HITACHI
Inspire the Next

Hitachi Universal Storage Platform V
セキュリティターゲット

発行日:	2008 年 10 月 8 日
バージョン:	1.13
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－

表目次

図目次

1　ST 概説

この章ではセキュリティターゲット（以下 ST と略す）、評価対象(TOE)、CC への適合性、ST の構成、専門用語、および製品概要を示す。

1.1　ST 識別

TOE 識別：	Hitachi Universal Storage Platform V, Hitachi Universal Storage Platform H24000, Hitachi Universal Storage Platform VM, Hitachi Universal Storage Platform H20000 用 制御プログラム バージョン 60-02-32-00/00(R6-02A-14)
ST 識別：	Hitachi Universal Storage Platform V セキュリティターゲット
ST バージョン：	1.13
ST 発行日：	2008 年 10 月 8 日
ST 作成：	株式会社　日立製作所
CC 識別：	Common Criteria for Information Technology Security Evaluation Version 2.3 補足-0512 適用

1.2 ST 概要

Hitachi Universal Storage Platform V（Hitachi Universal Storage Platform H24000 というブランド名でも販売されている。以下 USP V と略す。）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、ディザスタリカバリ機能、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。Hitachi Universal Storage Platform VM（Hitachi Universal Storage Platform H20000 というブランド名でも販売されている。以下 USP VM と略す。）は、ラックマウント式の省スペース型で、ディスク容量の拡張性以外は USP V と同じ機能を持っている。

ストレージ装置には SAN 環境や IP ネットワーク環境を介して、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、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、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、Hitachi Virtual Partition Manager 機能はポート、キャッシュメモリ、およびディスク（パリティグループ）を複数のディスクサブシステムに論理分割し、論理分割した各パーティションを管理する管理者を配置できるようにしている。そして、各パーティションの管理者にパーティション内に割り当てられたリソースを管理する権限を与えることにより、各パーティションの管理者は、他のパーティション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。

本 ST は、USP V および USP VM 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。

なお、本 ST で評価したバージョンの USP V および USP VM は株式会社 日立製作所 RAID システム事業部が製造し、出荷したものである。

1.3 CC 適合

本 ST の CC 適合性は以下の通りである。

- CCバージョン 2.3[1] パート 2 適合
- CC バージョン 2.3 パート 3 適合
- パッケージ適合 EAL2 適合
- 適合する PP はない。

[1]情報セキュリティ国際評価基準(CC) 2005 年 8 月, バージョン 2.3, CCMB-2005-08-001，CCMB-2005-08-002，CCMB-2005-08-003.

1.4　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 2.3 を参照する。

1.4.1　ST 専門用語

用語	説明
ディスクサブシステム	ストレージ装置のことで、Hitachi Universal Storage Platform V、Hitachi Universal Storage Platform VM 等を指す。
ストレージ論理パーティション (SLPR)	ストレージ装置内のキャッシュとハードディスクドライブを論理的に分割することによって作成されるパーティション。１つ以上の CLPR と１つ以上の対象ポートを割り当てる。
キャッシュ論理パーティション (CLPR)	キャッシュメモリを論理的に分割することによって作成されるパーティション。CLPR 内に 1 つ以上のパリティグループを割り当てる。
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。
パリティグループ (PG)	RAID(上記参照)を実現するためのハード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ハード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。
FC ストレージネットワーク	ファイバチャネルを利用したストレージ装置のネットワーク。
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	論理デバイス (Logical Device) の略。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。

用語	説明
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 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 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。
論理ユニット番号 (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。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。
キャッシュメモリ	最近または頻繁にアクセスされたデータの一時的な高速ストレージ領域。
Fibre Channel Security Protocol (FC-SP)	ホストまたはファイバチャネルスイッチとストレージ装置との通信を行なう際、お互いの機器認証を行なうためのプロトコル。認証には、DH-CHAP with NULL DH Group 認証を使用。

1.4.2　参照

この文書で参照する他の文書を次の略語で表現する。

[略記号]　文書名

[SSLv3.0] “The SSL Protocol Version 3.0”,http://wp.netscape.com/eng/ssl3/draft302.txt

[TLSv1.0] “The TLS Protocol Version 1.0”,ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt

1.4.3　略語

この文書では次の略語が使われている。

CC　Common Criteria

CHA　Channel Adapter

CLPR　Cache Logical Partition

DH-CHAP　Diffie Hellman - Challenge Handshake Authentication Protocol

DKA　Disk Adapter

DKC　Disk Controller

EAL	Evaluation Assurance Level
FC-SP	Fibre Channel Security Protocols
HDD	Hard disk drive
JRE	Java Runtime Environment
LAN	Local Area Network
LDEV	Logical Device
LU	Logical unit
LUN	Logical Unit Number
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SF	Security Function
SFP	Security Function Policy
SLPR	Storage Logical Partition
SOF	Strength of Function
SSL	Secure Sockets Layer
ST	Security Target
SVP	Service Processor
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
USP V	Universal Storage Platform V
USP VM	Universal Storage Platform VM
VPM	Virtual Partition Manager
WWN	World Wide Name

2　TOE 記述

本章では、TOE の種別と範囲・境界を定義し、TOE についての全般的な情報を提供する。

2.1　TOE の種別

TOE である、USP V および USP VM 用制御プログラム バージョン 60-02-32-00/00(R6-02A-14)は、株式会社日立製作所製ストレージ装置「Hitachi Universal Storage Platform V」、「Hitachi Universal Storage Platform H24000」、「Hitachi Universal Storage Platform VM」「Hitachi Universal Storage Platform H20000」上で動作するソフトウェアである。上記ストレージ装置は、ハードウェアとしての装置の規模は異なるが、ともに同一の制御プログラムを使用する。

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”で構成される。

DKCMAIN マイクロプログラムは、ストレージ装置内の複数の基板上に搭載され、ストレージ装置に接続されたホストと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 プログラムが 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。

本 TOE 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装置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を提供するものである。

2.2　ストレージ装置を含むシステムの一般的な構成

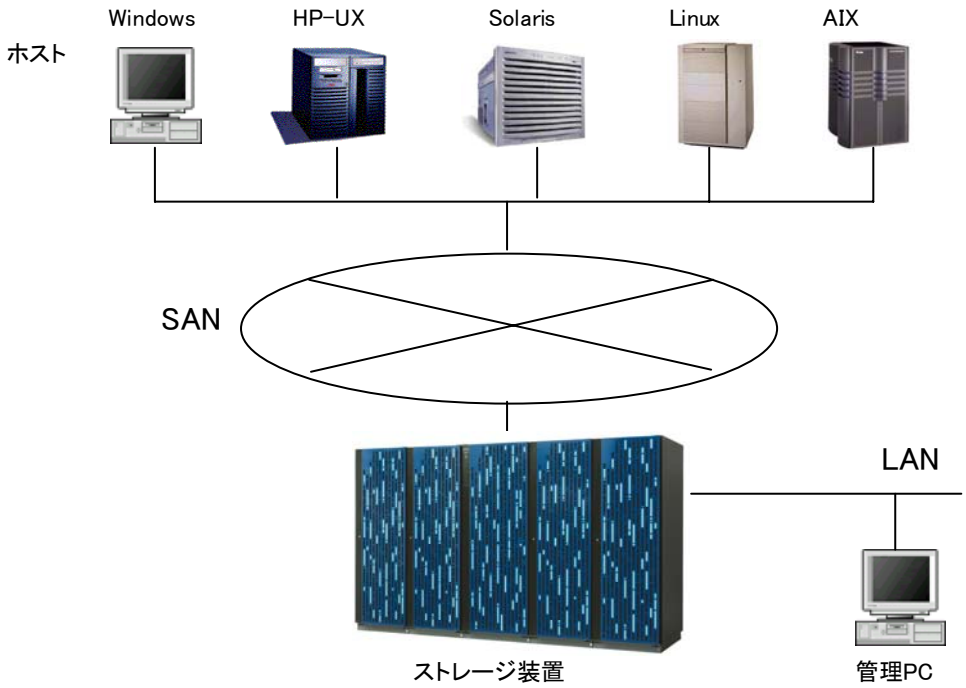

図 2.1 ストレージ装置を含むシステムの一般的な構成

図 2.1に、ストレージ装置を含むシステムの一般的な構成を示し、図に関する説明を以下に示す。

（1） ストレージ装置

通常、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、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。

ホストは顧客の運用において接続管理が行われており、ホストの識別情報を改造して、ストレージ装置の許可されていないユーザデータにアクセスするような高い攻撃能力は、本 ST では想定していない。しかし、ホスト識別情報の改造をストレージ装置の機能により防止することを顧客のポリシーで求められる場合、TOE はストレージ装置に接続されるホストまたは、ファイバチャネルスイッチの認証を行うことが可能である。

（3）管理 PC

管理 PC は、ストレージ装置の装置制御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、ストレージ装置の管理者が装置制御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 とストレージ装置は LAN(Local Area Network)を介して接続される。

2.3 TOE とストレージ装置

図 2.2に、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。

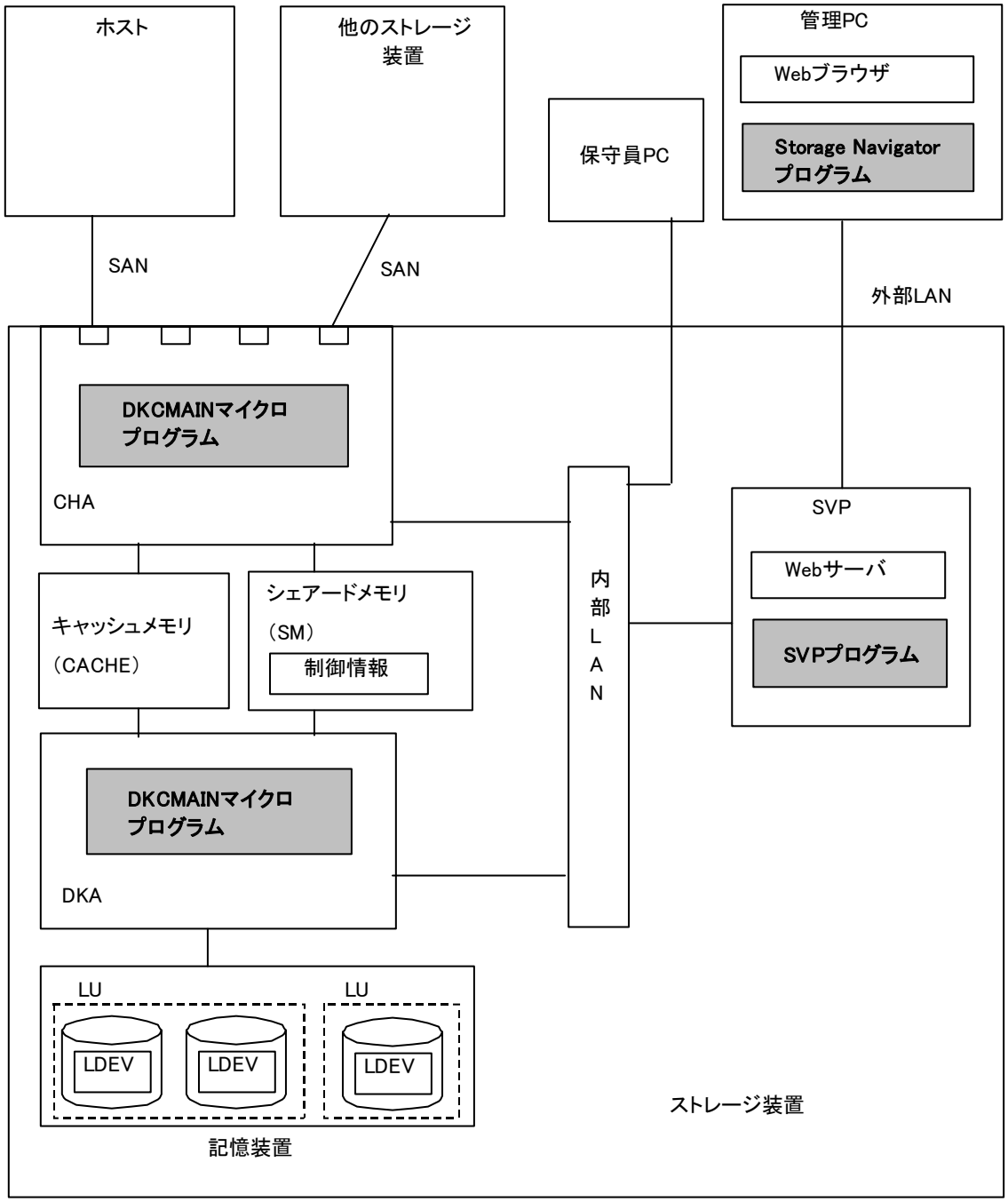

図 2.2 ストレージ装置の構成

ストレージ装置は、チャネルアダプタ（CHA）、シェアードメモリ（SM）、キャッシュメモリ（CACHE）、ディスクアダプタ（DKA）、記憶装置が含まれる制御系と、SVP（Service Processor）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。

2.3.1　制御系

（1）チャネルアダプタ

チャネルアダプタ（CHA）は、ホストからストレージ装置に対する命令を処理して、データ転送を制御するアダプタである。ホストはファイバチャネルを介して、CHA 上のファイバポートに接続される。CHA では、TOE の一部である DKCMAIN マイクロプログラムが動作する。

（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 では、TOE の一部である DKCMAIN マイクロプログラムが動作する。

（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、データの Read/Write を行うために使用する。

（4）シェアードメモリ

シェアードメモリ（SM）は、CHA 上の DKCMAIN マイクロプログラム、DKA 上の 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制御情報が格納される。この制御情報には、セキュリティ機能の動作に必要な設定情報も含まれる。シェアードメモリ上の制御情報は 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。また、制御情報の更新は、SVP、Storage Navigator からの指示により、TOE が行う。

（5）記憶装置

記憶装置は複数のハードディスクで構成されており、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（論理デバイス）が作成される。ユーザデータへのアクセスは、LDEV 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 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 にマッピングされる。
LDEV 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ハード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、SM、CACHE、DKA は高速クロスバ・スイッチで接続されている。

2.3.2　管理系

（１）SVP

SVP は、ストレージ装置全体の管理を行うためにストレージ装置に内蔵されているサービスプロセッサであり、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、ストレージ装置の保守機能（各種構成部品の増設・減設・交換やプログラムのアップデート等）および装置制御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 プログラムから受け取った装置制御情報の設定指示を 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、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。

（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。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 に接続して使用する。

（３）管理 PC

管理PCは、顧客のStorage Navigator利用者（2.4節参照）が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プログラムが動作する。管理PCとSVPは外部LANで接続される。

（４）Storage Navigator プログラム

Storage Navigatorプログラムは、顧客のStorage Navigator利用者（2.4節参照）がストレージ装置の装置制御情報の管理を行うために使用するソフトウェアである。以下、Storage Navigatorプログラムを単にStorage Navigatorと称する。

Storage Navigator は Java applet program であり、SVP から管理 PC にダウンロードされて Web ブラウザ上で動作する。SVP と Storage Navigator の通信には、SSL が使用される。Storage Navigator 利用者は管理 PC の Web ブラウザを使って Storage Navigator とやりとりをし、ストレージ装置の設定操作を行う。

また、Storage Navigator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。

（５）他のストレージ装置

ストレージ装置のポートには、ホスト以外に、他のストレージ装置を接続することができる。他のストレージ装置を接続することにより、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。他の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管理者が実施するものである。従って、ストレージ装置と接続する他のストレージ装置は、TOE を搭載するストレージ装置に限定される。

制御系ネットワーク（CHA、SM、CACHE、DKA の高速クロスバ・スイッチ接続）と管理系ネットワーク（内部 LAN、外部 LAN）は完全に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、管理 PC、保守員 PC から直接、SM、CACHE、記憶装置にアクセスすることはできない。そのため、管理系ネットワークからのユーザデータへの攻撃は完全に防御されている。

なお、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、顧客のStorage Navigator利用者、ストレージ利用者（2.4節参照）で準備したり、変更したりすることはない。

2.3.3　TOE の範囲

2.3.3.1　物理境界

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。

2.3.3.1.1　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。

TOE・環境	構成要素	説明
環境	Hitachi Universal Storage Platform V Hitachi Universal Storage Platform H24000	USP V ハードウェア。SVP ハードウェアを含む。 これらのモデルの違いは外部ラックのブランドの違いである。 ストレージ装置内の HDD 数やポート数は顧客のオーダーした構成により変わる。
環境	Hitachi Universal Storage Platform VM Hitachi Universal Storage Platform H20000	USP VM ハードウェア。SVP ハードウェアを含む。 これらのモデルの違いは外部ラックのブランドの違いである。 ストレージ装置内の HDD 数やポート数は顧客のオーダーした構成により変わる。
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
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 • CPU： Pentium 4 2.4GHz 相当以上 推奨：Pentium 4 3GHz 以上 • RAM： 512 MB 以上; 推奨： 1 GB • 有効な HDD 空き領域： 150 MB 以上 • モニター： High-Color 16-bit 以上; 解像度 1024x768 以上 • LAN カード： 100Base-T
環境	FC ストレージネットワーク	ファイバチャネルを利用したストレージ装置のネットワーク

2.3.3.1.2　ソフトウェア構成要素

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 60-02-32-00/00	CHA と DKA で動作する。
TOE	SVP プログラム バージョン 60-02-26/00	SVP 上で動作する SVP プログラムと 管理 PC で動作する Storage Navigator を含む
環境	Web サーバ	SVP 上で動作する。以下ソフトウェアを使用する • Apache 2.2.4
環境	管理 PC OS	管理 PC の OS。 • Windows XP (SP2 以降)
環境	Web ブラウザ	管理者 PC で起動している Web ブラウザ。 サポートしているブラウザ • Internet Explorer 6.0 SP2
環境	Java ランタイム環境	管理者 PC で起動している Java ランタイム環境。 • JRE 1.5.0_06

2.4 ストレージ装置の関与者

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。システム構築時、TOE には初期アカウントがビルドインされている。初期アカウントは以下の「全体アカウント管理者」の権限を持つ。これ以外の管理者は存在しない。

・ 全体アカウント管理者：

全体アカウント管理者は、管理者（全体ストレージ管理者、分割ストレージ管理者、全体アカウント管理者、分割アカウント管理者、監査ログ管理者）の Storage Navigator の操作に関するアカウントの登録、変更、削除が出来る。

・ 全体ストレージ管理者：

ストレージ装置全体の管理権限を持つ。

全体ストレージ管理者は、Virtual Partition Manager機能（詳細は 2.6.1節を参照）により、ストレージ装置のリソース（ポート、キャッシュメモリ、LDEV）を論理パーティションに分割することができる。

分割した論理パーティションにおいて、ホストから見えるLUの管理を行う分割ストレージ管理者および、分割アカウント管理者を登録することで、他の論理パーティションの存在やその影響を受けない仮想ディスクサブシステム（詳細は 2.6.1節を参照）の管理操作が可能になる。

仮想ディスクサブシステムでは、分割ストレージ管理者が他のストレージ管理者を置きたい時、またはその権限を取り消したい時に、Storage Navigator から論理パーティションの範囲でアカウント管理操作を行えるようにするために、分割アカウント管理者を設ける。

・ 分割ストレージ管理者：

全体ストレージ管理者に割り当てられた論理パーティション内のリソース(ポート、キャッシュメモリ、LDEV)を管理できる管理者で、ホストの識別情報である WWN と、アクセスを許可する LDEV 番号の関係付けを行う。

・ 分割アカウント管理者：

分割した論理パーティションのアカウントを管理できる管理者。

分割ストレージ管理者用アカウントおよび分割アカウント管理者用アカウントの作成、変更、削除を Storage Navigator を用いて行うことが可能である。

・ 監査ログ管理者：

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 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：

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。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。また、顧客からの要請により、全体ストレージ管理者、分割ストレージ管理者、全体アカウント管理者、分割アカウント管理者、監査ログ管理者が行う設定作業を代行する場合もある。保守員は、保守員用 PC から SVP へアクセスし、保守作業を実施する。直接、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。TOE は、保守員 PC を使用して SVP 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：

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

以下、全体ストレージ管理者、分割ストレージ管理者、全体アカウント管理者、分割アカウント管理者、監査ログ管理者をまとめて、Storage Navigator 利用者と呼ぶ。

2.5 保護対象資産

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、Storage Navigator 利用者による権限外の設定変更、またはストレージ利用者による権限外のアクセスからの保護が必要である。

本 ST では、複数に分割された論理パーティションが存在する環境において、パーティション内の LDEV 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、許可されていないストレージ利用者のアクセスから保護対象資産を保護する。さらに、論理パーティションで識別された範囲への操作権限を持たない分割ストレージ管理者による保護対象資産の削除を防止する。

2.6 TOE の機能

TOE が提供する IT 機能、およびストレージ装置のデータセキュリティ機能の概要を以下に示す。

2.6.1 Virtual Partition Manager 機能概要

USP V および USP VM ディスクサブシステムは、複数の組織（たとえば、複数の企業や企業内の複数の部署）によって共有することが可能である。そのため、1 台のディスクサブシステムに複数の異なる組織の管理者が存在することがある。このような状況では、ある組織の管理者が誤って他の組織のボリュームを壊してしまったり、不適切な操作をしたために、その影響が他の組織に波及してしまい、ディスクサブシステム全体の管理が複雑で困難になるおそれがある。

Virtual Partition Managerのストレージ管理分割機能(VPM機能)は、1 台のディスクサブシステム全体のリソース（ポート、キャッシュメモリ、LDEV）を複数の仮想ディスクサブシステムに分割し、それぞれの仮想ディスクサブシステムの管理者が、それぞれの仮想ディスクサブシステムだけにアクセスするため、ある管理者が他の組織のボリュームを壊したり、特定の組織のデータが漏洩したりすることを防ぐことができる。図 2.3に 仮想ディスクサブシステムの概要を示す。図 2.3では、1 台のディスクサブシステムを 2 つの仮想ディスクサブシステムに分割して、リソースを割り当てている。

ディスクサブシステムを分割することによって作成される仮想ディスクサブシステムを論理パーティション(SLPR：Storage Logical Partition)と呼ぶ。論理パーティションは、SLPR 番号を付けて識別する。TOE のリソースを分割し、特定の仮想ディスクサブシステムに割り当てるため、論理パーティションに、分割したリソースを識別するための SLPR 番号を付与している。各仮想ディスクサブシステムに割り当てられた分割ストレージ管理者は、管理する SLPR 番号で指定された範囲の論理パーティションのリソースに対して許可された操作権限を持つ。

また VPM 機能では、ディスクサブシステム内のキャッシュメモリを複数の仮想キャッシュメモリに分割することができる。これにより、利用できるキャッシュ容量を予めホストに割り当てておくことができ、特定のホストがキャッシュメモリの多くの領域を占有してしまうような状況を避けることができる。この分割した仮想キャッシュメモリを CLPR(Cache Logical Partition)と呼ぶ。

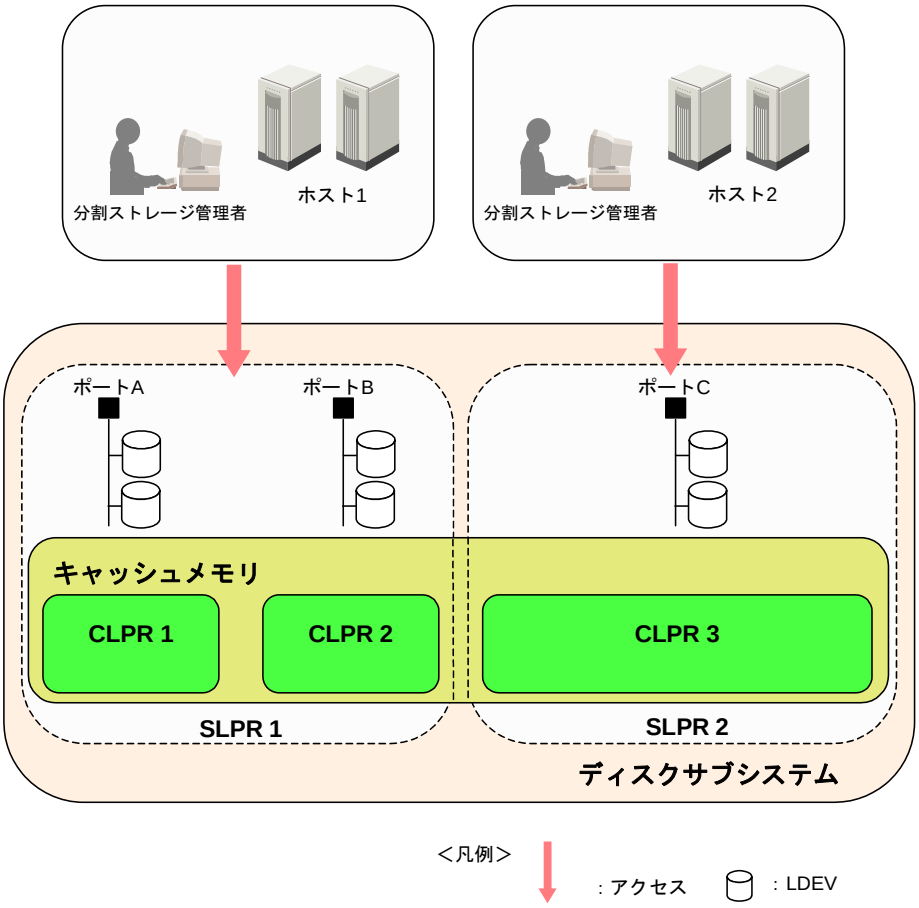

図 2.3仮想ディスクサブシステムの概要

2.6.2　TOE が提供するセキュリティ機能

2.6.2.1　LDEV へのアクセス制御

2.6.2.1.1　LUN Manager 機能

ユーザデータを格納する LDEV は Storage Navigator を利用して生成され、生成時に SLPR との関連付けが行われる。ホストから LDEV 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 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 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 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。

2.6.2.1.2　Virtual Partition Manager 機能

仮想ディスクサブシステムの分割ストレージ管理者は、自身が管理する仮想ディスクサブシステム以外の仮想ディスクサブシステムにはアクセスすることができない。そのため、他の仮想ディスクサブシステムの分割ストレージ管理者によるデータ破壊やデータ漏えいを防ぐことができる。

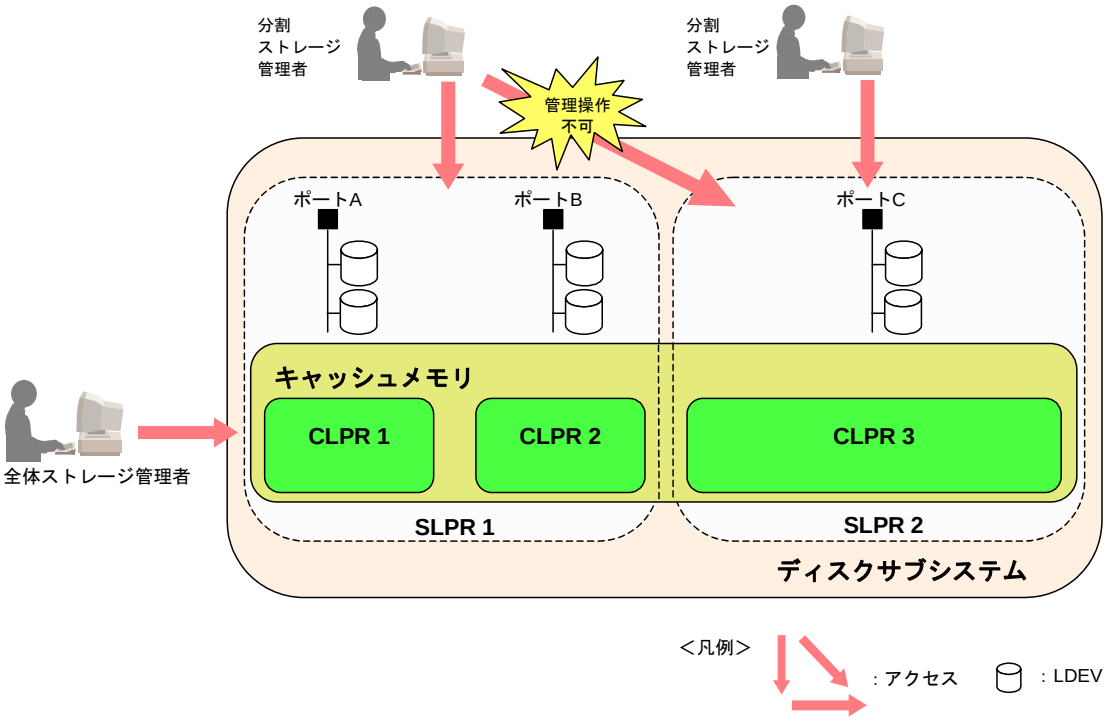

図 2.4 全体ストレージ管理者、分割ストレージ管理者の操作範囲

2.6.2.2　ホストの識別・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。顧客のポリシーにより、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、ホストまたは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 機能による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またはホストを認証でき、または、これらのスイッチ・ホストにディスクサブシステムのポートを認証させることもできる。ホスト認証の設定は、全体ストレージ管理者または分割ストレージ管理者が LUN Manager を使用して、ホストの認証を行うかどうかを各ホストに設定する。認証を行うホストはユーザ情報(WWN、シークレット)を登録する。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。

2.6.2.3　Storage Navigator による利用者の認証・機能

Storage Navigator は、顧客の Storage Navigator 利用者によって、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 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、TOE によりユーザの識別と認証が行なわれる。Storage Navigator を使用する際、ユーザ ID、パスワードを使用した識別認証が実行される。

パスワードは 6 文字から 256 文字の英数字、記号の組み合わせを可能とし、入力したパスワードは*で表示する。また、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。

2.6.2.4　Storage Navigator －SVP 間の暗号化通信

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 と SVP 間の通信は SSL により暗号化する。

2.6.2.5　管理者の権限管理

Storage Navigator での認証に用いられるユーザアカウントには、ユーザ種別と操作権限の情報が含まれる。

ユーザ種別には、全体管理者と分割管理者の種別が存在する。全体管理者は USP V/USP VM 全体を管理できる種別であり、分割管理者は割り当てられた論理パーティションの管理を行うことができる種別である(論理パーティションは SLPR 番号によって識別される)。

操作権限はロールとも呼ばれ、ロールにはアカウント管理者ロール、監査ログ管理者ロール、ストレージ管理者ロールがある。アカウント管理者ロールは、アカウント管理機能を使用してユーザアカウントを表示、作成、変更または削除できる。アカウント作成時には、ユーザ種別、操作権限、SLPR 番号を付与する。全体管理者が分割管理者のユーザアカウント作成時は、分割管理者に割り当てる SLPR 番号を指定して作成する。分割管理者は割り当てられた SLPR 番号を変更することはできない。

監査ログ管理者ロールは、ユーザ種別が全体管理者に付与することができる操作権限で、監査ログの参照やダウンロード、および syslog に関する設定ができる。

ストレージ管理者ロールはストレージリソースの設定および管理を行うことができる。

また、操作権限の定義においては、各ユーザアカウントがどのような役割を持っているのかを定義する。アカウント管理者ロールと監査ログ管理者ロールには disable、view、modify の権限を定義できる。ストレージ管理者ロールにはプログラムプロダクトの機能毎に disable と enable の権限を定義できる。

全体管理者または分割管理者は次の役割を与えられる。

- アカウント管理者の役割としてユーザアカウントの新規作成、変更、削除ができる。
- アカウント管理者は、ストレージ管理者の権限を決定できる。
- アカウント管理者は、ユーザ種別により、全体アカウント管理者と、操作可能な範囲(論理パーティション)内でアカウント管理が可能な分割アカウント管理者の役割が存在する。
- 全体アカウント管理者は、ストレージ管理者の操作可能な範囲を決定できる。
- 分割アカウント管理者が設定したアカウント管理者、およびストレージ管理者には、操

作可能な範囲が継承される。

- ストレージ管理者の役割として、Storage Navigator を利用したディスクサブシステムの管理ができる。
- ストレージ管理者には、ユーザ種別により、全体ストレージ管理者と、操作可能な範囲内でストレージ管理が可能な分割ストレージ管理者の役割が存在する。
- 全体ストレージ管理者は、ストレージ装置全体で LDEV の生成、削除、LU パス情報を設定することができる。
- 分割ストレージ管理者は、操作可能な範囲内において、LDEV の生成、削除、LU パス情報を設定することができる。
- 監査ログ管理者の役割として監査ログをダウンロードし、監査ログを参照できる。

2.6.2.6　監査ログ

監査ログ機能は、Storage Navigator および DKCMAIN マイクロプログラムによって提供される。Storage Navigator 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 512 文字で、最大 250,000 行分の情報が SVP 内の HDD に格納される。Storage Navigator は監査ログを参照するインタフェースを提供する。

3　TOE セキュリティ環境

本章では、ST が意図している TOE の使用環境や使用方法、保護すべき資産とそれらに対する脅威、および TOE が従うべき組織のセキュリティ方針を定義する。

3.1　前提条件

A.NOEVIL　Storage　Navigator 利用者のうち、全体ストレージ管理者、全体アカウント管理者、監査ログ管理者は、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。
分割ストレージ管理者、分割アカウント管理者は、権限を持つ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.NOEVIL_MNT　保守員は、ホストと CHA 上のポートとの接続作業を含むストレージ装置の保守全般を安全に行うために十分な能力をもち、手順書で定められた通りの正しい保守作業を行い、不正行為をはたらかないことを信頼できるものと想定する。

A.PHYSICAL_SEC　ストレージ装置は、全体ストレージ管理者、全体アカウント管理者、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ているものと想定する。

A.ILLEGAL_SOFT　管理 PC には不正なソフトウェアがインストールされないものと想定する。

A.CONNECT_STORAGE　TOE は、他のストレージ装置を接続してストレージ装置間のデータコピーまたは、データのバックアップを取得する機能を持っている。この機能を使用すれば、他のストレージ装置から、TOE の保護対象資産であるユーザデータの変更および閲覧が可能である。これらの機能の操作は、信頼できるストレージ管理者しか操作できない運用を想定する。

3.2　脅威

TOE または IT 環境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 Storage Navigator 利用者、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、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。

また、攻撃者の攻撃能力は「低」であると想定している。

T.ILLEGAL_XCNTL	Storage Navigator 利用者のうち、分割ストレージ管理者、分割アカウント管理者が、自身の権限を越えた範囲のストレージ装置の設定変更を行うことにより、ホストがアクセスを許可されていない LDEV にアクセスできてしまうかもしれない。
T.TSF_COMP	第三者が、Storage Navigator－SVP 間の通信路に不正に機器を接続し、データの盗聴または、改ざんを行うかもしれない。
T.LP_LEAK	ホスト機器管理者等の第三者が、接続を許可されていないホストを SAN に接続して LDEV にアクセスにすることにより、データの漏えい、改ざんが行なわれるかもしれない。
T.CHG_CONFIG	第三者が、Storage Navigator を使用してストレージ装置の設定を変更してしまうかもしれない。

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の識別認証が求められる場合、FC-SP の識別認証が終了するまでは、当該ポートのアクセスは禁止されなければならない。

4　セキュリティ対策方針

本章では、TOE およびその環境に対するセキュリティ対策方針を定義する。

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、Storage Navigator 利用者がディスクサブシステムの管理操作を行う前に、Storage Navigator 利用者の識別認証が成功していなければならない。

O.ADM_ROLE　TOE は、Storage Navigator 利用者の行う管理操作を以下のように制限できなければならない。

- 全体アカウント管理者は、装置全体のアカウント管理操作が可能。
- 全体ストレージ管理者は、装置全体のストレージ管理操作が可能。
- 分割ストレージ管理者は、許可された論理パーティション内のストレージ管理操作が可能。
- 分割アカウント管理者は、許可された論理パーティション内のアカウント管理操作が可能。

O.SEC_COMM　TOE は、Storage Navigator－SVP 間の通信路から通信データの盗聴または改ざんを防止するため、Storage Navigator－SVP 間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.HOST_AUTH　TOE はホストからの接続要求があった際には、ホストの識別認証を行なわなければならない。

O.HOST_ACCESS　TOE は識別されたホストが、許可された LDEV のみにアクセスするように制御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できなければならない。

4.2　環境のセキュリティ対策方針

環境のセキュリティ対策方針を以下に示す。

OE.NOEVIL　Storage　Navigator 利用者のうち、全体ストレージ管理者、全体アカウント管理者、監査ログ管理者は、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が割り当てられなければならない。分割ストレージ管理者、分割アカウント管理者は、権限を持つ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.NOEVIL-MNT　保守員は、ホストと CHA 上のポートとの接続作業を含むストレージ装置の保守全般を安全に行うために十分な能力をもち、手順書で定められた通りの正しい保守作業を行い、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　ストレージ装置は、全体ストレージ管理者、全体アカウント管理者、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ていなければならない。

OE.ILLEGAL_SOFT　管理 PC には不正なソフトウェアがインストールされてはならない。

OE.CONNECT_STORAGE　他のストレージ装置へのデータのリモートコピーまたは、バックアップ操作は、信頼できるストレージ管理者以外が操作できないように、TOE と接続する他のストレージ装置は、TOE から構成されたストレージ装置に限定しなければならない。

5　IT セキュリティ要件

TOEに課されるセキュリティ要件はSTのこのセクションで指定される。セキュリティ機能要件は 5.1節で定義される。IT環境に課されるセキュリティ機能要件はない。

5.1　TOE セキュリティ要件

5.1.1　TOE セキュリティ機能要件

以下のコンポーネントは CC のパート 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 ：Storage Navigator の認証機能

b ：LUN Manager のアクセス制御機能

FIA_ATD.1a　　利用者属性定義

下位階層： 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[割付：*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*]：ユーザ種別、操作権限、SLPR 番号

依存性： なし

FIA_USB.1a　　利用者・サブジェクト結合

下位階層： なし

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： *利用者セキュリティ属性のリスト*]

FIA_USB.1.2a　　TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない： [割付： *属性の最初の関連付けに関する規則*]

FIA_USB.1.3a　　TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない： [割付： *属性の変更に関する規則*]

[割付： *利用者セキュリティ属性のリスト*]：ユーザ種別、操作権限、SLPR 番号

[割付： *属性の最初の関連付けに関する規則*]：なし

[割付： *属性の変更に関する規則*]：なし

依存性： FIA_ATD.1 利用者属性定義

FIA_ATD.1b　　利用者属性定義

下位階層： 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[割付： *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*]：WWN、LU 番号

依存性： なし

FIA_USB.1b　　利用者・サブジェクト結合

下位階層： なし

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： *利用者セキュリティ属性のリスト*]

FIA_USB.1.2b　　TSF は、利用者を代行して動作するサブジェクトと利用者セキュリティ属性の最初の関連付けに関する次の規則を実施しなければならない： [割付： *属性の最初の関連付けに関する規則*]

FIA_USB.1.3b　　TSF は、利用者を代行して動作するサブジェクトに関連付けた利用者セキュリティ属性の変更管理に関する次の規則を実施しなければならない： [割付： *属性の変更に関する規則*]

[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に関する規則*]：なし

[割付： *属性の変更に関する規則*]：なし

依存性： FIA_ATD.1 利用者属性定義

FIA_AFL.1　　認証失敗時の取り扱い

下位階層： なし

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に達するか上回ったとき、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 での認証

[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

[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。

依存性： FIA_UAU.1 認証のタイミング

FIA_SOS.1a　　秘密の検証

下位階層： 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 文字までの半角英大文字、半角英小文字、半角数字、以下の 32 種の半角記号!”#$%&’()*+,-./:;<=>?@[\]^_`{|}~

依存性： なし

FIA_UAU.2　　アクション前の利用者認証

下位階層： FIA_UAU.1

FIA_UAU.2.1　　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者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：利用者]：Storage Navigator 利用者、保守員

依存性： FIA_UID.1 識別のタイミング

FIA_UAU.7　　保護された認証フィードバック

下位階層： なし

FIA_UAU.7.1　　TSF は、認証を行っている間、[割付： *フィードバックのリスト*]だけを利用者に提供しなければならない。

[割付： *フィードバックのリスト*]：入力した文字数分「*(アスタリスク)」を表示

[詳細化：利用者]：Storage Navigator 利用者

依存性： FIA_UAU.1 認証のタイミング

FIA_UID.2　　アクション前の利用者識別

下位階層： FIA_UID.1

FIA_UID.2.1　　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者に自分自身を識別することを要求しなければならない。

[詳細化：利用者]：Storage Navigator 利用者、保守員または、ホスト

依存性： なし

FMT_MSA.1　　セキュリティ属性の管理

下位階層： なし

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*]に制限するために[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、論理パーティション情報、ユーザ権限情報

[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 5.1、表 5.2 の「LUパス情報に対する操作」、表 5.3の「論理パーティション情報に対する操作」、表 5.4、表 5.5の「ユーザ権限情報に対する操作」に記述する操作。

[割付： *許可された識別された役割*]：表 5.1、表 5.2、表 5.3、表 5.4、表 5.5、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 5.1 ホストを代行するプロセスのセキュリティ属性に対する全体管理者の操作

役割	LU パス情報に対する操作		
	WWN	LU 番号	LDEV 番号
全体ストレージ管理者	問い合わせ、改変、作成、削除	問い合わせ、作成、削除	問い合わせ、作成、削除
全体アカウント管理者	－	－	－
監査ログ管理者	－	－	－

－：操作なし

表 5.2 ホストを代行するプロセスのセキュリティ属性に対する分割管理者の操作

役割	LU パス情報に対する操作					
	論理パーティションの SLPR 番号＝n			論理パーティションの SLPR 番号≠n		
	WWN	LU 番号	LDEV 番号	WWN	LU 番号	LDEV 番号
分割ストレージ管理者 (自身の SLPR 番号＝n)	問い合わせ、改変、作成、削除	問い合わせ、作成、削除	問い合わせ、作成、削除	－	－	－

役割	LU パス情報に対する操作					
	論理パーティションの SLPR 番号＝n			論理パーティションの SLPR 番号≠n		
	WWN	LU 番号	LDEV 番号	WWN	LU 番号	LDEV 番号
分割アカウント管理者 (自身の SLPR 番号＝n)	－	－	－	－	－	－

－：操作なし

表 5.3 Storage Navigator を代行するプロセスのセキュリティ属性(論理パーティション情報)に対する操作

役割	論理パーティション情報に対する操作
	SLPR 番号
全体ストレージ管理者	問い合わせ、作成、削除
全体アカウント管理者	－
監査ログ管理者	－
分割ストレージ管理者	自身のアカウントの SLPR 番号と一致する論理パーティションの SLPR 番号に対する問い合わせ
分割アカウント管理者	－

－：操作なし

表 5.4 Storage Navigator を代行するプロセスのセキュリティ属性(ユーザ権限情報)に対する全体管理者の操作

役割	ユーザ権限情報に対する操作		
	ユーザ種別	操作権限	SLPR 番号
全体アカウント管理者	設定、 問い合わせ	設定、 問い合わせ、 改変	設定、 問い合わせ
全体ストレージ管理者	(自身の)問い合わせ	(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	(自身の)問い合わせ

表 5.5 Storage Navigator を代行するプロセスのセキュリティ属性(ユーザ権限情報)に対する分割管理者の操作

役割	ユーザ権限情報に対する操作					
	操作対象アカウントの SLPR 番号＝n			操作対象アカウントの SLPR 番号≠n		
	ユーザ種別	操作権限	SLPR 番号	ユーザ種別	操作権限	SLPR 番号
分割アカウント管理者 (自身の SLPR 番号＝n)	設定、 問い合わせ	設定、 問い合わせ、 改変	設定、 問い合わせ	－	－	－
分割ストレージ管理者 (自身の SLPR 番号＝n)	(自身の)問い合わせ	(自身の)問い合わせ	(自身の)問い合わせ	－	－	－

－：操作なし

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.3　　静的属性初期化

下位階層： なし

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 ： から一つのみ選択*、[割付 ： *その他の特性*]]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とき、[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指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 ： から一つのみ選択*]：制限的

[割付： *その他の特性*]：なし

[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*]：表 5.6の「役割」に記述する。

表 5.6 全体／分割ストレージ管理者の初期値指定範囲

役割	初期値を指定できる範囲
全体ストレージ管理者	ストレージ装置内の全ての LDEV に対して、LDEV 生成後に LU パス情報を設定できる。
分割ストレージ管理者 (自身の SLPR 番号＝n)	ストレージ装置内の論理パーティションの SLPR 番号＝n に関係付けられている LDEV に対して、LDEV 生成後に LU パス情報を設定できる。

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_MTD.1　　TSF データの管理

下位階層： なし

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*]： Storage Navigator 利用者のユーザ ID、パスワード
ホストの WWN、シークレット

[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 5.7、表 5.8の「ユーザアカウント」に対する操作、表 5.9のリモートデスクトップ接続のユーザ名、パスワードに対する操作、表 5.10、表 5.11の「ホスト識別認証データ」に対する操作。

[割付：*許可された識別された役割*]：表 5.7、表 5.10、表 5.8、表 5.11、表 5.9の「役割」に記述する役割。

表 5.7 ユーザアカウントに対する全体管理者の操作

役割	ユーザアカウント	
	Storage Navigator のユーザ ID	Storage Navigator のパスワード
全体アカウント管理者	問い合わせ、作成、削除	改変
全体ストレージ管理者	(自身の) 問い合わせ	(自身の) 改変
監査ログ管理者	(自身の) 問い合わせ	(自身の) 改変

表 5.8 ユーザアカウントに対する分割管理者の操作

役割	ユーザアカウント			
	操作対象アカウントの SLPR 番号＝n		操作対象アカウントの SLPR 番号≠n	
	Storage Navigator のユーザ ID	Storage Navigator のパスワード	Storage Navigator のユーザ ID	Storage Navigator のパスワード
分割アカウント管理者 (自身の SLPR 番号＝n)	問い合わせ、 作成、削除	改変	－	－
分割ストレージ管理者 (自身の SLPR 番号＝n)	(自身の) 問い合わせ	(自身の) 改変	－	－

－：操作なし

表 5.9 リモートデスクトップ接続のユーザ名、パスワードに対する操作

役割	リモートデスクトップ接続	
	ユーザ名	パスワード
保守員	問い合わせ、改変	改変

－：操作なし

表 5.10 ホスト識別認証データに対する全体管理者の操作

役割	ホスト識別認証データ	
	ホストの WWN	ホストの シークレット
全体ストレージ管理者	問い合わせ、 作成、改変、削除	作成、改変、削除
全体アカウント管理者	－	－
監査ログ管理者	－	－

－：操作なし

表 5.11 ホスト識別認証データに対する分割管理者の操作

役割	ホスト識別認証データ			
	論理パーティションの SLPR 番号＝n		論理パーティションの SLPR 番号≠n	
	ホストの WWN	ホストの シークレット	ホストの WWN	ホストの シークレット
分割ストレージ管理者 (自身の SLPR 番号＝n)	問い合わせ、作成、改変、削除	作成、改変、削除	－	－
分割アカウント管理者 (自身の SLPR 番号＝n)	－	－	－	－

－：操作なし

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_SMF.1　　管理機能の特定

下位階層： なし

FMT_SMF.1.1　　TSF は、以下のセキュリティ管理機能を行う能力を持たねばならない：[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]。

[割付：*TSF によって提供されるセキュリティ管理機能のリスト*]：表 5.12の「管理機能」に記述するセキュリティ管理機能。

表 5.12 TSF によって提供されるセキュリティ管理機能のリスト

機能要件	管理機能	管理項目
FIA_ATD.1a	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	a) なし。
FIA_USB.1a	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を変更できる。	a) なし。常に固定のユーザ種別、操作権限、SLPR 番号である。 b) なし。常に固定のユーザ種別、操作権限、SLPR 番号である。
FIA_ATD.1b	a) もし割付に示されていれば、許可管理者は利用者に対する追加のセキュリティ属性を定義することができる。	a) なし。
FIA_USB.1b	a) 許可管理者は、デフォルトのサブジェクトのセキュリティ属性を定義できる。 b) 許可管理者は、デフォルトのサブジェクトの	a) なし。常に固定の WWN、LU 番号である。 b) なし。常に固定の WWN、LU 番号である。

機能要件	管理機能	管理項目
	セキュリティ属性を変更できる。	
FIA_AFL.1	a) 不成功の認証試行に対する閾値の管理 b) 認証失敗の事象においてとられるアクションの管理	a) なし。常に固定の閾値である。 b) なし。常に固定のアクションである。
FIA_SOS.1a	a) 秘密の検証に使用される尺度の管理。	a) なし。常に固定の尺度である。
FIA_UAU.2	a) 管理者による認証データの管理; このデータに関係する利用者による認証データの管理。	a) 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。リモートデスクトップ接続のユーザ名に対するパスワードを管理する。
FIA_UAU.7	－	－
FIA_UID.2	a) 利用者識別情報の管理。	a) ユーザアカウントのユーザ ID、リモートデスクトップ接続のユーザ名、ホスト識別(ホストの WWN)を管理する。
FMT_MSA.1	a) セキュリティ属性と相互に影響を及ぼし得る役割のグループを管理すること。	a) なし。常に固定の役割である。
FMT_MSA.3	a) 初期値を特定できる役割のグループを管理すること; b) 所定のアクセス制御 SFP に対するデフォルト値の許可的あるいは制限的設定を管理すること。	a) なし。常に固定の役割である。 b) なし。常に固定である。
FMT_MTD.1	a) TSF データと相互に影響を及ぼし得る役割のグループを管理すること。	a) なし。常に固定の役割である。
FMT_SMF.1	－	－
FMT_SMR.1	a) 役割の一部をなす利用者のグループの管理。	a) ユーザアカウントのユーザ種別と操作権限を管理する。
FCS_COP.1	－	－
FCS_CKM.1	a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	a) なし。
FCS_CKM.2	a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	a) なし。
FCS_CKM.4	a) 暗号鍵属性の変更の管理。鍵の属性の例としては、鍵種別(例えば、公開、秘密、共通)、有効期間、用途(例えば、ディジタル署名、鍵暗号化、鍵交換、データ暗号化)などがある。	a) なし。
FIA_SOS.1b	a) 秘密の検証に使用される尺度の管理。	a) なし。常に固定の尺度である。

機能要件	管理機能	管理項目
FIA_UAU.1	a) 管理者による認証データの管理; b) 関係する利用者による認証データの管理 利用者が認証される前にとられるアクションのリストを管理すること。	a) Storage Navigator の FC-SP 機能でホストの認証データを管理する。 b) なし。
FIA_UAU.5	a) 認証メカニズムの管理; b) 認証に対する規則の管理	a) なし。常に固定のメカニズムである。 b) なし。常に固定の規則である。
FMT_MOF.1	a) TSF の機能と相互に影響を及ぼし得る役割のグループを管理すること;	a) なし。常に固定の役割である。
FDP_ACC.1	－	－
FDP_ACF.1	a) 明示的なアクセスまたは拒否に基づく決定に使われる属性の管理。	a) なし。明示的なアクセスまたは拒否はない。
FAU_GEN.1	－	－
FAU_GEN.2	－	－
FPT_STM.1	a) 時間の管理。	a) なし。 （TOE としては時間の管理を行わない。但し、OS の時間として管理を行う。）
FAU_SAR.1	a) 監査記録に対して読み出し権のある利用者グループの維持(削除、改変、追加)。	a) なし。常に固定の役割である。
FAU_STG.1	－	－
FAU_STG.3	a) 閾値の維持; b) 監査格納失敗が切迫したときにとられるアクションの維持(削除、改変、追加)。	a) なし。常に固定の閾値である。 b) なし。常に固定のアクションである。
FPT_RVM.1	－	－
FPT_SEP.1	－	－

－：該当なし

依存性： なし

FMT_SMR.1　　セキュリティ役割

下位階層： なし

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づけなければならない。

[割付： *許可された識別された役割*]：・全体アカウント管理者
・全体ストレージ管理者
・分割アカウント管理者
・分割ストレージ管理者
・監査ログ管理者
・保守員
・ストレージ利用者

依存性： FIA_UID.1 識別のタイミング

FCS_COP.1　　暗号操作

下位階層：なし

FCS_COP.1.1　　TSF は、[割付：*標準のリスト*]に合致する、特定された暗号アルゴリズム[割付：*暗号アルゴリズム*]と暗号鍵長[割付：*暗号鍵長*]に従って、[割付：*暗号操作のリスト*]を実行しなければならない。

[割付：*標準のリスト*]：表 5.13の「規格」に示す。

[割付：*暗号アルゴリズム*]：表 5.13の「アルゴリズム」に示す。

[割付：*暗号鍵長*]：表 5.13の「鍵長(bit)」に示す。

[割付：*暗号操作のリスト*]：表 5.13の「暗号操作」に示す。

表 5.13 暗号操作

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	サーバ認証
RSA Security Inc. Public-Key Cryptography Standards(PKCS)#1 v2.1	RSA	512 以上	認証	サーバ認証
			鍵交換	セッション鍵交換
FIPS PUB 197	AES	256 128	データの暗号化、および復号	[SSLv3.0] および [TLSv1.0]のハンドシェー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-1	160	ハッシュ	ハッシュ関数
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。

依存性：[FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または

FDP_ITC.2 セキュリティ属性付き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 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.1　　暗号鍵生成

下位階層：なし

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]：セッション鍵

[割付：*標準のリスト*]：表 5.14の「規格」に示す。

[割付：*暗号鍵生成アルゴリズム*]：表 5.14の「アルゴリズム」に示す。

[割付：*暗号鍵長*]：表 5.14の「鍵長(bit)」に示す。

表 5.14 セッション鍵の生成操作

規格	アルゴリズム	鍵長(bit)
[SSLv3.0] および[TLSv1.0]	ハンドシェークプロトコルによりセッション鍵を生成する。	128、160

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

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.2　　暗号鍵配付

下位階層：なし

FCS_CKM.2.1　TSF は、以下の[割付：*標準のリスト*]に合致する、指定された暗号鍵配付方法[割付：*暗号鍵配付方法*]に従って、暗号鍵を配付しなければならない。

[詳細化：暗号鍵]：セッション鍵

[割付：*標準のリスト*]： PKCS#1

[割付：*暗号鍵配付方法*]：RSA で暗号化して配布

依存性：[FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または

FDP_ITC.2 セキュリティ属性付き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 暗号鍵破棄

FMT_MSA.2 セキュアなセキュリティ属性

FCS_CKM.4　　暗号鍵破棄

下位階層：なし

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]：セッション鍵

[割付：*標準のリスト*]：なし

[割付：*暗号鍵破棄方法*]：Storage Navigator 利用者が Storage Navigator からログオフして SSL セッションを解放したときにメモリから消去

依存性：[FDP_ITC.1 セキュリティ属性なし利用者データのインポート

または

FDP_ITC.2 セキュリティ属性付き利用者データのインポート

または

FCS_CKM.1 暗号鍵生成]

FMT_MSA.2 セキュアなセキュリティ属性

FIA_SOS.1b　　秘密の検証

下位階層： 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.-+@_=:/[],~

依存性：なし

FIA_UAU.1　　認証のタイミング

下位階層：なし

FIA_UAU.1.1　　TSF は、利用者が認証される前に利用者を代行して行われる[割付：*TSF 調停アクションのリスト*]を許可しなければならない。

FIA_UAU.1.2　　TSF は、その利用者を代行する他の TSF 調停アクションを許可する前に、各利用者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：利用者]：ホスト

[割付：*TSF 調停アクションのリスト*]：FC-SP 機能の認証方式である、DH-CHAP 認証コード送信

依存性：FIA_UID.1 識別のタイミング

FIA_UAU.5　　複数の認証メカニズム

下位階層：なし

FIA_UAU.5.1　　TSF は、利用者認証をサポートするため、[割付：*複数の認証メカニズムのリスト*]を提供しなければならない。

FIA_UAU.5.2　　TSF は、[割付：*複数の認証メカニズムがどのように認証を提供するかを記述する規則*]に従って、利用者が主張する識別情報を認証しなければならない。

[割付：*複数の認証メカニズムのリスト*]：表 5.15の「認証メカニズム」に示す。

[割付：*複数の認証メカニズムがどのように認証を提供するかを記述する規則*]：表 5.15の「規則」に示す。

表 5.15 認証メカニズムと規則

認証対象	認証メカニズム	規則
Storage Navigator 利用者	パスワードメカニズム	Storage Navigator 利用者が入力したパスワードと TOE が保持するパスワードが一致することを確認する。
保守員	パスワードメカニズム	保守員が入力したリモートデスクトップ接続のパスワードと TOE が保持するパスワードが一致することを確認する。
ホスト(FC-SP 認証動作中)	FC-SP 認証メカニズム	ホストから受信したシークレットと TOE が保持するシークレットが一致することを確認する。

依存性：なし

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

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 5.16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 5.16の「役割」に示す。

表 5.16 役割に操作を制限する機能のリスト

項番	役割	機能
1	全体ストレージ管理者	FC-SP 識別認証機能
2	分割ストレージ管理者	分割ストレージ管理者自身のセキュリティ属性である SLPR 番号と、論理パーティションの SLPR 番号が一致する範囲内での FC-SP 識別認証機能
3	保守員	FC-SP 識別認証機能

依存性：FMT_SMF.1 管理機能の特定

FMT_SMR.1 セキュリティ役割

FDP_ACC.1　　サブセットアクセス制御

下位階層： なし

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：ホストを代行するプロセス、Storage Navigator を代行するプロセス

オブジェクト：LDEV、SLPR

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

：LDEV へのアクセス、LDEV の生成と削除、SLPR の生成と削除

[割付： *アクセス制御 SFP*]： LM アクセス制御 SFP

依存性： FDP_ACF.1 セキュリティ属性によるアクセス制御

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

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、以下の追加規則に基づいて、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承認しなければならない： [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承認する規則*]。

FDP_ACF.1.4　TSF は、[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 を代行するプロセス

オブジェクト：LDEV、SLPR

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 5.17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 5.17 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
ホスト代行プロセス	WWN、LU 番号	LU パス情報(WWN、LU 番号、LDEV 番号)
Storage Navigator 代行プロセス	ユーザ権限情報（ユーザ種別、操作権限、SLPR 番号）	LDEV 生成：論理パーティション情報(SLPR 番号) LDEV 削除：LU パス情報(WWN、LU 番号、LDEV 番号)および、論理パーティション情報(SLPR 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 5.18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承認する規則*]：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 5.18 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	ホストを代行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
Storage Navigator を代行するプロセス	Storage Navigator 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) ユーザ種別が全体管理者、操作権限がストレージ管理者の場合 SLPR の生成、削除を許可する。	SLPR
	Storage Navigator 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) ユーザ種別が全体管理者、操作権限がストレージ管理者の場合 全ての LDEV の生成を許可する。 LDEV に関係付いた LU パス情報が存在しないとき、当該 LDEV の削除を許可する。 2) ユーザ種別が分割管理者、操作権限がストレージ管理者の場合 分割ストレージ管理者の SLPR 番号と、LDEV に関係付ける論理パーティションの SLPR 番号が一致しているとき LDEV の生成を許可する。 分割ストレージ管理者の SLPR 番号と LDEV に関係付けられた SLPR 番号が一致し、LDEV に関係付いた LU パス情報が存在しないときに、当該 LDEV の削除を許可する。	LDEV

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

FAU_GEN.1　　監査データ生成

下位階層： なし

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 5.19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 5.19 個別に定義した監査対象事象

機能要件	監査項目
FIA_ATD.1a	なし。
FIA_USB.1a	なし。
FIA_ATD.1b	なし。
FIA_USB.1b	なし。
FIA_AFL.1	なし。認証試行の閾値到達時はログに記録しない。
FIA_SOS.1a	なし。尺度の不一致はログに記録しない。
FIA_UAU.2	・ Storage Navigator 利用者の識別認証の成功または失敗をログに取得。
FIA_UAU.7	なし。
FIA_UID.2	・ Storage Navigator の識別認証の成功または失敗をログに取得。
FMT_MSA.1	・ LU パス情報の作成、削除、変更をログに取得。 ・ ユーザアカウントの操作権限の変更をログに取得。
FMT_MSA.3	なし。

機能要件	監査項目
FMT_MTD.1	・ 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。 ・ ホストの WWN、シークレットの作成、変更、削除をログに取得。
FMT_SMF.1	・ 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、操作権限の変更をログに取得。 ・ ホストの WWN、シークレットの作成、変更、削除をログに取得。
FMT_SMR.1	・ ユーザアカウントの操作権限の変更をログに取得。
FCS_COP.1	なし。
FCS_CKM.1	なし。
FCS_CKM.2	なし。
FCS_CKM.4	なし。
FIA_SOS.1b	なし。尺度の不一致はログに記録しない。
FIA_UAU.1	・ FC-SP によるホストの識別認証の結果をログに取得。
FIA_UAU.5	・ Storage Navigator 利用者の識別認証の成功または失敗をログに取得。
FMT_MOF.1	・ FC-SP によるホストの識別認証有無の設定変更をログに取得。
FDP_ACC.1	なし。
FDP_ACF.1	なし。
FAU_GEN.1	なし。
FAU_GEN.2	なし。
FPT_STM.1	なし。
FAU_SAR.1	なし。
FAU_STG.1	なし。
FAU_STG.3	なし。
FPT_RVM.1	なし。
FPT_SEP.1	なし。

依存性： FPT_STM.1 高信頼タイムスタンプ

FAU_GEN.2　　利用者識別情報の関連付け

下位階層: なし

FAU_GEN.2.1　　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。

依存性：FAU_GEN.1 監査データ生成

FIA_UID.1 識別のタイミング

FPT_STM.1　　高信頼タイムスタンプ

下位階層： なし

FPT_STM.1.1　　TSF は、それ自身の使用のために、高信頼タイムスタンプを提供できなければならない。

依存性： なし

FAU_SAR.1　　監査レビュー

下位階層： なし

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 5.20の「監査情報」に記述する。

表 5.20 監査情報

監査事象	監査情報
Storage Navigator 利用者の識別認証	・ Storage Navigator 利用者の識別認証の成功または失敗、識別認証実施日時、Storage Navigator のユーザ ID、Storage Navigator 動作 PC の IP アドレス
Storage Navigator 利用者のユーザアカウントの作成、変更、削除	・ ユーザアカウントのユーザ ID の作成、削除、パスワードの変更を実施した Storage Navigator のユーザ ID、操作対象のユーザ ID、操作内容（作成、変更、削除）、操作結果（成功、失敗）
Storage Navigator 利用者のユーザアカウントの操作権限変更	・ ユーザアカウントの操作権限の変更を実施した Storage Navigator のユーザ ID、操作対象のユーザ ID、操作権限、操作内容（変更）、操作結果（成功、失敗）
LU パス情報の作成、削除、変更	・ LU パス情報の作成、削除、変更を実施した Storage Navigator のユーザ ID、操作内容（作成、削除、変更）、WWN、LU 番号、LDEV 番号、操作結果（成功、失敗）
ホストの WWN、シークレットの追加、変更、削除	・ ホストの WWN、シークレットの作成、変更、削除を実施した Storage Navigator のユーザ ID、ホストの WWN、操作内容（作成、変更、削除）、操作結果（成功、失敗）
FC-SP によるホストの識別認証有無の設定変更	・ FC-SP によるホストの識別認証有無の変更を実施した Storage Navigator のユーザ ID、ホストの WWN、識別認証有無、操作内容（変更）、操作結果（成功、失敗）

依存性： FAU_GEN.1 監査データ生成

FAU_STG.1　　保護された監査証跡格納

下位階層： なし

FAU_STG.1.1　　TSF は、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、監査証跡内の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

依存性： FAU_GEN.1 監査データ生成

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

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 画面で警告

依存性： FAU_STG.1 保護された監査証跡格納

FPT_RVM.1　　TSP の非バイパス性

下位階層: なし

FPT_RVM.1.1　　TSF は、TSC 内の各機能の動作進行が許可される前に、TSP 実施機能が呼び出され成功することを保証しなければならない。

依存性：なし

FPT_SEP.1　　TSF ドメイン分離

下位階層: なし

FPT_SEP.1.1　　TSF は、それ自身の実行のため、信頼できないサブジェクトによる干渉や改ざんからそれを保護するためのセキュリティドメインを維持しなければならない。

FPT_SEP.1.2　　TSF は、TSC 内でサブジェクトのセキュリティドメイン間の分離を実施しなければならない。

依存性：なし

5.1.2　最小機能強度レベル

本 TOE の最小機能強度レベルは、SOF-基本である。

確率的または順列的メカニズムを利用する TOE セキュリティ機能要件は、上述の FIA_SOS.1a、FIA_UAU.2、FIA_UAU.7、FIA_UID.2、FCS_COP.1、FCS_CKM.1、FIA_SOS.1b、FIA_UAU.1、FIA_UAU.5 である。

5.1.3　TOE セキュリティ保証要件

TOE セキュリティ保証要件は、EAL2 に含まれる以下のものである。

表 5.21 TOE セキュリティ保証要件

セキュリティ保証要件	
ACM_CAP.2	構成要素
ADO_DEL.1	配付手続き
ADO_IGS.1	設置、生成、及び立上げ手順
ADV_FSP.1	非形式的機能仕様
ADV_HLD.1	記述的上位レベル設計
ADV_RCR.1	非形式的対応の実証
AGD_ADM.1	管理者ガイダンス
AGD_USR.1	利用者ガイダンス
ATE_COV.1	カバレージの証拠
ATE_FUN.1	機能テスト
ATE_IND.2	独立試験 – サンプル
AVA_SOF.1	TOE セキュリティ機能強度評価
AVA_VLA.1	開発者脆弱性分析

5.2　IT 環境に対するセキュリティ要件

TOE が IT 環境に依存するセキュリティ要件はない。

6　TOE 要約仕様

本章では、TOE セキュリティ要件を満たす TOE のセキュリティ機能および保証手段を記述する。

6.1　TOE セキュリティ機能

表 6.1に TOEセキュリティ機能とセキュリティ機能要件の対応を示す。

表 6.1 TOE セキュリティ機能とセキュリティ機能要件の対応

		TOE の IT セキュリティ機能				
		SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.AUDIT**
TOEセキュリティ機能要件	FIA_ATD.1a	X				
	FIA_USB.1a	X				
	FIA_ATD.1b	X				
	FIA_USB.1b	X				
	FIA_AFL.1			X		
	FIA_SOS.1a			X		
	FIA_UAU.2			X	X	
	FIA_UAU.7			X		
	FIA_UID.2		X	X	X	
	FMT_MSA.1				X	
	FMT_MSA.3	X				
	FMT_MTD.1				X	
	FMT_SMF.1				X	
	FMT_SMR.1				X	
	FCS_COP.1			X		
	FCS_CKM.1			X		
	FCS_CKM.2			X		
	FCS_CKM.4			X		
	FIA_SOS.1b		X			

	TOE の IT セキュリティ機能				
	SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.AUDIT**
FIA_UAU.1		X			
FIA_UAU.5		X	X	X	
FMT_MOF.1				X	
FDP_ACC.1	X				
FDP_ACF.1	X				
FAU_GEN.1					X
FAU_GEN.2					X
FPT_STM.1					X
FAU_SAR.1					X
FAU_STG.1					X
FAU_STG.3					X
FPT_RVM.1	X	X	X	X	X
FPT_SEP.1	X	X	X	X	X

6.1.1　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、ホストがストレージ装置内の LDEV 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、FDP_ACC.1、FDP_ACF.1、FPT_RVM.1、FPT_SEP.1

TOE は、Storage Navigator の属性情報（ユーザ種別、操作権限、SLPR 番号）を維持し、その属性を Storage Navigator のユーザアカウントに関連付ける。(FIA_ATD.1a、FIA_USB.1a)

TOE は、ホストの属性情報（WWN、LU 番号）を維持し、その属性をホストに関連付ける。(FIA_ATD.1b、FIA_USB.1b)

TOE は、ホストを代行するプロセスが LDEV へのアクセスを行うとき、および Storage Navigator を代行するプロセスが LDEV 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 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 を代行するプロセスが SLPR を生成、または削除する場合、Storage Navigator を代行するプロセスに渡された、「Storage Navigator のユーザ権限情報」（Storage Navigator のユーザ種別、操作権限、SLPR 番号）により、全体ストレージ管理者のみが SLPR を作成、または削除できる。

- Storage Navigator を代行するプロセスが LDEV を生成、または削除する場合、Storage Navigator を代行するプロセスに渡された、「Storage Navigator のユーザ権限情報」（Storage Navigator のユーザ種別、操作権限、SLPR 番号）により、全体ストレージ管理者は全ての LDEV を生成、または削除できる。分割ストレージ管理者は、分割ストレージ管理者のセキュリティ属性である SLPR 番号と、論理パーティションの SLPR 番号が一致するとき、当該論理パーティション内に LDEV を生成、または削除できる。

- LDEV を削除する際の条件：削除対象の LDEV に関係付いた LU パス情報が存在しないときに当該 LDEV を削除する。

- LDEV 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 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)

TOE は、TOE の機能が実行される際に、かならず「LM アクセス制御 SFP」が適用されることを保証する。また、SF.LM に関する TSF は自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらないことを保証する。(FPT_RVM.1、FPT_SEP.1)

6.1.2　SF.FCSP

TOE は、顧客のセキュリティポリシーにより必要な場合は、FC-SP により、ホストの識別認証を行う。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_UID.2、FIA_SOS.1b、 FIA_UAU.1、FIA_UAU.5、FPT_RVM.1、FPT_SEP.1

TOE は、FC-SP によるホストの識別認証を WWN、シークレットにて行い、ホストからのアクセスに関する他のセキュリティ機能の動作前に実施する。(FIA_UID.2、FIA_UAU.1)

TOE は、ホスト識別認証が有りの場合は、ホストからセキュリティ認証実施のコマンドを受信したときに、DH-CHAP 認証コードを生成し、ホストに送信する(FIA_UAU.1)。ホストから受信したシークレットと TOE が保持するシークレットが一致したときに、ホストとストレージ装置との接続を許可する (FIA_UAU.5)。

TOE は、FC-SP によるホストの識別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)

TOE は、ホストの識別認証が行われる場合、ホストがストレージ装置に接続する際に SF.FCSP を呼び出し、ホストの識別認証が行われることを保証する。また、SF.FCSP に関する TSF は自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらないことを保証する。(FPT_RVM.1、FPT_SEP.1)

6.1.3　SF.SN

【満たしている要件】FIA_AFL.1 、FIA_SOS.1a、FIA_UID.2、FIA_UAU.2、FIA_UAU.5、FIA_UAU.7、FCS_COP.1、FCS_CKM.1、FCS_CKM.2、FCS_CKM.4、FPT_RVM.1、FPT_SEP.1

TOE は、Storage Navigator 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_UAU.5、FIA_AFL.1)

TOE は、Storage Navigator での識別認証時に使用するパスワードの入力を 6 文字以上 256 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!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ に制限し、入力時は「*」表示とする。(FIA_SOS.1a、FIA_UAU.7)

TOEは、Storage NavigatorとSVP間の通信にSSLを使用し、TSFデータを暗号化することで、TSFデータの盗聴、改ざんを防止する。SSLは、公開鍵暗号方式によるサーバ、クライアント間認証、共通鍵暗号方式によるデータの暗号化、ハッシュ関数によるデータの同一性確保を提供する。SSLで使用する 暗号操作を 表 5.13に示す。暗号化アルゴリズムと鍵長はStorage Navigator－SVP間のネゴシエーションにより決定し、鍵は使用後にメモリから消去する。サポートするSSLのバージョンは、SSLバージョン 3.0 およびTLSバージョン 1.0 である。(FCS_COP.1、FCS_CKM.1、FCS_CKM.2、FCS_CKM.4)

TOE は Storage Navigator 利用者が Storage Navigator を使用してストレージ装置の管理操作を行う前に SF.SN を呼び出し、SSL による暗号化通信と Storage Navigator 利用者の識別認証が行われることを保証する。また、SF.SN に関する TSF は自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらないことを保証する。(FPT_RVM.1、FPT_SEP.1)

6.1.4　SF.ROLE

【満たしている要件】FMT_MSA.1 、FMT_MSA.3、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1 、FMT_MOF.1、FIA_UID.2、FIA_UAU.2、FIA_UAU.5、FPT_RVM.1、FPT_SEP.1

TOE は、Storage Navigator 利用者を代行するプロセスの SVP 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（WWN、LU番号、LDEV番号）の作成、改変、削除、参照の操作をユーザ種別、操作権限、SLPR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 5.1、表 5.2に示す。

- 「LMアクセス制御SFP」は、論理パーティション情報（SLPR番号）の作成、削除、参照の操作をユーザ種別、操作権限、SLPR番号に基づき制限する。(FMT_MSA.1) 論理パーティション情報に対して、各役割が実施できる操作を 表 5.3に示す。

- 「LMアクセス制御SFP」は、Storage Navigatorのユーザ権限情報（ユーザ種別、操作権限、SLPR番号）の設定、改変、参照の操作をユーザ種別、操作権限に基づき制限する。(FMT_MSA.1) ユーザ権限情報に対して、各役割が実施できる操作を 表 5.4、表 5.5に示す。

TOE は、以下の管理機能を有する。(FMT_MTD.1、FMT_SMF.1)

- Storage Navigatorのアカウント管理機能でユーザアカウントのユーザID、パスワード、ユーザ種別、操作権限、SLPR番号を管理する。各役割が実施できる管理操作をに 表 5.7、表 5.8

に示し、管理項目を 表 5.12示す。

・ 保守員がリモートデスクトップ接続を行うときのユーザ名とパスワードを管理する。リモートデスクトップ接続のユーザ名とパスワードに対する操作を 表 5.9に示し、管理項目を 表 5.12示す。

・ Storage NavigatorのFC-SP機能でホスト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に 表 5.10、表 5.11に示し、管理項目を 表 5.12示す。

TOEは、FC-SPによるホスト識別認証の有無(認証あり、認証なし)の設定操作を、ユーザ種別、操作権限に基づき制限する。各役割が実施できる操作を 表 5.16に示す(FMT_MOF.1)。

TOE は、役割（全体アカウント管理者、全体ストレージ管理者、分割アカウント管理者、分割ストレージ管理者、監査ログ管理者、保守員、ストレージ利用者）を維持する。(FMT_SMR.1)

TOE は、保守員が SVP に接続するときは、リモートデスクトップ接続のユーザ名とパスワードで保守員の識別認証を行う。(FIA_UID.2、FIA_UAU.2、FIA_UAU.5)

TOE は Storage Navigator 利用者が管理操作を行う際には SF.ROLE を呼び出し、Storage Navigator 利用者のユーザ種別と操作権限により、権限範囲外の管理操作が行われないことを保証する。また、SF.ROLE に関する TSF は自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらないことを保証する。(FPT_RVM.1、FPT_SEP.1)

6.1.5　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、FPT_RVM.1、FPT_SEP.1

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 5.20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 画面に超過した旨を通知し、ユーザ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。

TOE は、セキュリティ関連事象が発生した場合は、SF.AUDIT を呼び出し、監査記録が生成されることを保証する。また、SF.AUDIT に関する TSF は自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらないことを保証する。(FPT_RVM.1、FPT_SEP.1)

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 6.2 に示し、詳細情報の出力内容を 表 6.3に示す。

表 6.2 基本情報の出力内容

項番	項目	取得内容
1	ログインユーザ ID	Storage Navigator のユーザ ID を出力する。
2	SLPR 番号	ログインしたユーザ ID の SLPR 番号を出力する。
3	日付	事象発生日付を出力する。
4	時刻	事象発生時刻を出力する。
5	タイムゾーン	GMT（Greenwich Mean Time）との時差を出力する。
6	機能名	設定操作を実行した機能名を出力する。
7	操作名または事象名	機能毎の操作名称を略称で出力する。
8	パラメタ	実行した設定操作のパラメタを出力する。
9	操作の結果	操作結果を出力する。
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 6.3 詳細情報の出力内容

項番	監査事象	詳細情報
1	Storage Navigator 利用者の識別認証	・ Storage Navigator 動作 PC の IP アドレス
2	Storage Navigator 利用者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、操作内容（作成、変更、削除）、操作結果（成功、失敗）
3	Storage Navigator 利用者のユーザアカウントの操作権限変更	・ 操作対象のユーザ ID、操作権限、操作内容（変更）、操作結果（成功、失敗）
4	LU パス情報の作成、削除、変更	・ 操作内容（作成、削除、変更）、WWN、LU 番号、LDEV 番号、操作結果（成功、失敗）
5	ホストの WWN、シークレットの追加、変更、削除	・ ホストの WWN、操作内容（作成、変更、削除）、操作結果（成功、失敗）
7	FC-SP によるホストの識別認証有無の設定変更	・ ホストの WWN、識別認証有無、操作内容（変更）、操作結果（成功、失敗）

6.2 セキュリティ機能強度

本 TOE において、セキュリティ機能強度の対象となる順列的、確率的メカニズムを有するセキュリティ機能は、SF.FCSP、SF.SN である。これらセキュリティ機能のパスワード、シークレットに関する機能および SSL のセッション鍵生成に関する機能が機能強度レベル SOF-基本を持つ。

6.3 保証手段

以下に、セキュリティ保証要件を満たす文書の参照を示すことによって保証手段を定義する。

次の表のドキュメント名は評価の過程で新しいタイトル、バージョン番号に更新予定。

表 6.4 セキュリティ保証と保証手段

セキュリティ保証要件	保証手段
ACM_CAP.2　構成要素	・HITACHI USP V マイクロプログラム構成管理リスト ・DKCMAIN/SVP バージョンの付与方法
ADO_DEL.1　配付手続き	・HITACHI USP V 配付手順説明書
ADO_IGS.1　設置、生成、及び立上げ手順	[Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform H24000] ・A/H-65AA, A-65BA, HT-40BA ディスクサブシステム　メンテナンスマニュアル Rev.1.3 [Hitachi Universal Storage Platform VM / Hitachi Universal Storage Platform H20000] ・A/H-65AA, A-65BA, HT-40BA ディスクサブシステム　メンテナンスマニュアル [Hitachi Universal Storage Platform V] ・DKC610I Maintenance Manual Rev.1.3 [Hitachi Universal Storage Platform VM] ・DKC615I　Maintenance Manual
ADV_FSP.1　非形式的機能仕様	・Hitachi Universal Storage Platform V 機能仕様書
ADV_HLD.1　記述的上位レベル設計	・Hitachi Universal Storage Platform V 上位レベル設計書
ADV_RCR.1　非形式的対応の実証	・Hitachi Universal Storage Platform V 表現対応分析書
AGD_ADM.1　管理者ガイダンス	・Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM / Hitachi Universal Storage Platform H24000 / Hitachi Universal Storage Platform H20000

セキュリティ保証要件	保証手段
	ISO15408 認証取得機能　取扱説明書 ・Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM ISO15408 Certification Instructions Manual
AGD_USR.1　利用者ガイダンス	・Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM / Hitachi Universal Storage Platform H24000 / Hitachi Universal Storage Platform H20000 利用者ガイダンス ・Hitachi Universal Storage Platform V / Hitachi Universal Storage Platform VM User Guidance
ATE_COV.1　カバレージの証拠	・HITACHI Universal Storage Platform V テスト分析書
ATE_FUN.1　機能テスト	・HITACHI Universal Storage Platform V テスト仕様書
ATE_IND.2　独立試験 – サンプル	・TOE
AVA_SOF.1　TOE セキュリティ機能 強度評価	・HITACHI Universal Storage Platform V 機能強度分析書
AVA_VLA.1　開発者脆弱性分析	・HITACHI Universal Storage Platform V 脆弱性分析書

7　PP 主張

本 ST は、いかなる PP への適合も主張しない。

8　根拠

本章は、主に ST を評価する際に用いられる証拠を提示する。

8.1　セキュリティ対策方針根拠

本章では、セキュリティ対策方針が TOE セキュリティ環境において識別されたすべての側面をカバーするのに適していることを説明する。

表 8.1は、本STに記述されたセキュリティ対策方針が前提条件、脅威、組織のセキュリティ方針にまでたどれることを示している。

表 8.1 TOE セキュリティ環境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.HOST_AUTH	O.HOST_ACCESS	O.AUD_GEN	OE.NOEVIL	OE.NOEVIL-MNT	OE.PHYSICAL_SEC	OE.ILLEGAL_SOFT	OE.CONNECT_STORAGE
TOEセキュリティ環境	A.NOEVIL							X				
	A.NOEVIL_MNT								X			
	A.PHYSICAL_SEC									X		
	A.ILLEGAL_SOFT										X	
	A.CONNECT_STORAGE											X
	T.ILLEGAL_XCNTL	X	X				X					
	T.TSF_COMP			X								
	T.LP_LEAK					X						
	T.CHG_CONFIG	X					X					
	P.MASQ				X							

8.1.1　前提条件に対するセキュリティ対策方針の根拠

表 8.2は、セキュリティ対策方針によって前提条件がカバーされていることを示している。

表 8.2 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、ストレージ装置全体の管理・運用を行うために、全体ストレージ管理者、全体アカウント管理者、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、分割ストレージ管理者、分割アカウント管理者に信頼できる人物を割り当てることによって実現される。
A.NOEVIL_MNT	A.NOEVIL_MNT は、OE.NOEVIL_MNT にあるように、保守員に信頼できる人物を割り当てることによって実現される。
A.PHYSICAL_SEC	A.PHYSICAL_SEC は、OE.PHYSICAL_SEC にあるように、ストレージ装置は、全体ストレージ管理者、全体アカウント管理者、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。
A.ILLEGAL_SOFT	A.ILLEGAL_SOFT は、OE.ILLEGAL_SOFT にあるように、管理 PC に不正なソフトウェアがインストールされないことによって実現される。
A.CONNECT_STORAGE	A.CONNECT_STORAGE は、OE.CONNECT_STORAGE にあるように、他のストレージ装置へのリモートコピーまたは、バックアップ操作では、TOE の保護対象資産を変更、閲覧ができるため、接続する他のストレージ装置は TOE から構成されるストレージ装置に限定することで、リモートコピーやバックアップ操作を信頼できるストレージ管理者のみに許可できるため、前提条件を満たす運用が実現できる。

8.1.2　脅威に対するセキュリティ対策方針の根拠

表 8.3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 8.3 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.ILLEGAL_XCNTL	T.ILLEGAL_XCNTL 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。 ・ TOE は、Storage Navigator 利用者を識別認証し、Storage Navigator 利用者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。 ➢ 全体アカウント管理者は、装置全体のアカウント管理操作が可能。 ➢ 全体ストレージ管理者は、装置全体のストレージ管理操作が可能。 ➢ 分割ストレージ管理者は、許可された論理パーティション内のストレージ管理操作が可能。 ➢ 分割アカウント管理者は、許可された論理パーティション内のアカウント管理操作が可能。 ・ TOE はセキュリティに関係する設定変更の操作時のセキュリティ事象を追跡できる要件により、不正操作が行われたかどうかを追跡できるため、脅威は軽減される。
T.TSF_COMP	T.TSF_COMP は、下記に示す通り、O.SEC_COMM によって対抗される。 ・ Storage Navigator－SVP 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および、改ざんの脅威を軽減できるからである。
T.LP_LEAK	T.LP_LEAK は、下記に示す通り、O.HOST_ACCESS によって対抗される。 ・ TOE は、LU パス情報により、許可された識別されたホストが、許可された LDEV のみにアクセスできるように制御するため、脅威は除去される。
T.CHG_CONFIG	T.CHG_CONFIG は、下記に示す通り、O.ADM_AUTH および O.AUD_GEN によって対抗される。 ・ TOE は、Storage Navigator の利用者を、仮想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、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。

8.1.3　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 8.4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 8.4 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.MASQ は、下記に示す通り、O.HOST_AUTH によって実現される。 ・ TOE はホストから当該ポートにアクセスされる前に FC-SP によりホストの識別認証を行う。

8.2　セキュリティ要件根拠

本章では、セキュリティ要件のセットがセキュリティ対策方針を満たすのに適していることを説明する。

8.2.1　セキュリティ機能要件根拠

表 8.5は、本STに記述されたセキュリティ機能要件が対策方針にまでたどれることを示している。

表 8.5 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 のセキュリティ対策方針					
		O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O.AUD_GEN
TOEセキュリティ機能要件	FIA_ATD.1a	X					
	FIA_USB.1a	X					
	FIA_ATD.1b					X	
	FIA_USB.1b					X	
	FIA_AFL.1	X					
	FIA_SOS.1a	X					
	FIA_UAU.2	X					
	FIA_UAU.7	X					
	FIA_UID.2	X			X		
	FMT_MSA.1		X				
	FMT_MSA.3		X				
	FMT_MTD.1		X				
	FMT_SMF.1		X				
	FMT_SMR.1		X				
	FCS_COP.1			X			
	FCS_CKM.1			X			
	FCS_CKM.2			X			
	FCS_CKM.4			X			
	FIA_SOS.1b				X		

	TOE のセキュリティ対策方針					
	O.ADM_AUTH	O.ADM_ROLE	O.SEC_COMM	O.HOST_AUTH	O.HOST_ACCESS	O.AUD_GEN
FIA_UAU.1				X		
FIA_UAU.5	X			X		
FMT_MOF.1		X				
FDP_ACC.1		X			X	
FDP_ACF.1		X			X	
FAU_GEN.1						X
FAU_GEN.2						X
FPT_STM.1						X
FAU_SAR.1						X
FAU_STG.1						X
FAU_STG.3						X
FPT_RVM.1	X	X	X	X	X	X
FPT_SEP.1	X	X	X	X	X	X

表 8.6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 8.6 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	O.ADM_AUTH では、Storage Navigator 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。 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。 a. Storage Navigator の利用者の維持を行う。 TOE は Storage Navigator 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 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。

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
	b. TOE 利用前に Storage Navigator のユーザアカウントの識別認証を行う。 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 の全ての機能動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、FIA_UAU.5 である。 c. パスワードの管理を行う。 TOE がユーザアカウントを識別するためのパスワードは、6 文字から 256 文字までの半角英大文字、半角英小文字、半角数字、半角記号の組み合わせを入力可能とし、入力したパスワードは*(アスタリスク)に置き換えて表示している。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、FIA_UAU.7 である。 d. 識別認証を確実に実施する。 Storage Navigator の識別認証を行うためには、Storage Navigator の利用者が操作を開始する際に識別認証機能が必ず呼び出される必要がある。また、その仕組みが干渉・改ざんされることから保護しなければならない。さらに、信頼できないサブジェクトにより干渉・改ざんされることを、TSF が自己防衛的に保護する必要がある。この要件に該当するセキュリティ機能要件は、FPT_RVM.1 および FPT_SEP.1 である。 以上 a、b、c、d の対策を満たすことにより、O.ADM_AUTH を満足できる。 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_UAU.5、 FIA_UAU.7、FIA_UID.2、FPT_RVM.1、FPT_SEP.1 の達成により、O.ADM_AUTH を実現できる。
O.ADM_ROLE	O.ADM_ROLE では、認証されたユーザ ID のユーザ種別および操作権限に基づいて、Storage Navigator 利用者の管理操作を制限できることを要求している。 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。 a. ユーザ種別、操作権限、SLPR 番号の操作を制限する。 TOE はユーザアカウントのユーザ種別、操作権限に応じて、ユーザアカウントのユーザ種別、操作権限、SLPR 番号の設定、変更と SLPR 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。 b. 識別認証情報を管理する。 TOE はユーザアカウントのユーザ種別、操作権限に応じて、ユーザアカウントのユーザ ID、パスワードおよびホストの WWN、シークレットの変更を制御する必要がある。これにより、ユーザアカウントのユーザ ID、パスワードおよびホストの 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

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
	当するセキュリティ機能要件は FMT_MTD.1 である。 c. 管理機能を保有する。 TOE は Storage Navigator のユーザアカウント、ホストの識別認証情報、WWN の識別情報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。 d. 役割を維持する。 TOE は全体アカウント管理者、全体ストレージ管理者、分割アカウント管理者、分割ストレージ管理者、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、利用者と関連付ける必要がある。この要件に該当するセキュリティ機能要件は FMT_SMR.1 である。ただし、保守員は識別認証を実施しなくてもよい。なぜなら、ストレージ装置は、セキュアなエリアに設置され、保守員には信頼される人物が割り当てられているからである。 e. ホストの識別認証操作の管理を行う。 TOE はユーザアカウントのユーザ種別、操作権限に応じて、ホストの識別認証有無の変更を制御する必要がある。これにより、ホストの識別認証有無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。 f. アクセス制御を規定し、実施する。 TOE は Storage Navigator 利用者に対して、「LM アクセス制御 SFP」として定義された規則に従って SLPR の作成、削除および LDEV の生成、削除を行う必要がある。これにより、分割ストレージ管理者は割り当てられた SLPR 内の LDEV 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 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 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。 g. LM アクセス制御 SFP を確実に実施する。 TOE は Storage Navigator のユーザアカウントの操作権限の操作、SLPR の操作、識別認証データの管理が確実に行われるためには、LM アクセス制御 SFP はサブジェクトがオブジェクトを操作する際に必ず実施されなければならない。また、その仕組みが干渉・改ざんされることから保護しなければならない。さらに、信頼できないサブジェクトにより干渉・改ざんされることを、TSF が自己防衛的に保護する必要がある。この要件に該当するセキュリティ機能要件は、FPT_RVM.1 および FPT_SEP.1 である。 以上 a、b、c、d、e、f、g すべての対策を満たすことにより、O.ADM_ROLE を満足できる。 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、 FPT_RVM.1、FPT_SEP.1 の達成により、O.ADM_ROLE を実現できる。

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.SEC_COMM	O.SEC_COMM では、Storage Navigator－SVP 間の通信データに対する、盗聴または改ざんを防止するため、Storage Navigator－SVP 間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。 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。 a. 通信データを保護する。 Storage Navigator と SVP 間の通信データを暗号化する必要がある。これにより、通信データの盗聴、改ざんから保護している。暗号化には SSL を使用し、暗号化アルゴリズムと鍵長は Storage Navigator－SVP 間のネゴシエーションにより決定する。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_COP.1、FCS_CKM.1、FCS_CKM.2、FCS_CKM.4 である。 b. 暗号化を確実に実施する。 Storage Navigator と SVP 間の通信データを盗聴、改ざんから保護するために暗号化を確実に実施する必要がある。また、その仕組みが干渉・改ざんされることから保護しなければならない。さらに、信頼できないサブジェクトにより干渉・改ざんされることを、TSF が自己防衛的に保護する必要がある。この要件に該当するセキュリティ機能要件は、FPT_RVM.1 および FPT_SEP.1 である。 以上 a、b の対策を満たすことにより、O.SEC_COMM を満足できる。 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_COP.1、FCS_CKM.1、FCS_CKM.2、FCS_CKM.4、FPT_RVM.1、FPT_SEP.1 の達成により、O.SEC_COMM を実現できる。
O.HOST_AUTH	O.HOST_AUTH ではホストからの接続要求があった際には、ホストの識別認証を行うことを要求している。 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。 a. TOE 利用前にホストを認証する。 TOE はホストの認証が成功した場合のみ、ホストが LU 内のユーザデータへアクセスを可能とする必要がある。この要件に該当するセキュリティ機能要件は FIA_UID2、FIA_UAU.1、FIA_UAU.5 である。 b. FC-SP 機能を実施する。 TOE は、ホストからセキュリティ認証実施のコマンドを受信したときに、DH-CHAP 認証コードを生成し、ホストに送信する(FIA_UAU.1)。 c. シークレットの管理を行う。 TOE がホスト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。

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
	d. 識別認証を確実に実施する。 TOE はホストが LU に接続する際には、ホストの識別認証を行う必要がある。そのため、ホストが LU に接続するときには、必ず識別認証機能が呼び出される。また、その仕組みが干渉・改ざんされることから保護しなければならない。さらに、信頼できないサブジェクトにより干渉・改ざんされることを、TSF が自己防衛的に保護する必要がある。この要件に該当するセキュリティ機能要件は、FPT_RVM.1 および FPT_SEP.1 である。 以上 a、b、c、d すべての対策を満たすことにより、O.HOST_AUTH を満足できる。 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_UID2、FIA_UAU.1 、FIA_UAU.5、FIA_SOS.1b、FPT_RVM.1、FPT_SEP.1 の達成により、O.HOST_AUTH を実現できる。
O.HOST_ACCESS	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、自ホストに割り当てられたパーティション内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。 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。 a. ホストの維持を行う。 TOE はホストを識別するために、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。これにより、ホスト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.1b、FIA_USB.1b である。 b. アクセス制御を規定し、実施する。 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 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 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。 c. LM アクセス制御 SFP を確実に実施する。 ホストのアクセス制御が確実に行われるためには、LM アクセス制御 SFP はサブジェクトがオブジェクトを操作する際には必ず実施されなければならない。また、その仕組みが干渉・改ざんされることから保護しなければならない。さらに、信頼できないサブジェクトにより干渉・改ざんされることを、TSF が自己防衛的に保護する必要がある。この要件に該当するセキュリティ機能要件は、FPT_RVM.1 および FPT_SEP.1 である。 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。 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、FDP_ACC.1、FDP_ACF.1 、FPT_RVM.1、FPT_SEP.1 の達成により、O.HOST_ACCESS を実現できる。

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.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、削除が行われていないか管理することを要求している。 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。 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。 Storage Navigatorでの識別認証、ユーザアカウントの改ざん、SLPRの改ざんの事象が発生した場合、SVP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。FAU_GEN.1 では、識別認証の事象、および設定変更の操作事象について監査ログを取得しているので、対策方針を満足している。FAU_GEN.1 の 表 5.19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。 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 を論理デバイスとして認識できず、LDEV にアクセスすることができないため、ホストから LDEV 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。 FPT_STM.1 で提供するタイムスタンプは、SVP の OS のタイムスタンプであり、保守員以外は変更できないため、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。 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。 b. 監査記録の参照を制限する。 監査記録を参照する際は、Storage Navigator から SVP 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、監査ログ管理者権限の操作権限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。 c. 監査記録を改ざんから保護する。 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権限の操作権限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。 d. 監査記録の損失の恐れを警告する。 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 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。この要件に該当するセキュリテ

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
	ィ機能要件は、FAU_STG.3 である。 e. 監査記録を確実に生成する。 TOE は、セキュリティ関連の情報が不正に作成、改変、削除が行われていないか監査するため、セキュリティ関連事象が発生した場合は、確実に監査記録を生成する。また、その仕組みが干渉・改ざんされることから保護しなければならない。さらに、信頼できないサブジェクトにより干渉・改ざんされることを、TSF が自己防衛的に保護する必要がある。この要件に該当するセキュリティ機能要件は、FPT_RVM.1 および FPT_SEP.1 である。 以上 a、b、c、d、e すべての対策を満たすことにより、O.AUD_GEN を満足できる。 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、FPT_RVM.1、FPT_SEP.1 の達成により、O.AUD_GEN を実現できる。

8.2.2　セキュリティ要件内部一貫性根拠

表 8.7にセキュリティ機能要件の依存性について示す。

表 8.7 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 part2 に定義されている依存性	本 ST で対応する機能要件
1	TOE	FIA_ATD.1a	なし	－
2	TOE	FIA_USB.1a	FIA_ATD.1	FIA_ATD.1a
3	TOE	FIA_ATD.1b	なし	－
4	TOE	FIA_USB.1b	FIA_ATD.1	FIA_ATD.1b
5	TOE	FIA_AFL.1	FIA_UAU.1	FIA_UAU.2 *2
6	TOE	FIA_SOS.1a	なし	－
7	TOE	FIA_UAU.2	FIA_UID.1	FIA_UID.2 *1
8	TOE	FIA_UAU.7	FIA_UAU.1	FIA_UAU.2 *2
9	TOE	FIA_UID.2	なし	－
10	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
11	TOE	FMT_MSA.3	FMT_MSA.1	FMT_MSA.1
			FMT_SMR.1	FMT_SMR.1
12	TOE	FMT_MTD.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
13	TOE	FMT_SMF.1	なし	－
14	TOE	FMT_SMR.1	FIA_UID.1	FIA_UID.2 *1
15	TOE	FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
			FCS_CKM.4	FCS_CKM.4
			FMT_MSA.2	なし*3
16	TOE	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	FCS_COP.1
			FCS_CKM.4	FCS_CKM.4
			FMT_MSA.2	なし*3
17	TOE	FCS_CKM.2	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
			FCS_CKM.4	FCS_CKM.4
			FMT_MSA.2	なし*3
18	TOE	FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	FCS_CKM.1
			FMT_MSA.2	なし*3
19	TOE	FIA_SOS.1b	なし	－
20	TOE	FIA_UAU.1	FIA_UID.1	FIA_UID.2 *1
21		FIA_UAU.5	なし	－
22	TOE	FMT_MOF.1	FMT_SMF.1	FMT_SMF.1
			FMT_SMR.1	FMT_SMR.1
23	TOE	FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
24	TOE	FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
			FMT_MSA.3	FMT_MSA.3

項番	TOE/IT 環境	セキュリティ機能要件	CC part2 に定義されている依存性	本 ST で対応する機能要件
25	TOE	FAU_GEN.1	FPT_STM.1	FPT_STM.1
26	TOE	FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
			FIA_UID.1	FIA_UID.2 *1
27	TOE	FPT_STM.1	なし	－
28	TOE	FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
29	TOE	FAU_STG.1	FAU_GEN.1	FAU_GEN.1
30	TOE	FAU_STG.3	FAU_STG.1	FAU_STG.1
31	TOE	FPT_RVM.1	なし	－
32	TOE	FPT_SEP.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：FCS_CKM.1、FCS_CKM.2、FCS_CKM.4、及び FCS_COP.1 で取り扱うセキュリティ属性は、各暗号鍵に関するものである。それぞれが標準化されたアルゴリズムに従って、セキュアな属性値が決定されており、Storage Navigator または、SVP から設定・改変することはない。したがって、セキュアなセキュリティ属性の受け入れに関するセキュリティ機能要件 FMT_MSA.2 への依存関係が満たされなくても問題はない。

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 8.8に示す。

表 8.8 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	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_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.1 FIA_UAU.2 FIA_UAU.5 FIA_UAU.7 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 のユーザ ID とパスワード、②ホストの WWN とシークレット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。

項番	カテゴリ	セキュリティ機能要件	一貫性の根拠
4	監査	FAU_GEN.1 FAU_GEN.2 FAU_SAR.1 FAU_STG.1 FAU_STG.3	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_COP.1 FCS_CKM.1 FCS_CKM.2 FCS_CKM.4	これらの機能要件は、Storage Navigator と SVP 間の SSL 通信で使用する暗号化鍵の管理と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	補完	FPT_STM.1 FPT_RVM.1 FPT_SEP.1	これら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、FPT_RVM.1 はバイパス防止、FPT_SEP.1 はセキュリティドメイン分離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。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。
7	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	前述の通り FPT_RVM.1、FPT_SEP.1 が他の要件との間で競合や矛盾が生じないのは自明である。 また、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.1 に関しては、FMT_MOF.1 により FC-SP の識別認証機能の動作および停止を、全体ストレージ管理者および分割ストレージ管理者による Storage Navigator 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。その他のセキュリティ機能要件に関しては、操作による機能停止やふるまいの変更はできないため、非活性化防止については考慮する必要がない。

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。

8.2.3　最小機能強度レベル根拠

3.2 章において、脅威エージェントのもつ攻撃能力は「低」と想定している。

したがって、TOEは低レベルの脅威エージェントに対抗できる必要があり、最小機能強度レベルはSOF-基本が妥当である。また、5.1.2節においてTOEに対し最小機能強度レベルとしてSOF-基本を求めており、攻撃能力と最小機能強度レベルは一貫している。

8.2.4　評価保証レベル根拠

TOEを含むストレージ装置はセキュアなエリアに設置され、SANまたは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 もしくは、管理PCとストレージ装置間の通信路からの攻撃と、許可されていないホストをSANに接続する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「低」レベルの攻撃と考えることができる。

また、Storage Navigator 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、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、暗号機能を持っているものの、暗号鍵の実装は、インストール時に行われる。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障できると考えられ、EAL2の評価保証レベルは妥当である。

8.3　TOE 要約仕様根拠

本章では、TOE のセキュリティ機能および保証手段が TOE セキュリティ要件を満たすのに適していることを説明する。

8.3.1　TOE セキュリティ機能根拠

表 8.9は、本STに記述されたITセキュリティ機能が、TOEセキュリティ機能要件にまでたどれることを示している。

表 8.9 TOE セキュリティ機能の SFR へのマッピング

		TOE の IT セキュリティ機能				
		SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.AUDIT**
TOEセキュリティ機能要件	FIA_ATD.1a	X				
	FIA_USB.1a	X				
	FIA_ATD.1b	X				
	FIA_USB.1b	X				
	FIA_AFL.1			X		
	FIA_SOS.1a			X		
	FIA_UAU.2			X	X	
	FIA_UAU.7			X		
	FIA_UID.2		X	X	X	
	FMT_MSA.1				X	
	FMT_MSA.3	X				
	FMT_MTD.1				X	
	FMT_SMF.1				X	
	FMT_SMR.1				X	
	FCS_COP.1			X		
	FCS_CKM.1			X		
	FCS_CKM.2			X		

	TOE の IT セキュリティ機能				
	SF.LM	**SF.FCSP**	**SF.SN**	**SF.ROLE**	**SF.AUDIT**
FCS_CKM.4			X		
FIA_SOS.1b		X			
FIA_UAU.1		X			
FIA_UAU.5		X	X	X	
FMT_MOF.1				X	
FDP_ACC.1	X				
FDP_ACF.1	X				
FAU_GEN.1					X
FAU_GEN.2					X
FPT_STM.1					X
FAU_SAR.1					X
FAU_STG.1					X
FAU_STG.3					X
FPT_RVM.1	X	X	X	X	X
FPT_SEP.1	X	X	X	X	X

表 8.10は、ITセキュリティ機能がTOEセキュリティ機能要件を満たし、相互に補完し一体となって機能していることを示している。

表 8.10 TOE セキュリティ機能要件に対する IT セキュリティ機能の正当性

TOE セキュリティ機能要件	IT セキュリティ機能
FIA_ATD.1a	FIA_ATD.1a は、SF.LM に関して以下のように記述されており、この内容によって実現されている。 『TOE は、Storage Navigator の属性情報（ユーザ種別、操作権限、SLPR 番号）を維持し、…』

TOE セキュリティ機能要件	IT セキュリティ機能
FIA_USB.1a	FIA_USB.1a は、SF.LM に関して以下のように記述されており、この内容によって実現されている。 『TOE は、Storage Navigator の属性情報（ユーザ種別、操作権限、SLPR 番号）を維持し、その属性を Storage Navigator のユーザアカウントに関連付ける。』
FIA_ATD.1b	FIA_ATD.1b は、SF.LM に関して以下のように記述されており、この内容によって実現されている。 『TOE は、ホストの属性情報（WWN、LU 番号）を維持し、…』
FIA_USB.1b	FIA_USB.1b は、SF.LM に関して以下のように記述されており、この内容によって実現されている。 『TOE は、ホストの属性情報（WWN、LU 番号）を維持し、その属性をホストに関連付ける。』
FIA_AFL.1	FIA_AFL.1 は、SF.SN に関して以下のように記述されており、この内容によって実現されている。 『TOE は、Storage Navigator 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_SOS.1a	FIA_SOS.1a は、SF.SN に関して以下のように記述されており、この内容によって実現されている。 『TOE は、Storage Navigator での識別認証時に使用するパスワードの入力を 6 文字以上 256 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!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~に制限し、…』
FIA_UAU.2	FIA_UAU.2 は、SF.SN、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 ・SF.SN 『TOE は、Storage Navigator 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。…』 ・SF.ROLE 『TOE は、保守員が SVP に接続するときは、リモートデスクトップ接続のユーザ名とパスワードで保守員の識別認証を行う。』
FIA_UAU.7	FIA_UAU.7 は、SF.SN に関して以下のように記述されており、この内容によって実現されている。 『TOE は、Storage Navigator での識別認証時に使用するパスワードの入力を 6 文字以上 256 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!"#$%&'()*+,-

TOE セキュリティ機能要件	IT セキュリティ機能
	./:;<=>?@[\]^_`{|}~に制限し、入力時は「*」表示とする。』
FIA_UID.2	FIA_UID.2 は、SF.FCSP、SF.SN、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 ・SF.FCSP 『TOE は、FC-SP によるホストの識別認証を WWN、シークレットにて行い、ホストからのアクセスに関する他のセキュリティ機能の動作前に実施する。…』 ・SF.SN 『TOE は、Storage Navigator 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。…』 ・SF.ROLE 『TOE は、保守員が SVP に接続するときは、リモートデスクトップ接続のユーザ名とパスワードで保守員の識別認証を行う。』
FMT_MSA.1	FMT_MSA.1 は、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 『「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（WWN、LU 番号、LDEV 番号）の作成、改変、削除、参照の操作をユーザ種別、操作権限に基づき制限する。 ・ 「LM アクセス制御 SFP」は、論理パーティション情報（SLPR 番号）の作成、削除、参照の操作をユーザ種別、操作権限、SLPR 番号に基づき制限する。 ・ 「LM アクセス制御 SFP」は、Storage Navigator のユーザ権限情報（ユーザ種別、操作権限、SLPR 番号）の設定、改変、参照の操作をユーザ種別、操作権限に基づき制限する。』
FMT_MSA.3	FMT_MSA.3 は、SF.LM に関して以下のように記述されており、この内容によって実現されている。 『「LM アクセス制御 SFP」は、以下の規則からなる。 ・ LDEV 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 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_MTD.1	FMT_SMF.1 は、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 『TOE は、以下の管理機能を有する。 ・ Storage Navigator のアカウント管理機能でユーザアカウントのユーザ ID、パスワード、ユーザ種別、操作権限、SLPR 番号を管理する。･･･ ・ 保守員がリモートデスクトップ接続を行うときのユーザ名とパスワードを管理する。･･･

TOE セキュリティ機能要件	IT セキュリティ機能
	・ Storage Navigator の FC-SP 機能でホストの認証データである、WWN、シークレットを管理する。･･･』
FMT_SMF.1	FMT_SMF.1 は、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 『TOE は、以下の管理機能を有する。 ・ Storage Navigator のアカウント管理機能でユーザアカウントのユーザ ID、パスワード、ユーザ種別、操作権限、SLPR 番号を管理する。 ・ 保守員がリモートデスクトップ接続を行うときのユーザ名とパスワードを管理する。･･･ ・ Storage Navigator の FC-SP 機能でホストの認証データである、WWN、シークレットを管理する。･･･』
FMT_SMR.1	FMT_SMR.1 は、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 『TOE は、役割（全体アカウント管理者、全体ストレージ管理者、分割アカウント管理者、分割ストレージ管理者、監査ログ管理者、保守員、ストレージ利用者）を維持する。』
FCS_COP.1	FCS_COP.1 は、SF.SN に関して以下のように記述されており、この内容によって実現されている。 『SSL は、公開鍵暗号方式によるサーバ、クライアント間認証、共通鍵暗号方式によるデータの暗号化、ハッシュ関数によるデータの同一性確保を提供する。』
FCS_CKM.1	FCS_CKM.1 は、SF.SN に関して以下のように記述されており、この内容によって実現されている。 『SSLは、公開鍵暗号方式によるサーバ、クライアント間認証、共通鍵暗号方式によるデータの暗号化、ハッシュ関数によるデータの同一性確保を提供する。SSLで使用する 暗号操作を 表 5.13 に示す。暗号化アルゴリズムと鍵長はStorage Navigator－SVP 間のネゴシエーションにより決定し、･･･』
FCS_CKM.2	FCS_CKM.2 は、SF.SN に関して以下のように記述されており、この内容によって実現されている。 『SSL は、公開鍵暗号方式によるサーバ、クライアント間認証、共通鍵暗号方式によるデータの暗号化、ハッシュ関数によるデータの同一性確保を提供する。SSL で使用する暗号化アルゴリズムと鍵長は Storage Navigator－SVP 間のネゴシエーションにより決定し、･･･』
FCS_CKM.4	FCS_CKM.4 は、SF.SN に関して以下のように記述されており、この内容によって実現されている。 『SSL で使用する暗号化アルゴリズムと鍵長は Storage Navigator－SVP 間のネゴシエーションにより決定し、鍵は使用

TOE セキュリティ機能要件	IT セキュリティ機能
	後にメモリから消去する。』
FIA_SOS.1b	FIA_SOS.1b は、SF.FCSP に関して以下のように記述されており、この内容によって実現されている。 『TOE は、FC-SP によるホストの識別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 種類の記号.-+@_=:/[],~に制限する。』
FIA_UAU.1	FIA_UAU.1 は、SF.FCSP に関して以下のように記述されており、この内容によって実現されている。 『TOE は、ホスト識別認証が有りの場合は、ホストからセキュリティ認証実施のコマンドを受信したときに、DH-CHAP 認証コードを生成し、ホストに送信する。』
FIA_UAU.5	FIA_UAU.5 は、SF.FCSP、SF.SN、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 ・SF.FCSP 『ホストから受信したシークレットと TOE が保持するシークレットが一致したときに、ホストとストレージ装置との接続を許可する。』 ・SF.SN 『TOE は、Storage Navigator 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。...』 ・SF.ROLE 『TOE は、保守員が SVP に接続するときは、リモートデスクトップ接続のユーザ名とパスワードで保守員の識別認証を行う。』
FMT_MOF.1	FMT_MOF.1 は、SF.ROLE に関して以下のように記述されており、この内容によって実現されている。 『TOE は、FC-SP によるホスト識別認証の有無(認証あり、認証なし)の設定操作を、ユーザ種別、操作権限に基づき制限する。』
FDP_ACC.1	FDP_ACC.1 は、SF.LM に関して以下のように記述されており、この内容によって実現されている。 『「LM アクセス制御 SFP」は、以下の規則からなる。 ・ ホストを代行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 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 を代行するプロセスが SLPR を生成、または削除する場合、Storage Navigator を代行するプロセスに渡された、「Storage Navigator のユーザ権限情報」

TOE セキュリティ機能要件	IT セキュリティ機能
	（Storage Navigator のユーザ種別、操作権限、SLPR 番号）により、全体ストレージ管理者のみが SLPR を作成、または削除できる。 ・ Storage Navigator を代行するプロセスが LDEV を生成、または削除する場合、Storage Navigator を代行するプロセスに渡された、「Storage Navigator のユーザ権限情報」（Storage Navigator のユーザ種別、操作権限、SLPR 番号）により、全体ストレージ管理者は全ての LDEV を生成、または削除できる。分割ストレージ管理者は、分割ストレージ管理者に対して割り当てられた SLPR 番号と一致する論理パーティション内に LDEV を生成、または削除できる。』
FDP_ACF.1	FDP_ACF.1 は、SF.LM に関して以下のように記述されており、この内容によって実現されている。 『「LM アクセス制御 SFP」は、以下の規則からなる。 ・ ホストを代行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 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 を代行するプロセスが SLPR を生成、または削除する場合、Storage Navigator を代行するプロセスに渡された、「Storage Navigator のユーザ権限情報」（Storage Navigator のユーザ種別、操作権限、SLPR 番号）により、全体ストレージ管理者のみが SLPR を作成、または削除できる。 ・ Storage Navigator を代行するプロセスが LDEV を生成、または削除する場合、Storage Navigator を代行するプロセスに渡された、「Storage Navigator のユーザ権限情報」（Storage Navigator のユーザ種別、操作権限、SLPR 番号）により、全体ストレージ管理者は全ての LDEV を生成、または削除できる。分割ストレージ管理者は、分割ストレージ管理者に対して割り当てられた SLPR 番号と一致する論理パーティション内に LDEV を生成、または削除できる。』
FAU_GEN.1	FAU_GEN.1 は、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 『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。…』
FAU_GEN.2	FAU_GEN.2 は、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 『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。…』

TOE セキュリティ機能要件	IT セキュリティ機能
FPT_STM.1	FPT_STM.1 は、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 『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 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。』
FAU_SAR.1	FAU_SAR.1 は、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 『TOE は、以下の監査機能を有する。 ・ 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。』
FAU_STG.1	FAU_STG.1 は、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 『TOE は、以下の監査機能を有する。 ・ 監査記録の不正な改変、削除を行える役割は存在しない。』
FAU_STG.3	FAU_STG.3 は、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 『TOE は、以下の監査機能を有する。 ・ 監査記録の 175,000 行を超えた時点で、Storage Navigator 画面に超過した旨を通知し、ユーザに監査記録のダウンロードを促す。』
FPT_RVM.1	FPT_RVM.1 は、SF.LM、SF.FCSP、SF.SN、SF.ROLE、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 ・SF.LM 『TOE は、TOE の機能が実行される際に、かならず「LM アクセス制御 SFP」が適用されることを保証する。』 ・SF.FCSP 『TOE は、ホストの識別認証が行われる場合は、ホストがストレージ装置に接続する際に SF.FCSP を呼び出し、ホストの識別認証が行われることを保証する。』 ・SF.SN 『TOE は Storage Navigator 利用者が Storage Navigator を使用してストレージ装置の管理操作を行う前に SF.SN を呼び出し、SSL による暗号化通信と Storage Navigator 利用者の識別認証が行われることを保証する。』 ・SF.ROLE 『TOE は Storage Navigator 利用者が管理操作を行う際には SF.ROLE を呼び出し、Storage Navigator 利用者のユーザ種別

TOE セキュリティ機能要件	IT セキュリティ機能
	と操作権限により、権限範囲外の管理操作が行われないことを保証する。』 ・SF.AUDIT 『TOE は、セキュリティ関連事象が発生した場合は、SF.AUDIT を呼び出し、監査記録が生成されることを保証する。』
FPT_SEP.1	FPT_SEP.1 は、SF.LM、SF.FCSP、SF.SN、SF.ROLE、SF.AUDIT に関して以下のように記述されており、この内容によって実現されている。 『SF.・・・に関する TSF は自身を保護し、信頼できないサブジェクトからの干渉と改ざんが起こらないことを保証する。』

8.3.2　TOE 機能強度根拠

本TOEにおいて、確率的かつ順列的メカニズムに基づくセキュリティ機能は、SF.FCSP、SF.SNである。SF.FCSP、SF.SNのセキュリティ機能強度は、6.2 節において、「SOF-基本」を指定している。一方、5.1.2にてTOEの 最小機能強度レベルは「SOF-基本」を指定している。従って両者は一貫している。

8.3.3　保証手段根拠

表 6.4に示した保証手段は、対応したセキュリティ保証要件を満たしていることが読み取れる名称の文書名となっており、セキュリティ保証要件と保証手段の対応が取れている。なお、保証手段に関する特記事項を以下に示す。

- ADO_IGS.1 に関しては、4 種類のマニュアルを記載しているが、下の 2 つのマニュアルは上記の 2 種類の装置に対応したマニュアルの英語版であり、内容については同一である。
- AGD_ADM.1 に関しては、2 種類のマニュアルを記載しているが、これらは日本語版と英語版の違いだけであり、内容については同一である。
- AGD_USR.1 に関しては、2 種類のマニュアルを記載しているが、これらは日本語版と英語版の違いだけであり、内容については同一である。

上記の通り、本 ST に記述された各保証手段が、TOE セキュリティ保証要件にまでたどれることを示し、また記述されたすべての保証手段が実装されることによってすべての TOE セキュリティ保証要件が満たされることも示している。

8.4　PP 主張根拠

本 ST は、いかなる PP への適合も主張しない。

9　参考文献

・Common Criteria for Information Technology Security Evaluation
Part 1:Introduction and general model, Version 2.3, August 2005, CCMB-2005-08-001

・Common Criteria for Information Technology Security Evaluation
Part 2:Security functional requirements, Version 2.3, August 2005, CCMB-2005-08-002

・Common Criteria for Information Technology Security Evaluation
Part 3:Security assurance requirements, Version 2.3, August 2005, CCMB-2005-08-003

・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 2.3, 2005 年 8 月, CCMB-2005-08-001, 平成 17 年 12 月翻訳第 1.0 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：セキュリティ機能要件,
バージョン 2.3, 2005 年 8 月, CCMB-2005-08-002, 平成 17 年 12 月翻訳第 1.0 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：セキュリティ保証要件,
バージョン 2.3, 2005 年 8 月, CCMB-2005-08-003, 平成 17 年 12 月翻訳第 1.0 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

・補足-0512（Interpretations-0512）, 平成 17 年 12 月, 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