HITACHI
Inspire the Next

Hitachi Adaptable Modular Storage 2300 用
マイクロプログラム

セキュリティターゲット

Rev.11

2009 年 4 月 13 日

株式会社 日立製作所

他社商標

- AIX は、米国 International Business Machines Corp.の登録商標です。
- HP-UX は、米国 Hewlett-Packard Company のオペレーティングシステムの名称です。
- Java およびすべての Java 関連の商標およびロゴは、米国およびその他の国における米国 Sun Microsystems, 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登録商標または商標です。
- Microsoft®、Windows®、および Windows Server は、米国およびその他の国における米国 Microsoft Corp.の登録商標または商標です。
- Microsoft Internet Explorer は、米国 Microsoft Corp.の商品名称です。
- Mozilla は、Mozilla Foundation の米国およびその他の国における商標です。
- Red Hat は、米国およびその他の国で Red Hat, Inc.の登録商標または商標です。
- Solaris は、米国 Sun Microsystems, Inc.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。
- IRIX は、Silicon Graphics, Inc.の登録商標です。
- VxWorks は、米国 Wind River Systems, Inc.の登録商標です。
- その他、各会社名、各製品名は、各会社の登録商標、商標、または商品名称です。なお、本文中では、®と ™ は明記しておりません。

－更新履歴－

Rev.	日付	頁	変更内容
0	2008.03.21	全	新規作成
1	2008.04.15	2、3、4、5、6、8 章	ホスト識別機能削除に伴い、該当箇所を修正
2	2008.05.29	2、3、5、6、8 章	所見報告書 BES-EOR-0001-00 に基づく修正
3	2008.06.11	2、3、5、6、8 章	脅威、識別に関する記述の修正、誤植の修正
4	2008.06.25	2、3、5、6、8 章	セキュリティ機能要件の修正、誤植の修正
5	2008.06.27	3、5、6、8 章	脅威、FIA_UID、FIA_UAU の修正、誤植の修正
6	2008.07.31	2、3、4、5、6、8 章	所見報告書 BES-EOR-0004-00、BES-EOR-0301-00 に基づく修正
7	2008.10.17	5 章	監査対象事象を修正
8	2009.02.10	2、3、4、5、6、8 章	セキュリティ機能範囲の見直しに基づく修正
9	2009.03.18	2、3、4、5、6、8 章	セキュリティ機能範囲の見直しに基づく修正
10	2009.03.23	2、3、4、6、8 章	システム構成の記述の修正
11	2009.04.13	1、3、4、8 章	ST 概要の追記、セキュリティ環境・対策の追記

－目次－

1. ST 概説

本章では ST や TOE の識別情報、ST の概要、および CC への適合性や使用する用語の説明を記述する。

1.1. ST 識別

以下に、ST および ST が対象とする TOE の識別情報を示す。

(1) ST 識別

ST 名称	Hitachi Adaptable Modular Storage 2300 用マイクロプログラム セキュリティターゲット
Rev.	11
作成者	株式会社 日立製作所
作成日	2009 年 4 月 13 日

(2) TOE 識別

TOE 識別	Hitachi Adaptable Modular Storage 2300 用マイクロプログラム
バージョン	0862/ A-M
製造者	株式会社 日立製作所

(3) 適用する CC のバージョン

CC 識別	Common Criteria for Information Technology Security Evaluation Version 2.3 Interpretations-0512 適用

1.2. ST 概要

日立製作所製ディスクアレイ装置「Hitachi Adaptable Modular Storage 2300」(以下 Hitachi AMS2300 と略す)は、大容量、高信頼性とモジュラー構造による柔軟なシステム拡張を実現したミッドレンジ向けディスクアレイ装置である。

ディスクアレイ装置にはホスト利用者にとって重要なデータが保管される。このため、それらデータの完全性や機密性が損なわれるようなディスクアレイ装置の設定変更が行われないよう、管理者毎に設定可能な操作を限定する必要がある。

本 ST では、Hitachi AMS2300 用マイクロプログラムを評価対象(TOE)として、その提供するセキュリティ機能について記述する。

なお、本 ST で評価した Hitachi AMS2300 用マイクロプログラム(TOE)とそのハードウェア(Hitachi AMS2300)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 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

1.4. 参考資料

- 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
- 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
- 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

1.5. 用語集

本 ST で使用する用語を以下の表に示す。

表 1 用語集

用語	説明
FC	Fibre Channel の略。コンピュータと周辺機器を接続するための高速データ伝送技術(プロトコル)。接続には光ファイバーや銅線が用いられる。
FC-SAN	Fibre Channel - Storage Area Network の略。ネットワークとして Fibre Channel を利用する SAN の一形態である。
Hitachi AMS 2300	Hitachi Adaptable Modular Storage 2300 の略。本 ST で取り扱う TOE が動作するディスクアレイ装置である。
Hitachi Storage Navigator Modular 2	ディスクアレイ装置管理設定用のソフトウェア。本文中では for CLI と for GUI を総称して単に「Hitachi Storage Navigator Modular 2」あるいは略称で「HSNM2」と記述する場合がある。
Hitachi Storage Navigator Modular 2 (for CLI)	コマンドラインインタフェースにより操作を行う Hitachi Storage Navigator Modular 2。
Hitachi Storage Navigator Modular 2 (for GUI)	GUI により操作を行う Hitachi Storage Navigator Modular 2。Web ベースのアプリケーションであり、Hitachi Storage Navigator Modular 2 (for GUI)が導入されたコンピュータをサーバとし、同一あるいは異なるコンピュータの Web ブラウザから操作を行う。
HSNM2(for CLI)	Hitachi Storage Navigator Modular 2 (for CLI)の略。
HSNM2(for GUI)	Hitachi Storage Navigator Modular 2 (for GUI)の略。
IP-SAN	Internet Protocol - Storage Area Network の略。SAN の一形態であり、ネットワークとして安価に構築できる Ethernet およびその上で動作する TCP/IP を利用し、通信制御には iSCSI を用いる。
iSCSI	internet Small Computer System Interface の略。SCSI プロトコルを TCP/IP ネットワーク上で使用する規格。
LU	Logical Unit の略。論理的に分けたディスクスペースの事。これら複数の論理ユニットを識別するために付与されるアドレスを LUN（Logical Unit Number）と呼ぶ。
RAID	Redundant Arrays of Inexpensive(もしくは Independent) Disks の略。ハードディスクなどの記憶装置を複数台用いてアクセスを分散させることにより、高速、大容量で信頼性の高いディスク装置を実現するための技術。
RAID Manager	ディスクアレイ装置管理設定用のソフトウェア。RAID Manager はホスト上で動作し、SAN 経由でディスクアレイ装置に対して設定指示を行う。
SAN	Storage Area Network の略。ディスク装置やテープ装置などのストレージとサーバとを接続するための専用ネットワーク。
SCSI	Small Computer System Interface の略。主にコンピュータとストレージなどの周辺機器を接続しデータのやりとりを行うためのインタフェース。
有償オプション	有償で提供されるディスクアレイ装置のオプション機能。機能の有効化、無効化の設定が可能。
リソース操作権限	Account Authentication 機能でログインした管理者に割り当てられる権限。2 人以上のユーザが同時に設定変更を行って、アレイ装置が意図しない状態（設定）になるのを防ぐ為のものである。権限には「更新モード」と「参照モード」があり、アカウントのログイン時に決定される。ログインするアカウントと同一ロールをもった別のアカウントが既にログインしている場合は、参照モードが与えられる（同一ロールをもった別アカウントがログインしていない場合は、更新モード）。更新モードの場合、ロールに従った管理操作が可能となる。参照モードの場合、ロール割り当てにかかわらず管理情報の参照のみが可能となる。

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、Hitachi AMS 2300 用マイクロプログラム バージョン 0862/A-M は、株式会社日立製作所ディスクアレイ装置「Hitachi AMS2300」上で動作する制御プログラム（ソフトウェア）であり、ディスクアレイ装置とディスクアレイ装置に接続されたホストとの間のデータ転送の制御など、ディスクアレイ装置の動作を制御する役割を持つ。

本 TOE は、事前に許可された管理者に対してのみディスクアレイ装置の管理操作を許可する機能、管理操作の事象を記録する監査ログ機能をセキュリティ機能として提供するものである。

2.2. ディスクアレイ装置を含むシステムの一般的な構成

下図に、ディスクアレイ装置を含むシステムの一般的な構成を示す。

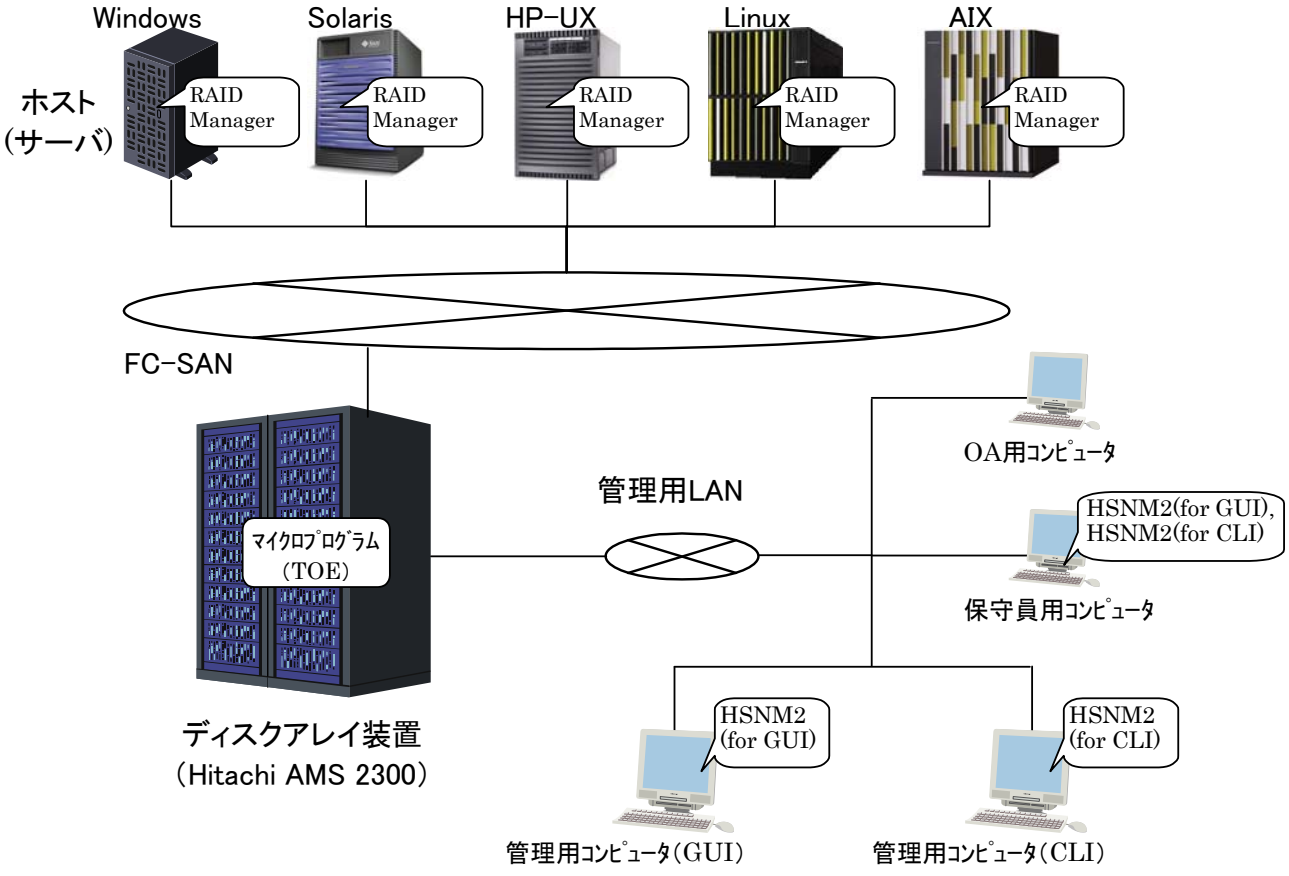

図 1　ディスクアレイ装置を含むシステムの一般的な構成

(1) ホスト

ディスクアレイ装置に接続され、ディスクアレイ装置を利用する Windows、Solaris、HP-UX 等の各種オープン系サーバである。本 ST では、これらの機器をホストと総称する。本機器を利用するのは後述するホスト利用者である。ホストにはディスクアレイ装置の装置制御情報を管理するためのソフトウェアである RAID Manager の導入が可能である。なお、本 ST では RAID Manager を使用していない装置

構成を対象とする。(RAID Manager を使用するには、Hitachi Storage Navigator Modular 2 にて事前にディスクアレイ装置に設定を行う必要があるが、本 ST ではそのような設定がなされていない環境を想定している。)

(2) FC-SAN(Fibre Channel - Storage Area Network)

ホストとディスクアレイ装置をFibre Channelを利用し接続するストレージシステム専用ネットワークである。本ネットワークは、ストレージシステム以外の用途では利用されない。

(3) ディスクアレイ装置

Hitachi AMS 2300 である。TOE が動作する装置であり、FC-SAN を介してホストと接続される。評価構成であるディスクアレイ装置はホストとの接続インタフェースとして Fibre Channel (FC-SAN)を利用する。Hitachi AMS 2300 は、FC-SANもしくはIP-SAN のどちらか片方を排他で利用可能であるが、評価構成は FC-SAN を利用したものである。

(4) 管理用 LAN

ディスクアレイ装置と管理用コンピュータを接続する Ethernet ネットワークである。このネットワークは、他の社内ネットワークと共用しOA 用コンピュータが接続される場合があり、独立したネットワークとは限らないが、インターネット等外部のネットワークから直接アクセス出来ないようファイアウォール等によって保護されている。

(5) 管理用コンピュータ(GUI)

ディスクアレイ装置の設定や運用・管理を行うために利用するコンピュータであり、ディスクアレイ装置設定用プログラムである Hitachi Storage Navigator Modular 2(for GUI)が導入されている。また、HSNM2(for GUI)は画面表示の一部に Java を使用しているため、本装置には JRE が導入されている。本装置を操作するのは後述する管理者(ディスクアレイ管理者、アカウント管理者、監査ログ管理者)もしくは保守員である。本装置とディスクアレイ装置は管理用 LAN を介して接続される。

本装置上のHitachi Storage Navigator Modular 2(for GUI)に対して、HTTPプロトコルを使用しアクセスする。そのため、Web ブラウザを使用して、HSNM2(for GUI)を起動し、ディスクアレイ装置の TOE にアクセスする(表示画面によってはHSNM2(for GUI)にて JRE を起動する場合がある)。

(6) 管理用コンピュータ(CLI)

ディスクアレイ装置の設定や運用・管理を行うために利用するコンピュータであり、ディスクアレイ装置設定用プログラムである Hitachi Storage Navigator Modular 2(for CLI)が導入されている。本装置とディスクアレイ装置は管理用LANを介して接続される。本装置を操作するのは後述する管理者(ディスクアレイ管理者、アカウント管理者、監査ログ管理者)もしくは保守員である。本装置の HSNM2(for CLI)を起動し、ディスクアレイ装置の TOE にアクセスする。

(7) 保守員用コンピュータ

保守員がディスクアレイ装置の保守作業を行うために使用するコンピュータである。保守作業を行うために必要な Hitachi Storage Navigator Modular 2 (for GUI)または(for CLI)が導入されている(HSNM2(for GUI)の場合はJREも導入されている)。また、保守作業のためにWebブラウザからWebメンテナンス画面を使用し、ディスクアレイ装置の TOE にアクセスすることがある(Web メンテナンス画面は、Web ブラウザでディスクアレイ装置の IP アドレスを入力すると表示される Web ページである)。本装置とディスクアレイ装置は保守作業を行う場合のみ管理用 LAN に接続される。

本 ST では上記(5)～(7)のコンピュータを総称して管理用コンピュータと呼ぶ場合がある。また、管理用コンピュータ(GUI)と管理用コンピュータ(CLI)は同一ハードウェアで共用することができる。

(8) Hitachi Storage Navigator Modular 2

ディスクアレイ装置の構成設定と表示、情報の表示及び障害を監視するために使われるプログラムであり、管理用コンピュータにインストールして使用する。Web ベースの GUI である Hitachi Storage Navigator Modular 2 (for GUI)と、コマンドラインインタフェースである Hitachi Storage Navigator Modular 2 (for CLI)の 2 種類がある。

上記(5)(6)(7)に示すコンピュータは、後述するハードウェアの構成要素の条件を満たせば、HSNM2(for GUI)と(for CLI)を各々のコンピュータ上で共存させることが可能である。

なお、上記機器のうちホスト、ディスクアレイ装置とそれらを接続する FC-SAN は限定された人物のみがアクセスできる環境に設置され、それら以外は一般的な企業のオフィス等に設置されることが想定される。

2.2.1. ハードウェアの一般的な構成

ハードウェアの一般的な構成を下表に示す。

表 2 ハードウェアの構成要素

構成要素	説明または動作条件
ディスクアレイ装置	Hitachi Adaptable Modular Storage 2300である。HDDやポート数は顧客のオーダーした構成により変わる。
ホスト	ディスクアレイ装置にアクセスするコンピュータ。
管理用コンピュータ(GUI)	動作条件を以下に示す。 ■Windows ・OS: Windows2000(SP3、SP4)/XP(SP2)/Vista、 Windows Server 2003(SP1、SP2) Windows Server 2003(R2)(32/64bit) Windows Server 2008(32/64bit)(32/64bit) ・CPU: 1GHz 以上(2GHz 以上推奨) ・メモリ: 1GB 以上(2 GB 以上推奨) ・ブラウザ: Internet Explorer6.0(SP1)、Internet Explorer7.0 ・Java(JRE): Java6.0 Update10(1.6.0_10) ・ディスク容量: 1.5 GB 以上の空き容量 ・モニタ解像度: 1024×768 以上推奨(256 色以上)
	■Sun(SPARC) ・OS: Solaris 8、9、10 ・CPU:SPARC1GHz 以上(2GHz 以上推奨) ・メモリ: 1GB 以上(2GB 以上推奨) ・ブラウザ: Mozilla1.7 ・Java(JRE): Java6.0 Update10(1.6.0_10) ・ディスク容量: 1.5 GB 以上の空き容量 ・モニタ解像度: 1024×768 以上推奨(256 色以上)
	■RedHatLinux(x86) ・OS: Red Hat Enterprise Linux AS4.0 Update1/Update5(共に 32bit) ・CPU: 1GHz 以上(2GHz 以上推奨) ・メモリ: 1GB 以上(2GB 以上推奨) ・ブラウザ: Mozilla1.7 ・Java(JRE): Java6.0 Update10(1.6.0_10) ・ディスク容量:1.5 GB 以上の空き容量 ・モニタ解像度: 1024×768 以上推奨(256 色以上)

構成要素	説明または動作条件
管理用コンピュータ(CLI)	動作条件を以下に示す。 ■Windows ・OS: Windows2000/XP/Vista、 Windows Server2003(SP1、SP2) Windows Server 2003(R2)(32/64bit) Windows Server 2008(32/64bit) ・CPU: 233MHz 以上 ・メモリ: 256 MB 以上 ・ディスク容量: 30 MB 以上の空き容量
	■Sun(SPARC) ・OS:Solaris 8、9、10 ・CPU: SPARC 以上(周波数は問わない) ・メモリ: 256 MB 以上 ・ディスク容量: 54 MB 以上の空き容量 ・漢字コード: EUC-JP
	■Sun(x86、32bit) ・OS:Solaris 10 ・CPU: 256MHz以上 ・メモリ: 256 MB 以上 ・ディスク容量: 54 MB 以上の空き容量 ・漢字コード: EUC-JP
	■SGI ・OS: IRIX 6.5 ・CPU: R10000 以上(周波数は問わない) ・メモリ: 256 MB 以上 ・ディスク容量: 90.5 MB 以上の空き容量 ・漢字コード: EUC-JP
	■HP ・OS: HP-UX 11.0、11i、11i v2.0 ・CPU: PA8000 以上、11iv2.0 は Itanium 2(周波数は問わない) ・メモリ: 256 MB 以上 ・ディスク容量: 65 MB 以上の空き容量 ・漢字コード: SJIS/EUC-JP
	■IBM ・OS: AIX 5L v5.1、5.2 ・CPU: PowerPC/RS64 II 以上(周波数は問わない) ・メモリ: 256 MB 以上 ・ディスク容量: 46.5 MB 以上の空き容量 ・漢字コード: SJIS ・前提プログラム: VisualAge C++ Runtime 6.0.0.0 以降。IY33524 のパッチが必要。
	■Red Hat Linux(x86) ・OS: Red Hat Enterprise Linux AS4 Update1(32bit) ・CPU: 233 M Hz 以上 ・メモリ: 256 MB 以上 ・ディスク容量: 35 MB 以上の空き容量 ・漢字コード: SJIS/EUC-JP
保守員用コンピュータ	管理用コンピュータを保守員用コンピュータとして使用可能である。そのため、動作条件は管理用コンピュータ(GUI)または(CLI)のいずれかを満たしていればよい。

2.2.2. ソフトウェアの一般的な構成

ソフトウェアの一般的な構成を下表に示す。

表 3 ソフトウェアの構成要素

構成要素	説明

構成要素	説明
マイクロプログラム	TOEであり、ディスクアレイ装置のコントローラ上で動作するファームウェア。 バージョン:0862/A-M
リアルタイムOS	ディスクアレイ装置で動作するリアルタイムOS。 パッケージ名:WindRiver Platform for Network Equipment, Vxworks Edition 3.5 (旧:Tornado) OS: VxWorks 6.5 Web: Wind River CLI,Web,MIBway 4.6 (旧:WindManageWeb) Security: WindRiver Security Library 1.3 SSL: Wind River SSL 1.3 (OpenSSL:version 0.9.8a)
Hitachi Storage Navigator Modular 2 (for GUI)	管理用コンピュータ(GUI)上で動作するディスクアレイ装置を管理するためのプログラム。 バージョン: 6.20
Hitachi Storage Navigator Modular 2 (for CLI)	管理用コンピュータ(CLI)上で動作するディスクアレイ装置を管理するためのプログラム。 バージョン: 6.20
管理用コンピュータ(GUI)のOS	詳細は表2の「管理用コンピュータ(GUI)」参照。
管理用コンピュータ(CLI)のOS	詳細は表2の「管理用コンピュータ(CLI)」参照。
Webブラウザ(HSNM2)	管理コンピュータ(GUI)からHitachi Storage Navigator Modular2にアクセス可能なWebブラウザ。 ・ Internet Explorer6.0 (SP1) ・ Internet Explorer7.0 ・ Mozilla 1.7
Webブラウザ(Webメンテナンス画面)	保守員用コンピュータからディスクアレイ装置のWebメンテナンス画面にアクセス可能なWebブラウザ。 ・ Internet Explorer6.0 (SP1) ・ Internet Explorer7.0 ・ Mozilla 1.7
Javaランタイム環境	管理用コンピュータ(GUI)でHitachi Storage Navigator Modular 2 for GUIのJavaアプレットを起動する際に必要となるJavaランタイム環境。 ・ Java6.0 Update10(1.6.0_10)

2.3. TOE の物理的範囲

本 TOE の物理構成を下図に示す。

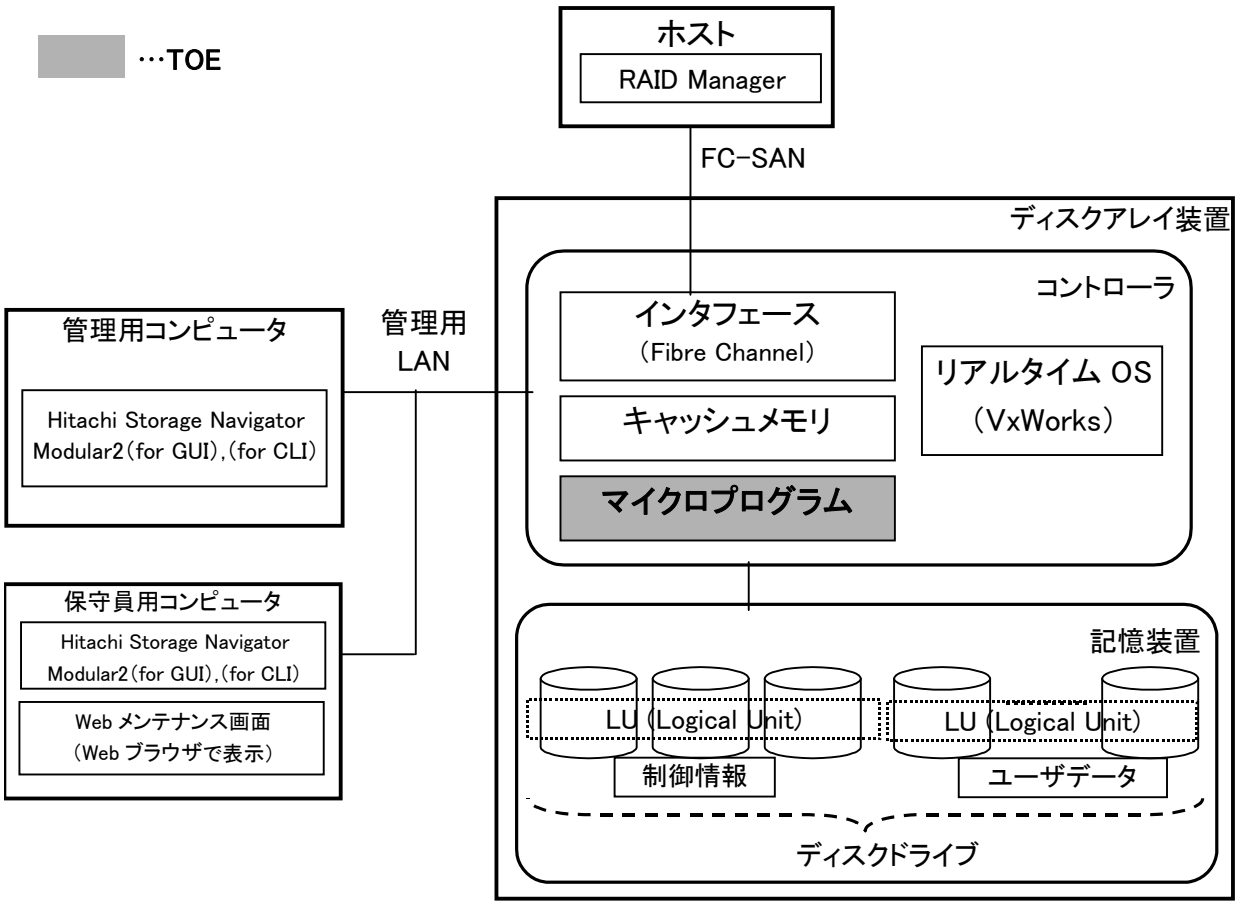

図 2 TOE の物理構成

ディスクアレイ装置は、ディスクアレイ装置の動作を制御するコントローラと、ユーザデータを記録する記憶装置から構成される。また、ディスクアレイ装置の動作に関する設定や、運用保守のために管理用コンピュータ、保守員用コンピュータが利用される。各々の構成要素の説明を以下に記述する。

なお、ディスクアレイ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いる。

(1) コントローラ

ディスクアレイ装置の動作を制御する部品である。コントローラには、管理用コンピュータと接続する為の LAN 用インタフェース、ホストと接続する為の Fibre Channel 用インタフェース、ディスクドライブと接続する為のインタフェース、ホストと送受信するデータを一時的に保存するキャッシュメモリ等が含まれる。また、コントローラ上では TOE であるマイクロプログラムが動作する。

なお、管理用 LAN と FC-SAN および記憶装置は完全に独立した構造となっている。このため、管理用 LAN に接続された機器から FC-SAN やキャッシュメモリ、記憶装置に対してアクセスすることは不可能である。

(2) Fibre Channel 用インタフェース

ディスクアレイ装置がホストからの通信を受け付ける部品であり、Fibre Channel 用インタフェース（FC-SAN に利用）が搭載されている。なお、耐障害性の為、同種のインタフェースを複数搭載する場合が有る。

(3) キャッシュメモリ

キャッシュメモリは、ホストから記憶装置に対してユーザデータの Read/Write を行う際にデータを一時保存し、処理の高速化のため使用する。

(4) マイクロプログラム

本 ST で取り扱う TOE である。本プログラムがディスクアレイ装置の動作を制御する。

なお、マイクロプログラムは有償にて追加オプション機能（以下、有償オプション）を提供することができる。本 TOE の構成では、有償オプションのうちセキュリティ機能である Account Authentication、Audit Logging のみが提供され、それ以外の有償オプションは提供されないものとする。

(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、およびディスクアレイ装置の設定情報である制御情報が記憶される。記憶装置は RAID 構成により信頼性を向上させている。記憶装置は、ホストから LU(Logical Unit)の単位で認識され、LU 内にユーザデータが格納される。

(6) 管理用コンピュータ

ディスクアレイ装置設定用プログラムである Hitachi Storage Navigator Modular 2 が導入されたコンピュータである。本機器は管理用コンピュータ（GUI）と管理用コンピュータ（CLI）を兼ねている。また、本機器には Hitachi Storage Navigator Modular2（for GUI）と（for CLI）を共存させる（HSNM2（for GUI）が導入されている場合は JRE も導入されている）。本機器を操作するのは後述する管理者（ディスクアレイ管理者、アカウント管理者、監査ログ管理者）もしくは保守員である。

(7) 保守員用コンピュータ

本機器は保守作業を行うために使用するコンピュータである。ディスクアレイ装置設定用プログラムである Hitachi Storage Navigator Modular 2 が導入されており、このプログラムを用いて保守作業を行う。本機器には Hitachi Storage Navigator Modular2（for GUI）と（for CLI）を共存させる。また、Web ブラウザによってディスクアレイ装置の Web メンテナンス画面にアクセスし、保守作業を行う。本機器を操作するのは保守員であり、保守作業を行う場合のみ管理用 LAN に接続される。

(8) Hitachi Storage Navigator Modular 2

ディスクアレイ装置設定用プログラムであり、ディスクアレイ装置の構成設定と表示、情報の表示及び障害を監視するために使われる。Web ベースの GUI である Hitachi Storage Navigator Modular 2 (for GUI)と、コマンドラインインタフェースである Hitachi Storage Navigator Modular 2 (for CLI)の 2 種類を総称している。本 TOE の設定操作が可能なのはバージョン 6.20 以降のものである。

なお、本プログラムは TOE には含まれない。

(9) ホスト

ディスクアレイ装置に接続され、ディスクアレイ装置のユーザデータの領域を利用するオープン系サーバである。本機器を利用するのは後述するホスト利用者である。RAID Manager の導入が可能である。

なお、本機器からディスクアレイ装置の制御情報（後述する保護対象資産）へは、RAID Manager を除いてアクセスできない。

(10) RAID Manager

ディスクアレイ装置の装置制御情報の管理を行うために使用する、ホスト上で動作するソフトウェアである。本 ST では RAID Manager を使用していない装置構成を対象とする（RAID Manager を使用するには、Hitachi Storage Navigator Modular 2 にて事前にディスクアレイ装置に設定を行う必要がある

が、本 ST ではそのような設定がなされていない環境を想定している)。本プログラムは TOE には含まれない。

2.3.1. TOE のハードウェア構成

本評価にて検証した TOE のハードウェア構成を下表に示す。

表 4 ハードウェアの構成

構成要素	説明
ディスクアレイ装置	Hitachi Adaptable Modular Storage 2300
ホスト	■Windows ・OS: Windows Server 2003 (R2) ・CPU: Xeon 2.8GHz ・メモリ: 1 GB ・Host Bus Adapter(Fibre Channel接続用として)
管理用コンピュータ	本機器は、管理用コンピュータ(GUI)、(CLI)を兼ねる。そのため、これらの動作環境を全て満たす構成とする。以下を参照。 ■Windows ・OS: Windows Vista ・CPU: AMD Opteron 2GHz ・メモリ: 2 GB ・ディスク空き容量: 200 GB 以上
保守員用コンピュータ	上記「管理用コンピュータ」に同じ。

2.3.2. TOE のソフトウェア構成

本評価にて検証した TOE のソフトウェア構成を下表に示す。

表 5 ソフトウェアの構成

構成要素	説明
マイクロプログラム	バージョン: 0862/A-M (ただし、有償オプションはAccount Authentication、Audit Loggingのみ提供)
リアルタイムOS	パッケージ名:WindRiver Platform for Network Equipment, Vxworks Edition 3.5 (旧:Tornado) OS:VxWorks 6.5 Web: Wind River CLI,Web,MIBway 4.6 (旧:WindManageWeb) Security: WindRiver Security Library 1.3 SSL: Wind River SSL 1.3 (OpenSSL:version 0.9.8a)
Hitachi Storage Navigator Modular 2 (for GUI)	バージョン: 6.20
Hitachi Storage Navigator Modular 2 (for CLI)	バージョン: 6.20
管理用コンピュータのOS	詳細は表4の「管理用コンピュータ」参照。
Webブラウザ(HSNM2)	Internet Explorer 7.0
Webブラウザ(Webメンテナンス画面)	Internet Explorer 7.0
Javaランタイム環境	Java6.0 Update10(1.6.0_10)

2.4. TOE の関与者

本 TOE には、下記の人物が関与する。

(1) ディスクアレイ管理者

管理用コンピュータからHitachi Storage Navigator Modular 2を操作し、ディスクアレイ装置の管理を行う人物。

この人物には、少なくとも Storage Administrator (View and Modify)のロールが割り振られる。

(2) アカウント管理者

管理用コンピュータから Hitachi Storage Navigator Modular 2 を操作し、ディスクアレイ管理者、アカウント管理者、監査ログ管理者のアカウントの管理を行う人物。TOE の機能である Account Authentication 機能を使用してアカウントの作成、変更、削除が可能である。

この人物には、少なくとも Account Administrator (View and Modify)のロールが割り振られる。

(3) 監査ログ管理者

管理用コンピュータからHitachi Storage Navigator Modular 2を操作し、ディスクアレイ装置で取得している監査ログを管理する人物。TOEの機能であるAudit Logging機能を使用して監査ログの設定（ログ取得の有効、無効）や消去に関する設定が可能である。

この人物には、少なくとも Audit Log Administrator (View and Modify)のロールが割り振られる。

(4) 保守員

ディスクアレイ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物。保守員専用のマニュアルを使用し、保守作業（ディスクアレイ装置を設置する際の初期立上げ、部品の交換や追加などに伴う設定変更、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、上記の管理者が行う設定作業を代行する場合もある。保守作業を行う際は、Hitachi Storage Navigator Modular 2とWebメンテナンス画面（Webブラウザでディスクアレイ装置のIPアドレスを入力すると表示される画面）を使用する。Hitachi Storage Navigator Modular2 を使用する場合、保守員は顧客のアカウント管理者から何らかの管理者ロールを割り当てられ、その権限の範囲内の管理操作を行う。Webメンテナンス画面を使用する場合、操作は保守員のみが行うため管理者ロールの権限は不要で、後述する識別認証と監査ログの取得は行わない。

本 ST では上記(1)～(4)の人物を総称して管理者と呼ぶ場合がある。

(5) ホスト利用者

ディスクアレイ装置に接続されたホストを利用する人物。ホストから、ディスクアレイ装置の記憶領域に対してデータの読み書きが行われる。なお、この人物はディスクアレイ装置の管理は行わない。

2.5. 保護対象資産

ディスクアレイ装置にはホスト利用者にとって重要なデータが保管される。このため、それらデータの完全性や機密性が損なわれるようなディスクアレイ装置の設定変更が行われないよう、管理者毎に設定可能な操作を限定する必要がある。よって、本 ST ではディスクアレイ装置に記録されるホスト利用者のデータの完全性、機密性に影響する設定が不正に行われないよう、マイクロプログラムの一般機能設定パラメータを保護対象資産とし、特定の管理者が限定された範囲内で設定変更を行えるよう制御を行う。

以下に一般機能として設定が可能な項目を示す。

- RAID グループの作成・削除・参照、LU の作成・削除・参照
- ホストへの LU の割り当て（ホストアクセス制御の設定）
- ディスクアレイ装置の構成情報（IP アドレス、ポート番号、ドライブ復旧時の動作設定等）の設定
- Audit Logging機能とAccount Authentication機能以外の有償オプションの設定（解錠、施錠、有効、無効）。

2.6. TOE の論理的範囲

TOE が提供する一般的な IT 機能、およびセキュリティ機能の概要を以下に示す。

2.6.1. TOE の一般機能

マイクロプログラムは、ディスクアレイ装置の動作を制御するソフトウェアで、ホストとディスクアレイ装置間のデータ転送と、キャッシュメモリと記憶装置間のデータ転送を制御する。

2.6.2. TOE のセキュリティ機能

TOE では、ディスクアレイ装置の操作を行う人物に対して管理者ロールが割り当てられる。管理者ロールは Account Administrator (View and Modify)、Account Administrator (View Only)、Audit Log Administrator (View and Modify)、Audit Log Administrator (View Only)、Storage Administrator (View and Modify)、Storage Administrator (View Only)の 6 種類があり、Hitachi Storage Navigator Modular 2 の操作者は少なくともこのうち 1 つのロールが割り振られる。

本 ST では、Account Administrator (View and Modify)が割り振られている操作者をアカウント管理者と、Audit Log Administrator (View and Modify)が割り振られている操作者を監査ログ管理者と、Storage Administrator (View and Modify)が割り振られている操作者をディスクアレイ管理者として取り扱う。なお、操作者は複数のロールを兼ね備える場合がある。各々の View and Modify と View Only の違いは、設定操作が行えるか、それとも許可された範囲の設定情報（ディスクアレイ装置の設定パラメータを格納しているテーブル）の閲覧が許可されているか、という点である。

TOE は、セキュリティ機能として以下の機能を提供する。

(1)Account Authentication 機能

当機能は以下の機能から構成される。

【識別・認証】

マイクロプログラムは、操作者がディスクアレイ装置の設定を行う際に操作者の識別・認証要求を受け付けると、登録済みのアカウント情報（ユーザ ID、パスワード）と入力値を比較する。それらが合致し、かつ当該アカウントに対し「アカウント無効」属性が設定されていない場合に識別・認証を成功とする。

また、識別・認証に成功すると当該アカウントに対応したセッション ID を発行し、Hitachi Storage Navigator Modular 2 に配付する。ディスクアレイ装置を管理する際に Hitachi Storage Navigator Modular 2 は操作コマンドとセッション ID をあわせてディスクアレイ装置に送信する。マイクロプログラムはセッション ID が発行されたものと一致した場合に、当該アカウントをセッション ID と関連付けられる操作者と判断し、下記のロールによる実行制御を実施する。

【ロールによる実行制御】

セッション ID の確認に成功した場合、当該アカウントに付与されたロールが受信したコマンドの実行を許可している場合に限り、当該コマンドを実行する。アカウントに付与されたロールがコマンド実行を許可していない場合には実行されない。

【タイムアウト機能】

一定時間操作が行われない場合には、当該セッション ID を無効とする。

【アカウント管理】

マイクロプログラムは、アカウント毎のユーザ ID、パスワード、アカウント無効属性、ロールの対応をアカウント情報として管理する。また、アカウント情報の設定管理を行う手段を提供する。

(2)Audit Logging 機能

当機能は以下の機能から構成される。

【監査ログの取得】

マイクロプログラムは、管理者のログイン成功／失敗など、TOE 内のセキュリティ機能に関する監査事象発生時に、その事象の監査ログを取得（生成・保存）する。また、監査ログの取得の有効／無効設定を行う手段を提供する。

【監査ログの消去】

マイクロプログラムは、監査ログの消去（全監査ログの一括消去）を行う手段を提供する。

(3)設定機能

マイクロプログラムは、Account Authentication 機能、Audit Logging 機能を有効化もしくは無効化する手段を提供する。

以下に管理者とセキュリティ機能の設定項目の関係を示す。

表 6 セキュリティ機能の設定項目

セキュリティ機能		セキュリティ機能の設定項目	実行可能な管理者
Account Authentication 機能	アカウント管理	・アカウントの作成（ユーザ ID、パスワード、ロール割当）、変更、削除、参照	アカウント管理者
Audit Logging 機能	監査ログの生成	・監査ログ取得の有効無効設定	監査ログ管理者
	監査ログの消去（全監査ログの一括消去）	・監査ログ消去設定	監査ログ管理者
設定機能		・Account Authentication 機能の有効/無効化	アカウント管理者
		・Audit Logging 機能の有効/無効化	監査ログ管理者

3. TOE セキュリティ環境

本章では、TOE のセキュリティ環境を規定する。

3.1. 前提条件

本 TOE は、以下の前提条件の下で利用されることを想定する。

A.Administrator

ディスクアレイ管理者、アカウント管理者、監査ログ管理者はディスクアレイ装置の管理操作を行うために充分な能力を持つ信頼できる人物であり、ディスクアレイ装置のセキュリティに支障をきたす操作・設定を故意に行うことは無いものと想定する。

A.CustomerEngineer

保守員は、ディスクアレイ装置の保守作業全般を安全に行うために充分な能力・知識をもち、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人物であると想定する。

A.Environment

本 TOE の利用環境として下記を想定する。

・ディスクアレイ装置、ホスト、および両者を接続する FC-SAN は、ディスクアレイ管理者、アカウント管理者、監査ログ管理者、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こと。

・FC-SAN はディスクアレイ装置とホストを接続する目的のみに使用され、FC-SAN が他のネットワークに接続されたり、他の用途に利用されたりしないこと。

・ホストのアカウント管理は適切に行われ、ホスト利用者以外の第三者が不正にホストを利用することが出来ないこと。

・管理用 LAN はファイアウォール等によってインターネット等の外部ネットワークから直接アクセスされない構成となっていること。

・管理用コンピュータ、保守員用コンピュータは不正なプログラム（キーロガー等のマルウェア）がインストールされたり、コンピュータウィルスに感染したりすることが無いよう適切な管理が行われること。

・TOE が動作するディスクアレイ装置において RAID Manager が使用できない設定となっていること

・Account Authentication 機能のアカウントのパスワードは、半角文字のうち、数字、アルファベット、記号（!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ のいずれか）を組み合わせた文字列とすること。

・管理用 LAN を通じて管理者がディスクアレイ装置にアクセスする際には、Hitachi Storage Navigator Modular 2 のみを使用し、Hitachi Storage Navigator Modular 2 が生成しないような変則的パケットによるアクセスが行われないこと（ただし、保守員が Web ブラウザから Web メンテナンス画面へのアクセスすることは許可する）。

・保守作業において、Web ブラウザからアクセスする Web メンテナンス画面において、設定操作（装置の時刻設定等）の手順は保守員だけに提供される安全が保証された作業であること。また、保守員以外の管理者が Web メンテナンス画面での設定操作ができないこと。

・保守員用コンピュータは保守作業を行う場合のみ管理用 LAN に接続され、それ以外は保守員が本コンピュータへ許可されない物理的なアクセスが行われないよう管理すること。

A.SSL

Hitachi Storage Navigator Modular 2 と、ディスクアレイ装置間の通信路は、改ざんおよび暴露から保護されているものと想定する。

3.2. 脅威

以下の記載の中で第三者とはディスクアレイ管理者、アカウント管理者、監査ログ管理者、保守員、ホスト利用者のいずれにも該当しない人物であり、ディスクアレイ装置の操作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.MaliciousClient

第三者が管理されていないコンピュータ（OA 用コンピュータ）を使用し、管理用コンピュータ（GUI）の Hitachi Storage Navigator Modular2（for GUI）にアクセスして、ディスクアレイ装置にログインし TOE の設定値（マイクロプログラムの管理情報設定パラメータ）を変更してしまうかもしれない。

T.MaliciousApplication

第三者が Hitachi Storage Navigator Modular2 を不正に入手し、管理されていないコンピュータ（OA 用コンピュータ）にインストールを行い、管理用 LAN に接続後、不正にログインしディスクアレイ装置の TOE の設定値（マイクロプログラムの管理情報設定パラメータ）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

本 TOE に適用される組織のセキュリティ方針は以下の事項である。

P.Role

ディスクアレイ装置の設定操作に際し、操作者が行える管理操作をその操作者のアカウントに設定されたロールに基づいて制限すること。その際に、管理操作の事象を記録すること。

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規定する。

4.1. TOE のセキュリティ対策方針

以下に TOE のセキュリティ対策方針を示す。

O.I&A

TOE は、操作者がディスクアレイ装置の管理操作を行う前に、必ず操作者を識別・認証しなければならない。

O.Log

TOE は、操作者の識別認証の事象、管理操作より生じた一般機能設定パラメータ変更またはディスクアレイ装置の状態変更に関する事象を記録しなければならない。また、 TOE は監査ログ管理者に対してのみ監査ログを消去する機能を提供しなければならない。

O.Role

TOE は、操作者が行える管理操作を、その操作者のアカウントに設定されたロールに基づいて制限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

本節では、TOE の環境に対して要求される対策方針を示す。

4.2.1. IT 環境のセキュリティ対策方針

以下に IT 環境に対して要求されるセキュリティ対策方針を示す。

OE.SSL

Hitachi Storage Navigator Modular 2 とディスクアレイ装置間の通信路は、IT 環境が提供する SSL 機能を利用して改ざんおよび暴露から保護しなければならない。

4.2.2. Non-IT 環境のセキュリティ対策方針

以下に Non-IT 環境に対して要求されるセキュリティ対策方針を示す。

OE.Administrator

ディスクアレイ管理者、アカウント管理者、監査ログ管理者には、信頼できる人物を割り当てなければならない。また、その人物に対して適宜教育を行い、セキュリティに支障をきたす操作・設定を故意に行わないよう、徹底しなければならない。

OE.CustomerEngineer

保守員には、ディスクアレイ装置の保守作業全般を安全に行うために充分な能力・知識をもち、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人物を割り当てなければならない。

OE.Environment

本 TOE は以下を満足する環境で利用しなければならない。

・ディスクアレイ装置、ホスト、および両者を接続する FC-SAN は、ディスクアレイ管理者、アカウント管理者、監査ログ管理者、保守員のみに入退出を許可したセキュアなエリアに設置し、許可されない物理的アクセスから完全に保護しなければならない。
・FC-SAN はディスクアレイ装置とホストを接続する目的のみに使用しなければならず、また FC-SAN を他のネットワークに接続したり、他の用途に利用したりしてはならない。
・ホスト利用者以外の第三者が不正にホストを利用出来ないよう、ホストのアカウント管理を適切に行わなければならない。
・管理用 LAN とインターネット等の外部ネットワークを接続する際にはファイアウォール等によって外部ネットワークから直接アクセス出来ないようにしなければならない。
・管理用コンピュータ、保守員用コンピュータは不正なプログラム（キーロガー等のマルウェア）がインストールされたり、コンピュータウィルスに感染したりすることが無いよう適切に管理を行わなければならない。
・TOE が動作するディスクアレイ装置では RAID Manager を使用できる設定としてはならない。
・Account Authentication 機能のアカウントのパスワードは、半角文字のうち、数字、アルファベット、記号（!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~ のいずれか）を組み合わせた文字列としなければならない。
・管理用 LAN を通じてディスクアレイ装置にアクセスする際には、Hitachi Storage Navigator Modular 2 が生成しないような変則的パケットによるアクセスが行われないようにしなければならない。
・保守作業において、Web メンテナンス画面での設定操作（装置の時刻設定等）は、事前にディスクアレイ装置上のハードスイッチの操作がなければ実施することができないようにしなければならない。また、そのハードスイッチの操作方法は保守員だけに提供され、保守員以外の管理者が Web メンテナンス画面での設定操作を行うことがないようにしなければならない。
・保守員用コンピュータは保守作業を行う場合のみ管理用 LAN に接続され、それ以外は保守員が本コンピュータへ許可されない物理的なアクセスが行われないよう管理しなければならない。

5. IT セキュリティ要件

本章では、TOE またはその環境が満たしていなければならない IT セキュリティ要件を定義する。
なお、セキュリティ要件に対して詳細化を行った場合には[ ]で括った上、下線を引いてその箇所を示す。

5.1. TOE セキュリティ要件

本節では、TOE セキュリティ要件について記述する。

5.1.1. TOE セキュリティ機能要件

本項で利用しているすべての機能要件コンポーネントは CC パート 2 で規定されているものである。

(1) クラス FAU:セキュリティ監査

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ログ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、各監査ログ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]

依存性: FPT_STM.1 高信頼タイムスタンプ

[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]
下表に示す項目

表 7 監査対象事象

機能要件	予見される監査対象事象	監査記録項目
FAU_GEN.1	なし	-
FAU_GEN.2	なし	-
FAU_STG.1	なし	-
FAU_STG.4	a) 基本: 監査格納失敗によってとられるアクション。	なし
FDP_ACC.1	なし	-
FDP_ACF.1	a) 最小: SFPで扱われるオブジェクトに対する操作の実行における成功した要求。 b) 基本: SFPで扱われるオブジェクトに対する操作の実行におけるすべての要求。 c) 詳細: アクセスチェック時に用いられる特定のセキュリティ属性。	管理操作により生じた一般機能パラメータ変更またはディスクアレイ装置状態(表8に示すオブジェクトの各テーブルに格納されるパラメータ)の変更時にその実行結果(成功、失敗)と操作事象を記録する。
FIA_ATD.1	予見される監査対象事象はない。	-

FIA_SOS.1	a) 最小:TSFによる、テストされた秘密の拒否; b) 基本: TSFによる、テストされた秘密の拒否または受け入れ; c) 詳細: 定義された品質尺度に対する変更の識別。	なし
FIA_UAU.2	最小: 認証メカニズムの不成功になった使用; 基本: 認証メカニズムのすべての使用。	基本:識別認証試行時に、その実行結果(成功、失敗)と識別認証の試みを記録する。
FIA_UID.2	a) 最小: 提供される操作者識別情報を含む、操作者識別メカニズムの不成功使用; b) 基本: 提供される操作者識別情報を含む、操作者識別メカニズムのすべての使用。	b)識別認証試行時に、その実行結果(成功、失敗)と識別認証の試みを記録する。
FIA_USB.1	a) 最小: 利用者セキュリティ属性のサブジェクトに対する不成功結合(例えば、サブジェクトの生成)。 b) 基本: 利用者セキュリティ属性のサブジェクトに対する結合の成功及び失敗(例えば、サブジェクトの生成の成功または失敗)。	なし
FMT_MOF.1	a) 基本: TSFの機能のふるまいにおけるすべての改変。	以下の操作の実行時に、その実行結果(成功、失敗)と操作事象を記録する。 ・Account Authentication機能の解錠、施錠、有効化(成功のみ)、無効化(成功のみ) ・Audit Logging機能の解錠(成功のみ)、施錠、有効化(成功のみ)、無効化(成功のみ)
FMT_MSA.1	a) 基本: セキュリティ属性の値の改変すべて。	以下の操作の実行時に、その実行結果(成功、失敗)と操作事象を記録する。 ・ロール(割当て)の改変(ただし、「アカウント設定」の操作事象として記録する)
FMT_MTD.1	a) 基本:TSFデータの値のすべての改変。	以下の操作の実行時に、その実行結果(成功、失敗)と操作事象を記録する。 ・ユーザIDの削除/作成、すべてのパスワードの改変/削除/作成、自分自身のパスワードの改変(ただし、これらは「アカウント設定」の操作事象として記録する) ・タイムゾーンの改変 ・セッションIDの削除(強制ログアウト) ・アカウント無効属性の改変(アカウント有効、無効(ただし、これらは「アカウント設定」の操作事象として記録する))
FMT_SMF.1	a) 最小:管理機能の使用	他のFMTクラスの機能要件に対応する事象(以下参照)を記録する。 ・Account Authentication機能の解錠、施錠、有効化(成功のみ)、無効化(成功のみ) ・Audit Logging機能の解錠(成功のみ)、施錠、有効化(成功のみ)、無効化(成功のみ) ・ロール(割当て)の改変(ただし、「アカウント設定」の操作事象として記録する) ・ユーザIDの削除/作成、すべてのパスワードの改変/削除/作成、自分自身のパスワードの改変(ただし、これらは「アカウント設定」の操作事象として記録する) ・タイムゾーンの改変 ・セッションIDの削除(強制ログアウト) ・アカウント無効属性の改変(アカウント有効、無効(ただし、これらは「アカウント設定」の操作事象として記録する))
FMT_SMR.1	a) 最小: 役割の一部をなす操作者のグループに対する改変; b) 詳細: 役割の権限の使用すべて。	なし。
FPT_RVM.1	なし。	-

FPT_SEP.1	なし。	-
FPT_STM.1	a) 最小: 時刻の変更; b) 詳細: タイムスタンプの提供。	なし。
FTA_SSL.3	a) 最小: セッションロックメカニズムによる対話セッションの終了。	セッションタイムアウト時にセッションの終了を記録する。
FTA_TSE.1	a) 最小: セッション確立メカニズムによるセッション確立の拒否。 b) 基本: 操作者セッション確立におけるすべての試み。 c) 詳細: 選択されたアクセスパラメタ(例:アクセスの場所、アクセスの日時)の値の取得。	a)識別認証試行時に、その実行結果(成功、失敗)と、セッション確立の試みを記録する。

[割付: その他の監査関連情報]
なし

FAU_GEN.2 操作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、その原因となった操作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

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、格納された監査ログ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ログへの不正な改変を[選択: 防止、検出: から一つのみ選択]できねばならない。

依存性: FAU_GEN.1 監査データ生成

[選択: 防止、検出: から一つのみ選択]
防止

FAU_STG.4 監査データ損失の防止
下位階層: FAU_STG.3

FAU_STG.4.1 TSF は、監査証跡が満杯になった場合、[選択: 監査対象事象の無視、特権を持つ許可操作者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査ログへの上書き: から一つのみ選択]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]を行わねばならない。

依存性: FAU_STG.1 保護された監査証跡格納

[選択: 監査対象事象の無視、特権を持つ許可操作者に関わるもの以外の監査対象事象の抑止、最も古くに格納された監査ログへの上書き: から一つのみ選択]
最も古くに格納された監査ログへの上書き
[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

(2) クラス FDP:利用者データ保護

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。

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

[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:操作者を代行するプロセス(マイクロプログラムの制御動作)
オブジェクト:
RAIDグループ/LU情報テーブル、LU割当て情報テーブル、構成情報テーブル、有償オプション情報テーブル(Audit Logging機能、Account Authentication機能除く)
操作:参照、変更
[割付: アクセス制御SFP]
ディスクアレイ装置SFP

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。

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

[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:操作者を代行するプロセス(マイクロプログラムの制御動作)

オブジェクト:

RAIDグループ/LU情報テーブル、LU割当て情報テーブル、構成情報テーブル、有償オプション情報テーブル(Audit Logging機能、Account Authentication機能除く)

サブジェクトの属性:ロール

オブジェクトの属性:なし

[割付: アクセス制御 SFP]

ディスクアレイ装置 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]

サブジェクトは、その属性(ロール)に基づいて、オブジェクトに対して下表に示す規則に従いアクセス制御を行う。

表 8 オブジェクトとサブジェクトの属性の関係

オブジェクト / サブジェクトの属性(ロール)	RAIDグループ/LU情報テーブル	LU割当て情報テーブル	構成情報テーブル	有償オプション情報テーブル(Audit Logging機能、Account Authentication機能除く)
Account Administrator (View and Modify)	×	×	×	○
Account Administrator (View Only)	×	×	×	○
Audit Log Administrator (View and Modify)	×	×	×	○
Audit Log Administrator (View Only)	×	×	×	○
Storage Administrator (View and Modify)	◎	◎	◎	◎
Storage Administrator (View Only)	○	○	○	○
オブジェクトに関係する設定操作の説明	以下に示すディスクアレイ装置の構成の設定。 ・RAIDグループ/LU情報テーブル: RAIDグループの作成・削除・参照、LUの作成・削除・参照 ・LU割当て情報テーブル: ホストへのLUの割り当て(ホストアクセス制御の設定) ・構成情報テーブル: ディスクアレイ装置の構成情報(ドライブ復旧時の動作設定、ベリファイ、LUフォーマットモード等)設定			以下に示す設定。 ・有償オプション情報テーブル: Audit Logging機能とAccount Authentication機能以外の有償オプションの設定(解錠、施錠、有効、無効)

◎:参照および変更が可能

○:参照のみ可能

×:権限なし

[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

(3) クラス FIA:識別と認証

FIA_ATD.1 利用者属性定義

下位階層: なし

FIA_ATD.1.1 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。

依存性: なし

[割付:セキュリティ属性のリスト]
ユーザ ID、セッション ID、ロール、アカウント無効

FIA_SOS.1 秘密の検証
下位階層: なし

FIA_SOS.1.1 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。

依存性: なし

[割付: 定義された品質尺度]
文字数: 6 文字以上

FIA_UAU.2 アクション前の利用者認証 （パスワードによる認証）
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。

依存性: FIA_UID.1 識別のタイミング

FIA_UID.2 アクション前の利用者識別 （ユーザ ID による識別）
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。

依存性: なし

FIA_USB.1 利用者・サブジェクト結合
下位階層: なし

FIA_USB.1.1 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.1.2 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.1.3 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]

依存性: FIA_ATD.1 利用者属性定義

[割付: 利用者セキュリティ属性のリスト]
ユーザ ID、セッション ID、ロール

[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

(4) クラス FMT:セキュリティ管理

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。

依存性: FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

本機能要件の割付、選択について次の表に示す。

表 9 FMT_MOF に関する操作

機能のリスト	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	許可された識別された役割
Account Authentication機能	を停止する、を動作させる	Account Administrator (View and Modify)
Audit Logging機能	を停止する、を動作させる	Audit Log Administrator (View and Modify)

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。

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

本機能要件の割付、選択について以下の表に示す。

表 10 FMT_MSA.1 に関する操作

セキュリティ属性のリスト	デフォルト値変更、問い合わせ、改変、削除、その他の操作	許可された識別された役割	アクセス制御SFP、情報フロー制御SFP
ロール	問い合わせ、改変	Account Administrator (View and Modify)	ディスクアレイ装置SFP
	問い合わせ	Account Administrator (View Only)	

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。

依存性:　　FMT_SMF.1 管理機能の特定
FMT_SMR.1 セキュリティ役割

本機能要件の割付、選択について以下の表に示す。

表 11 FMT_MTD.1 に関する操作

TSF データのリスト	デフォルト値変更、問い合わせ、改変、削除、消去、その他の操作	許可された識別された役割
ユーザ ID	問い合わせ、削除、その他の操作: 作成	Account Administrator (View and Modify)
	問い合わせ	Account Administrator (View Only)
すべてのパスワード	改変、削除、その他の操作:作成	Account Administrator (View and Modify)
自分自身のパスワード	改変	Account Administrator (View Only) Audit Log Administrator (View and Modify) Audit Log Administrator (View Only) Storage Administrator (View and Modify) Storage Administrator (View Only)
ログ	消去	Audit Log Administrator(View and Modify)
セッション ID	削除	Account Administrator（View and Modify）
アカウント無効	問い合わせ、改変	Account Administrator（View and Modify）
	問い合わせ	Account Administrator（View Only）

上表 11 の事象のうち、「ログ消去」の事象については、監査ログを記録しない。これは、「ログ消去」が、ディスクアレイ装置内部への監査ログの保存設定が「無効」（すなわち、全ての発生事象について監査ログを記録しない設定）の場合のみ実行可能であるという仕様による。

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]。

依存性:　　なし

本機能要件の割付について以下の表に示す。

表 12 FMT_SMF.1 に関する操作

機能要件	予見される管理アクティビティ	管理項目
FAU_GEN.1	なし	-
FAU_GEN.2	なし	-
FAU_STG.1	なし	-
FAU_STG.4	a) 監査格納失敗時にとられるアクションの維持(削除、改変、追加)。	a) なし。アクションは固定である。
FDP_ACC.1	なし	-
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。明示的な承認もしくは拒否する規則は存在しない。
FIA_MTD.1	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。セキュリティ属性は固定である。
FIA_SOS.1	a) 秘密の検証に使用される尺度の管理。	a) なし。尺度は固定である。
FIA_UAU.2	管理者による認証データの管理; このデータに関係する操作者による認証データの管理。	・Account Administrator (View and Modify)によるパスワードの作成および改変、削除、作成。 ・各ユーザによる自分自身のパスワードの改変。
FIA_UID.2	a) 操作者識別情報の管理。	a)・Account Administrator (View and Modify)によるユーザIDの作成、削除、問い合わせ。 ・Account Administrator (View Only)によるユーザIDの問い合わせ。
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。役割のグループは固定である。
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。役割のグループは固定である。
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。役割のグループは固定である。
FMT_SMF.1	なし	-
FMT_SMR.1	a) 役割の一部をなす操作者のグループの管理。	a) なし。役割の一部をなす操作者のグループは固定である。
FPT_RVM.1	なし	-
FPT_SEP.1	なし	-
FPT_STM.1	a) 時間の管理。	a)なし。保守員による保守作業としての時刻情報の改変のみを提供。
FTA_SSL.3	a) 個々の操作者に対し対話セッションの終了を生じさせる操作者が非アクティブである時間の特定; b) 対話セッションの終了を生じさせる操作者が非アクティブであるデフォルト時間の特定。	a)なし。 b)なし。デフォルト時間は固定である。
FTA_TSE.1	a) 許可管理者によるセッション確立条件の管理。	a) なし。セッション確立条件は固定である。

上記の他に以下の管理機能が存在する。

- Account Authentication機能の有効化、無効化
- Audit Logging機能の有効化、無効化
- セッションIDの削除
- アカウント無効属性の問い合わせ、改変
- ロールの問い合わせ、改変
- 監査ログの消去

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、操作者を役割に関連づけなければならない。

依存性: FIA_UID.1 識別のタイミング

[割付: 許可された識別された役割]
Account Administrator (View and Modify)
Account Administrator (View Only)
Audit Log Administrator (View and Modify)
Audit Log Administrator (View Only)
Storage Administrator (View and Modify)
Storage Administrator (View Only)

(5) クラス FPT:TSF の保護

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

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

(6) クラス FTA:TOE アクセス

FTA_SSL.3 TSF起動による終了
下位階層: なし

FTA_SSL.3.1 TSFは、[割付: 操作者が非アクティブである時間間隔]後に対話セッションを終了しなければならない。

依存性: なし

[割付: 操作者が非アクティブである時間間隔]
Account Administrator (View and Modify)が指定した時間。
20分、25分、30分、35分、40分、45分、50分、55分、60分、70分、80分、90分、100分、110分、120分、24時間、のいずれかとする。

FTA_TSE.1 TOEセッション確立
下位階層: なし

FTA_TSE.1.1 TSFは、[割付: 属性]に基づきセッション確立を拒否できなければならない。

依存性: なし

[割付: 属性]
アカウント無効

5.1.2. 最小機能強度

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に基づくセキュリティ機能要件は、FIA_UAU.2 である。

5.1.3. TOE セキュリティ保証要件

本 TOE の評価保証レベルは EAL2 である。すべての保証要件コンポーネントは CC part3 で規定されている EAL2 のコンポーネントを直接使用する。本 TOE に適用されるセキュリティ保証要件を下表に示す。

表 13 TOE セキュリティ保証要件

保証クラス	保証コンポーネント	
構成管理(ACM)	ACM_CAP.2	構成要素
配付と運用(ADO)	ADO_DEL.1	配付手続き
	ADO_IGS.1	設置、生成、及び立上げ手順
開発(ADV)	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
ガイダンス文書 (AGD)	AGD_ADM.1	管理者ガイダンス
	AGD_USR.1	利用者ガイダンス
テスト(ATE)	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
脆弱性評定 (AVA)	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

本節では、IT 環境が提供するセキュリティ機能要件について記述する。本節で利用しているすべての機能要件コンポーネントは、CC Part2 で規定されているものである。

FTP_ITC.1　　TSF間高信頼チャネル
下位階層:　　なし

FTP_ITC.1.1　TSFは、それ自身とリモート高信頼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及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、リモート高信頼IT製品]が、高信頼チャ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: 高信頼チャネルが要求される機能のリスト]のために、高信頼チャネルを介して通信を開始しなければならない。
依存性:　　なし

[選択: TSF、リモート高信頼IT製品]
　　リモート高信頼IT製品

[割付: 高信頼チャネルが要求される機能のリスト]
　　Hitachi Storage Navigator Modular 2を介したディスクアレイ装置に対するすべてのアクセス

6. TOE 要約仕様

本章では、TOE セキュリティ機能、セキュリティ機能強度、セキュリティ保証手段について記述する。

6.1. TOE セキュリティ機能

本節では、TOEセキュリティ機能について記述する。表 14に示すように、本節で説明するセキュリティ機能は、5.1.1項で記述したTOEセキュリティ機能要件を満足している。

表 14 TOE セキュリティ機能と TOE セキュリティ機能要件の対応

セキュリティ機能要件 / セキュリティ機能	FAU_GEN.1	FAU_GEN.2	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FIA_SOS.1	FIA_ATD.1	FIA_UAU.2	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MTD.1	FMT_SMF.1	FMT_SMR.1	FPT_RVM.1	FPT_SEP.1	FPT_STM.1	FTA_SSL.3	FTA_TSE.1
SF.Account_Authentication			○		○	○	○	○	○	○	○		○	○	○	○	○	○		○	○
SF.Audit_Logging	○	○		○										○	○		○	○	○		
SF.Configuration												○		○	○		○	○			

6.1.1. SF.Account_Authentication

SF.Account_Authentication は操作者が Hitachi Storage Navigator Modular 2 よりディスクアレイ装置の設定を行う際に操作者の識別・認証とその維持を行い、またアカウント管理に関する機能を提供する。また、SF.Account_Authentication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。

(1) 識別・認証

SF.Account_Authentication は、操作者がディスクアレイ装置の設定を行う際に Hitachi Storage Navigator Modular 2 からのユーザ ID、パスワードによる操作者の識別・認証要求を受け付けると、登録済みのアカウント情報（ユーザ ID、パスワード）と入力値を比較する。

ユーザ ID およびパスワードが入力値と合致し、かつ当該アカウントに対し「アカウント無効」属性が設定されていない場合に限り場合に識別・認証を成功と判断し、当該アカウントに対応したセッション ID を生成してユーザ ID、ロールと関連づける。生成したセッション ID は Hitachi Storage Navigator Modular 2 に配付する。

ディスクアレイ装置を管理する際に Hitachi Storage Navigator Modular 2 は操作コマンドとセッション IDをあわせてディスクアレイ装置に送信する。TSF はセッション ID が発行されたものと一致した場合に、当該アカウントのセッション ID と関連付けられる操作者と判断し、操作者を代行するプロセス（マイクロプログラムの制御動作）と提供されたセッション ID、ユーザ ID、ロールを関連づける。

SF.Account_Authentication は、Hitachi Storage Navigator Modular 2 からの操作者の識別・認証要求を受け付けたとき、SF.Account_Authentication が必ず実施されることを保証する。

（2） アカウント管理

SF.Account_Authentication は、アカウント毎のユーザ ID、パスワード、アカウント無効属性、ロールの対応をアカウント情報として管理する。SF.Account_Authentication は、操作者からの要求に応じて、ユーザ ID の問い合わせ、作成、削除、パスワードの作成、改変、削除（アカウント全体として削除）、アカウント無効属性およびロールの問い合わせ、改変、セッション ID の削除（強制ログアウト）の操作を行う手段を提供する。

SF.Account_Authentication は、Account Administrator (View and Modify)のロールを持つ操作者に対して上記の全ての操作を許可し、Account Administrator (View Only)のロールを持つ操作者には上記属性の問い合わせのみ許可する。それ以外の操作者については自分自身のパスワード改変の操作のみ許可する。

SF.Account_Authentication は、パスワードが作成、あるいは改変される際には、文字数が 6 文字以上であるという品質尺度を満たしているかどうかの確認を行い、品質尺度を満たさないパスワードの設定を認めない。

SF.Account_Authentication は、セキュリティ属性であるユーザ ID、セッション ID、ロール、アカウント無効の各属性を維持する。

（3） セッションタイムアウト機能

SF.Account_Authentication は、Hitachi Storage Navigator Modular 2 からのログイン後一定時間無操作の場合、つまり一定時間セッション ID の確認が行われない場合にセッションをタイムアウトとし、再度の識別・認証を要求する。セッションタイムアウト時間として指定できる値は、20 分、25 分、30 分、35 分、40 分、45 分、50 分、55 分、60 分、70 分、80 分、90 分、100 分、110 分、120 分、24 時間のいずれかである。

（4） ロールによる実行制御

SF.Account_Authenticationは、セッションIDに関連付いたアカウントに付与されたロールが受信したコマンドの実行を許可している場合に限り、当該コマンドの実行を許可し、関連するマイクロプログラムの一般機能設定パラメータにアクセスする。テーブルとロールの関係は表 8に示す。

（5） 監査ログへのアクセス制限

SF.Account_Authentication は、Audit Log Administrator (View and Modify)のロールを持つ操作者に対してのみ監査ログの消去（全監査ログの一括削除）を許可する。これにより、監査ログが不正な改変、削除から保護されることを保証する。

6.1.2. SF.Audit_Logging

SF.Audit_Logging は、以下の監査機能を有する。SF.Audit_Logging 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。

（1） 監査ログの生成

SF.Audit_Loggingは、TOE内のセキュリティ機能に関する監査事象発生時に監査ログを生成する。ログの対象となる監査対象事象は表 7　監査対象事象に示した通りである。生成する監査ログには、各監査対象事象の原因となったアカウントのユーザIDを付与する。また、監査ログ生成時に使用する日時に関しては、ディスクアレイ装置のOSが管理している時刻を元にして監査ログを生成する。

SF.Audit_Logging は、監査対象事象が発生した場合に SF.Audit_Logging が必ず実施されることを保証する。

（2） 監査ログの保存

SF.Audit_Logging は、ディスクアレイ装置の内部に 2,048 件までの監査ログを保存する。監査ログが 2,048 件を超過する場合、最も古い監査ログを消去し、新たに発生した監査ログを上書きする。

6.1.3. SF.Configuration

SF.Configuration は、Account Authentication 機能（SF.Account_Authentication の全ての機能）、Audit Logging 機能（SF.Audit_Logging の全ての機能）を有効化もしくは無効化する手段を提供する。SF.Configuration 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。

Account Authentication 機能の有効/無効の設定は Account Administrator (View and Modify)のみに、Audit Logging 機能の有効/無効の設定は Audit Log Administrator (View and Modify)のみが可能である。

SF.Configuration は、上記設定に関する要求を受け付けたとき、SF.Configuration が必ず実施されることを保証する。

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.Account_Authentication である。これらセキュリティ機能のパスワードに関する機能が、機能強度レベル SOF-基本を持つ。

6.3. 保証手段

表 15に本TOEに適用するセキュリティ保証要件とセキュリティ保証手段の対応を示す。

表 15 TOE セキュリティ保証手段

セキュリティ保証要件	セキュリティ保証手段
ACM_CAP.2 構成要素	・Hitachi Adaptable Modular Storage2300 構成管理リスト ・Hitachi Adaptable Modular Storage2300 バージョン付与規則
ADO_DEL.1 配付手続き	・Hitachi Adaptable Modular Storage2300 配付手順説明書
ADO_IGS.1 設置、生成、及び立上げ手順	・Hitachi Adaptable Modular Storage2300 ISO/IEC15408認証取得機能 取扱説明書(保守員編)
ADV_FSP.1 非形式的機能仕様	・Hitachi Adaptable Modular Storage2300 機能仕様書
ADV_HLD.1 記述的上位レベル設計	・Hitachi Adaptable Modular Storage2300 上位レベル設計書
ADV_RCR.1 非形式的対応の実証	・Hitachi Adaptable Modular Storage2300 表現対応分析書
AGD_ADM.1 管理者ガイダンス	・Hitachi Adaptable Modular Storage2300 ISO/IEC15408認証取得機能 取扱説明書(管理者編)
AGD_USR.1 利用者ガイダンス	・Hitachi Adaptable Modular Storage2300 ISO/IEC15408認証取得機能 取扱説明書(利用者編)
ATE_COV.1 カバレージの証拠	・Hitachi Adaptable Modular Storage2300 テスト分析書
ATE_FUN.1 機能テスト	・Hitachi Adaptable Modular Storage2300 テスト仕様書
ATE_IND.2 独立試験 － サンプル	・Hitachi Adaptable Modular Storage2300 テスト仕様書 ・TOE
AVA_SOF.1 TOEセキュリティ機能強度評価	・Hitachi Adaptable Modular Storage 2300 機能強度分析書
AVA_VLA.1 開発者脆弱性分析	・Hitachi Adaptable Modular Storage 2300 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

本章では、セキュリティ対策方針根拠、セキュリティ要件根拠、TOE 要約仕様根拠について示す。

8.1. セキュリティ対策方針根拠

本節では、セキュリティ対策方針の根拠を示す。

セキュリティ対策方針は、TOEセキュリティ環境で規定した脅威に対抗し、前提条件と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抗する脅威、実現する前提条件及び組織のセキュリティ方針の対応関係を表 16に示す。下表より、各セキュリティ対策方針は1つ以上の前提条件、脅威、または組織のセキュリティ方針に対応していることは明白である。

表 16 セキュリティ対策方針と TOE セキュリティ環境の対応

セキュリティ対策方針 / セキュリティ環境	TOE			IT環境	Non-IT環境		
	O.I&A	O.Log	O.Role	OE.SSL	OE.Administrator	OE.CustomerEngineer	OE.Environment
A.Administrator					○		
A.CustomerEngineer						○	
A.Environment							○
A.SSL				○			
T.MaliciousClient	○	○					
T.MaliciousApplication	○	○					
P.Role		○	○				

次に、各脅威がセキュリティ対策方針で対抗できること、また前提条件・組織のセキュリティ方針がセキュリティ対策方針で実現できることを示す。

(1) 前提条件

A.Administrator

本前提条件は、OE.Administrator にあるようにディスクアレイ管理者、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ことによって実現できる。また、その人物に対して教育することにより、セキュリティに支障を及ぼす設定や操作を行う可能性を排除できる。

A.CustomerEngineer

本前提条件は、OE.CustomerEngineer にあるように保守員として充分な能力を持ちかつ不正行為をはたらかないことを信頼できる人物を割り当てることによって実現できる。

A.Environment

本前提条件は、OE.Environment にあるようにディスクアレイ装置、ホスト、および両者を接続する FC-SAN を物理的に保護すること、FC-SAN をディスクアレイ装置とホスト間の接続専用とすること、

ホストをホスト利用者のみが利用できるように管理すること、管理用 LAN と外部ネットワークとの間にファイアウォール等を設置し通信を制御すること、管理用コンピュータ・保守員用コンピュータに不正なプログラムが混入しないよう管理すること、ディスクアレイ装置を RAID Manager が使用できない設定とすること、Hitachi Storage Navigator Modular 2 が生成するパケットのみがアクセスを行うこと、保守作業において、Web メンテナンス画面での設定操作の手順は保守員にのみ公開されること（保守員以外の管理者が管理 LAN 上から偶然 Web メンテナンス画面へアクセスした場合に設定操作ができないよう、設定操作の手順に保守員だけが知るディスクアレイ装置の物理的な操作を含むこと）、保守員用コンピュータは保守作業を行う場合のみ管理用 LAN に接続され、それ以外は保守員が本コンピュータへ許可されない物理的なアクセスが行われないよう管理すること、により実現できる。

なお、Web メンテナンス画面の操作は保守員が行う安全の保証された保守作業であるため、識別認証と監査ログの取得は不要である。

A.SSL

本前提条件は、OE.SSL にあるように IT 環境が提供する SSL 機能を利用することにより実現できる。

(2) 脅威

T.MaliciousClient

本脅威は、O.I&A、O.Log によって除去される。

O.I&A により、運用環境に用意された HSNM2 からの接続要求であったとしても、操作を許可する前に操作者の識別・認証を行い、事前に登録された管理者以外の操作権限が与えられていない第三者によるログインは拒否されるため、不正な操作を防止することができる。

O.Log により、操作事象が発生した場合、操作者の情報とその事象の情報が監査ログとして必ず記録される。本脅威でブルートフォース攻撃など多量のアクセスが発生した場合、識別認証の監査ログが多量に記録されるため、異常を検知することができ、適切に対応することで攻撃を抑止することができる。ディスクアレイ装置内部に保存可能な監査ログの件数は 2048 件であるが、攻撃を検知には充分な件数である。また、監査ログを消去できるのは監査ログ管理者のみであり、この管理者は前提条件より信頼できる人物である。

T.MaliciousApplication

本脅威は、O.I&A、O.Log によって除去される。

O.I&A により、操作を許可する前に操作者の識別・認証を行い、事前に登録された管理者以外の操作権限が与えられていない第三者によるログインは拒否されるため、不正な操作を防止することができる。

O.Log により、操作事象が発生した場合、操作者の情報とその事象の情報が監査ログとして必ず記録される。本脅威でブルートフォース攻撃など多量のアクセスが発生した場合、識別認証の監査ログが多量に記録されるため、異常を検知することができ、適切に対応することで攻撃を抑止することができる。ディスクアレイ装置内部に保存可能な監査ログの件数は 2048 件であるが、攻撃を検知には充分な件数である。また、監査ログを消去できるのは監査ログ管理者のみであり、この管理者は前提条件より信頼できる人物である。

(3) 組織のセキュリティポリシー

P.Role

本組織のセキュリティポリシーは、O.Role にあるようにディスクアレイ装置の設定操作に際し、操作者が行える管理操作をその操作者のアカウントに設定されたロールに基づいて制限することによっ

て実現される。また、O.Log により管理操作の事象（一般機能設定パラメータ変更またはディスクアレイ装置の状態変更）を記録することによって実現される。

8.2. セキュリティ要件根拠

本節では、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

TOE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、およびIT環境のセキュリティ機能要件とIT環境のセキュリティ対策方針の対応関係を表 17に示す。下表より、TOEの各セキュリティ機能要件は 1 つ以上のTOEセキュリティ対策方針に対応しており、またIT環境の各セキュリティ機能要件は 1 つ以上のIT環境のセキュリティ対策方針に対応していることは明白である。

表 17 セキュリティ機能要件とセキュリティ対策方針の対応

セキュリティ対策方針 / セキュリティ機能要件		TOE			IT環境
		O.I&A	O.Log	O.Role	OE.SSL
TOE	FAU_GEN.1		○		
	FAU_GEN.2		○		
	FAU_STG.1		○		
	FAU_STG.4		○		
	FDP_ACC.1			○	
	FDP_ACF.1			○	
	FIA_ATD.1			○	
	FIA_SOS.1	○			
	FIA_UAU.2	○			
	FIA_UID.2	○			
	FIA_USB.1	○			
	FMT_MOF.1			○	
	FMT_MSA.1			○	
	FMT_MTD.1			○	
	FMT_SMF.1			○	
	FMT_SMR.1			○	
	FPT_RVM.1	○	○	○	
	FPT_SEP.1	○	○	○	
	FPT_STM.1		○		
	FTA_SSL.3	○			
	FTA_TSE.1	○			
環境	FTP_ITC.1				○

次に、各セキュリティ対策方針がセキュリティ機能要件によって実現できることを示す。

O.I&A

本 TOE セキュリティ対策方針は、FIA_SOS.1、FIA_UAU.2、FIA_UID.2、FIA_USB.1、FPT_RVM.1、FPT_SEP.1、FTA_SSL.3、FTA_TSE.1 によって実現される。

FIA_UAU.2、FIA_UID.2 により、TOE は Hitachi Storage Navigator Modular 2 からディスクアレイ装置の管理設定を行う前に必ず操作者の識別・認証を行い、成功しない限りディスクアレイ装置に対していかなる管理・設定操作も許可することはない。

FIA_USB.1 により、上記の識別・認証が成功した場合、操作者（を代行するプロセス）とユーザ ID、セッション ID、ロールを対応づけている。

FIA_SOS.1 により、TOE は認証に用いる秘密（パスワード）の品質尺度を維持する。
FTA_TSE.1 により、TOE はアカウントが無効となっていない操作者に対してのみセッションの確立を許可し、無効なアカウントによるログインを防止している。
FPT_RVM.1 により、TOE は管理設定操作が行われる際には必ずアカウント無効の確認を含む識別・認証機能、セッションタイムアウト機能が呼び出され成功することを保証する。
FPT_SEP.1 により TOE は、TSF の実行のため、信頼できないサブジェクトによる干渉と改ざんから TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。
FTA_SSL.3 により、TOE は操作者が非アクティブである時間間隔（Account Administrator（View and Modify）が指定した時間。20 分、25 分、30 分、35 分、40 分、45 分、50 分、55 分、60 分、70 分、80 分、90 分、100 分、110 分、120 分、24 時間のいずれか）後に操作者のセッションを終了させる。

O.Log

本 TOE セキュリティ対策方針は、FAU_GEN.1、FAU_GEN.2、FAU_STG.1、FAU_STG.4、FPT_RVM.1、FPT_SEP.1、FPT_STM.1 によって実現される。
FAU_GEN.1 により、TOE は決められた事象（操作者の識別認証の事象、管理操作より生じた一般機能設定パラメータ変更またはディスクアレイ装置の状態変更に関する事象）の監査ログを生成する。その際、TOE は FPT_STM.1 により時刻情報を取得し、また FAU_GEN.2 により、TOE はその事象を発生させた操作者のユーザ ID を監査ログに付与する。これにより監査対象事象とその発生日時、操作したユーザ ID を特定することが可能となる。
FAU_STG.1 により、TOE は監査ログへの不正な改変を防止する。
FAU_STG.4 により、TOE は監査ログが所定の最大数を超えた際に、最も古い監査ログを上書きして最新の監査対象事象が記録されない事態を防止する。
FPT_RVM.1 により、TOE は監査ログの作成・保護に関する機能が呼び出され成功することを保証する。
FPT_SEP.1 により、TOE は TSF の実行のため、信頼できないサブジェクトによる干渉と改ざんから TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。

O.Role

本 TOE セキュリティ対策方針は、FAU_STG.1、FDP_ACC.1、FDP_ACF.1、FIA_ATD.1、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1、FPT_RVM.1、FPT_SEP.1 によって実現される。
FMT_MOF.1 により、TOE はセキュリティ機能のふるまいの管理を行える操作者を特定の管理者に限定している。
FMT_MSA.1 により、TOE はセキュリティ属性の管理を行える操作者を特定の管理者に限定している。
FMT_MTD.1 により、TOE はセキュリティ機能のふるまいに影響を与える TSF データを管理できる操作者を特定の管理者に限定している。
FMT_SMF.1 により、TOE はディスクアレイ装置を操作する際のアカウント管理、時刻情報の管理といったセキュリティ機能に影響を与える設定を管理する為の機能を提供している。また、
FMT_SMR.1 により TOE はホスト、Account Administrator (View and Modify)、Account Administrator (View Only)、Audit Log Administrator (View and Modify)、Audit Log Administrator (View Only)、Storage Administrator (View and Modify)、Storage Administrator (View Only)の役

割を維持し、操作者と関連付けている。更に、FDP_ACC.1、FDP_ACF.1 により、操作者のロールに基づいて操作できるマイクロプログラムの一般機能設定パラメータを制限している。さらに、FIA_ATD.1 により、TOE は操作者のセキュリティ属性を維持している。
FPT_RVM.1 により、TOE はセキュリティ機能および一般機能の管理設定を行える操作者を限定する機能が呼び出され成功することを保証する。
FPT_SEP.1 により、TOE は TSF の実行のため、信頼できないサブジェクトによる干渉と改ざんから TSF を保護するためのセキュリティドメインを維持し、サブジェクトのセキュリティドメイン間の分離を実施する。

OE.SSL

本 IT 環境のセキュリティ対策方針は、FTP_ITC.1 によって実現される。
FTP_ITC.1 により、IT 環境は Hitachi Storage Navigator Modular 2 とディスクアレイ装置間の通信路を暴露、改変から保護されたものとする。

8.2.2. セキュリティ機能要件依存性

表 18にセキュリティ機能要件の依存性とその充足状況を示す。下表の通り、本STで利用した全てのセキュリティ機能要件が持つ依存性について充足されている。

表 18 セキュリティ機能要件の依存性

#	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で対応するセキュリティ機能要件
1	TOE	FAU_GEN.1	FPT_STM.1	#20
2	TOE	FAU_GEN.2	FAU_GEN.1	#1
			FIA_UID.1	#11※1
3	TOE	FAU_STG.1	FAU_GEN.1	#1
4	TOE	FAU_STG.4	FAU_STG.1	#3
5	TOE	FDP_ACC.1	FDP_ACF.1	#6
6	TOE	FDP_ACF.1	FDP_ACC.1	#5
			FMT_MSA.3	なし※2
7	TOE	FIA_ATD.1	なし	N/A
8	TOE	FIA_SOS.1	なし	N/A
9	TOE	FIA_UAU.2	FIA_UID.1	#11※1
10	TOE	FIA_UID.2	なし	N/A
11		FIA_USB.1	FIA_ATD.1	#7
12	TOE	FMT_MOF.1	FMT_SMF.1	#16
			FMT_SMR.1	#17
13	TOE	FMT_MSA.1	[FDP_ACC.1またはFDP_IFC.1]	#5
			FMT_SMF.1	#16
			FMT_SMR.1	#17
14	TOE	FMT_MTD.1	FMT_SMF.1	#16
			FMT_SMR.1	#17
15	TOE	FMT_SMF.1	なし	N/A
16	TOE	FMT_SMR.1	FIA_UID.1	#11※1
17	TOE	FPT_RVM.1	なし	N/A
18	TOE	FPT_SEP.1	なし	N/A
19	TOE	FPT_STM.1	なし	N/A
20	TOE	FTA_SSL.3	なし	N/A
21	TOE	FTA_TSE.1	なし	N/A
22	IT環境	FTP_ITC.1	なし	N/A

※1 本来 FIA_UID.1 に対して依存しているが、その上位階層の FIA_UID.2 により依存性を充足している。

※2 本 TOE で扱うオブジェクトは新たに生成されることは一切無いため、FMT_MSA.3 への依存性は除去できる。

8.2.3. セキュリティ機能要件相互補完性

前項の依存性以外にも、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補完がなされている。

迂回:

FPT_RVM.1 により、全ての TOE セキュリティ機能要件が必ず実行され、迂回されないことが保証される。

干渉:

FPT_SEP.1 により、すべての TOE セキュリティ機能要件が信頼できないサブジェクトによる干渉と改ざんから保護される。

非活性化:

FMT_MOF.1 により、FAU_GEN.1 の動作および停止を監査ログ管理者に、FIA_ATD.1、FIA_UAU.2、FIA_UID.2、FIA_USB.1、FMT_MOF.1、FMT_MSA.1、FMT_MTD.1 の動作および停止をアカウント管理者に制限し、各々Hitachi Storage Navigator Modular 2 からの操作によりその動作および停止を指示できる。
この他の手段ではセキュリティ機能要件の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。

8.2.4. セキュリティ要件内部一貫性根拠

各セキュリティ機能要件が内部的に一貫しており、矛盾していないことを以下に示す。

(1) 監査

監査に関連するセキュリティ機能要件は、FAU_GEN.1、FAU_GEN.2、FAU_STG.1、FAU_STG.4 の 4 要件である。これらのセキュリティ機能要件は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。

これら要件と依存関係がある FIA_UID.2 は、FAU_GEN.2 を支援し、FPT_STM.1 は FAU_GEN.1 を支援する。FMT_MTD.1 は監査ログの管理についても定義しており、FAU_STG.1 を支援する。また、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り、競合や矛盾は生じない。

(2) アクセス制御

アクセス制御に関連するセキュリティ機能要件は、FDP_ACC.1、FDP_ACF.1 の 2 要件である。これらのセキュリティ機能要件は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。

また、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り、競合や矛盾は生じない。

(3) 識別・認証

識別・認証に関連するセキュリティ機能要件は、FIA_ATD.1、FIA_SOS.1、FIA_UAU.2、FIA_UID.2、FIA_USB.1 の 5 要件である。これらのセキュリティ機能要件は Hitachi Storage Navigator Modular 2 からのアクセスに対するユーザ ID とパスワードによる識別・認証およびその後のセッション ID による識別、操作者を代行するプロセス(マイクロプログラムの制御動作)と操作者の対応付け、セキュリティ属性の維持について各々定義しており、これらの間で競合や矛盾は存在せず、その内容は一貫している。

また、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り、競合や矛盾は生じない。

(4) セキュリティ管理

セキュリティ管理に関連するセキュリティ機能要件は、FMT_MSA.1、FMT_MTD.1、FMT_SMF.1、FMT_SMR.1 の 4 要件である。これらのセキュリティ機能要件は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。

これらの要件と依存関係のある FIA_UID.2 は、FMT_SMR.1 を支援する。また、FDP_ACC.1 は FMT_MSA.1 を支援するが、両者の間で同一の SFP を参照しており競合や矛盾は存在しない。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り、競合や矛盾は生じない。

(5) TSF の保護

TSF の保護に関連するセキュリティ機能要件は、FPT_RVM.1、FPT_SEP.1、FPT_STM.1 の 3 要件である。FPT_STM.1 は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り、これらのセキュリティ機能要件間、および他のセキュリティ機能要件との間では競合や矛盾が生じないのは自明である。

(6) TOE アクセス

TOE アクセスに関連するセキュリティ機能要件は、FTA_SSL.3、FTA_TSE.1 の 2 要件である。これらのセキュリティ機能要件は TOE のセッション確立に関して制約を設けるものであるが、両者、および他のセキュリティ機能要件との間で競合や矛盾は存在せず、その内容は一貫している。

また、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り、競合や矛盾は生じない。

8.2.5. 最小機能強度レベル根拠

3.2節において、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項においてTOEに対し最小機能強度レベルとして「SOF-基本」を主張しており、脅威エージェントの持つ攻撃能力と最小機能強度レベルは一貫している。

8.2.6. 評価保証レベル根拠

本 TOE を含むディスクアレイ装置は、入退室が管理されているセキュアなエリアに設置されており、TOE への攻撃経路としては管理用 LAN のインタフェース経由に限定される。このため、明白な脆弱性に対する評価を実施すれば充分である。

また、TOE はソフトウェアであり、かつ暗号鍵などの秘匿すべき情報を含まないので、開発セキュリティでの保護は不要である。

したがって、評価保証レベルとして EAL2 が妥当である。

8.3. TOE 要約仕様根拠

8.3.1. TOE セキュリティ機能根拠

6.1節TOEセキュリティ機能の表 14で示したように、各TOEセキュリティ機能が 1 つ以上のTOEセキュリティ機能要件に対応している。以下に、各TOEセキュリティ機能要件が、TOEセキュリティ機能により実現できることの根拠を記述する。

FAU_GEN.1:監査データ生成

SF.Audit_Loggingは、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ログを生成する。記録の対象となる監査対象事象は表 7 監査対象事象に示した通りである。
SF.Audit_Logging は、監査ログ生成時に使用する日時に関して、ディスクアレイ装置の OS が管理している時刻を元にして、監査ログを生成する。
したがって、SF.Audit_Logging により、FAU_GEN.1 は実現される。

FAU_GEN.2:操作者識別情報の関連付け

SF.Audit_Logging は、生成する監査ログに、各監査対象事象の原因となったアカウントのユーザ ID を付与する。
したがって、SF.Audit_Logging により、FAU_GEN.2 は実現される。

FAU_STG.1:保護された監査証跡格納

SF.Account_Authentication は、Audit Log Administrator (View and Modify)のロールを持つ操作者に対してのみ監査ログの消去(全監査ログの一括削除)を許可する。
したがって、SF.Account_Authentication により、FAU_STG.1 は実現される。

FAU_STG.4:監査データ損失の防止

SF.Audit_Logging は、ディスクアレイ装置の内部に 2,048 件までの監査ログを保存する。監査ログが 2,048 件を超過する場合、最も古い監査ログを消去し、新たに発生した監査ログを上書きする。
したがって、SF.Audit_Logging により、FAU_STG.4 は実現される。

FDP_ACC.1:サブセットアクセス制御

SF.Account_Authentication は、操作者が RAID グループ/LU 情報テーブル、LU 割当て情報テーブル、構成情報テーブル、有償オプション情報テーブル(Audit Logging 機能、Account Authentication 機能除く)内の値を変更・参照する際に、操作者のアカウントに設定されたロールを確認し、許可された範囲の操作のみを許可するアクセス制御を行う。
したがって、SF.Account_Authentication により、FDP_ACC.1 は実現される。

FDP_ACF.1:セキュリティ属性によるアクセス制御

SF.Account_Authentication は、操作者が RAID グループ/LU 情報テーブル、LU 割当て情報テーブル、構成情報テーブル、有償オプション情報テーブル(Audit Logging 機能、Account Authentication 機能除く)内の値を変更・参照する際に、操作者のアカウントに設定されたロールを確認し、許可された範囲の操作のみを許可するアクセス制御を行う。
したがって、SF.Account_Authentication により、FDP_ACF.1 は実現される。

FIA_ATD.1:利用者属性定義

SF.Account_Authentication は、セキュリティ属性であるユーザ ID、セッション ID、ロール、アカウント無効の各属性を維持する。
したがって、SF.Account_Authentication により、FIA_ATD.1 は実現される。

FIA_SOS.1:秘密の検証

SF.Account_Authentication は、パスワードの文字数が 6 文字以上であるという品質尺度を満たしているかどうかの確認を行い、品質尺度を満たさないパスワードの設定を認めない。したがって、SF.Account_Authentication により、FIA_SOS.1 は実現される。

FIA_UAU.2：アクション前の利用者認証 （パスワードによる認証）

SF.Account_Authentication は、ユーザ ID、パスワードによる識別・認証に成功しない限り、ディスクアレイ装置に対していかなる管理・設定操作も認めない。
したがって、SF.Account_Authentication により、FIA_UAU.2 は実現される。

FIA_UID.2：アクション前の利用者識別 （ユーザ ID による識別）

SF.Account_Authentication は、ユーザ ID による識別・認証に成功しない限り、ディスクアレイ装置に対していかなる管理・設定操作も認めない。
したがって、SF.Account_Authentication により、FIA_UID.2 は実現される。

FIA_USB.1：利用者・サブジェクト結合

SF.Account_Authentication は、識別・認証が成功した場合に操作者を代行するプロセス（マイクロプログラムの制御動作）と提供されたセッション ID、ユーザ ID、ロールを関連づける。
したがって、SF.Account_Authentication、SF.Configuration により、FMT_USB.1 は実現される。

FMT_MOF.1：セキュリティ機能のふるまいの管理

SF.Configuration は、Account Authentication 機能の有効/無効の設定は Account Administrator (View and Modify)のロールが付与された操作者のみ、Audit Logging 機能の有効/無効の設定は Audit Log Administrator (View and Modify)のロールが付与された操作者のみが可能である。
したがって、SF.Account_Authentication、SF.Configuration により、FMT_MOF.1 は実現される。

FMT_MSA.1：セキュリティ属性の管理

SF.Account_Authentication は、ロールの問い合わせ、改変の操作を行う手段を提供する。Account Administrator (View and Modify)のロールを持つ操作者に対して上記の全ての操作を許可し、Account Administrator (View Only)のロールを持つ操作者には上記属性の問い合わせのみ許可する。
したがって、SF.Account_Authentication により、FMT_MSA.1 は実現される。

FMT_MTD.1：TSF データの管理

SF.Account_Authentication は、操作者からの要求に応じて、ユーザ ID の問い合わせ、作成、削除、パスワードの作成、改変、削除（アカウント全体として削除）、アカウント無効属性の問い合わせ、改変、セッション ID の削除（強制ログアウト）の操作を行う手段を提供する。そして、Account Administrator (View and Modify)のロールを持つ操作者に対して上記の全ての操作を許可し、それ以外の操作者については自分自身のパスワード改変の操作のみ許可する。

SF.Audit_Logging は、Audit Log Administrator (View and Modify)のロールを持つ操作者に対してのみ監査ログの消去（全監査ログの一括削除）を許可する。したがって、
SF.Account_Authentication、SF.Audit_Logging により、FMT_MTD.1 は実現される。

FMT_SMF.1：管理機能の特定

SF.Account_Authentication は、操作者からの要求に応じて、ユーザ ID の問い合わせ、作成、削除、パスワードの作成、改変、削除（アカウント全体として削除）、アカウント無効属性およびロールの問い合わせ、改変、セッション ID の削除の操作を行う手段を提供する。Account Administrator (View

and Modify)のロールを持つ操作者に対して上記の全ての操作を許可し、Account Administrator (View Only)のロールを持つ操作者には上記属性の問い合わせのみ許可する。それ以外の操作者については自分自身のパスワード改変の操作のみ許可する。
SF.Audit_Logging は、Audit Log Administrator (View and Modify)のロールを持つ操作者に対してのみ監査ログの消去(全監査ログの一括削除)を許可する。
SF.Configuration は、Account Authentication 機能の有効/無効の設定する機能を Account Administrator (View and Modify)のみに、Audit Logging 機能の有効/無効の設定する機能を Audit Log Administrator (View and Modify)のみに提供する。
したがって、SF.Account_Authentication、SF.Audit_Logging により、FMT_SMF.1 は実現される。

FMT_SMR.1:セキュリティ役割

SF.Account_Authentication は、識別・認証成功後、当該アカウントに対し役割を関連付け維持する。
したがって、SF.Account_Authentication により、FMT_SMR.1 は実現される。

FMT_RVM.1:TSP の非バイパス性

SF.Account_Authentication は、Hitachi Storage Navigator Modular 2 からのユーザ ID・パスワードもしくはセッション ID による操作者の識別・認証要求を受け付けたとき、操作者が管理機能にアクセスする際に SF.Account_Authentication が必ず実施されることを保証する。
SF.Audit_Logging は、監査対象事象が発生した場合に SF.Audit_Logging が必ず実施されることを保証する。
SF.Configuration は、Account Authentication 機能の有効/無効の設定、Audit Logging 機能の有効/無効の設定関する要求を受け付けたとき、SF.Configuration が必ず実施されることを保証する。
したがって、SF.Account_Authentication、SF.Audit_Logging、SF.Configuration が確実に呼び出されて、識別認証、アクセス制御、ログ生成などが実施され、これら機能をバイパスできないことにより、FMT_RVM.1 は実現される。

FMT_SEP.1:TSF ドメイン分離

SF.Account_Authentication、SF.Audit_Logging、SF.Configuration はそれぞれの機能に用いられる TSF 自身を保護し、信頼できないサブジェクトからの干渉・改ざん等から保護する。
したがって、SF.Account_Authentication、SF.Audit_Logging、SF.Configuration により、FMT_SEP.1 は実現される。

FMT_STM.1:高信頼タイムスタンプ

SF.Audit_Logging は、監査ログ生成時に使用する日時に関して、ディスクアレイ装置の OS が管理している時刻を元にして、監査ログを生成する。
したがって、SF.Audit_Logging により、FMT_STM.1 は実現される。

FTA_SSL.3:TSF 起動による終了

SF.Account_Authentication は、ログイン後一定時間無操作の場合にセッションをタイムアウトとし、再度の識別・認証を要求する。
したがって、SF.Account_Authentication により、FTA_SSL.3 は実現される。

FTA_TSE.1:TOE セッション確立

SF.Account_Authentication は、当該アカウントに対し「アカウント無効」属性が設定されていない場合に限り場合に識別・認証を成功としている。
したがって、SF.Account_Authentication により、FTA_TSE.1 は実現される。

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.Account_Authenticationである。これらセキュリティ機能のセキュリティ機能強度は、6.2節において、「SOF-基本」と主張している。一方、5.1.2項においてTOEの最小機能強度はレベルを「SOF-基本」と主張している。従って両者は一貫している。

8.3.3. 保証手段根拠

本項では、セキュリティ保証手段が評価保証レベル EAL2 において規定されたセキュリティ保証要件に対して必要かつ充分である事を記述する。
セキュリティ保証要件とセキュリティ保証手段の対応関係を表 15に示す。表 15より、すべてのセキュリティ保証手段が、何らかのセキュリティ保証要件のために必要であることが示される。また、保証手段に記述される内容は、本STが規定したセキュリティ保証要件が要求する証拠を網羅する。

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。