Hitachi Unified Storage130用
マイクロプログラム
セキュリティターゲット

第1.2版

2013年9月25日

HITACHI
Inspire the Next

改訂履歴

No	版数	日付	章	内容
1	0.96	2012/08/15	全	初版発行
2	0.97	2012/10/02	全	指摘事項反映
3	0.98	2012/10/12	全	指摘事項反映
4	0.99	2012/10/19	3.4 4.2 6.1.1 7.1.1	指摘事項反映 A.Administrator OE.administrator FAU_GEN.1.2表6-2 FAU_GEN.1/FAU_GEN.2表7-1
5	0.991	2012/11/09	6.1.1 7.1.1	FAU_GEN.1.2表6-2 FAU_GEN.1/FAU_GEN.2表7-1
6	0.992	2012/12/05	1.3.3 1.4.1 3.2 3.4 6.1.1 7.1.1	本文修正 T.Ilegal_assign A.Administrator 表6-1 表7-1
7	0.993	2012/12/06	1.4.2	表1-2　利用者ガイダンス一覧
8	0.994	2012/12/07	全	TOE利用前提条件の変更
9	0.995	2012/12/10	1.3.2	A.Environmentへの一貫性の対応
10	0.996	2013/1/24	全	指摘事項反映
11	0.997	2013/1/29	3章	P.User_roleとO.User_roleの内容変更
12	0.998	2013/1/31	3章	P.User_roleとO.User_roleの内容変更
13	0.999	2013/4/26	全	指摘事項反映
14	0.9991	2013/6/10	全	指摘事項反映
15	0.9992	2013/8/22	1.3.2 1.3.3	HUSの説明文修正 管理用端末の説明文修正
16	0.9993	2013/9/2	7.1.7	指摘事項反映
17	1.0	2013/9/4	全	Ver1.0に改定
18	1.1	2013/9/24	3章	組織のセキュリティ方針を追加
19	12	2013/9/25	3.3 4.1 4.3. 6.3.1 6.3.2	P.Illegar_assign,O.Illegar_assign削除 P.User_role,O.User_roleの内容修正

目次

1 ST概説

1.1 ST参照

タイトル: Hitachi Unified Storage 130用マイクロプログラム セキュリティターゲット

版数: 1.2

発行: 2013年9月25日

作成者: 株式会社 日立製作所

キーワード: ディスクアレイ、共用ディスクアレイ、ストレージ、SAN

1.2 TOE参照

名称: Hitachi Unified Storage130用マイクロプログラム

版数: 0917/A

開発者:株式会社 日立製作所

1.3 TOE概要

1.3.1 TOE種別

TOEは、ディスクアレイ装置内部で動作する制御プログラム (ソフトウェア) である。このディスクアレイ装置とは、日立製作所の製品であるHitachi Unified Storage 130である。以下、このディスクアレイ装置をHUSと呼ぶ。TOEは、HUSの一部を構成し、HUSに接続される複数のホストコンピュータがディスクアレイの記録領域にアクセスするための制御を実行する。なお、HUSはシリーズ製品であり、製品名に付与された数字部分で各製品を区別する。本STでHUSと称する場合、数字“130”が付与された特定の製品を指すものとする。

1.3.2 TOEの用途と主要セキュリティ機能

(1) TOE用途と構成

[HUSの説明]

TOEは、HUSの一部を構成するソフトウェアである。まず、TOEを含むHUS全体の説明を行う。

HUSは、日立製作所が提供するディスクアレイ装置のミッドレンジに位置するストレージ製品である。消費者の要求に応じてスケーラブルなディスクアレイを構築でき、最上位の製品構成では、最大252台のドライブを収容 (ドライブ1台あたりの容量: 3TB) する。ディスクドライブの多重障害に対応するため、RAIDによる冗長構成に対応するが (RAID0/RAID1/RAID1+0/RAID5/RAID6) 、RAID構成に関わる部分はTOEのセキュリティ機能外である。

HUSが使用されるIT環境の構成イメージを図1-1に示す。TOEはHUS内部に格納されるソフトウェアであるが、図中には表示されていない。

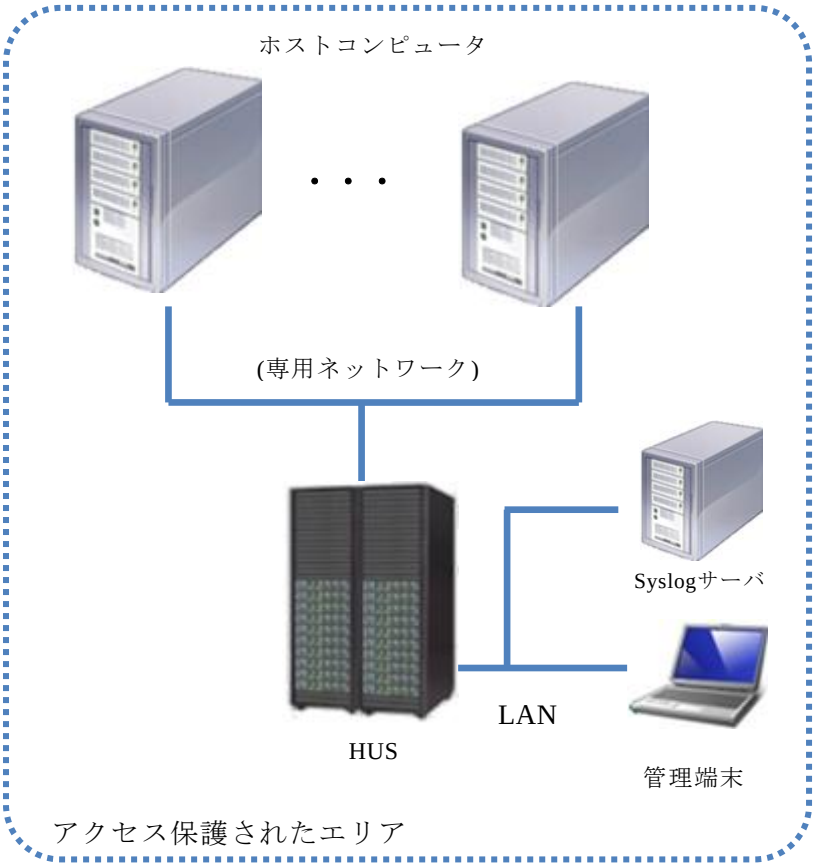

図1-1　HUSとIT環境

HUSは、複数のホストコンピュータと専用ネットワークで相互接続され、RAID構造を持つ大容量ディスクアレイとしてサービスを提供する。ホストコンピュータ、HUS、及びそれらを相互接続する専用ネットワークは、物理的かつ、論理的にアクセス保護されたセキュアな環境で使用されることを想定している。

専用ネットワークには、FC-SANとIP-SANの二種類を使用できる。FC-SAN (Fibre Channel Storage Area Network) は光ファイバーを媒体とするネットワーク、IP-SAN (IP Storage Area Network) はEthernetなどのIPネットワーク上でSCSIプロトコルを使用するネットワークである。

HUSには、ポート数4～16の専用ネットワーク接続ポートが実装される。FC-SAN、IP-SANのどちらも、ポートごとに複数のホストコンピュータを多重接続できる。それぞれのネットワークによって収容可能なホストコンピュータ数、デー

タ伝送容量が異なるので、消費者は、用途に合わせた適切なネットワーク構成を選択する。

FC-SANでは、ポートごとの最大ホストグループ数は128、一つのホストグループに含まれる最大ホストコンピュータ数 (正確には、ネットワークインタフェース数) は128である。ホストグループとは、共通のOSで動作する複数のホストコンピュータで構成されるグループをいう。IP-SANでは、ポートごとの最大ホストコンピュータ数は255である。これらの数は理論的上限値であり、同時使用可能な装置数を保証するものではない。どのタイプのネットワークを使用する場合でも、ネットワークの伝送速度とホストコンピュータに必要なデータ伝送量を考慮し、適切なネットワーク設計を行わねばならない。ネットワーク設計の詳細は、HUSに添付されるガイダンスに説明される。

HUSを利用するホストコンピュータは、特定の機種・種別に限定されない。Windows、HP-UX、Solarisなど、多様なOSで動作するホストコンピュータを同時にHUSに収容できる。

ホストコンピュータには、それぞれにディスクアレイ上の専用の記録領域が割り当てられる。この記録領域は、物理的なディスクアレイ上に構築される論理的記録領域であり、ホストコンピュータからは一つのボリュームとして扱われる。一つのホストコンピュータに割り当てられる論理的記録領域は、他のホストコンピュータの記録領域と論理的に分離され、相互干渉は生じない。ホストコンピュータが割り当て外の記録領域にアクセスすることはできない。なお、評価構成ではFC-SAN,IP-SANそれぞれ、ホストコンピュータを2台使用した構成で評価している。

図1-1では、管理端末がLANを介してHUSに接続されている。LANはEthernetで構成され、物理的かつ、論理的にアクセス管理された領域内で使用される。同図ではHUSが単独のディスクアレイ装置として示されているが、実際の運用環境では、複数のディスクアレイ装置やそのほかの周辺機器もLANを共有する。同図には示されていないが、HUSやその他の装置の監査ログデータを共通管理するサーバ装置等が接続されることもある。これらの装置や機器はTOEの利用者に該当せず、TOEのセキュリティ機能に影響を及ぼさない。

HUSには保守員向けインタフェースが設けられる (図1-1には示されていない) 。保守員の役割は、HUS構成部品の保守である。保守操作において、HUS構成部品の情報読出しのためにTOE機能の一部が使用される。TOEはこの機能の利用者に対する識別・認証を行わず、匿名利用者として扱う。 (以下の[TOEの説明] (2) (b) 参照)しかし、所定の手続き*によりTOE設定や構成を変更するような保守作業が可能となるが、このような保守作業とその結果の環境はISO/IEC15408認証の評価構成の対象外であるため、保証対象外とする。(所定の手続き* : Hitachi Unified Storage 100ISO/IEC15408 認証取得機能取扱説明書（保守員編）3.1節参照)

HUSは管理端末からトレース情報を採取できる。トレース情報は、装置のハードウェアの状態や、TOEを含む内蔵ソフトウェアのバージョンや状態を示す情報で、管理端末へファイル出力される。装置に障害(故障)が発生した場合に、保守員の指示により採取され、原因分析に使用される。

[TOEの説明]

次に、HUS内部で動作するTOEを説明する。

HUSは、ディスクアレイ装置として複数のホストコンピュータにそれぞれの専用データ記録領域を提供する。HUSに搭載される多数の物理的ディスクドライブは、ディスクアレイとして一つの論理的記録領域に統合され、さらに、ホストコンピュータごとの専用記録領域として分割・割り当てが行われる。この制御はTOEによって行われる。ホストコンピュータは、TOEのサービスを利用する利用者に該当する。なお、後述する管理者もTOEの利用者である。

TOEは、HUSの物理的ディスクドライブ記録媒体上に、ホストコンピュータごとの論理的記録領域を設定して割り当てる。ホストコンピュータは、割り当てられた記録領域を専有使用できるが、TOEの制御によって他のホストコンピュータの記録領域には干渉できない。記録領域の管理・制御をセキュアに実施するため、TOEは、組織のセキュリティ方針を反映したセキュリティ機能を備える。

多数のホストコンピュータの記録装置をディスクアレイに集約して共通資源とすることで、記録装置を効率的に利用できるだけでなく、運用・保守作業やセキュリティ対策も一元化できる。システム全体の経済化、効率化、信頼性向上など、多くのメリットが生じる。

(2) 主要セキュリティ機能

TOEを含むHUSは、接続されるホストコンピュータ、ホストコンピュータを接続する専用ネットワーク及び管理端末、管理端末を接続するLAN共々、物理的かつ、論理的にアクセス保護されたセキュアな運用環境で使用される (消費者は、そのような運用環境を準備しなければならない) 。この運用環境では、TOEとその主要なIT環境に対する物理的及び論理的攻撃が排除される。さらにTOEのセキュリティ機能によって、運用・保守に伴うTOEのセキュリティ上のリスクが軽減される。TOEの主要セキュリティ機能を以下 (a) 〜 (c) に示す。

(a) 記録領域の専有制御

ディスクドライブ記録媒体 (HUSに含まれるが、TOE外) が提供する物理的記録領域上にTOEが管理する論理的記録領域を構築し、TOE利用者に該当する各ホストコンピュータに専有的な論理的記録領域を割り当てて使用させる。

(b) 利用者管理

TOE利用者は、ホストコンピュータとHUS利用者 (本STのTOE管理者および保守員) の二つに大別される。本項の利用者管理機能は、管理者に関わるセキュリティ機能である。管理者を識別・認証し、管理者役割に応じた権限を提供することで、TOE資源のセキュアな運用管理を実現する。本TOEには、アカウント管理者、ディスクアレイ管理者、監査ログ管理者の3タイプの管理者役割がある。それぞれの役割は、さらに設定権限を持つ者、設定データを読み出す権限だけの者の二つに区分され、合計6タイプの管理者役割がTOEに設定される。

ただし、アカウント管理者とディスクアレイ管理者による読み出し権限の行使は一般機能であり、本機能の対象でない。

また、HUS利用者がHUSの構成部品情報を読み出す際にTOEの機能が使用される。TOEはHUS利用者を個人別に管理せず、匿名利用者として扱う。HUS利用者は、TOEによる識別・認証を受けることなく限定された情報だけを読み出すことができる。

(c) 監査

TOEは、利用者 (管理者) によるTOEの操作を監査ログデータとして監査証跡に記録する。監査ログデータは、TOEから読み出すほか、外部装置のSyslogサーバへ転送することができる。

1.3.3 TOE以外のハードウェア/ソフトウェア/ファームウェア

TOEに必要となるTOE以外のハードウェア/ソフトウェア/ファームウェアを説明する。

[HUS]

TOEは、ディスクアレイ装置であるHUSの内部で動作するソフトウェアである。TOEの動作環境として、下位のハードウェアが必要である。さらに、HUSがディスクアレイ装置としてのサービスを提供するために、記録媒体資源としてディスクドライブ群が使用される。日本国内向けには、これらはすべてHUSという一体化されたディスクアレイ製品として消費者に提供されるので、消費者がこれらTOEの動作環境を別途準備する必要はない。海外顧客向けには、TOEファイル、マニュアル、ディスクドライブ群を含むハードウェアが提供(出荷)される。海外顧客は、準備手続きおよび利用者ガイダンスに従って、TOEの動作環境を準備する。

HUSとは、1.3.1に示すとおり “Hitachi Unified Storage 100” の名称で代表されるシリーズ製品を指す。TOE下位の主要なIT環境構成要素は、表1-1に示すとおりである。

表1-1 TOEの下位で使用される主要IT環境

項目	名称

制御部ハードウェア	HT-4066-SS/SL(DF850S)※
ディスクドライブユニット	HT-F4066-DBS/L/X (2.5型ドライブ24台用/3.5型ドライブ12台用/3.5型48台ドライブ筐体)

※ SS/SLはそれぞれ2.5型ドライブ24台/3.5型ドライブ12台を内蔵するモデルであるため、必ずディスクアレイユニットを接続する必要はない。

[管理用端末]

TOEの管理用端末としてPCが使用される。このPCはOSがWindows XP SP3であり、WEBブラウザ(IE ver.8.0)が動作する汎用製品だが、管理者向けTOEサービスを利用するための専用ユーティリティプログラム (名称: Hitachi Storage Navigator Modular 2) が搭載される。このユーティリティプログラムは、TOEが提供するサービス(管理機能)を利用するために必要なソフトウェアであり、HUSに付随して消費者に提供される。管理用端末に関わる詳しい情報は、HUSに付随するガイダンスに説明される。

専用ユーティリティプログラム(Hitachi Storage Navigator Modular 2)のバージョンを以下に示す。運用環境を評価構成と同一とするために、以下に示すユーティリティプログラム(Hitachi Storage Navigator Modular 2)を使用する必要がある。

名称: Hitachi Storage Navigator Modular 2

版数: 21.70

開発者:株式会社 日立製作所

[ホストコンピュータ]

HUSのサービスを利用するホストコンピュータは、TOEの利用者に該当する。ホストコンピュータは、TOEの接続制御プロセスを介して、HUSが提供するディスクアレイ機能を利用する。HUSを利用できるホストコンピュータのOSは、Windows、HP-UX、Solaris、Linux、AIXなど多様であるが、TOEセキュリティ機能との関わり合いはない。ホストコンピュータに関わる詳しい情報は、HUSに付随するガイダンスに説明される。

[IT環境に関わる詳細情報]

TOEを含むHUSを利用するために、専用ネットワークの構成、ディスクドライブ構成等を適切に設計しなければならない。これらIT環境に関わる詳しい情報は、HUSに付属するガイダンスに示される。

1.4　TOE記述

1.4.1　TOEとそのIT環境

まず、一体化されたIT製品であるHUSと、その内部で動作するTOEの関係を説明する。

TOEは、HUS内部で動作するソフトウェアである。TOEとそれに関わるIT環境を模式化したものを図1-2に示す。TOEは、HUSに搭載されるディスクドライブ群上に論理的記録領域を構築し、HUSに接続される個々のホストコンピュータごとに論理的記録領域を区分して割り当て、ホストコンピュータがそれぞれの記録領域を専有使用できるような制御を行う。

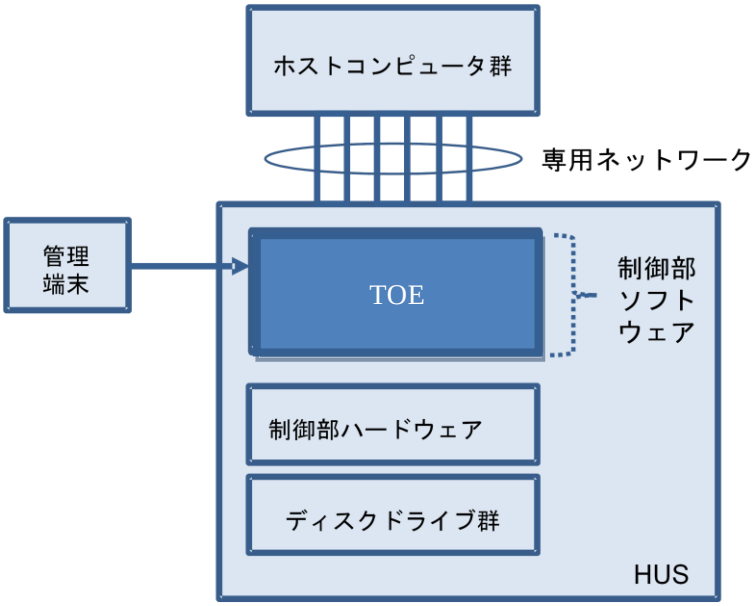

図1-2　TOEとIT環境

図1-2では、ホストコンピュータをまとめて「ホストコンピュータ群」と表示している。各ホストコンピュータは、専用ネットワーク – 1.3.2 (1) に説明したとおり、FC-SANとIP-SANの二つのタイプがある – によってHUSに接続され、TOEの制御によって、ディスクドライブ群上に構築される論理的記録領域を利用する。

TOEのことを制御部ソフトウェアと呼ぶ。制御部ソフトウェアは、制御部ハードウェア上で動作する。これら制御部ソフトウェア及び制御部ハードウェアによってディスクドライブ群が管理され、ホストコンピュータがそれぞれに割り当てられた記録領域資源を利用できるようになる。

次に、ホストコンピュータとディスクドライブ上に構築される論理的記録領域との接続制御について図1-3を用いて説明する。

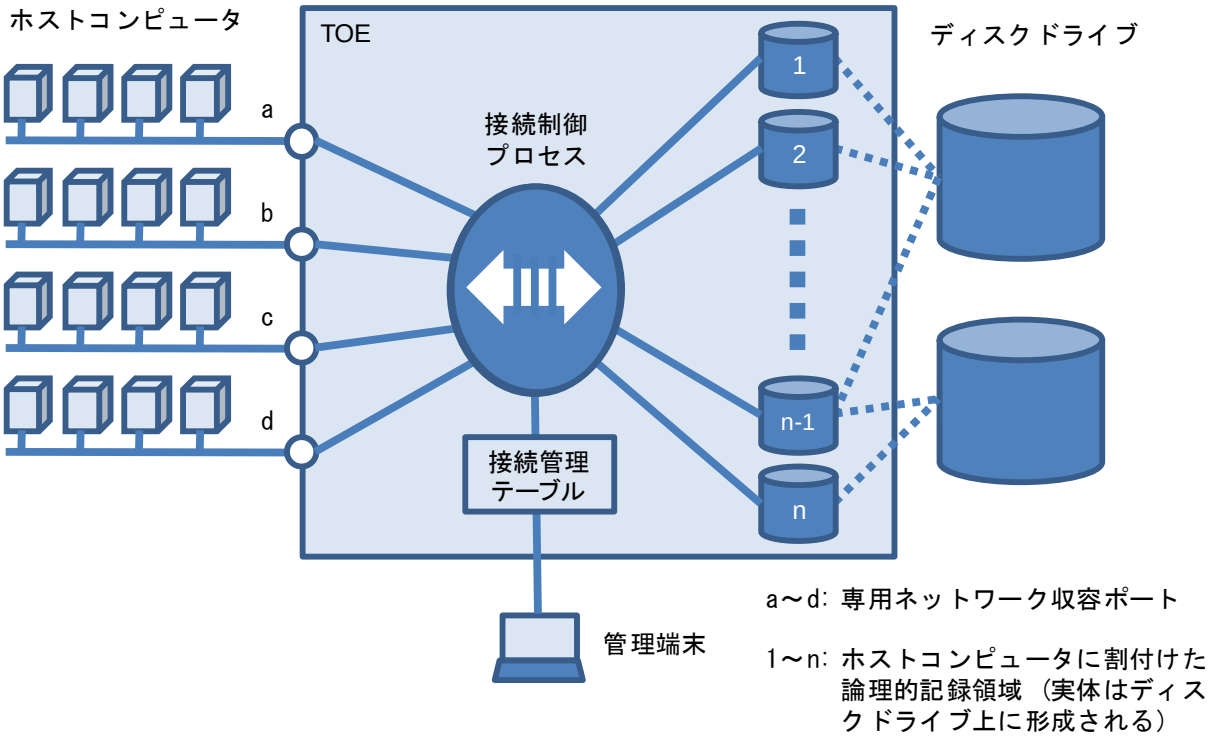

図1-3　ホストコンピュータと論理的記録領域の接続制御

図1-3では、ホストコンピュータが専用ネットワークを経由してTOEのポート (a～d) に収容されている。TOE内では、個々のホストコンピュータから送出される要求を接続制御プロセスが受け付け、その要求に従って、各ホストコンピュータに専用に割り当てた論理的記録領域 (1～n) へアクセスする。接続制御プロセスはTOE内のサブジェクト (能動的エンティティ) であり、TOE内の論理的記録領域 (1～n) はTOE内のオブジェクト (受動的エンティティ) である。この論理的記録領域は、ディスクドライブ記録媒体の物理的記録領域上に構築され、TOEセキュリティ機能 (TSF) によってホストコンピュータと対応付けられる。

ホストコンピュータは、接続制御プロセスに向けてデータ書込み・読出し要求を送出する。要求を受けた接続制御プロセスは、接続管理テーブルを参照してホストコンピュータと論理的記録領域を対応付け、ホストコンピュータに割り当てられた論理的記録領域にアクセスしてデータ書込み・読出しを実行し、実行結果をホストコンピュータへ返す。これらの処理は接続制御プロセスによって多重処理され、複数のホストコンピュータの要求が同時に実行される。ホストコンピュータは割り当てられた記録領域を専有使用できるが、それ以外の記録領域にアクセスすることはTSFによって禁止される。

管理者 (ディスクアレイ管理者) が接続管理テーブルを書き換えることで、ホストコンピュータと論理的記録領域の対応付けを変更できる。接続管理テーブル書き換えは管理端末を使用して行われる。

1.4.2 物理的範囲

TOEの物理的構成要素は、以下に示す (a) 、 (b) の二つである。

(a) Hitachi Unified Storage130用マイクロプログラム

(b) 利用者ガイダンス: 詳細は表1-2で示す

表1-2 利用者ガイダンス一覧

種類	名称	版数 (英語版：版数)
プログラムプロダクト ユーザーズガイド	Account Authenticationユーザーズガイド（HUS100 シリーズ） (英語版:Hitachi Unified Storage 100 Account Authentication User's Guide)	第6版 (5th)
	Audit Loggingユーザーズガイド (HUS100 シリーズ） (英語版:Hitachi Unified Storage 100 Audit Logging User's Guide)	第5版 (5th)
	LUN Managerユーザーズガイド （HUS100 シリーズ） (英語:Hitachi Unified Storage 100 LUN Manager User's Guide)	第4版 (4th)
ディスクアレイ ユーザーズガイド （保守あり）	HUS100シリーズディスクアレイ ユーザーズガイド (英語版:Hitachi Unified Storage 100 Series Disk Array System User’s Guide)	第6版 (6th)
	HUS100シリーズディスクアレイ サービスガイド (英語版:Hitachi Unified Storage 100 Series Disk Array System Service Guide)	第6版 (6th)
ディスクアレイ ユーザーズガイド （保守なし）	Hitachi Unified Storage 130/150 ディスクアレイ ユーザーズ ガイド (英語版:Hitachi Unified Storage 130/150 Disk Array System User’s Guide)	第6版 (6th)
Hitachi Storage Navigator Modular 2ユーザーズガイド	Hitachi Storage Navigator Modular 2（for GUI） ユーザーズガイド (英語版:Hitachi Storage Navigator Modular 2（for GUI）User's Guide)	第54版 (54th)
	Hitachi Storage Navigator Modular 2（for CLI） ユーザーズガイド (英語版:Hitachi Storage Navigator Modular 2（for CLI） User's Guide)	第58版 (58th)
ホストインストールガイド	Hitachi Unified Storage 100シリーズ Fibre Channel接続用 ホストインストールガイド (英語版: Hitachi Unified Storage 100Series Host Installation Guide for Fibre Channel Connection)	第3版 (3rd)
	Hitachi Unified Storage 100シリーズ	第2版

	iSCSI接続用　ホストインストールガイド (英語版: Hitachi Unified Storage 100 Series Host Installation Guide for iSCSI Connection)	(2nd)
Hitachi Unified Storage 100ISO/IEC15408 認証取得機能取扱説明書	Hitachi Unified Storage 100 ISO/IEC15408認証取得機能取扱説明書(管理者/利用者編) (英語版:Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Administrators/Users))	第2版 (2nd)
	Hitachi Unified Storage 100 ISO/IEC15408認証取得機能取扱説明書(保守員編) (英語版:Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Maintenance))	初版 (1st)

上記 (a) は、図1-2のTOEと記された部分に該当する。図1-2におけるTOE以外の構成要素は、すべてTOEのIT環境である。

上記 (b) は、HUSに付属するガイダンスである。TOEとそのIT環境について、運用・管理に関わる側面が記載される。

1.4.3 論理的範囲

TOEが提供するセキュリティ機能は、以下 (a) ～ (c) に示す範囲である。

(a) 記録領域の専有制御

TOEは、ディスクドライブ記録媒体 (TOE外) が提供する物理的記録領域をTOE上で論理的記録領域として管理する。論理的記録領域をホストコンピュータごとに割り当て、割り当てた記録領域がそれぞれのホストコンピュータ専用のボリュームとして使用されるよう、ホストコンピュータによるディスクドライブのアクセスを制御する。

ホストコンピュータとディスクドライブ間のアクセス制御は、TOEが持つ接続管理テーブルの情報に基づいて行われる。接続管理テーブルの情報は、ディスクアレイ管理者の役割を持つ管理者によって管理される。この管理者の役割には、ホストコンピュータごとの論理的記録領域生成と、アクセス権限の初期値設定が含まれる。

(b) 利用者管理

利用者管理機能の対象となるTOE利用者は、以下に示す6つの役割 (権限区分) に分かれた管理者である。ホストコンピュータもTOE利用者であるが、管理者には該当せず、本機能の対象でない。利用者管理機能は、1) 利用者を識別・認証し、2) 認証された利用者に対して利用者の権限区分に応じたTOE資源の利用許可を与える。

TOEが管理する利用者 (管理者) の役割は、以下の3つの分野に大別され、さらにそれぞれが設定権限を持つ者及び設定情報の読出し権限だけを持つ者の二つに区分される。合わせて、6つの管理者役割が存在する。

- アカウント管理　　全管理者のアカウントに関わる管理
- ディスクアレイ管理　　ホストコンピュータの記録領域割り当てに関わる管理
- 監査ログ管理　　TOEセキュリティ機能の動作に関わる監査証跡の管理

ただし、アカウント管理者とディスクアレイ管理者による読み出し権限の行使は一般機能であり、本機能の対象でない。

HUS利用者がHUSの構成部品情報を読み出す際にTOEの機能が使用される。HUS利用者がHUS構成部品を読み出す場合だけTOEの利用者管理対象外であり、匿名利用者として扱われる。TOEは、利用者の識別・認証を行うことなく、限定された情報の読み出しだけを許可する。

(c) 監査

TOEは、それぞれの利用者 (管理者) によるTOE操作を監査ログデータとして監査証跡に記録する。監査証跡が所定のサイズを超えると、古いデータから順に新しいデータで上書きする。記録された監査ログデータは、監査ログ管理者だけがアクセスできる。監査ログデータは、TOEから直接読み出すほか、TOEの設定によって、別装置のSyslogサーバ (TOE外) へ自動転送できる。Syslogサーバへの転送を行うと、TOEとSyslogサーバの両方に監査ログデータが格納される。Syslogサーバは十分なデータ格納領域を持つので、TOE内では上書きによって自動削除されるデータも、Syslogサーバ上での長期保管が可能になる。

2 適合主張

2.1 CC適合主張

本STおよびTOEは、CC バージョン3.1 リリース3に適合する。

ST開発に使用したCCは、JISEC公開の日本語版である。適合主張は以下のとおりである。

- パート2: セキュリティ機能コンポーネント バージョン3.1 改訂第3版 [翻訳第1.0版] への適合を主張する。
- パート3: セキュリティ保証コンポーネント バージョン3.1 改訂第3版 [翻訳第1.0版] への適合を主張する。

2.2 PP主張

本STは、他のPPへの適合を主張しない。

2.3 パッケージ主張

本STにおいて、TOEに対して適用する保証パッケージは、EAL2である。

2.4 適合根拠

本STは、他のPPへの適合を主張しないので、適合根拠の記述を行わない。

3 セキュリティ課題定義

TOEに関わるセキュリティ課題定義を示す。脅威、組織のセキュリティ方針、前提条件について、それぞれ、[T.xxxx]、[P.xxxx]、[A.xxxx]の形式で識別名称を付与する。

3.1 保護資産

TOEを構成要素の一部に含むHUSは、接続する各々のホストコンピュータが専有的に使用するデータ記録領域を提供する。その記録領域には、HUSに登録され対応付けられたホストコンピュータだけがアクセスできる。

TOEの主たる保護資産は、HUSによるデータ記録領域提供サービスである。このサービスは、利用者であるホストコンピュータに対し、割り当てたデータ記録領域のセキュアな利用環境を提供する。ホストコンピュータが利用するデータ記録領域は、TOEのセキュリティ機能によって他のホストコンピュータからの干渉から保護される。TOEのセキュリティ機能 (TSF) 、あるいはTSFが使用するデータ (TSFデータ) は、すべてこの主たる保護資産をセキュアに保つために必要なものである。

3.2 脅威

本TOEに関して、対抗すべき脅威はない。

3.3 組織のセキュリティ方針

P.Exclusive_assign　ホストコンピュータごとの論理的記録領域の割り当ては、各ホストコンピュータに専有的に与えられる。すなわち、あるホストコンピュータが使用する論理的記録領域には、他のホストコンピュータからのアクセスが禁止される。

P.Audit　TOEは、利用者 (管理者) の操作結果による以下の事象を監査データとして記録する。監査データは、権限を持つ利用者だけにアクセスが許可される。監査データ記録領域が満

杯になったとき、古いデータから順に新しいデータで上書きすることで、新しい監査データの損失を防ぐ。

- 利用者 (管理者) に対する識別・認証の成功・失敗事象
- 監査ログデータのSyslogサーバ転送設定(転送する・しない)の成功事象
- 無操作時間継続の上限値に対する改変操作の成功事象
- ログイン中利用者(管理者)の強制ログアウト処理の成功・失敗事象
- ホストコンピュータと論理的記録領域を対応付ける情報 (接続管理テーブル) への初期設定・改変・削除のいずれかに該当する操作の成功・失敗事象

P.User_role

TOEは、以下の利用者役割を区別する。

- アカウント管理者[設定]
- アカウント管理者[読出し](一般機能を提供される)
- ディスクアレイ管理者[設定]
- ディスクアレイ管理者[読出し] (一般機能を提供される)
- 監査ログ管理者[設定]
- 監査ログ管理者[読出し]

また、以下のTOE操作は、それぞれの権限を持つ利用者のみに許可する。

- アカウント管理者[設定]：全管理者に対するアカウント設定、ログイン中利用者の強制ログアウト処理
- アカウント管理者[設定]：無操作時間継続の上限値の設定
- ディスクアレイ管理者[設定]：ディスクドライブ記録媒体へのアクセス制御に関わる設定
- 監査ログ管理者[設定]：監査証跡読出し、監査ログデータのSyslogサーバ転送の有無の設定
- 監査ログ管理者[読出し]: 監査証跡読出し

P.Session_timeout

TOEは、管理者の無操作継続時間が、アカウント管理者[設定]の定める上限値を超えたときに、その管理者のセッションを強制終了する。

3.4 前提条件

A.Environment

TOE及びTOEを含むHUSは、接続されるホストコンピュータ、ホストコンピュータを接続する専用ネットワーク及び管理端末、管理端末を接続するLAN共々、物理的かつ、論理的にアクセスの制限されたセキュアな環境※に設置される。

TOEの監査ログデータがHUSに接続するSyslogサーバへ転送される場合、Syslogサーバに転送されるTOE監査ログデータは、TOEのセキュリティ方針を侵害しないようセキュアに管理される。

※物理的かつ、論理的にアクセスの制限されたセキュアな環境・・・「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おり、各ネットワークが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できないように設定されているセキュアなエリア」

A.Administrator

TOE利用者である管理者は、それぞれの役割実行に際し、TOEのセキュリティ侵害につながる悪意ある操作を行わず設定操作や環境の構築を行う。

A.Configuration

TOEのセキュリティ機能に関わる設定は、それぞれの機能に関わる管理者によって適正な動作状態に設定される。適正な動作状態とは、以下の状態がすべて満たされていることである。

- 監査機能及び利用者 (管理者) に対する識別・認証機能が動作状態に設定される。
- 記録領域の専有制御機能が動作状態に設定される。

4 セキュリティ対策方針

3章に示したセキュリティ課題に対して、TOE及びその環境におけるセキュリティ対策方針を示す。TOEによって対処するセキュリティ対策方針を4.1に、その環境によって対処するセキュリティ対策方針を4.2に記載する。これらセキュリティ対策方針がセキュリティ課題に対して適切であることの根拠を4.3に示す。

TOEのセキュリティ対策方針、運用環境のセキュリティ対策方針は、それぞれ、先頭に “O.”、“OE.” を付与した識別名で示される。

4.1 TOEのセキュリティ対策方針

セキュリティ課題として定義された組織のセキュリティ方針に関して、課題解決のためにTOEが対処すべきセキュリティ対策方針を示す。

O.Exclusive_access　TOEは、ホストコンピュータごとに専有的に割り当てる論理的記録領域に対し、他のホストコンピュータによるアクセスを禁止しなくてはならない。

O.Audit　TOEは、利用者(管理者)の操作結果による以下の事象を監査データとして記録しなければならない。監査データは、権限を持たない者による不正アクセスから保護されねばならない。記録領域が満杯になったとき、古いデータから順に新しいデータで上書きすることで、新しい監査データの損失を防がねばならない。

- 利用者 (管理者) に対する識別・認証の成功・失敗事象
- 監査ログデータのSyslogサーバ転送設定(転送する・しない) の成功事象
- 無操作時間継続の上限値に対する改変操作の成功事象
- ログイン中利用者(管理者)の強制ログアウト処理の成功・失敗事象
- ホストコンピュータと論理的記録領域を対応付ける情報 (接続管理テーブル) への初期設定・改変・削除のいずれかに該当する操作の成功・失敗事象

O.User_role　TOEは、以下の利用者役割を維持する。設定操作の矛盾を防ぐため、同一役割の複数の利用者が同時にTOE設定を行うのを禁止しなければならない。

- アカウント管理者[設定]
- アカウント管理者[読出し](一般機能を提供される)
- ディスクアレイ管理者[設定]
- ディスクアレイ管理者[読出し] (一般機能を提供される)
- 監査ログ管理者[設定]
- 監査ログ管理者[読出し]

また、以下のTOE操作は、それぞれの権限を持つ利用者のみに許可する。

- アカウント管理者[設定]：全管理者に対するアカウント設定、ログイン中利用者の強制ログアウト処理
- アカウント管理者[設定]：無操作時間継続の上限値の設定
- ディスクアレイ管理者[設定]：ディスクドライブ記録媒体へのアクセス制御に関わる設定
- 監査ログ管理者[設定]：監査証跡読出し、監査ログデータのSyslogサーバ転送の有無の設定
- 監査ログ管理者[読出し]: 監査証跡読出し

O.Session_timeout　TOEは、管理者のTOEへの無操作継続時間が、アカウント管理者[設定]の定める上限値を超えたとき、その管理者のセッションを強制終了しなくてはならない。

4.2　運用環境のセキュリティ対策方針

セキュリティ課題として定義された組織のセキュリティ方針及び前提条件に関して、課題解決のためにTOEの運用環境が対処すべきセキュリティ対策方針を示す。

OE.Environment　TOE及びTOEを含むHUSは、接続されるホストコンピュータ、ホストコンピュータを接続する専用ネットワーク及び管理端末、管理端末を接続するLAN共々、物理的かつ、論理的にアクセスの制限されたセキュアな環境※に設置される。

TOEの監査ログデータをHUSに接続するSyslogサーバへ転送する場合、Syslogサーバに転送されるTOE監査ログデータは、TOEのセキュリティ方針を侵害しないようセキュアに管理される。

※物理的かつ、論理的にアクセスの制限されたセキュアな環境・・・「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おり、各ネットワークが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できないように設定されているセキュアなエリア」

OE.Administrator　TOE利用者である管理者がその役割実行に際してTOEのセキュリティ侵害につながる悪意ある操作を行わないようにするため、HUSを導入する消費者は、信頼できる管理者を選任し、その任にあてて、設定操作や環境の構築を行わせる。

OE.Configuration　TOEのセキュリティ機能に関わる設定は、それぞれの機能に関わる管理者が適正な動作状態に設定する。適正な動作状態とは、以下の状態がすべて満たされていることである。

- 監査機能及び利用者 (管理者) に対する識別・認証機能が動作状態に設定される。
- 記録領域の専有制御機能が動作状態に設定される。

4.3　セキュリティ対策方針根拠

4.3では、上述のセキュリティ対策方針がセキュリティ課題定義の各項目に対して有効であることの根拠を示す。4.3.1では、各々のセキュリティ対策方針がいずれかのセキュリティ課題にさかのぼれること、4.3.2では、各々のセキュリティ課題が対応するセキュリティ対策方針によって有効に対処されることを説明する。

4.3.1　セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義とセキュリティ対策方針の対応を表4-1に示す。ここに示すとおり、すべてのセキュリティ対策方針は、一つのセキュリティ課題定義の項目にさかのぼることができる。

表4-1　セキュリティ課題定義とセキュリティ対策方針の対応

セキュリティ課題定義 ＼ セキュリティ対策方針	O.Exclusive_access	O.Audit	O.User_role	O.Session_timeout	OE.Environment	OE.Administrator	OE.Configuration
P.Exclusive_assign	x						
P.Audit		x					
P.User_role			x				
P.Session_timeout				x			
A.Environment					x		
A.Administrator						x	
A.Configuration							x

4.3.2 セキュリティ対策方針の根拠説明

TOE及び環境に対するセキュリティ対策方針によって、識別された組織のセキュリティ方針が実施され、さらに、前提条件が適切に満たされることの根拠を示す。

P.Exclusive_assign　O.Exclusive_accessは、P.Exclusive_assignが定める組織のセキュリティ方針をすべてカバーしており、P.Exclusive_assignが適切に実施される。

P.Audit　O.Auditは、P.Auditが定める組織のセキュリティ方針を直接支持しており、P.Auditが適切に実施される。

P.User_role　O.User_roleは、P.User_roleが定める組織のセキュリティ方針を支持し、さらに、利用者役割区分が有効に機能するよう、TOE設定操作の衝突を回避する対策を明示している。このセキュリティ対策方針によって、P.User_roleが適切に実施される。

P.Session_timeout　O.Session_timeoutは、P.Session_timeoutが定める組織のセキュリティ方針を直接支持しており、P.Session_timeoutが適切に実施される。

A.Environment	OE.Environmentは、A.Environmentが定める組織のセキュリティ方針を直接支持しており、A.Environmentが適切に実施される。
A.Administrator	OE.Administratorは、A.Environmentが定める組織のセキュリティ方針を直接支持しており、A.Environmentが適切に実施される。
A.Configuration	OE.Configurationは、A.Configurationが定める組織のセキュリティ方針を直接支持しており、A.Configurationが適切に実施される。

5　拡張コンポーネント定義

本STでは、拡張セキュリティ機能要件を定義しない。

6 セキュリティ要件

6.1 セキュリティ機能要件

本STで規定するSFRは、すべてCCパート2に含まれるコンポーネントを使用したものである。表6-1にSFRのリストを示す。

表6-1　SFRリスト

6.1.1	FAU_GEN.1	監査データ生成
6.1.2	FAU_GEN.2	利用者識別情報の関連付け
6.1.3	FAU_SAR.1	監査レビュー
6.1.4	FAU_SAR.2	限定監査レビュー
6.1.5	FAU_STG.1	保護された監査証跡格納
6.1.6	FAU_STG.4	監査データ損失の防止
6.1.7	FDP_ACC.1	サブセットアクセス制御
6.1.8	FDP_ACF.1	セキュリティ属性によるアクセス制御
6.1.9	FIA_ATD.1	利用者属性定義
6.1.10	FIA_SOS.1	秘密の検証
6.1.11	FIA_UAU.1	認証のタイミング
6.1.12	FIA_UAU.2	アクション前の利用者認証
6.1.13	FIA_UAU.5	複数の認証メカニズム
6.1.14	FIA_UID.1	識別のタイミング
6.1.15	FIA_UID.2	アクション前の利用者識別
6.1.16	FIA_USB.1	利用者-サブジェクト結合
6.1.17	FMT_MOF.1	セキュリティ機能のふるまいの管理
6.1.18	FMT_MSA.1	セキュリティ属性の管理
6.1.19	FMT_MSA.3	静的属性初期化
6.1.20	FMT_MTD.1	TSFデータの管理
6.1.21	FMT_REV.1	取り消し
6.1.22	FMT_SMF.1	管理機能の特定
6.1.23	FMT_SMR.1	セキュリティの役割
6.1.24	FPT_STM.1	高信頼タイムスタンプ
6.1.25	FRU_RSA.1	最大割り当て
6.1.26	FTA_SSL.3	TSF起動による終了

それぞれのセキュリティ機能コンポーネントに必要な操作を施すことによってSFRを規定する。操作内容は、各SFRにおいて、以下の表記方法で示される。

- 割付あるいは選択操作の箇所を[割付: *XXX*(斜体)]、[選択: *XXX*(斜体)]の形式で示す。
- 選択操作において、選択対象外の項目を~~抹消線~~ (抹消線) で示す。
- 詳細化操作において、詳細化部分を***斜体・太字***で示す。

以下、本STで規定するSFRを示す。

6.1.1 FAU_GEN.1 監査データ生成

下位階層: なし

依存性: FPT_STM.1 高信頼タイムスタンプ

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

a) 監査機能の起動と終了;

b) 監査の[選択: ~~*最小、基本、詳細、*~~*指定なし*: から1つのみ選択]レベルのすべての監査対象事象; 及び

c) [割付: *表6-2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 (該当する場合) 、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: *なし*]。

表6-2

監査事象
利用者 (管理者) の識別・認証の成功・失敗事象
監査ログデータのSyslogサーバ転送設定(転送する・しない) の成功事象
ホストコンピュータと論理的記録領域を対応付ける情報 (接続管理テーブル) への初期設定・改変・削除のいずれかに該当する操作の成功・失敗事象
以下のTSFデータに対する改変操作の成功事象 *無操作時間継続の上限値*
ログイン中利用者(管理者)の強制ログアウト処理の成功・失敗事象

6.1.2 FAU_GEN.2 利用者識別情報の関連付け

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FIA_UID.1 識別のタイミング

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

6.1.3 FAU_SAR.1 監査レビュー

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

FAU_SAR.1.1 TSFは、[割付: *監査ログ管理者[設定]及び監査ログ管理者[読出し]*]が、[割付: *記録された情報のすべて*]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。

6.1.4 FAU_SAR.2 限定監査レビュー

下位階層: なし

依存性: FAU_SAR.1 監査レビュー

FAU_SAR.2.1 TSFは、明示的な読み出しアクセスを承認された利用者を除き、すべての利用者に監査記録への読み出しアクセスを禁止しなければならない。

6.1.5 FAU_STG.1 保護された監査証跡格納

下位階層: なし

依存性: FAU_GEN.1 監査データ生成

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

FAU_STG.1.2 TSFは、監査証跡に格納された監査記録への不正な改変を[選択: *防止*~~、*検出*~~: から1つのみ選択]できなければならない。

6.1.6 FAU_STG.4 監査データ損失の防止

下位階層: FAU_STG.3 監査データ消失の恐れ発生時のアクション

依存性: FAU_STG.1 保護された監査証跡格納

FAU_STG.4.1 TSFは、監査証跡が満杯になった場合、[選択: ~~*監査事象の無視、特別な権利を持つ許可利用者に関わるもの以外の監査事象の抑止、最*~~*も古くに格納された監査記録への上書き*: から1つのみ選択]及び[割付: *なし*]を行わなければならない。

6.1.7 FDP_ACC.1 サブセットアクセス制御

下位階層: なし

依存性: FDP_ACF.1 セキュリティ属性によるアクセス制御

FDP_ACC.1.1　TSFは、[割付: *サブジェクト:<接続制御プロセス[*1]>、オブジェクト:<論理的記録領域[*2]>、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:<データ書込み及びまたは読出し>*]に対して[割付: *HUSアクセス制御SFP*]を実施しなければならない。

[*1] TOE内で動作するプロセス。個々のホストコンピュータからディスクアレイへのデータ書込み・読出し要求を受け、そのホストコンピュータに割り当てられたTSF制御下の論理的記録領域に対してその要求を実行し、結果をホストコンピュータへ戻す。TOE内でただ一つ生成される。TOE動作中は常時作動し、すべてのホストコンピュータからの要求を多重処理する。

[*2] TSF制御下の論理的記録領域であり、実体となるディスクドライブ (TOE外) の記録媒体上に構築される。個々のホストコンピュータごとに、対応するオブジェクト (一つあるいは複数) が生成される。

6.1.8　FDP_ACF.1　セキュリティ属性によるアクセス制御

下位階層: なし

依存性:　FDP_ACC.1 サブセットアクセス制御

FMT_MSA.3 静的属性初期化

FDP_ACF.1.1　TSFは、以下の[割付: *示されたSFP下において制御されるサブジェクトとオブジェクトのリスト:<表6-3参照>、及び各々に対応する、SFP関連セキュリティ属性: <表6-3参照>*]に基づいて、オブジェクトに対して、[割付: *HUSアクセス制御SFP*]を実施しなければならない。

表6-3

エンティティ	*セキュリティ属性*
サブジェクト: *接続制御プロセス*	*・サブジェクトに要求を送出したホストコンピュータの識別情報* *・オブジェクトの識別情報 (ホストコンピュータからの要求に含まれる)*
オブジェクト: *論理的記録領域*	*・オブジェクトの識別情報* *・ホストコンピュータの識別情報*

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を決定するために、次の規則を実施しなければならない: [割付: *サブジェクトとオブジェクトそれぞれに含まれるオブジェクトの識別情報が一致し、「サブジェクトに要求を送出したホストコンピュータの識別情報」がアクセス対象として識別されたオブジェクトのセキュリティ属性に含まれる「ホストコンピュータの識別情報」と一致した場合、サブジェクトは、ホストコンピュータから要求された操作をオブジェクトに対して実行できる*]

FDP_ACF.1.3　TSFは、次の追加規則、[割付: *なし*]に基づいて、オブジェクトに対して、サブジェクトのアクセスを明示的に許可しなければならない。

FDP_ACF.1.4　TSFは、次の追加規則、[割付: *なし*]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。

6.1.9　FIA_ATD.1　利用者属性定義

下位階層: なし

依存性:　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を維持しなければならない。: [割付: *表6-4に示すセキュリティ属性のリスト*]

表6-4

利用者種別	*セキュリティ属性のリスト*
ホストコンピュータ	・ *ホストコンピュータの識別情報* ・ *オブジェクトの識別情報 (一つまたは複数のオブジェクトがホストコンピュータに割り当てられ、その情報はオブジェクトに関連付けて維持される。)*
管理者	・ *識別情報 (個人を識別できる情報)* ・ *役割 (表6-9に示す6つの役割のいずれか; 複数の役割を兼ねることも可能)* ・ *認証状態 (認証済みか否かを示す情報)*

6.1.10　FIA_SOS.1　秘密の検証

下位階層: なし

依存性:　なし

FIA_SOS.1.1　TSFは、秘密が[割付: *6桁以上の文字列*]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。

6.1.11　FIA_UAU.1　認証のタイミング

下位階層: なし

依存性:　FIA_UID.1 識別のタイミング

FIA_UAU.1.1　TSFは、***管理者に相当する***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: *HUS構成情報 (構成部品種別・数量・ステータス・トレース情報) の読出し*]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すべてのTSF仲介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。

6.1.12 FIA_UAU.2　　アクション前の利用者認証

下位階層: FIA_UAU.1 認証のタイミング

依存性:　FIA_UID.1 識別のタイミング

FIA_UAU.2.1　TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、***ホストコンピュータに相当する***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。

6.1.13 FIA_UAU.5　　複数の認証メカニズム

下位階層: なし

依存性:　なし

FIA_UAU.5.1　TSFは、利用者認証をサポートするため、[割付: *表6-5に示す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: *表6-5に示す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。

表6-5

認証メカニズム	*認証メカニズムが認証を提供する規則*
パスワードによる認証	*管理者に相当する利用者に適用*
ホストコンピュータに搭載されるFibre Channel HBA (Host Bus Adaptor) の固有番号であるWWN (World Wide Name) による認証	*ホストコンピュータに相当する利用者に適用*
ホストコンピュータに搭載されるiSCSI HBAの固有情報であるiSCSI NAMEによる認証	*ホストコンピュータに相当する利用者に適用*
なし	*HUSのwebポート経由のアクセスに適用（匿名利用者がFIA_UAU.1/FIA_UID.1に規定する特定データだけを読出せる)*

6.1.14 FIA_UID.1　　識別のタイミング

下位階層: なし

依存性:　なし

FIA_UID.1.1　TSFは、***管理者に相当する***利用者が識別される前に利用者を代行して実行される[割付: *HUS構成情報（構成部品種別・数量・ステータス・ト*

レース情報) の読出し]を許可しなければならない。

FIA_UID.1.2　TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、各利用者に識別が成功することを要求しなければならない。

6.1.15 FIA_UID.2　アクション前の利用者識別

下位階層: FIA_UID.1 識別のタイミング

依存性:　なし

FIA_UID.2.1　TSFは、その利用者を代行する他のTSF仲介アクションを許可する前に、***ホストコンピュータに相当する***各利用者に識別が成功することを要求しなければならない。

6.1.16 FIA_USB.1　利用者-サブジェクト結合

下位階層: なし

依存性:　FIA_ATD.1 利用者属性定義

FIA_USB.1.1　TSFは、以下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: *ホストコンピュータの識別情報*]

FIA_USB.1.2　TSFは、以下の利用者セキュリティ属性の最初の関連付けの規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *サブジェクトが一つのホストコンピュータからディスクドライブへの書き込みまたは読出し要求を受けたとき、サブジェクトは、そのホストコンピュータの識別情報をサブジェクトのセキュリティ属性に関係付ける*]

FIA_USB.1.3　TSFは、以下の利用者セキュリティ属性への変更を管理する規則を、その利用者を代行して動作するサブジェクトと共に実施しなければならない。: [割付: *サブジェクトがホストコンピュータから新たな要求を受けたとき、サブジェクトは、実行中の処理を終了後、サブジェクトに関係付けたセキュリティ属性を新たな要求に関係付けられるホストコンピュータの識別情報で置き換える。新たな要求に関係付けられるホストコンピュータは、前のホストコンピュータと同一でも異なってもよい。*]

6.1.17 FMT_MOF.1　セキュリティ機能のふるまいの管理

下位階層: なし

依存性:　FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MOF.1.1　TSFは、機能[割付: *監査ログデータのSyslogサーバ転送*][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: *監査ログ管理者[設定]*]に制限しなければならない。

6.1.18 FMT_MSA.1　セキュリティ属性の管理

下位階層: なし

依存性:　[FDP_ACC.1 サブセットアクセス制御、または

FDP_IFC.1 サブセット情報フロー制御]

FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MSA.1.1　TSFは、セキュリティ属性[割付: *オブジェクトの識別情報、オブジェクトに対応付けられたホストコンピュータの識別情報*]に対し[選択: *表6-6参照*]をする能力を[割付: *表6-6に示す管理者*]に制限する[割付: *HUSアクセス制御SFP*]を実施しなければならない。

表6-6

管理者	*選択項目*
ディスクアレイ管理者[設定]	~~*デフォルト値変更、改変、削除、[割付: その他の操作]*~~

6.1.19 FMT_MSA.3　静的属性初期化

下位階層: なし

依存性:　FMT_MSA.1 セキュリティ属性の管理

FMT_SMR.1 セキュリティの役割

FMT_MSA.3.1　TSFは、そのSFPを実施するために使われるセキュリティ属性に対して[選択: *制限的*~~*、許可的、[割付: その他の特性]*~~*: から1つのみ選択*]デフォルト値を与える[割付: *HUSアクセス制御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: *ディスクアレイ管理者[設定]*]が、デフォルト値を上書きする代替の初期値を特定することを許可しなければならない。

6.1.20 FMT_MTD.1　TSFデータの管理

下位階層: なし

依存性:　FMT_SMR.1 セキュリティの役割

FMT_SMF.1 管理機能の特定

FMT_MTD.1.1 TSFは、[割付: *表6-7に示す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: 表6-7に示す操作]*]する能力を[割付: *表6-7に示す許可された識別された役割*]に制限しなければならない。

表6-7

役割	*TSFデータ*	*操作*
アカウント管理者[設定]	*利用者識別情報*	*初期設定、削除*
	利用者パスワード(全ての利用者)	*初期設定、改変*
	利用者役割	*初期設定、改変*
	無操作時間継続の上限値	*改変*
アカウント管理者[読出し]	*自身のパスワード*	*改変*
監査ログ管理者[設定]	*監査証跡*	*読出し*
	自身のパスワード	*改変*
監査ログ管理者[読出し]	*監査証跡*	*読出し*
	自身のパスワード	*改変*
ディスクアレイ管理者[設定]	*ホストコンピュータ識別情報*	*初期設定、改変、削除*
	自身のパスワード	*改変*
ディスクアレイ管理者[読出し]	*自身のパスワード*	*改変*

6.1.21 FMT_REV.1 取消し

下位階層: なし

依存性: FMT_SMR.1 セキュリティの役割

FMT_REV.1.1 TSFは、TSFの制御下で、[選択: ***管理者に相当する****利用者*~~*、サブジェクト、オブジェクト、[割付: その他追加の資源]*~~]に関連した[割付： *認証状態がログイン中であることを示すセキュリティ属性*]を取り消す能力を、[割付: *アカウント管理者[設定]*]に制限しなければならない。

FMT_REV.1.2 TSFは、規則[割付: *該当する利用者の認証状態を直ちにログインからログアウトに変更し、該当する利用者を代行するTSF仲介アクションの停止*]を実施しなければならない。

6.1.22 FMT_SMF.1　管理機能の特定

下位階層: なし

依存性:　なし

FMT_SMF.1.1　TSFは、以下の管理機能を実行することができなければならない。: [割付: *表6-8に示すTSFによって提供される管理機能のリスト*]

表6-8

管理機能	*備考: 対応するFMTクラス要件*
監査ログデータのSyslogサーバ転送有無を設定	*FMT_MOF.1*
ホストコンピュータと論理的記録領域（オブジェクト）を対応付けるセキュリティ属性の管理	*FMT_MSA.1*
オブジェクト生成時のセキュリティ属性の設定	*FMT_MSA.3*
表6-7に示すTSFデータの管理	*FMT_MTD.1*

6.1.23 FMT_SMR.1　セキュリティの役割

下位階層: なし

依存性:　FIA_UID.1 識別のタイミング

FMT_SMR.1.1　TSFは、役割[割付: *表6-9に示す許可された識別された役割*]を維持しなければならない。

表6-9

役割
アカウント管理者[設定]
アカウント管理者[読出し]
ディスクアレイ管理者[設定]
ディスクアレイ管理者[読出し]
監査ログ管理者[設定]
監査ログ管理者[読出し]

FMT_SMR.1.2　TSFは、利用者を役割に関連付けなければならない。

6.1.24 FPT_STM.1　高信頼タイムスタンプ

下位階層: なし

依存性:　なし

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

6.1.25 FRU_RSA.1 最大割当て

下位階層: なし

依存性: なし

FRU_RSA.1.1 TSFは、[選択: *~~個々の利用者、~~定義された利用者のグループ~~、サブジェクト~~*]が[選択: *同時に~~、特定した時間の間~~*]使用できる、以下の資源[割付: *同一の設定権限を持つ利用者役割のログイン数*]の最大割当て<***ログイン数 "1"***>を実施しなければならない。

6.1.26 FTA_SSL.3 TSF起動による終了

下位階層: なし

依存性: なし

FTA_SSL.3.1 TSFは、[割付: *アカウント管理者[設定]が定める管理者端末が非アクティブである時間間隔*]後に対話セションを終了しなければならない。

6.2 セキュリティ保証要件

本TOEに適用するセキュリティ保証要件は、表6-10に示す保証コンポーネントで定義される。これらは、すべて、CC パート3に含まれる。

表6-10に示すすべてのコンポーネントにおいて、本STでは、操作を適用していない。

表6-10 保証コンポーネント

保証クラス	保証コンポーネント
セキュリティターゲット評価	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
開発	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
ガイダンス文書	AGD_OPE.1
	AGD_PRE.1
ライフサイクルサポート	ALC_CMC.2
	ALC_CMS.2

	ALC_DEL.1
テスト	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
脆弱性評定	AVA_VAN.2

6.3 セキュリティ要件根拠

6.3.1 セキュリティ機能要件根拠

6.3.1では、定義されたSFRがTOEのセキュリティ対策方針を適切に達成することの根拠を示す。6.3.1.1では、各々のSFRがいずれかのTOEのセキュリティ対策方針にさかのぼれること、6.3.1.2では、各々のTOEのセキュリティ対策方針が対応する有効なSFRによって適切に満たされることを説明する。

6.3.1.1 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に対応するSFRを表6-11に示す。この表は、すべてのSFRが少なくとも一つのTOEのセキュリティ対策方針にさかのぼれることの根拠となる。

表6-11 TOEセキュリティ対策方針とSFRの対応

TOEセキュリティ対策方針 / SFR	FAU_GEN.1	FAU_GEN.2	FAU_SAR.1	FAU_SAR.2	FAU_STG.1	FAU_STG.4	FDP_ACC.1	FDP_ACF.1	FIA_ATD.1	FIA_SOS.1	FIA_UAU.1	FIA_UAU.2	FIA_UAU.5	FIA_UID.1	FIA_UID.2	FIA_USB.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3	FMT_MTD.1	FMT_REV.1	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FRU_RSA.1	FTA_SSL.3
O.Exclusive_access							x	x	x			x	x		x	x										
O.Audit	x	x	x	x	x	x														x		x		x		
O.User_role									x	x	x		x	x			x	x	x	x	x	x	x		x	
O.Session_timeout																										x

6.3.1.2 対応関係の根拠説明

TOEのセキュリティ対策方針がそれに対応づけられるSFRによって満たされることの根拠を示す。個々のSFRがTOEのセキュリティ対策方針を満たす上での有効性を持つことも同時に示される。

O.Exclusive_access ホストコンピュータごとにTOEの論理的記録領域が割り当てられる。この割り当ては、ホストコンピュータからのディスクドライブへのアクセス要求をTOE内の接続制御プ

ロセス (すなわちTOE内サブジェクト) が受け付け、対応する論理的記録領域 (すなわちTOE内オブジェクト) に対してその要求を実行することで実現される。

TOEは、アクセス要求を送出したホストコンピュータを特定し、かつそのホストコンピュータがTOEに登録された適正なものであることを確認するため、ホストコンピュータを識別・認証する。これは、FIA_UAU.2、FIA_UAU.5及びFIA_UID.2で規定される。要求を受け付けたTOEのサブジェクトは、識別したホストコンピュータのセキュリティ属性をサブジェクトのセキュリティ属性に結合する。この要件はFIA_USB.1で規定される。ホストコンピュータごとのセキュリティ属性は、FIA_ATD.1で規定される。サブジェクトに結合された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基づき、ホストコンピュータの要求によるディスクドライブ記録領域へのアクセスが制御される。このアクセス制御要件は、FDP_ACC.1及びFDP_ACF.1によって規定される。

これらSFRによって、O.Exclusive_accessが適切に実施される。

O.Audit

O.Auditは、セキュリティ機能に関わる監査データ収集項目を規定し、監査データの保護を要求する。監査データ収集項目の要求は、FAU_GEN.1及びFAU_GEN.2が対応する。FAU_GEN.2は、利用者識別情報を監査データに含めることを規定する。監査データに付与される時刻情報の要件としてFPT_STM.1を規定する。特定の利用者 (すなわち監査ログ管理者) だけに監査データ読出しを許可する要件として、FAU_SAR.1及びFAU_SAR.2を適用する。監査データ保護のため、FAU_STG.1で不正な削除・改変の防止、FAU_STG.4で記録領域満杯時の損失防止を規定する。管理者による監査データの管理は、FMT_MTD.1/FMT_SMF.1で規定する。これらSFRによって、O.Auditが適切に実施される。

O.User_role

TOEが6種類の利用者役割を維持する要件はFMT_SMR.1で規定される。役割に対応する利用者の識別・認証が必要であり、その要件をFIA_UAU.1、FIA_UAU.5及びFIA_UID.1で規定する。利用者認証データの品質尺度の検査要件として、FIA_SOS.1を用いる。利用者のセキュリティ属性には役割が含まれ、その要件をFIA_ATD.1で規定する。

各役割に関連付けられる利用者の操作にはTSFデータ操作が含まれ、その要件がFMT_MTD.1/FMT_SMF.1に規定され

る。役割の一つであるアカウント管理者[設定]はログイン中の管理者の認証状態を管理する。認証状態がログイン中のセキュリティ属性廃棄の要件がFMT_REV.1に規定される。役割の一つであるディスクアレイ管理者[設定]はアクセス制御に関わるセキュリティ属性を管理し、その要件がFMT_MSA.1、FMT_MSA.3及びFMT_SMF.1に規定される。役割の一つである監査ログ管理者[設定]は、監査ログデータのSyslogサーバ転送の有無を設定する。その要件がFMT_MOF.1/FMT_SMF.1に規定される。

同じ役割の管理者が同時に同じリソースに管理操作を行うと、操作結果に矛盾が生じる。この事態を避けるため、該当するリソースに対する利用者割り当て制限が必要になる。この要件をFRU_RSA.1で規定する。

これらSFRによって、O.User_roleが適切に実施される。

O.Session_timeout　FTA_SSL.3は、管理端末の無操作継続時間がアカウント管理者[設定]の規定する時間に達したとき、その管理端末を使用する管理者アカウントの対話セッションを強制的に終了させることを要求する。これはO.Session_timeoutの対策方針をすべてカバーしており、O.Session_timeoutが適切に実施される。

6.3.1.3　セキュリティ機能要件の依存性

各SFRに規定された依存性とその対応状況を表6-12に示す。

表6-12において、「依存性の要求」欄にはSFRに規定された依存性を示す。「依存性の対応」欄には、規定された依存性がST中のどのSFRによって満たされるかを示す。各SFRに対し、要求されるすべての依存性が満たされる。

表6-12　SFRの依存性

SFR	依存性の要求	依存性への対応
FAU_GEN.1	FPT_STM.1	FPT_STM.1が対応し、依存性が満たされる。
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1及びFIA_UID.1が対応し、依存性が満たされる。
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1が対応し、依存性が満たされる。
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1が対応し、依存性が満たされる。
FAU_STG.1	FAU_GEN.1	FAU_GEN.1が対応し、依存性が満たされ

		る。
FAU_STG.4	FAU_STG.1	FAU_STG.1が対応し、依存性が満たされる。
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1が対応し、依存性が満たされる。
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1及びFMT_MSA.3が対応し、依存性が満たされる。
FIA_ATD.1	なし	–
FIA_SOS.1	なし	–
FIA_UAU.1	FIA_UID.1	FIA_UID.1が対応し、依存性が満たされる。
FIA_UAU.2	FIA_UID.1	FIA_UID.2が対応し、依存性が満たされる。
FIA_UAU.5	なし	–
FIA_UID.1	なし	–
FIA_UID.2	なし	–
FIA_USB.1	FIA_ATD.1	FIA_ATD.1が対応し、依存性が満たされる。
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1及びFMT_SMF.1が対応し、依存性が満たされる。
FMT_MSA.1	[FDP_ACC.1または FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1、FMT_SMR.1及びFMT_SMF.1が対応し、依存性が満たされる。
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1、FMT_SMR.1が対応し、依存性が満たされる。
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1及びFMT_SMF.1が対応し、依存性が満たされる。
FMT_REV.1	FMT_SMR.1	FMT_SMR.1が対応し、依存性が満たされる。
FMT_SMF.1	なし	–
FMT_SMR.1	FIA_UID.1	FIA_UID.1が対応し、依存性が満たされる。
FPT_STM.1	なし	–
FRU_RSA.1	なし	–
FTA_SSL.3	なし	–

6.3.2 セキュリティ保証要件根拠

TOEは、セキュアな領域で運用される。TOEのサービスを利用するホストコンピュータ、TOEとホストコンピュータ間を接続するネットワークも同じ環境に置かれる。

TOEの使用環境が比較的穏和であり、不特定の外部の者による長時間の攻撃を想定する必要性は低い。TOEの外部インタフェースは限定的であり、内部構造の脆弱性を悪用する攻撃が行われる蓋然性は高くない。さらに、TOE開発環境に向けられる攻撃は限定的と考えられる。

TOEのこのような特性を鑑みれば、保証要件としてEAL2が適切である。

7 TOE要約仕様

7.1 セキュリティ機能要件実現手段の概要

TOEにおけるセキュリティ機能要件実現手段の概要を説明する。6.1章に記載した各々のSFRごとに実現手段を示す。

7.1.1 FAU_GEN.1/FAU_GEN.2

監査機能の起動と終了の日時・時刻を記録する。さらに、監査対象とするセキュリティ機能の動作に伴い、表7-1に示す事象が生じたときに以下の情報を監査データとして記録する。

[監査データに含まれる情報]

- 事象の日付・時刻
- 事象の種別
- 利用者 (管理者) 識別情報
- 事象の結果 (成功または失敗)

表7-1 記録対象となる監査事象

SFR	監査事象
FIA_UAU.1/FIA_UID.1	利用者の識別・認証のメカニズム動作 (該当する利用者は、管理者)の成功・失敗事象
FMT_MOF.1	監査ログデータのSyslogサーバ転送設定(転送する・しない)の成功事象
FMT_MSA.1/FMT_MSA.3	ホストコンピュータと論理的記録領域を対応付ける情報 (接続管理テーブル) への初期設定・改変・削除のいずれかに該当する操作の成功・失敗事象
FMT_MTD.1	以下のTSFデータに対する改変操作*の成功事象* *・無操作時間継続の上限値*
FMT_REV.1	ログイン中利用者(管理者)の強制ログアウト処理の成功・失敗事象

7.1.2 FAU_SAR.1/FAU_SAR.2

TOEは、利用者 (管理者) ログイン時に利用者を識別・認証し、監査ログ管理者の役割を持つ利用者だけが監査データを読み出せるようにする。利用者は、HUS専用のユーティリティプログラムがインストールされた管理者端末を使用してTOE内の監査データにアクセスする。監査データは、TOEから直接読み出す機能に加え、管理者によるTOE設定によって、TOE外のSyslogサーバへ転送できる。なお、Syslogサーバに送られた監査ログを監査ログ管理者以外が読み出すこと

は、TOEの本セキュリティ方針に違反する。SyslogサーバはTOE外であるが、その運用・管理は、TOEのセキュリティ方針に反しないよう実施されるべきである。

7.1.3 FAU_STG.1/FAU_STG.4

監査証跡の記録容量を2,048件 (1件: 1,024バイト) とし、満杯になったときは、古いデータから順に新しいデータで上書きする。

監査証跡に格納された監査記録 (監査データ) は、監査ログ管理者が一括読出しできる。TOE動作中は監査機能が動作しており、監査証跡に対する消去 (初期化) ・改変は行えない。

7.1.4 FDP_ACC.1/FDP_ACF.1

ホストコンピュータから送出されるディスクアレイへのアクセス要求 (書込み・読出し) は、TOEで常時動作する接続制御プロセスによって処理される。接続制御プロセスは、ホストコンピュータからの要求を受け付け、要求データに含まれるホストコンピュータ識別情報をTOE内の接続制御テーブルと突き合わせ、対応する論理的記録領域に対して要求された操作を実行する。ホストコンピュータ識別情報が未登録の場合　、要求が拒否される。

7.1.5 FIA_ATD.1

セキュリティ属性を持つ利用者は、ホストコンピュータと管理者の2つの種別に分けられる。それぞれの利用者は、表7-2に示す属性を持つ。

表7-2　利用者のセキュリティ属性

利用者種別	セキュリティ属性のリスト
ホストコンピュータ	・ ホストコンピュータの識別情報 ・ ホストコンピュータに割り当てられたオブジェクトの識別情報 (一つまたは複数のオブジェクトを割り当てられ、その情報はオブジェクトに関連付けて維持される。ホストコンピュータが送出する要求にアクセス対象のオブジェクト識別情報が含まれるが、そのときに指定されるのは一つのオブジェクトである。)
管理者	・ 識別情報 (個人を識別できる情報) ・ 役割 (アカウント管理者[設定/読出し]、ディスクアレイ管理者[設定/読出し]、監査ログ管理者[設定/読出し]の6つ) ; 一つの識別情報を持つ個人に複数の役割の割り当て可 ・ 認証状態(認証済みか否かを示す情報)

7.1.6 FIA_SOS.1

管理者によるパスワード登録時、文字数をチェックする。パスワードが条件 [6桁の文字列] に合致しない場合、パスワード登録を拒否する。

7.1.7 FIA_UAU.1/FIA_UAU.2/FIA_UAU.5/FIA_UID.1/FIA_UID.2

FIA_UAU.1とFIA_UID.1は管理者に相当する利用者の識別・認証、FIA_UAU.2とFIA_UID.2はホストコンピュータの識別・認証、FIA_UAU.5はこれら両方の認証に関わる複数の認証メカニズムを規定する要件である。

[FIA_UAU.1/FIA_UAU.5/FIA_UID.1]

IDとパスワードによって管理者を個人ごとに識別・認証する。管理者によるTOEのサービス利用は、HUS専用のユーティリティプログラム “Hitachi Storage Navigator Modular 2” を搭載した管理端末を介して行う。管理端末はLANを経由してHUSに接続される。管理端末からTOEに送られるコマンドに利用者のIDとパスワードが含まれ、識別・認証に成功したときにそのコマンドが受理され実行される。

HUS利用者は、HUSのURLを指定することによって、識別・認証を受けずにHUSの構成部品に関わる情報 (構成部品の種別・数量・ステータス・トレース情報) を読み出すことができる。HUS利用者がHUSの構成部品に関わる情報を読み出す場合は、TOEによる利用者管理の対象外である。

[FIA_UAU.2/FIA_UAU.5/FIA_UID.2]

ホストコンピュータの識別・認証は、ホストコンピュータに搭載されるHBA (Host Bus Adaptor) によって、使用するデータが異なる。Fibre Channel HBAの場合はその固有番号であるWWN (World Wide Name) によって行い、iSCSI HBAの場合は固有情報であるiSCSI Nameで行う。ホストコンピュータの登録時にこれらのデータがTOEに読み込まれる。ホストコンピュータからの要求データに含まれるWWNあるいはiSCSI NameがTOEに登録されたデータと一致したとき、TOEによるホストコンピュータの識別・認証が成功し、ホストコンピュータの要求が受け付けられる。

7.1.8 FIA_USB.1

TOE内では、常時一つの接続制御プロセスが動作している。接続制御プロセスがホストコンピュータからの要求を受取り、その要求に含まれるWWNあるいはiSCSI Nameによってホストコンピュータを識別・認証すると、接続制御プロセスはその識別情報を自らのセキュリティ属性と関係付け、論理的記録領域に対して要求された操作を実行する。

ホストコンピュータからの要求ごとに、接続制御プロセスに関係づけられるセキュリティ属性が新しい情報 (ホストコンピュータの識別情報) で置き換えられる。

7.1.9 FMT_MOF.1

TOEの監査機能について、監査ログ管理者[設定]は、監査ログデータのSyslogサーバ (TOE外) 転送の有無を設定できる。なお、Syslogサーバへの転送の有無に関わらず、監査ログデータはTOE内に監査証跡として記録される。この設定操作は、管理端末に設けられる専用のインタフェース (“Hitachi Storage Navigator Modular 2” と呼ぶユーティリティプログラム) を介して実行される。

7.1.10 FMT_MSA.1

ホストコンピュータの要求とTOEが管理する論理的記録領域との関連付けは、TOEに設けた接続管理テーブルの情報に基づいて行われる。この接続管理テーブルの情報は、ディスクアレイ管理者が管理端末を使用して管理する。

7.1.11 FMT_MSA.3

ディスクアレイ管理者は、ホストコンピュータごとに論理的記録領域 (オブジェクト) を設定し、オブジェクトに対して許可される操作を初期設定する。初期設定以前のデフォルト値は、「どの記録領域へのアクセスも許可しない」である。

7.1.12 FMT_MTD.1

各管理者のTSFデータ操作権限を表7-3のとおりとする。

表7-3 TSFデータ操作に関わる管理者役割と権限

役割	TSFデータ	操作
アカウント管理者 [設定]	利用者識別情報	初期設定、改変、削除
	利用者パスワード (全ての利用者)	初期設定、改変
	利用者役割	初期設定、改変
	無操作時間継続の上限値	改変
アカウント管理者 [読出し]	自身のパスワード	改変
監査ログ管理者 [設定]	監査証跡	読出し
	自身のパスワード	改変
監査ログ管理者 [読出し]	監査証跡	読出し
	自身のパスワード	改変
ディスクアレイ管理者[設定]	ホストコンピュータ識別情報	初期設定、改変、削除
	自身のパスワード	改変
ディスクアレイ管理者[読出し]	自身のパスワード	改変

7.1.13 FMT_REV.1

本要件は、TOEまたはそのIT環境における障害等によって、管理者の認証状態が“ログイン中”に固定されてしまうような状況に対処するための機能である。アカウント管理者[設定]は、該当する管理者の認証状態を強制的に“ログアウト”に書き換えることができる。

7.1.14 FMT_SMF.1

関係するSFRに関わるセキュリティ機能メカニズムを表7-4のとおり実現する。

表7-4　セキュリティ管理機能のメカニズム

SFR	管理機能のメカニズム
FMT_MOF.1	識別・認証された管理者のうち、監査ログ管理者[設定]のグループに属する管理者は、監査ログデータのSyslogサーバ転送の有無を設定できる。
FMT_MSA.1	識別・認証された管理者のうち、ディスクアレイ管理者のグループに属する管理者は、接続管理テーブルを使用し、オブジェクト (論理的記録領域) ごとに以下のようにホストコンピュータとの対応付けを管理できる。 (オブジェクト生成時に限り、FMT_MSA.3の管理機能が適用される。) ・ ディスクアレイ管理者[設定]は、上記の設定を行える。
FMT_MSA.3	識別・認証された管理者のうち、ディスクアレイ管理者[設定]のグループに属する管理者は、オブジェクト生成時、そのオブジェクトとホストコンピュータを対応付ける情報、を接続管理テーブルに設定できる。
FMT_MTD.1	識別・認証された管理者は、所属する役割ごとに、表7-3に規定されるTSFデータの操作を実行できる。規定外の操作は許可されない。

7.1.15 FMT_SMR.1

管理者の役割として、アカウント管理者[設定]・アカウント管理者[読出し]・ディスクアレイ管理者[設定]・ディスクアレイ管理者[読出し]・監査ログ管理者[設定]・監査ログ管理者[読出し]の6つの役割グループをTOEに設定する。すべての管理者が一つあるいは複数のグループに登録される。

7.1.16 FPT_STM.1

下位のハードウェアから時刻情報を取得し、その時刻情報を監査データに付加する。

7.1.17 FRU_RSA.1

設定権限を持つ利用者役割は、アカウント管理者[設定]、監査ログ管理者[設定]、ディスクアレイ管理者[設定]の三つである。これらそれぞれの役割ごとに、同時ログインが “1” を超えないよう制限する。設定権限を持たない管理者の同時ログイン数は制限しない。

7.1.18 FTA_SSL.3

ログインした管理者ごとにセッションを管理し、管理端末からの無操作時間を監視する。無操作時間が上限値を超過した場合、その利用者 (管理者) のセッションを強制終了する。無操作時間の上限値は、アカウント管理者[設定]が設定・変更できる。

8 用語

8.1 CC関連

PP	Protection Profile: TOEの調達者あるいは開発に関わる業界などが共通仕様として定めるセキュリティ要件定義書。
CC	Common Criteria; IT装置のセキュリティ評価基準。CCと同一の内容がISO/IEC 15408規格としても制定される。
ST	Security Target: 個々のIT製品に対するセキュリティ要件定義書。
TOE	Target of Evaluation; 評価対象。IT製品全体がTOEに該当することもあり、IT製品の一部をTOEと定義することもある。TOEの範囲は、STによって厳密に定義される。

8.2 TOE関連

ディスクアレイ	複数のディスクドライブ (ハードディスクが一般的) を論理的に統合して一つのディスクドライブとして扱えるようにしたもの。さらに、統合した一つのディスクドライブを論理的に分割し、それぞれを別々のホストコンピュータに割り当てて使用させるディスクアレイ装置もある。本STのTOEは、このタイプである。 ディスクアレイはホストコンピュータから独立した装置として提供されることが一般的である。ディスクアレイの構成にRAID (Redundant Array of Independent Disks) を使用すると、ハードウェア障害に対する信頼性を向上できる。多数のディスクドライブを統合することで、非常に大容量のディスクドライブを実現することも可能である。ホストコンピュータからディスクドライブを分離して管理することで、保守性も向上する。
SAN	Storage Area Networkの省略形。 ディスクアレイ等のストレージデバイスをホストコンピュータに接続させる専用ネットワーク。ホストコンピュータ (のOS) から見ると、ローカルストレージデバイスが直接接続されたのと同等になる。ホストコンピュータのOSに依存しない、ブロックレベルの高速データ伝送を行う。ホストコンピュータとストレージデバイス間の通信プロトコルにはSCSIが使用される。従来のSCSI規格には、伝送速度320Mbps、伝送距離25mの制限があるが、SANに適用されるFC (Fibre Channel)

を用いると、8Gbps・100km (以上) の高速・長距離伝送が可能になる。FCの代わりにEthernetとIPプロトコルをベースとしたSANも構築できる。通信プロトコルは、iSCSI (IPネットワーク上のSCSI) が使用される。

ホストコンピュータ　本STでは、HUSが提供するディスクアレイサービスの利用者をホストコンピュータと呼ぶ。HUSがホストコンピュータに提供するインタフェースは特定のファイルシステムに依存しないので、Windows、HP-UX、Solarisなど多様なOSのホストコンピュータがHUSのディスクアレイ資源を利用できる。同一OSで動作する複数のコンピュータにHUS上の同一の論理記録領域 (ボリューム) を共有させることができる。