの [テスト Email 送信] をクリックします。
3. アラート送信先に指定したメールアドレスで、テストメールを受信したことを確認します。
 - ・ テストメールのメッセージに含まれる SIM リファレンスコードは、7fffff (テスト用のコード) です。
 - ・ 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を解除してください。改行コードの自動削除機能が解除されていないとメールの文章が改行されずに表示されます。

次の作業

[5.6 監査ログが Syslog サーバに転送されるようにする](#)

アラートの Syslog サーバ転送、SNMP トラップ送信を設定する場合は、以下に進んでください。

- ・ [5.5.3 アラートが Syslog サーバに転送されるようにする](#)
- ・ [5.5.5 アラートが SNMP トラップ送信されるようにする \(SNMP v1、または v2c の場合\)](#)
- ・ [5.5.6 アラートが SNMP トラップ送信されるようにする \(SNMP v3 の場合\)](#)

5.5.3 アラートが Syslog サーバに転送されるようにする

ストレージシステムの障害発生時に、アラートが Syslog サーバに転送されるようにします。本設定を実施すると、Syslog サーバにストレージシステムのアラートが蓄積されます。

前提条件

- ・ Syslog サーバ転送に必要な設定内容を確認しておくこと。



メモ

- ・ Syslog 転送プロトコルに、UDP/RFC3164 を使う場合は、ネットワークの設計時に UDP の特性を考慮してください。詳細については、IETF が発行する文書「RFC3164」を参照してください。
- ・ Syslog 転送プロトコルに、TLS/RFC5424 を使う場合は、Syslog サーバのルート証明書の証明書ファイルや、クライアントの証明書ファイルをストレージシステムに設定する必要があります。証明書の要件については、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。
- ・ ストレージシステムへアップロードするクライアントの証明書ファイルは、PKCS#12 形式のファイルである必要があります。PKCS#12 形式のクライアント証明書ファイル作成方法については「[G.10 SSL/TLS 証明書を PKCS#12 形式に変換](#)」を参照してください。

操作手順

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

4. [Syslog] タブを選択して、各設定項目を指定します。

設定項目	説明
転送プロトコル	Syslog 転送プロトコルを選択します。
プライマリサーバ	[有効] を選択して、以下の設定項目を指定します。 • Syslog サーバ ホスト名、または IP アドレス、および転送に使用するポート番号を入力します。 • クライアント証明書ファイル名、パスワード、およびルート証明書ファイル名 Syslog 転送プロトコルに、TLS/RFC5424 を使用する場合にのみ指定します。
セカンダリサーバ	Syslog サーバの代替サーバがある場合は、[有効] を選択して、プライマリサーバと同様に設定項目を指定します。
ロケーション識別名	アラート発行元のストレージシステムを識別するために、任意の名称を設定します。
リトライ、リトライ間隔	Syslog 転送プロトコルに、TLS/RFC5424 を使用する場合にのみ指定します。

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

次の作業

[5.5.4 Syslog サーバにテストメッセージを送信する](#)

5.5.4 Syslog サーバにテストメッセージを送信する

アラートの Syslog 転送の設定が完了したら、Syslog サーバにテストメッセージを送信します。

前提条件

- アラートの Syslog 転送の設定が完了していること。
- 管理 LAN 上に通信可能な Syslog サーバを設置していること。
- ストレージシステムと Syslog サーバ間にファイアウォールを設置している場合は、Syslog の転送に使用するポート番号を開放済みであること。

操作手順

1. maintenance utility の [管理] メニューから [アラート通知] を選択します。
[アラート通知] 画面が表示されます。
2. [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。
3. アラート転送先に指定した 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、"RefCode : 7FFFFFFF, This is Test Report."が含まれています。
 - 7FFFFFFF は、テスト用の SIM リファレンスコードです。

次の作業

[5.6 監査ログが Syslog サーバに転送されるようにする](#)

アラートの SNMP トラップ送信を設定する場合は、以下に進んでください。

- [5.5.5 アラートが SNMP トラップ送信されるようにする \(SNMP v1、または v2c の場合\)](#)
- [5.5.6 アラートが SNMP トラップ送信されるようにする \(SNMP v3 の場合\)](#)

5.5.5 アラートが SNMP トラップ送信されるようにする (SNMP v1、または v2c の場合)

ストレージシステムの障害発生時に、アラートが SNMP トラップ送信されるように、SNMP エージェントを設定します。本項は、SNMP v1、または v2c を使用する場合の操作手順です。

前提条件

- SNMP エージェントに必要な設定内容を確認しておくこと。

操作手順

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

設定項目	説明
SNMP エージェント	[有効] を選択します。
SNMP バージョン	[v1]、または [v2c] を選択します。

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

設定項目	説明
コミュニティ	[新規] チェックボックスを選択し、テキストボックスにコミュニティ名を入力します。 [新規] チェックボックスの選択を解除すると、プルダウンメニューから登録済みのコミュニティを選択できます。
トラップ送信先	[新規] チェックボックスを選択し、トラップ送信先の IP アドレスを指定します。 [新規] チェックボックスの選択を解除すると、プルダウンメニューから登録済みの IP アドレスを選択できます。

- c. [OK] をクリックします。
入力した情報が [アラート通知設定] 画面の [トラップ送信設定] に反映されます。
6. リクエスト許可設定を行う場合は、以下の手順に従ってください。
 - a. [リクエスト許可設定] の [追加] をクリックします。
[リクエスト許可設定追加] 画面が表示されます。
 - b. [リクエスト許可設定追加] 画面で、以下の項目を指定します。

設定項目	説明
コミュニティ	[新規] チェックボックスを選択し、テキストボックスにコミュニティ名を入力します。

設定項目	説明
	[新規] チェックボックスの選択を解除すると、プルダウンメニューから登録済みのコミュニティを選択できます。
リクエスト許可対象	すべてのマネージャの REQUEST オペレーションを許可する場合は、[全て] のチェックボックスを選択します。 REQUEST オペレーションを許可するマネージャを指定する場合は、[新規] チェックボックスを選択し、IP アドレスを入力します。[新規] チェックボックスの選択を解除すると、プルダウンメニューから登録済みの IP アドレスを選択できます。

- c. [OK] をクリックします。

入力した情報が [アラート通知設定] 画面の [リクエスト許可設定] に反映されます。

7. [システムグループ情報] を入力します。

8. 設定内容を確認し [適用] をクリックします。

[アラート通知] 画面が表示されます。

9. [SNMP] タブを選択し、設定内容が正しいことを確認します。

次の作業

[5.5.8 SNMP マネージャヘトラップをテスト送信する](#)

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

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

前提条件

- SNMP エージェントに必要な設定内容を確認しておくこと。

操作手順

1. maintenance utility の [管理] メニューから [アラート通知] を選択します。

[アラート通知] 画面が表示されます。

2. [アラート通知] 画面の [設定] をクリックします。

[アラート通知設定] 画面が表示されます。

3. [アラート通知設定] 画面の [アラート通知] で、アラート通知対象の SIM を選択します。

対象の SIM の選択は、すべての通知方法 (Email、Syslog、SNMP) で共通の設定です。

4. [アラート通知設定] 画面の [SNMP] タブを選択して、以下の項目を指定します。

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

5. トラップ送信先を指定します。以下の手順に従ってください。

- a. [トラップ送信設定] の [追加] をクリックします。

[トラップ送信設定追加] 画面が表示されます。

- b. [トラップ送信設定追加] 画面で、以下の項目を指定します。

設定項目	説明
トラップ送信先	トラップ送信先の IP アドレスを指定します。

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

- c. [OK] をクリックします。
入力した情報が [アラート通知設定] 画面の [トラップ送信設定] に反映されます。
6. リクエスト許可設定を行う場合は、以下の手順に従ってください。
 - a. [リクエスト許可設定] の [追加] をクリックします。
[リクエスト許可設定追加] 画面が表示されます。
 - b. [リクエスト許可設定追加] 画面で、以下の項目を指定します。

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

- c. [OK] をクリックします。
入力した情報が [アラート通知設定] 画面の [リクエスト許可設定] に反映されます。
7. [SNMP エンジン ID] を入力します。
 - ・ SNMP エンジン ID を指定する必要がある場合：
[ID をランダムに生成] を選択してください。
 - ・ SNMP エンジン ID を指定したい場合：
10～64 桁の 16 進数を、文字数が偶数になるように（16 進数のため）入力してください。
8. [システムグループ情報] を入力します。
9. 設定内容を確認し [適用] をクリックします。
[アラート通知] 画面が表示されます。
10. [SNMP] タブを選択し、設定内容が正しいことを確認します。

次の作業

[5.5.7 SNMP エンジン ID を SNMP マネージャに登録する \(SNMP v3 の場合\)](#)

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

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

前提条件

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

操作手順

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

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

2. [管理] メニューから [アラート通知] を選択します。
[アラート通知] 画面が表示されます。
3. [SNMP] タブの [SNMP エンジン ID] の値を確認します。
4. 各 AMC の SNMP エンジン ID を SNMP マネージャに登録します。
登録方法は、お使いの SNMP マネージャのマニュアルを参照してください。

次の作業

[5.5.8 SNMP マネージャへトラップをテスト送信する](#)

5.5.8 SNMP マネージャへトラップをテスト送信する

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

前提条件

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

操作手順

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

次の作業

- [5.6 監査ログが Syslog サーバに転送されるようにする](#)

5.6 監査ログが Syslog サーバに転送されるようにする

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。

ストレージシステムに保存できる監査ログの容量に限りがあります。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、監査ログを常時自動で取得する Syslog サーバへの転送設定を推奨します。なお、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。

Syslog サーバへの転送設定の流れを示します。

監査ログのSyslogサーバ転送設定

監査ログのテストメッセージの送信



メモ

- Syslog サーバに異常が発生したときなど、Syslog サーバから監査ログを取得できない場合は、監査ログを管理ツールの操作端末にエクスポートできます。操作手順は、「[D.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](#)」を参照してください。
- Syslog サーバへの監査ログ転送は、各 AMC の管理ポートの固定 IP アドレスから管理 LAN を介して行われます。AMC が障害により動作を停止している場合は正常な AMC の管理ポートの固定 IP アドレスから転送されます。このため各 AMC の管理ポートは必ず管理 LAN に接続してください。一方の AMC の管理ポートだけが管理 LAN に接続されていると、監査ログが正しく転送されない可能性があります。

次の作業

[5.6.1 監査ログの Syslog サーバへの転送を設定する](#)

5.6.1 監査ログの Syslog サーバへの転送を設定する

監査ログを Syslog サーバに転送する設定手順を示します。

前提条件

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



注意

- Syslog 転送プロトコルに、UDP/RFC3164 を使う場合は、ネットワークの設計時に UDP の特性を考慮してください。詳細については、IETF が発行する文書 RFC3164 を参照してください。
- Syslog 転送プロトコルに、TLS/RFC5424 を使う場合は、Syslog サーバのルート証明書の証明書ファイルや、クライアントの証明書ファイルをストレージシステムに設定する必要があります。証明書の要件については、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。
- ストレージシステムへアップロードするクライアントの証明書ファイルは、次のいずれかの形式である必要があります。
 - PKCS#12 形式
 - PEM 形式
 - DER 形式
- PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合は、PKCS#12 形式に変換してください（「[G.10 SSL/TLS 証明書を PKCS#12 形式に変換](#)」を参照）。
- PEM 形式または DER 形式でアップロードする場合は、事前に秘密鍵と CSR（公開鍵）を作成してください（「[D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する](#)」を参照）。

参照)。この際、[目的] に [Audit Syslog Client (Primary)]、[Audit Syslog Client (Secondary)] または [Audit Syslog Client (Primary and Secondary)] を選択してください。
この CSR に基づいて署名された証明書を準備してください。

操作手順

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

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

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

次の作業

[5.6.2 Syslog サーバに監査ログのテストメッセージを送信する](#)

5.6.2 Syslog サーバに監査ログのテストメッセージを送信する

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

前提条件

- 監査ログの転送設定が完了していること。

操作手順

1. maintenance utility の [管理] メニューから [監査ログ設定] を選択します。

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

次の作業

[5.7 データ暗号化の環境を構築する](#)

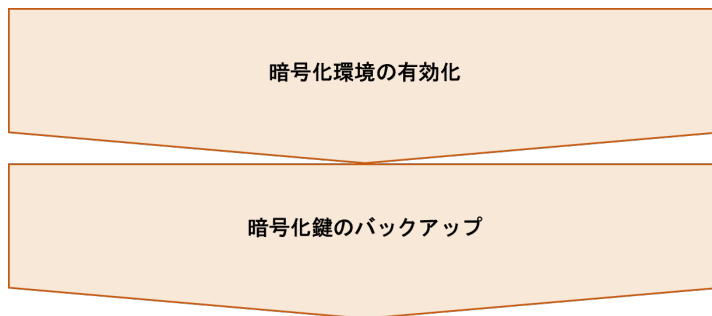
5.7 データ暗号化の環境を構築する

ホスト（サーバ）からストレージシステムにデータを書き込む際に、データを暗号化したい場合に、データ暗号化の環境を構築します。

データ暗号化の環境を構築した上で、暗号化を有効にしたプール、またはパリティグループに、ボリュームを作成すると、そのボリュームのデータが暗号化されます。

データ暗号化の仕様やシステム要件については、『Encryption License Key ユーザガイド』を参照してください。

データ暗号化の環境構築設定の流れを示します。



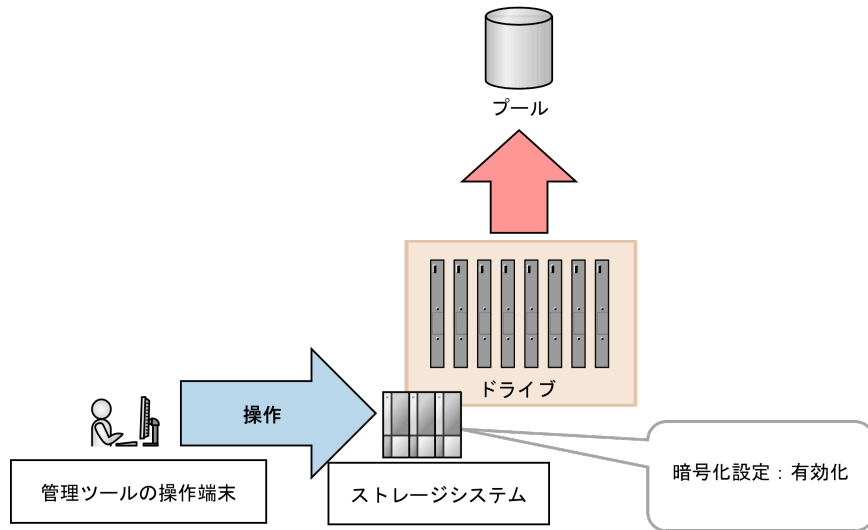
これらの作業は、詳細 API または VSP One Block Administrator で設定します。詳細 API の各 API の詳細については、『VSP Block Storage REST API リファレンスガイド』を参照してください。VSP One Block Administrator での操作の詳細については、『VSP One Block Administrator ユーザガイド』を参照してください。

次の作業

[5.7.1 暗号化環境を有効化する](#)

5.7.1 暗号化環境を有効化する

暗号化環境を有効化します。暗号化が有効なプール、またはパリティグループを作成するには、事前に、暗号化環境の有効化が必要です。VSP One Block Administrator、または詳細 API による操作手順を説明します。



(1) VSP One Block Administrator での操作手順（暗号化環境を有効化する）

前提条件

- 実行ユーザにセキュリティ管理者（参照・編集）が割り当てられていること。



メモ

詳細 API または VSP One Block Administrator を実行するユーザが、対象ストレージシステムのリソースを詳細 API または VSP One Block Administrator でロックしている場合、次の操作手順に示す操作を実行できません。その場合は、ロックを解除してから実行してください。

操作手順

- VSP One Block Administrator のナビゲーションツリーから [設定] - [格納データ暗号化] - [暗号化環境設定] を選択します。
[暗号化環境設定] 画面が表示されます。
- [暗号化環境設定] 画面で、[暗号化環境設定編集] をクリックします。
[暗号化環境設定編集] 画面が表示されます。
- [暗号化環境設定編集] 画面の [暗号化環境] で [有効] を選択して、[実行] をクリックします。
[暗号化環境設定] 画面が表示されます。
- [暗号化環境設定] 画面で、暗号化環境が有効化されたことを確認します。

次の作業

[5.7.2 暗号化鍵をバックアップする](#)

(2) 詳細 API での操作手順（暗号化環境を有効化する）

ここでは、詳細 API のリクエストラインのみ説明します。リクエストラインの設定情報、参照情報については、『VSP Block Storage REST API リファレンスガイド』を参照してください。

前提条件

- ・ 実行ユーザにセキュリティ管理者（参照・編集）が割り当てられていること。



メモ

詳細 API または VSP One Block Administrator を実行するユーザが、対象ストレージシステムのリソースを詳細 API または VSP One Block Administrator でロックしている場合、次の操作手順に示す操作を実行できません。その場合は、ロックを解除してから実行してください。

操作手順

1. 暗号化環境を有効化します。

リクエストライン

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

2. 暗号化環境が有効化されたことを確認します。

リクエストライン

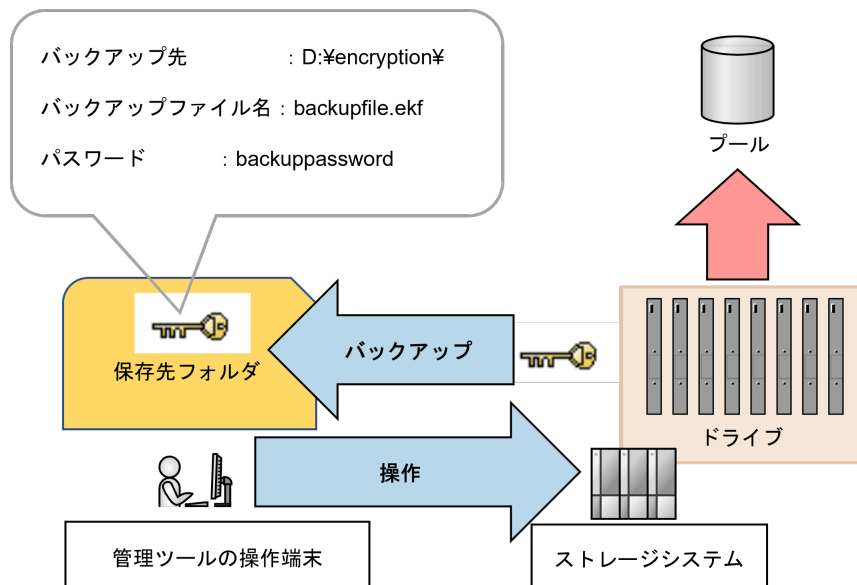
```
GET <ベース URL> /v1/objects/encryption-settings/instance
```

次の作業

[5.7.2 暗号化鍵をバックアップする](#)

5.7.2 暗号化鍵をバックアップする

暗号化鍵を管理ツールの操作端末上のファイルにバックアップします。VSP One Block Administrator、または詳細 API による操作手順を説明します。



(1) VSP One Block Administrator での操作手順（暗号化鍵をバックアップする）

前提条件

- ・ 実行ユーザにセキュリティ管理者（参照・編集）が割り当てられていること。
- ・ 管理ツールの操作端末のバックアップファイル保存先、バックアップファイル名を確認しておくこと。

- ・ 管理ツールの操作端末にバックアップファイルが保存できるだけの空き容量が確保されていること。



メモ

- ・ 詳細 API または VSP One Block Administrator を実行するユーザが、対象ストレージシステムのリソースを詳細 API または VSP One Block Administrator でロックしている場合、次の操作手順に示す操作を実行できません。その場合は、ロックを解除してから実行してください。
- ・ 鍵のバックアップに失敗した場合でも、バックアップ回数が増えることがあります。

操作手順

1. ナビゲーションツリーから [設定] - [格納データ暗号化] - [暗号化鍵] を選択します。
[暗号化鍵] 画面が表示されます。
2. [暗号化鍵] 画面右上の三点リーダーから [ファイルに暗号化鍵をバックアップ] をクリックします。
[ファイルに暗号化鍵をバックアップ] 画面が表示されます。
3. [ファイルに暗号化鍵をバックアップ] 画面で、必要な項目を指定して、[実行] をクリックします。
4. 管理ツールの操作端末に暗号化鍵ファイルがバックアップされたことを確認します。

次の作業

これで、ストレージシステムで使用する機能設定（プログラムプロダクトのインストール、アラート通知手段の設定、データ暗号化の環境構築）は完了です。

(2) 詳細 API での操作手順（暗号化鍵をバックアップする）

ここでは、詳細 API のリクエストラインのみ説明します。リクエストラインの設定情報、参照情報、ファイルダウンロード（暗号化鍵バックアップ）のサンプルコードについては、『VSP Block Storage REST API リファレンスガイド』を参照してください。

前提条件

- ・ 実行ユーザにセキュリティ管理者（参照・編集）が割り当てられていること。
- ・ 管理ツールの操作端末のバックアップファイル保存先、バックアップファイル名を確認しておくこと。
- ・ 管理ツールの操作端末にバックアップファイルが保存できるだけの空き容量が確保されていること。



メモ

- ・ 詳細 API または VSP One Block Administrator を実行するユーザが、対象ストレージシステムのリソースを詳細 API または VSP One Block Administrator でロックしている場合、次の操作手順に示す操作を実行できません。その場合は、ロックを解除してから実行してください。
- ・ 鍵のバックアップに失敗した場合でも、バックアップ回数が増えることがあります。

操作手順

1. 暗号化鍵ファイルをバックアップします。

リクエストライン

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



メモ

サンプルコードを提供しています。ファイルダウンロード（暗号化鍵バックアップ）記載したファイルは次のとおりです。

backup_encryption_keys.py

2. 暗号化鍵ファイルがバックアップされたことを確認します。

詳細 API クライアントの指定したパスに、暗号化鍵ファイルのバックアップファイルが作成されたことを確認してください。

次の作業

[5.8 コモンクライテリア認証に準拠する設定を実施する](#)

5.8 コモンクライテリア認証に準拠する設定を実施する

ストレージシステムがサポートしているコモンクライテリア認証の要件に準拠するセキュリティ機能の一部は、デフォルトで無効です。

コモンクライテリア認証に準拠するセキュリティ機能を使用したい場合は、[コモンクライテリア認証設定] 画面で機能の有効化を実施してください。

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] - [コモンクライテリア認証設定] を選択します。
3. [コモンクライテリア認証設定] 画面が表示されます。

コモンクライテリア認証設定に関わる機能の有効、または無効を指定してください。

「コモンクライテリア認証に準拠する」のチェックボックスを ON にすると、次の表の各機能を一括で有効化できます。

設定項目	内容
管理ポート TLS 通信ログの 監査ログ出力	有効または無効を設定します。 有効にすると管理ポートとの TLS 通信※1 が、監査ログに記録されるようになります。
証明書ファイルアップロー ド時の検証項目追加	有効または無効を設定します。 有効にすると証明書ファイルアップロード時に実施する検証項目が追加※2 され、より厳しい検証が実施されます。

注※1

管理ツールの操作端末から Web ブラウザまたは詳細 API クライアントを使用してリクエストを送信した際、TLS 通信の開始または終了が監査ログに記録されます。

注※2

「証明書ファイルアップロード時の検証項目追加」を有効化すると、有効化前まではアップロードできていた証明書もアップロードできなくなる可能性がありますので、十分にご注意ください。

有効化した際に追加される証明書の検証項目の詳細は、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。

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るので、[閉じる] をクリックします。

ESM が再起動され、ログイン画面が表示されます。

6. 再度、保守用アカウントでログインします。
7. 左下の [メニュー] – [システム管理] – [コモンクライテリア認証設定] を選択します。
[コモンクライテリア認証設定] 画面が表示されます。
8. [コモンクライテリア認証設定] 画面で、コモンクライテリア認証に準拠する設定が正しく設定されていることを確認します。

次の作業

これで、ストレージシステムで使用する機能設定（プログラムプロダクトのインストール、アラート通知手段の設定、データ暗号化の環境構築、コモンクライテリア認証に準拠する設定）は完了です。

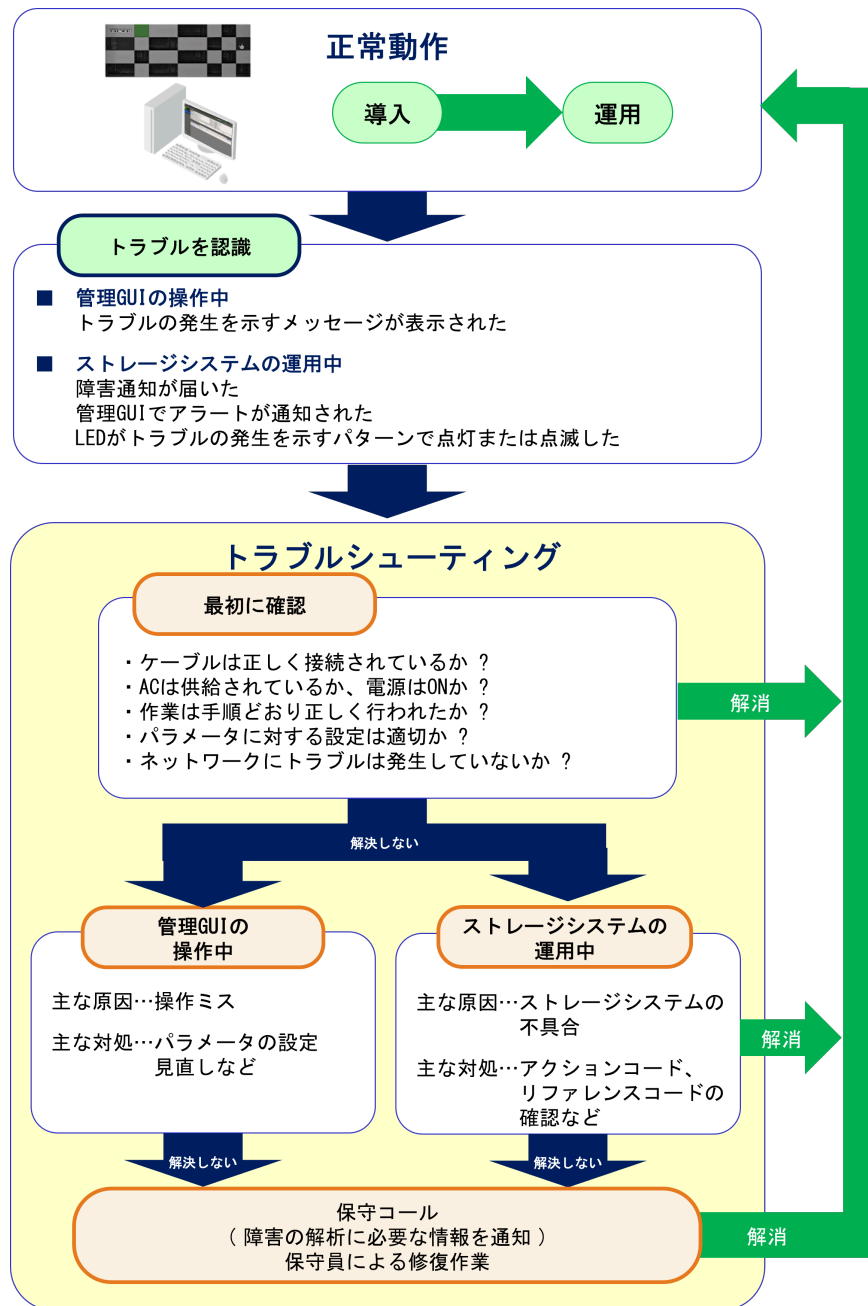
トラブルシューティング

初期構築作業時、管理 GUI（VSP One Block Administrator、maintenance utility）および内蔵 CLI の起動あるいは操作時に発生したトラブルシューティングについて説明します。

- 6.1 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
- 6.2 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
- 6.3 トラブルシューティング作業前の確認
- 6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法
- 6.5 maintenance utility の内部アラート詳細の確認手順
- 6.6 maintenance utility の FRU（Field Replacement Unit）に関するアラートの確認手順
- 6.7 管理 GUI を起動する際にトラブルが発生した場合の対処方法
- 6.8 障害通知を受け取った場合の対処方法
- 6.9 ホスト（サーバ）がストレージシステムを認識できない場合の対処方法
- 6.10 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

6.1 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。

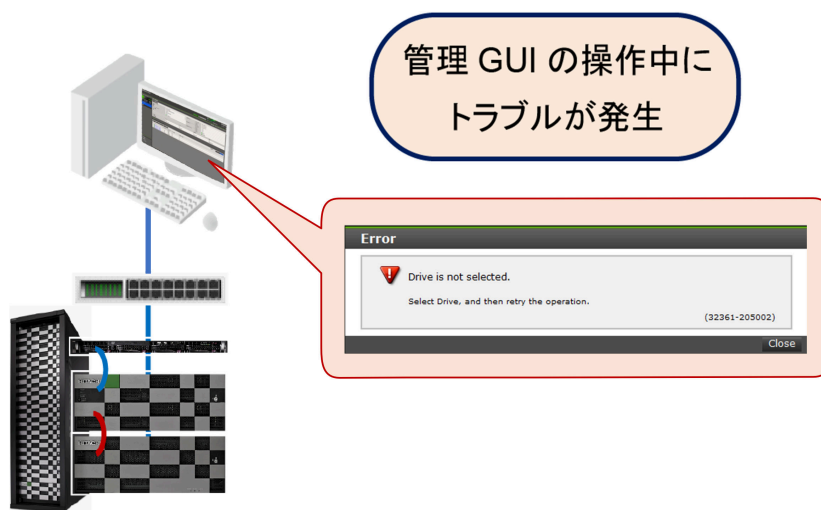


6.2 トラブルを認識する状況とトラブルシューティング手順の参照先

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。



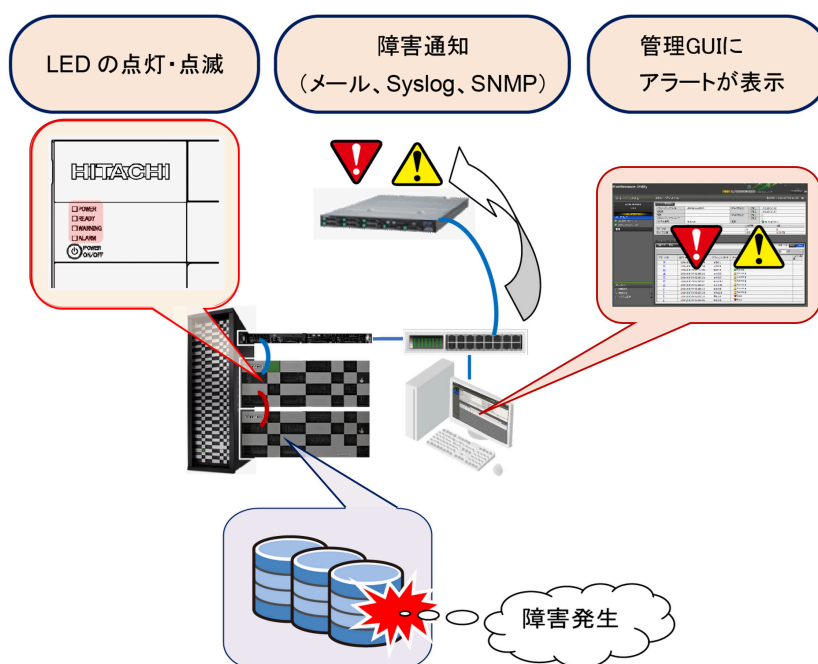
maintenance utility の操作中にトラブルを認識した場合は、「[6.3 トラブルシューティング作業前の確認](#)」および「[6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法](#)」を参照してください。

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、「[6.3 トラブルシューティング作業前の確認](#)」および「[6.9 ホスト（サーバ）がストレージシステムを認識できない場合の対処方法](#)」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。「[6.3 トラブルシューティング作業前の確認](#)」および「[6.8 障害通知を受け取った場合の対処方法](#)」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。「[6.3 トラブルシューティング作業前の確認](#)」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、弊社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。「[6.3 トラブルシューティング作業前の確認](#)」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。

- ・ ダンプファイルの採取によるトラブルシューティング
弊社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。弊社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、「[D.11.9 システムダンプのダウンロード](#)」を参照してください。



メモ

お客様が用意した管理ツールの操作端末の本体、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。

6.3 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。

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	

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

初期構築作業は、参照先の手順に従って行ってください。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、LDAP サーバへ登録する必要がある場合もあります。

6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法

maintenance utility の操作中にトラブルを認識した場合、次の表を参照し、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。	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 アドレスを保守員に連絡してください。 - 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:: ~ FDFE: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::xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値) - グローバルユニキャストアドレス : [2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値) - グローバルユニキャストアドレス : [2002:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)

分類	障害内容	対処方法
	- 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（「3.2.4 ストレージシステムの管理ポートのネットワーク情報を設定する」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。
ログイン障害	- maintenance utility の操作中に 32061-205006 エラーが発生する。 - maintenance utility にログインできない。	ログインにおけるユーザ名、またはパスワードが正しいか確認してください。間違っていた場合は、正しいユーザ名とパスワードにて再度ログインしてください。DNS サーバや外部認証サーバを利用して認証を実施している場合、ネットワークで問題が発生していないか、ネットワークおよびサーバ設定の確認をしてください。 外部認証サーバを利用して認証を実施している場合、外部認証サーバの証明書が要件を満たしていること、外部認証サーバが TLS 通信の要件を満たしていることを確認してください。要件については、「G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信」を参照ください。
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。 - 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 7c2000 が発生した。 - NTP サーバを使用した日時設定に失敗する。 - SIM コード 7d20xx、7d1dxx、または 7d1exx が発生した。	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。 - 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ないか確認してください。 - Syslog 転送プロトコルに TLS/RFC5424 を使用している場合は、Syslog サーバの証明書ファイルやクライアントの証明書ファイルが要件を満たしていること、Syslog サーバが TLS 通信の要件を満たしていることを確認してください。

分類	障害内容	対処方法
		要件については、「G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信」を参照ください。 ストレージシステムが接続されているネットワークの負荷を確認してください。
	maintenance utility の接続時に「接続がプライベートではありません」と表示され、接続できない。	設定されている IP アドレスやドメイン名が「HSTS プリロードリスト」に含まれ、かつ Web サーバ証明書が信頼済み証明書として登録されていない可能性があります。 - 使用されている IP アドレスが正しいか確認してください。 - 設定されているサービスの IP アドレスまたは AMC の IP アドレスで、「HSTS プリロードリスト」に含まれない IP アドレス、またはドメイン名で maintenance utility にアクセスして、Web サーバ証明書を更新してください。 Google Chrome の場合、アドレスバーに [chrome://net-internals/#hsts] と入力すると、HSTS に関するページから「HSTS プリロードリスト」を確認できます。例えば、IP アドレス 1.0.0.1 は、static_sts_domain: 1.0.0.1 と表示され、「HSTS プリロードリスト」に登録されていることがわかります。
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 - Windows 画面下部の [虫眼鏡マーク] で [control] を入力します。検索結果一覧から [コントロールパネル] を選択します。[コントロールパネル] 画面が表示されます。 [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。 [セキュリティ] タブを選択します。 [信頼済みサイト] - [サイト] をクリックします。 [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。 [この Web サイトをゾーンに追加する] に AMC-0 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。※ - 同様に、AMC-1 の IP アドレスも追加します。※ [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 - Windows 画面下部の [虫眼鏡マーク] で [control] を入力します。検索結果一覧から [コントロールパネル] を選択します。[コントロールパネル] 画面が表示されます。 [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。 [セキュリティ] タブを選択します。 [信頼済みサイト] - [サイト] をクリックします。 [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。

分類	障害内容	対処方法
		6. [この Web サイトをゾーンに追加する] に AMC-0 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。※ 7. 同様に、AMC-1 の IP アドレスも追加します。※ 8. [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ままになっている。	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。
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イ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。
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、強制再読み込みをします。
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. 画面左上の [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。

分類	障害内容	対処方法
操作抑制	maintenance utility を操作しようとする、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。”というエラー画面が表示される。	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。 上記以外の場合は、次の手順で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。 システムロックの強制解除を行う際は、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ことを確認してください。 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。
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。 - 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수에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、「(8) アカウントロックの解除」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いる場合は、「(9) アカウントの有効化」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。 「(2) ユーザアカウントのパスワードポリシー設定」を参照して、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※

AMC-0、AMC-1 の IP アドレスは、maintenance utility の [管理] メニューから [ネットワーク設定] 画面を表示して確認してください。

6.5 maintenance utility の内部アラート詳細の確認手順

保守員からアラート詳細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 のヘッダエリアで、[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、[内部アラート参照・DKC]、または [内部アラート参照・ESM] を選択します。
[内部アラート (DKC)]、または [内部アラート (ESM)] 画面が表示されます。
3. [内部アラート (DKC)] 画面の場合
[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。
[内部アラート (ESM)] 画面の場合
[SSB (AMC-0)] タブ、または [SSB (AMC-1)] タブを選択します。
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。
[内部アラート詳細] が表示されます。保守員の指示に従ってください。

6.6 maintenance utility の FRU (Field Replacement Unit) に関するアラートの確認手順

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、アラート対象のハードウェアを選択します。ハードウェアの [状態] リンクのアイコンを確認し、リンクをクリックします。
[関連アラート] 画面が表示されます。
ハードウェアごとの [関連アラート] 画面起動方法は、次に示します。

部位	メイン画面	タブ	[状態] リンク
HSN ボックス-x	[HSN ボックス (HSNBX-x)] 画面	AMC	状態
		HSNPANEL	状態
		ISW	状態
		PS	状態
DKC-x	[コントローラシャーシ] 画面	CTL	CTL
			CMG 状態
		FANM	状態
		BAT	状態

部位	メイン画面	タブ	〔状態〕 リンク
		HIE	状態
		CHB	状態
			SFP 状態※
		DKB	DKB 状態
		SMC	状態
		PS	状態
	〔Small Form-Factor Pluggable〕 画面	-	SFP 状態
DKU-xx : DB-XXX&XXX	〔DKU-xx : ドライブボックス (DB-xxx&xxx)〕 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〕リンクのアイコンの意味を、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	
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”	オレンジ	

状態	意味	部品の枠の色	状態のアイコン
	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。		
Copying n % (TYPE to spare area)	[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" 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	
Copying n % (TYPE from spare area)	[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" 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 to spare area)	[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" 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	
Pending (TYPE from spare area)	[ドライブ状態限定] コピーが中断している状態です。	オレンジ	

状態	意味	部品の枠の色	状態のアイコン
	TYPE : "Copy back" "Dynamic sparing" "Drive copy" 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。		
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] スペアドライブを使用できない状態です。	オレンジ	

2. [関連アラート] 画面から、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であるアラートが表示されます。

[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。
3. [アラート ID] の文字列をクリックします。
[アラート詳細] 画面が表示されます。
4. [アラート詳細] 画面でアラートを確認し、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。

6.7 管理 GUI を起動する際にトラブルが発生した場合の対処方法

管理 GUI (VSP One Block Administrator、maintenance utility) を起動する際にトラブルが発生した場合の対処方法を説明します。

項番	障害内容	対処方法
1	管理ツールの操作端末から管理 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「3.2.4 ストレージシステムの管理ポートのネットワーク情報を設定する」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 ・ 「D.11.15 TLS セキュリティ設定を管理する」の手順に従い、maintenance utility で TLS 通信のセキュリティ設定を変更している場合、ストレージシステムに登録されている Web サーバ接続用証明書が、設定に必要な要件を満たしているか、確認してください。
2	LDAP サーバを使用した外部認証にて、LDAP サーバ設定変更後にログインができない。	LDAP サーバの設定内容に問題ないか「4.3 LDAP サーバを使用した外部認証および認可を設定する」で確認してください。 設定内容に問題がない場合、「D.11.7 ESM のリブート」を実施後、ログインの再操作を行ってください。

項番	障害内容	対処方法
3	VSP One Block Administrator が操作できない。	接続できる AMC の maintenance utility にログインして、手動フェールオーバーを実行してください。その後に VSP One Block Administrator を起動してください。
4	両方の AMC の maintenance utility にアクセスできない。または、maintenance utility の ESM クラスターロールに Starting が存在する。	弊社保守員に障害内容を連絡して対策を依頼してください。
5	管理 GUI を起動すると「接続がプライベートではありません」と表示される。	設定されている IP アドレスやドメイン名が「HSTS プリロードリスト」に含まれ、かつ Web サーバ証明書が信頼済み証明書として登録されていない可能性があります。 - 使用されている IP アドレスが正しいか確認してください。 - 設定されているサービスの IP アドレスまたは AMC の IP アドレスで、「HSTS プリロードリスト」に含まれない IP アドレス、またはドメイン名で maintenance utility にアクセスして、Web サーバ証明書を更新してください。 Google Chrome の場合、アドレスバーに [chrome://net-internals/#hsts] と入力すると、HSTS に関するページから「HSTS プリロードリスト」を確認できます。例えば、IP アドレス 1.0.0.1 は、static_sts_domain: 1.0.0.1 と表示され、「HSTS プリロードリスト」に登録されていることがわかります。

6.8 障害通知を受け取った場合の対処方法

「[5.5 アラート通知手段を設定する](#)」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。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。



メモ

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。

6.9 ホスト（サーバ）がストレージシステムを認識できない場合の対処方法

ホスト（サーバ）からストレージシステムを認識できない場合の主な原因と、その対処方法を説明します。

- ホスト（サーバ）に障害が発生している場合の現象、主要要因および対処方法

項番	現象	主な原因	対処方法
1	HBA、NIC、または CNA のリンクアップランプが消灯	ファイバチャネルケーブル、または STP 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。 - Ethernet（iSCSI、NVMe/TCP）接続の場合、日立がサポートとしている 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方法

項番	現象	主な原因	対処方法
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、またはストレージシステム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	ファイバチャネルケーブル、または STP 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	- ファイバチャネル接続の場合は、ゾーニング設定を見直してください。 - Ethernet 接続の場合は、VLAN 設定を見直してください。

- ホスト（サーバ）とストレージシステムが通信できない原因が iSCSI、NVMe/TCP にあると推定された場合、以下の表に示す確認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。

項番	確認項目
1	ホスト（サーバ）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（サーバ）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（サーバ）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。

項番	確認項目
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（サーバ）の iSCSI ドライバまたは NVMe/TCP ドライバの設定を確認してください。
9	ストレージシステムのポートに対して、ホスト（サーバ）の IPsec が OFF ですか？ ホスト（サーバ）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（サーバ）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（サーバ）、スイッチなど）でストレージシステム iSCSI Port または NVMe/TCP 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でアドレスの状態を確認してください。※
11	ホスト（サーバ）が iSCSI ドライバまたは NVMe/TCP ドライバを認識できていますか？
12	- iSCSI の場合 ホスト（サーバ）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？ - NVMe/TCP の場合 ホスト（サーバ）から Target に誤った IP アドレスと Host NQN でログインしていませんか？
13	ホスト（サーバ）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（サーバ）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（サーバ）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（サーバ）に正しく設定できていますか？
20	- iSCSI の場合 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。 - NVMe/TCP の場合 Namespace 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 Host NQN のリストに、接続する Initiator の Host NQN がありますか？ リストにない場合、接続する Initiator の Host NQN を Target に割り当ててください。

注※：次の IPv6 確認事項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。

確認事項		対策
接続する iSCSI Port または NVMe/TCP 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 または NVMe/TCP 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（サーバ）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 または NVMe/TCP 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。
	無効	iSCSI Port または NVMe/TCP Port がリンクダウンしている状態です。iSCSI Port または NVMe/TCP 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 または NVMe/TCP Port の IPv6 アドレスが、接続ネットワーク内の他のホスト（サーバ）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 または NVMe/TCP 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 または NVMe/TCP Port の IPv6 アドレスには、iSCSI Port または NVMe/TCP 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 または NVMe/TCP 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（サーバ）、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 または NVMe/TCP 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 または NVMe/TCP 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。

6.10 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

ESM の状態監視で、ESM の停止を検出した場合、救済措置として、ESM 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。

ESM 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。



ポート情報

ポート情報について説明します。

- A.1 各管理ツールが利用するポート情報

A.1 各管理ツールが利用するポート情報

各管理ツールで利用するポートは次の通りです。

ストレージシステムのポートの設定は、「[D.5.2 ネットワーク拒否設定の変更](#)」を参照してください。

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

管理ツールの起動および終了

管理 GUI (VSP One Block Administrator、maintenance utility)、内蔵 CLI の起動および終了について説明します。

- B.1 管理ツールの起動方法
- B.2 管理ツールの終了方法

B.1 管理ツールの起動方法

管理ツールの起動方法を説明します。

B.1.1 VSP One Block Administrator の起動

VSP One Block Administrator の起動方法を説明します。

VSP One Block Administrator の表示内容や操作の詳細については、『VSP One Block Administrator ユーザガイド』を参照してください。

前提条件

- 要件を満たした管理ツールの操作端末を用意していること。
- 管理ツールの操作端末とストレージシステムの管理 LAN が通信可能な状態であること。
- 利用ブラウザが Microsoft Edge、Mozilla Firefox、または Google Chrome の場合、ポップアップブロックが無効であること。
- ファイアウォールを使用している場合は、以下のポートを開放済みであること。
 - HTTP を使用する場合、80 番ポート
 - HTTPS を使用する場合、443 番ポート



メモ

管理ツールの操作端末の要件については、『VSP One Block Administrator ユーザガイド』を参照してください。

操作手順

1. Web ブラウザを起動し、次の URL を指定します。

<プロトコル>://<管理ポートの IP アドレス>/

ログイン画面が表示されます。



メモ

- プロトコルには、ストレージシステムの設定で有効なプロトコルが指定できます。SSL/TLS 通信の場合は https、非 SSL/TLS 通信の場合は http です。
- Web ブラウザを何度起動しても起動に失敗する場合は、現在起動している Web ブラウザの画面をすべて閉じてから、Web ブラウザのキャッシュをクリアしてください。
Web ブラウザのキャッシュをクリアしても起動に失敗する場合は、「[B.1.3 AMC の IP アドレス指定による maintenance utility の起動](#)」を実行して、アラートを確認してください。
アラートを確認するには、Maintenance User Group（ビルトイングループ）に登録されているユーザで maintenance utility にログインしてください。

2. ログイン画面で、ストレージシステムのアカウントユーザ名および、パスワードを入力し、ログインします。

VSP One Block Administrator が起動されます。



メモ

- ・ ログインが失敗し、パスワードの変更が必要なメッセージが表示された場合は、maintenance utility でパスワードを変更してから再度 VSP One Block Administrator にログインしてください。
- ・ ログインに 3 回続けて失敗すると、アカウントが 60 秒間ロックされます。ロックアウトポリシーが設定されている場合、その設定に従った挙動となります。詳細は「[D.2.8 ユーザーアカウントポリシーの設定](#)」を参照してください。

B.1.2 VSP One Block Administrator 経由での maintenance utility の起動

VSP One Block Administrator 経由で maintenance utility を起動する方法について説明します。

maintenance utility の画面説明については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。

前提条件

- ・ VSP One Block Administrator が起動していること。

操作手順

1. ナビゲーションバーの  をクリックして [Maintenance Utility] を選択してください。
maintenance utility が起動されます。

B.1.3 AMC の IP アドレス指定による maintenance utility の起動

ブラウザのアドレスバーに AMC-0 もしくは AMC-1 の IP アドレスを入力することで、maintenance utility を起動する方法を説明します。

maintenance utility の画面説明については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。

前提条件

- ・ 要件を満たした管理ツールの操作端末を用意していること。
- ・ 管理ツールの操作端末とストレージシステムの管理 LAN が通信可能な状態であること。

操作手順

1. Web ブラウザを起動し、次の URL を指定します。

<プロトコル>://<AMC の管理ポートの IP アドレス> /MaintenanceUtility

ログイン画面が表示されます。



メモ

- ・ プロトコルには、ストレージシステムの設定で有効なプロトコルが指定できます。SSL/TLS 通信の場合は https、非 SSL/TLS 通信の場合は http です。
- ・ ストレージシステムへアクセスするための AMC の管理ポートの IP アドレスは、2 種類の IP アドレスがあります。
 - サービス IP アドレス
 - 固定 IP アドレス詳細は、「[1.4.4 ストレージシステムへアクセスするための IP アドレス](#)」を参照してください。

- Web ブラウザを何度起動しても起動に失敗する場合は、現在起動している Web ブラウザの画面をすべて閉じてから、Web ブラウザのキャッシュをクリアしてください。

2. ログイン画面で、ストレージシステムのアカウントユーザ名および、パスワードを入力し、ログインします。
maintenance utility が起動されます。

B.1.4 VSP One Block Administrator 経由での内蔵 CLI の起動

VSP One Block Administrator 経由で内蔵 CLI を起動し、RAID Manager にログインする方法について説明します。

前提条件

- VSP One Block Administrator が起動していること。

操作手順

1. ナビゲーションバーの  をクリックして [コマンドコンソール] を選択します。
内蔵 CLI 画面が起動します。
内蔵 CLI は、VSP One Block Administrator のログインユーザ、パスワードで内蔵 CLI にログインした状態で起動します。
2. 内蔵 CLI にログインできていることを確認します。
プロンプトに装置製番、AMC 番号が表示されることを確認してください。
例：装置製番：800001、AMC 番号：2 の場合

```
800001-2:$
```

B.1.5 SSH 接続による内蔵 CLI の起動

Windows の管理ツールの操作端末の内蔵 CLI で、コマンドプロンプトから ssh コマンドを使用して、RAID Manager にログインする方法を説明します。

SSH 接続の方法については、使用するオペレーションシステム、プログラムプロダクトによって異なります。詳細については、各ベンダが提供する情報を確認してください。管理ツールの操作端末で ESM の IP アドレスと接続ポートを入力して、ESM に SSH 接続します。接続ポートは、20522 を指定してください。20522 ポートはデフォルトでブロックされているため、maintenance utility からポートを開放してください（「[3.3.3 管理 LAN の暗号化通信を設定する](#)」参照）。

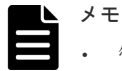
前提条件

- 要件を満たした管理ツールの操作端末を用意していること。
- 管理ツールの操作端末とストレージシステムの管理 LAN が通信可能な状態であること。
- 管理ツールの操作端末が SSH クライアントとして使用可能であること。

操作手順

1. コマンドプロンプトを起動します。
2. 管理 LAN の IP アドレスと、ポート番号 20522 を指定して ssh コマンドを実行します。
例：管理 LAN の IP アドレス：192.168.1.3、ログインするユーザ：maintenance の場合

```
>ssh 192.168.1.3 -p 20522 -l maintenance
```



メモ

- 管理ツールの操作端末で指定する ESM の IP アドレスとして、サービス IP アドレスを使用してログインしてください。または、AMC-0 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。AMC-0 に障害が発生してエラーとなる場合は、AMC-1 の管理ポートの IP アドレスを使用してください。
- 初めて接続する場合、以下のような警告が表示される場合があります。

```
RSA key fingerprint is SHA256:XXXXXXXXXXXXXXXXXXXXX
Are you sure you want to continue connecting (yes/no)?
```

yes を入力後、[Enter] キーを押して操作を継続してください。

- ストレージシステムユーザのパスワードを入力します。
- 内蔵 CLI にログインできたことを確認します。
プロンプトに装置製番、AMC 番号が表示されることを確認してください。
例：装置製番：800001、AMC 番号：2 の場合

```
800001-2:$
```

B.2 管理ツールの終了方法

管理ツールの終了方法を説明します。

B.2.1 VSP One Block Administrator の終了

VSP One Block Administrator の終了方法を説明します。

VSP One Block Administrator の表示内容については、『VSP One Block Administrator ユーザガイド』を参照してください。

前提条件

- VSP One Block Administrator にログインしていること。

操作手順

- ナビゲーションバーの  をクリックして [ログアウト] します。
ログアウトが完了し、ログイン画面が表示されます。
- ブラウザのタブを閉じます。

B.2.2 VSP One Block Administrator 経由で起動した maintenance utility の終了

VSP One Block Administrator 経由で起動した maintenance utility の終了方法を説明します。

maintenance utility の画面説明については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。

前提条件

- VSP One Block Administrator 経由で起動した maintenance utility にログインしていること。

操作手順

1. ヘッダエリアの [ログアウト] をクリックします。
ログアウト完了画面が表示されます。
2. ブラウザのタブを閉じます。
タブを閉じる際、サイトから移動を促すメッセージが表示される場合があります。
表示された場合は、移動する選択肢を選んでタブを閉じてください。



メモ

maintenance utility の画面を閉じる場合は、必ずログアウトを実施してください。
ログアウトをせずにウィンドウを閉じるとシステムロック状態が残る可能性があります。

B.2.3 AMC の IP アドレス指定で起動した maintenance utility の終了

ブラウザのアドレスバーに AMC の IP アドレスを入力して起動した maintenance utility を終了する方法を説明します。

maintenance utility の画面説明については、「[付録 C. maintenance utility の画面説明](#)」を参照してください。

前提条件

- AMC の IP アドレス指定で起動した maintenance utility にログインしていること。

操作手順

1. ヘッダエリアの [ログアウト] をクリックします。
ログアウトが完了し、ログイン画面が表示されます。
2. ブラウザのタブを閉じます。
タブを閉じる際、サイトから移動を促すメッセージが表示される場合があります。
表示された場合は、移動する選択肢を選んでタブを閉じてください。

B.2.4 VSP One Block Administrator 経由で起動した内蔵 CLI の終了

VSP One Block Administrator 経由で起動した内蔵 CLI からログインした RAID Manager を終了する方法を説明します。

前提条件

- 内蔵 CLI で RAID Manager にログインしていること。

操作手順

1. exit コマンドを実行します。
内蔵 CLI から切断されたメッセージが表示され、プロンプトの表示が変更されます。
例：

```
接続中...
接続されました。
Hitachi Virtual Storage Platform One Block 26

800068-2:$ exit
logout

切断されました。コマンドコンソールを閉じてください。
```

2. 内蔵 CLI の画面右上、 をクリックして画面を終了します。

B.2.5 内蔵 CLI の終了

Windows の管理ツールの操作端末の内蔵 CLI で、コマンドプロンプトから `ssh` コマンドを使用してログインした **RAID Manager** を終了する方法を説明します。

SSH 接続の方法については、使用するオペレーションシステム、プログラムプロダクトによって異なります。詳細については、各ベンダが提供する情報を確認してください。

前提条件

- 内蔵 CLI で **RAID Manager** にログインしていること。

操作手順

1. `exit` コマンドを実行します。

内蔵 CLI から切断されたメッセージが表示され、プロンプトの表示が変更されます。

例：

```
800001-2:$exit
logout
Connection to 192.168.1.3 closed.
>
```

2. 再度、`exit` コマンドを実行しコマンドプロンプトを終了します。



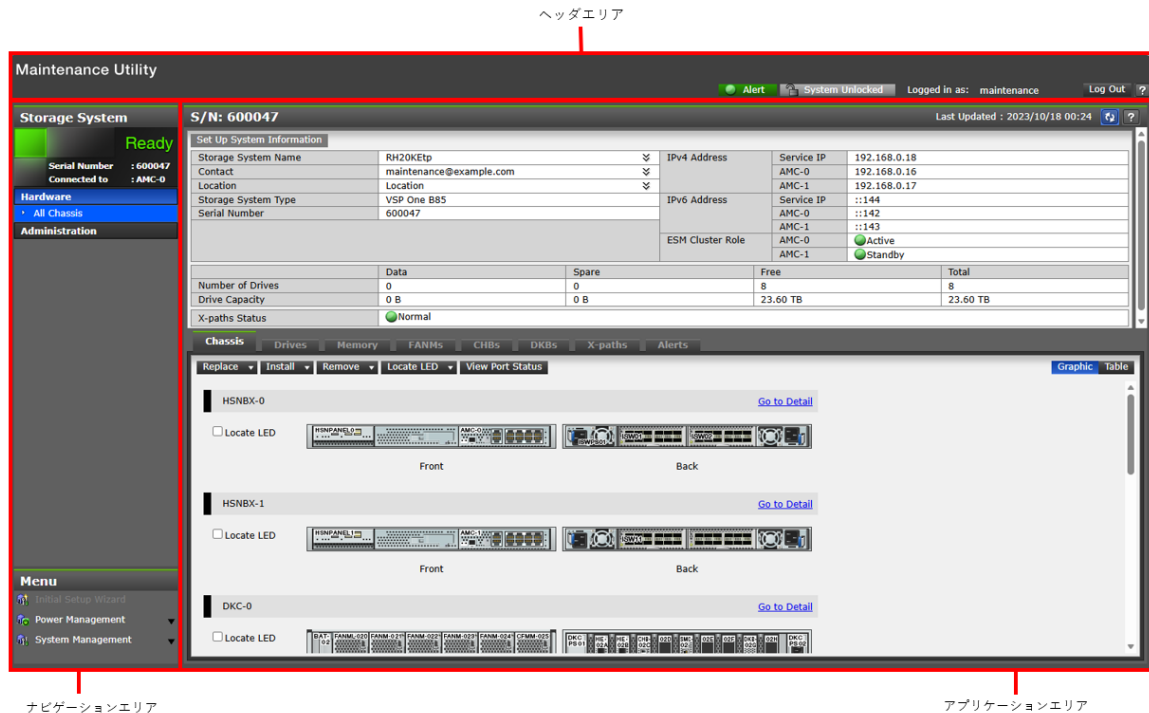
maintenance utility の画面説明

maintenance utility の画面構成について説明します。

- C.1 基本フレームワーク
- C.2 ヘッダエリア
- C.3 ナビゲーションエリア
- C.4 アプリケーションエリア

C.1 基本フレームワーク

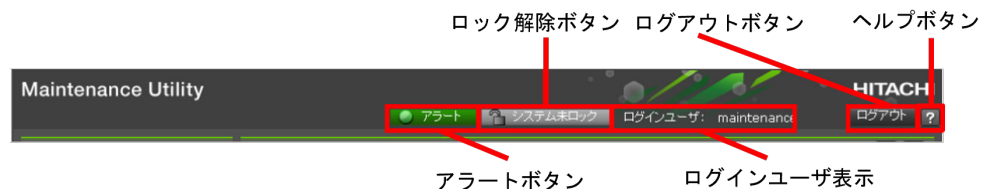
maintenance utility の画面は、「ヘッダエリア」、「ナビゲーションエリア」、「アプリケーションエリア」の3つのエリアで構成されています。



エリア	内容
ヘッダエリア	共通情報（アラート表示、システムロック表示、ユーザ名など）が常に表示されます。
ナビゲーションエリア	システム管理用メニューを表示します。
アプリケーションエリア	システムに関する情報表示や設定をします。

C.2 ヘッダエリア

メイン画面で共通となるヘッダエリアの構成について説明します。



画面項目	内容
アラートボタン	- クリックすると、[ストレージシステム] 画面の [アラート] タブを表示します。 - アラートボタンの表示イメージは、ナビゲーションエリアのストレージシステム状態（「C.3 ナビゲーションエリア」を参照）に従い、アラートボタンの表示イメージを切り替えます。

画面項目	内容
ロック解除ボタン	- クリックすると、[システムロック強制解除] 画面が起動します。※ - システムロック状態をロック中、未ロックで切り替えます。
ログインユーザ表示	ログインに使用しているユーザ名称を表示します。 ログイン名称が長く、ウィンドウの伸縮によって配置エリアに収まりきらない場合は、末尾に“...”を表示します。
ログアウトボタン	クリックするとログアウトを行います。
ヘルプボタン	全項目のヘルプを表示します。 また、ポップアップ画面上に同様のヘルプボタンがあります。 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。

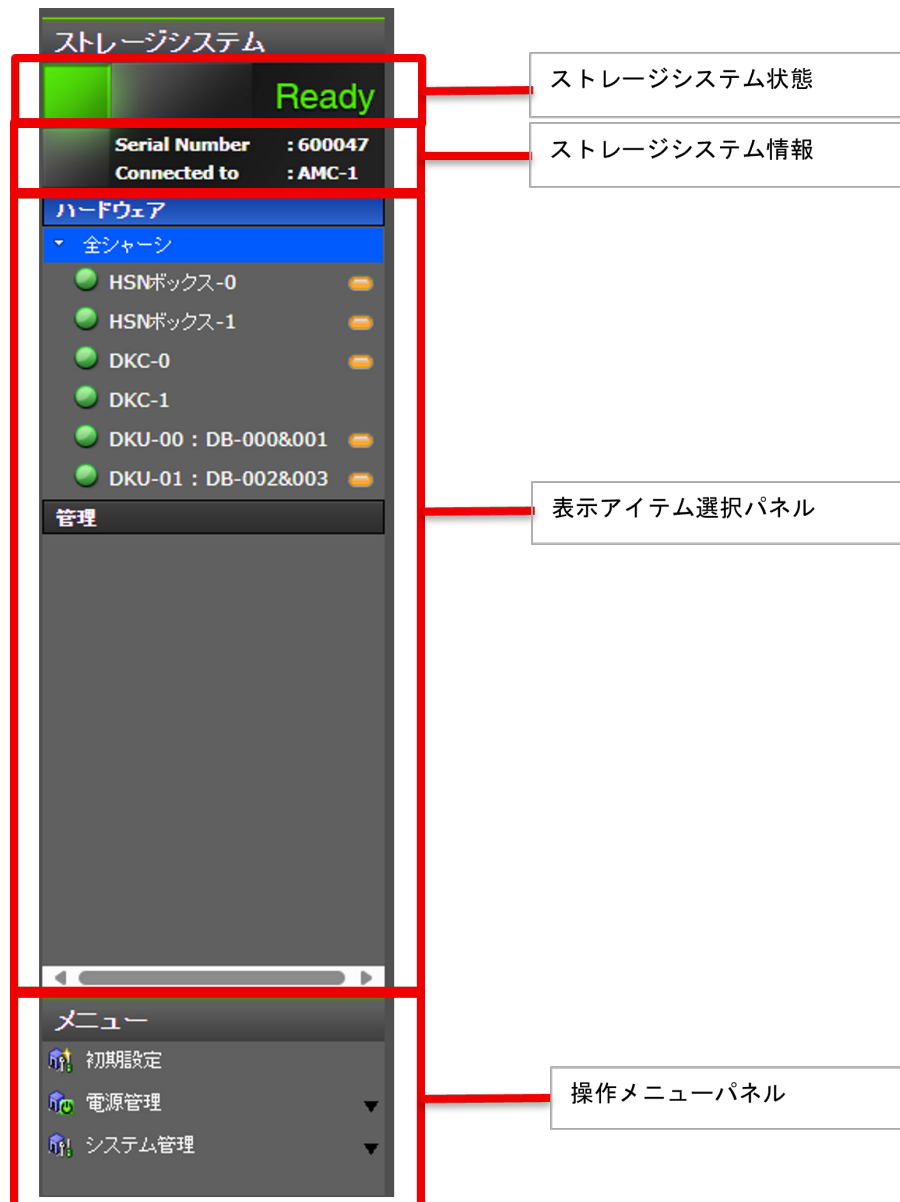
注※

システムロック強制解除は、他のユーザの設定変更がエラーなどにより正しく完了しなかったときに、強制的にシステムロックを解除する機能です。

システムロックの強制解除を実施するときは、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ことを確認してください。

C.3 ナビゲーションエリア

ナビゲーションエリアの構成について説明します。



画面項目	内容
ストレージシステム状態	ストレージシステム状態イメージを表示します（次の表「ストレージシステム状態の詳細」を参照）。
ストレージシステム情報	1行目に装置製番を表示します。 2行目に現在接続中のAMC番号を表示します。 - このエリアをクリックすると、アプリケーションエリアに装置情報（メイン画面）を表示します。
表示アイテム選択パネル	使用するメニューを「ハードウェア」と「管理」に分けて表示します。メニューを選択するとアプリケーションエリアに内容が表示されます。

画面項目	内容
	「ハードウェア」メニューでは、ハードウェア名称文字列の左側のアイコンは、そのハードウェアの状態を示します。
操作メニューパネル	システム全体に関する操作メニューを配置します。

ストレージシステム状態の詳細は以下となります。

部品ごとの状態については、「[6.6 maintenance utility の FRU \(Field Replacement Unit\) に関するアラートの確認手順](#)」を参照してください。

状態	条件	ナビゲーションエリア	未コンプライート SIM 有無	アラートボタンのアイコンと色
Failed	システムダウンが発生している可能性のある状態		なし	/ 赤
			あり	/ 赤
Warning	部品状態に Blocked/Warning がある状態		なし	/ オレンジ
			あり	/ オレンジ
Ready	部品状態すべて正常		なし	/ 緑
			あり	/ 緑
Power-on in progress	PS ON 処理中		—	/ グレー
Power-off in progress	PS OFF 処理中		—	/ グレー
Unknown	その他 (PS ON する前の状態など)		—	/ グレー

C.4 アプリケーションエリア

メイン画面で共通となるアプリケーションエリアの構成について説明します。



画面項目	内容
装置製番表示	装置製番を表示します。
最終更新日時表示	画面表示情報の最終更新日時を表示します（YYYY/MM/DD hh:mm）。
更新ボタン	表示情報を更新します。
ヘルプボタン	操作中のヘルプを表示します。 また、ポップアップ画面上に同様のヘルプボタンがあります。 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。



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。

- ☐ D.1 ファームウェア
- ☐ D.2 ユーザ管理
- ☐ D.3 アラート通知
- ☐ D.4 ライセンス
- ☐ D.5 ネットワーク設定
- ☐ D.6 日時設定
- ☐ D.7 監査ログ
- ☐ D.8 外部認証
- ☐ D.9 初期設定
- ☐ D.10 電源管理
- ☐ D.11 システム管理
- ☐ D.12 アラートの表示
- ☐ D.13 SIM のコンプリート

D.1 ファームウェア

D.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。

D.1.2 ファームウェアの更新

ファームウェアの更新は、保守員が実施します。ファームウェアをバージョンアップしたい場合は、弊社営業にお問い合わせください。



メモ

ファームウェアの更新後に VSP One Block Administrator をご使用する場合は、VSP One Block Administrator 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。

D.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、[「1.4.5 各ツールのログイン方法」](#)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、管理ツールの操作端末から IP アドレスを直接指定して起動するか、または VSP One Block Administrator のメニューから起動してください。

D.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。

D.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

ロール	操作できる項目
ストレージ管理者（システムリソース管理）	- MP ユニットの設定 - リソース排他の強制解除 - LUN セキュリティの設定 - リモートコピーの操作全般 - ポート属性の設定
ストレージ管理者（プロビジョニング）	- キャッシュの設定 - LDEV、プール、仮想ボリュームの設定 - LDEV のフォーマット - 外部ボリュームの設定 - Dynamic Provisioning に関する設定 - ホストグループ、パス、WWN の設定 - NVM サブシステム、Namespace、パス、ホスト NQN の設定 - Volume Migration の設定（RAID Manager を使用した場合の Volume Migration ペアの削除を除く） - LDEV のアクセス属性の設定 - LUN セキュリティの設定 - Namespace セキュリティの設定 - global-active device で使用する Quorum ディスクの作成、削除 - global-active device ペアの作成および削除 - Compatible PAV のエイリアスボリューム設定
ストレージ管理者（ローカルバックアップ管理）	- ローカルコピーのペア操作 - ローカルコピー用の環境設定 - Volume Migration のペア解除
ストレージ管理者（リモートバックアップ管理）	- リモートコピーの操作全般 - global-active device ペアの操作（作成および削除を除く）
ストレージ管理者（パフォーマンス管理）	エクスポートツール 2 の操作
セキュリティ管理者（参照）	- ユーザアカウントおよび暗号設定に関する情報の参照 - maintenance utility による外部認証の情報参照 - セッションタイムアウト時間の参照 - コモンクライテリア認証設定の参照 - TLS セキュリティ設定の参照
セキュリティ管理者（参照・編集）	- ユーザアカウントの設定 - ユーザアカウントポリシーの設定 - maintenance utility による外部認証の設定 - 暗号鍵の生成と削除 - 暗号の設定 - 暗号鍵のバックアップ、リストア - 外部サーバへの接続設定 - SSL/TLS 通信で使用する証明書の設定 - コモンクライテリア認証の設定

ロール	操作できる項目
	- リソースグループの設定 - 仮想管理設定の編集 - CSR 作成および自己署名証明書作成 - global-active device の予約属性の設定 - セッションタイムアウト時間の編集 - TLS セキュリティ設定の変更
監査ログ管理者（参照）	監査ログに関する画面の参照、および監査ログのダウンロード
監査ログ管理者（参照・編集）	監査ログに関する設定、および監査ログのダウンロード
保守（ベンダ専用）	ベンダ保守に関する操作（通常日立の保守員が実施する操作です。）
保守（ユーザ）	- 装置状態の参照 - 簡易の保守操作 - SIM のコンプリート

D.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。

D.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。

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）	全リソースグループ

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

D.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

管理ツール	ビルトイングループ
	Maintenance User
VSP One Block Administrator	Administrator
	Maintenance User
内蔵 CLI または RAID Manager	Administrator
エクスポートツール 2	Administrator
REST API	Administrator
	Maintenance User

D.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。

(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)
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)
USP モード編集	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)
証明書ファイル更新	セキュリティ管理者 (参照・編集)
CSR 作成および自己署名証明書作成	セキュリティ管理者 (参照・編集)
コモンクライテリア認証設定	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)
ESM フェールオーバー	ストレージ管理者 (初期設定) または保守 (ユーザ)
ESM リポート	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)

操作項目	必要なロール
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）
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）
セッションタイムアウト時間編集	セキュリティ管理者（参照・編集）
SIM のコンプリート	保守（ユーザ）

(2) VSP One Block Administrator の操作に必要なロール

VSP One Block Administrator の操作に必要なロールは、『VSP One Block Administrator ユーザガイド』の各操作の説明を参照してください。

VSP One Block Administrator のユーザには、すべてのリソースグループが割り当てられている必要があります。割り当てられていないリソースがある場合、この管理ツールは使用できません。

リソースグループが作成された環境で使用する場合、ユーザが属するユーザグループにすべてのリソースグループを割り当ててください。

(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）

(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）

(5) エクスポートツール 2 の操作に必要なロール

- ・ サンプル間隔確認機能、蓄積データ期間確認機能、および性能メトリクスエクスポート機能を利用するために必要なロール：ストレージ管理者（パフォーマンス管理）または保守（ベンダ専用）
- ・ サンプル間隔設定機能を利用するために必要なロール：ストレージ管理者（パフォーマンス管理）

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

注※1

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

注※2

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

注※3

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

パスワードの制限

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

管理ツール	制限※1	
	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「[\(2\) ユーザアカウントのパスワードポリシー設定](#)」を参照してください。

注※2

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

D.2.8 ユーザアカウントポリシーの設定

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

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

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

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

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

パスワードの有効期限を設定する場合の注意点を示します。

- **maintenance utility** は、パスワードの期限が切れる 30 日前、および 14 日前から当日までの間、パスワードの期限切れを警告する SIM (SIM リファレンスコード「7c21xx」) 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（「[D.2.10 パスワードの変更](#)」を参照）またはパスワードの有効期間を無期限に変更（「[\(5\) ユーザ個別のパスワードポリシーの適用](#)」を参照）してください。

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

(1) ユーザアカウントポリシーを利用する場合のユーザ管理

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

ユーザアカウントポリシー利用時の、ユーザ管理操作と管理ツールの指定

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

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

注※1

管理ツールの操作端末から IP アドレスを直接指定して起動してください。詳細は「[1.4.5 各ツールのログイン方法](#)」を参照してください。

注※2

ユーザアカウントポリシーの設定状態により、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「[\(2\) ユーザアカウントのパスワードポリシー設定](#)」および「[\(5\) ユーザ個別のパスワードポリシーの適用](#)」を参照してください。

ユーザ管理操作に指定とは異なる管理ツールを使用した場合の注意事項

ユーザ管理操作	VSP One Block Administrator を利用する構成で、 maintenance utility 以外から操作した場合
初回ログインのパスワード変更	[初回ログイン時にパスワード変更を要求する]を設定済みのユーザの場合は、maintenance utility を除く全インターフェースからログインができなくなります。VSP One Block Administrator にログインを試みた際は、メッセージとともに maintenance utility のログイン画面へのリンクが表示されます。

(2) ユーザアカウントのパスワードポリシー設定

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



注意

- パスワード有効期限が切れたユーザはログインができなくなります。
- パスワードの有効期限が切れないようにするには、パスワードの有効期限が切れる日の 23 時 59 分までに、パスワードを変更する必要があります。パスワードの有効期限が切れた場合は、セキュリティ管理者がそのユーザアカウントを有効にしてパスワードをリセットする必要があります。詳細は「[\(9\) アカウントの有効化](#)」を参照してください。
- セキュリティ管理者（参照・編集）ロールを持つ最後のユーザは、パスワード有効期限が切れた場合でも継続してログインできます。
- セキュリティ管理者（参照・編集）ロールを持つ最後のユーザが複数で、同時にパスワード有効期限が切れた場合でも、この複数のユーザは継続してログインできます。
- セキュリティ管理者（参照・編集）ロールを持つユーザの場合、パスワード変更禁止期間内でも、他のユーザについて、パスワード変更を実施できます。
- パスワード文字数は使用する管理ツールによって制限があります。複数の管理ツールを使用する場合は、どの管理ツールにも適用可能な範囲でパスワードポリシーを設定してください。各管理ツールのパスワード文字数制限については、「[D.2.7 ユーザ名とパスワードの文字数と使用可能文字](#)」を参照してください。
- ユーザアカウントポリシーと、各ユーザアカウントに対して、異なるパスワードの有効日数を設定できます。なお、ユーザアカウントポリシーに設定する有効日数を変更すると、変更された日数分が、各ユーザアカウントのパスワードの有効日数に反映されます。例えば、あるユーザアカウントのパスワードの有効日数が 50 日（250 日を設定してから 200 日が経過）の場合、ユーザアカウントポリシーの有効日数を 350 日から、250 日に変更すると（有効日数を 100 日少なくなるように変更）、ユーザアカウントの有効日数も 100 日少なくなるように変更されるため、ユーザアカウントのパスワードの有効期限が、すでに 50 日超過しているものとして扱われます。これにより、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全体でのパスワードポリシー設定後、既存のユーザにはパスワードポリシーは適用されていません。既存のユーザにパスワードポリシーを適用するためには、パスワードポリシーの設定後に、対象ユーザのパスワードを変更する必要があります。ユーザ個別でのパスワードポリシーの適用方法は、「[\(5\) ユーザ個別のパスワードポリシーの適用](#)」を参照してください。
- パスワードポリシー変更前のパスワードが、変更後のパスワードポリシーに従わなくなった場合でも、対象ユーザのパスワードを変更するまでは、変更前のパスワードを使用できます。

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

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

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

〔Policy〕 タブ
パスワードポリシー

項目		説明	デフォルト値
最小文字数	数字 (0-9)	パスワードの最小文字数 (数字 (0-9)) を設定します。 ・ [0-256] : ユーザ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。	3

項目	説明	デフォルト値
	[1-999] : ログイン試行回数 [空白] : 無制限	
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

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

(3) メールサーバの設定

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

前提条件

- 必要なロール : セキュリティ管理者 (参照・編集) ロール

操作手順

- maintenance utility にログインします。
- [管理] - [ユーザアカウントポリシー] を選択します。
- [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。
- [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。
- 各項目を入力します。

[Email] タブ

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

項目		説明
	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)

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

(4) テストメールの送信

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

前提条件

- ユーザアカウントポリシーで、[テスト送信メールアドレス] が指定されていること。
- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

- maintenance utility にログインします。
- [管理] - [ユーザアカウントポリシー] を選択します。
- [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。
- [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。
- 完了メッセージが表示されます。[OK] をクリックします。
- 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

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

(5) ユーザ個別のパスワードポリシーの適用

パスワードポリシーを、ユーザ個別に適用するかどうかを設定します。



注意

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

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。
2. [管理] - [ユーザ管理] を選択します。
3. [ユーザグループ] 画面で、対象ユーザが存在する [ユーザグループ] を選択します。
4. [ユーザ] タブのユーザー一覧から、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。

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

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

(6) ユーザ個別のメールアドレスの設定

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

本項目の設定と「[\(3\) メールサーバの設定](#)」により、「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 (7c2000) が送信されます。SIM が送信された場合は、次の項目を確認して不具合を訂正してください。
 - 「[\(3\) メールサーバの設定](#)」で設定した内容
 - 「[6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法](#)」に示す障害内容と対処方法を訂正完了後、「[\(4\) テストメールの送信](#)」を実施し、メールが送信できることを確認してください。

前提条件

- ・ 必要なロール: セキュリティ管理者 (参照・編集) ロール

操作手順

1. maintenance utility にログインします。
2. [管理] - [ユーザ管理] を選択します。
3. [ユーザグループ] 画面で、対象ユーザが存在するユーザグループを選択します。
4. [ユーザ] タブのユーザー一覧から、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 (! # \$ % & ` + - * / ' ^ { } _ . @ ~ = ?)

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

(7) ユーザアカウント状態の確認

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

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

- maintenance utility にログインします。
- [管理] - [ユーザ管理] を選択します。
- [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。
- [ユーザ] タブのユーザー一覧で、対象ユーザの [アカウント状態] 列を確認します。
 - [Locked] が表示されている場合は、対象ユーザのアカウントはアカウントロックされている状態です。
 - [Disabled] が表示されている場合、対象ユーザのアカウントは無効化された状態です。
 - [Enabled] が表示されている場合、対象ユーザのアカウントは有効な状態です。

(8) アカウントロックの解除

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

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

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

- maintenance utility にログインします。
- [管理] - [ユーザ管理] を選択します。
- [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。
- [ユーザ] タブのユーザー一覧から、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。
- [編集] をクリックします。
- [ユーザ編集] 画面で、[新しいパスワード] と [パスワード再入力] に新規のパスワードを入力します。



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

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

(9) アカウントの有効化

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

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。
2. [管理] - [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] タブのユーザー一覧で、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。

D.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 512 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、「[D.2.8 ユーザアカウントポリシーの設定](#)」を参照ください。



メモ

ユーザアカウント作成後は AMC 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（「[D.2.13 ユーザアカウントのバックアップ](#)」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（「[D.2.14 ユーザアカウントのリストア](#)」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。

項目	説明
ユーザ名	作成するユーザ名を設定します。 • 文字数：1～256 文字 • 使用可能文字：半角英数字と記号（＃\$&'*. / = ? @ ^ _ ` { } ~ !） ユーザ名の文字数や使用可能文字はストレージシステムの管理アプリケーションにより異なります。すべての管理アプリケーションを使用するユーザを作成する場合は、次の条件で設定してください。 • 文字数：1～63 文字 • 使用可能文字：半角英数字と記号（-.@_）
アカウント状態	アカウント状態を選択します。 • [有効]：アカウントを有効にする。 • [無効]：アカウントを無効にする。
認証	認証方法を選択します。 • [Local]：認証サーバを使用せず、ストレージシステムの管理アプリケーション専用のパスワードを使用します。 • [External]：認証サーバを使用します。
パスワード	パスワードを設定します。 • 文字数：6～256 文字 • 使用可能文字：半角英数字とすべての記号 パスワードの文字数や使用可能文字はストレージシステムの管理アプリケーションにより異なります。すべての管理アプリケーションを使用するユーザを作成する場合は、次の条件で設定してください。 • パスワード：6～63 文字 • 使用可能文字：半角英数字と記号（-.,: @ _）
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する • [いいえ]：初回ログイン時にパスワード変更を要求しない
パスワード有効期間（日）	パスワード有効期間（日）（ユーザ単位）を設定します。 • [システムポリシーに従う]：ユーザアカウントポリシー設定に従う • [無制限]：設定しない（無期限）
Email アドレス	パスワードの有効期限切れ間近、または有効期限切れの通知先 Email 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（"(),;:<>[¥]）とスペースを除く）
ユーザグループ	ユーザを所属させるユーザグループを選択します。



メモ

パスワードに設定可能な文字列は、パスワードポリシーに従う必要があります。詳細は「[D.2.8 ユーザアカウントポリシーの設定](#)」を参照してください。

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

D.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

操作手順

1. maintenance utility にログインします。
2. [管理] - [ユーザ管理] を選択します。
3. [ユーザグループ] の一覧から、パスワードを変更したいユーザが所属するユーザグループをクリックします。
4. [ユーザ] タブのユーザー一覧から、パスワードを変更したいユーザアカウントを選択します。
(ユーザアカウントの左横にあるチェックボックスにチェックマークを入れます。)
5. [編集] を選択します。
6. ユーザ編集画面が表示されます。各項目を入力します。

項目	説明
ユーザ名	操作対象のユーザ名が表示されます。
アカウント状態	アカウント状態を選択します。 [有効]: アカウントを有効にする。 [無効]: アカウントを無効にする。
認証	認証方法を選択します。 [Local]: 認証サーバを使用せず、ストレージシステムの管理アプリケーション専用のパスワードを使用します。 [External]: 認証サーバを使用します。
新しいパスワード	変更後のパスワードを設定します。 文字数: 6~256 文字 使用可能文字: 半角英数字とすべての記号 パスワードの文字数や使用可能文字はストレージシステムの管理アプリケーションにより異なります。すべての管理アプリケーションを使用するユーザを作成する場合は、次の条件で設定してください。 パスワード: 6~63 文字 使用可能文字: 半角英数字と記号 (-, . : @ _)
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する [いいえ]: 初回ログイン時にパスワード変更を要求しない
パスワード有効期間 (日)	パスワード有効期間 (日) (ユーザ単位) を設定します。 [システムポリシーに従う]: ユーザアカウントポリシー設定に従う [無制限]: 設定しないユーザ単位 (無期限)
Email アドレス	パスワードの有効期限切れ間近、または有効期限切れの通知先 Email 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 (" () , ; < > [¥] とスペースを除く)
ユーザグループ	ユーザアカウントが所属しているユーザグループが表示されます。 ユーザアカウントの所属先ユーザグループを追加する場合は、所属先のユーザグループを選択します。

項目	説明
	ユーザアカウントをユーザグループから削除する場合は、ユーザグループの選択状態を解除します。



メモ

パスワードに設定可能な文字列は、パスワードポリシーに従う必要があります。詳細は「[D.2.8 ユーザアカウントポリシーの設定](#)」を参照してください。

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

D.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

- maintenance utility にログインします。
- [管理] - [ユーザ管理] を選択します。
- [ユーザ] タブのユーザー一覧から、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。）
- [編集] を選択します。
- 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。
- 設定内容を確認し [完了] をクリックします。
- 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。
- 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。

D.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 を含む管理ツールを利用できます。

操作手順

- maintenance utility にログインします。
- [管理] - [ユーザ管理] を選択します。
- [ユーザ] タブのユーザー一覧から、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。）
- [削除] を選択します。
- 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。
- 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。

D.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。

D.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。

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。

D.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 AMC に実装されています。各 AMC 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 AMC 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（「[D.3.7 SNMP エンジン ID を確認する](#)」を参照）。



メモ

障害情報は各 AMC の管理ポートの固定 IP アドレスから管理 LAN を介して通知されます。AMC が障害により動作を停止している場合は正常な AMC の管理ポートの固定 IP アドレスから通知されます。このため各 AMC の管理ポートは必ず管理 LAN に接続してください。一方の AMC 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。

D.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、「[J.1 障害通知メールの内容](#)」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。

[Email] タブ

項目	説明
Email 通知	障害情報をメールで通知するかどうかを選択します。 ・ [有効]：アラート（SIM）をメールで通知する。 ・ [無効]：アラート（SIM）をメールで通知しない。
メールアドレス（To）	障害情報を送信する属性とメールアドレスが [登録アドレス] テーブルに表示されます。 [Email 通知] で [有効] を選択した場合、必ず設定してください。 ・ [追加]： [メールアドレス追加] 画面が表示されます。 アラート通知先として追加するメールアドレスを設定し、送信種類（[To]、[Cc]、[Bcc]）を選択します。 メールアドレスには、最大で半角 255 文字の名称を入力できます。 使用可能文字：半角英数字と記号（"（）,;:<>[¥] とスペースを除く） ・ [削除]：

項目	説明
	削除したいメールアドレスを選択（複数可）してクリックすると、[登録アドレス] テーブルから削除されます。
メールアドレス（From）	障害情報を通知するメールの送信元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（"（）,;:<>[¥]とスペースを除く） [Email 通知] で [有効] を選択した場合、必ず設定してください。
メールアドレス（Reply To）	メールの返信先アドレスを設定します。このアドレスを設定すると、メール受信者からの返信がこのアドレスに送信されます。このアドレスを省略すると、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）
通知する付加情報	メールの本文冒頭に表示される内容を入力します。 使用可能文字：半角英数字、スペース、記号（!"#\$%&'()*+,-./:;<=>@[¥]^_`{ }~） 最大で半角 511 文字まで入力できます。空白、改行も入力できます。改行は 2 文字としてカウントされます。
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。すべて 0 の IP アドレスは設定できません。 [Identifier] : ホスト名を指定するには [Identifier] を選択し、最大で半角 255 文字の名称を設定できます。 使用可能文字：半角英数字と記号（"¥;:, *?<> / #& +=[]'{}^とスペースを除く） [IPv4] : IPv4 アドレスを使用する場合に選択します。 [IPv6] : IPv6 アドレスを使用する場合に選択します。IPv6 アドレスの省略形も設定できます。 [Email 通知] で [有効] を選択した場合、必ず設定してください。
メールサーバ設定－SMTP 認証	SMTP 認証をするかどうかを選択します。 [有効] : SMTP 認証をする。 [無効] : SMTP 認証をしない。 [有効] を選択した場合は、[アカウント] と [パスワード] を必ず設定してください。 使用可能文字：半角英数字と記号（"¥;:, *?<> / #& +=[]'{}^とスペースを除く）

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

D.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。
 - ・ 「[D.3.1 メール通知の設定](#)」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。
 - ・ 「[D.3.1 メール通知の設定](#)」で設定した内容
 - ・ 「[6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法](#)」に示す障害内容と対処方法



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
「[D.3.1 メール通知の設定](#)」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
SNMP トラップで報告される障害内容です。
- ・ 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、『障害通知ガイド』を参照してください。

D.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。

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、「[J.2 Syslog メッセージの内容](#)」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

- Syslog 転送プロトコルに TLS/RFC5424 を使う場合は、Syslog サーバのルート証明書の証明書ファイルやクライアントの証明書ファイルをストレージシステムに設定する必要があります。証明書の要件については、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。
- ストレージシステムへアップロードするクライアントの証明書ファイルは、PKCS#12 形式のファイルである必要があります。PKCS#12 形式のクライアント証明書ファイル作成方法については「[G.10 SSL/TLS 証明書を PKCS#12 形式に変換](#)」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:: ~ FDFE: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::xxxx:xxxx:xxxx:xxxx]` (xxxx は任意の数値)
 - グローバルユニキャストアドレス : `[2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]` (xxxx は任意の数値)
 - グローバルユニキャストアドレス : `[2002:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]` (xxxx は任意の数値)

操作手順

- maintenance utility にログインします。
- [管理] — [アラート通知] を選択します。
- [設定] を選択します。
- 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。
- 各項目を入力します。

[Syslog] タブ

項目	説明
転送プロトコル	Syslog を転送するプロトコルを選択します。 [TLS/RFC5424] [UDP/RFC3164]
プライマリサーバ	Syslog サーバを使用するかどうかを選択します。 [有効] : Syslog サーバにアラート (SIM) を Syslog で通知する。 [無効] : Syslog サーバにアラート (SIM) を Syslog で通知しない。

項目	説明
プライマリサーバ - Syslog サーバ	Syslog サーバとして設定したいサーバのホスト名/IP アドレスを設定します。すべて 0 の IP アドレスは設定できません。 [Identifier] : ホスト名を使用する場合に選択します。 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) [IPv4] : IPv4 アドレスを使用する場合に選択します。 [IPv6] : IPv6 アドレスを使用する場合に選択します。IPv6 アドレスの省略形も設定できます。 [プライマリサーバ] で [有効] を選択したときは必ず設定してください。
プライマリサーバ - ポート 番号	Syslog サーバで使用するポート番号を設定します。 [プライマリサーバ] で [有効] を選択したときは必ず設定してください。
プライマリサーバ - クライ アント証明書ファイル名	証明書ファイルを設定します。[ファイルの選択] をクリックし、証明書ファイルを設定してください。 [転送プロトコル] で [TLS/RFC5424] を選択し、[プライマリサーバ] で [有効] を選択したときは必ず設定します。 設定を適用した後、再度設定を適用する場合、証明書が未設定 (空白) であれば、前回更新した証明書が使用されます。
プライマリサーバ - パスワ ード	クライアント証明書のパスワードを設定します。最大で半角 128 文字のパスワードを設定できます。 使用可能文字 : 半角英数字と記号 (! # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~)
プライマリサーバ - ルート 証明書ファイル名	証明書ファイルを設定します。[ファイルの選択] をクリックし、証明書ファイルを設定してください。 [転送プロトコル] で [Syslog プロトコル TLS/RFC5424] を選択し、[プライマリサーバ] で [有効] を選択したときは必ず設定します。 設定を適用した後、再度設定を適用する場合、証明書が未設定 (空白) であれば、前回更新した証明書が使用されます。
セカンダリサーバ	Syslog サーバの代替サーバを使用するかどうかを選択します。 [有効] : Syslog サーバの代替サーバにアラート (SIM) を Syslog で通知する。 [無効] : Syslog サーバの代替サーバにアラート (SIM) を Syslog で通知しない。
セカンダリサーバ - Syslog サーバ	Syslog サーバの代替サーバとして設定したいサーバのホスト名/IP アドレスを設定します。すべて 0 の IP アドレスは設定できません。 [Identifier] : ホスト名を使用する場合に選択します。 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) [IPv4] : IPv4 アドレスを使用する場合に選択します。 [IPv6] : IPv6 アドレスを使用する場合に選択します。IPv6 アドレスの省略形も設定できます。 [セカンダリサーバ] で [有効] を選択したときは必ず設定してください。

項目	説明
セカンダリサーバー ポート番号	Syslog サーバの代替サーバで使用するポート番号を設定します。 [セカンダリサーバ] で [有効] を選択したときは必ず設定してください。
セカンダリサーバー クライアント証明書ファイル名	証明書ファイルを指定します。[ファイルの選択] をクリックし、証明書ファイルを設定してください。 [転送プロトコル] で [TLS/RFC5424] を選択し、[セカンダリサーバ] で [有効] を選択したときは必ず設定します。 設定を適用した後、再度設定を適用する場合、証明書が未設定（空白）であれば、前回更新した証明書が使用されます。
セカンダリサーバー パスワード	クライアント証明書のパスワードを設定します。最大で半角 128 文字のパスワードを設定できます。 使用可能文字：半角英数字と記号（!#\$%&'()*+,-./:;<=>?@[¥]^_`{ }~）
セカンダリサーバー ルート証明書ファイル名	証明書ファイルを指定します。[ファイルの選択] をクリックし、証明書ファイルを設定してください。 [転送プロトコル] で [TLS/RFC5424] を選択し、[セカンダリサーバ] で [有効] を選択したときは必ず設定します。 設定を適用した後、再度設定を適用する場合、証明書が未設定（空白）であれば、前回更新した証明書が使用されます。
ロケーション識別名	Syslog サーバにアラート（SIM）を転送するストレージシステムを識別するために、任意の名称を設定します。最大で半角 32 文字の名称を設定できます。 使用可能文字：半角英数字と記号（!#\$%&'()*+,-./:;<=>?@[¥]^_`{ }~） [プライマリサーバ] または [セカンダリサーバ] が [有効] のときは必ず設定してください。
リトライ	リトライ設定内容が表示されます。 [有効]：Syslog サーバとの通信に失敗した場合にリトライする。 [無効]：Syslog サーバとの通信に失敗した場合にリトライしない。 [転送プロトコル] で [TLS/RFC5424] を選択したときのみ設定できます。
リトライ間隔	Syslog サーバとの通信に失敗した場合のリトライ間隔を、1～60 秒の間で設定します。 [リトライ] で [有効] を選択したときは必ず設定してください。

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

D.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

- 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 : 7FFFFFFF

This is Test Report.

7FFFFFFF 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、『障害通知ガイド』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。

- ・ 「[D.3.3 アラート通知を蓄積するための Syslog の設定](#)」で設定した内容
- ・ 「[6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法](#)」に示す障害内容と対処方法

D.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、「[J.3 SNMP メッセージの内容](#)」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、『障害通知ガイド』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。
入力内容は、『障害通知ガイド』の SNMP の設定を参照してください。
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『障害通知ガイド』を参照）。

D.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 : 7FFFFFFF

This is a test code.

7FFFFFFF 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、『障害通知ガイド』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。

- 「[D.3.5 SNMP エージェントの設定](#)」で設定した内容
- 「[6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法](#)」に示す障害内容と対処方法

D.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 AMC に実装されています。SNMP v3 プロトコルを使用する場合は、各 AMC 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 AMC 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 AMC の IP アドレスを指定して、maintenance utility を起動します。

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

2. [管理] 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 AMC の SNMP エンジン ID を確認します。



メモ

SNMP を一度も有効にしていない場合は、SNMP エンジン ID が「0x00000000000000000000000000000000」になっていますので、SNMP を有効にして設定した後に再確認してください。

D.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。

D.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
Temporary キーでインストール	Installed	Temporary	—	残日数
Emergency キーでインストール	Installed	Emergency	—	残日数
Permanent キーまたは Term キーでインストール 容量不足の状態	Not Enough License	Permanent キーまたは Term	許可容量と使用量	—
Permanent キーまたは Term キーでインストール LDEV を追加したためライセンス容量不足の状態	Grace Period	Permanent キーまたは Term	許可容量と使用量	残日数
Temporary キーでインストール 有効期限切れの状態	Expired	Temporary	—	残日数
Term キーまたは Emergency 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

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）
Temporary キーでインストール後、Permanent キーでインストール 容量不足の状態	Installed	Temporary	許可容量と使用量	残日数
Permanent キーまたは Term キーでインストール後に Emergency キーでインストール	Installed	Emergency	許可容量と使用量	残日数

D.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。

D.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。)

D.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、[キータイプ] が [Term] かつ [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。)

D.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。)

D.4.6 ライセンスの状態を更新

プログラムプロダクトのライセンスの状態を更新します。

ライセンス容量が足りない状態 ([Not Enough License]) や、ライセンス容量を増やすまでの猶予期間にある状態 ([Grace Period]) に対処しても、ライセンスの状態が変わらない場合があります。

この場合は、プログラムプロダクトのライセンスの状態を更新してください。

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。



メモ

特定のライセンスを選択しても、すべてのライセンスが更新の対象となります。

3. [ライセンス状態更新] をクリックします。
4. 確認メッセージが表示されます。[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。

D.5 ネットワーク設定

D.5.1 ネットワーク設定の変更



注意

- 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
- プロトコルは、IPv4 のみ、または IPv4/IPv6 を組み合わせて指定できますが、IPv6 のみの指定はできません。
- 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。
- プロトコルを IPv4/IPv6 両方を設定した場合、DNS サーバは 3 個までしか設定できません。
- 設定する IP アドレスやドメイン名が「HSTS プリロードリスト」に含まれないことを、事前に確認してください。「HSTS プリロードリスト」に含まれる IP アドレスやドメイン名を設定する場合、検証可能な証明書を、Web サーバ証明書として登録する必要があります。
Google Chrome の場合、アドレスバーに [chrome://net-internals/#hsts] と入力すると、HSTS に関するページから「HSTS プリロードリスト」を確認できます。例えば、IP アドレス 1.0.0.1 は、static_sts_domain: 1.0.0.1 と表示され、「HSTS プリロードリスト」に登録されていることがわかります。
- 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:: ~ FDFE: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::xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)
 - ・ グローバルユニキャストアドレス：[2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)
 - ・ グローバルユニキャストアドレス：[2002:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)
- ・ 内部ネットワークの変更を行うと AMC-0 と AMC-1 の ESM の状態 (Active または Standby) が入れ替わる場合があります。この操作は、サービス IP アドレスを使用しているすべての接続を一時的に切断します。サービス IP アドレスを利用している人がいないか確認してください。

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。

項目	説明
プロトコル	設定するプロトコル形式を選択します。 [IPv4]：IPv4 構成のみを設定する場合に選択します。 [IPv6]：IPv6 構成のみを設定する場合に選択します。 [IPv4/IPv6]：IPv4 構成と IPv6 構成を設定する場合に選択します。
MAC アドレス	コントローラボード 1 とコントローラボード 2 の MAC アドレスが表示されます。
IPv4 構成	サービス IP とコントローラボード 1、コントローラボード 2 のネットワーク設定情報を入力します。
IPv6 構成	サービス IP とコントローラボード 1、コントローラボード 2 のネットワーク設定情報を入力します。IPv6 アドレスの自動取得はサポートしてません。
DNS サーバ 1 DNS サーバ 2 DNS サーバ 3	DNS サーバとして設定したいサーバの IP アドレスを設定します。すべて 0 の IP アドレスは設定できません。 [IPv4]： IPv4 アドレスを使用する場合に選択します。 [IPv6]： IPv6 アドレスを使用する場合に選択します。IPv6 アドレスの省略形も設定できます。
ネットワーク接続モード	ネットワーク接続モードを選択します。
DNS サーチ順※1	[追加] ボタンをクリックして、検索するドメインサフィックスを入力します。 [ドメインサフィックス追加] 画面が表示されます。 ピリオド (.) を含め、3 文字以上、255 文字以下の半角英数字で入力します。 ドメイン名の 1 つのラベル (ピリオド [.] で区切られた部分) は、63 文字以内の半角英数字で入力します。 次の記号は使用できません。 (! " # \$ % & ' () * + , / ; < = > ? @ [] ^ _ ` { } ~) スペースも使用できません。 DNS サーバを検索する順にドメインサフィックスを追加してください。 一覧に表示される上のドメインサフィックスから順に優先して検索され

項目	説明
	ます。優先順位を変更するドメインサフィックスを指定してから、[上へ] または [下へ] ボタンをクリックすると、1 行分上下へ移動します。ドメインサフィックスを 1 つ指定してから、[削除] ボタンをクリックすると削除できます。ドメイン名は最大 6 つまで入力できます。
保守ポート※1	保守ポートのネットワークアドレスとホストアドレスをそれぞれ選択します。 [ホストアドレス] ドロップダウンリストの値は、"/"の前がコントローラボード 1 用、"/"の後がコントローラボード 2 用です。
内部ネットワーク※1	内部ネットワークの IP アドレスを選択します。 ドロップダウンリストの値は、"/"の前がコントローラボード 1 用、"/"の後がコントローラボード 2 用です。

注※1

[オプション] をクリックした場合にのみ表示されます。

- 設定内容を確認し [適用] をクリックします。
- 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。

D.5.2 ネットワーク拒否設定の変更

操作手順

- maintenance utility にログインします。
- [管理] — [ネットワーク設定] を選択します。
- [ネットワーク拒否設定] をクリックします。
- 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。

項目	説明
TCP ポート (HTTP) (TCP:80)	通信ポートの有効、無効を選択します。 [有効]：通信ポートが使用できます。 [無効]：通信ポートが使用できません。
UDP ポート (UDP:31001/31002)	
UDP ポート (DTLS) (UDP:37001/37002)	
TCP ポート (SSH) (TCP:20522)	
TCP ポート (MPC) (TCP:10500)	

- 設定内容を確認し [確認] をクリックします。
- 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。

D.6 日時設定

D.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。
- 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:: ~ FDFE: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::xxxx:xxxx:xxxx:xxxx]` (xxxx は任意の数値)
 - グローバルユニキャストアドレス : `[2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]` (xxxx は任意の数値)
 - グローバルユニキャストアドレス : `[2002:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]` (xxxx は任意の数値)
- NTP サーバを使用した日時設定に失敗した場合は「[6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法](#)」に示す障害内容と対処方法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。
 - a. NTP サーバを使用する場合 :
 - [NTP サーバを使用] の [はい] を選択します。
 - [NTP サーバ] に IP アドレス、またはホスト名を入力します。
 - [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。
- b. NTP サーバを使用しない場合：
- ・ 「NTP サーバを使用」の「いいえ」を選択します。
 - ・ 「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。

D.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。

D.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。

D.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。

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 サーバのルート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、「[F.1.1 Syslog の転送プロトコル \(TLS/RFC5424\) の要件](#)」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。
- Syslog 転送プロトコルに UDP/RFC3164 を使う場合は、ネットワークの設計時に UDP の特性を考慮してください。詳細については、IETF が発行する文書 RFC3164 を参照してください。
- Syslog 転送プロトコルに TLS/RFC5424 を使う場合は、Syslog サーバのルート証明書の証明書ファイルやクライアントの証明書ファイルをストレージシステムに設定する必要があります。証明書の要件については、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。
- ストレージシステムへアップロードするクライアントの証明書ファイルは、次のいずれかの形式である必要があります。
 - PKCS#12 形式
 - PEM 形式
 - DER 形式
- PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合は、PKCS#12 形式に変換してください（「[G.10 SSL/TLS 証明書を PKCS#12 形式に変換](#)」を参照）。
- PEM 形式または DER 形式でアップロードする場合は、事前に秘密鍵と CSR（公開鍵）を作成してください（「[D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する](#)」を参照）。この際、[目的] に [Audit Syslog Client (Primary)]、[Audit Syslog Client (Secondary)] または [Audit Syslog Client (Primary and Secondary)] を選択してください。この CSR に基づいて署名された証明書を準備してください。
- 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:: ~ FDFE: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::xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)
 - グローバルユニキャストアドレス：[2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)
 - グローバルユニキャストアドレス：[2002:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)

操作手順

- maintenance utility にログインします。
- [管理] - [監査ログ設定] を選択します。
- [Syslog サーバ設定] をクリックします。
- 監査ログ設定画面が表示されます。各項目を入力します。

項目	説明
転送プロトコル	監査ログ情報を Syslog サーバに転送するプロトコル（[TLS/RFC5424] または [UDP/RFC3164]）を選択します。
プライマリサーバ	Syslog サーバを使用するかどうかを選択します。 [有効]：Syslog サーバに監査ログ情報を転送します。 [無効]：Syslog サーバに監査ログ情報を転送しません。
プライマリサーバーSyslog サーバ	Syslog サーバのホスト名または IP アドレス（IPv4 または IPv6）を入力します。
プライマリサーバーポート番号	Syslog サーバで使用するポート番号を入力します。

項目	説明
プライマリサーバクライアント証明書ファイルフォーマット	証明書ファイルのアップロード形式を指定します。 PKCS#12：証明書と秘密鍵を一つのファイルにまとめて格納するためのファイルフォーマット PEM or DER：証明書単体のファイルフォーマット
プライマリサーバ期待する Subject Key Identifier	証明書ファイルフォーマットを PEM or DER とする場合に、期待する Subject Key Identifier の値を示します。表示される値と同じ Subject Key Identifier 情報を持つ証明書をアップロードしてください。 なお、証明書ファイルフォーマットが PKCS#12 形式の場合、またはストレージシステム内に秘密鍵が存在しない場合は常に "-" が表示されます。 Maintenance Utility を利用して秘密鍵および公開鍵を生成済みにもかかわらず、期待する Subject Key Identifier が "-" で示される場合は、鍵情報の取得に失敗しているか、秘密鍵および公開鍵の生成に失敗している可能性があります。
プライマリサーバクライアント証明書ファイル名※	証明書ファイルを指定します。 [ファイルの選択] をクリックし、証明書ファイルを指定してください。
プライマリサーバパスワード※	クライアント証明書のパスワードを指定します。 [クライアント証明書ファイルフォーマット] を PKCS#12 に設定していて、PKCS#12 作成時にパスワードを設定している場合にはパスワードを入力してください。
プライマリサーバルート証明書ファイル名※	証明書ファイルを指定します。 [ファイルの選択] をクリックし、証明書ファイルを指定してください。
セカンダリサーバ	Syslog サーバを使用するかどうかを選択します。 [有効]：Syslog サーバに監査ログ情報を転送します。 [無効]：Syslog サーバに監査ログ情報を転送しません。
セカンダリサーバ Syslog サーバ	Syslog サーバのホスト名または IP アドレス (IPv4 または IPv6) を入力します。
セカンダリサーバポート番号	Syslog サーバで使用するポート番号を入力します。
セカンダリサーバクライアント証明書ファイルフォーマット	証明書ファイルのアップロード形式を指定します。 PKCS#12：証明書と秘密鍵を一つのファイルにまとめて格納するためのファイルフォーマット PEM or DER：証明書単体のファイルフォーマット
セカンダリサーバ期待する Subject Key Identifier	証明書ファイルフォーマットを PEM or DER とする場合に、期待する Subject Key Identifier の値を示します。表示される値と同じ Subject Key Identifier 情報を持つ証明書をアップロードしてください。 なお、証明書ファイルフォーマットが PKCS#12 形式の場合、またはストレージシステム内に秘密鍵が存在しない場合は常に "-" が表示されます。 Maintenance Utility を利用して秘密鍵および公開鍵を生成済みにもかかわらず、期待する Subject Key Identifier が "-" で示される場合は、鍵情報の取得に失敗しているか、秘密鍵および公開鍵の生成に失敗している可能性があります。
セカンダリサーバクライアント証明書ファイル名※	証明書ファイルを指定します。 [ファイルの選択] をクリックし、証明書ファイルを指定してください。
セカンダリサーバパスワード※	クライアント証明書のパスワードを指定します。 [クライアント証明書ファイルフォーマット] を PKCS#12 に設定していて、PKCS#12 作成時にパスワードを設定している場合にはパスワードを入力してください。
セカンダリサーバルート証明書ファイル名※	証明書ファイルを指定します。 [ファイルの選択] をクリックし、証明書ファイルを指定してください。

項目	説明
ロケーション識別名	Syslog サーバに監査ログ情報を転送するストレージシステムを識別するために、任意の名称を入力します。最大で半角 32 文字の名称を入力できます。 使用可能文字：半角英数字と記号（! " # \$ % & ' () * + - . / : ; < = > ? @ [\] ^ _ ` { } ~）。カンマ（,）とスペースは使用できません。
リトライ※	Syslog サーバとの通信に失敗した場合にリトライするかどうかを選択します。 [有効]：Syslog サーバとの通信に失敗した場合にリトライします。 [無効]：Syslog サーバとの通信に失敗した場合にリトライしません。
リトライ間隔※	Syslog サーバとの通信に失敗した場合のリトライ間隔を 1～60 秒の間で入力します。デフォルトは 1 秒です。
詳細情報出力	監査ログの詳細情報を Syslog サーバに転送するかどうかを選択します。 [有効]：Syslog サーバに監査ログ情報を転送します。 [無効]：Syslog サーバに監査ログ情報を転送しません。

注※

[転送プロトコル] で [TLS/RFC5424] を選択したときのみ指定します。

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。

D.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。

- 「[D.7.1 監査ログを蓄積するための Syslog の設定](#)」で設定した内容
- 「[6.4 maintenance utility の操作時にトラブルが発生した場合の対処方法](#)」に示す障害内容と対処方法

D.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、ESM の監査ログと DKC の監査ログがあります。ESM の監査ログは、AMC-0 および AMC-1 のそれぞれに蓄積されています。一つ目の AMC から ESM

の監査ログのエクスポートを終えた後、もう一方の AMC から ESM の監査ログをエクスポートしてください。

AMC-0 および AMC-1 の IP アドレスで maintenance utility にログインして、ESM の監査ログをエクスポートすることを推奨します。

操作手順

1. AMC-0 の固定 IP アドレスを指定して、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] — [ESM]、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

監査ログエクスポートをダンプ採取中に実施すると、30762-204720 エラーが発生する可能性があります。

ダンプ採取の実行が終了してから、監査ログエクスポートを実施してください。



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。

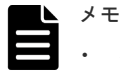
6. ファイルのダウンロード画面が表示されます。エクスポートはファイルのダウンロードとして行われます。[DKC] を選択したときは、ファイルのダウンロード画面が表示されるまで 2~3 分かかります。



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。

11. maintenance utility からログアウトします。
12. AMC-0 の固定 IP アドレスを AMC-1 の固定 IP アドレスに変更して、手順 1～11 を繰り返します。



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
「[D.7.1 監査ログを蓄積するための Syslog の設定](#)」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
「[D.6.1 日時設定の変更](#)」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。

D.8 外部認証

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

設定は、maintenance utility で行います。



メモ

- ・ 外部認証サーバを使用するには、外部認証サーバへの接続設定やネットワークの設定が必要です。設定値は外部認証サーバの管理者に問い合わせてください。ネットワークの設定に関しては、ネットワークの管理者に問い合わせてください。
- ・ 外部認証サーバとの通信には、外部認証サーバのルート証明書の証明書ファイルをストレージシステムに設定する必要があります。証明書の要件については、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。
- ・ 外部認証サーバに登録されているユーザの所属先ユーザグループと、ストレージシステムにローカルに登録されているユーザの所属先ユーザグループが異なる場合、ストレージシステムでの所属先ユーザグループが優先されます。
- ・ ユーザアカウントを maintenance utility で作成しない場合、ユーザグループの割り当て（認可）は外部認証サーバに設定してください。この場合、ストレージシステムに定義されているユーザグループと同じ名称のグループを外部認証サーバに定義してください。ビルトイングループの名称は、「[D.2.4 ユーザグループ](#)」を参照してください。ユーザアカウントを maintenance utility で作成する場合、認証の手段として外部認証を選択できますが、ユーザグループの割り当て（認可）は maintenance utility での設定が適用されます。ユーザグループの割り当て（認可）を外部認証サーバに設定しても適用されません。

D.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ストレージシステムにルート証明書を設定する必要があります。証明書については、LDAP ディレクトリサーバの管理者に問い合わせてください。

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

注※

証明書の要件など詳細については、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。

D.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:: ~ FDFE: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::xxxx:xxxx:xxxx:xxxx]（xxxx は任意の数値）
- グローバルユニキャストアドレス：[2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]（xxxx は任意の数値）
- グローバルユニキャストアドレス：[2002:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx]（xxxx は任意の数値）



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。

項目	説明
証明書ファイル名	証明書ファイルを指定します。[ファイルの選択] ボタンをクリックし、証明書ファイルを指定してください。次のフォーマットをサポートします。 X509 DER X509 PEM
DNS Lookup	外部認証・認可サーバの指定方法を設定します。 [有効]：DNS サーバの SRV レコードで、外部認証・認可サーバを指定します。 [無効]：ホスト名または IP アドレスで、外部認証・認可サーバを指定します。
認証プロトコル	LDAP プロトコルを設定します。次のプロトコルが使用できます。 LDAP over SSL/TLS STARTTLS [DNS Lookup] で有効を選択した場合、LDAP over SSL/TLS は選択できません。
外部ユーザグループ連携	指定した LDAP ディレクトリサーバを認可サーバとしても使用するかを設定します。 [有効]：使用する [無効]：使用しない
プライマリサーバ・ホスト名	LDAP ディレクトリサーバのホスト名、または IP アドレスを設定します。 ルート証明書のコモンネームと同一のホスト名、または IP アドレスを設定してください。 [DNS Lookup] で有効を選択した場合、この項目は入力不要です。
プライマリサーバ・ポート番号	LDAP ディレクトリサーバのポート番号を設定します。 [DNS Lookup] で有効を選択した場合、この項目は入力不要です。
プライマリサーバ・ドメイン名称	LDAP ディレクトリツリーのドメイン名称を設定します。
プライマリサーバ・ユーザ名属性	認証で使用するユーザ ID の値が定義されている属性名を設定します。 使用可能文字：半角英数字と記号 (! # \$ % & ' () * + , - . / : ; < = > ? @ [¥] ^ _ ` { } ~) 階層モデルの場合：ユーザを特定できる値が格納されている属性名を設定します。 フラットモデルの場合：ユーザエントリの RDN の属性名を設定します。
プライマリサーバ・タイムアウト	LDAP ディレクトリサーバとの接続タイムアウトを検出するまでの時間(秒)を設定します。
プライマリサーバ・リトライ間隔	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ間隔(秒)を設定します。
プライマリサーバ・リトライ回数	LDAP ディレクトリサーバとの通信に失敗した場合のリトライ回数を設定します。
プライマリサーバ - Base DN	認証するユーザを検索するときに基点となる DN を設定します。 使用可能文字：半角英数字とすべての記号 階層モデルの場合：すべての検索対象のユーザを含む階層の DN を設定します。 フラットモデルの場合：検索対象のユーザより 1 つ上の階層の DN を設定します。 記号 (+ ; , < = > など) を入力する場合は、1 文字ごとに記号の直前に円記号 (¥) を入力してエスケープしてください。ただし、¥、/、"を入力す

項目	説明
	るときは、次のとおり円記号 (¥) を入力したあとに ASCII コードを入力してください。 「¥」は、「¥5c」と入力します。 「/」は、「¥2f」と入力します。 「"」は、「¥22」と入力します。
プライマリサーバ - 検索用ユーザ DN	検索用ユーザの DN を設定します。 使用可能文字：半角英数字とすべての記号 [プライマリサーバ - ユーザ名属性] に sAMAccountName を指定した場合、または [外部ユーザグループ連携] で有効を選択した場合にのみ、入力が必要です。 記号 (+; , <=> など) を入力する場合は、1 文字ごとに記号の直前に円記号 (¥) を入力してエスケープしてください。ただし、¥、/、" を入力するときは、次のとおり円記号 (¥) を入力したあとに ASCII コードを入力してください。 「¥」は、「¥5c」と入力します。 「/」は、「¥2f」と入力します。 「"」は、「¥22」と入力します。
プライマリサーバ - パスワード	検索用ユーザのパスワードを設定します。LDAP ディレクトリサーバに登録しているパスワードと同じ値を設定してください。 使用可能文字：半角英数字と記号 (! # \$ % & ' () * + - . = @ ¥ ^ _ / ; < > ? [] ` { } ~ " , とスペース) [プライマリサーバ - ユーザ名属性] に sAMAccountName を指定した場合、または [外部ユーザグループ連携] で有効を選択した場合にのみ、入力が必要です。
プライマリサーバ - パスワード再入力	[プライマリサーバ - パスワード] で入力したパスワードを再度入力します。
セカンダリサーバ	LDAP ディレクトリサーバの代替サーバを使用するかを設定します。 [有効]：代替サーバを使用する [無効]：代替サーバを使用しない [DNS Lookup] で有効を選択した場合、この項目は入力不要です。
セカンダリサーバ - ホスト名	LDAP ディレクトリサーバの代替サーバのホスト名、または IP アドレスを設定します。 ルート証明書のコモンネームと同一のホスト名、または IP アドレスを設定してください。 [セカンダリサーバ] で無効を選択した場合、この項目は入力不要です。
セカンダリサーバ - ポート番号	LDAP ディレクトリサーバの代替サーバのポート番号を設定します。 [セカンダリサーバ] で無効を選択した場合、この項目は入力不要です。
テストユーザ名	[サーバ構成テスト] で使用するユーザ名を設定します。 使用可能文字：半角英数字と記号 (! # \$ % & ' * + - . / = ? @ ¥ ^ _ { } ~)
テストユーザ名 - パスワード	[サーバ構成テスト] で使用するユーザのパスワードを設定します。 使用可能文字：半角英数字と記号 (! # \$ % & ' () * + , - . / ; < = > ? @ [¥] ^ _ { } ~)
サーバ構成テスト	[チェック] ボタンをクリックし、設定された内容で外部認証・認可サーバへの接続テストを行います。
サーバ構成テスト - 結果	外部認証・認可サーバへの接続テストの結果が表示されます。

- 設定内容を確認し、LDAP の設定画面の [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。

5. テストの結果を確認し [適用] をクリックします。
6. AMC-0 の管理ポートと AMC-1 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、AMC-1 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。

D.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。

D.9 初期設定

D.9.1 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。
- プロトコルは、IPv4 のみ、または IPv4/IPv6 を組み合わせて指定できますが、IPv6 のみの指定はできません。
- 設定する IP アドレスやドメイン名が「HSTS プリロードリスト」に含まれないことを、事前に確認してください。「HSTS プリロードリスト」に含まれる IP アドレスやドメイン名を設定する場合、検証可能な証明書、Web サーバ証明書として登録する必要があります。
Google Chrome の場合、アドレスバーに [chrome://net-internals/#hsts] と入力すると、HSTS に関するページから「HSTS プリロードリスト」を確認できます。例えば、IP アドレス 1.0.0.1 は、static_sts_domain: 1.0.0.1 と表示され、「HSTS プリロードリスト」に登録されていることがわかります。
- 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 AMC-0 と AMC-1 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:: ~ FDFE: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::xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)
 - グローバルユニキャストアドレス : [2001:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)
 - グローバルユニキャストアドレス : [2002:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx] (xxxx は任意の数値)

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。
各項目の詳細については、「[D.5.1 ネットワーク設定の変更](#)」を参照してください。



注意

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。

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。

D.10 電源管理

D.10.1 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

- PDU 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

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。

D.10.2 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。

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. 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. 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 4.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

D.10.3 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。

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。

D.11 システム管理

D.11.1 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。

操作手順

1. maintenance utility を起動します。

2. 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。
3. 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。
4. [完了] をクリックします。
5. 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。
6. 確認画面が表示されます。[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。

D.11.2 ログインメッセージの編集

maintenance utility のログイン画面と、SSH 接続による内蔵 CLI のコンソールに、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。

D.11.3 Web サーバ接続用証明書をストレージシステムへアップロード

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

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



注意

- アップロードする Web サーバ接続用証明書の要件については、「[G.3 ストレージシステムと管理ツールの操作端末間の SSL/TLS 通信](#)」を参照ください。
- ストレージシステムへアップロードする証明書ファイルは、次のいずれかの形式である必要があります。
 - PKCS#12 形式
 - PEM 形式
 - DER 形式
- PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合は、PKCS#12 形式に変換してください（「[G.10 SSL/TLS 証明書を PKCS#12 形式に変換](#)」を参照）。
- PEM 形式または DER 形式でアップロードする場合は、事前に秘密鍵と CSR（公開鍵）を作成してください（「[D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する](#)」を参照）。この際、[目的] に [Web Server] を選択してください。この CSR に基づいて署名された証明書を準備してください。
- 中間証明書が存在する場合は、中間証明書を含んだ証明書チェーンで構成された、署名付き公開鍵証明書を準備してください。
- アップロードする証明書の証明書チェーンの階層数は、ルート CA 証明書を含めて 20 階層以下です。
- アップロードする証明書の公開鍵暗号方式は、RSA です。

操作手順

1. maintenance utility にログインします。
2. 左下の [メニュー] - [システム管理] - [証明書ファイル更新] を選択します。
3. 証明書ファイル更新画面が表示されます。

更新対象の証明書の左横のチェックボックスを選択してください。

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

4. アップロードする証明書ファイルの形式を選択します。

形式	説明
PKCS#12	サーバ証明書ファイルと秘密鍵ファイルを含む形式です。
PEM or DER	サーバ証明書ファイルのみの形式です。 [期待する Subject Key Identifier] 欄と、Subject Key Identifier 情報が一致する証明書ファイルをアップロードしてください。証明書ファイルの Subject Key Identifier 情報は、証明書の拡張属性に記載されています。[PEM or DER] を選択しても [期待する Subject Key Identifier] 欄に "-" (ハイフン) が表示される場合は、鍵情報の取得に失敗している可能性があります。3 分程度あけて、再度、「 D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する 」の手順に従って秘密鍵および CSR (公開鍵) の作成をしてください。

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

D.11.4 maintenance utility を利用して秘密鍵および公開鍵を生成する

maintenance utility から、CSR (公開鍵)、秘密鍵、および自己署名証明書を作成できます。認証局から証明書を発行してもらう場合は、CSR と秘密鍵を作成し、認証局に CSR を送付してください。



注意

- 秘密鍵および公開鍵の生成からダウンロード開始までには数秒程度掛かります。鍵生成に掛かる時間は、ご使用の環境によって異なります。
- この手順で生成した CSR や秘密鍵を用いて作成した証明書や、この手順で生成した自己署名証明書は、Hitachi Virtual Storage Platform One Block 以外の用途では使用できません。



メモ

maintenance utility で作成した公開鍵は、openssl コマンドでカスタマイズできます (詳細は「[G.6 公開鍵を作成](#)」を参照)。

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. [システム管理] - [CSR 作成および自己署名証明書作成] を選択します。
3. 各入力項目を記入します。

項目	説明
CSR 設定	
国名（必須）	国名を半角英字 2 文字で入力します（例：JP）。
都道府県名（必須）	都道府県名を指定します（例：Kanagawa）。
市区町村名または地域名（必須）	市区町村名または地域名を入力します（例：Yokohama）。
組織名（必須）	組織名を入力します（例：Hitachi Vantara）。
部門名（必須）	部門名を入力します（例：Storage）。
一般名（必須）	サーバの IP アドレスまたはホスト名を入力します。
別の組織名（任意）	追加の組織名を入力します。
サブジェクト代替名（任意）	[サブジェクト代替名を使用] のチェックボックスにチェックを付けるとサブジェクト代替名を入力できます。 サブジェクト代替名に設定する項目をプルダウンメニューで選択し、テキストボックスに値を入力します。選択可能な項目名は次のとおりです。 - E-mail アドレス - DNS 名 - IP アドレス [Add Subject Alternative Name] ボタンをクリックすることでサブジェクト代替名を入力するテキストボックスを追加できます。また、不要なテキストボックスはテキストボックス右側の [-] ボタンをクリックすることで削除できます。
秘密鍵設定	
鍵タイプ（必須）	プルダウンメニューをクリックし、RSA または ECDSA を選択します。
鍵長（必須）	プルダウンメニューをクリックし、鍵長を選択します。鍵タイプによって選択できる鍵長は異なります。 - RSA: 2048bits, 3072bits, 4096bits - ECDSA: 256bits(secp256r1), 384bits(secp384r1), 521bits(secp521r1)
目的	秘密鍵の用途を選択します。 - Any : すべての用途に使用可能 - Web Server : Web サーバ証明書向け - Audit Syslog Client(Primary) : 監査ログプライマリサーバのクライアント証明書向け - Audit Syslog Client(Secondary) : 監査ログセカンダリサーバのクライアント証明書向け - Audit Syslog Client(Primary and Secondary) : 監査ログプライマリサーバと監査ログセカンダリサーバのクライアント証明書向け 自己署名証明書を作成する場合は、必ず Any を選択してください。 Any 以外を選択する場合の動作を示します。 - 秘密鍵はストレージシステム内に保存され、ダウンロードされません。 - すでに Any 以外で秘密鍵を作成している場合、ストレージシステム内の秘密鍵は上書きされます。問題ないか事前に確認してください。
パスワード（任意）	秘密鍵のパスワードを入力します。 半角英数字（12～20 文字）を入力できます。英字の場合は、大文字および小文字が区別されます。 ここで入力するパスワードは自己署名証明書を PKCS#12 形式で保護する際にも使用します。 [秘密鍵設定] の [目的] で Any を選択した場合のみ、入力できます。Any を選択すると、秘密鍵がダウンロードされるため、パスワードによる保護が必要となります。

項目	説明
	す。Any 以外を選択すると、秘密鍵はストレージシステム内に保存されてダウンロードされないため、パスワードによる保護は不要です。
パスワード(再入力) (パスワードを設定した場合、必須)	「パスワード」で設定したパスワードを再入力します。
CSR ファイル作成 および秘密鍵ファイル作成	ファイルのダウンロード画面に遷移します。 CSR 設定および秘密鍵設定の必須項目をすべて入力、または選択しないかぎり、ボタンは活性化されません。 自己署名証明書を作成する場合は、このボタンをクリックしないでください。
自己署名証明書を作成する	自己署名証明書を作成する場合は、チェックを入れます。デフォルトではオフになっています。
プロファイル (.cfg ファイル)	- デフォルト：システムが自動でデフォルトの設定を適用し、ファイル選択は不要となります。 - カスタム：プロファイルの参照位置を選択します。[参照] または [ファイルの選択] をクリックし、使用するプロファイルを指定します。クリックするボタンの名称は、ブラウザによって異なります。 プロファイル (.cfg ファイル) 設定の詳細については、この表の後に記載している「プロファイル (.cfg ファイル)」を参照してください。
自己署名証明書ファイル作成	自己署名証明書ファイルを作成します。 以下の必須項目をすべて入力、または選択しないかぎり、ボタンは活性化されません。 - CSR 設定 - 秘密鍵設定 - プロファイル (デフォルトまたはカスタムを選択します。カスタムの場合は、ファイルを選択します。)
閉じる	ファイル設定画面を閉じます。

必要情報の記入が完了したら、自己署名証明書の作成有無により、次の手順を実施してください。

- ・ 自己署名証明書を作成する場合：
[CSR および秘密鍵を作成] をクリックせずに、手順 4 に進んでください。
 - ・ 自己署名証明書を作成しない場合：
[CSR および秘密鍵を作成] をクリックしてから、手順 5 に進んでください。
4. [自己署名証明書を作成する] のチェックボックスを選択します。
[プロファイル] 欄にある下記の項目から、該当する項目を選択します。
- ・ [デフォルト]：この項目を選択した場合、証明書の有効日数として 365 日、証明書のハッシュアルゴリズムとして SHA-256 が設定されます。デフォルト設定のままでよい場合は、[自己署名証明書ファイル作成] をクリックします。
 - ・ [カスタム]：この項目を選択した場合、.cfg ファイルによって自己署名証明書の有効日数とハッシュアルゴリズムが指定できます。「プロファイル (.cfg ファイル)」を参照し、作成した.cfg ファイルを [参照] または [ファイルの選択] から選択し、[自己署名証明書ファイル作成] をクリックします。クリックするボタンの名称は、ブラウザによって異なります。
5. 既存の秘密鍵の上書きについて確認する画面が表示された場合は、上書きの可否を選択してください。
- ・ 上書きする場合：
[確認しました] のチェックボックスにチェックマークを入れ、[OK] をクリックします。

- ・ 上書きしない場合：
[キャンセル] をクリックします。



メモ

ストレージシステム内に秘密鍵が保存されている状態で、手順 3 の [秘密鍵設定] - [目的] で Any 以外を選択した場合に表示されます。

6. 手順 3 または手順 4 を実施した後、[ファイルのダウンロード] 画面が表示されます。[保存] をクリックし、所定のフォルダに作成したファイルが保存されているか確認します。
7. [CSR 作成および自己署名証明書作成] 画面で、[閉じる] をクリックします。

プロファイル (.cfg ファイル)

プロファイル (.cfg ファイル) は自己署名証明書で設定するパラメータを定義するファイルです。

プロファイルの形式と書式、および定義されるパラメータについて説明します。

- ・ ファイル形式
 - 形式：テキスト
 - 拡張子：.cfg
 - 文字コード：ISO-8859-1
 - 行末記号：CRLF
- ・ ファイル書式
 - パラメータ 1=パラメータ 1 の設定値
 - パラメータ 2=パラメータ 2 の設定値

プロファイル (.cfg) の記載例

```
days=3650  
hashAlgorithm=SHA384
```

プロファイルで定義されるパラメータ

パラメータ名	説明
days	自己署名証明書作成時点から証明書が有効である日数を指定します。1 から 3650 までの整数値が指定できます。
hashAlgorithm	自己署名証明書で使用するハッシュアルゴリズムを指定します。SHA256 または SHA384 が指定できます。 SHA256 を指定した場合、自己署名証明書のハッシュアルゴリズムとして SHA-256 が設定されます。 SHA384 を指定した場合、自己署名証明書のハッシュアルゴリズムとして SHA-384 が設定されます。 このパラメータを指定しない場合は自己署名証明書のハッシュアルゴリズムとして SHA-256 が設定されます。

D.11.5 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。

D.11.6 ESM の状態確認



注意

AMC 上の ESM の状態が以下の場合、5 分程度待ってからリロードを実行し、改めて状態を確認してください。何度かリロードを実行しても状態が変わらない場合は、保守員に問い合わせてください。

- ESM の状態
 - 両方の AMC が共に Active の場合
 - 両方の AMC が共に Standby の場合
 - Starting が含まれる場合
 - Error が含まれる場合

操作手順

1. maintenance utility にログインします。
2. maintenance utility のメイン画面左側のツールバーにある [ストレージシステム] に記載の "Connected to:AMC-X"を確認し、現在接続している AMC を確認します。
3. 左上の [ハードウェア] - [全シャーシ] を選択します。
4. 右上の [システム情報設定] - [ESM クラスタロール] より、現在接続している AMC 上の ESM の状態 (Active または Standby) を確認します。

D.11.7 ESM のリブート



注意

- AMC-0、AMC-1 の順に、両方の AMC の ESM をリブートしてください。
両方の AMC の ESM を同時にリブートすると、管理ツールの操作端末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、「[D.2.4 ユーザグループ](#)」を参照してください。
- ESM リブートを実施する際には、接続している AMC 上の ESM の状態が Standby である必要があります。
事前に接続している AMC 上の ESM の状態確認を行い、Active 状態である場合に ESM のフェールオーバーを実施してください。詳細は、下記操作手順の手順 2 を参照してください。

操作手順

1. AMC-0 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. 現在接続している AMC 上の ESM の状態 (Active または Standby) を確認します。ESM の状態については、「[D.11.6 ESM の状態確認](#)」を参照してください。
交換する AMC 上の ESM の状態が Standby である場合、手順 3 へ進んでください。
交換する AMC 上の ESM の状態が Active である場合、手動フェールオーバーを実行してください。手動フェールオーバーを実行してから、再度 ESM の状態確認を行い、状態が Standby であることを確認し、手順 3 から再開してください。手動フェールオーバーについては、「[D.11.8 ESM の手動フェールオーバー](#)」を参照してください。
3. 左下の [メニュー] - [システム管理] - [ESM リブート] を選択します。

4. [リブート] をクリックします。
5. 警告画面が表示されます。[OK] 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。
7. ESM のリブートが開始されます。
ログアウト画面が表示されたら、[×] をクリックして画面を閉じます。
8. Web ブラウザのアドレスバーに ESM をリブートした AMC 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。

9. AMC-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。
10. 手順 2~手順 8 を実施して、AMC-1 の ESM をリブートします。

D.11.8 ESM の手動フェールオーバー



注意

- 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"ストレージ管理者（初期設定）"ロール又は、"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、[「D.2.4 ユーザグループ」](#)を参照してください。
- Active ESM と Standby ESM を切り替えます。この操作は、サービス IP アドレスを使用しているすべてのコネクションを一時的に切断します。サービス IP アドレスを利用している人がいないか確認してください。ESM フェールオーバー完了後、サービス IP アドレスのコネクションを確認してください。この操作は、セッションが切断される場合がありますので、maintenance utility に再度接続してください。

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] - [ESM フェールオーバー] を選択します。
3. [適用] をクリックします。
「Active ESM を強制停止する」のチェックボックスには、チェックを入れないでください。
4. 保守パスワード要求画面が表示されます。ユーザパスワードタイプのパスワードを入力し、[OK] をクリックします。
5. ESM のフェールオーバーが開始されます。
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。
7. ログアウト画面が表示される場合があります。ログアウト画面が表示された場合は、[×] をクリックして画面を閉じます。

D.11.9 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

システムダンプのダウンロードを監査ログエクスポート実行中に実施すると、30762-204720 エラーが発生する可能性があります。
監査ログエクスポートの実行が終了してから、システムダンプのダウンロードを実施してください。



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（ファームウェアバージョン先頭 2 桁＋装置名 4 桁＋ストレージシステムの装置製番 6 桁）を付けることを推奨します。

ファイル名：hdcp_dump_（装置識別番号）.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 AMC 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。

D.11.10 スモールシステムダンプのダウンロード

スモールシステムダンプのダウンロードは保守員が行う作業です。お客様による操作は不要です。

D.11.11 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。

D.11.12 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。

D.11.13 セッションタイムアウト時間の編集

maintenance utility または VSP One Block Administrator で使用する管理ツールの操作端末と、ストレージシステム間のセッションタイムアウト時間を編集できます。この機能は内蔵 CLI、RAID Manager、詳細 API には適用されません。この機能で設定されたセッションタイムアウト時間は、ストレージシステム全体に適用され、ユーザは編集できません。



メモ

設定前に確立していたセッションに対しては、設定後のセッションタイムアウト時間が反映されないおそれがあります。

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. 左下の [メニュー] - [システム管理] - [セッションタイムアウト時間編集] を選択します。

3. プルダウンメニューから時間を選択してください。以下の値が選択できます。デフォルトは 60 分です。

選択可能時間（単位：分）
60（デフォルト）
90
120

4. [適用] をクリックします。

D.11.14 コモンクライテリア認証に準拠する設定を実施する

コモンクライテリア認証に準拠するセキュリティ機能を使用したい場合は、[コモンクライテリア認証設定] 画面で機能の有効化を実施してください。なお、[コモンクライテリア認証設定] 画面で設定する機能は、デフォルトでは無効となっています。

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. 左下の [メニュー] - [システム管理] - [コモンクライテリア認証設定] を選択します。
3. [コモンクライテリア認証設定] 画面が表示されます。
各項目の有効、無効を選択します。

項目	説明
管理ポート TLS 通信ログの 監査ログ出力	有効または無効を設定します。 有効にすると管理ポートとの TLS 通信※1 が、監査ログに記録されるようになります。
証明書ファイルアップロード 時の検証項目追加	有効または無効を設定します。 有効にすると証明書ファイルアップロード時に実施する検証項目が追加※2 され、より厳しい検証が実施されます。

注※1

管理ツールの操作端末から Web ブラウザまたは REST API クライアントを使用してリクエストを送信した際、TLS 通信の開始または終了が監査ログに記録されます。

注※2

「証明書ファイルアップロード時の検証項目追加」を有効化すると、有効化前まではアップロードできていた証明書もアップロードできなくなる可能性がありますので、十分にご注意ください。

有効化した際に追加される証明書の検証項目の詳細はマニュアルを参照してください。

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。

D.11.15 TLS セキュリティ設定を管理する

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

前提条件

- 必要なロール：セキュリティ管理者（参照・編集）ロール

操作手順

1. maintenance utility にログインします。
2. 左下の [メニュー] - [システム管理] - [TLS セキュリティ選択] を選択します。[TLS セキュリティ選択] 画面が表示されます。
3. 各項目を設定します。設定項目の詳細は「[G.13.1 SSL/TLS 通信のセキュリティ設定項目](#)」を参照してください。



注意

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

SSL/TLS 通信時に、上記の条件を満たさない証明書を使用している場合は、証明書検証や TLS ハンドシェイクが失敗し、通信できなくなる場合があります。証明書の署名アルゴリズム、鍵長、ハッシュアルゴリズムが要件を満たしているか、事前に確認ください。

5. TLS セキュリティ設定を変更した場合、ブラウザからストレージシステムへのアクセスや、ストレージシステムから外部サーバ等への TLS 通信に失敗する可能性があります。ブラウザや外部サーバに登録している証明書が、変更する TLS セキュリティ設定に対応しているか事前に確認してください。確認が取れない場合、事前に TCP ポート (SSH) (TCP:20522) が有効であるかを確認し、有効でない場合は一時的に TCP ポートの (SSH) または (TCP:20522) を有効にしてください。
6. TLS セキュリティ設定後に、ブラウザや外部サーバとの通信に成功した場合は、TCP ポートの (SSH) または (TCP:20522) の設定を元に戻してください。設定画面へ接続ができない場合は、「[G.13.3 SSL/TLS 通信のセキュリティ設定を初期化する](#)」を参照して、TLS セキュリティ設定を初期化した後に、再度 TLS セキュリティを設定してください。再度設定した後も、TLS 通信失敗が解消されない場合は、お問い合わせください。

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

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

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

D.12 アラートの表示

弊社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。

D.12.1 アラート表示

「[6.5 maintenance utility の内部アラート詳細の確認手順](#)」を参照してください。

D.12.2 FRU に関するアラート表示

「[6.6 maintenance utility の FRU（Field Replacement Unit）に関するアラートの確認手順](#)」を参照してください。

D.13 SIM のコンプリート

アラート（SIM）に示されている障害を解決したあとに、SIM が解決されたこと（SIM のコンプリート）を、ストレージシステムに報告します。

操作手順

1. maintenance utility にログインします。
2. ヘッダエリアの [アラート] をクリックします。
3. [アラート] タブが表示されます。右上の [DKC]、[ESM (AMC-0)]、[ESM (AMC-1)] をそれぞれクリックして、SIM を確認します。
4. 障害を解決した SIM の状態が、未コンプリートの場合、左側のチェックボックスを選択して [コンプリート] をクリックします。
5. [アラートコンプリート] 画面が表示されます。指定した SIM が表示されていることを確認して [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。[OK] をクリックします。
7. 指定した SIM の状態がコンプリート済になったことを確認します。



ストレージシステムの障害情報の通知手段

ストレージシステムの障害情報の通知について説明します。

□ E.1 ストレージシステムの障害情報の通知手段

E.1 ストレージシステムの障害情報の通知手段

ストレージシステムの障害情報（SIM）を Syslog、SNMP トラップ、およびメールで通知できます。

メールで通知される障害は、SIM や、SNMP トラップで報告される SIM と同じものです。SNMP トラップでは、障害の有無を確認するためにユーザが SNMP マネージャにアクセスする必要がありますが、Syslog やメールによる通知では、ユーザは Syslog やメールをチェックするだけで障害の発生を知ることができます。

- 障害を通知するメールの情報を設定
「[D.3.1 メール通知の設定](#)」を参照してください。
- 障害を通知する Syslog 情報の設定
「[D.3.3 アラート通知を蓄積するための Syslog の設定](#)」を参照してください。
- 障害を通知する SNMP ラップを設定
「[D.3.5 SNMP エージェントの設定](#)」を参照してください。
- テスト送信の実施
テストメール送信の詳細は、「[D.3.2 テストメールの送信](#)」を参照してください。
Syslog サーバへのテストメッセージ送信の詳細は、「[D.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](#)」を参照してください。
テストメール送信の詳細は、「[D.3.2 テストメールの送信](#)」を参照してください。
SNMP マネージャへのトラップのテスト送信の詳細は、「[D.3.6 テスト SNMP トラップの送信](#)」、および『障害通知ガイド』を参照してください。

E.1.1 Syslog の転送プロトコル（TLS/RFC5424）の要件

Syslog の転送プロトコル（TLS/RFC5424）を使用する場合、次の要件を満たしている必要があります。

- 動作確認済みの、TLS1.2 をサポートした Syslog サーバ
- Syslog サーバのルート証明書とクライアント証明書がストレージシステムに設定されていること。
Syslog サーバのルート証明書とクライアント証明書の要件は、「[G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信](#)」を参照ください。

これらの証明書については Syslog サーバの管理者にお問い合わせください。証明書の管理については Syslog サーバの管理者とご相談の上、適切に管理してください。

証明書には期限があります。期限が切れると Syslog サーバと接続できなくなるため、証明書を準備するときは証明書の期限にご注意ください。

Syslog サーバの CA 局（Certificate Authority）によって署名されたクライアント証明書を、PKCS#12 形式に変換してください「[E.1.2 クライアント証明書を取得する（Syslog プロトコルを使用する場合）](#)」を参照。

PKCS#12 形式のクライアント証明書に設定されたパスワードがわからない場合は、Syslog サーバの管理者にお問い合わせください。

E.1.2 クライアント証明書の取得（Syslog プロトコルを使用する場合）

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

クライアント証明書を作成するためのプログラムは、OpenSSL のホームページ (<http://www.openssl.org/>) からダウンロードしてください。OpenSSL のバージョンは 3.0.7 以降を使用してください。ここでは、OpenSSL が C:\openssl フォルダにインストールされているものとします。また、クライアント証明書は、PKCS#12 形式に変換する必要があります。

SSL/TLS 通信の設定については、「[付録 G. SSL/TLS 通信の設定](#)」を参照してください。

E.1.3 テストメールの例

送信されるテストメールの例を次に示します。

```
メールタイトル:StorageSystem Report
// StorageSystem //VSP //////////////////////////////////////
// Ver 1.1 e-Mail Report
////////////////////////////////////
Date:01/23/2023
Time:13:45:56
Machine:StorageSystem(Serial# 800001)
RefCode:7ffffff
Detail:This is Test Report.
```

障害発生時に送信されるメールの詳細を次の表に示します。

項目	項目説明
メールタイトル	メールのタイトル (ストレージシステムの装置名) + (Report)
通知する付加情報	[アラート通知設定] 画面で入力した内容です。未入力の場合は、何も表示されません。
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	リファレンスコード SNMP トラップで報告されるものと同じです。
Detail	Detail 障害内容 SNMP トラップで報告されるものと同じです。
Action Code	Action Code 保守作業に必要な不良の個所の情報です。テストメールには記載されません。



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。

- F.1 ストレージシステムに対してネットワーク監視 (Ping 応答またはリンクアップ/リンクダウンによる監視) をする場合
- F.2 SSD 電源オフ時間の注意

F.1 ストレージシステムに対してネットワーク監視（Ping 応答またはリンクアップ/リンクダウンによる監視）をする場合

ESM の状態監視で、ESM の停止を検出した場合、救済措置として、ESM 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。

ESM 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。

F.2 SSD 電源オフ時間の注意

フラッシュドライブ SSD（NVMe）は、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。

フラッシュドライブ（NVMe）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 ヶ月以上継続した場合、保証および保守契約による交換の対象になりません。

SSL/TLS 通信の設定

管理ツールの操作端末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/TLS 通信を構築します。

- G.1 SSL/TLS とは
- G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信
- G.3 ストレージシステムと管理ツールの操作端末間の SSL/TLS 通信
- G.4 SSL/TLS 通信の設定の流れ
- G.5 秘密鍵を作成
- G.6 公開鍵を作成
- G.7 署名付き証明書を取得
- G.8 署名付きの信頼できる証明書を取得
- G.9 CSR 作成および自己署名証明書作成
- G.10 SSL/TLS 証明書を PKCS#12 形式に変換
- G.11 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
- G.12 詳細 API サーバ間の SSL 通信用の証明書を詳細 API サーバへアップロード
- G.13 TLS セキュリティ設定を管理する
- G.14 セキュリティ警告が表示されたときの対処方法

G.1 SSL/TLS とは

SSL (Secure Socket Layer) / TLS (Transport Layer Security) 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/TLS 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。

管理ツールの操作端末を使用する場合、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、ストレージシステムは自分がサーバであることと鍵の所有者であることを管理ツールの操作端末に証明します。これによって管理ツールの操作端末とストレージシステムは SSL/TLS 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 上で管理ツールの操作端末とストレージシステム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、管理ツールの操作端末からストレージシステムに接続できなくなります。
- 証明機関から SSL/TLS サーバ証明書を発行する場合には数日かかります。

G.2 ストレージシステムと外部サーバ間の SSL/TLS 通信

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

プロトコルの暗号スイートを、次に示します。

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

プロトコルの暗号スイートは、変更できます（「[G.13 TLS セキュリティ設定を管理する](#)」を参照）。

鍵交換でのアルゴリズムと鍵長を、次に示します。

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

鍵交換でのアルゴリズムと鍵長は、変更できます（「[G.13 TLS セキュリティ設定を管理する](#)」を参照）。

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

表 4 サポートされている署名アルゴリズム・鍵長・ハッシュアルゴリズム

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

署名アルゴリズム、鍵長、およびハッシュアルゴリズムは、変更できます（「[G.13 TLS セキュリティ設定を管理する](#)」を参照）。

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

表 5 証明書の要件

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

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

凡例

- ：必須項目
- △：通信対象サーバの要件に依存する項目
- ×

注※

「[G.13 TLS セキュリティ設定を管理する](#)」に示す操作で、セキュリティモードを設定することにより、署名アルゴリズム、鍵長、およびハッシュアルゴリズムの絞り込みができます。

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

検証対象

- ・ syslog サーバ※1
- ・ 外部認証サーバ※2
- ・ 鍵管理サーバ※4

- ・ 外部ストレージシステムの詳細 API サーバ※3

注※1

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

注※2

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

注※3

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

注※4

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

検証項目は、検証のタイミングによって変わります。

検証タイミングごとの検証内容については、「[G.2.1 証明書のアップロード時に実施する証明書検証項目](#)」および「[G.2.2 外部サーバとの通信時に実施する証明書検証項目](#)」を参照してください。

G.2.1 証明書のアップロード時に実施する証明書検証項目

ストレージシステムにアップロードするルート証明書またはクライアント証明書について、証明書のアップロード時に証明書チェーンの有効性を検証します。検証項目を、次に示します。

検証項目

- ・ 証明書の要件を満たしていること。※1
- ・ 証明書チェーンに含まれるすべての証明書の署名が正しいこと、および「[表 5 証明書の要件](#)」に示す#6 (拡張属性 (basicConstraints)) の要件を満たしていること。※2、※3
- ・ ストレージシステム内の秘密鍵とアップロードされた証明書のペアが正しいこと。※4

注※1

「[表 5 証明書の要件](#)」に示す証明書の要件のうち、#1 (形式) と#3 (署名のアルゴリズム/鍵長/ハッシュアルゴリズム) の内容を検証します。

注※2

- ・ [コモンクライテリア認証設定] で「証明書ファイルアップロード時の検証項目追加」が有効の場合にのみ検証が実施されます。
有効化する方法は、「[D.11.14 コモンクライテリア認証に準拠する設定を実施する](#)」を参照ください。
- ・ 次の条件をすべて満たす場合は、必ずクライアント証明書を 2 段以上のチェーン構成でアップロードしてください。

- 。 アップロード対象のクライアント証明書が自己署名証明書でない。
- 。「証明書ファイルアップロード時の検証項目追加」が有効である。
- ・ 「証明書ファイルアップロード時の検証項目追加」が有効の場合、接続先サーバに設定するサーバ証明書には2段以上のチェーン構成の証明書を使用してください。自己署名証明書を使用した場合、通信に失敗することがあります。

注※3

鍵管理サーバの場合、この検証項目は検証対象外です。

注※4

クライアント証明書ファイルを PEM 形式または DER 形式でアップロードする場合にのみ検証します。

G.2.2 外部サーバとの通信時に実施する証明書検証項目

ストレージシステムは外部サーバと通信する際、サーバから受信した証明書チェーンの有効性を検証します。検証項目を、次に示します。

検証項目

- ・ 証明書の要件を満たしていること。
- ・ 証明書が失効していないこと。
- ・ 証明書の有効期限が期限切れでないこと。
- ・ 証明書チェーンに含まれるすべての証明書の署名が正しいこと。
- ・ 証明書チェーンの段数が20段以内で構築されていること。



メモ

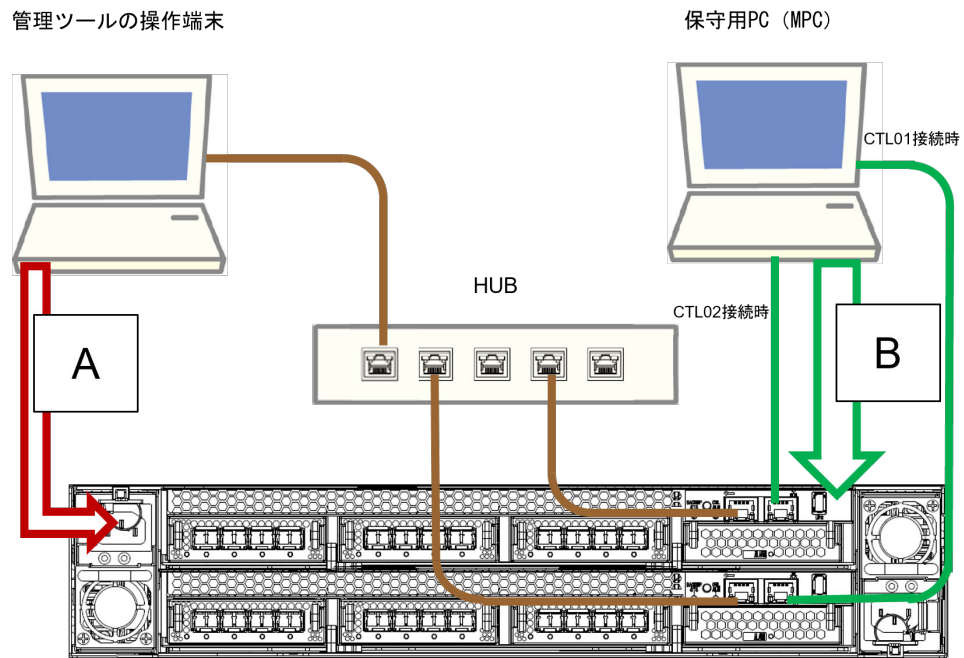
- ・ サーバ証明書の失効検証方法には、CRL または OCSP を用いた方法があります。
- ・ CRL を用いて失効検証をする場合、CRL リポジトリの URI (Uniform Resource Identifier) が中間証明書とサーバ証明書の cRLDistributionPoint (CRL 配布点) に設定されている必要があります。また、ルート証明書、中間証明書の拡張属性 (keyUsage) に cRLSign が設定されている必要があります。
- ・ OCSP を用いて失効検証をする場合、OCSP レスポンダの URI が中間証明書とサーバ証明書の authorityInfoAccess (機関アクセス情報) に設定されている必要があります。また、OCSP レスポンスで提示される OCSP 証明書に OCSP Signing Purpose (1.3.6.1.5.5.7.3.9) が設定されている必要があります。
- ・ サーバ証明書の失効検証をする場合、CRL リポジトリまたは OCSP レスポンダが、ストレージシステムからアクセスできるネットワーク上に存在し、ストレージシステムと通信できる状態にしてください。ストレージシステムと、CRL リポジトリや OCSP レスポンダが通信できない場合、外部サーバに接続できません。

G.3 ストレージシステムと管理ツールの操作端末間の SSL/TLS 通信

ストレージシステムでは、次の図に示す接続経路で、SSL/TLS 通信を使用します。

SSL/TLS 通信で使用する暗号プロトコルは TLS バージョン 1.2 と TLS バージョン 1.3 です。

図 2 SSL/TLS 通信の接続経路



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
VSP One Block Administrator などの管理ツールを使用する	A	管理ツールの操作端末とストレージシステム間	maintenance utility、VSP One Block Administrator、内蔵 CLI、ExportTool2 の操作、および REST API へのアクセスなど
保守員が保守用 PC (MPC) を使用する	B	保守用 PC とストレージシステム間	保守員による保守操作

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
VSP One Block Administrator などの管理ツールを使用する	A	Web サーバ接続用証明書 (PEM 形式または DER 形式)	ストレージシステム
保守員が保守用 PC (MPC) を使用する	B	MPC 接続用証明書 (PEM 形式または DER 形式)	ストレージシステム

管理モデルで使用する証明書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※
VSP One Block Administrator などの管理ツールを使用する	A	管理ツールの操作端末とストレージシステム間	- 次のいずれかの暗号スイートを使用できます。 - TLS バージョン 1.3 の場合 - TLS_AES_128_GCM_SHA256 - TLS_AES_256_GCM_SHA384 - TLS バージョン 1.2 の場合

管理モデル	記号	接続経路	暗号スイート※
			◦ TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 ◦ TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 ◦ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ◦ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ◦ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 ◦ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

注※

「[G.13 TLS セキュリティ設定を管理する](#)」に示す操作により、使用できる暗号スイートの絞り込みができます。

SSL/TLS 通信する際、管理モデルで使用する鍵交換での鍵長を、次に示します。

管理モデル	記号	接続経路	鍵長※
VSP One Block Administrator などの管理ツールを使用する	A	管理ツールの操作端末とストレージシステム間	次のいずれかの鍵長を使用できます。 • 鍵交換アルゴリズム DHE の場合 ◦ 2048bit ◦ 3072bit ◦ 4096bit • 鍵交換アルゴリズム ECDHE の場合 ◦ secp256r1 ◦ secp384r1 ◦ secp521r1

注※

「[G.13 TLS セキュリティ設定を管理する](#)」に示す操作により、各アルゴリズムで使用可能な下限鍵長を設定できます。

管理モデルでサポートする証明書の署名アルゴリズム、鍵長、ハッシュアルゴリズムを、次に示します。

管理モデル	記号	接続経路	署名アルゴリズム・鍵長・ハッシュアルゴリズム※
VSP One Block Administrator などの管理ツールを使用する	A	管理ツールの操作端末とストレージシステム間	• 署名アルゴリズムが RSA、かつ、鍵長が 2048/3072/4096bits の場合 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512 • 署名アルゴリズムが ECDSA、かつ、鍵長が secp256r1 (P-256) の場合 ◦ SHA-256 • 署名アルゴリズムが ECDSA、かつ、鍵長が secp384r1 (P-384) の場合 ◦ SHA-384 • 署名アルゴリズムが ECDSA、かつ、鍵長が secp521r1 (P-521) の場合

管理モデル	記号	接続経路	署名アルゴリズム・鍵長・ハッシュアルゴリズム※
			。 SHA-512

注※

「[G.13 TLS セキュリティ設定を管理する](#)」に示す操作で、セキュリティモードを設定することにより、署名アルゴリズム、鍵長、およびハッシュアルゴリズムの絞り込みができます。



メモ

- アップロードする証明書の証明書チェーンの階層数は、ルート CA 証明書を含めて 20 階層以下です。
- 証明書をアップロードする際、[コモンクライトリア認証設定] で「証明書ファイルアップロード時の検証項目追加」が有効な場合にのみ次の検証が実施されます。
 - 証明書チェーンに含まれるすべての証明書の署名が正しいこと。
 - 「[表 5 証明書の要件](#)」に示す#6（拡張属性（basicConstraints））の要件を満たしていること。
- 次の条件をすべて満たす場合は、必ずサーバ証明書を 2 段以上のチェーン構成でアップロードしてください。
 - アップロード対象のサーバ証明書が自己署名証明書でない。
 - 「証明書ファイルアップロード時の検証項目追加」が有効である。
- ストレージシステムとエクスポートツール 2 の SSL/TLS 通信では、通信時に証明書の検証が行われます。アップロードしたサーバ証明書が、「[表 5 証明書の要件](#)」を満たしていない場合、通信が失敗することがあります。

G.4 SSL/TLS 通信の設定の流れ

SSL/TLS 通信に必要な設定の流れを次に示します。

作業項目	操作方法、参照先		必須/任意
	OpenSSL	maintenance utility	
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。OpenSSL のバージョンは 3.0.7 以降を使用してください。	—	任意
秘密鍵の作成	「 G.5 秘密鍵を作成 」	「 G.9 CSR 作成および自己署名証明書作成 」	必須
公開鍵の作成	「 G.6 公開鍵を作成 」		必須
署名付き証明書の取得	- 自己署名付きの証明書の場合：「G.7 署名付き証明書を取得」 - 認証局発行の証明書の場合：「G.8 署名付きの信頼できる証明書を取得」		必須
証明書アップロードの前処理	「 G.10 SSL/TLS 証明書を PKCS#12 形式に変換 」		必須※
証明書のアップロード	「 D.11.3 Web サーバ接続用証明書をストレージシステムへアップロード 」		必須

作業項目	操作方法、参照先		必須/任意
	OpenSSL	maintenance utility	
TLS セキュリティ設定の変更	・ 「 G.13 TLS セキュリティ設定を管理する 」		任意
トラブルシュート	「 G.14 セキュリティ警告が表示されたときの対処方法 」		—

注※

PEM 形式の証明書ファイルと秘密鍵ファイルを合わせて使用する場合のみ

G.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。
2. OpenSSL をインストールした場合は、openssl フォルダのプロパティを表示し、読み込み専用属性が付いている場合は解除します。
3. Windows のコマンドプロンプトを起動します。
4. カレントディレクトリを鍵ファイルを出力するフォルダ（例:C:\key）に移動し、次に示すコマンドを実行します。

OpenSSL をインストールした場合：C:\key>c:\openssl\bin\openssl genrsa -out server.key 2048

秘密鍵として、server.key ファイルが C:\key フォルダに作成されます。

G.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 req -new -noenc -out c:\key\server.csr -keyout c:\key\server.key -config c:\key\req.txt
```

req.txt の例を示します。

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

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

```
[req_ext]
```

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

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

`extendedKeyUsage` には証明書の使用用途を設定します。サーバ認証用途で使用する場合は `serverAuth` を設定し、クライアント認証用途で使用する場合は `clientAuth` を設定してください。

`basicConstraints` には CA フラグを設定します。自己署名証明書を作成する場合は、自己を署名するために `CA:TRUE` を設定してください。

`[alt_names]`以降に表示される `DNS.1` にストレージシステムのホスト名を、`IP.1` にはストレージシステムの IP アドレスを入力してください。この項目に入力した名称が、SSL/TLS 通信をするときのサーバ名称（ホスト名）になります。サーバ名称は任意に決定できますが、入力したサーバ名称とストレージシステムの名称（ホスト名）を一致させてください。

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

G.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、管理ツールの操作端末をホスト名で指定してください。また、別途費用がかかります。

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

自己署名付きの証明書を取得する

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

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

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



メモ

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

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

G.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。

G.9 CSR 作成および自己署名証明書作成

「[D.11.4 maintenance utility](#) を利用して秘密鍵および公開鍵を生成する」を参照してください。

G.10 SSL/TLS 証明書を PKCS#12 形式に変換

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

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



メモ

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

前提条件

- 秘密鍵と SSL/TLS 証明書を同じフォルダに格納していること。

操作手順

- Windows のコマンドプロンプトを管理者権限で起動します。
- 次のコマンドを実行します。

```
OpenSSL をインストールした場合：C:\key>c:\openssl\bin\openssl△pkcs12△-export△-in△client.crt△-inkey△client.key△-out△client.p12
```

△：半角スペース

- 任意のパスワードを入力します。

このパスワードは、PKCS#12 形式の SSL/TLS 証明書をストレージシステムにアップロードするときに使用します。

PKCS#12 形式の SSL/TLS 証明書を作成するときのパスワードに使用できる文字は、次のとおりです。128 文字以下の文字列で指定します。

A~Z a~z 0~9 ! # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

- C:\key フォルダに、client.p12 ファイルが作成されます。この client.p12 ファイルが PKCS#12 形式に変換された SSL/TLS 証明書です。

5. コマンドプロンプトを閉じます。

G.11 Web サーバ接続用証明書をストレージシステムへアップロード

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

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

詳細は、「[D.11.3 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](#)」を参照してください。

G.12 詳細 API サーバ間の SSL 通信用の証明書を詳細 API サーバへアップロード

VSP Block Storage REST API リファレンスガイド「証明書ファイルをアップロードする (外部サーバー検証用)」の API を使って、詳細 API サーバ間の SSL 通信で使用する証明書をアップロードします。



メモ

詳細 API サーバ間の SSL 通信で使用する証明書の検証機能は、VSP Block Storage REST API リファレンスガイド「証明書ファイルをアップロードする (外部サーバー検証用)」の API を利用して、初めてルート証明書をアップロードしたときに有効になります。有効になった証明書検証機能は無効にすることはできません。複数の通信先のサーバを利用していた場合、どれかの通信先のサーバのルート証明書をアップロードした時点ですべての通信先のサーバの証明書の検証機能が有効になります。通信先のサーバが検証できなかった場合は通信に失敗します。

G.12.1 詳細 API での操作手順

ここでは、各手順のリクエストラインのみ説明します。リクエストラインの設定情報、参照情報については『VSP Block Storage REST API リファレンスガイド』を参照してください。

前提条件

- 実行ユーザにセキュリティ管理者 (参照・編集) が割り当てられていること。

操作手順

1. 証明書ファイルをアップロードします。

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

2. 証明書ファイルがアップロードされたことを確認します。

```
GET <ベース URL>/v1/objects/server-verification-certificates
```

G.13 TLS セキュリティ設定を管理する

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

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

プロトコル	ポート番号
HTTPS	443



メモ

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

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

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

G.13.1 SSL/TLS 通信のセキュリティ設定項目

次に示す項目を設定できます。

- SSL/TLS 通信のセキュリティモード

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

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

プロトコル	暗号スイート	CNSA1.0 モード 有効時	デフォルト値
TLS1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	選択不可	有効
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	選択可	有効
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	選択不可	有効
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	選択可	有効
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	選択不可	有効

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

- SSL/TLS 通信時の鍵交換で許可する、最小の鍵長

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



注意

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

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

G.13.2 SSL/TLS 通信のセキュリティ設定を変更する

SSL/TLS 通信のセキュリティ設定操作手順は、「[D.11.15 TLS セキュリティ設定を管理する](#)」を参照してください。

G.13.3 SSL/TLS 通信のセキュリティ設定を初期化する

管理ツールの操作端末と ESM を SSH 接続すると、内蔵 CLI で SSL/TLS 通信のセキュリティ設定を初期化できます。「[D.11.15 TLS セキュリティ設定を管理する](#)」で設定変更した結果、maintenance utility に接続ができなくなってしまう場合に操作してください。

前提条件

必要なロール：セキュリティ管理者（参照・編集）ロール、または保守（ベンダ専用）ロール

操作手順

1. 管理ツールの操作端末と ESM を SSH 接続します。
2. `mgmtcom tlssettingreset` を実行します。
完了メッセージが表示されます。
3. `maintenance utility` にログインします。
4. 画面左下の [メニュー] — [システム管理] — [TLS セキュリティ選択] を選択します。
[TLS セキュリティ選択] 画面が表示されます。
5. TLS セキュリティ設定の各項目が、デフォルトの値に初期化されていることを確認します。

G.14 セキュリティ警告が表示されたときの対処方法

SSL/TLS 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。

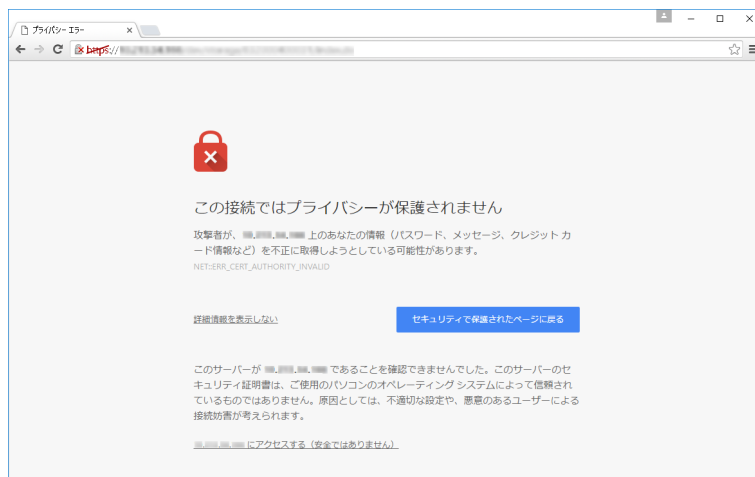
Microsoft Edge の場合の警告表示例 (Web ブラウザのバージョンにより表示が異なる場合があります。)



< 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/TLS 対応に設定された VSP One Block Administrator や maintenance utility 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。



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](#)
- [H.2 iSCSI、NVMe/TCP ホスト](#)

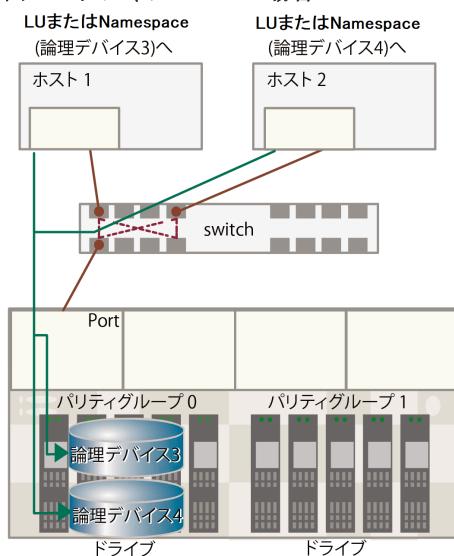
H.1 Fibre Channel ホスト

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

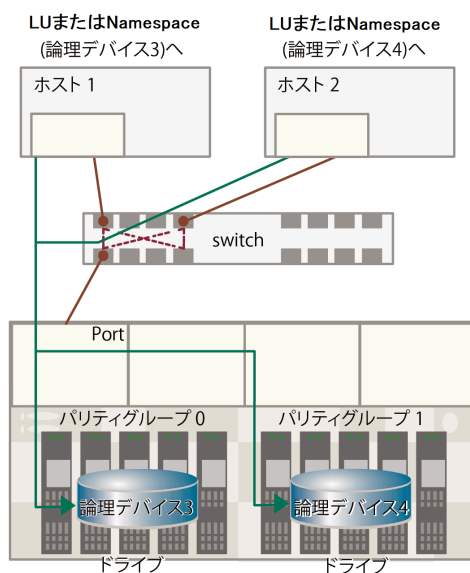
複数のホストを 1 台のストレージシステムに接続したとき、それぞれのホストに割り当てられた論理デバイスが同じパリティグループに存在すると、同じドライブへのアクセスが発生します。このときドライブへのアクセスが競合し、性能が劣化する可能性があります。

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。

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、Solaris、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 6 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。 Target ポートの場合、ポート当たり 最大 2048、Bidirectional ポートの場合、ポート当たり最大 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、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、NVMe/TCP ホスト

iSCSI、NVMe/TCP 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、NVMe/TCP の概要

日立がサポートする Ethernet Channel Board は、TCP/IP 上で動作する iSCSI または NVMe/TCP プロトコルを用いて、ホストと通信できます。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。
- iSCSI ポートまたは NVMe/TCP 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。
- ファームウェア更新中のリブート時や、障害発生中のリセット時、ホスト I/O を継続させるためにマルチパス構成で接続してください。このためストレージシステムには冗長パスが必要となります（詳細は「[\(1\) ホストとストレージシステムの接続構成に関する注意事項](#)」を参照）。
- Ethernet 25Gbps チャンネルボードを使用する場合、ファームウェアの更新時や、障害発生中に交替パスの障害が発生した場合のアクセスロスに備えて、ホスト側のパラメータ設定が必要となります（詳細は「[\(2\) ホスト OS とマルチパスソフトウェアに関する注意事項](#)」を参照）。
- iSCSI ポートを適用する場合、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できます。LUN Manager を併用すれば、複数のターゲットごとに CHAP によるホスト認証および双方向認証を設定できます。

H.2.2 iSCSI、NVMe/TCP I/F の仕様

表 7 iSCSI、NVMe/TCP I/F 仕様

プロトコル層	項目	仕様
全般	iSCSI、NVMe/TCP ターゲット機能	サポート
	iSCSI、NVMe/TCP イニシエータ機能	サポート

プロトコル層	項目	仕様
		ただし、100Gbps Channel Board ではサポートしていません。
	バス切替	- iSCSI の場合 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 詳しくは、弊社担当営業までお問い合わせください。 - NVMe/TCP の場合 Linux : NVMe Native MultiPath を使用可能 VMware : High Performance Plugin (HPP) を使用可能 詳しくは、弊社担当営業までお問い合わせください。
	接続ホスト（コネクション/サブシステム）数	- Ethernet 25Gbps チャンネルボードの場合 255 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。 - Ethernet 100Gbps チャンネルボードの場合 255 サブシステム/Port 接続数が多くなると、NVMe/TCP Port への負荷が増大するため、127 サブシステム/Port 以下での接続を推奨します。
物理層、MAC 層	リンク	『ハードウェアリファレンスガイド』の「ハードウェア詳細仕様」を参照してください。
	転送速度	『ハードウェアリファレンスガイド』の「ハードウェア詳細仕様」を参照してください。
	コネクタ形状	『ハードウェアリファレンスガイド』の「ハードウェア詳細仕様」を参照してください。
	ケーブル	『ハードウェアリファレンスガイド』の「ハードウェア詳細仕様」を参照してください。
	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 (10GBASE-SR) 準拠 25Gbps : IEEE802.3by (25GBASE SR SFP28) 準拠 100Gbps (Optic) : IEEE802.3bm (100GBASE-SR4) 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

プロトコル層	項目	仕様
		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	- iSCSI の場合 : 3260 (デフォルト) - NVMe/TCP の場合 : Discovery Controller 8009 (デフォルト) IO Controller 4420 (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。 - アクセスするホストの設定も変更してください。 - 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。 - NVMe/TCP の IO Controller では、設定可能な範囲は 49152～65535 (Discovery Controller で使用しているポート番号を除く) となります。
	Fragment	未サポート
	Window Scale	サポート - iSCSI の場合 Window Size 64KB/128KB/256KB (デフォルト) / 512KB/1MB/2MB - NVMe/TCP の場合 Window Size 64KB/128KB/256KB/512KB/1MB (デフォルト) /2MB
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 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)

プロトコル層	項目	仕様
		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。
NVMe/TCP	Header digest、Data digest	サポート 通信のヘッダ、データ情報をエラーから保護します。 NVMe/TCP 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）。

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.1994-04.jp.co.hitachi:rsd.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 Ethernet (iSCSI、NVMe/TCP) 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
- 10Gbps (Optic) 接続 :
 - IEEE 802.3ae 10GBASE-SR
- 25Gbps 接続 :

- IEEE 802.3by 25GBASE-SR
- 100Gbps 接続：
 - IEEE 802.3bm 100GBASE-SR4
- 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

Ethernet (iSCSI、NVMe/TCP) 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 ポートまたは NVMe/TCP ポート／ストレージシステムの CTL／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、NVMe/TCP 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、NVMe/TCP が阻害します。
 - iSCSI、NVMe/TCP 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、NVMe/TCP 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、NVMe/TCP 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、NVMe/TCP 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 ポートまたは NVMe/TCP ポートや単一の CTL 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 ポートまたは NVMe/TCP 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 ポートまたは NVMe/TCP ポートから同時に 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 ポートまたは NVMe/TCP 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 ポートまたは NVMe/TCP 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、NVMe/TCP 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、NVMe/TCP の転送性能低下または応答時間遅延に繋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、NVMe/TCP 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 ポートまたは NVMe/TCP ポート設定
ホスト接続の状態では iSCSI ポートまたは NVMe/TCP ポート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 ポートまたは NVMe/TCP ポート設定変更後 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 ポートまたは NVMe/TCP ポートの 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 や NVMe/TCP への接続に遅延が生じる場合があります。
iSCSI ポートまたは NVMe/TCP ポートの 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、NVMe/TCP software initiator と NIC で iSCSI、NVMe/TCP プロトコルの通信をする場合は、iSCSI、NVMe/TCP 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、NVMe/TCP Digest 設定を有効にすることで、iSCSI、NVMe/TCP Data Digest および iSCSI、NVMe/TCP 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、NVMe/TCP 構成において iSCSI、NVMe/TCP Header Digest および iSCSI、NVMe/TCP 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、NVMe/TCP 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、NVMe/TCP 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。

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。
- 1 つの iSCSI ポートで同時に最大 255 コネクションの通信ができます。そのため最大 255 ホストとの通信ができます。ただし、Linux software initiator (RHEL5.0 未満) では、1 ホストからの接続に 2 つのコネクションを確立するため通信相手に含まれる場合は、その特性により接続できるホスト数の上限が減少します。例えばすべてのホストが Linux software initiator (RHEL5.0 未満) を用いる場合は、1 つの iSCSI ポートは最大 127 ホストと通信できます。

Solaris ホスト

- 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。これによりホストの不要な通信や負荷を軽減します。

H.2.6 Ethernet 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 8 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 ドライバまたは NVMe/TCP ドライバの設定を確認してください。
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 または NVMe/TCP 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。 Router Advertisement (RA) を使用して、Ethernet 25Gbps チャネルボードのデフォルトゲートウェイを自動で設定した場合、デフォルトゲートウェイの IP アドレスは手動で設定できません。
11	ホストが iSCSI ドライバまたは NVMe/TCP ドライバを認識できていますか？
12	- iSCSI の場合 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？ - NVMe/TCP の場合 ホストから Target に誤った IP アドレスと Host NQN 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。

項番	確認項目
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	- iSCSI の場合 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。 - NVMe/TCP の場合 Namespace 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 Host NQN のリストに、接続する Initiator の Host NQN がありますか？リストにない場合、接続する Initiator の Host NQN 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 9 IPv6 接続障害対策表

確認項目		対策
接続する iSCSI Port または NVMe/TCP 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 または NVMe/TCP 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 または NVMe/TCP Port 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 または NVMe/TCP 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。
	無効	iSCSI Port または NVMe/TCP Port がリンクダウンしている状態です。 iSCSI Port または NVMe/TCP 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 または NVMe/TCP 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 または NVMe/TCP Port の IPv6 アドレスが、同一 iSCSI Port または NVMe/TCP Port 内でアドレス重複している状態です。

確認項目		対策
		iSCSI Port または NVMe/TCP Port の IPv6 アドレスには、iSCSI Port または NVMe/TCP 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 または NVMe/TCP 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 または NVMe/TCP 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 または NVMe/TCP 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 Ethernet 25Gbps チャンネルボード使用時の注意事項

Ethernet 25Gbps チャンネルボードと接続可能なホストの OS を次に示します。

- Windows Server 2019/2022
- Red Hat Enterprise Linux
- SUSE Linux
- VMware ESXi (iSCSI イニシエータとして使用する場合)

ホストの OS に Red Hat Enterprise Linux または SUSE Linux を使用し、マルチパスソフトウェアに Hitachi Dynamic Link Manager を使用する場合は、次のバージョンを使用してください。

- Hitachi Dynamic Link Manager : 8.8.8 以降

(1) ホストとストレージシステムの接続構成に関する注意事項

ホストとストレージシステム間は、マルチパス構成で接続してください。このためストレージシステムには冗長パスが必要となります。

Ethernet 25Gbps チャンネルボードの場合、ファームウェア更新中のリブート時や障害発生中のリセット時に、I/O を再開するまで最大 130 秒程度を要します。この間もホスト I/O を継続させるために、マルチパス構成でホストと接続してください。



注意

シングルパス構成の場合は、ファームウェア更新中のリブート時や障害発生中のリセット時に、最大 130 秒程度の間、ホスト I/O を継続できなくなるため、ホストの I/O 停止またはホスト I/O エラーが発生するおそれがあります。

異なる CTL 上のチャンネルボードのポートを使用して、マルチパスを構成してください。異なる CTL 上のチャンネルボードを使用できない場合は、異なるチャンネルボードのポートを使用して、マルチパスを構成してください。

(2) ホスト OS とマルチパスソフトウェアに関する注意事項

ホスト OS とマルチパスソフトウェアに、障害からの回復を監視する時間を変更するためのパラメータを設定してください。

ファームウェア更新中のリブート時や障害発生中のリセット時に、交替パス側で障害が発生した場合は、リブートやリセットが完了するまでの間、両方のパスが一時的にアクセス不可の状態になります。

Ethernet 25Gbps チャンネルボードは、リブートに最大 130 秒程度を要します。この間に I/O が停止しても I/O エラーとならないように、障害からの回復を監視する時間を変更するためのパラメータ設定が必要です。



注意

ホストのパラメータを設定していない場合に、ファームウェア更新中のリブート時や障害発生中のリセット時に、交替パス側で障害が発生すると、I/O 停止またはホスト I/O エラーが発生するおそれがあります。

パラメータ設定が必要なホスト OS とマルチパスソフトウェアを示します。

- Windows Server 2019/2022 (Microsoft DSM/MPIO または Hitachi Dynamic Link Manager)
- Red Hat Enterprise Linux (Device Mapper Multipath または Hitachi Dynamic Link Manager)
- SUSE Linux (Device Mapper Multipath または Hitachi Dynamic Link Manager)

なお、VMware でゲスト OS の iSCSI イニシエータを利用する場合は、ゲスト OS の Windows や Red Hat Enterprise Linux、SUSE Linux に、同様のパラメータ設定が必要です。

VMware ESXi を iSCSI イニシエータとして使用する場合、パラメータ設定は不要です。

(3) Windows Server 2019/2022 (Microsoft DSM/MPIO または Hitachi Dynamic Link Manager) のパラメータ設定の例

レジストリに設定されている PDORemovePeriod の値を 115 以上に設定してください。



メモ

ホストが、I/O の停止を検知してパスが切断されたと判断するまでの時間 (35 秒) を起点に、障害からの回復を監視する時間を、パラメータに設定します。なお、チャンネルボードのファームウェア更新中のリブートや障害発生中のリセットに要する時間は 130 秒ですが、ホストやネットワークの処理時間を考慮して、150 秒となる時間 (115 秒) を設定します。

操作手順

1. Windows の PowerShell を起動します。
2. Get-MPIOSetting コマンドで、PDORemovePeriod の値を確認します。

```
PS C:\Users\Administrator> Get-MPIOSetting

PathVerificationState      : Disabled
PathVerificationPeriod     : 30
PDORemovePeriod           : 20
RetryCount                 : 3
RetryInterval              : 1
UseCustomPathRecoveryTime  : Disabled
CustomPathRecoveryTime     : 40
DiskTimeoutValue           : 60
```

PDORemovePeriod の値が、115 以上の場合は、変更不要です。

PDORemovePeriod の値が、115 未満の場合は、以降の手順に従って 115 以上に設定してください。

3. 次のコマンドを実行します（PDORemovePeriod の値を 115 に設定する例を示します）。

```
Set-MPIOSetting -NewPDORemovePeriod 115
```

4. Get-MPIOSetting コマンドで、PDORemovePeriod の値が変更されたことを確認します。

```
PS C:\Users\Administrator> Get-MPIOSetting

PathVerificationState      : Disabled
PathVerificationPeriod     : 30
PDORemovePeriod           : 115
RetryCount                 : 3
RetryInterval              : 1
UseCustomPathRecoveryTime  : Disabled
CustomPathRecoveryTime     : 40
DiskTimeoutValue           : 60
```

5. ホスト OS をリブートします。

(4) Red Hat Enterprise Linux (Device Mapper Multipath) のパラメータ設定の例

Device Mapper Multipath のパラメータ no_path_retry の値を 30 以上に設定してください。



メモ

ホストは障害の発生を 5 秒間隔で監視します。また、障害を監視する回数をパラメータに設定します。なお、チャンネルボードのファームウェア更新中のリブートや障害発生中のリセットに要する時間は 130 秒ですが、ホストやネットワークの処理時間を考慮して、150 秒となる回数（30）を設定します。

操作手順

1. ストレージシステムのデバイスに対して no_path_retry を設定するため、/etc/multipath.conf に、パラメータ no_path_retry を追記します。次に no_path_retry の値を 30 に設定する例を示します。

全デバイスに共通する設定とする場合：defaults セクションに追記

```
defaults {
    no_path_retry 30
    find_multipaths yes
    user_friendly_names yes
}
```

デバイスごとに設定する場合：devices セクションに device を追記

```
devices {
    device {
```

```
vendor "HITACHI"
product "^OPEN-"
path_grouping_policy "multibus"
no_path_retry 30
}
```

2. 次のコマンドを実行して、変更後の設定を有効にします。

```
# systemctl reload multipathd.service
```

(5) Red Hat Enterprise Linux (Hitachi Dynamic Link Manager) のパラメータ設定の例

Hitachi Dynamic Link Manager のパラメータ `ErrorPathRetry` の値を 5 以上に設定してください。

Hitachi Dynamic Link Manager のパラメータ `ErrorPathDelay` の値を 30 以上に設定してください。



メモ

障害が発生したパスに対して、I/O を試行する回数と、I/O を試行するまでの待ち時間を、パラメータに設定します。なお、チャンネルボードのファームウェア更新中のリブートや障害発生中のリセットに要する時間は 130 秒ですが、ホストやネットワークの処理時間を考慮して、150 秒となるように、I/O を試行する回数（5 回）と障害パスで I/O を試行するまでの待ち時間（30 秒）を設定します。

操作手順

1. Hitachi Dynamic Link Manager (HDLM) ドライバオプション設定ユーティリティ (`dlnmsetopt`) を使用して、`ErrorPathRetry` に「5」を設定します。

HDLM が `/opt` の下にインストールされている例

```
# /opt/DynamicLinkManager/bin/dlnmsetopt -epr 5
```

実行結果

```
KAPL12554-I The utility for setting HDLM driver option has started.
KAPL12555-I The utility for setting HDLM driver option completed normally.
KAPL12558-I Please restart the computer so that the option settings take effect.
```

2. `dlnmsetopt` を使用して、`ErrorPathDelay` に「30」を設定します。

```
# /opt/DynamicLinkManager/bin/dlnmsetopt -epd 30
```

操作手順 1. と同じ実行結果が表示されます。

3. ホスト OS をリブートします。

(6) SUSE Linux (Device Mapper Multipath または Hitachi Dynamic Link Manager) のパラメータ設定の例

Red Hat Enterprise Linux (Device Mapper Multipath または Hitachi Dynamic Link Manager) の場合と同様のパラメータを設定してください。

(7) Ethernet 25Gbps チャンネルボードのポートに関する注意事項

- 複数のポートに同じ IP アドレスを設定できません。このため LACP (IEEE 802.3ad Link Aggregation Control Protocol) も適用できません。

- ・ リモートパス、外部パス用のポートとして使用できません。
- ・ 転送速度に、Auto ネゴシエーションを設定できません。
接続先の NIC やスイッチのポートの転送速度に合わせて、CHB ポートの転送速度を 10Gbps、または 25Gbps に設定してください。
- ・ 選択型 ACK は有効に設定されています。無効にできません。
- ・ Router Advertisement (RA) を使用して、デフォルトゲートウェイを自動で設定する場合、デフォルトゲートウェイの IP アドレスを、手動で設定しないでください。手動で設定すると、同一ネットワーク内に複数の IPv6 ルータが存在する場合には、性能遅延が発生する可能性があります。手動による設定は、次の方法で回避できます。
 - RAID Manager を使用する場合 : raidcom modify port コマンドに対して、IP アドレスを指定するオプションを使用しない。

H.2.8 Ethernet 100Gbps チャンネルボードを使用する場合の注意事項

(1) 接続可能なホスト

Ethernet 100Gbps チャンネルボードと接続可能なホストの OS を次に示します。

- ・ Red Hat Enterprise Linux 9 以降
- ・ SUSE Linux 15 SP2 以降
- ・ Oracle Enterprise Linux 7.9 UEK6 以降
- ・ Oracle Enterprise Linux 8.2 UEK6 以降
- ・ VMware ESXi 8.0 Update 3 以降 (NVMe/TCP イニシエータとして使用する場合)

(2) ホストとストレージシステムの接続構成に関する注意事項

ホストとストレージシステムの接続構成に関する注意事項

1. マルチパス接続の推奨

ホストとストレージシステム間は、マルチパス構成で接続してください。このためストレージシステムには冗長パスが必要となります。

Ethernet 100Gbps チャンネルボードの場合、ファームウェア更新中のリブート時や障害発生中のリセット時に、I/O を再開するまで最大 130 秒程度を要します。この間もホスト I/O を継続させるために、マルチパス構成でホストと接続してください。



注意

シングルパス構成の場合は、ファームウェア更新中のリブート時や障害発生中のリセット時に、最大 130 秒程度の間、ホスト I/O を継続できなくなるため、ホストの I/O 停止またはホスト I/O エラーが発生するおそれがあります。

2. ポートに関する注意事項

- ・ 複数のポートに同じ IP アドレスを設定できません。このため LACP (IEEE 802.3ad Link Aggregation Control Protocol) も適用できません。
- ・ リモートパス、外部パス用のポートとして使用できません。
- ・ 転送速度に、Auto ネゴシエーションを設定できません。
CHB ポートの転送速度を 100Gbps に設定してください。
- ・ 選択型 ACK は有効に設定されています。無効にできません。

- Route Advertisement(RA)を使用して、デフォルトゲートウェイを自動で設定する場合、デフォルトゲートウェイの IP アドレスを、手動で設定しないでください。手動で設定すると、同一ネットワーク内に複数の IPv6 ルータが存在する場合に、性能遅延が発生する可能性があります。なお、手動で設定する場合は、RAID Manager の `raidcom modify port` コマンドに対して、IP アドレスを指定するオプションを設定しないでください。

H.2.9 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。



ASSIST の構成

ASSIST（遠隔保守支援システム）は、ストレージシステムの障害発生時に障害情報を ASSIST センタに自動通報することで、迅速な障害対応を支援するサービスです。

ここでは ASSIST の構成について説明します。なお ASSIST を利用するには、保守会社とサービスを締結する必要があります。

□ 1.1 ASSIST の構成

I.1 ASSIST の構成

ASSIST 対応に必要なシステム構成を以下に示します。ASSIST は、管理 LAN（顧客 LAN）と保守 LAN のいずれのネットワークにも対応します。

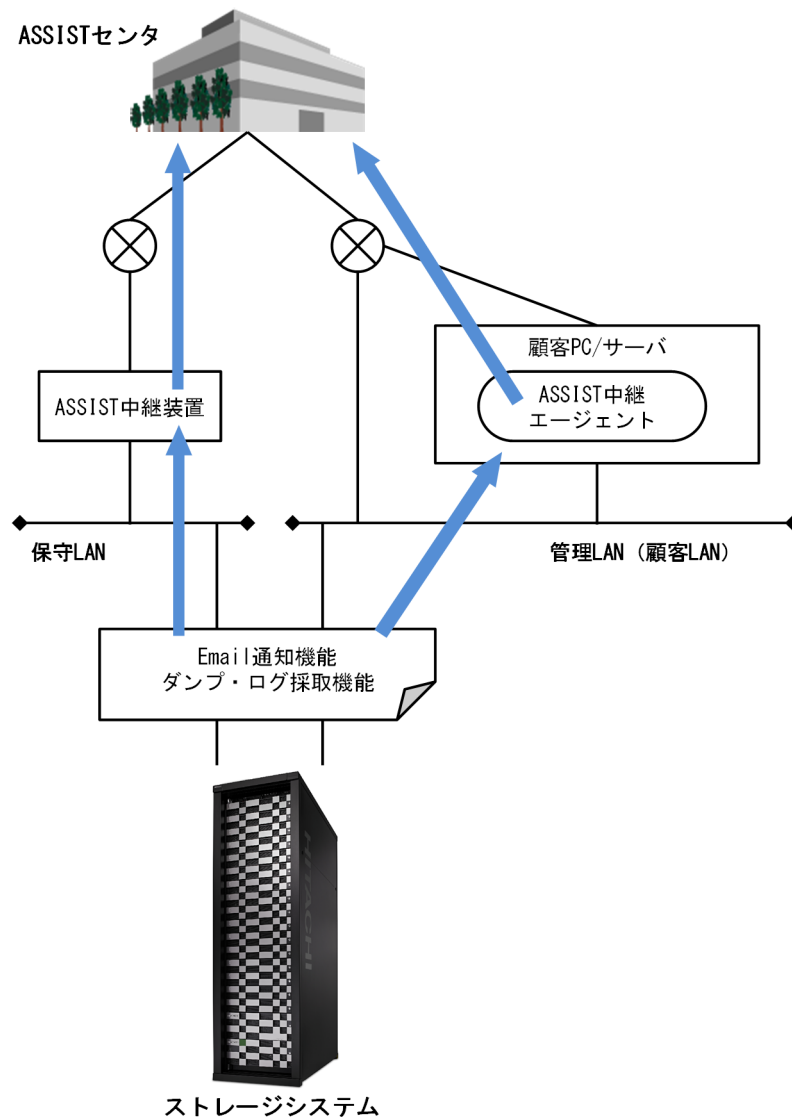


表 10 各機器・ソフトウェアの説明

機器・ソフトウェア	説明
ストレージシステム	保守の対象となるストレージシステム
- ASSIST 中継装置 - ASSIST 中継エージェント	Email 通知などの情報を ASSIST センタに中継するための装置またはソフトウェア
ASSIST センタ	ストレージシステムを監視して、障害対応を支援するためのサービス拠点



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。

- [J.1 障害通知メールの内容](#)
- [J.2 Syslog メッセージの内容](#)
- [J.3 SNMP メッセージの内容](#)

J.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

```
StorageSystem Report
//StorageSystem //////////////////////////////////////
//e-Mail Report
////////////////////////////////////
Date : 20/04/2018
Time : 00:20:00
Machine : StorageSystem(Serial# 800001)
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	StorageSystem Report	(ストレージシステムの装置名) + Report
付加情報	//StorageSystem ////////////////////////////////////// //e-Mail Report ////////////////////////////////////	「 D.3.1 メール通知の設定 」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	StorageSystem(Serial# 800001)	「 D.3.1 メール通知の設定 」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。

J.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、「[D.3.3 アラート通知を蓄積するための Syslog の設定](#)」および「[D.7.1 監査ログを蓄積するための Syslog の設定](#)」を参照してください。

図 3 RFC3164 に準拠した syslog メッセージのフォーマット

```
<149>Jan 24 18:10:30 ESM Storage: 0000001571,Service,H2(Serial#800001),Japan-Tokyo,
1      2      3      4      5      6      7      8
RefCode:7FFA00,Synchronization time failure
9
```

表 11 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	「ESM」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 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	ストレージシステム名と、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。

注※

ログに出力される日付と時刻は、maintenance utility に設定された日付と時刻です。ストレージシステム内で ESM 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 4 RFC5424 に準拠した syslog メッセージのフォーマット

```
<149>1 2017-01-24T18:17:09.0+09:00 ESM Storage --- 0000001572,Service,H2(Serial#8000001),
Japan-Tokyo, RefCode:7FFA00,Synchronization time failure
```

1 2 3 4 5 6 7 8 9 10 11 12 13

表 12 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 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	「ESM」 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

項番	項目	説明
		Severity は 5 です。
11	ハードウェア識別情報	ストレージシステム名と、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。

注※

ログに出力される日付と時刻は、maintenance utility に設定された日付と時刻です。ストレージシステム内で ESM 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。

J.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、『障害通知ガイド』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 5 SNMP の表示例

The screenshot shows a window titled 'イベントログ詳細' (Event Log Details). It contains several input fields and buttons. The '発生日時' (Occurrence Date/Time) is '2023/08/11 11:28:02'. The '状態' (Status) is '重度' (Severe). The '種別' (Type) is 'TRAP'. The '関連ノード' (Related Node) is '10.164.137.101'. There are buttons for '前のイベント' (Previous Event), '次のイベント' (Next Event), '通知登録' (Notification Registration), and '閉じる' (Close). A checkbox is checked with the label '前後のイベント検索は、同じ関連ノードについて行う。' (Search for events before and after for the same related node). The 'イベント内容' (Event Content) text area shows the following details:

```

sysUpTimeInstance = Timeticks: (72010) 0:12:00.10
TRAP種別 = OID: raideventUsermoderate
eventTrapSerialNumber = INTEGER: 800001
eventTrapNickname = STRING: "VSP One B28"
eventTrapREFCODE = STRING: "7d0300"
eventTrapPartsID = OID: dkchWEnvironment
eventTrapDate = STRING: "2023/08/12"
eventTrapTime = STRING: "13:28:58"
eventTrapDescription = STRING: "ESM audit log lost"

```

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	raideventUsermoderate	障害レベル
eventTrapSerialNumber	800001	装置製品番号
eventTrapNickname	"VSP One B80"	製品名
eventTrapREFCODE	"7d0300"	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	"2023/08/12"	SNMPAgent が受信した日付
eventTrapTime	"13:28:58"	SNMPAgent が受信した時間
eventTrapDescription	"ESM audit log lost"	保守作業に必要な不良個所の情報



ロケーションの対応表

MP#および Port とロケーションの対応表を示します。

□ K.1 MP#とロケーションの対応

K.1 MP#とロケーションの対応

MP#とロケーションの対応は次のとおりです。

- CBX ペア 0

DKC#	ロケーション			MP#	ロケーション			MP#
DKC0	CTL01	MPU-010	MP010-00	00	CTL02	MPU-020	MP020-00	14
			MP010-01	01			MP020-01	15
			MP010-02	02			MP020-02	16
			MP010-03	03			MP020-03	17
			MP010-04	04			MP020-04	18
			MP010-05	05			MP020-05	19
			MP010-06	06			MP020-06	1A
			MP010-07	07			MP020-07	1B
			MP010-08	08			MP020-08	1C
			MP010-09	09			MP020-09	1D
			MP010-0A	0A			MP020-0A	1E
			MP010-0B	0B			MP020-0B	1F
			MP010-0C	0C			MP020-0C	20
			MP010-0D	0D			MP020-0D	21
			MP010-0E	0E			MP020-0E	22
			MP010-0F	0F			MP020-0F	23
			MP010-10	10			MP020-10	24
			MP010-11	11			MP020-11	25
			MP010-12	12			MP020-12	26
			MP010-13	13			MP020-13	27
DKC1	CTL11	MPU-110	MP110-00	28	CTL12	MPU-120	MP120-00	3C
			MP110-01	29			MP120-01	3D
			MP110-02	2A			MP120-02	3E
			MP110-03	2B			MP120-03	3F
			MP110-04	2C			MP120-04	40
			MP110-05	2D			MP120-05	41
			MP110-06	2E			MP120-06	42
			MP110-07	2F			MP120-07	43
			MP110-08	30			MP120-08	44
			MP110-09	31			MP120-09	45
			MP110-0A	32			MP120-0A	46
			MP110-0B	33			MP120-0B	47
			MP110-0C	34			MP120-0C	48
			MP110-0D	35			MP120-0D	49

DKC#	ロケーション			MP#	ロケーション			MP#
			MP110-0E	36			MP120-0E	4A
			MP110-0F	37			MP120-0F	4B
			MP110-10	38			MP120-10	4C
			MP110-11	39			MP120-11	4D
			MP110-12	3A			MP120-12	4E
			MP110-13	3B			MP120-13	4F

- CBX ペア 1

DKC#	ロケーション			MP#	ロケーション			MP#
DKC2	CTL21	MPU-210	MP210-00	50	CTL22	MPU-220	MP220-00	64
			MP210-01	51			MP220-01	65
			MP210-02	52			MP220-02	66
			MP210-03	53			MP220-03	67
			MP210-04	54			MP220-04	68
			MP210-05	55			MP220-05	69
			MP210-06	56			MP220-06	6A
			MP210-07	57			MP220-07	6B
			MP210-08	58			MP220-08	6C
			MP210-09	59			MP220-09	6D
			MP210-0A	5A			MP220-0A	6E
			MP210-0B	5B			MP220-0B	6F
			MP210-0C	5C			MP220-0C	70
			MP210-0D	5D			MP220-0D	71
			MP210-0E	5E			MP220-0E	72
			MP210-0F	5F			MP220-0F	73
			MP210-10	60			MP220-10	74
			MP210-11	61			MP220-11	75
			MP210-12	62			MP220-12	76
			MP210-13	63			MP220-13	77
DKC3	CTL31	MPU-310	MP310-00	78	CTL32	MPU-320	MP320-00	8C
			MP310-01	79			MP320-01	8D
			MP310-02	7A			MP320-02	8E
			MP310-03	7B			MP320-03	8F
			MP310-04	7C			MP320-04	90
			MP310-05	7D			MP320-05	91
			MP310-06	7E			MP320-06	92
			MP310-07	7F			MP320-07	93
			MP310-08	80			MP320-08	94
			MP310-09	81			MP320-09	95

DKC#	ロケーション			MP#	ロケーション			MP#
			MP310-0A	82			MP320-0A	96
			MP310-0B	83			MP320-0B	97
			MP310-0C	84			MP320-0C	98
			MP310-0D	85			MP320-0D	99
			MP310-0E	86			MP320-0E	9A
			MP310-0F	87			MP320-0F	9B
			MP310-10	88			MP320-10	9C
			MP310-11	89			MP320-11	9D
			MP310-12	8A			MP320-12	9E
			MP310-13	8B			MP320-13	9F

• CBX ペア 2

DKC#	ロケーション			MP#	ロケーション			MP#
DKC4	CTL41	MPU-410	MP410-00	A0	CTL42	MPU-420	MP420-00	B4
			MP410-01	A1			MP420-01	B5
			MP410-02	A2			MP420-02	B6
			MP410-03	A3			MP420-03	B7
			MP410-04	A4			MP420-04	B8
			MP410-05	A5			MP420-05	B9
			MP410-06	A6			MP420-06	BA
			MP410-07	A7			MP420-07	BB
			MP410-08	A8			MP420-08	BC
			MP410-09	A9			MP420-09	BD
			MP410-0A	AA			MP420-0A	BE
			MP410-0B	AB			MP420-0B	BF
			MP410-0C	AC			MP420-0C	C0
			MP410-0D	AD			MP420-0D	C1
			MP410-0E	AE			MP420-0E	C2
			MP410-0F	AF			MP420-0F	C3
			MP410-10	B0			MP420-10	C4
			MP410-11	B1			MP420-11	C5
			MP410-12	B2			MP420-12	C6
			MP410-13	B3			MP420-13	C7
DKC5	CTL51	MPU-510	MP510-00	C8	CTL52	MPU-520	MP520-00	DC
			MP510-01	C9			MP520-01	DD
			MP510-02	CA			MP520-02	DE
			MP510-03	CB			MP520-03	DF
			MP510-04	CC			MP520-04	E0
			MP510-05	CD			MP520-05	E1

DKC#	ロケーション			MP#	ロケーション			MP#
			MP510-06	CE			MP520-06	E2
			MP510-07	CF			MP520-07	E3
			MP510-08	D0			MP520-08	E4
			MP510-09	D1			MP520-09	E5
			MP510-0A	D2			MP520-0A	E6
			MP510-0B	D3			MP520-0B	E7
			MP510-0C	D4			MP520-0C	E8
			MP510-0D	D5			MP520-0D	E9
			MP510-0E	D6			MP520-0E	EA
			MP510-0F	D7			MP520-0F	EB
			MP510-10	D8			MP520-10	EC
			MP510-11	D9			MP520-11	ED
			MP510-12	DA			MP520-12	EE
			MP510-13	DB			MP520-13	EF



用語解説

(英字)

AMC

(Array Management Controller)

HSNBX に搭載される ESM アプリケーションが動作するハードウェア。

ALUA

(Asymmetric Logical Unit Access)

SCSI の非対称論理ユニットアクセス機能です。

ストレージ同士、またはサーバとストレージシステムを複数の冗長パスで接続している構成の場合に、どのパスを優先して使用するかをストレージシステムに定義して、I/O を発行できます。優先して使用するパスに障害が発生した場合は、他のパスに切り替わります。

bps

(bits per second)

データ転送速度の標準規格です。

CBX

(Controller Box)

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

CC

(Concurrent Copy)

IBM 社の Concurrent Copy 機能のことです。

CHAP

(Challenge Handshake Authentication Protocol)

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

CHB

(Channel Board)

詳しくは「チャネルボード」を参照してください。

Child

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

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

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

CLPR

(Cache Logical Partition)

キャッシュメモリを論理的に分割すると作成されるパーティション（区画）です。

CM

(Cache Memory (キャッシュメモリ))

詳しくは「キャッシュ」を参照してください。

CNA

(Converged Network Adapter)

HBA と NIC を統合したネットワークアダプタ。

CRC

(Cyclic Redundancy Check)

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

CSV

(Comma-Separated Values)

データベースソフトや表計算ソフトのデータをファイルとして保存するフォーマットの 1 つで、主にアプリケーション間のファイルのやり取りに使われます。それぞれの値はコンマで区切られています。

CTG

(Consistency Group)

詳しくは「コンシステンシーグループ」を参照してください。

CU

(Control Unit (コントロールユニット))

主に磁気ディスク制御装置を指します。

CV

(Customized Volume)

任意のサイズに設定できる論理ボリュームです。

CYL

(Cylinder (シリンダ))

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

DKB

(Disk Board)

ドライブとキャッシュメモリ間のデータ転送を制御するモジュールです。

DKC

(Disk Controller)

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

DKU

(Disk Unit)

各種ドライブを搭載するためのシャーシ（筐体）です。

DP-VOL

詳しくは「仮想ボリューム」を参照してください。

EAV

(Extended Address Volume)

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

ECC

(Error Check and Correct)

ハードウェアで発生したデータの誤りを検出し、訂正することです。

ENC

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

ESE-VOL

(Extent Space - Efficient Volume)

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

ESM

(Embedded Storage Manager)

本ストレージシステムにおける管理系ソフトウェアです。

ESMOS

(Embedded Storage Manager Operating System)

ESM を動作させるための OS や OSS を含んだファームウェアです。

ExG

(External Group)

外部ボリュームを任意にグループ分けしたものです。詳しくは「外部ボリュームグループ」を参照してください。

External MF

詳しくは「マイグレーションボリューム」を参照してください。

External ポート

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

Failover

故障しているものと機能的に同等のシステムコンポーネントへの自動的置換。
この **Failover** という用語は、ほとんどの場合、同じストレージデバイスおよびホストコンピュータに接続されているインテリジェントコントローラに適用されます。
コントローラのうちの 1 つが故障している場合、**Failover** が発生し、残っているコントローラがその I/O 負荷を引き継ぎます。

Family

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

FC

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

FICON

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

FM

(Flash Memory (フラッシュメモリ))
詳しくは「フラッシュメモリ」を参照してください。

GID

(Group ID)
ホストグループを作成するときに付けられる 2 桁の 16 進数の識別番号です。

GUI

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

HBA

(Host Bus Adapter)
詳しくは「ホストバスアダプタ」を参照してください。

Hyper PAV

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

I/O モード

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

I/O レート

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

In-Band 方式

RAID Manager のコマンド実行方式の 1 つです。コマンドを実行すると、管理ツールの操作端末またはサーバから、ストレージシステムのコマンドデバイスにコマンドが転送されます。

Initiator

属性が RCU Target のポートと接続するポートを持つ属性です。

iSNS

(Internet Storage Naming Service)

iSCSI デバイスで使われる、自動検出、管理および構成ツールです。

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

LACP

(Link Aggregation Control Protocol)

複数回線を 1 つの論理的な回線として扱うための制御プロトコル。

LCU

(Logical Control Unit)

主に磁気ディスク制御装置を指します。

LDEV

(Logical Device (論理デバイス))

RAID 技術では冗長性を高めるため、複数のドライブに分散してデータを保存します。この複数のドライブにまたがったデータ保存領域を論理デバイスまたは LDEV と呼びます。ストレージ内の LDEV は、LDKC 番号、CU 番号、LDEV 番号の組み合わせで区別します。LDEV に任意の名前を付けることもできます。

このマニュアルでは、LDEV (論理デバイス) を論理ボリュームまたはボリュームと呼ぶことがあります。

LDEV 名

LDEV 作成時に、LDEV に付けるニックネームです。あとから LDEV 名の変更もできます。

LDKC

(Logical Disk Controller)

複数の CU を管理するグループです。各 CU は 256 個の LDEV を管理しています。

LUN/LU

(Logical Unit Number)

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

LUN セキュリティ

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

LUN パス、LU パス

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

LUSE ボリューム

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

MCU

(Main Control Unit)

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

Mfibre

(Mainframe Fibre)

IBM のメインフレームのファイバチャネルを示す用語です。

MP ユニット

データ入出力を処理するプロセッサを含んだユニットです。データ入出力に関連するリソース（LDEV、外部ボリューム、ジャーナル）ごとに特定の MP ユニットの割り当てると、性能をチューニングできます。特定の MP ユニットの割り当ての方法と、ストレージシステムが自動的に選択した MP ユニットの割り当ての方法があります。MP ユニットに対して自動割り当ての設定を無効にすると、その MP ユニットがストレージシステムによって自動的にリソースに割り当てられることはないため、特定のリソース専用の MP ユニットとして使用できます。

MTIR

(Multi Target Incremental Resynchronization)

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

MU

(Mirror Unit)

1つのプライマリボリュームと1つのセカンダリボリュームを関連づける情報です。

MVS

(Multiple Virtual Storage)

IBM 社のメインフレームシステム用 OS です。

Namespace

複数 LBA 範囲をまとめた、論理ボリュームの空間のことです。

Namespace Globally Unique Identifier

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

Namespace ID

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

NGUID

(Namespace Globally Unique Identifier)

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

NQN

(NVMe Qualified Name)

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

NSID

(Namespace ID)

Namespace を特定するための、4Byte の識別情報です。

NVM

(Non-Volatile Memory)

不揮発性メモリです。

NVMe

(Non-Volatile Memory Express)

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

NVMe over Fabrics

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

NVMe/TCP

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

NVMe コントローラ

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

NVM サブシステム

NVM のデータストレージ機能を提供する制御システムです。

NVM サブシステムポート

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

Open/MF コンシステンシーグループ

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

Out-of-Band 方式

RAID Manager のコマンド実行方式の 1 つです。コマンドを実行すると、クライアントまたはサーバから LAN 経由で ESM/AMC/RAID Manager サーバの中にある仮想コマンドデバイスにコマンドが転送されます。仮想コマンドデバイスからストレージシステムに指示を出し、ストレージシステムで処理が実行されます。

Parent

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

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

PAV

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

PCB

(Printed Circuit Board)

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

Point to Point

2 点を接続して通信するトポロジです。

PPRC

(Peer-to-Peer Remote Copy)

IBM 社のリモートコピー機能です。

Quorum ディスク

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

RAID

(Redundant Array of Independent Disks)

独立したディスクを冗長的に配列して管理する技術です。

RAID Manager

コマンドインタフェースでストレージシステムを操作するためのプログラムです。

RCU

(Remote Control Unit)

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

RCU Target

属性が Initiator のポートと接続するポートが持つ属性です。

RCU Target ポート

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

RDEV

(Real Device)

IBM 用語です。DASD の実装置アドレスを意味します。

Read Hit 率

ストレージシステムの性能を測る指標の 1 つです。ホストがディスクから読み出そうとしていたデータが、どのくらいの頻度でキャッシュメモリに存在していたかを示します。単位はパーセントです。Read Hit 率が高くなるほど、ディスクとキャッシュメモリ間のデータ転送の回数が少なくなるため、処理速度は高くなります。

S/N

(Serial Number)

ストレージシステムに一意に付けられたシリアル番号（装置製番）です。

SAN

(Storage-Area Network)

ストレージシステムとサーバ間を直接接続する専用の高速ネットワークです。

SIM

(Service Information Message)

ストレージシステムのコントローラがエラーやサービス要求を検出したときに生成されるメッセージです。原因となるエラーを解決し、VSP One Block Administrator 画面上で SIM が解決したことを報告することを、「SIM をコンプリートする」と言います。

SM

(Shared Memory)

詳しくは「シェアドメモリ」を参照してください。

SMS

(Storage Management Subsystem)

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

SNMP

(Simple Network Management Protocol)

ネットワーク管理するために開発されたプロトコルの 1 つです。

SSID

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

SSL

(Secure Sockets Layer)

インターネット上でデータを安全に転送するためのプロトコルであり、Netscape Communications 社によって最初に開発されました。SSL が有効になっている 2 つのピア（装置）は、秘密鍵と公開鍵を利用して安全な通信セッションを確立します。どちらのピア（装置）も、ランダムに生成された対称キーを利用して、転送されたデータを暗号化します。

Super PAV

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

T10 PI

(T10 Protection Information)

SCSI で定義された保証コード基準の一つです。T10 PI では、512 バイトごとに 8 バイトの保護情報 (PI) を追加して、データの検証に使用します。T10 PI にアプリケーションおよび OS を含めたデータ保護を実現する DIX (Data Integrity Extension) を組み合わせることで、アプリケーションからディスクドライブまでのデータ保護を実現します。

Target

ホストと接続するポートが持つ属性です。

TSE-VOL

(Track Space - Efficient Volume)

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

UPS

(Uninterruptible Power System)

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

URL

(Uniform Resource Locator)

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

UUID

(User Definable LUN ID)

ホストから論理ボリュームを識別するために、ストレージシステム側で設定する任意の ID です。

Vary Offline

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

Vary Online

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

vClone Parent 属性のボリューム

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

vClone 属性のボリューム

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

VDEV

(Virtual Device)

IBM 用語です。DASD の仮想アドレスを意味します。

または、Hitachi 用語でパリティグループ内にある論理ボリュームのグループを意味します。

VDEV は任意のサイズの論理ボリューム (CV) とフリースペースから構成されます。VDEV 内に任意のサイズの論理ボリューム (CV) とフリースペースを作成することもできます。

VLAN

(Virtual LAN)

スイッチの内部で複数のネットワークに分割する機能です (IEEE802.1Q 規定)。

VOLSER

(Volume Serial Number)

個々のボリュームを識別するために割り当てられる番号です。VSN と呼びます。LDEV 番号や LUN とは無関係です。

VSN

(Volume Serial Number)

個々のボリュームを識別するために割り当てられる番号です。VOLSER と呼びます。

VSP One Block Administrator

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

VTOC

(Volume Table of Contents)

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

Write Hit 率

ストレージシステムの性能を測る指標の 1 つです。ホストがディスクへ書き込もうとしていたデータが、どのくらいの頻度でキャッシュメモリに存在していたかを示します。単位はパーセントです。Write Hit 率が高くなるほど、ディスクとキャッシュメモリ間のデータ転送の回数が少なくなるため、処理速度は高くなります。

WWN

(World Wide Name)

ホストバスアダプタの ID です。ストレージ装置を識別するためのもので、実体は 16 桁の 16 進数です。

zHyperWrite 機能

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

(ア行)

アクセス属性

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

アクセスパス

ストレージシステム内の、データとコマンドの転送経路です。

インクリメンタルリシンク

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

インスタンス

特定の処理を実行するための機能集合のことです。

インスタンス番号

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

エクステント

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

エミュレーション

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

(力行)

外部ストレージシステム

本ストレージシステムに接続されているストレージシステムです。

外部パス

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

外部ボリューム

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

外部ボリュームグループ

外部ストレージシステムのボリュームをマッピングしている、本ストレージシステム内の仮想
的なボリュームです。
外部ボリュームグループはパリティ情報を含みませんが、管理上はパリティグループと同じよ
うに取り扱います。

鍵管理サーバ

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

書き込み待ち率

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

仮想ボリューム

実体を持たない、仮想的なボリュームです。Dynamic Provisioning、または Dynamic Provisioning for Mainframe で使用する仮想ボリュームを DP-VOL と呼びます。

監査ログ

ストレージシステムに対して行われた操作や、受け取ったコマンドの記録です。Syslog サーバへの転送設定をすると、監査ログは常時 Syslog サーバへ転送され、Syslog サーバから監査ログを取得・参照できます。

管理ツールの操作端末

ストレージシステムを操作するためのコンピュータです。

キャッシュ

チャンネルとドライブの間にあるメモリです。中間バッファとしての役割があります。キャッシュメモリとも呼ばれます。

共用メモリ

詳しくは「シェアドメモリ」を参照してください。

形成コピー

ホスト I/O プロセスとは別に、プライマリボリュームとセカンダリボリュームを同期させるプロセスです。

更新コピー

形成コピー（または初期コピー）が完了したあとで、プライマリボリュームの更新内容をセカンダリボリュームにコピーして、プライマリボリュームとセカンダリボリュームの同期を保持するコピー処理です。

構成定義ファイル

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

コピー系プログラムプロダクト

ストレージシステムに備わっているプログラムのうち、データをコピーするものを指します。ストレージシステム内のボリューム間でコピーするローカルコピーと、異なるストレージシステム間でコピーするリモートコピーがあります。

コピーグループ

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

コマンドデバイス

ホストから RAID Manager コマンドを実行するために、ストレージシステムに設定する論理デバイスです。コマンドデバイスは、ホストから RAID Manager コマンドを受け取り、実行対象の論理デバイスに転送します。

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

コマンドデバイスセキュリティ

コマンドデバイスに適用されるセキュリティです。

コレクションコピー

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

コンシステンシーグループ

コピー系プログラムプロダクトで作成したペアの集まりです。コンシステンシーグループ ID を指定すれば、コンシステンシーグループに属するすべてのペアに対して、データの整合性を保ちながら、特定の操作を同時に実行できます。

コントローラシャーシ

ストレージシステムを制御するコントローラが備わっているシャーシ（筐体）です。コントローラシャーシは DKC、CBX と同義語です。

(サ行)

サーバ証明書

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

サイドファイル

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

サイドファイルキャッシュ

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

サブシステム NQN

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

差分テーブル

コピー系プログラムプロダクトおよび Volume Migration で共有するリソースです。Volume Migration 以外のプログラムプロダクトでは、ペアのプライマリボリュームとセカンダリボリュームのデータに差分があるかどうかを管理するために使用します。Volume Migration では、ボリュームの移動中に、ソースボリュームとターゲットボリュームの差分を管理するために使用します。

差分データ

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

シェアドメモリ

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

自己署名付きの証明書

自分自身で自分用の証明書を生成します。この場合、証明の対象は証明書の発行者と同じになります。ファイアウォールに守られた内部 LAN 上でクライアントとサーバ間の通信が行われている場合は、この証明書でも十分なセキュリティを確保できるかもしれません。

システムディスク

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

システムプールボリューム、システムプール VOL

プールを構成するプールボリュームのうち、1 つのプールボリュームがシステムプールボリュームとして定義されます。システムプールボリュームは、プールを作成したとき、またはシステムプールボリュームを削除したときに、優先順位に従って自動的に設定されます。なお、システムプールボリュームで使用可能な容量は、管理領域の容量を差し引いた容量になります。管理領域とは、プールを使用するプログラムプロダクトの制御情報を格納する領域です。

ジャーナルボリューム

Universal Replicator と Universal Replicator for Mainframe の用語で、プライマリボリュームからセカンダリボリュームにコピーするデータを一時的に格納しておくためのボリュームのことです。ジャーナルボリュームには、プライマリボリュームと関連づけられているマスタジャーナルボリューム、およびセカンダリボリュームと関連づけられているリストアジャーナルボリュームとがあります。

詳細 API

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

状態遷移

ペアボリュームのペア状態が変化することです。

冗長パス

チャンネルボードの故障などによって LUN パスが利用できなくなったときに、その LUN パスに代わってホスト I/O を引き継ぐ LUN パスです。交替パスとも言います。

初期コピー

新規にコピーペアを作成すると、初期コピーが開始されます。初期コピーでは、プライマリボリュームのデータがすべて相手のセカンダリボリュームにコピーされます。初期コピー中も、ホストサーバからプライマリボリュームに対する Read/Write などの I/O 操作は続行できます。

署名付きの信頼できる証明書

証明書発行要求を生成したあとで、信頼できる CA 局に送付して署名してもらいます。CA 局の例としては VeriSign 社があります。

シリアル番号

ストレージシステムに一意に付けられたシリアル番号（装置製番）です。

シンプル API

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

スナップショットグループ

Thin Image Advanced で作成した複数のペアの集まりです。複数のペアに対して同じ操作を実行できます。

スナップショットデータ

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

スワップ

プライマリボリューム/セカンダリボリュームを逆転する操作のことです。

正 VOL、正ボリューム

詳しくは「プライマリボリューム」を参照してください。

正サイト

通常時に、業務（アプリケーション）を実行するサイトを指します。

セカンダリボリューム

ペアとして設定された 2 つのボリュームのうち、コピー先のボリュームを指します。なお、プライマリボリュームとペアを組んでいるボリュームをセカンダリボリュームと呼びますが、Thin Image Advanced では、セカンダリボリューム（仮想ボリューム）ではなく、プールにデータが格納されます。

絶対 LUN

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

センス情報

エラーの検出によってペアがサスペンドされた場合に、正サイトまたは副サイトのストレージシステムが、適切なホストに送信する情報です。ユニットチェックの状況が含まれ、災害復旧に使用されます。

専用 DASD

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

ソースボリューム

Compatible FlashCopy®、および Volume Migration の用語で、Compatible FlashCopy®の場合はボリュームのコピー元となるボリュームを、Volume Migration の場合は別のパリティグループへと移動するボリュームを指します。

ゾーニング

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

(タ行)

ターゲットボリューム

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

チャンネルエクステンダ

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

チャンネルボード

ストレージシステムに内蔵されているアダプタの一種で、ホストコマンドを処理してデータ転送を制御します。

重複排除用システムデータボリューム（データストア）

容量削減の設定が重複排除および圧縮の仮想ボリュームが関連づけられているプール内で、重複データを格納するためのボリュームです。

重複排除用システムデータボリューム（フィンガープリント）

容量削減の設定が重複排除および圧縮の仮想ボリュームが関連づけられているプール内で、重複排除データの制御情報を格納するためのボリュームです。

ディスクボード

ストレージシステムに内蔵されているアダプタの一種で、キャッシュとドライブの間のデータ転送を制御します。

データ削減共有ボリューム

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

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

転送レート

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

同期コピー

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

トポロジ

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

ドライブボックス

各種ドライブを搭載するためのシャーシ（筐体）です。

（ナ行）

内部ボリューム

本ストレージシステムが管理するボリュームを指します。

(ハ行)

パリティグループ

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

非対称アクセス

global-active device でのクロスパス構成など、サーバとストレージシステムを複数の冗長パスで接続している場合で、ALUA が有効のときに、優先して I/O を受け付けるパスを定義する方法です。

非同期コピー

ホストから書き込み要求があった場合に、プライマリボリュームへの書き込み処理とは非同期に、セカンダリボリュームにデータを反映する方式のコピーです。複数のボリュームや複数のストレージシステムにわたる大量のデータに対して、災害リカバリを可能にします。

ピントラック

(pinned track)

物理ドライブ障害などによって読み込みや書き込みができないトラックです。固定トラックとも呼びます。

ファイバチャネル

光ケーブルまたは銅線ケーブルによるシリアル伝送です。ファイバチャネルで接続された RAID のディスクは、ホストからは SCSI のディスクとして認識されます。

プール

プールボリューム（プール VOL）を登録する領域です。Dynamic Provisioning、Dynamic Provisioning for Mainframe、および Thin Image Advanced がプールを使用します。

プールボリューム、プール VOL

プールに登録されているボリュームです。Dynamic Provisioning および Dynamic Provisioning for Mainframe ではプールボリュームに通常のデータを格納し、Thin Image Advanced ではスナップショットデータをプールボリュームに格納します。

副 VOL、副ボリューム

詳しくは「セカンダリボリューム」を参照してください。

副サイト

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

プライマリボリューム

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

フラッシュメモリ

各プロセッサに搭載され、ソフトウェアを格納している不揮発性のメモリです。

ブロック

ボリューム容量の単位の一つです。1 ブロックは 512 バイトです。

ペア

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

ペア状態

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

ペアテーブル

ペアを管理するための制御情報を格納するテーブルです。

ページ

DP の領域を管理する単位です。Dynamic Provisioning の場合、1 ページは 42MB、Dynamic Provisioning for Mainframe の場合、1 ページは 38MB です。

ポートモード

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

ホスト-Namespace パス

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

ホスト NQN

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

ホストグループ

ストレージシステムの同じポートに接続し、同じプラットフォーム上で稼働しているホストの集まりのことです。あるホストからストレージシステムに接続するには、ホストをホストグループに登録し、ホストグループを LDEV に結び付けます。この結び付ける操作のことを、LUN パスを追加するとも呼びます。

ホストグループ 0 (ゼロ)

「00」という番号が付いているホストグループを指します。

ホストデバイス

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

ホストバスアダプタ

(Host Bus Adapter)

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

ホストモード

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

(マ行)

マイグレーションボリューム

異なる機種のストレージシステムからデータを移行させる場合に使用するボリュームです。

マッピング

本ストレージシステムから外部ボリュームを操作するために必要な管理番号を、外部ボリュームに割り当てることです。

ミニディスク DASD

IBM 用語です。z/VM 上で定義される仮想 DASD を意味します。

(ヤ行)

容量削減設定が無効なデータ削減共有ボリューム

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

容量削減設定が有効なデータ削減共有ボリューム

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

(ラ行)

リソースグループ

ストレージシステムのリソースを割り当てたグループを指します。リソースグループに割り当てられるリソースは、LDEV 番号、パリティグループ、外部ボリューム、ポートおよびホストグループ番号です。

リモートコマンドデバイス

外部ストレージシステムのコマンドデバイスを、本ストレージシステムの内部ボリュームとしてマッピングしたものです。リモートコマンドデバイスに対して RAID Manager コマンドを発行すると、外部ストレージシステムのコマンドデバイスに RAID Manager コマンドを発行でき、外部ストレージシステムのペアなどを操作できます。

リモートストレージシステム

ローカルストレージシステムと接続しているストレージシステムを指します。

リモートパス

リモートコピー実行時に、遠隔地にあるストレージシステム同士を接続するパスです。

リンクアグリゲーション

複数のポートを集約して、仮想的にひとつのポートとして使う技術です。これによりデータリンクの帯域幅を広げるとともに、ポートの耐障害性を確保します。

レコードセット

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

レスポンスタイム

モニタリング期間内での平均の応答時間。あるいは、エクスポートツール 2 で指定した期間内でのサンプリング期間ごとの平均の応答時間。単位は、各モニタリング項目によって異なります。

ローカルストレージシステム

管理ツールの操作端末を接続しているストレージシステムを指します。

◎ 日立ヴァンタラ株式会社

〒 244-0817 神奈川県横浜市戸塚区吉田町 292 番地
