

Hitachi Virtual Storage Platform G1000/
Hitachi Virtual Storage Platform VX7

セキュリティターゲット

発行日:	2016年4月18日
バージョン:	3.4
作成:	株式会社 日立製作所

他社商標

Microsoft、Windows は、米国およびその他の国における米国 Microsoft Corp.の商標または登録商標です。

Solaris は、米国およびその他の国における Sun Microsystems, Inc.の商標または登録商標です。

HP-UX は、米国 Hewlett-Packard Company の登録商標です。

RedHat は、米国およびその他の国で RedHat, Inc.の商標または登録商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標または登録商標です。

AIX は、IBM Corporation の商標または登録商標です。

その他記載されている会社名、製品名は各社の商標または登録商標です。

— 目次 —

1	ST 概説	1
1.1	ST 参照	1
1.2	TOE 参照	1
1.3	TOE 概要	2
1.3.1	TOE 種別.....	2
1.3.2	TOE が利用される環境.....	2
1.3.3	TOE への関与者.....	3
1.3.4	TOE の使用方法と主要セキュリティ機能.....	4
1.3.5	TOE と TOE 以外の構成要素.....	5
1.3.5.1	ハードウェアの構成要素.....	5
1.3.5.2	ソフトウェアの構成要素.....	6
1.4	TOE 記述	7
1.4.1	制御系.....	10
1.4.2	管理系.....	11
1.4.3	他のディスクストレージ装置.....	11
1.4.4	TOE の機能.....	12
1.4.4.1	TOE が提供する基本機能	12
1.4.4.2	TOE が提供するセキュリティ機能	13
1.4.5	ガイダンス文書.....	16
1.5	評価環境.....	18
2	適合主張	21
2.1	CC 適合主張	21
2.2	PP 主張	21
2.3	パッケージ主張.....	21
3	セキュリティ課題定義	22
3.1	TOE 資産	22
3.2	脅威.....	22
3.3	組織のセキュリティ方針.....	22
3.4	前提条件.....	23
4	セキュリティ対策方針	24
4.1	TOE のセキュリティ対策方針	24
4.2	運用環境のセキュリティ対策方針.....	25
4.3	セキュリティ対策方針根拠.....	25
4.3.1	前提条件に対するセキュリティ対策方針の根拠.....	26
4.3.2	脅威に対するセキュリティ対策方針の根拠.....	27
4.3.3	組織のセキュリティ方針に対するセキュリティ対策方針の根拠.....	29
5	拡張コンポーネント定義	31
6	セキュリティ要件	32
6.1	セキュリティ機能要件.....	32
6.2	セキュリティ保証要件.....	50
6.3	セキュリティ要件根拠.....	51
6.3.1	セキュリティ機能要件根拠.....	51
6.3.2	セキュリティ要件内部一貫性根拠.....	59
6.3.3	セキュリティ保証要件根拠.....	61
7	TOE 要約仕様	63
7.1	TOE セキュリティ機能	63

7.1.1	<i>SF.LM</i>	64
7.1.2	<i>SF.FCSP</i>	65
7.1.3	<i>SF.SN</i>	65
7.1.4	<i>SF.ROLE</i>	66
7.1.5	<i>SF.HDD</i>	67
7.1.6	<i>SF.AUDIT</i>	68
8	参考文献	72
8.1	ドキュメントで使用する用語.....	73
8.1.1	<i>ST</i> 専門用語.....	73
8.1.2	略語.....	74

表目次

表 1-1 TOE によって提供される基本機能.....	12
表 1-2 ロールの分類と操作内容.....	14
表 1-3 テストで使用した TOE 構成要素.....	18
表 1-4 テストで使用した Hitachi Unified Storage VM の物理構成要素.....	18
表 1-5 テストで使用したホスト.....	19
表 1-6 テストで使用した管理 PC.....	19
表 1-7 テストで使用した保守員 PC.....	19
表 1-8 テストで使用した外部認証サーバ.....	19
表 1-9 テストで使用したファイバチャネルスイッチ.....	19
表 1-10 テストで使用したファイバチャネル接続アダプタ.....	19
表 4-1 TOE セキュリティ課題とセキュリティ対策方針の対応.....	26
表 4-2 前提条件に対するセキュリティ対策方針の正当性.....	26
表 4-3 脅威に対するセキュリティ対策方針の正当性.....	27
表 4-4 組織のセキュリティ方針に対するセキュリティ対策方針の正当性.....	29
表 6-1 個別に定義した監査対象事象.....	32
表 6-2 監査情報.....	34
表 6-3 暗号鍵の生成操作.....	37
表 6-4 暗号鍵破棄方法.....	37
表 6-5 サブジェクトとオブジェクト間の操作.....	38
表 6-6 SFP 関連セキュリティ属性.....	39
表 6-7 サブジェクトとオブジェクト間の規則.....	39
表 6-8 役割に操作を制限する機能のリスト.....	43
表 6-9 ホストを代行するプロセスのセキュリティ属性(LU パス情報)に対するストレージ管理者 および保守員の操作.....	44
表 6-10 Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセスのセキュリティ 属性(ユーザグループ情報)に対するストレージ管理者および保守員の操作.....	44
表 6-11 ユーザアカウントに対するストレージ管理者および保守員の操作.....	46
表 6-12 ホストが接続されるファイバチャネルスイッチの認証データに対するストレージ管理者 および保守員の操作.....	46
表 6-13 格納データ暗号化の暗号鍵に対するストレージ管理者および保守員の操作.....	46
表 6-14 ユーザの認証方式に対するストレージ管理者および保守員の操作.....	47
表 6-15 セキュリティ対策方針とセキュリティ機能要件の対応.....	51
表 6-16 TOE のセキュリティ対策方針に対するセキュリティ機能要件の正当性.....	52
表 6-17 セキュリティ機能要件の依存性.....	59
表 6-18 セキュリティ機能要件間の一貫性.....	60

表 7-1 TOE セキュリティ機能とセキュリティ機能要件との対応関係	63
表 7-2 SSL で使用する暗号関連のアルゴリズム	66
表 7-3 基本情報の出力内容	68
表 7-4 詳細情報の出力内容	71

図目次

図 1-1 ディスクストレージ装置を含むシステムの一般的な構成.....	2
図 1-2 ディスクストレージ装置の構成.....	9
図 1-3 ユーザ、ユーザグループ、ロール、リソースグループの関係.....	13

1 ST 概説

本章では、ST 参照、TOE 参照、TOE 概要、および TOE 記述について記述する。

1.1 ST 参照

本節では ST の識別情報を記述する。

タイトル	: Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 セキュリティターゲット
バージョン	: 3.4
発行日	: 2016 年 4 月 18 日
作成	: 株式会社 日立製作所

1.2 TOE 参照

本節では TOE の識別情報を記述する。

TOE	: Hitachi Virtual Storage Platform G1000、Hitachi Virtual Storage Platform VX7 用制御プログラム
TOE のバージョン	: 80-01-25-00/00(R8-01A-06_Z) 以下のプログラムから構成される。 <ul style="list-style-type: none"> • DKCMAIN マイクロプログラム 80-01-25-00/00 • SVP プログラム 80-01-25/00 (Storage Navigator プログラム(ストレージ管理ユーザインタフェースソフトウェア)を含む) • JDK 1.7.0_21 • Apache 2.4.4 • Apache Tomcat 7.0.39 • OpenSSL 1.0.1g • ActivePerl 5.16.2.1602 • Flash Player 11.6.602.180
TOE の消費者	: 国内の TOE の消費者は TOE を含むディスクストレージ製品の購入者と定義し、同製品のエンドユーザに受け渡すまでの配付手続きを保証する。海外の TOE の消費者は顧客 Hitachi Data Systems であり Hitachi Data Systems に TOE を受け渡すまでの配付手続きを保証するものとなっている。
キーワード	: ディスクストレージ、SAN、RAID、仮想化、ロールベースアクセス制御
開発者	: 株式会社 日立製作所

1.3 TOE 概要

1.3.1 TOE 種別

TOE は、株式会社 日立製作所のディスクストレージ製品 Hitachi Virtual Storage Platform G1000 (Hitachi Virtual Storage Platform VX7 というブランド名でも販売されている。以下 VSP と略す。) ディスクストレージ装置を動作させる制御プログラム(ソフトウェア)である。

1.3.2 TOE が利用される環境

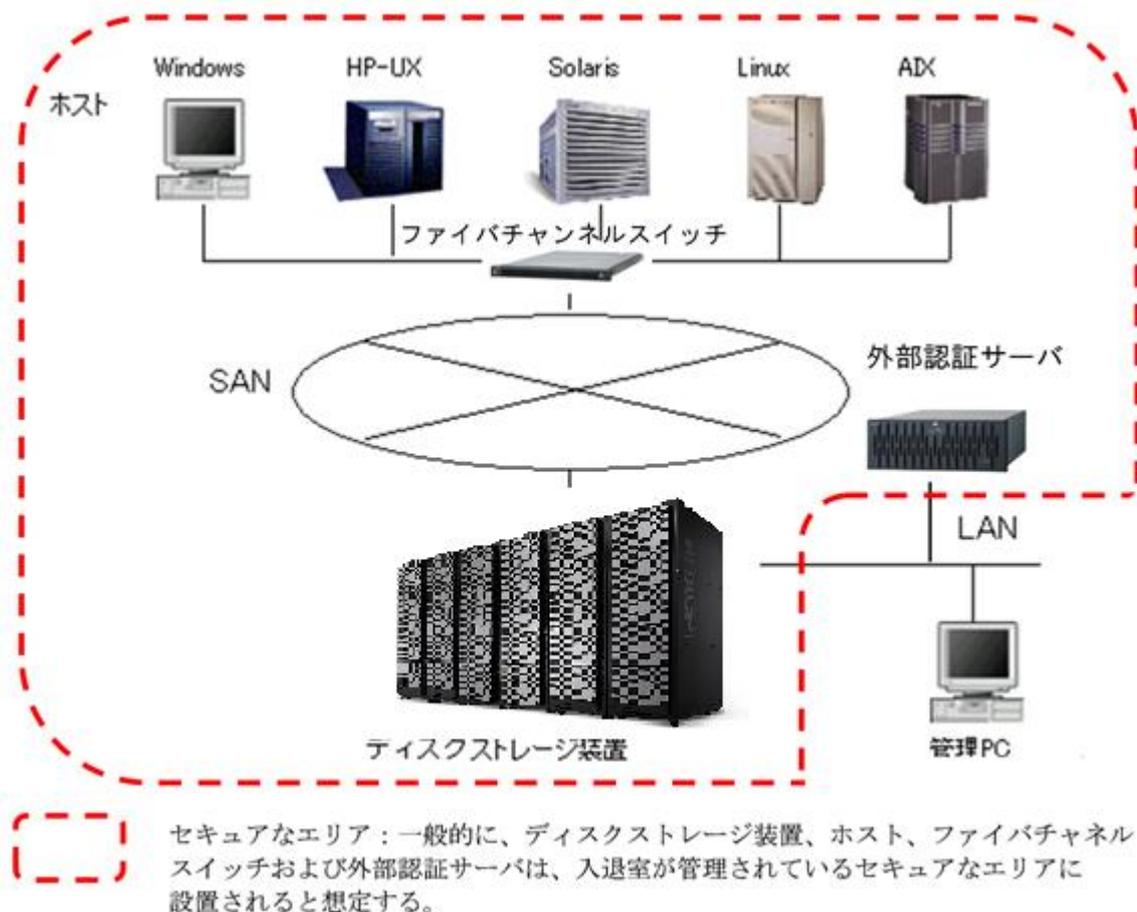


図 1-1 ディスクストレージ装置を含むシステムの一般的な構成

図 1-1 に示される環境に登場する機器を説明する。

(1) ディスクストレージ装置

通常、TOE が搭載されるディスクストレージ装置は、入退室が管理されているセキュアなエリアに設置される。

(2) SAN とホスト

Windows、HP-UX、Solaris 等の各種オープン系サーバ（本 ST ではこれらの機器を“ホスト”と総称する）とディスクストレージ装置との接続は、SAN (Storage Area Network) を介して行われる。SAN は、ホストとディスクストレージ装置をファイバチャネルによって接続するストレージシステム専用ネットワークである。

ホストを SAN に接続するには、ホストにファイバチャネル接続アダプタ（ハードウェア、ソフトウェア）のインストールが必要であり、ディスクストレージ装置は、ファイバチャネル接続アダプタ内の識別情報を使用してホストを識別している。ファイバチャネル接続アダプタ内の識別情報は、ホストをディスクストレージ装置に接続するときに、ストレージリソース管理者 (1.3.3 節参照) が設定する。通常、ホストは入退室が管理されているセキュアなエリアに設置される。

また、組織のセキュリティ方針で求められる場合、TOE はディスクストレージ装置に接続されるファイバチャネルスイッチの識別・認証を行うことが可能である。このとき、ファイバチャネルスイッチは接続されるホストを識別・認証する必要がある。ディスクストレージ装置は、ファイバチャネルスイッチ内の識別情報を使用してファイバチャネルスイッチを識別している。ファイバチャネルスイッチ内の識別情報は、ファイバチャネルスイッチをディスクストレージ装置に接続するときに、セキュリティ管理者 (1.3.3 節参照) が設定する。通常、ファイバチャネルスイッチは入退室が管理されているセキュアなエリアに設置される。

(3) 管理 PC

管理 PC は、ディスクストレージ装置の構成情報の設定をリモートから行うための PC である。管理 PC 上で、ディスクストレージ装置の管理者が構成情報の設定を行うためのプログラムを動作させる。管理 PC とディスクストレージ装置は LAN (Local Area Network) を介して接続される。

(4) 外部認証サーバ

外部認証サーバは、ディスクストレージ装置の管理者がディスクストレージ装置にアクセスするときに、使用者の識別・認証を行うサーバである。ディスクストレージ装置とホストと同様に通常は、入退室が管理されているセキュアなエリアに設置される。

1.3.3 TOE への関与者

ディスクストレージ装置に関係する者として、本 ST では以下のような利用者を想定している。

- ・ セキュリティ管理者 :

セキュリティ管理者は、Storage Navigator プログラム (1.4.2 節参照) と呼ばれるストレージ管理ユーザインタフェース (UI) ソフトウェアを使用して管理者アカウントの登録、変更、削除ができる。また、リソースグループと呼ばれるストレージリソースの集合の管理権限を特定のユーザに割り当てることができる。その他、ホストの識別およびファイバチャネルスイッチの識別・認証設定、格納データの暗号化操作を実施できる。

- ・ ストレージリソース管理者 :

Storage Navigator プログラム (ストレージ管理 UI ソフトウェア) を使用して、セキュリティ管理者に割り当てられたリソース (ポート、キャッシュメモリ、ディスク等) を管理できる管理者。

- ・ 監査ログ管理者 :

ディスクストレージ装置で取得している監査ログを管理できる管理者。管理 PC 上の Storage Navigator プログラム (ストレージ管理 UI ソフトウェア) を用いて、監査ログの参照やダウンロード、および syslog に関する設定が可能である。

- ・ 保守員 :

ディスクストレージ装置を利用する顧客が保守契約を結んだ、保守専門の組織に所属する人。ディスクストレージ装置を設置する際の初期立上げ処理、部品の交換や追加などの保守作業に伴う設定変更、異常時の復旧処理などを担当する。

保守員は、保守員用の PC を使用して、ディスクストレージ装置に対する保守・管理用のインタフェースを提供している SVP PC (管理保守インタフェース(IF) PC) (1.4.2 節参照)と呼ばれる PC へアクセスし、保守作業を実施する。直接、ディスクストレージ装置内の機器に触ったり、内部 LAN に接続した機器を操作したりできるのは、保守員だけである。保守員はディスクストレージ装置内の全てのリソースが割り当てられていて保守員ロール(表 1-2 参照)で許可されている操作を実施できる。TOE は、保守員 PC(1.4.2 節参照)を使用して SVP PC (管理保守 IF PC)へアクセスするインタフェースを使用する者を「保守員」役割と認識する。

- ・ ストレージ利用者 :

ディスクストレージ装置の利用者でホストを表す。ディスクストレージ装置と接続されたホストから、ディスクストレージ装置内に保存されたデータを使用する。

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

1.3.4 TOE の使用方法と主要セキュリティ機能

VSP は、マルチプラットフォーム、高性能、高速レスポンスの大容量企業向けディスクストレージ装置であり、拡張可能な接続性、外部ストレージの仮想化、論理資源の分割、リモートコピー機能、拡張可能なディスク容量を異種システム環境で提供する。

ディスクストレージ装置には SAN 環境や IP ネットワーク環境 (本 ST では、SAN 環境を用いてディスクストレージ運用方法を述べる) を介して、様々なプラットフォームの多数のホストが接続される。このディスクストレージ装置への接続において、不正操作が行われた場合、ディスクストレージ装置内に存在するユーザデータへ意図しないアクセスが行われる可能性がある。そのため、ディスクストレージ装置内のユーザデータに対し、アクセス制御を実施する必要がある。

また、ディスクサブシステム内のリソース(ポート、キャッシュメモリ、ディスク等)を複数のストレージリソース管理者が管理する状況では、権限を越えた設定が行われる可能性がある。そのため、TOE はディスクストレージ装置内のポート、ディスク(パリティグループ(8.1.1 節参照))、キャッシュメモリなどを複数のリソースグループに分割し、分割したリソースグループを各ストレージリソース管理者に割当てて、そして、各ストレージリソース管理者にリソースを管理する権限を与えることにより、各ストレージリソース管理者は、他のリソースに影響することなく管理するリソースへのアクセスを行うことができる。TOE である VSP 用制御プログラムは DKCMAIN マイクロプログラム、SVP プログラム、Storage Navigator プログラム(ストレージ管理 UI ソフトウェア)、JDK、Apache、Apache Tomcat、OpenSSL、Flash player、ActivePerl から構成される。DKCMAIN マイクロプログラムがディスクストレージ装置内のリソースを制御し、SVP プログラムがディスクストレージ装置の管理者の権限管理を行う。Storage Navigator プログラム(ストレージ管理 UI ソフトウェア) は SVP プログラムに含まれており、SVP PC (管理保守 IF PC) から管理 PC にダウンロードして使用する。以下、Storage Navigator プログラム(ストレージ管理 UI ソフトウェア) を単に Storage Navigator (ストレージ管理 UI ソフトウェア) と称する。JDK、Apache、Apache Tomcat、OpenSSL、Flash player、ActivePerl は、SVP PC(管理保守 IF PC)が提供する機能を実現するために搭載しているソフトウェア (アプリケーション・ライブラリ) である。

本 ST は、特定のストレージ利用者に割り当てられたストレージリソースに対する他のストレージ利用者からの不正アクセスを防止する機能とディスクドライブ内のユーザデータを暗号化およびシュレディングする機能を提供することにより VSP におけるユーザデータの完全性・機密性を保護するためのセキュリティ機能について記述したものである。

TOE が提供するセキュリティ機能の概要を以下(a)～(h)に示す。

[TOE が提供するセキュリティ機能]

(a) ストレージ管理者および保守員のアクセス制御機能：

TOE にアクセスするストレージ管理者および保守員のアカウントはグループに所属し、グループに 1 つ以上のロール (1.4.4.2.1 節参照) と 1 つ以上のリソースグループを割り当てる。リソースグループは、ストレージリソースを複数のグループに分割したもので、各アカウントは割り当てられたリソースグループ内のリソースに対してロールによって許可された管理操作のみを実行できる。

(b) ホストのアクセス制御機能：

ホストからディスクストレージ装置内の LDEV (論理ボリューム) に対するアクセス制御を行う。

(c) ホストが接続されるファイバチャネルスイッチの識別・認証機能：

不正なホストからディスクストレージ装置に接続されないようにするため、ファイバチャネルスイッチの識別・認証を行う。

(d) ストレージ管理者および保守員の識別・認証機能：

TOE にアクセスするストレージ管理者および保守員の管理、および識別・認証を行う。また、外部に設置した認証サーバ (外部認証サーバ) を使用してストレージ管理者および保守員の識別・認証を実施することもできる。

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

Storage Navigator (ストレージ管理 UI ソフトウェア)–SVP PC (管理保守 IF PC)間および SVP PC (管理保守 IF PC)–外部認証サーバ間通信の暗号化を行う。

(f) 格納データ暗号化機能:

ディスクストレージ装置内に保存するユーザデータの暗号化を行う。

(g) シュレディング機能：

ディスクストレージ装置内ユーザデータのシュレディングを行う。

(h) 監査ログ機能：

ディスクストレージ装置に対する構成変更操作等のログを採取し、参照・管理を可能にする。

1.3.5 TOE と TOE 以外の構成要素

この節では製品のハードウェアとソフトウェアの構成要素を記載し、どれが TOE に含まれ、どれが動作環境に含まれるか表示する。なお、ディスクストレージ装置に内蔵される機器およびソフトウェアは出荷時に組み込まれており、ストレージ管理者、ストレージ利用者 (1.3.3 節参照) で準備したり、変更したりすることはない。

1.3.5.1 ハードウェアの構成要素

次の表は必要なハードウェアの構成要素を示し、それぞれの構成要素が TOE に含まれるかどうか示す。環境は TOE 以外の構成要素であることを示す。

TOE・環境	構成要素	説明
--------	------	----

TOE・環境	構成要素	説明
環境	Hitachi Virtual Storage Platform G1000 Hitachi Virtual Storage Platform VX7	ディスクストレージ装置の名称であり、ディスクストレージ装置を構成するハードウェアおよび TOE などのソフトウェアにより構成されている。TOE を除く部分は環境として利用する部分である。
環境	ホスト	ディスクサブシステムにアクセスするコンピュータ。ホストの OS は、Windows、HP-UX、Solaris、Linux、AIX を想定する。
環境	ファイバチャネル接続アダプタ	SAN に接続するためにコンピュータに搭載するアダプタ。
環境	ファイバチャネルスイッチ	ホストとディスクストレージ装置を接続し、SAN を構成するスイッチ。ホストと TOE を搭載するディスクストレージとの接続において必須の構成要素である。
環境	管理 PC	TOE を管理するためのコンピュータ。 コンピュータの必要条件 <ul style="list-style-type: none"> • CPU：Pentium 4 640 3.2GHz 相当以上 推奨：Core 2 Duo E6540 2.33GHz 以上 • RAM：2GB 以上 推奨 3GB • 有効な HDD 空き領域：500 MB 以上 • モニター：True Color 32 bit 以上; 解像度 1280x1024 以上 • LAN カード：100Base-T or 1000Base-T
環境	SAN	ファイバチャネル技術を利用して、ディスクストレージ装置とコンピュータ間を接続する高速のネットワーク。
環境	他のディスクストレージ装置	TOE を搭載するディスクストレージ装置と接続する他のディスクストレージ装置。他のディスクストレージ装置は TOE が搭載されるディスクストレージ装置に限定される。
環境	保守員 PC	保守員が保守作業を行う際に使用するコンピュータで、保守員が用意する。
環境	外部認証サーバ	LDAP サーバ、および RADIUS サーバを利用して利用者の識別・認証を行うサーバ。 <ul style="list-style-type: none"> • LDAP サーバは LDAPv3 を備えたサーバ。 • RADIUS サーバは RFC2865 準拠のサーバ。
環境	外部 LAN	ディスクストレージ装置と管理 PC、外部認証サーバを接続する LAN
環境	内部 LAN	ディスクストレージ装置内のパッケージおよび、保守員 PC を接続する LAN

1.3.5.2 ソフトウェアの構成要素

次の表は必要なソフトウェアの構成要素を示し、それぞれの構成要素が TOE に含まれるかどうかを示す。

TOE・環境	構成要素	説明
TOE	DKCMAIN マイクロプログラム バージョン 80-01-25-00/00	TOE はディスクストレージ装置出荷時に組み込まれて提供される。

TOE・環境	構成要素	説明
TOE	SVP プログラム バージョン 80-01-25/00	SVP PC (管理保守 IF PC) 上で動作する SVP プログラムと管理 PC で動作する Storage Navigator (ストレージ管理 UI ソフトウェア)を含む。 TOE はディスクストレージ装置出荷時に組み込まれて提供される。
TOE	JDK バージョン 1.7.0_21	SVP PC (管理保守 IF PC) 上で動作する。TOE はディスクストレージ装置出荷時に組み込まれて提供される。
TOE	Apache バージョン 2.4.4	SVP PC (管理保守 IF PC) 上で動作する。TOE はディスクストレージ装置出荷時に組み込まれて提供される。
TOE	Apache Tomcat バージョン 7.0.39	SVP PC (管理保守 IF PC) 上で動作する。TOE はディスクストレージ装置出荷時に組み込まれて提供される。
TOE	OpenSSL バージョン 1.0.1g	SVP PC (管理保守 IF PC) 上で動作する。TOE はディスクストレージ装置出荷時に組み込まれて提供される。
TOE	ActivePerl バージョン 5.16.2.1602	SVP PC (管理保守 IF PC) 上で動作する。TOE はディスクストレージ装置出荷時に組み込まれて提供される。
TOE	Flash Player バージョン 11.6.602.180	SVP PC (管理保守 IF PC) 上で動作する。TOE はディスクストレージ装置出荷時に組み込まれて提供される。
環境	SVP PC (管理保守 IF PC) OS	SVP PC (管理保守 IF PC) の OS。 <ul style="list-style-type: none"> Windows 7 US 版 (64bit 版) SP1 ディスクストレージ装置出荷時に組み込まれて提供される。
環境	管理 PC OS	管理 PC の OS。 <ul style="list-style-type: none"> Windows 7 (SP1)
環境	保守員 PC OS	保守員 PC の OS。 <ul style="list-style-type: none"> Windows 7 (SP1)
環境	Web ブラウザ	管理 PC で起動している Web ブラウザ。 以下ブラウザをサポートする。 <ul style="list-style-type: none"> Internet Explorer 8
環境	Flash Player	Web ブラウザのプラグインとして管理 PC で動作する。以下のバージョンを使用する。 <ul style="list-style-type: none"> Flash Player 11.6
環境	Java ランタイム環境	管理 PC で起動している Java ランタイム環境。 <ul style="list-style-type: none"> JRE 7.0 Update 21(1.7.0_21)

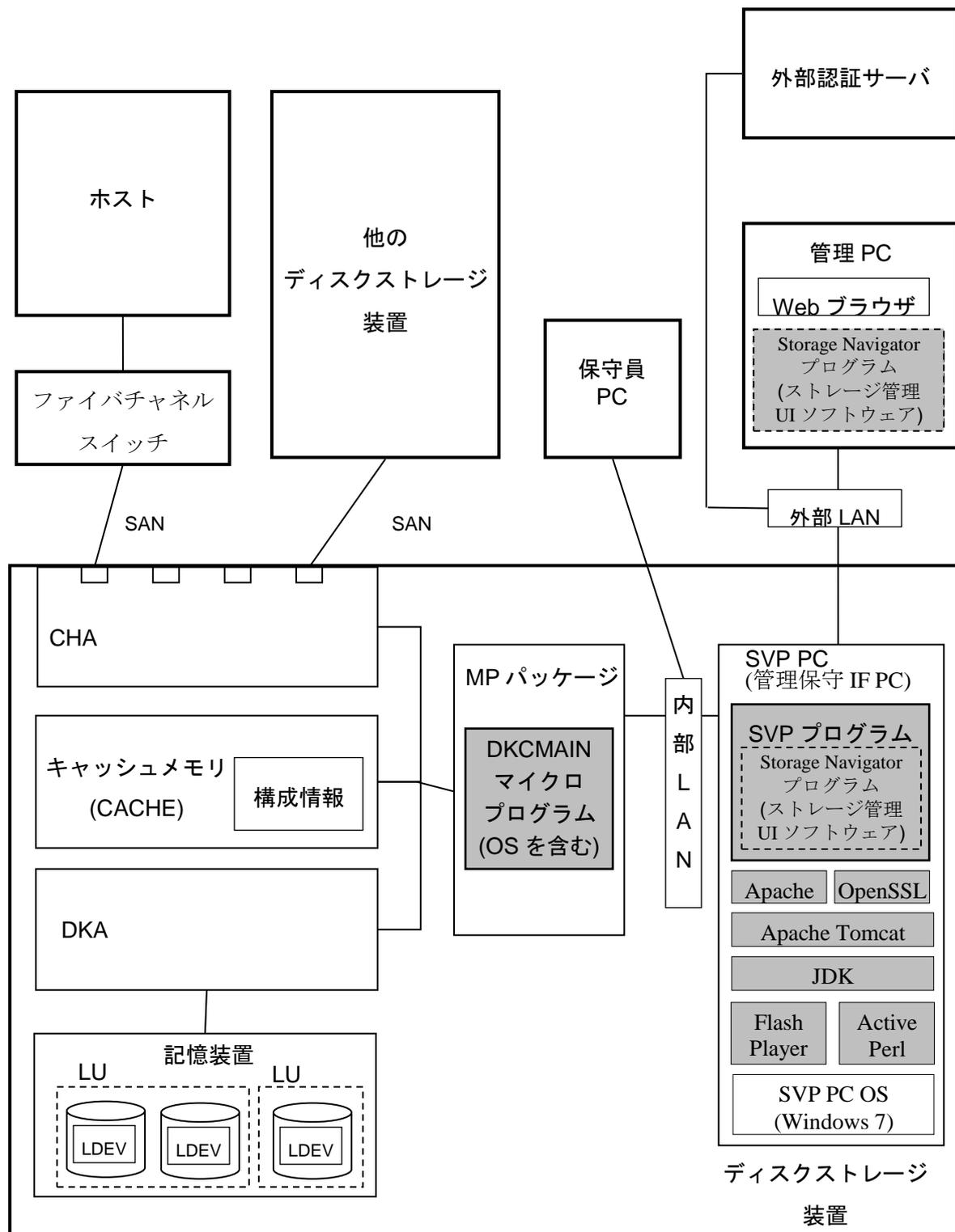
1.4 TOE 記述

TOE は“DKCMAIN マイクロプログラム”、“SVP プログラム”、“Storage Navigator (ストレージ管理 UI ソフトウェア)”、“JDK”、“Apache”、“Apache Tomcat”、“OpenSSL”、“Flash player”、“ActivePerl”で構成される。

DKCMAIN マイクロプログラムは、ディスクストレージ装置内の複数の MP パッケージ (1.4.1 節参照) 上に搭載され、ディスクストレージ装置に接続されたホストとディスクストレージ装置

との間のデータ転送を制御する役割を持つ。SVP プログラムはディスクストレージ装置の運用と保守を行うためのプログラムであり、Storage Navigator (ストレージ管理 UI ソフトウェア)が SVP プログラムのユーザインタフェース機能を提供している。

図 1-2 に、ディスクストレージ装置を構成するハードウェア要素と、識別された TOE のサブセットがどの構成要素上で動作しているかを示す。



- Storage Navigator プログラム(ストレージ管理 UI ソフトウェア)は、Flex アプリケーションと Java アプレットで構成され、SVP および管理 PC で動作する。
- LU : 論理ユニット。ホストから使用するアクセス単位で 1 個または複数の LDEV(論理ボリューム)から構成される。

図 1-2 ディスクストレージ装置の構成

ディスクストレージ装置は、チャネルアダプタ(CHA)、キャッシュメモリ(CACHE)、ディスク

アダプタ(DKA)、MP(Micro Processor) パッケージ、記憶装置が含まれる制御系と、SVP(Service Processor) PCが含まれる管理系に分けられる。制御系は、記憶装置へのデータ入出力の制御を行い、管理系はディスクストレージ装置の保守や管理を行う。これらの構成要素の説明を以下に示す。

なお、制御系ネットワーク(CHA、CACHE、DKA、MP パッケージの高速クロスバススイッチ接続)と管理系ネットワーク(内部 LAN、外部 LAN)は独立したものである。この構造により、内部 LAN や外部 LAN に接続されている SVP PC (管理保守 IF PC)、管理 PC、保守員 PC から、CACHE、記憶装置にアクセスすることはできない。

1.4.1 制御系

(1) チャネルアダプタ

チャネルアダプタ(CHA)は、他のディスクストレージ装置、およびファイバチャネルスイッチを介したホストから自ディスクストレージ装置に対するコマンドを処理して、データ転送を制御するアダプタである。他のディスクストレージ装置、およびファイバチャネルスイッチが CHA 上のファイバポートに接続される。

(2) ディスクアダプタ

ディスクアダプタ(DKA)は、CACHE と記憶装置間のデータ転送を制御するアダプタである。DKA には、格納データ暗号化機能の暗号化および復号を行う LSI が搭載されている。

(3) キャッシュメモリ

キャッシュメモリ(CACHE)は、CHA と DKA との間にあるメモリであり、DKCMAIN マイクロプログラムから共通にアクセス可能なメモリである。CHA、DKA からデータにアクセスするための構成情報が格納され、データの Read/Write を行うために使用する。メモリ上の構成情報は DKCMAIN マイクロプログラムを経由しないとアクセスできない。

(4) MP パッケージ

1 枚の MP パッケージに、クワッドコアの CPU が 1 つ 搭載され、DKCMAIN マイクロプログラムが動作する。

(5) 記憶装置

記憶装置は複数のディスクドライブで構成されており、ユーザデータが記憶される。記憶装置内には、ユーザデータを格納するボリュームである LDEV (論理ボリューム) が作成される。ユーザデータへのアクセスは、LDEV (論理ボリューム) の単位で管理され、DKCMAIN マイクロプログラムを経由して行われる。LDEV (論理ボリューム) 内のデータの一部または、全体をキャッシュメモリに割り当てることができる。キャッシュメモリに割り当てることにより、データの高速アクセスが可能になる。LU(論理ユニット)はホストからのアクセス単位であり、1 個または複数の LDEV (論理ボリューム) にマッピングされる。

LDEV (論理ボリューム) は、記憶装置に構成されるパリティグループ上に作成する。パリティグループは、1 つのデータグループとして扱われる一連のディスクドライブで、ユーザデータとパリティ情報を格納して RAID を構成している。RAID 構成により、パリティグループ内の 1 つまたは複数のドライブが利用できない場合でもユーザデータにアクセスでき、信頼性を向上させている。

CHA、CACHE、DKA、MP パッケージは高速クロスバススイッチで接続されている。

1.4.2 管理系

(1) SVP PC (管理保守 IF PC)

SVP PC (管理保守 IF PC)は、ディスクストレージ装置に対する保守・管理用のインタフェースを提供している PC である。ディスクストレージ装置全体の管理を行うためにディスクストレージ装置に内蔵されているサービスプロセッサとして働き、TOE の一部である SVP プログラムが動作する。SVP プログラムは、ディスクストレージ装置の保守機能および構成情報の管理を行うためのソフトウェアであり、管理 PC 上で動作する Storage Navigator (ストレージ管理 UI ソフトウェア) から受け取った構成情報の設定指示を DKCMAIN マイクロプログラムに対して送信する機能を有する。SVP プログラムは、ディスクストレージ装置におけるセキュリティ機能の動作に関わる設定機能を有する。JDK、Apache、Apache Tomcat、OpenSSL、Flash player、ActivePerl は、SVP PC (管理保守 IF PC) が提供する機能を実現するために搭載しているソフトウェア (アプリケーション・ライブラリ) である。

(2) 保守員 PC

保守員 PC は、保守員が保守作業を行う際に使用する PC である。ディスクストレージ装置内ネットワークである内部 LAN 経由で、リモートデスクトップ機能により SVP PC (管理保守 IF PC) に接続して使用する。

(3) 管理 PC

管理 PC は、ストレージ管理者(1.3.3 節参照)がディスクストレージ装置の運用と保守作業を行うために使用する顧客の PC であり、TOE の一部である Storage Navigator (ストレージ管理 UI ソフトウェア) が動作する。管理 PC と SVP PC (管理保守 IF PC) は外部 LAN で接続される。

(4) 外部認証サーバ

外部認証サーバは、ストレージ管理者(1.3.3 節参照)が Storage Navigator (ストレージ管理 UI ソフトウェア) を使用して TOE にアクセスするときに、SVP プログラムからの要求により、使用者の識別・認証を行い、認証結果と認証成功時には認可情報の元になるユーザグループ情報(1.4.4.2.1 節参照)を SVP プログラムに返す。SVP PC (管理保守 IF PC)ー外部認証サーバ間の通信は暗号化通信を行う。

(5) Storage Navigator プログラム (ストレージ管理 UI ソフトウェア)

Storage Navigator (ストレージ管理 UI ソフトウェア) は、ストレージ管理者(1.3.3 節参照)がディスクストレージ装置の構成情報の管理を行うために使用するソフトウェアである。

Storage Navigator (ストレージ管理 UI ソフトウェア) は Flex アプリケーションと Java アプレットから構成される。Flex アプリケーションは管理 PC の Web ブラウザから指定した操作を SVP PC (管理保守 IF PC) 上で実行し、結果を管理 PC の Web ブラウザに表示する。Java アプレットはプログラムを SVP PC (管理保守 IF PC) から管理 PC にダウンロードし、管理 PC 上で動作する。SVP PC (管理保守 IF PC) と Storage Navigator (ストレージ管理 UI ソフトウェア) の通信には、SSL が使用される。ストレージ管理者は管理 PC の Web ブラウザを使って Storage Navigator (ストレージ管理 UI ソフトウェア) とやりとりをし、ディスクストレージ装置の設定操作を行う。

Storage Navigator (ストレージ管理 UI ソフトウェア) は、悪意を持った第三者 (3.2 節参照) による不正使用を抑止するため、SVP プログラムと連携して、利用者の識別・認証を行う。

1.4.3 他のディスクストレージ装置

ディスクストレージ装置に搭載されるチャンネルアダプタのポートには、ホスト以外に、他のディスクストレージ装置を接続することができる。ディスクストレージ装置はチャンネルアダプタを経由して他のディスクストレージ装置とコマンドを送受信することにより、ディスクストレージ

装置間のデータコピー、バックアップなどが可能になる。データ送信側でデータコピーを実施すると、データ受信側でバックアップが実施される。他のディスクストレージ装置から実施されるコピー操作は、信頼できるストレージリソース管理者が実施するものである。また、ディスクストレージ装置と接続する他のディスクストレージ装置は、相互にユーザデータを利用するため、信頼できるストレージリソース管理者が必須である。従って、ディスクストレージ装置と接続する他のディスクストレージ装置は、TOE を搭載するディスクストレージ装置に限定される。

1.4.4 TOE の機能

TOE が提供する基本機能、およびセキュリティ機能を以下に示す。

1.4.4.1 TOE が提供する基本機能

表 1-1 は TOE が提供する基本機能の一部である。

表 1-1 TOE によって提供される基本機能

機能	概要
可変ボリュームサイズ機能	可変ボリュームサイズ機能は、複数の LDEV（論理ボリューム）を纏めて空きスペースとみなし、任意のサイズのカスタマイズされたボリュームを複数作成することができる。これによりディスク容量を効率良く使用することができる。
キャッシュメモリ管理機能	LDEV（論理ボリューム）内の特定のデータをキャッシュメモリ内に常駐化する。常駐化したデータは常にメモリアクセス性能でアクセス可能となる。
性能情報管理機能	ディスクサブシステム内リソース利用率監視、ディスク負荷、ポート負荷測定等を可能にする。
外部ストレージ管理機能	ディスクストレージのバーチャリゼーション(仮想化技術)を実現する機能。外部ストレージ管理機能を利用することで、VSP を含む複数のディスクサブシステムを1つのディスクサブシステムであるかのように扱うことができる。システム管理者は機種異なる複数のディスクストレージ装置を容易に管理できる。
リモートコピー機能	VSP では、サーバ非経由でリモート(遠隔)サイトにレプリカボリュームを作成することが可能。レプリカボリュームは、局所的/地域的な災害のみでなく広域災害対策等を目的としたバックアップとして利用可能。ホストフリー(非経由)で、レプリカボリュームの更新をメインサイトの更新処理に同期して、ディスクサブシステム間のリモート(遠隔)コピーを実現する。ディスクサブシステム間の接続には、ファイバチャネルを使用する。
非同期リモートコピー機能	非同期リモートコピー機能は、新技術を採用した非同期リモートコピー機能である。キャッシュよりも大容量のディスクドライブに更新履歴(ジャーナル)を蓄積する技術により、回線帯域や業務トラフィックの変動に影響されにくい安定したコピーを実現できる。
ローカルコピー機能	ディスクサブシステム内にホストフリー(非経由)で論理ボリュームのレプリカを作成する、ボリュームレプリケーションを実現する。このレプリカを利用することで、データベースに対するオンライン業務を継続し、且つ業務の性能への影響を極小化しつつ、同データベースのバック

機能	概要
	アップを取得したり、バッチ業務の実行などの並列処理を実現することができる。
仮想ボリューム管理機能	仮想ボリューム管理機能では仮想ボリュームを経由してプール内のボリュームのデータにアクセスする。仮想ボリュームやプールボリュームには、しきい値を設定し、領域があふれないように継続して管理することにより次の効果が得られる。 <ul style="list-style-type: none"> ・ボリュームの稼働率を上げることで導入コストを削減。 ・システム再構築中の運用中断による管理コストや不稼働時間の増大を防止。

1.4.4.2 TOE が提供するセキュリティ機能

1.4.4.2.1 ストレージ管理者および保守員のアクセス制御機能

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

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

ストレージ管理者および保守員のアクセス制御機能はユーザグループの単位で、ロール(権限)を付与し、そのロールで管理できるリソースの集合をリソースグループとして付与する。ユーザ(管理者)、ユーザグループ、リソースグループ、およびロールの対応関係を図 1-3 に示す。

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

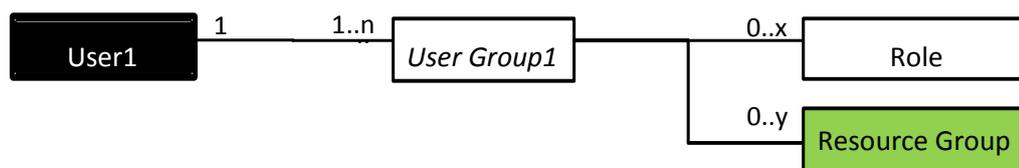


図 1-3 ユーザ、ユーザグループ、ロール、リソースグループの関係

ユーザは、1つ以上のユーザグループに所属する。ユーザグループは、ロールおよびリソースグループが割り当てられ、認可情報として使用する。ユーザグループの情報は SVP PC (管理保守 IF PC) 内部または外部認証サーバから取得して使用する。各アカウントは付与されたリソースに対してロールによって許可された管理操作のみを実行できる。

(1) ロール

セキュリティ管理者は、Storage Navigator (ストレージ管理 UI ソフトウェア) を使用してユーザアカウントを作成し、ユーザグループに登録する。

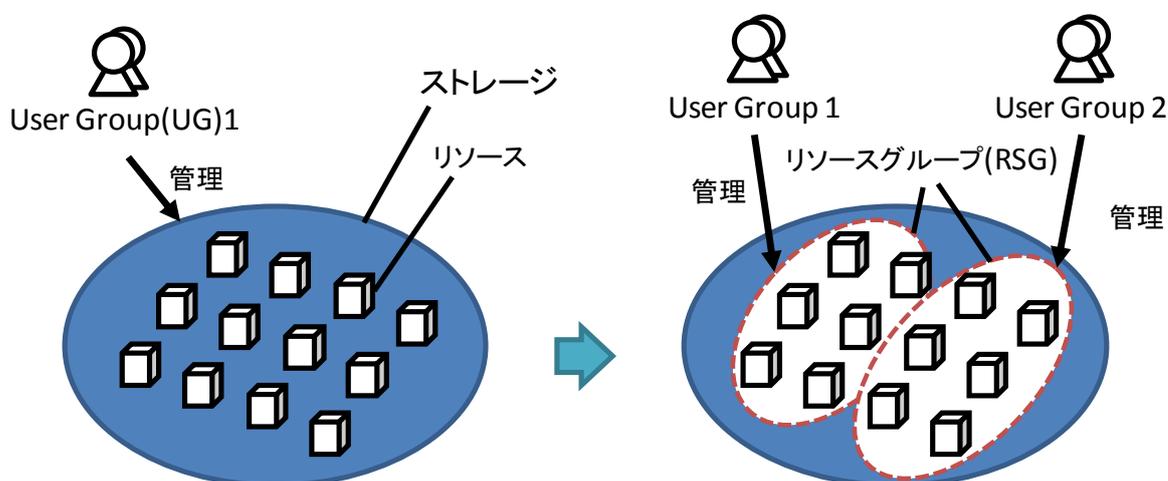
ユーザにどの操作を許可するかは、ユーザグループに付与されているロールで決定する。ロールには、次の分類がある。

表 1-2 ロールの分類と操作内容

ロール	実施可能な操作
セキュリティ管理者ロール	セキュリティ管理者に付与するロールで、ユーザ管理操作、リソース管理操作、ホストおよびファイバチャネルスイッチの識別・認証設定操作、格納データ暗号化操作、外部認証サーバの管理が可能。
監査ログ管理者ロール	監査ログ管理者に付与するロールで、監査ログに関する操作が可能。
ストレージ管理者ロール	ストレージリソース管理者に付与するロールで、許可されたリソースグループ内のストレージ管理操作が可能。
保守員ロール	保守員に付与するロールで、ディスクストレージ装置の保守操作が可能。

(2) リソースグループ

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



1.4.4.2.2 ホストのアクセス制御機能

ユーザデータを格納する LDEV (論理ボリューム) は Storage Navigator (ストレージ管理 UI ソフトウェア)を利用して生成される。ホストから LDEV (論理ボリューム) へアクセスを行うためには、ホストを接続した CHA 上のポートと LDEV (論理ボリューム) の関連付けを行う。具体的には、ホストとアクセスを許可する LDEV (論理ボリューム) とを関係付ける LU 番号を付与して LU パスを設定する。当該 LDEV (論理ボリューム) に対するデータの読み書きは、LU パス設定が行なわれたホストからのみ可能となり、LU パス設定が行なわれていないホストからのデータの読み書きは許可されない。

1.4.4.2.3 ホストが接続されるファイバチャネルスイッチの識別・認証機能

ホストを SAN に接続する場合、不正なホストが接続されないように、顧客運用の中で接続管理が行われる。組織のセキュリティ方針により、より安全を確保するため、不正ホストのなりすまし等を防ぐことが求められる場合、ファイバチャネルスイッチとディスクサブシステムのポートとの通信において、FC-SP 機能(8.1.1 節参照)による識別・認証を行うことができる。ディスクサブシステムのポートは、ファイバチャネルスイッチを識別・認証でき、または、これらのファイバチャネルスイッチにディスクサブシステムのポートを識別・認証させることもできる。ファイバチャネルスイッチの識別・認証設定は、セキュリティ管理者がファイバチャネルスイッチのアクセス制御機能を使用して、ファイバチャネルスイッチの識別・認証を行うかどうかを各ファイバチャネルスイッチに設定する。また、セキュリティ管理者は識別・認証を行うファイバチャネルスイッチの認証データ(WWN、シークレット)をディスクサブシステムに登録する。シークレットは認証用のパスワードであり、12 文字から 32 文字の英数字、記号の組み合わせが可能である。

1.4.4.2.4 ストレージ管理者および保守員の識別・認証機能

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

ユーザの認証方式には以下に示す 2 種類をサポートする。

(1)SVP PC (管理保守 IF PC)内部認証方式

SVP PC (管理保守 IF PC)内に利用者の ID とパスワードを登録し、TOE にて認証する方式。利用者の認証に使用するパスワードは 6 文字から 256 文字(保守員のパスワードは 127 文字)の英数字、記号の組み合わせを可能としている。

(2)外部認証サーバ方式

SVP PC (管理保守 IF PC)で利用者の ID、パスワードを管理せず、外部に設置した認証サーバに ID とパスワードを送信して認証結果を受け取る方式。外部認証サーバで認証成功後に認証サーバからユーザグループ情報を取得し、認可情報として使用することもできる。利用者認証の protocols として LDAP(暗号化は LDAPS、starttls をサポート)、および RADIUS(認証 protocols は CHAP)をサポートする。

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

ディスクストレージ装置と管理 PC 間の通信データの漏洩、改ざんを防ぐため、Storage Navigator (ストレージ管理 UI ソフトウェア)と SVP PC (管理保守 IF PC)間の通信は SSL により暗号化する。また、SVP PC (管理保守 IF PC)–外部認証サーバ間の通信は LDAPS、starttls、および RADIUS(認証 protocols は CHAP) protocols のいずれかを使用することによりストレージ管理者および保守員のパスワードを保護する。

1.4.4.2.6 格納データ暗号化機能

TOE はストレージシステム内のボリュームに格納されたデータを暗号化できる。暗号化および復号は、DKA に搭載されている LSI を利用する。データを暗号化すると、ストレージシステム内のディスクドライブを交換するとき、あるいは、これらが盗難にあったときに情報の漏えいを防ぐことができる。また、以下の鍵管理機能が備わっている。

- 暗号鍵作成機能
- 暗号鍵削除機能
- 暗号鍵バックアップ、リストア機能

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

1.4.4.2.7 シュレッディング機能

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

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

シュレッディング機能はストレージ管理者ロールを持ったユーザアカウントだけが実施できる。

1.4.4.2.8 監査ログ機能

監査ログ機能は、SVP プログラム(Storage Navigator (ストレージ管理 UI ソフトウェア)を含む)および DKCMAIN マイクロプログラムによって提供される。Storage Navigator (ストレージ管理 UI ソフトウェア)は、ログインの成功・失敗、構成や設定の変更などのセキュリティに関連するイベントを記録している。

監査ログ 1 行あたりの最大文字数は、半角 1,024 文字で、最大 250,000 行分の情報が SVP PC (管理保守 IF PC)内の HDD に格納される。Storage Navigator (ストレージ管理 UI ソフトウェア)は監査ログを参照するインタフェースを提供する。

1.4.5 ガイダンス文書

本 TOE を構成するガイダンス文書は以下のとおりである。

(1)セキュリティ機能のユーザズガイド

- Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 ISO15408 認証取得機能 取扱説明書 Ver. 2.9
- Hitachi Virtual Storage Platform G1000 Hitachi Device Manager - Storage Navigator ユーザガイド 初版
- Hitachi Virtual Storage Platform G1000 Storage Navigator メッセージガイド 初版
- Hitachi Virtual Storage Platform G1000 オープンシステム構築ガイド 初版
- Hitachi Virtual Storage Platform G1000 Encryption License Key ユーザガイド初版
- Hitachi Virtual Storage Platform G1000 Volume Shredder ユーザガイド 初版

- Hitachi Virtual Storage Platform G1000 監査ログ リファレンスガイド 初版
- Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 利用者ガイダンス Ver.1.7
- Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 Manual for Obtaining ISO15408 Certification Ver. 2.2
- Hitachi Virtual Storage Platform G1000 Mainframe System Administrator Guide MK-92RD8016-00
- Hitachi Virtual Storage Platform G1000 Hitachi Storage Navigator Messages MK-92RD8017-00i
- Hitachi Virtual Storage Platform G1000 Provisioning Guide for Open Systems MK-92RD8014-00
- Hitachi Virtual Storage Platform G1000 Encryption License Key User Guide MK-92RD8009-00
- Hitachi Virtual Storage Platform G1000 Hitachi Volume Shredder User Guide MK-92RD8025-00
- Hitachi Virtual Storage Platform G1000 Hitachi Audit Log User Guide MK-92RD8008-00i
- Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 User's Guidance Ver.1.4

※出荷時に何れのブランドに応じて対応したガイダンスが一式配付される。

(2)ディスクサブシステムの保守マニュアル

- Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 ISO15408 認証取得機能 メンテナンスマニュアル Ver. 2.3
- A/H-65AD A-65BD HT-40BD ディスクアレイシステム メンテナンスマニュアル REV.0.1
- Hitachi Virtual Storage Platform G1000 / Hitachi Virtual Storage Platform VX7 Obtaining ISO15408 Certification Maintenance Manual Ver. 2.0
- DKC810I Maintenance Manual REV.0.1

※A/H-65AD A-65BD HT-40BD は VSP の国内の型名であり、DKC810I は VSP の海外の型名である。出荷時に何れのブランドに応じて対応した保守マニュアルが一式配付される。

1.5 評価環境

本 TOE の評価環境を下記に示す。管理 PC、ファイバチャネルスイッチ、ファイバチャネル接続アダプタは TOE 評価の実施期間、以下の何れかの環境を使用する。

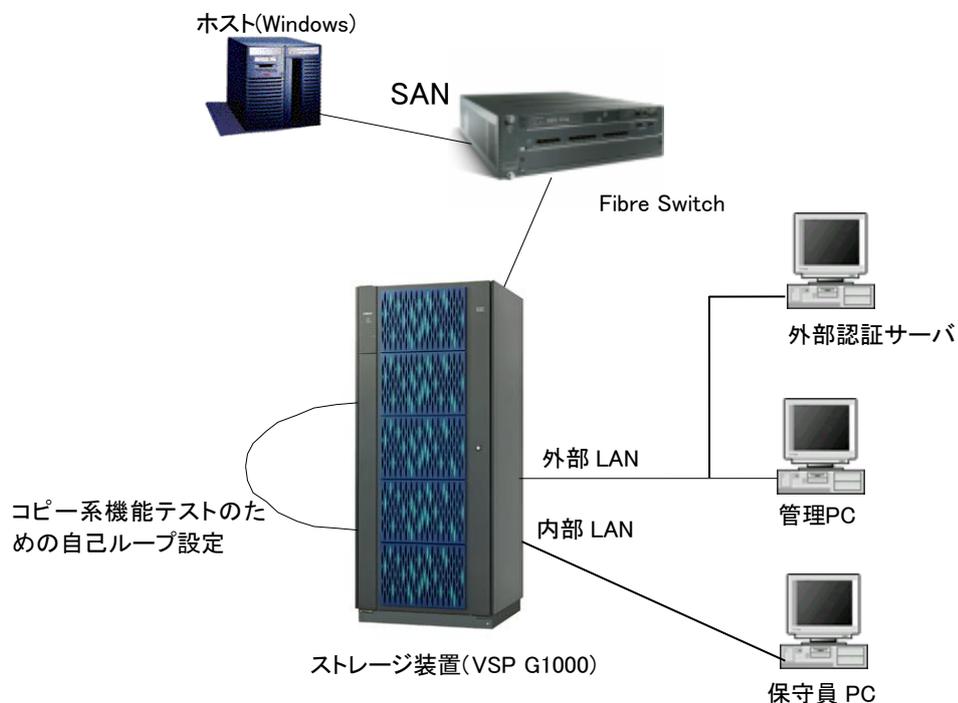


表 1-3 テストで使用した TOE 構成要素

項番	構成要素	ソフトウェア/OS
1	Hitachi Virtual Storage Platform G1000	DKCMAIN マイクロプログラム : 80-01-25-00/00
2	SVP	SVP プログラム : 80-01-25/00 JDK : 1.7.0_21 Apache : 2.4.4 Apache Tomcat : 7.0.39 OpenSSL : 1.0.1g ActivePerl : 5.16.2.1602 Flash Player : 11.6.602.180

表 1-4 テストで使用した Hitachi Unified Storage VM の物理構成要素

項番	構成要素	数	備考
1	Hitachi Virtual Storage Platform G1000	1 台	
1-1	MP パッケージ	2 台	

1-2	CHA	4 台	
1-3	暗号 DKA	2 台	
1-4	Cache	16G×4 枚	
1-5	2.5 インチ ディスクドライブ	12 台	RAID1(2D+2D)の パリティグループ 3 個

表 1-5 テストで使用したホスト

項番	ホスト OS
1	Windows 2008 Server

表 1-6 テストで使用した管理 PC

項番	管理 PC OS	Java ランタイム環境	Web ブラウザおよびプラグイン
1	Windows7(SP1)	JRE 1.7.0_21	Internet Explorer 10.0 Flash Player 11.6

表 1-7 テストで使用した保守員 PC

項番	保守員 PC OS	Java ランタイム環境	Web ブラウザおよびプラグイン
1	Windows7 (SP1)	JRE 1.7.0_21	Internet Explorer 10.0 Flash Player 11.6

表 1-8 テストで使用した外部認証サーバ

項番	外部認証サーバ OS	ソフトウェア
1	Windows 2008 Server	Active Directory LDAP v3 サポート RFC2865 準拠

表 1-9 テストで使用したファイバチャネルスイッチ

項番	スイッチ	型名	FW version
1	Brocade300	BR-360-0008	Fabric OS v6.4.1b
2	Brocade6505	ER-7000-0340	Fabric OS v7.2.0c

表 1-10 テストで使用したファイバチャネル接続アダプタ

項番	ファイバチャネル接続アダプタ	型名	ドライバ	バージョン
1	Emulex LightPulse	Lpe12002-M-HI	Storport Miniport Driver	7.2.20.6
2	Brocade 16G FC HBA	BR-1860-2P00	bfa	3.2.1.0
3	Qlogic Fibre Channel Adapter	QLE2564-CK	Fibre Channel Adapter STOR miniport driver	9.1.4.6

2 適合主張

2.1 CC 適合主張

本 ST は以下の規格に適合する。

情報技術セキュリティ評価のためのコモンクライテリア

パート 1：概説と一般モデル バージョン 3.1 改訂第 4 版 翻訳第 1.0 版

パート 2：セキュリティ機能コンポーネント バージョン 3.1 改訂第 4 版 翻訳第 1.0 版

パート 3：セキュリティ保証コンポーネント バージョン 3.1 改訂第 4 版 翻訳第 1.0 版

セキュリティ機能要件：パート 2 適合

セキュリティ保証要件：パート 3 適合

2.2 PP 主張

本 ST が適合している PP はない。

2.3 パッケージ主張

本 ST はパッケージ：EAL2 に適合する。ALC_FLR.1 の保証コンポーネントを追加する。

3 セキュリティ課題定義

3.1 TOE 資産

ディスクストレージ装置にとって最も重要な資産は、ディスクドライブ内に格納されているストレージ利用者のユーザデータである。ユーザデータの完全性および機密性を維持するため、ストレージ管理者による権限外の設定変更、第三者による権限外のアクセスからユーザデータを保護する。また、外部 LAN に接続可能な第三者による Storage Navigator (ストレージ管理 UI ソフトウェア)–SVP PC (管理保守 IF PC)間および SVP PC (管理保守 IF PC)–外部認証サーバ間通信データの盗聴に対して、高信頼チャネルを使用することにより、通信データに含まれる TSF データ(ユーザ ID、パスワードなど)を保護する必要がある。

本 ST では、ディスクサブシステム内に複数の会社・部署・システム・アプリケーションのデータが混在する大規模ストレージ集約環境において、リソースグループ内に存在するストレージ利用者のユーザデータが保護対象資産であり、第三者による権限外のアクセスから保護対象資産を保護する。

3.2 脅威

TOE はこの章に示した脅威に対抗している。以下の記載の中で第三者とはストレージ管理者、ストレージ利用者、保守員のいずれにも該当しない人物であり、ディスクストレージ装置の利用権限を持たないことを想定している。

T.TSF_COMP	第三者が、外部 LAN から不正にストレージ管理者の ID とパスワードなどを含む通信データを取得することにより、ストレージ管理者になりすましてディスクストレージ装置の設定を変更し、ユーザデータが格納されている LDEV (論理ボリューム) にアクセスできてしまうかもしれない。
T.LP_LEAK	複数のホストが同一ポートに接続する SAN 環境で、第三者が、他のホストから特定ホストの LDEV (論理ボリューム) にアクセスすることにより、ユーザデータの漏洩、改ざん、削除が行えるかもしれない。
T.CHG_CONFIG	第三者が、ディスクストレージ装置の LDEV (論理ボリューム) へのアクセス設定を不正に変更することにより、ユーザデータの漏洩、改ざん、削除が行えるかもしれない。
T.HDD_THEFT	予防保守や故障のため、ディスクドライブをベンダに返却する際、そのディスクドライブの搬送中に盗難され、ユーザデータが漏えいするかもしれない。
T.HDD_REUSE	ディスクストレージ装置の再使用または、ディスクドライブの再使用により、ディスクドライブ内に残っているユーザデータが第三者に漏洩するかもしれない。

3.3 組織のセキュリティ方針

P.MASQ	顧客要求によってホストが接続されるファイバチャネルスイッチの識別・認証が求められる場合は、ホストが接続されるファイバチャネルスイッチの識別・認証が行われる。
--------	--

3.4 前提条件

- A.NOEVIL** ストレージ管理者のうち、セキュリティ管理者、監査ログ管理者は、ディスクストレージ装置全体の管理・運用を行うために十分な能力を持ち、手順書で定められた通りの操作を行い、不正行為を働かないことを信頼できるものと想定する。
ストレージリソース管理者は、セキュリティ管理者から許可された範囲内においてディスクサブシステムの管理・運用を行うために十分な能力を持ち、手順書で定められた通りの操作を行い、不正行為を働かないことを信頼できるものと想定する。
- A.PHYSICAL_SEC** セキュリティ管理者は、ディスクストレージ装置、ホスト(ファイバチャネル接続アダプタを含む)、SAN 環境を構成する機器(ファイバチャネルスイッチ、ケーブル)、他のディスクストレージ装置、外部認証サーバを入退室が管理されたセキュアなエリアに設置し、各機器に設定されている設定値 (WWN など) や接続状態 (SAN への接続状態) が維持されるよう適切に運用管理が行われるものと想定する。
- A.MANAGE_SECRET** ホストが接続されるファイバチャネルスイッチに設定されているファイバチャネルスイッチ認証用のシークレットは、セキュリティ管理者の責任において、許可されていない人物に利用されないように管理されているものと想定する。
- A.MANAGEMENT_PC** ストレージ管理者は、管理 PC の不正な利用が行われないように適切に設置および管理を行うものと想定する。
- A.MAINTENANCE_PC** 組織の責任者が、保守契約を結んだ場合は、保守員と保守員 PC の受入れを許可し、セキュアなエリアで保守員に入室させ、保守員に保守員 PC の設置を許可する。また保守員以外の人間が保守員 PC に不正に利用しないと想定する。
- A.CONNECT_STORAGE** TOE に接続する他のディスクストレージ装置は TOE の搭載されているディスクストレージ装置に限定される運用を想定する。
- A.EXTERNAL_SERVER** 外部認証サーバは、TOE がサポートする SVP PC (管理保守 IF PC) との通信を保護することができる認証プロトコル(LDAPS、starttls、および RADIUS(認証プロトコルは CHAP))が利用可能であり、ユーザ識別情報およびユーザグループ情報を TOE と整合の取れた状態で適切に登録および管理できるものと想定する。

4 セキュリティ対策方針

本章では TOE のセキュリティ対策方針、運用環境のセキュリティ対策方針、およびセキュリティ対策方針根拠について記述する。

4.1 TOE のセキュリティ対策方針

TOE のセキュリティ対策方針を以下に示す。

O.ADM_AUTH	TOE は、ストレージ管理者および保守員がディスクサブシステムの管理操作を行う前に、ストレージ管理者および保守員の識別・認証が成功していなければならない。
O.ADM_ROLE	TOE は、ストレージ管理者および保守員の行う管理操作を以下のように制限しなければならない。 <ul style="list-style-type: none"> ・ セキュリティ管理者は、ユーザ管理操作、リソース管理操作、ホストおよびファイバチャネルスイッチの識別・認証設定操作、格納データ暗号化操作、外部認証サーバの管理操作が可能。 ・ 監査ログ管理者は、監査ログに関する操作が可能。 ・ ストレージリソース管理者は、許可されたリソースグループ内のストレージ管理操作が可能。 ・ 保守員は、ディスクストレージ装置の保守操作が可能。
O.SEC_COMM	TOE は、Storage Navigator (ストレージ管理 UI ソフトウェア)–SVP PC (管理保守 IF PC)間の通信路および SVP PC (管理保守 IF PC)–外部認証サーバ間の通信路から通信データの盗聴を防止するため、Storage Navigator (ストレージ管理 UI ソフトウェア)–SVP PC (管理保守 IF PC)間の通信データおよび SVP PC (管理保守 IF PC)–外部認証サーバ間の通信データの暗号化によるセキュアな通信機能を提供しなければならない。
O.SWITCH_AUTH	TOE はファイバチャネルスイッチが接続された際には、FC-SP 機能によりホストが接続されるファイバチャネルスイッチの識別・認証を行わなければならない。
O.HOST_ACCESS	TOE はホストを識別し、ディスクストレージ装置に接続を許可されているホストが、許可された LDEV (論理ボリューム) のみにアクセスするように制御しなければならない。
O.HDD_ENC	TOE は、ディスクストレージ装置から取り出したディスクドライブからユーザデータが漏洩しないように、格納データ暗号化の暗号鍵を管理しなければならない。
O.HDD_SHRED	TOE は、ディスクストレージ装置のディスクドライブを交換または使用停止するときに、ディスクドライブ内のユーザデータが残らないようにユーザデータをシュレディングしなければならない。
O.AUD_GEN	TOE は、識別認証の事象、または設定変更の操作事象など、セキュリティに関連する事象を追跡しなければならない。

4.2 運用環境のセキュリティ対策方針

運用環境のセキュリティ対策方針を以下に示す。

- OE.NOEVIL** 組織の責任者は、ストレージ管理者のうち、セキュリティ管理者、監査ログ管理者には、ディスクストレージ装置全体の管理・運用を行うために十分な能力を持ち、手順書で定められた通りの操作を行い、不正行為を働かないことを信頼できる人物を割り当てられなければならない。ストレージリソース管理者は、セキュリティ管理者から許可された範囲内においてディスクサブシステムの管理・運用を行うため、手順書で定められた通りの操作を行えるように研修が行われ、不正行為を働かないことを信頼できる人物が割り当てられなければならない。
- OE.PHYSICAL_SEC** セキュリティ管理者は、ディスクストレージ装置、ホスト(ファイバチャネル接続アダプタを含む)、SAN 環境を構成する機器(ファイバチャネルスイッチ、ケーブル)、他のディスクストレージ装置、外部認証サーバをストレージ管理者および保守員のみ入退出が許可されているセキュアなエリアに設置し、許可されていない設定値の変更や接続先の付け替えなどから完全に保護されていないなければならない。
- OE.MANAGE_SECRET** セキュリティ管理者は、ファイバチャネルスイッチに設定されているファイバチャネルスイッチ認証用のシークレットを許可されていない人物に利用されないように管理しなければならない。
- OE.MANAGEMENT_PC** ストレージ管理者は、管理 PC が不正に利用されないように適切に設置および管理しなければならない。
- OE.MAINTENANCE_PC** 保守員は、組織の責任者の指示に従い、保守員 PC をセキュアなエリアに適切に設置する。保守員 PC は保守員以外の人間が利用できないようにしなければならない。
- OE.CONNECT_STORAGE** TOE と接続する他のディスクストレージ装置は、TOE から構成されたディスクストレージ装置に限定しなければならない。
- OE.EXTERNAL_SERVER** セキュリティ管理者は、外部認証サーバに TOE がサポートしている SVP PC (管理保守 IF PC)との通信を保護することができるプロトコル(LDAPS、starttls、および RADIUS(認証プロトコルは CHAP))を使用しなければならない。また、ユーザ識別情報およびユーザグループ情報を TOE と整合の取れた状態で適切に登録および管理しなければならない。
- OE.FC-SP_HBA** ホストが接続されるファイバチャネルスイッチの識別・認証が必要な場合は、FC-SP 機能付きのファイバチャネル接続アダプタおよび FC-SP 機能付きのファイバチャネルスイッチを使用しなければならない。
- OE.HDD_ENC** 運用環境では、ディスクドライブからユーザデータが漏洩しないように、DKA に搭載されている LSI を利用してユーザデータを暗号化できるディスクストレージ装置を使用しなければならない。

4.3 セキュリティ対策方針根拠

セキュリティ対策は、セキュリティ課題定義で規定した前提条件に対応するためのもの、ある

いは脅威に対抗するためのもの、あるいは組織のセキュリティ方針を実現するためのものである。セキュリティ対策方針と対応する前提条件、対抗する脅威、組織のセキュリティ方針の対応関係を表 4-1 に示す。

表 4-1 TOE セキュリティ課題とセキュリティ対策方針の対応

		セキュリティ対策方針																	
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.SWITCH_AUTH	O.HOST_ACCESS	O.AUD_GEN	O.HDD_ENC	O.HDD_SHRED	OE.NOEVIL	OE.PHYSICAL_SEC	OE.MANAGE_SECRET	OE.MANAGEMENT_PC	OE.MAINTENANCE_PC	OE.CONNECT_STORAGE	OE.EXTERNAL_SERVER	OE.FC-SP_HBA	OE.HDD_ENC	
TOEセキュリティ課題	A.NOEVIL									X									
	A.PHYSICAL_SEC										X								
	A.MANAGE_SECRET											X							
	A.MANAGEMENT_PC												X						
	A.MAINTENANCE_PC													X					
	A.CONNECT_STORAGE														X				
	A.EXTERNAL_SERVER																X		
	T.TSF_COMP			X													X		
	T.LP_LEAK					X					X								
	T.CHG_CONFIG	X	X				X												
	T.HDD_THEFT							X											X
	T.HDD_REUSE								X										
	P.MASQ				X													X	

4.3.1 前提条件に対するセキュリティ対策方針の根拠

表 4-2 は、セキュリティ対策方針によって、前提条件が対応されていることを示している。

表 4-2 前提条件に対するセキュリティ対策方針の正当性

前提条件	前提条件がカバーされていることの根拠
A.NOEVIL	A.NOEVIL は、OE.NOEVIL にあるように、ディスクストレージ装置全体の管理・運用を行うために、セキュリテ

	イ管理者、監査ログ管理者に信頼できる人物を割り当てる。また、権限を持つ管理者から許可された範囲内のディスクサブシステムの管理・運用を行うために、ストレージリソース管理者に信頼できる人物を割り当てることによって充足する。
A.PHYSICAL_SEC	A.PHYSICAL_SEC は、OE.PHYSICAL_SEC にあるように、ディスクストレージ装置、ホスト(ファイバチャネル接続アダプタを含む)、SAN 環境を構成する機器(ファイバチャネルスイッチ、ケーブル)、他のディスクストレージ装置、外部認証サーバは、セキュリティ管理者、ストレージリソース管理者、監査ログ管理者および保守員のみ入退出が許可されているセキュアなエリアに設置され、許可されていない設定値の変更や接続先の付け替えなどから完全に保護される。
A.MANAGE_SECRET	A.MANAGE_SECRET は、OE.MANAGE_SECRET にあるように、セキュリティ管理者によりホストが接続されるファイバチャネルスイッチの認証用のシークレットが許可されていない人物に利用されないように管理されることによって充足する。
A.MANAGEMENT_PC	A.MANAGEMENT_PC は、OE.MANAGEMENT_PC にあるように、ストレージ管理者が管理 PC の不正な利用が行われぬように適切に設置および管理することによって充足する。
A.MAINTENANCE_PC	A.MAINTENANCE_PC は、OE.MAINTENANCE_PC にあるように、保守員が適切に保守員 PC を管理し、保守員以外の人間が利用できないことによって充足する。
A.CONNECT_STORAGE	A.CONNECT_STORAGE は、OE.CONNECT_STORAGE にあるように、TOE に接続する他のディスクストレージ装置は TOE から構成されるディスクストレージ装置に限定することで、前提条件を満たす運用が実現できる。
A.EXTERNAL_SERVER	A.EXTERNAL_SERVER は、OE.EXTERNAL_SERVER にあるように、外部認証サーバは、TOE がサポートする SVP PC (管理保守 IF PC)との通信を保護することができる認証プロトコルが利用可能で、ユーザ識別情報およびユーザグループ情報を TOE と整合の取れた状態で適切に登録および管理できるため、前提条件を満たす運用が実現できる。

4.3.2 脅威に対するセキュリティ対策方針の根拠

表 4-3 は、セキュリティ対策方針によって、脅威が対抗されていることを示している。

表 4-3 脅威に対するセキュリティ対策方針の正当性

脅威	脅威が対抗されていることの根拠
T.TSF_COMP	<p>T.TSF_COMP は、下記に示す通り、O.SEC_COMM および OE.EXTERNAL_SERVER によって対抗される。</p> <ul style="list-style-type: none"> • Storage Navigator (ストレージ管理 UI ソフトウェア) – SVP PC (管理保守 IF PC)間の通信は暗号化通信を使用しており、不正に機器を接続することによる盗聴などの脅威を軽減できる。 • SVP PC (管理保守 IF PC) – 外部認証サーバ間の通信は、暗号化通信を使用しており、不正に機器を接続することによる盗聴などの脅威を軽減できる。 • SVP PC (管理保守 IF PC) – 外部認証サーバ間の通信プロトコルには、LDAPS、starttls、および RADIUS (認証プロトコルは CHAP) のいずれかを使用し、外部認証サーバに登録されているユーザ種別情報およびグループ情報を TOE と整合の取れた状態で適切に管理することで、ストレージ管理者および保守員のユーザ ID、パスワード、グループ情報が漏洩する脅威を軽減できる。
T.LP_LEAK	<p>T.LP_LEAK は、下記に示す通り、O.HOST_ACCESS および OE.PHYSICAL_SEC によって対抗される。</p> <ul style="list-style-type: none"> • TOE はホストを識別し、ディスクストレージ装置に接続を許可されているホストが、許可された LDEV (論理ボリューム) のみにアクセスできるように制御するため、脅威は軽減される。 • ディスクストレージ装置、ホスト(ファイバチャネル接続アダプタを含む)、ファイバチャネルスイッチ、他のディスクストレージ装置、外部認証サーバは、セキュリティ管理者、ストレージリソース管理者、監査ログ管理者および保守員のみ入退出が許可されているセキュアなエリアに設置され、許可されない物理的アクセスから完全に保護されるため、脅威は軽減される。
T.CHG_CONFIG	<p>T.CHG_CONFIG は、下記に示す通り、O.ADM_AUTH、O.ADM_ROLE、O.AUD_GEN によって対抗される。</p> <ul style="list-style-type: none"> • TOE は、Storage Navigator (ストレージ管理 UI ソフトウェア)の利用者を、ディスクサブシステムの管理操作を行う前に、識別・認証し、成功しなければ操作を拒否するため、第三者からの不正アクセスは軽減される。 • TOE は、ストレージ管理者および保守員を識別・認証し、ストレージ管理者および保守員の行う管理操作を以下のように制限することにより、脅威を軽減する。 <ul style="list-style-type: none"> ➤ セキュリティ管理者は、ユーザ管理操作、リソース管理操作、ホストおよびファイバチャネル

脅威	脅威が対抗されていることの根拠
	<p>スイッチの識別・認証設定操作、格納データ暗号化操作、外部認証サーバの操作が可能。</p> <ul style="list-style-type: none"> ➤ 監査ログ管理者は、監査ログに関する操作が可能。 ➤ ストレージリソース管理者は、許可されたリソースグループ内のストレージ管理操作が可能。 ➤ 保守員は、ディスクストレージ装置の保守操作が可能。 <p>・ TOE は、識別・認証失敗時のセキュリティに関する事象を追跡できるため、第三者からの不正アクセスの発生を軽減することができる。</p>
T.HDD_THEFT	<p>T.HDD_THEFT は、下記に示す通り、O.HDD_ENC および OE.HDD_ENC によって対抗される。</p> <ul style="list-style-type: none"> ・ TOE は、ディスクドライブ内のユーザデータを暗号化するとき使用する暗号鍵を管理することにより、ディスクドライブからユーザデータが漏洩する脅威を軽減できる。 ・ ディスクストレージ装置の DKA に搭載されている LSI を利用してユーザデータを暗号化できるため、ディスクストレージ装置から持ち出したディスクドライブからユーザデータが漏洩する脅威を軽減することができる。
T.HDD_REUSE	<p>T.HDD_REUSE は、下記に示す通り、O.HDD_SHRED によって対抗される。</p> <ul style="list-style-type: none"> ・ TOE は、ディスクストレージ装置のディスクドライブの使用停止時にディスクドライブ内のユーザデータをシュレッディングすることにより使用を停止したディスクドライブからユーザデータが漏洩する脅威を除去することができる。

4.3.3 組織のセキュリティ方針に対するセキュリティ対策方針の根拠

表 4-4 は、セキュリティ対策方針によって、組織のセキュリティ方針が実現されていることを示している。

表 4-4 組織のセキュリティ方針に対するセキュリティ対策方針の正当性

組織のセキュリティ方針	組織のセキュリティ方針が実現されていることの根拠
P.MASQ	<p>P.MASQ は、下記に示す通り、O.SWITCH_AUTH および OE.FC-SP_HBA によって実現される。</p> <ul style="list-style-type: none"> ・ ホストが接続されるファイバチャネルスイッチの識別・認証を行う場合は、ホストに FC-SP 機能付きのファイバチャネル接続アダプタを搭載し、FC-SP 機能

	<p>付きのファイバチャネルスイッチを使用する。</p> <ul style="list-style-type: none">• TOE はファイバチャネルスイッチから当該ポートにアクセスされる前に FC-SP 機能によりファイバチャネルスイッチとの識別・認証を行う。
--	---

5 拡張コンポーネント定義

本 ST は CC パート 2 および CC パート 3 に適合しており、拡張コンポーネントは定義しない。

6 セキュリティ要件

本章では、セキュリティ要件を記述する。

6.1 セキュリティ機能要件

TOE が提供するセキュリティ機能要件を記述する。

以下のコンポーネントは CC パート 2 に含まれるものである。

機能要件の操作（選択、割付、詳細化）について、表記方法を以下に示す。

選択の場合は、[選択：機能要件の記述]：選択した内容

割付の場合は、[割付：機能要件の記述]：割付した内容

詳細化の場合は、[詳細化：機能要件の記述]：詳細化した内容 のように表記する。

また、重複して定義している機能要件の末尾のアルファベットは、以下の内容を示している。

- a：ストレージ管理者および保守員の識別・認証とアクセス制御に関する機能要件を示す。
- b：ホストが接続されるファイバチャネルスイッチの識別・認証とホストのアクセス制御に関する機能要件を示す。

○セキュリティ監査 (FAU)

FAU_GEN.1 監査データ生成

下位階層：なし

依存性：FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.1.1 TSF は、以下の監査対象事象の監査記録を生成できなければならない：

- a) 監査機能の起動と終了;
- b) 監査の[選択：最小、基本、詳細、指定なし：から一つのみ選択]レベルのすべての監査対象事象; 及び
- c) [割付：上記以外の個別に定義した監査対象事象]。

FAU_GEN.1.2 TSF は、各監査記録において少なくとも以下の情報を記録しなければならない：

- a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗); 及び
- b) 各監査事象種別に対して、PP/ST の機能コンポーネントの監査対象事象の定義に基づいた、[割付：その他の監査関連情報]

[選択：最小、基本、詳細、指定なし：から一つのみ選択]：指定なし

[割付：上記以外の個別に定義した監査対象事象]：表 6-1 の「監査項目」に記述する監査事象。

[割付：その他の監査関連情報]：なし

表 6-1 個別に定義した監査対象事象

機能要件	監査項目
FAU_GEN.1	なし。

機能要件	監査項目
FAU_GEN.2	なし。
FAU_SAR.1	なし。
FAU_STG.1	なし。
FAU_STG.3	なし。
FAU_STG.4	なし。
FCS_CKM.1	・ 格納データ暗号化の暗号鍵生成の成功または失敗をログに取得。
FCS_CKM.4	・ 格納データ暗号化の暗号鍵削除の成功または失敗をログに取得。
FDP_ACC.1	なし。
FDP_ACF.1	なし。
FDP_RIP.1	・ ユーザデータのシュレディング開始、停止の成功または失敗をログに取得。
FIA_AFL.1	なし。認証試行の閾値到達はログに記録しない。
FIA_ATD.1a	なし。
FIA_ATD.1b	なし。
FIA_SOS.1a	なし。尺度の不一致はログに記録しない。
FIA_SOS.1b	なし。尺度の不一致はログに記録しない。
FIA_UAU.2	<ul style="list-style-type: none"> ・ ストレージ管理者および保守員の識別・認証の成功または失敗をログに取得。 ・ FC-SP によるホストが接続されるファイバチャネルスイッチの識別・認証の結果をログに取得。
FIA_UID.2	<ul style="list-style-type: none"> ・ ストレージ管理者および保守員の識別・認証の成功または失敗をログに取得。 ・ FC-SP によるホストが接続されるファイバチャネルスイッチの識別・認証の結果をログに取得。
FIA_USB.1a	なし。
FIA_USB.1b	なし。
FMT_MOF.1	<ul style="list-style-type: none"> ・ 格納データ暗号化機能の有効/無効設定操作をログに取得。 ・ FC-SP によるファイバチャネルスイッチの認証有無の設定変更をログに取得。 ・ シュレディング機能の開始、停止の操作をログに取得。
FMT_MSA.1	<ul style="list-style-type: none"> ・ LU パス情報の作成、削除をログに取得。 ・ ユーザグループにユーザアカウントを追加または削除したことをログに取得。 ・ ユーザグループにロールを追加または削除したことをログに取得。 ・ ユーザグループにリソースグループを追加または削除したことをログに取得。
FMT_MSA.3	なし。
FMT_MTD.1	<ul style="list-style-type: none"> ・ ユーザアカウントのユーザ ID 作成、削除、パスワードの変更をログに取得。 ・ ファイバチャネルスイッチの WWN、シークレットの作成、変更、削除をログに取得。 ・ 格納データ暗号化の暗号鍵の生成、削除、バックアップ、リストアをログに取得。

機能要件	監査項目
	<ul style="list-style-type: none"> ユーザ認証方式の変更をログに取得。
FMT_MTD.3	<ul style="list-style-type: none"> 格納データ暗号化の暗号鍵をリストアしたことをログに取得。
FMT_SMF.1	<ul style="list-style-type: none"> ユーザアカウントのユーザ ID 作成、削除、パスワードの変更、所属するユーザグループの変更をログに取得。 ファイバチャネルスイッチの WWN、シークレットの作成、変更、削除をログに取得。
FMT_SMR.1	<ul style="list-style-type: none"> ユーザアカウントの所属するユーザグループの変更をログに取得。 ユーザグループにロールを追加または削除したことをログに取得。
FPT_STM.1	なし。
FTP_ITC.1	<ul style="list-style-type: none"> ストレージ管理者および保守員の識別・認証の成功または失敗をログに取得。
FTP_TRP.1	<ul style="list-style-type: none"> ストレージ管理者および保守員の識別・認証の成功または失敗をログに取得。

FAU_GEN.2 利用者識別情報の関連付け

下位階層：なし

依存性：FAU_GEN.1 監査データ生成
FIA_UID.1 識別のタイミング

FAU_GEN.2.1 識別された利用者のアクションがもたらした監査事象に対し、TSFは、各監査対象事象を、その原因となった利用者の識別情報に関連付けられなければならない。

FAU_SAR.1 セキュリティ監査レビュー

下位階層：なし

依存性：FAU_GEN.1 監査データ生成

FAU_SAR.1.1 TSFは、[割付：許可利用者]が、[割付：監査情報のリスト]を監査記録から読み出せるようにしなければならない。

FAU_SAR.1.2 TSFは、利用者に対し、その情報を解釈するのに適した形式で監査記録を提供しなければならない。

[割付：許可利用者]：監査ログ管理者

[割付：監査情報のリスト]：表 6-2 の「監査情報」に記述する。

表 6-2 監査情報

監査事象	監査情報
ストレージ管理者の識別・認証	<ul style="list-style-type: none"> ストレージ管理者の識別・認証の成功または失敗、識別・認証実施日時、Storage Navigator (ストレージ管理 UI ソフトウ

監査事象	監査情報
	エア)のユーザ ID、管理 PC の IP アドレス
保守員の識別・認証	<ul style="list-style-type: none"> 保守員の識別・認証の成功または失敗、識別・認証実施日時、保守員のユーザ ID、保守員 PC の IP アドレス
ストレージ管理者および保守員のユーザアカウントの作成、変更、削除	<ul style="list-style-type: none"> ユーザアカウントのユーザ ID の作成、削除を実施したセキュリティ管理者のユーザ ID、操作日時、操作対象のユーザ ID、認証方式、操作内容（作成、変更、削除）、操作結果（成功、失敗）
ストレージ管理者および保守員のユーザアカウントのパスワード変更	<ul style="list-style-type: none"> ユーザアカウントのパスワードを変更したストレージ管理者および保守員のユーザ ID、操作日時、操作対象のユーザ ID、操作結果（成功、失敗）
ストレージ管理者および保守員のユーザアカウントが所属するユーザグループの変更	<ul style="list-style-type: none"> ユーザグループの変更を実施したセキュリティ管理者のユーザ ID、操作日時、ユーザグループ名称、ロール名称、リソースグループ名称、操作内容（ロール追加、ロール削除、RSG 番号追加、RSG 番号削除）、操作結果（成功、失敗）
LU パス情報の作成、削除	<ul style="list-style-type: none"> LU パス情報の作成、削除を実施したストレージリソース管理者のユーザ ID、操作日時、操作内容（作成、削除）、ポート番号、ホストの WWN、LU 番号、LDEV（論理ボリューム）番号、操作結果（成功、失敗）
ファイバチャネルスイッチの WWN、シークレットの作成、変更、削除	<ul style="list-style-type: none"> ファイバチャネルスイッチの WWN、シークレット（セキュリティ管理者のみ可能）の作成、変更、削除を実施したストレージリソース管理者、セキュリティ管理者、保守員のユーザ ID、操作日時、ポート番号、ファイバチャネルスイッチの WWN、操作内容（作成、変更、削除）、操作結果（成功、失敗）
FC-SP によるファイバチャネルスイッチの認証有無の設定変更	<ul style="list-style-type: none"> FC-SP によるファイバチャネルスイッチの認証有無の変更を実施したセキュリティ管理者のユーザ ID、操作日時、ファイバチャネルスイッチの WWN、認証有無、操作内容（変更）、操作結果（成功、失敗）
FC-SP によるファイバチャネルスイッチの認証	<ul style="list-style-type: none"> 認証を行ったファイバチャネルスイッチの WWN、認証実施日時、認証結果
格納データ暗号化の有効/無効設定	<ul style="list-style-type: none"> 格納データ暗号化の有効/無効設定を設定したセキュリティ管理者のユーザ ID、操作日時、パリティグループ番号、暗号化有効/無効設定内容、設定したパリティグループの数、操作結果（成功、失敗）
格納データ暗号化の暗号鍵の生成、削除、バックアップ、リストア	<ul style="list-style-type: none"> 格納データ暗号化の暗号鍵の生成、削除、バックアップ、リストアを実施したセキュリティ管理者のユーザ ID、操作日時、操作内容（生成、削除、バックアップ、リストア）、暗

監査事象	監査情報
	号鍵番号、操作した暗号鍵の数、操作結果（成功、失敗）
シュレディングの開始、停止	<ul style="list-style-type: none"> ボリュームシュレディングを実施したストレージリソース管理者のユーザ ID、操作日時、操作内容（開始、停止）、書込みデータ、書込み回数、対象 LDEV（論理ボリューム）番号、対象 LDEV（論理ボリューム）数、シュレディング処理の実行順番、操作結果（成功、失敗）

FAU_STG.1 セキュリティ監査証跡格納

下位階層：なし

依存性：FAU_GEN.1 監査データ生成

FAU_STG.1.1 TSF は、監査証跡に格納された監査記録を不正な削除から保護しなければならない。

FAU_STG.1.2 TSF は、監査証跡に格納された監査記録への不正な改変を[選択：防止、検出：から一つのみ選択]できねばならない。

[選択：防止、検出：から一つのみ選択]：防止

FAU_STG.3 監査データ損失の恐れ発生時のアクション

下位階層：なし

依存性：FAU_STG.1 保護された監査証跡格納

FAU_STG.3.1 TSF は、監査証跡が[割付：事前に定義された限界]を超えた場合、[割付：監査格納失敗の恐れ発生時のアクション]をとらなければならない。

[割付：事前に定義された限界]：175,000 行

[割付：監査格納失敗の恐れ発生時のアクション]：Storage Navigator (ストレージ管理 UI ソフトウェア)画面で警告

FAU_STG.4 監査データ損失の防止

下位階層：FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性：FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[選択：監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き：から1つのみ選択]及び[割付：監査格納失敗時にとられるその他のアクション]を行わなければならない。

[選択：監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最も古くに格納された監査記録への上書き：から1つのみ選択]：最も古くに格納された監査記録への上書き

[割付：監査格納失敗時にとられるその他のアクション]：なし

○暗号サポート (FCS)

FCS_CKM.1 暗号鍵生成

下位階層：なし

依存性：[FCS_CKM.2 暗号鍵配付、または

FCS_COP.1 暗号操作]

FCS_CKM.4 暗号鍵破棄

FCS_CKM.1.1 TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵生成アルゴリズム[割付：暗号鍵生成アルゴリズム]と指定された暗号鍵長[割付：暗号鍵長]に従って、暗号鍵を生成しなければならない。

[詳細化：暗号鍵]：格納データ暗号化の暗号鍵

[割付：標準のリスト]：表 6-3 の「規格」に示す。

[割付：暗号鍵生成アルゴリズム]：表 6-3 の「アルゴリズム」に示す。

[割付：暗号鍵長]：表 6-3 の「鍵長(bit)」に示す。

表 6-3 暗号鍵の生成操作

暗号鍵	規格	アルゴリズム	鍵長(bit)
格納データ暗号化の暗号鍵	FIPS PUB 197	AES	256

FCS_CKM.4 暗号鍵破棄

下位階層：なし

依存性：[FDP_ITC.1 セキュリティ属性なし利用者データインポート、または

FDP_ITC.2 セキュリティ属性を伴う利用者データのインポート、または

FCS_CKM.1 暗号鍵生成]

FCS_CKM.4.1 TSF は、以下の[割付：標準のリスト]に合致する、指定された暗号鍵破棄方法[割付：暗号鍵破棄方法]に従って、暗号鍵を破棄しなければならない。

[詳細化：暗号鍵]：格納データ暗号化の暗号鍵

[割付：標準のリスト]：なし

[割付：暗号鍵破棄方法]：表 6-4 の「暗号鍵破棄方法」に示す。

表 6-4 暗号鍵破棄方法

暗号鍵	暗号鍵破棄方法
格納データ暗号化の暗号鍵	セキュリティ管理者の指示により、指定された暗号鍵情報を削除し、当該鍵情報が格納されていたメモリを開放する。

○利用者データ保護 (FDP)

FDP_ACC.1 サブセットアクセス制御

下位階層：なし

依存性：FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1 TSF は、[割付：サブジェクト、オブジェクト、及びSFP で扱われるサブジェクトとオブジェクト間の操作のリスト]に対して[割付：アクセス制御SFP]を実施しなければならない。

[割付：サブジェクト、オブジェクト、及びSFP で扱われるサブジェクトとオブジェクト間の操作のリスト]

サブジェクト：表 6-5 のサブジェクトに示す。

オブジェクト：表 6-5 のオブジェクトに示す。

SFP で扱われるサブジェクトとオブジェクト間の操作のリスト

：表 6-5 のサブジェクトとオブジェクト間の操作に示す。

[割付：アクセス制御SFP]：LM アクセス制御 SFP

表 6-5 サブジェクトとオブジェクト間の操作

サブジェクト	オブジェクト	サブジェクトとオブジェクト間の操作
ホストを代行するプロセス	LDEV (論理ボリューム)	➤ LDEV (論理ボリューム) へのアクセス
Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセス	LDEV (論理ボリューム)	➤ LDEV (論理ボリューム) の生成と削除
	RSG	➤ RSG の生成と削除

FDP_ACF.1 セキュリティ属性によるアクセス制御

下位階層：なし

依存性：FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性初期化

FDP_ACF.1.1 TSF は、以下の[割付：示されたSFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、またはSFP 関連セキュリティ属性の名前付けされたグループ]に基づいて、オブジェクトに対して、[割付：アクセス制御SFP]を実施しなければならない。

FDP_ACF.1.2 TSF は、制御されたサブジェクトと制御されたオブジェクト間での操作が許されるかどうか決定するために、次の規則を実施しなければならない：[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則]。

FDP_ACF.1.3 TSF は、次の追加規則、[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

FDP_ACF.1.4 TSF は、次の追加規則、[割付：セキュリティ属性に基づいてオブジェクトに

対するサブジェクトのアクセスを明示的に拒否する規則に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に拒否しなければならない。

[割付：示された SFP 下において制御されるサブジェクトとオブジェクトのリスト、及び各々に対応する、SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ]：

サブジェクト：ホストを代行するプロセス、Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセス

オブジェクト：LDEV (論理ボリューム)、RSG

SFP 関連セキュリティ属性、または SFP 関連セキュリティ属性の名前付けされたグループ：表 6-6 の「サブジェクトのセキュリティ属性」と「オブジェクトのセキュリティ属性」に示す。

表 6-6 SFP 関連セキュリティ属性

サブジェクト	サブジェクトのセキュリティ属性	オブジェクトのセキュリティ属性
ホストを代行するプロセス	WWN、LU 番号	LU パス情報(ホストの WWN、LU 番号、LDEV (論理ボリューム) 番号)
Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセス	ユーザグループ情報 (ロール、RSG 番号)	リソースグループ情報(RSG 番号) LU パス情報(ホストの WWN、LU 番号、LDEV (論理ボリューム) 番号)

[割付：アクセス制御 SFP]：LM アクセス制御 SFP

[割付：制御されたサブジェクトと制御されたオブジェクト間で、制御されたオブジェクトに対する制御された操作に使用するアクセスを管理する規則：表 6-7 の「規則」に記述した規則

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に許可する規則]：なし

[割付：セキュリティ属性に基づいてオブジェクトに対するサブジェクトのアクセスを明示的に拒否する規則]：なし

表 6-7 サブジェクトとオブジェクト間の規則

サブジェクト	規則	オブジェクト
ホストを代行するプロセス	ホストからホストを代行するプロセスに渡された WWN、LU 番号と、該当するオブジェクトのセキュリティ属性である LU パス情報が一致している場合、オブジェクトに対するアクセスを許可する。LU パス情報が不一致の場合、アクセスを拒否する。	LDEV (論理ボリューム)

サブジェクト	規則	オブジェクト
Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセス	Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセスがオブジェクトを生成、または削除する規則 1) セキュリティ管理者ロールの場合 RSG 番号が重複していない場合に生成を許可し、RSG 番号が存在する場合に削除を許可する。	RSG
	Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセスがオブジェクトを生成、または削除する規則 1) ストレージ管理者ロールの場合 ストレージリソース管理者に割当てられた RSG 番号のリソースグループに、生成する LDEV (論理ボリューム) 番号が含まれているとき当該 LDEV (論理ボリューム) の生成を許可する。 ストレージリソース管理者に割当てられた RSG 番号のリソースグループに、削除する LDEV (論理ボリューム) 番号が含まれている。かつ、LDEV (論理ボリューム) に関係付いた LU パス情報が存在しないときに、当該 LDEV (論理ボリューム) の削除を許可する。	LDEV (論理ボリューム)

FDP_RIP.1**サブセット残存情報保護**

下位階層：なし

依存性：なし

FDP_RIP.1.1

TSF は、[割付：オブジェクトのリスト]のオブジェクト[選択：への資源の割当て、からの資源の割当て解除]において、資源の以前のどの情報の内容も利用できなくすることを保証しなければならない。

[割付：オブジェクトのリスト]：LDEV (論理ボリューム)

[選択：への資源の割当て、からの資源の割当て解除]：からの資源の割当て解除

○識別と認証 (FIA)**FIA_AFL.1****認証失敗時の取り扱い**

下位階層：なし

依存性：FIA_UAU.1 認証のタイミング

FIA_AFL.1.1

TSF は、[割付：認証事象のリスト]に関して、[選択：[割付：正の整数値]、[割付：許容可能な値の範囲] 内における管理者設定可能な正の整数値]回の不成功認証試行が生じたときを検出しなければならない。

FIA_AFL.1.2

不成功の認証試行が定義した回数[選択：に達する、を上回った]とき、TSF は、[割付：アクションのリスト]をしなければならない。

[割付：認証事象のリスト]：Storage Navigator (ストレージ管理 UI ソフトウェア)

ア)での認証、SVP PC (管理保守 IF PC)にリモートデスクトップ接続するときの認証

[詳細化：管理者]：セキュリティ管理者

[選択： [割付： 正の整数値]、[割付： 許容可能な値の範囲]内における管理者設定可能な正の整数値]]：3

[選択： に達する、を上回った]：に達する

[割付： アクションのリスト]：当該ユーザのログインを1分間拒否。

その後、不成功認証試行回数を0にする。

FIA_ATD.1a

利用者属性定義

下位階層：なし

依存性：なし

FIA_ATD.1.1a

TSFは、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。：[割付：セキュリティ属性のリスト]

[割付：セキュリティ属性のリスト]：ロール、RSG 番号

FIA_ATD.1b

利用者属性定義

下位階層：なし

依存性：なし

FIA_ATD.1.1b

TSFは、個々の利用者に属する以下のセキュリティ属性のリストを維持しなければならない。：[割付：セキュリティ属性のリスト]

[割付：セキュリティ属性のリスト]：WWN、LU 番号

FIA_SOS.1a

秘密の検証

下位階層：なし

依存性：なし

FIA_SOS.1.1a

TSFは、秘密が[割付：定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付：定義された品質尺度]：6文字以上256文字(保守員のパスワードは127文字)までの半角英大文字、半角英小文字、半角数字、以下の32種類の半角記号!"#\$%&'()*+,-./:;<=>@[^_`{|}~

FIA_SOS.1b

秘密の検証

下位階層：なし

依存性：なし

FIA_SOS.1.1b

TSFは、秘密が[割付：定義された品質尺度]に合致することを検証するメカニズムを提供しなければならない。

[割付：定義された品質尺度]：12~32文字の半角英大文字、半角英小文字、半角数字、半角スペース、以下の12種類の記号.+@_=:/[],~

FIA_UAU.2	アクション前の利用者認証 下位階層： FIA_UAU.1 認証のタイミング 依存性： FIA_UID.1 識別のタイミング
FIA_UAU.2.1	TSF は、その <u>利用者</u> を代行する他の TSF 仲介アクションを許可する前に、各 <u>利用者</u> に認証が成功することを要求しなければならない。 [詳細化： <u>利用者</u>]： ストレージ管理者、保守員、またはファイバチャネルスイッチ
FIA_UID.2	アクション前の利用者識別 下位階層： FIA_UID.1 識別のタイミング 依存性： なし
FIA_UID.2.1	TSF は、その <u>利用者</u> を代行する他の TSF 仲介アクションを許可する前に、各 <u>利用者</u> に識別が成功することを要求しなければならない。 [詳細化： <u>利用者</u>]： ストレージ管理者、保守員、ホスト、またはファイバチャネルスイッチ
FIA_USB.1a	利用者・サブジェクト結合 下位階層： なし 依存性： FIA_ATD.1 利用者属性定義
FIA_USB.1.1a	TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない： [割付： <i>利用者セキュリティ属性のリスト</i>]
FIA_USB.1.2a	TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。： [割付： <i>属性の最初の関連付けの規則</i>]
FIA_USB.1.3a	TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。： [割付： <i>属性の変更の規則</i>] [割付： <i>利用者セキュリティ属性のリスト</i>]： ロール、RSG 番号 [割付： <i>属性の最初の関連付けの規則</i>]： なし [割付： <i>属性の変更の規則</i>]： なし
FIA_USB.1b	利用者・サブジェクト結合 下位階層： なし 依存性： FIA_ATD.1 利用者属性定義
FIA_USB.1.1b	TSF は、次の利用者セキュリティ属性を、その利用者を代行して動作するサブジェクトに関連付けなければならない： [割付： <i>利用者セキュリティ属性のリスト</i>]

FIA_USB.1.2b TSF は、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。：[割付：属性の最初の関連付けの規則]

FIA_USB.1.3b TSF は、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。：[割付：属性の変更の規則]

[割付：利用者セキュリティ属性のリスト]：WWN、LU 番号

[割付：属性の最初の関連付けの規則]：なし

[割付：属性の変更の規則]：なし

○セキュリティ管理 (FMT)

FMT_MOF.1 セキュリティ機能のふるまいの管理

下位階層：なし

依存性：FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_MOF.1.1 TSF は、機能[割付：機能のリスト][選択：のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]能力を[割付：許可された識別された役割]に制限しなければならない。

[割付：機能のリスト]：表 6-8 の「機能」に示す。

[選択：のふるまいを決定する、を停止する、を動作させる、のふるまいを改変する]：を停止する、を動作させる

[割付：許可された識別された役割]：表 6-8 の「役割」に示す。

表 6-8 役割に操作を制限する機能のリスト

項番	役割	機能
1	セキュリティ管理者	<ul style="list-style-type: none"> ➤ 格納データ暗号化機能 ➤ FC-SP 認証機能 ➤ 外部認証サーバの接続機能
2	ストレージリソース管理者	<ul style="list-style-type: none"> ➤ シュレディング機能
3	保守員	---

FMT_MSA.1 セキュリティ属性の管理

下位階層：なし

依存性：[FDP_ACC.1 サブセットアクセス制御または

FDP_IFC.1 サブセット情報フロー制御]

FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FMT_MSA.1.1 TSFは、セキュリティ属性[割付：セキュリティ属性のリスト]に対し[選択：デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]]をする能力を[割付：許可された識別された役割]に制限する[割付：アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

[割付：セキュリティ属性のリスト]：LUパス情報、ユーザグループ情報

[選択：デフォルト値変更、問い合わせ、改変、削除、[割付：その他の操作]]：表 6-9 の「LUパス情報に対する操作」、表 6-10 の「ユーザグループ情報に対する操作」に記述する操作。

[割付：許可された識別された役割]：表 6-9、表 6-10 の「役割」に記述する役割。

[割付：アクセス制御 SFP、情報フロー制御 SFP]：LM アクセス制御 SFP

表 6-9 ホストを代行するプロセスのセキュリティ属性(LUパス情報)に対するストレージ管理者および保守員の操作

役割	LUパス情報に対する操作					
	RSG 番号=n			RSG 番号≠n		
	ホストの WWN	LU 番号	LDEV (論理ボリューム) 番号	ホストの WWN	LU 番号	LDEV (論理ボリューム) 番号
ストレージリソース管理者(RSG 番号=n)	問い合わせ、作成、削除	問い合わせ、作成、削除	問い合わせ、作成、削除	—	—	—
セキュリティ管理者	—	—	—	—	—	—
監査ログ管理者	—	—	—	—	—	—
保守員(保守員には全てのリソースグループを割当てる。)	問い合わせ、作成、削除	問い合わせ、作成、削除	問い合わせ、作成、削除	/		

—：操作なし

ホストの識別は、LUパス情報に設定されたホストの WWN が使用される。

表 6-10 Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセスのセキュリティ属性(ユーザグループ情報)に対するストレージ管理者および保守員の操作

役割	ユーザグループ情報に対する操作	
	ロール	RSG 番号
セキュリティ管理者	<ul style="list-style-type: none"> ➤ 追加 ➤ 削除 ➤ 問い合わせ 	<ul style="list-style-type: none"> ➤ 追加 ➤ 削除 ➤ 問い合わせ

役割	ユーザグループ情報に対する操作	
	ロール	RSG 番号
ストレージリソース管理者	➤ (自身の問い合わせ)	➤ (自身の問い合わせ)
監査ログ管理者	➤ (自身の問い合わせ)	➤ (自身の問い合わせ)
保守員	➤ (自身の問い合わせ)	➤ (自身の問い合わせ)

FMT_MSA.3 静的属性初期化

下位階層：なし

依存性：FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1 TSF は、その SFP を実施するために使われるセキュリティ属性として、[選択： 制限的、許可的、[割付： その他の特性]： から1つのみ選択]デフォルト値を与える[割付： アクセス制御 SFP、情報フロー制御 SFP]を実施しなければならない。

FMT_MSA.3.2 TSF は、オブジェクトや情報が生成される時、[割付： 許可された識別された役割]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

[選択： 制限的、許可的、[割付： その他の特性]： から1つのみ選択]： 制限的

[割付： アクセス制御 SFP、情報フロー制御 SFP]： LM アクセス制御 SFP

[割付： 許可された識別された役割]： なし

FMT_MTD.1 TSF データの管理

下位階層：なし

依存性：FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティの役割

FMT_MTD.1.1 TSF は、[割付： TSF データのリスト]を[選択： デフォルト値変更、問い合わせ、改変、削除、消去、[割付： その他の操作]]する能力を[割付： 許可された識別された役割]に制限しなければならない。

[割付： TSF データのリスト]：

ストレージ管理者および保守員のユーザ ID、パスワード

ファイバチャネルスイッチの WWN、シークレット

格納データ暗号化の暗号鍵

ユーザの認証方式

[選択： デフォルト値変更、問い合わせ、改変、削除、消去、[割付： その他の操作]]： 表 6-11 の「ユーザアカウント」に対する操作、表 6-12 の「ホストが接続されるファイバチャネルスイッチの認証データ」に対する操作、表 6-13 の「格納データ暗号化の暗号鍵」に対する操作、表 6-14 の「ユー

ザの認証方式」に対する操作。

[割付：許可された識別された役割]：表 6-11、表 6-12、表 6-13、表 6-14 の「役割」に記述する役割。

表 6-11 ユーザアカウントに対するストレージ管理者および保守員の操作

役割	ストレージ管理者および保守員の ユーザアカウント	
	ユーザ ID	パスワード
セキュリティ管理者	問い合わせ、 作成、削除	変更
ストレージリソース 管理者	(自身の) 問い合わせ	(自身の) 変更
監査ログ管理者	(自身の) 問い合わせ	(自身の) 変更
保守員	(自身の) 問い合わせ	(自身の) 変更

表 6-12 ホストが接続されるファイバチャネルスイッチの認証データに対するストレージ管理者
および保守員の操作

役割	ファイバチャネルスイッチ認証データ	
	ファイバチャネルスイッ チの WWN	ファイバチャネルスイ ッチの シークレット
セキュリティ管理者	問い合わせ、 作成、変更、削除	作成、変更、削除
ストレージリソース 管理者	問い合わせ、 作成、変更、削除	—
監査ログ管理者	—	—
保守員	問い合わせ、 作成、変更、削除	—

—：操作なし

表 6-13 格納データ暗号化の暗号鍵に対するストレージ管理者および保守員の操作

役割	格納データ暗号化の暗号鍵
セキュリティ管理者	作成、削除、問い合わせ、変更

役割	格納データ暗号化の暗号鍵
ストレージリソース管理者	—
監査ログ管理者	—
保守員	—

— : 操作なし

表 6-14 ユーザの認証方式に対するストレージ管理者および保守員の操作

役割	ユーザの認証方式
セキュリティ管理者	問い合わせ、改変
ストレージリソース管理者	—
監査ログ管理者	—
保守員	—

— : 操作なし

FMT_MTD.3 セキュアな TSF データ

下位階層 : なし

依存性 : FMT_MTD.1 TSF データの管理

FMT_MTD.3.1

TSF は、[割付 : TSF データのリスト]としてセキュアな値だけが受け入れられることを保証しなければならない。

[割付 : TSF データのリスト] : 格納データ暗号化の暗号鍵

FMT_SMF.1

管理機能の特定

下位階層 : なし

依存性 : なし

FMT_SMF.1.1

TSF は、以下の管理機能を実行することができなければならない。 : [割付 : TSF によって提供される管理機能のリスト]。

[割付 : TSF によって提供される管理機能のリスト] : 以下の管理機能を提供する。

- ユーザアカウントのユーザ ID、ホスト識別を管理する機能
- ユーザアカウントのユーザ ID に対するパスワードを管理する機能
- ファイバチャネルスイッチの認証データを管理する機能
- ユーザアカウントのロールを管理する機能

- ホストを代行するプロセスのセキュリティ属性を管理する機能
- Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセスのセキュリティ属性を管理する機能
- ユーザアカウントに対するストレージ管理者および保守員の操作を管理する機能
- ホストが接続されるファイバチャネルスイッチの認証データに対するストレージ管理者および保守員の操作を管理する機能
- 格納データ暗号化の暗号鍵に対するストレージ管理者および保守員の操作を管理する機能
- 格納データ暗号化機能の停止、動作を管理する機能
- FC-SP 認証機能の停止、動作を管理する機能
- シュレディング機能停止、動作を管理する機能
- 外部認証サーバの接続機能の停止、動作を管理する機能

FMT_SMR.1 セキュリティの役割

下位階層：なし

依存性：FIA_UID.1 識別のタイミング

FMT_SMR.1.1 TSF は、役割[割付：許可された識別された役割]を維持しなければならない。

FMT_SMR.1.2 TSF は、利用者を役割に関連付けなければならない。

[割付：許可された識別された役割]：

- ・セキュリティ管理者
- ・ストレージリソース管理者
- ・監査ログ管理者
- ・保守員
- ・ストレージ利用者

○TSF の保護 (FPT)

FPT_STM.1 高信頼タイムスタンプ

下位階層：なし

依存性：なし

FPT_STM.1.1 TSF は、高信頼タイムスタンプを提供できなければならない。

○高信頼パス/チャネル (FTP)

FTP_ITC.1 TSF 間高信頼チャネル

下位階層: なし

依存性: なし

FTP_ITC.1.1 TSF は、それ自身と他の高信頼 IT 製品間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、および改変や暴露からのチャネルデータの保護を提供する通信チャネルを提供しなければならない。

- FTP_ITC.1.2 TSF は、[選択：TSF、他の高信頼 IT 製品]が、高信頼チャンネルを介して通信を開始するのを許可しなければならない。
- FTP_ITC.1.3 TSF は、[割付：高信頼チャンネルが要求される機能のリスト]のために、高信頼チャンネルを介して通信を開始しなければならない。
[詳細化：他の高信頼 IT 製品]：外部認証サーバ
[選択：TSF、リモート高信頼 IT 製品]：TSF
[割付：高信頼チャンネルが要求される機能のリスト]：ストレージ管理者および保守員の識別・認証（外部認証サーバ方式）にて使用するユーザアカウントのユーザ ID、パスワードの送信
- FTP_TRP.1 高信頼パス**
下位階層: なし
依存性: なし
- FTP_TRP.1.1 TSF は、それ自身と[選択：リモート、ローカル]利用者間に、他の通信パスと論理的に区別され、その端点の保証された識別と、[選択：改変、暴露、[割付：ほかのタイプの完全性、または機密性侵害]]からの通信データの保護を提供する通信パスを提供しなければならない。
- FTP_TRP.1.2 TSF は、[選択：TSF、ローカル利用者、リモート利用者]が、高信頼パスを介して通信を開始することを許可しなければならない。
- FTP_TRP.1.3 TSF は、[選択：最初の利用者認証、[割付：高信頼パスが要求される他のサービス]]に対して、高信頼パスの使用を要求しなければならない。
[選択：リモート、ローカル]：リモート
[選択：改変、暴露、[割付：ほかのタイプの完全性、または機密性侵害]]：暴露
[選択：TSF、ローカル利用者、リモート利用者]：リモート利用者
[選択：最初の利用者認証、[割付：高信頼パスが要求される他のサービス]]：
[割付：高信頼パスが要求される他のサービス]：Storage Navigator (ストレージ管理 UI ソフトウェア)を使用した通信

6.2 セキュリティ保証要件

TOE セキュリティ保証要件を示す。

本 TOE の評価保証レベルは EAL2 であり、追加する保証コンポーネント ALC_FLR.1 である。全てのセキュリティ保証要件は CC パート 3 に規定されているセキュリティ保証コンポーネントを直接使用する。

(1) 開発 (ADV)

- ADV_ARC.1 : セキュリティアーキテクチャ記述
- ADV_FSP.2 : セキュリティ実施機能仕様
- ADV_TDS.1 : 基本設計

(2) ガイダンス文書 (AGD)

- AGD_OPE.1 : 利用者操作ガイダンス
- AGD_PRE.1 : 準備手続き

(3) ライフサイクルサポート (ALC)

- ALC_CMC.2 : CM システムの使用
- ALC_CMS.2 : TOE の一部の CM 範囲
- ALC_DEL.1 : 配付手続き
- ALC_FLR.1 : 基本的な欠陥修正

(4) セキュリティターゲット評価 (ASE)

- ASE_CCL.1 : 適合主張
- ASE_ECD.1 : 拡張コンポーネント定義
- ASE_INT.1 : ST 概説
- ASE_OBJ.2 : セキュリティ対策方針
- ASE_REQ.2 : 派生したセキュリティ要件
- ASE_SPD.1 : セキュリティ課題定義
- ASE_TSS.1 : TOE 要約仕様

(5) テスト (ATE)

- ATE_COV.1 : カバレッジの証拠
- ATE_FUN.1 : 機能テスト
- ATE_IND.2 : 独立テスト - サンプル

(6) 脆弱性評価 (AVA)

- AVA_VAN.2 : 脆弱性分析

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

セキュリティ機能要件と TOE セキュリティ対策方針の対応関係を表 6-15 に示す。この表で示す通り、各セキュリティ機能要件が、少なくとも 1 つの TOE セキュリティ対策方針に対抗している。

表 6-15 セキュリティ対策方針とセキュリティ機能要件の対応

		TOE セキュリティ対策方針							
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.SWITCH_AUTH	O.HOST_ACCESS	O_HDD_ENC	O_HDD_SHRED	O.AUD_GEN
TOE セキュリティ 機能要件	FAU_GEN.1								X
	FAU_GEN.2								X
	FAU_SAR.1								X
	FAU_STG.1								X
	FAU_STG.3								X
	FAU_STG.4								X
	FCS_CKM.1						X		
	FCS_CKM.4						X		
	FDP_ACC.1		X			X			
	FDP_ACF.1		X			X			
	FDP_RIP.1							X	
	FIA_AFL.1	X							
	FIA_ATD.1a	X							
	FIA_ATD.1b					X			
	FIA_SOS.1a	X							
	FIA_SOS.1b				X				
	FIA_UAU.2	X			X				
	FIA_UID.2	X			X	X			
	FIA_USB.1a	X							
FIA_USB.1b					X				

	TOE セキュリティ対策方針							
	O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.SWITCH_AUTH	O.HOST_ACCESS	O_HDD_ENC	O_HDD_SHRED	O.AUD_GEN
FMT_MOF.1		X						
FMT_MSA.1		X						
FMT_MSA.3		X						
FMT_MTD.1		X				X		
FMT_MTD.3						X		
FMT_SMF.1		X						
FMT_SMR.1		X						
FPT_STM.1								X
FTP_ITC.1			X					
FTP_TRP.1			X					

表 6-16 は、TOE のセキュリティ機能要件によって、TOE のセキュリティ対策方針が実現されていることを示している。

表 6-16 TOE のセキュリティ対策方針に対するセキュリティ機能要件の正当性

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
O.ADM_AUTH	<p>O.ADM_AUTH では、Storage Navigator (ストレージ管理 UI ソフトウェア) の利用者がディスクサブシステムの管理操作を行う前に、必ず利用者の識別と認証を行うことを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. Storage Navigator (ストレージ管理 UI ソフトウェア) の利用者の維持を行う。</p> <p>TOE は Storage Navigator (ストレージ管理 UI ソフトウェア) の利用者を識別するために、ユーザアカウントを定義し、利用者とユーザアカウントを関連付け、維持しなければならない。これにより、Storage Navigator (ストレージ管理 UI ソフトウェア) の利用者を識別することが可能となる。この要件に該当するセキュリティ機能要件は FIA_ATD.1a、FIA_USB.1a である。</p> <p>b. TOE 利用前に Storage Navigator (ストレージ管理 UI ソフトウェア) のユーザアカウントの識別・認証を行う。</p> <p>TOE が利用される前に、TOE はユーザアカウントを識別しなければならない。よって、Storage Navigator (ストレージ管理 UI ソフトウェア) の全ての機能動</p>

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
	<p>作前にユーザアカウントの識別・認証を実施する必要がある。この要件に該当するセキュリティ機能要件は FIA_UID.2、FIA_UAU.2 である。</p> <p>c. パスワードの管理を行う。</p> <p>TOE がユーザアカウントを認証するためのパスワードは、6 文字から 256 文字(保守員のパスワードは 127 文字)までの半角英大文字、半角英小文字、半角数字、以下の 32 種類の半角記号!"#\$%&'()*+,-./:;<=>?@[^_`{ }~の組み合わせを入力可能としている。また、不正パスワード入力による認証失敗が 3 回連続したときには、当該ユーザ ID のログインを 1 分間拒否することにより、パスワードが破られる可能性を低減している。この機能に該当するセキュリティ機能要件は FIA_AFL.1、FIA_SOS.1a である。</p> <p>以上 a、b、c の対策を満たすことにより、O.ADM_AUTH を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FIA_ATD.1a、FIA_USB.1a、FIA_AFL.1、FIA_SOS.1a、FIA_UAU.2、FIA_UID.2 の達成により、O.ADM_AUTH を実現できる。</p>
O.ADM_ROLE	<p>O.ADM_ROLE では、識別・認証されたユーザ ID のロールに基づいて、ストレージ管理者および保守員の管理操作を制限できることを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. ロール、RSG 番号の操作を制限する。</p> <p>TOE はユーザアカウントが保持するロールに応じて、ユーザアカウントのロール、RSG 番号の追加、削除と RSG の作成、削除を制限しなければならない。よって、TOE は「LM アクセス制御 SFP」として定義された規則にしたがって、ユーザアカウントに対する変更を制御する必要がある。この要件に該当するセキュリティ機能要件は FMT_MSA.1 である。</p> <p>b. 識別・認証情報を管理する。</p> <p>TOE はユーザアカウントのロールに応じて、ユーザアカウントのユーザ ID、パスワード、認証方式およびファイバチャネルスイッチの WWN、シークレットの変更を制限する必要がある。これにより、ユーザアカウントのユーザ ID、パスワード、認証方式およびファイバチャネルスイッチの WWN、シークレットの不正な変更を防止している。この要件に該当するセキュリティ機能要件は FMT_MTD.1 である。</p> <p>c. 管理機能を保有する。</p> <p>TOE は Storage Navigator (ストレージ管理 UI ソフトウェア)のユーザアカウント、ユーザアカウントのロール、ファイバチャネルスイッチの識別・認証情報、LU パス情報、ユーザグループ情報を管理する機能を有する必要がある。</p> <p>TOE はストレージ管理者および保守員の操作を管理する機能を有する必要がある。また、格納データ暗号化機能、FC-SP 認証機能、シュレディング機能、外部認証サーバの接続機能の停止と動作を管理する機能を有する必要がある。この要件に該当するセキュリティ機能要件は FMT_SMF.1 である。</p> <p>d. 役割を維持する。</p> <p>TOE はセキュリティ管理者、ストレージリソース管理者、監査ログ管理者、保守員、ストレージ利用者の役割を維持し、利用者に関連付ける必要がある。</p>

TOEのセキュリティ対策方針	TOEのセキュリティ対策方針が実現されていることの根拠
	<p>この要件に該当するセキュリティ機能要件は FMT_SMR.1 である。</p> <p>e. セキュリティ機能のふるまいを管理する。</p> <p>TOE はユーザアカウントのロールに応じて、格納データ暗号化・非暗号化、ファイバチャネルスイッチの認証有無、外部認証サーバとの接続有無、シュレディング機能の開始と停止を制御する必要がある。これにより、各機能の使用・使用停止の不正な変更を防止している。この要件に該当するセキュリティ機能要件は FMT_MOF.1 である。</p> <p>f. アクセス制御を規定し、実施する。</p> <p>TOE はストレージ管理者および保守員に対して、「LM アクセス制御 SFP」として定義された規則に従って RSG の作成、削除および LDEV (論理ボリューム) の生成、削除を行う必要がある。これにより、ストレージリソース管理者は割り当てられた RSG 内の LDEV (論理ボリューム) に対して生成、削除が可能となるように制御できる。また、LDEV (論理ボリューム) を生成するとき、アクセス属性として制限的デフォルト値を与える。これは、LDEV (論理ボリューム) 生成時には LU パス情報が存在しないため、ホストからのアクセスが制限されることを意味する。この要件に該当するセキュリティ機能要件は FDP_ACC.1、FDP_ACF.1、FMT_MSA.3 である。</p> <p>以上 a、b、c、d、e、f すべての対策を満たすことにより、O.ADM_ROLE を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FMT_MSA.1、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FMT_MOF.1、FDP_ACC.1、FDP_ACF.1 の達成により、O.ADM_ROLE を実現できる。</p>
O.SEC_COMM	<p>O.SEC_COMM では、Storage Navigator (ストレージ管理 UI ソフトウェア) – SVP PC (管理保守 IF PC) 間および SVP PC (管理保守 IF PC) – 外部認証サーバ間の通信データに対する、盗聴を防止するため、Storage Navigator (ストレージ管理 UI ソフトウェア) – SVP PC (管理保守 IF PC) 間および SVP PC (管理保守 IF PC) – 外部認証サーバ間の通信データの暗号化によるセキュアな通信機能を提供することを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. Storage Navigator (ストレージ管理 UI ソフトウェア) – SVP PC (管理保守 IF PC) 間の通信データを保護する。</p> <p>Storage Navigator (ストレージ管理 UI ソフトウェア) と SVP PC (管理保守 IF PC) 間の通信は高信頼パスを使用する。これにより、通信データの盗聴から保護している。この機能に該当するセキュリティ機能要件は FTP_TRP.1 である。</p> <p>b. SVP PC (管理保守 IF PC) – 外部認証サーバ間の通信データを保護する。</p> <p>識別・認証に外部認証サーバを使用する場合 (外部認証サーバ方式)、SVP PC (管理保守 IF PC) と外部認証サーバ間の通信は高信頼チャネルを使用する。これにより、通信データの盗聴から保護している。この機能に該当するセキュリティ機能要件は FTP_ITC.1 である。</p> <p>以上 a、b すべての対策を満たすことにより、O.SEC_COMM を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、</p>

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
	FTP_TRP.1、FTP_ITC.1 の達成により、O.SEC_COMM を実現できる。
O.SWITCH_AUTH	<p>O.SWITCH_AUTH では、ファイバチャネルスイッチの識別・認証の設定適用後、適切に設定されたファイバチャネルスイッチと TOE がケーブルで接続されたことを検知した際には、ファイバチャネルスイッチの識別・認証を行うことを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. FC-SP 機能を実施する。</p> <p>TOE は、ファイバチャネルスイッチに対して、セキュリティ認証実施のコマンドを送信し、DH-CHAP 認証コードを使用してファイバチャネルスイッチを識別・認証する。この機能に該当するセキュリティ要件は、FIA_UID.2、FIA_UAU.2 である。</p> <p>b. シークレットの管理を行う。</p> <p>TOE がファイバチャネルスイッチを認証するためのシークレットは、12 文字から 32 文字の半角英大文字、半角英小文字、半角数字、半角スペース、以下の 12 種類の半角記号.-+@_=:/[]~,~の組み合わせを設定可能とし、パスワードが破られる可能性を低減している。この機能に該当するセキュリティ機能要件は FIA_SOS.1b である。</p> <p>以上 a、b すべての対策を満たすことにより、O.SWITCH_AUTH を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FIA_UID.2、FIA_UAU.2、FIA_SOS.1b の達成により、O.SWITCH_AUTH を実現できる。</p>
O.HOST_ACCESS	<p>O.HOST_ACCESS では、本 TOE が保護対象資産である LU のユーザデータにホストがアクセスする際、ホストを識別し、自ホストに割り当てられた LDEV（論理ボリューム）のみアクセス可能となるようにアクセス制御を行うことを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. ホストの維持を行う。</p> <p>TOE は、ホストの属性情報(WWN、LU 番号)を定義し、その属性をホストに関連付け、維持しなければならない。この要件に該当するセキュリティ機能要件は FIA_ATD.1b、FIA_USB.1b である。</p> <p>b. TOE 利用前にホストの識別を行う。</p> <p>TOE が利用される前に、TOE はホストを識別する必要がある。この要件に該当するセキュリティ機能要件は FIA_UID2 である。</p> <p>c. アクセス制御を規定し、実施する。</p> <p>TOE は各ホストに対して、「LM アクセス制御 SFP」として定義された規則に従って LDEV（論理ボリューム）へのアクセスを決定し、その通りにアクセス制御を行う必要がある。これにより、ホストは割り当てられた LDEV（論理ボリューム）内のユーザデータのみアクセス可能となるように制御できる。この要件</p>

TOEのセキュリティ対策方針	TOEのセキュリティ対策方針が実現されていることの根拠
	<p>に該当するセキュリティ機能要件は FDP_ACC.1 および FDP_ACF.1 である。</p> <p>以上 a、b、c すべての対策を満たすことにより、O.HOST_ACCESS を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FIA_ATD.1b、FIA_USB.1b、FIA_UID2、FDP_ACC.1、FDP_ACF.1 の達成により、O.HOST_ACCESS を実現できる。</p>
O.HDD_ENC	<p>O.HDD_ENC では、ディスクストレージ装置から取り出したディスクドライブからユーザデータが漏洩しないように格納データ暗号化の暗号鍵を管理することを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. 格納データ暗号化の暗号鍵の生成、削除を行う。</p> <p>ディスクドライブ内に格納されているユーザデータを暗号化する必要がある。これにより、予防保守により交換したディスクドライブからユーザデータが漏洩することを防止している。暗号化および復号は DKA に搭載されている LSI を利用する。TOE は暗号化に使用する暗号鍵を生成し、暗号鍵は使用後にメモリから消去している。この機能に該当するセキュリティ機能要件は FCS_CKM.1、FCS_CKM.4 である。</p> <p>b. 格納データ暗号化の暗号鍵に対する操作を制限する。</p> <p>TOE はユーザアカウントのロールに応じて、格納データ暗号化の暗号鍵に対する操作を制限する必要がある。また、バックアップした暗号鍵以外はリストア出来ないように制御している。これにより、暗号鍵に対する不正な変更を防止している。この要件に該当するセキュリティ機能要件は FMT_MTD.1 および FMT_MTD.3 である。</p> <p>以上 a、b すべての対策を満たすことにより、O.HDD_ENC を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FCS_CKM.1、FCS_CKM.4、FMT_MTD.1、FMT_MTD.3 の達成により、O.HDD_ENC を実現できる。</p>
O.HDD_SHRED	<p>O.HDD_SHRED では、ディスクストレージ装置のディスクドライブを再使用するとき以前にユーザデータが漏洩しないようにディスクドライブ内のユーザデータをシュレディングすることを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. ディスクドライブ内のユーザデータを保護する。</p> <p>ディスクドライブの使用を停止したときに、ディスクドライブ内に格納されているユーザデータをシュレディングする必要がある。これにより、使用を停止したディスクドライブからユーザデータが漏洩することを防止している。この機能に該当するセキュリティ機能要件は FDP_RIP.1 である。</p> <p>以上の対策を満たすことにより、O.HDD_SHRED を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FDP_RIP.1 の達成により、O.HDD_SHRED を実現できる。</p>
O.AUD_GEN	O.AUD_GEN では、セキュリティ関連の情報が不正に作成、改変、削除が行

TOEのセキュリティ対策方針	TOEのセキュリティ対策方針が実現されていることの根拠
	<p>われていないか管理することを要求している。</p> <p>この要求に対し、必要な対策の詳細と求められる機能は以下の通りである。</p> <p>a. セキュリティ機能に関する事象の監査記録の生成を実施する。</p> <p>Storage Navigator (ストレージ管理 UI ソフトウェア)での識別・認証、ユーザアカウントの改ざん、ロールおよびRSGの改ざん的事象が発生した場合、SVP PC (管理保守 IF PC)は事象の監査記録を生成する必要がある。これにより、これらの情報が不正に改ざんされた場合、監査記録から識別することが可能となる。この要件に該当するセキュリティ機能要件はFAU_GEN.1である。</p> <p>FAU_GEN.1では、識別・認証の事象、各種設定変更の操作事象、格納データ暗号化機能に関する操作事象およびユーザデータシュレディング機能に関する操作事象について監査ログを取得しているため、対策方針を満足している。</p> <p>FAU_GEN.1の表6-1で監査項目が「なし」としている項目はセキュリティ事象の追跡に効果が無いか、または、他の監査事象に含まれ、必ず実行される要件のため追跡が可能であり、監査項目が無くても問題ない。</p> <p>また、LUパス情報が設定されていない状態では、ホストは当該LDEV (論理ボリューム) を論理デバイスとして認識できず、LDEV (論理ボリューム) にアクセスすることができないため、ホストからLDEV (論理ボリューム) にアクセスするセキュリティ機能要件に関する監査事象を取得しなくても問題ない。</p> <p>FPT_STM.1で提供するタイムスタンプは、SVP PC (管理保守 IF PC)のOSのタイムスタンプであり、保守員以外に変更できないため、時刻設定変更などの事象について監査ログを取得する必要はない。</p> <p>監査記録を生成する際、その事象が発生した日時、操作したユーザのユーザIDを監査記録に付与する必要がある。これにより、事象が発生した日時、操作したユーザを特定することが可能となる。この要件に該当するセキュリティ機能要件はFAU_GEN.2およびFPT_STM.1である。</p> <p>b. 監査記録の参照を制限する。</p> <p>監査記録を参照する際は、Storage Navigator (ストレージ管理 UI ソフトウェア)からSVP PC (管理保守 IF PC)にある監査記録をダウンロードする必要がある。監査記録のダウンロードは、監査ログ管理者ロールをもっているユーザアカウントに制限する。これにより、不正に監査記録を参照されることを保護する。この要件に該当するセキュリティ機能要件は、FAU_SAR.1である。</p> <p>c. 監査記録を改ざんから保護する。</p> <p>TOEは許可されていない利用者が監査記録の削除、改ざんすることを防止する必要がある。監査記録のダウンロードは監査ログ管理者ロールを持っているユーザアカウントに制限している。また、TOEは監査記録を改変する機能を持っていない。これにより、監査記録は不正な削除や改変から保護されている。この要件に該当するセキュリティ機能要件は、FAU_STG.1である。</p> <p>d. 監査記録の損失の恐れを警告する。</p> <p>監査記録は最大250,000行の生成が可能だが、それを超過すると古い日時の監査記録は損失するため、175,000行を超過した場合は、Storage Navigator (ストレージ管理 UI ソフトウェア)の画面上に超過した旨を警告し、ユーザに監査記録のダウンロードを促す。これにより、監査記録を損失する恐れを解消する。こ</p>

TOE のセキュリティ対策方針	TOE のセキュリティ対策方針が実現されていることの根拠
	<p>の要件に該当するセキュリティ機能要件は、FAU_STG.3、FAU_STG.4 である。</p> <p>以上 a、b、c、d すべての対策を満たすことにより、O.AUD_GEN を満足できる。</p> <p>よって、それぞれの対策に必要なセキュリティ機能要件として該当する、FAU_GEN.1、FAU_GEN.2、FPT_STM.1、FAU_SAR.1、FAU_STG.1、FAU_STG.3、FAU_STG.4 の達成により、O.AUD_GEN を実現できる。</p>

6.3.2 セキュリティ要件内部一貫性根拠

セキュリティ要件のコンポーネントの依存性を表 6-17 に示す。

表 6-17 セキュリティ機能要件の依存性

項番	TOE/IT 環境	セキュリティ機能要件	CC パート 2 に定義されている依存性	本 ST で対応する機能要件
1	TOE	FAU_GEN.1	FPT_STM.1	FPT_STM.1
2	TOE	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
			FIA_UID.1	FIA_UID.2 *1
3	TOE	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
4	TOE	FAU_STG.1	FAU_GEN.1	FAU_GEN.1
5	TOE	FAU_STG.3	FAU_STG.1	FAU_STG.1
6	TOE	FAU_STG.4	FAU_STG.1	FAU_STG.1
7	TOE	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	なし *3
			FCS_CKM.4	FCS_CKM.4
8	TOE	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
9	TOE	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
10	TOE	FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
			FMT_MSA.3	FMT_MSA.3
11	TOE	FDP_RIP.1	なし	—
12	TOE	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 *2
13	TOE	FIA_ATD.1a	なし	—
14	TOE	FIA_ATD.1b	なし	—
15	TOE	FIA_SOS.1a	なし	—
16	TOE	FIA_SOS.1b	なし	—
17	TOE	FIA_UAU.2	FIA_UID.1	FIA_UID.2 *1
18	TOE	FIA_UID.2	なし	—
19	TOE	FIA_USB.1a	FIA_ATD.1	FIA_ATD.1a
20	TOE	FIA_USB.1b	FIA_ATD.1	FIA_ATD.1b
21	TOE	FMT_MOF.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
22	TOE	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1
			FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
23	TOE	FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
			FMT_SMR.1	FMT_SMR.1
24	TOE	FMT_MTD.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
25	TOE	FMT_MTD.3	FMT_MTD.1	FMT_MTD.1
26	TOE	FMT_SMF.1	なし	—
27	TOE	FMT_SMR.1	FIA_UID.1	FIA_UID.2 *1
28	TOE	FPT_STM.1	なし	—
29	TOE	FTP_ITC.1	なし	—
30	TOE	FTP_TRP.1	なし	—

*1： FIA_UID.1 の上位階層コンポーネントである FIA_UID.2 により依存関係を充足している。

*2： FIA_UAU.1 の上位階層コンポーネントである FIA_UAU.2 により依存関係を充足している。

*3 : TOE はソフトウェアであり、暗号化および復号はハードウェアにより実現しているため該当する機能要件はなし。

各 TOE セキュリティ機能要件について、同カテゴリの機能要件についてその定義が一貫性を持つことの根拠を表 6-18 に示す。

表 6-18 セキュリティ機能要件間の一貫性

項番	カテゴリ	セキュリティ機能要件	一貫性の根拠
1	アクセス制御	FDP_ACC.1 FDP_ACF.1 FDP_RIP.1	これらの機能要件によりアクセス制御について定義しているが、同一のサブジェクト、オブジェクトに対して同一の SFP の適用を要求しており競合や矛盾は存在せず、その内容は一貫している。
2	管理	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_MTD.3 FMT_SMF.1 FMT_SMR.1	これらの機能要件によりセキュリティ管理について定義しているが、対象とするセキュリティ属性やアクションにおいて競合や矛盾は存在せず、その内容は一貫している。
3	識別と認証	FIA_AFL.1 FIA_ATD.1a FIA_ATD.1b FIA_SOS.1a FIA_SOS.1b FIA_UAU.2 FIA_UID.2 FIA_USB.1a FIA_USB.1b	この機能要件により識別と認証を実現している。TSF として、①Storage Navigator (ストレージ管理 UI ソフトウェア) のユーザ ID とパスワード、②ファイバチャネルスイッチの WWN とシークレット、③ホストの WWN を別々に定義しており、競合や矛盾は存在せず、その内容は一貫している。
4	監査	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_STG.1 FAU_STG.3 FAU_STG.4	これらの機能要件により監査ログについて定義しており、競合や矛盾は存在せず、その内容は一貫している。
5	暗号鍵管理・操作	FCS_CKM.1 FCS_CKM.4	これらの機能要件は、格納データ暗号化機能で使用する暗号鍵の操作について定義しており、競合や矛盾は存在せず、その内容は一貫している。
6	高信頼パス/チャンネル	FTP_ITC.1 FTP_TRP.1	これらの機能要件は、Storage Navigator (ストレージ管理 UI ソフトウェア) - SVP PC (管理保守 IF PC) 間および SVP PC (管理保守 IF PC) - 外部認証サーバ間の通信パス、チャンネルについて定義しており、競合や矛盾は存在せず、その内容は一貫している。
7	補完	FPT_STM.1	この機能要件は他の機能要件を補完するものである。FPT_STM.1 は監査ログのタイムスタンプの要件であることから他の要件と競合や矛盾が無いのは自明である。

項番	カテゴリ	セキュリティ機能要件	一貫性の根拠
			る。このカテゴリの機能要件間では競合や矛盾は存在せず、その内容は一貫している。
8	カテゴリ間	#1-#2	アクセス制御の要件は保護対象資産である LU 内のユーザデータに対する制御を定義しており、管理の要件は TSF データの管理を定義するものであることから両者に競合や矛盾は存在しない。
		#1-#3 #2-#3	識別の要件とアクセス制御もしくは管理の要件との間では競合や矛盾は存在しない。
		#1-#4 #2-#4 #3-#4	アクセス制御、管理、識別と認証の要件の監査を記録するものであり、各要件との間では競合や矛盾は存在しない。
		#1-#5 #2-#5 #3-#5 #4-#5	アクセス制御、管理、識別と認証、監査記録の要件との間では競合や矛盾は存在しない。
		#1-#6 #2-#6 #3-#6 #4-#6 #5-#6	アクセス制御、管理、識別と認証、監査記録、暗号鍵管理・操作の要件との間では競合や矛盾は存在しない。
		#1-#7 #2-#7 #3-#7 #4-#7 #5-#7 #6-#7	FPT_STM.1 は FAU_GEN.1 に対して時間情報を提供するものであり、その他の要件との間で競合や矛盾は存在しない。

さらに、以下に述べるように依存関係のないセキュリティ機能要件によっても相互支援がなされている。

- FIA_UID.2 および FIA_UAU.2 に関しては、FMT_MOF.1 によりセキュリティ機能の動作および停止をロールにより限定し、操作は Storage Navigator (ストレージ管理 UI ソフトウェア) からの操作に限定している。その他の手段では動作を停止させることは出来ず、非活性化を防止している。

上述のとおり、ST に記述された IT セキュリティ要件は一体となって相互にサポートし、内部的に一貫性がある全体を形成している。

6.3.3 セキュリティ保証要件根拠

TOE を含むディスクストレージ装置はセキュアなエリアに設置され、LAN を利用する攻撃経路以外は想定していない。3.2 節では Storage Navigator (ストレージ管理 UI ソフトウェア) もしくは、管理 PC とディスクストレージ装置間およびディスクストレージ装置と外部認証サーバ間の通信路からの攻撃を想定しており、これらは特別な知識や技能、ツールを必要としない攻撃と考えることができる。

また、Storage Navigator (ストレージ管理 UI ソフトウェア) が動作する管理 PC には不正なソフト

ウェアのインストールを運用環境で禁止しているため、ディスクストレージ装置との詳細なインタフェースに基づく潜在的な脅威は想定から除外され、「明白な脆弱性」に対する評価を行うことで想定する脅威とのバランスがとれている。

TOEは、DKAに搭載されているLSIを利用してディスクドライブに格納するユーザデータを暗号化する機能を持っているものの、暗号鍵の実装は、インストール時および信頼されるセキュリティ管理者の操作により行われる。そのため「機密」に扱わないとTOEの脆弱性につながるTOEのセキュリティ特性は存在しない。

TOEはソフトウェアであり、設計資料に基づくセキュリティ機能の実装と、そのテストにより評価することで、セキュリティ機能が想定する脅威に対抗することを保証できると考えられ、EAL2の評価保証レベルは妥当である。尚、TOEの配付手続きにより、TOE参照のTOE消費者に示した消費者に対して、TOE配付におけるセキュリティが維持される。

また昨今、セキュリティ脆弱性問題への対応が重要となってきている。本製品はディスクストレージ装置の管理を行う重要な部分を受け持ち、セキュリティ欠陥を追跡し、脆弱性に対する迅速な対応が求められる。セキュリティ欠陥に対する、保証は、利用者に対する安心を担保するうえで重要であり ALC_FLR.1 コンポーネントを適用する。

7 TOE 要約仕様

本章では、TOE が提供するセキュリティ機能の要約仕様について述べる。

7.1 TOE セキュリティ機能

表 7-1 に TOE セキュリティ機能とセキュリティ機能要件（SFR）との対応関係について示す。ここで示される通り、本節で説明するセキュリティ機能は、6.1 節に記述される全ての SFR を満たすものである。

表 7-1 TOE セキュリティ機能とセキュリティ機能要件との対応関係

		TOE の IT セキュリティ機能					
		SF.LM	SF.FCSP	SF.SN	SF.ROLE	SF.HDD	SF.AUDIT
TOE セキュリティ 機能要件	FAU_GEN.1						X
	FAU_GEN.2						X
	FAU_SAR.1						X
	FAU_STG.1						X
	FAU_STG.3						X
	FAU_STG.4						X
	FCS_CKM.1					X	
	FCS_CKM.4					X	
	FDP_ACC.1	X					
	FDP_ACF.1	X					
	FDP_RIP.1					X	
	FIA_AFL.1			X			
	FIA_ATD.1a	X					
	FIA_ATD.1b	X					
	FIA_SOS.1a			X			
	FIA_SOS.1b		X				
	FIA_UAU.2		X	X			
	FIA_UID.2	X	X	X			
	FIA_USB.1a	X					
	FIA_USB.1b	X					

	TOE の IT セキュリティ機能					
	SF.LM	SF.FCSP	SF.SN	SF.ROLE	SF.HDD	SF.AUDIT
FMT_MOF.1				X		
FMT_MSA.1				X		
FMT_MSA.3	X					
FMT_MTD.1				X	X	
FMT_MTD.3					X	
FMT_SMF.1				X		
FMT_SMR.1				X		
FPT_STM.1						X
FTP_ITC.1			X			
FTP_TRP.1			X			

以下では各 TOE セキュリティ機能に関して、その概要および対応する SFR の具体的な実現方法について説明する。

7.1.1 SF.LM

TOE は、SAN 環境を介してホストと接続されている。SAN はホストとディスクストレージ装置をファイバチャネルによって接続するストレージ専用ネットワークである。TOE は SF.LM により、ホストがディスクストレージ装置内の LDEV（論理ボリューム）にアクセスする際のアクセス制御を行う。

【満たしている要件】 FIA_ATD.1a、FIA_USB.1a、FIA_ATD.1b、FIA_USB.1b、FIA_UID.2、FDP_ACC.1、FDP_ACF.1、FMT_MSA.3

TOE は、ユーザグループ情報（ロール、RSG 番号）を維持し、Storage Navigator (ストレージ管理 UI ソフトウェア) を代行するプロセスに関連付ける。(FIA_ATD.1a、FIA_USB.1a)

TOE は、ホストの属性情報（WWN、LU 番号）を維持し、ホストを代行するプロセスに関連付ける。(FIA_ATD.1b、FIA_USB.1b)

TOE は、ホストからのアクセスに関するセキュリティ機能の動作前に LU パス情報に設定されているホストの WWN を使用してホストを識別する。ファイバチャネルスイッチとの識別・認証が設定されている場合は、その識別・認証が成功した後、この機能は動作する。(FIA_UID.2)

TOE は、ホストを代行するプロセスが LDEV（論理ボリューム）へのアクセスを行うとき、および Storage Navigator (ストレージ管理 UI ソフトウェア) を代行するプロセスが LDEV（論理ボリューム）の生成、削除を行うときに「LM アクセス制御 SFP」を実施する。

「LM アクセス制御 SFP」は、以下の規則からなる。(FDP_ACC.1、FDP_ACF.1、FMT_MSA.3)

- ・ ホストを代行するプロセスに渡された WWN、LU 番号と、該当するオブジェクトのセキュリティ属性である LU パス情報が一致している場合、LDEV (論理ボリューム) に対するアクセスを許可する。LU パス情報が不一致の場合、アクセスを拒否する。
- ・ Storage Navigator (ストレージ管理 UI ソフトウェア) を代行するプロセスが RSG を生成、または削除する場合、Storage Navigator (ストレージ管理 UI ソフトウェア) を代行するプロセスに渡された、「Storage Navigator (ストレージ管理 UI ソフトウェア) のユーザグループ情報」 (ロール、RSG 番号) により、セキュリティ管理者のみが RSG を作成、または削除できる。
- ・ Storage Navigator (ストレージ管理 UI ソフトウェア) を代行するプロセスが LDEV (論理ボリューム) を生成、または削除する場合、Storage Navigator (ストレージ管理 UI ソフトウェア) を代行するプロセスに渡された、「Storage Navigator (ストレージ管理 UI ソフトウェア) のユーザグループ情報」 (ロール、RSG 番号) により、ストレージリソース管理者は、自身が所属するユーザグループに割当てられている RSG 番号と、LDEV (論理ボリューム) の RSG 番号が一致するとき、当該リソースグループ内に LDEV (論理ボリューム) を生成、または削除できる。
- ・ LDEV (論理ボリューム) を削除する際の条件：削除対象の LDEV (論理ボリューム) に関係付いた LU パス情報が存在しないときに当該 LDEV (論理ボリューム) を削除する。
- ・ ストレージリソース管理者が LDEV (論理ボリューム) を生成するとき、アクセス属性として制限的デフォルト値を与える。これは、LDEV (論理ボリューム) 生成時には LU パス情報が存在しないため、ホストからのアクセスが制限されることを意味する。(FMT_MSA.3)

7.1.2 SF.FCSP

TOE は、組織のセキュリティ方針により必要な場合は、FC-SP により、ファイバチャネルスイッチの識別・認証を行う。認証には、DH-CHAP(with NULL DH Group 認証)を使用する。

【満たしている要件】 FIA_SOS.1b、FIA_UID.2、FIA_UAU.2

TOE は、ホストが接続されるファイバチャネルスイッチの認証が有りの設定を適用後、ファイバチャネルスイッチと TOE がケーブルで接続されたことを検出した際に、ファイバチャネルスイッチの識別・認証の機能を動作させる。ファイバチャネルスイッチに対してセキュリティ認証実施確認コマンド処理を実行後、ファイバチャネルスイッチのポートの WWN、シークレットを用いた DH-CHAP により識別・認証を行う(FIA_UID.2、FIA_UAU.2)。この識別・認証が成功したときにファイバチャネルスイッチとディスクストレージ装置との接続を許可する(FIA_UAU.2)。

TOE は、FC-SP によるファイバチャネルスイッチの認証時に使用するシークレットの設定時、入力を 12~32 文字の半角英大文字、半角英小文字、半角数字、半角スペース、12 種類の半角記号.+@_=:/[~,~に制限する。(FIA_SOS.1b)

7.1.3 SF.SN

【満たしている要件】 FIA_AFL.1、FIA_SOS.1a、FIA_UID.2、FIA_UAU.2、FTP_TRP.1、FTP_ITC.1

TOE は、Storage Navigator (ストレージ管理 UI ソフトウェア) および SVP PC (管理保守 IF PC) へのリモートデスクトップ接続での識別・認証をユーザ ID およびパスワードにて行い、他のセキュリティ機能の動作前に実施する。なお、識別・認証が 3 回連続で失敗した場合は当該ユーザの識別・認証を 1 分間拒否する。(FIA_UID.2、FIA_UAU.2、FIA_AFL.1)

TOE は、SVP PC (管理保守 IF PC) 内部認証方式で使用するストレージ管理者および保守員の認証用のパスワードを設定するときに、入力文字を 6 文字以上 256 文字(保守員のパスワードは 127

文字)以下の半角英大文字、半角英小文字、半角数字、32種の半角記号!"#\$%&'()*+,-./:;<=>@[|^_{}`~に制限する。(FIA_SOS.1a)

TOEは、ストレージ管理者および保守員の識別・認証を行う際に、SVP PC (管理保守 IF PC)内部認証方式で認証を行い、入力されたユーザ ID が TOE 内に存在しない場合は外部認証サーバ方式で認証を行う。

TOEは、ストレージ管理者および保守員の識別・認証を外部認証サーバ方式で行う場合は、SVP PC (管理保守 IF PC)–外部認証サーバ間の通信に LDAPS、starttls、および RADIUS(認証プロトコルは CHAP)のいずれかを使用して通信を開始し、ストレージ管理者および保守員の識別・認証で使用するユーザアカウントのユーザ ID、パスワードを送信する。SVP PC (管理保守 IF PC)と外部認証サーバ間の通信に LDAPS、starttls、および RADIUS(認証プロトコルは CHAP)を使用することで、TSFデータの盗聴を防止する。(FTP_ITC.1)

TOEは、ストレージ管理者が管理 PC で Storage Navigator (ストレージ管理 UI ソフトウェア)を起動したときに通信を開始すること許可する。また、Storage Navigator (ストレージ管理 UI ソフトウェア)と SVP PC (管理保守 IF PC)間の通信に SSL を使用することで、TSFデータの盗聴を防止する。(FTP_TRP.1)

Storage Navigator (ストレージ管理 UI ソフトウェア)と SVP PC (管理保守 IF PC)間の通信に使用する SSL は、[TLSv1.0]をサポートする。SSL で使用する暗号関連のアルゴリズムを表 7-2 に示す。

表 7-2 SSL で使用する暗号関連のアルゴリズム

規格	アルゴリズム	鍵長(bit)	暗号操作	使用方法等
ANSI X9.30 Part1-1997	DSA	1024	認証	管理 PC に対して SVP PC (管理保守 IF PC)であることの証明(サーバ認証)に使用する。
RSA Security Inc. Public-Key Cryptography Standards(PKCS)#1 v2.1	RSA	512 以上	鍵交換	
FIPS PUB 197	AES	256 128	通信データの暗号化、および復号	[TLSv1.0]のハンドシェイクプロトコルによりセッション鍵に使用するアルゴリズムを選択する。
FIPS PUB 46-3	3DES	168		
FIPS PUB 180-2	SHA-256	256	ハッシュ	ハッシュ値算出時に使用する。
IEEE P1363 G.7 準拠	SHA1PRNG	64	乱数	セッション鍵を生成する際の鍵情報として使用する。

7.1.4 SF.ROLE

【満たしている要件】 FMT_MSA.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FMT_MOF.1

TOEは、Storage Navigator (ストレージ管理 UI ソフトウェア)を代行するプロセスの SVP PC (管理保守 IF PC)へのアクセスに対して、「LM アクセス制御 SFP」を実施する。

「LM アクセス制御 SFP」は、以下の規則からなる。

- ・ 「LM アクセス制御 SFP」は、LU パス情報（ホストの WWN、LU 番号、LDEV（論理ボリューム）番号）の作成、削除、参照の操作をロール、RSG 番号に基づき制限する。(FMT_MSA.1) LU パス情報に対して、各役割が実施できる操作を表 6-9 に示す。
- ・ 「LM アクセス制御 SFP」は、ユーザグループ情報（ロール、RSG 番号）の追加、削除、参照の操作をロールに基づき制限する。(FMT_MSA.1) ユーザグループ情報に対して、各役割が実施できる操作を表 6-10 に示す。

TOE は、以下の TSF データを管理する。(FMT_MTD.1)

- ・ Storage Navigator (ストレージ管理 UI ソフトウェア)のアカウント管理機能でストレージ管理者および保守員のユーザアカウントのユーザ ID、パスワード、ロール、RSG 番号を管理する。各役割が実施できる管理操作を表 6-10、表 6-11 に示す。
- ・ Storage Navigator (ストレージ管理 UI ソフトウェア)の FC-SP 機能でファイバチャネルスイッチの認証データである、WWN、シークレットを管理する。各役割が実施できる管理操作を表 6-12 に示す。
- ・ Storage Navigator (ストレージ管理 UI ソフトウェア)の格納データ暗号化機能でユーザデータの暗号化に使用する暗号鍵を管理する。各役割が実施できる管理操作を表 6-13 に示す。
- ・ Storage Navigator (ストレージ管理 UI ソフトウェア)のアクセス制御機能でユーザの認証方式を管理する。各役割が実施できる管理操作を表 6-14 に示す。

TOE は、以下の管理機能を有する。(FMT_SMF.1)

- ・ Storage Navigator (ストレージ管理 UI ソフトウェア)のユーザアカウント、ユーザアカウントのロール、ファイバチャネルスイッチの認証情報、WWN の識別情報、LU パス情報、ユーザグループ情報を管理する機能を有する。
- ・ ストレージ管理者および保守員の操作を管理する機能を有する。
- ・ 格納データ暗号化機能、FC-SP 認証機能、シュレディング機能、外部認証サーバの接続機能の停止と動作を管理する機能を有する。

TOE は、FC-SP によるホストが接続されるファイバチャネルスイッチの認証の有無(認証あり、認証なし)の設定操作をロールに基づき制限する。各役割が実施できる操作を表 6-8 に示す(FMT_MOF.1)。

TOE は、格納データ暗号化機能を使用する／使用しないの設定操作をロールに基づき制限する。各役割が実施できる操作を表 6-8 に示す(FMT_MOF.1)。

TOE は、外部認証サーバの接続機能を使用する／使用しないの設定操作（接続設定パラメータを含む）をロールに基づき制限する。各役割が実施できる操作を表 6-8 に示す(FMT_MOF.1)。

TOE は、シュレディング機能の開始と停止の操作をロールに基づき制限する。各役割が実施できる操作を表 6-8 に示す(FMT_MOF.1)。

TOE は、役割（セキュリティ管理者、ストレージリソース管理者、監査ログ管理者、保守員、ストレージ利用者）を維持し、関連付ける。(FMT_SMR.1)

7.1.5 SF.HDD

【満たしている要件】 FCS_CKM.1、FCS_CKM.4、FMT_MTD.1、FMT_MTD.3、FDP_RIP.1

TOE は、ユーザデータをディスクドライブに格納する際に暗号化して格納する。暗号化および復号には、DKA に搭載されている LSI を利用する。TOE は格納データ暗号化に使用する暗号鍵を生成する。暗号鍵生成のアルゴリズムを表 6-3 に示し、暗号鍵破棄方法を表 6-4 に示す(FCS_CKM.1、FCS_CKM.4)。

TOE は、格納データ暗号化に使用する暗号鍵に対する操作を実施できる管理者を制限する。セキュリティ管理者だけが暗号鍵の作成、削除、バックアップ（問い合わせ）、リストア（問い合わせ、改変）を実施できる(FMT_MTD.1)。

TOE は、格納データ暗号化に使用する暗号鍵を管理 PC にバックアップすることができる。また、バックアップした暗号鍵を管理 PC からディスクストレージ装置にリストアすることができる。リストアを行う際は、バックアップ時にバックアップデータ内に設定したハッシュ値とリストアするデータのハッシュ値の検証を行い、ハッシュ値が一致したときのみリストアする。ハッシュ値にはディスクストレージ装置の製造番号が含まれているため、バックアップしたディスクストレージ装置以外にはリストアできない(FMT_MTD.3)。

TOE は、使用を停止した LDEV（論理ボリューム）内のユーザデータをシュレディングする(FDP_RIP.1)。

7.1.6 SF.AUDIT

【満たしている要件】 FAU_GEN.1、FAU_GEN.2、FPT_STM.1、FAU_SAR.1、FAU_STG.1、FAU_STG.3、FAU_STG.4

TOE は、以下の監査機能を有する。

- TOE 内のセキュリティ機能に関する監査事象発生時は監査記録を生成する。生成する監査記録には、各監査対象事象の原因となったユーザアカウントのユーザ ID を付与する。また、監査記録生成時に使用する日時に関しては、SVP PC (管理保守 IF PC)上の OS が管理している時刻を元にして、監査記録を生成する。監査情報は、表 6-2 に記載する。
- 監査記録の不正な改変、削除を行える役割は存在しない。
- 監査記録は最大で 250,000 行保存する。監査記録が最大行数に達した場合は、保存を開始した行に戻って新しい情報を上書きするため、古い情報は消去される（ラップアラウンド方式）。監査記録が 175,000 行を超えた時点で、Storage Navigator (ストレージ管理 UI ソフトウェア)画面に超過した旨を通知し、監査ログ管理者に監査記録のダウンロードを促す。監査記録をダウンロードすると、監査記録の格納行数をリセットし、1 行から記録を開始する。
- 監査記録をダウンロードできるのは監査ログ管理者だけである。
- 監査機能の起動と終了は、TOE の起動と終了に連動させる。

TOE が取得する監査ログは、基本情報と詳細情報から構成される。基本情報の出力内容を表 7-3 に示し、詳細情報の出力内容を表 7-4 に示す。

表 7-3 基本情報の出力内容

項番	項目	取得内容
1	日付	事象発生日付を出力する。
2	時刻	事象発生時刻を出力する。
3	タイムゾーン	GMT (Greenwich Mean Time) との時差を出力する。
4	ユーザ ID	Storage Navigator (ストレージ管理 UI ソフトウェア)のユーザ ID を出力する。

項番	項目	取得内容													
5	機能名	<p>設定操作を実行した機能名を示す文字列を出力する。</p> <table border="1" data-bbox="735 327 1455 1041"> <thead> <tr> <th data-bbox="735 327 1455 394">機能名</th> </tr> </thead> <tbody> <tr> <td data-bbox="735 394 1455 495">ストレージ管理者および保守員の識別・認証機能の名称</td> </tr> <tr> <td data-bbox="735 495 1455 595">ユーザアカウント作成、変更、削除、パスワード変更、ユーザグループ変更機能の名称</td> </tr> <tr> <td data-bbox="735 595 1455 775">LU パス情報の作成、削除機能、ファイバチャネルスイッチの WWN、シークレットの作成、変更、削除、FC-SP によるファイバチャネルスイッチの認証有無の設定変更機能の名称</td> </tr> <tr> <td data-bbox="735 775 1455 875">FC-SP によるファイバチャネルスイッチの認証機能の名称</td> </tr> <tr> <td data-bbox="735 875 1455 976">格納データ暗号化の有効/無効設定、暗号鍵の生成、削除、バックアップ、リストア機能の名称</td> </tr> <tr> <td data-bbox="735 976 1455 1041">シュレディング機能の名称</td> </tr> </tbody> </table>	機能名	ストレージ管理者および保守員の識別・認証機能の名称	ユーザアカウント作成、変更、削除、パスワード変更、ユーザグループ変更機能の名称	LU パス情報の作成、削除機能、ファイバチャネルスイッチの WWN、シークレットの作成、変更、削除、FC-SP によるファイバチャネルスイッチの認証有無の設定変更機能の名称	FC-SP によるファイバチャネルスイッチの認証機能の名称	格納データ暗号化の有効/無効設定、暗号鍵の生成、削除、バックアップ、リストア機能の名称	シュレディング機能の名称						
機能名															
ストレージ管理者および保守員の識別・認証機能の名称															
ユーザアカウント作成、変更、削除、パスワード変更、ユーザグループ変更機能の名称															
LU パス情報の作成、削除機能、ファイバチャネルスイッチの WWN、シークレットの作成、変更、削除、FC-SP によるファイバチャネルスイッチの認証有無の設定変更機能の名称															
FC-SP によるファイバチャネルスイッチの認証機能の名称															
格納データ暗号化の有効/無効設定、暗号鍵の生成、削除、バックアップ、リストア機能の名称															
シュレディング機能の名称															
6	操作名または事象名	<p>機能毎の操作名称を略称で出力する。</p> <table border="1" data-bbox="735 1108 1455 1995"> <thead> <tr> <th data-bbox="735 1108 1455 1176">操作名称</th> </tr> </thead> <tbody> <tr> <td data-bbox="735 1176 1455 1243">ストレージ管理者および保守員の識別・認証</td> </tr> <tr> <td data-bbox="735 1243 1455 1310">ユーザアカウントの作成</td> </tr> <tr> <td data-bbox="735 1310 1455 1377">ユーザアカウントの変更</td> </tr> <tr> <td data-bbox="735 1377 1455 1444">ユーザアカウントの削除</td> </tr> <tr> <td data-bbox="735 1444 1455 1512">ユーザアカウントのパスワード変更</td> </tr> <tr> <td data-bbox="735 1512 1455 1579">ユーザグループにロールを追加</td> </tr> <tr> <td data-bbox="735 1579 1455 1646">ユーザグループからロールを削除</td> </tr> <tr> <td data-bbox="735 1646 1455 1713">ユーザグループに RSG 番号を追加</td> </tr> <tr> <td data-bbox="735 1713 1455 1780">ユーザグループから RSG 番号を削除</td> </tr> <tr> <td data-bbox="735 1780 1455 1848">LU パス情報の作成</td> </tr> <tr> <td data-bbox="735 1848 1455 1915">LU パス情報の削除</td> </tr> <tr> <td data-bbox="735 1915 1455 1995">ファイバチャネルスイッチの WWN、シークレットの作成</td> </tr> </tbody> </table>	操作名称	ストレージ管理者および保守員の識別・認証	ユーザアカウントの作成	ユーザアカウントの変更	ユーザアカウントの削除	ユーザアカウントのパスワード変更	ユーザグループにロールを追加	ユーザグループからロールを削除	ユーザグループに RSG 番号を追加	ユーザグループから RSG 番号を削除	LU パス情報の作成	LU パス情報の削除	ファイバチャネルスイッチの WWN、シークレットの作成
操作名称															
ストレージ管理者および保守員の識別・認証															
ユーザアカウントの作成															
ユーザアカウントの変更															
ユーザアカウントの削除															
ユーザアカウントのパスワード変更															
ユーザグループにロールを追加															
ユーザグループからロールを削除															
ユーザグループに RSG 番号を追加															
ユーザグループから RSG 番号を削除															
LU パス情報の作成															
LU パス情報の削除															
ファイバチャネルスイッチの WWN、シークレットの作成															

項番	項目	取得内容
		ファイバチャネルスイッチの WWN、シークレットの変更 ファイバチャネルスイッチの WWN、シークレットの削除 FC-SP によるファイバチャネルスイッチの認証有無の設定変更 FC-SP によるファイバチャネルスイッチの認証 格納データ暗号化の有効/無効設定 格納データ暗号化の暗号鍵の生成 格納データ暗号化の暗号鍵の削除 格納データ暗号化の暗号鍵のバックアップ 格納データ暗号化の暗号鍵のリストア シュレディングの開始 シュレディングの停止
7	パラメータ	実行した設定操作のパラメータを出力する。
8	操作の結果	操作結果を出力する。
9	送信元ホスト識別情報	管理 PC または保守員 PC の IP アドレスを出力する。 FC-SP によるファイバチャネルスイッチ認証時は、ファイバチャネルスイッチの WWN を出力する。
10	ログ情報の通し番号	保存されているログ情報の通し番号を出力する。

表 7-4 詳細情報の出力内容

項番	監査事象	詳細情報
1	ストレージ管理者の識別・認証	・ なし
2	保守員の識別・認証	・ なし
3	ストレージ管理者および保守員のユーザアカウントの作成、変更、削除	・ 操作対象のユーザ ID、有効／無効設定情報、認証方式、ユーザグループ名称、操作結果（成功、失敗）
4	ストレージ管理者および保守員のユーザアカウントのパスワード変更	・ 操作対象のユーザ ID、操作結果（成功、失敗）
5	ストレージ管理者および保守員の所属するユーザグループの変更	・ 操作対象のユーザ ID、ユーザグループ名称、ロール、RSG 番号、操作結果（成功、失敗）
6	LU パス情報の作成、削除	・ ポート番号、ホストの WWN、LU 番号、LDEV（論理ボリューム）番号
7	ファイバチャネルスイッチの WWN、シークレットの作成、変更、削除	・ ポート番号、ファイバチャネルスイッチの WWN、ポートの数
8	FC-SP によるファイバチャネルスイッチの認証有無の設定変更	・ ポート番号、ポートの WWN、認証有無、操作内容（変更）、ポートの数
9	FC-SP によるファイバチャネルスイッチの認証	・ なし
10	格納データ暗号化の有効／無効設定	・ パリティグループ番号、暗号化有効／無効設定内容、操作した暗号鍵の番号、設定したパリティグループの数
11	格納データ暗号化の暗号鍵の生成、削除、バックアップ、リストア	・ 暗号鍵番号、操作した暗号鍵の数
12	シュレディングの開始、停止	・ 書込みデータ、書込み回数、対象 LDEV（論理ボリューム）番号、対象 LDEV（論理ボリューム）数、シュレディング処理の実行順番

8 参考文献

- Common Criteria for Information Technology Security Evaluation
Part1: Introduction and general model Version 3.1 Revision 4
CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation
Part2: Security functional components Version 3.1 Revision 4
CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation
Part3: Security assurance components Version 3.1 Revision 4
CCMB-2012-09-003
- Common Methodology for Information Technology Security Evaluation
Evaluation methodology Version 3.1 Revision 4
CCMB-2012-09-004
- 情報技術セキュリティ評価のためのコモンクライテリア
パート 1: 概説と一般モデル 2012 年 9 月 バージョン 3.1 改訂第 4 版 最終版
CCMB-2012-09-001
平成 24 年 11 月 翻訳第 1.0 版 最終版
独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア
パート 2: セキュリティ機能コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 4 版 最終版
CCMB-2012-09-002
平成 24 年 11 月 翻訳第 1.0 版 最終版
独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
- 情報技術セキュリティ評価のためのコモンクライテリア
パート 3: セキュリティ保証コンポーネント 2012 年 9 月 バージョン 3.1 改訂第 3 版 最終版
CCMB-2012-09-003
平成 24 年 11 月 翻訳第 1.0 版 最終版
独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室
- 情報技術セキュリティ評価のための共通方法
評価方法 2012 年 9 月 バージョン 3.1 改訂第 4 版 最終版
CCMB-2012-09-004
平成 24 年 11 月 翻訳第 1.0 版 最終版
独立行政法人 情報処理推進機構 セキュリティセンター 情報セキュリティ認証室

8.1 ドキュメントで使用する用語

一般的に使用されている CC の用語の定義については、CC パート 1 セクション 4 を参照する。

8.1.1 ST 専門用語

用語	説明
ディスクサブシステム	ディスクストレージ装置のことで、Hitachi Virtual Storage Platform G1000、Hitachi Virtual Storage Platform VX7 を指す。
Redundant Array of Independent Disks (RAID)	複数のディスクドライブにデータを拡散、または重複させることによりディスクの破壊から素早く復元し、性能を良くし、データの冗長性を備える方法。一般的に使われる RAID タイプには、RAID 0(データストライピング)、RAID 1(ディスクミラーリング)、RAID 5(分散パリティを付加したストライピング)などがある。
Storage Navigator	ディスクストレージ装置の設定を行う GUI を提供するプログラム。Flex アプリケーションと Java アプレットで構成され、SVP PC (管理保守 IF PC)および管理 PC で動作する。ストレージ管理者および保守員が使用する。
パリティグループ	RAID(上記参照)を実現するためのディスクドライブのグループ。 パリティグループはユーザデータとパリティ情報を格納した複数のディスクドライブで構成され、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でもユーザデータへのアクセスが可能である。
SAN	Storage Area Network の略。ファイバチャネルによりディスクストレージ装置とホストコンピュータを接続した、ストレージ専用のネットワークである。ファイバチャネルにより、高速・高信頼のデータ通信が可能。
ファイバチャネル	Storage Area Network (SAN) を構築するための高速ネットワークテクノロジー。
ファイバチャネルスイッチ	ファイバチャネルインタフェースの各種装置を相互に接続するスイッチ。ファイバチャネルスイッチを使うことで、複数のホストとディスクストレージ装置を高速接続し、SAN (Storage Area Network) を構築することができる。
LDEV (論理ボリューム)	論理デバイス (Logical Device) の略。ディスクストレージ装置内のユーザ領域に作成するボリュームの単位。論理ボリュームとも呼ばれる。
LDEV (論理ボリューム) 番号	論理デバイス (Logical Device)作成時に付与するユニークな番号。
論理ユニット (LU)	オープンシステムのホストから使用する LDEV (論理ボリューム) を LU と呼ぶ。オープンシステムのファイバチャネルインタフェースでは 1 個または、複数の LDEV (論理ボリューム) にマッピングされた LU にアクセスできる。
LU パス	オープンシステム用ホストと LU 間を結ぶデータ入出力経路。

用語	説明
LU 番号 (LUN)	ファイバチャネルポートに関係付けられて、ホストからアクセス可能である LDEV (論理ボリューム)。または、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。
ポート	ファイバチャネルの終端。各ポートはポート番号により識別される。
Fibre Channel Security Protocol (FC-SP)	ホストとファイバチャネルスイッチ、およびファイバチャネルスイッチとディスクストレージ装置との通信を行う際、お互いの機器認証を行うためのプロトコル。認証には、DH-CHAP with NULL DH Group 認証を使用。
外部認証サーバの接続設定パラメータ	外部認証サーバを使用して識別・認証を行うために SVP PC (管理保守 IF PC)に設定するパラメータで、以下の情報が存在する。 外部認証サーバの種別(LDAP, RADIUS)、外部認証サーバのアドレス、外部認証サーバの証明書、プロトコル(LDAPS, starttls, CHAP)、ポート番号など。
starttls	LDAP に接続する TCP セッションを暗号化するプロトコル。
RADIUS	認証とアカウントングを実現するプロトコル。
CHAP	認証の時にクライアントからサーバ間に送信するパスワードを暗号化するプロトコル。
DH-CHAP	FC-SP で使用するプロトコルで、CHAP プロトコルを使用して鍵交換を行う。
A/H-65AD A-65BD HT-40BD	Hitachi Virtual Storage Platform G1000 の国内版型名。
DKC810I	Hitachi Virtual Storage Platform G1000 の海外版型名。

8.1.2 略語

この文書では次の略語が使われている。

CACHE	CACHE memory
CC	Common Criteria
CHA	Channel Adapter
CHAP	Challenge Handshake Authentication Protocol
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKA	Disk Adapter
DKC	Disk Controller
EAL	Evaluation Assurance Level

FC-SP	Fibre Channel Security Protocol
HDD	Hard disk drive
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over TLS
LDEV	Logical Device
LSI	Large Scale Integration
LU	Logical unit
LUN	Logical Unit Number
PC	Personal Computer
PP	Protection Profile
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SF	Security Function
SFP	Security Function Policy
SSL	Secure Sockets Layer
ST	Security Target
SVP	Service Processor
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
VSP	Virtual Storage Platform
WWN	World Wide Name