認 証 報 告 書

独立行政法人 情報処理推進機構
理事長　西垣　浩司 原紙 押印済

評価対象

申請受付日（受付番号）	**平成20年3月25日** (IT**認証**8210)
認証番号	C0220
認証申請者	**株式会社 日立製作所**
TOE**の名称**	Hitachi Adaptable Modular Storage 2300 **用マイクロプログラム**
TOE**のバージョン**	0862/ A-M
PP**適合**	**なし**
適合する保証パッケージ	EAL2
開発者	**株式会社 日立製作所**
評価機関の名称	**株式会社電子商取引安全技術研究所　評価センター**

上記のTOEについての評価は、以下のとおりであることを認証したので報告します。
平成21年6月29日

セキュリティセンター 情報セキュリティ認証室
技術管理者　山里 拓己

評価基準等：「ITセキュリティ評価及び認証制度の基本規程」で定める下記の規格に基づいて評価された。

① Common Criteria for Information Technology Security Evaluation Version 2.3
② Common Methodology for Information Technology Security Evaluation Version 2.3

評価結果：合格

「Hitachi Adaptable Modular Storage 2300 用マイクロプログラム」は、独立行政法人 情報処理推進機構が定めるITセキュリティ認証申請手続等に関する規程に従い、定められた規格に基づく評価を受け、所定の保証要件を満たした。

目次

1 全体要約 1
1.1 はじめに 1
1.2 評価製品 1
1.2.1 製品名称 1
1.2.2 製品概要 1
1.2.3 TOEの範囲と動作概要 2
1.2.4 TOEの関係者 5
1.2.5 TOEの機能 6
1.3 評価の実施 8
1.4 評価の認証 8
1.5 報告概要 9
1.5.1 PP適合 9
1.5.2 EAL 9
1.5.3 セキュリティ機能強度 9
1.5.4 セキュリティ機能 9
1.5.5 脅威 9
1.5.6 組織のセキュリティ方針 10
1.5.7 構成条件 10
1.5.8 操作環境の前提条件 10
1.5.9 製品添付ドキュメント 12
2 評価機関による評価実施及び結果 13
2.1 評価方法 13
2.2 評価実施概要 13
2.3 製品テスト 13
2.3.1 開発者テスト 13
2.3.2 評価者テスト 15
2.4 評価結果 16
3 認証実施 17
4 結論 18
4.1 認証結果 18
4.2 注意事項 22
5 用語 23
6 参照 24

1 全体要約

1.1 はじめに

この認証報告書は、「Hitachi Adaptable Modular Storage 2300 用マイクロプログラム」（以下「本TOE」という。）について株式会社電子商取引安全技術研究所　評価センター（以下「評価機関」という。）が行ったITセキュリティ評価に対し、その内容の認証結果を申請者である株式会社 日立製作所に報告するものである。

本認証報告書の読者は、本書と共に、対応するSTや本TOEに添付されるマニュアル（詳細は「1.5.9 製品添付ドキュメント」を参照のこと）を併読されたい。前提となる環境条件、対応するセキュリティ対策方針とその実施のためのセキュリティ機能要件、保証要件及びそれらの要約仕様は、STにおいて詳述されている。また、動作条件及び機能仕様は本TOEに添付されるドキュメントに詳述されている。

本認証報告書は、本TOEに対して、適合の保証要件に基づく認証結果を示すものであり、個別のIT製品そのものを認証するものではないことに留意されたい。

注：本認証報告書では、ITセキュリティ評価及び認証制度が定めるITセキュリティ評価基準、ITセキュリティ評価方法の各々をCC、CEMと総称する。

1.2 評価製品

1.2.1 製品名称

本認証が対象とする製品は以下のとおりである。

名称：　Hitachi Adaptable Modular Storage 2300 用マイクロプログラム
バージョン：　0862/ A-M
開発者：　株式会社 日立製作所

1.2.2 製品概要

TOE は、株式会社日立製作所ディスクアレイ装置「Hitachi Adaptable Modular Storage 2300」（以下Hitachi AMS2300 と略す）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。

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。

1.2.3 TOEの範囲と動作概要

TOEを含むディスクアレイ装置は一般的に図1-1の構成で使用される。

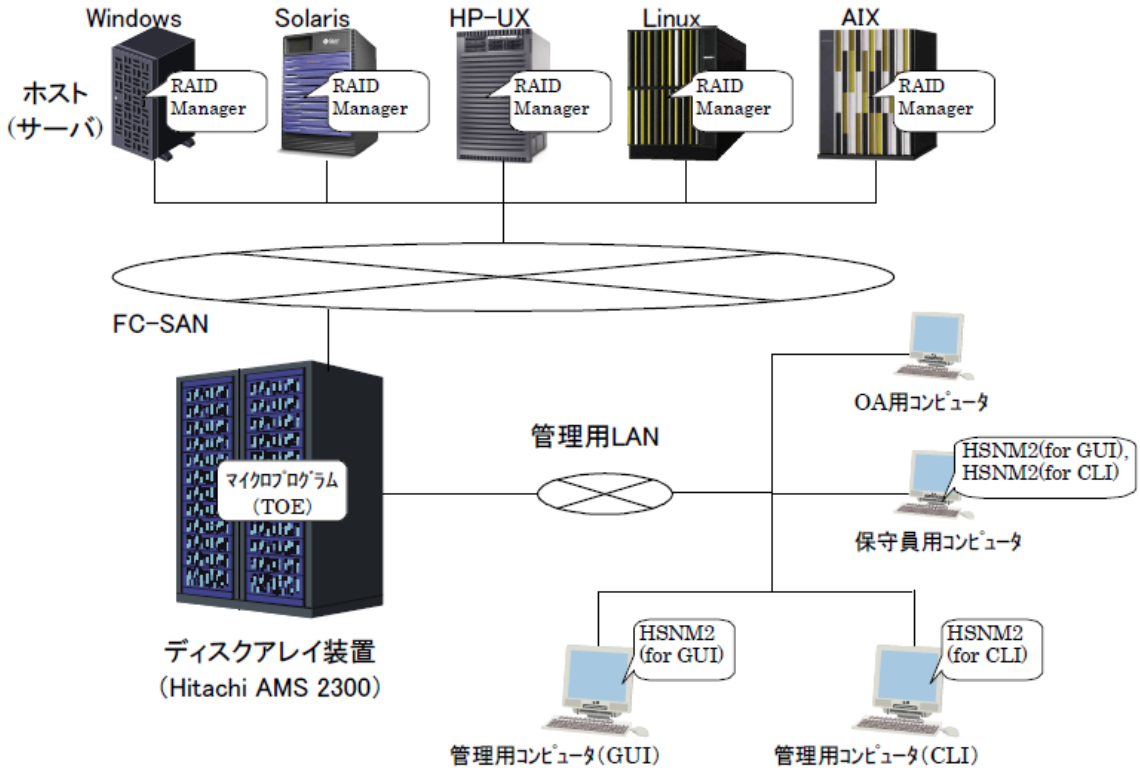

図1-1　ディスクアレイ装置を含むシステム構成

以下にシステム構成を説明する。

（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。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が、本評価ではRAID Manager を使用していない装置構成を対象とする。

（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。

（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）（以下Hitachi Storage Navigator Modular 2をHSNM2と略す）が導入されている。本コンピュータ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。本コンピュータとディスクアレイ装置は管理用LAN を介して接続される。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。

（6） 管理用コンピュータ（CLI）

管理用コンピュータ（GUI）と同様、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HSNM2（for CLI）が導入されている。

（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HSNM2（for GUI）または（for CLI）が導入されている。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。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。

（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。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。

ディスクアレイ装置の構成とTOEの関係は図1-2であり、TOEは、「マイクロプログラム」である。

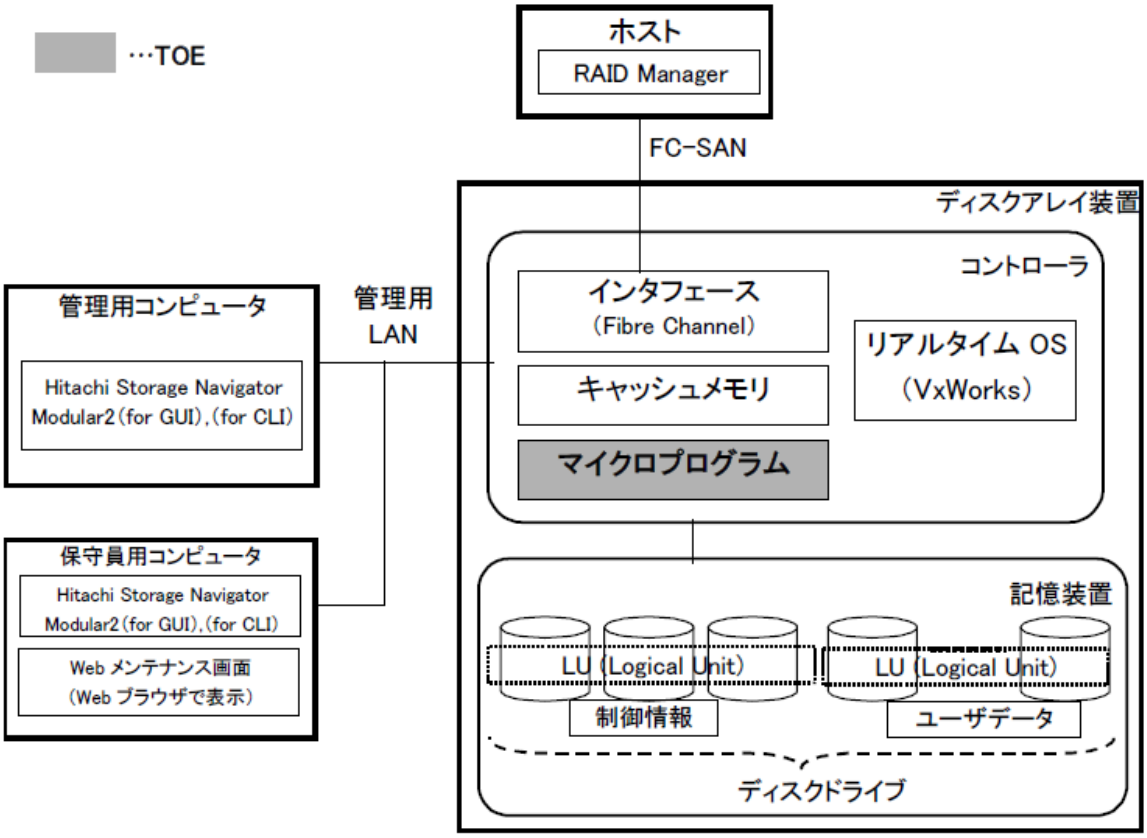

図1-2　ストレージ装置の構成とTOE

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。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。

以下にディスクアレイ装置の構成を説明する。

（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） インタフェース（Fibre Channel）

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。

（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

本評価の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。

（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。

1.2.4 TOEの関係者

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HSNM2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、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HSNM2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、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HSNM2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、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、HSNM2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。HSNM2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。

本報告書では上記(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。

1.2.5 TOEの機能

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。

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、HSNM2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。

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、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、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】

TOE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、HSNM2に配付する。ディスクアレイ装置を管理する際にHSNM2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。TOE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】

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】

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】
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

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。

1.3 評価の実施

認証機関が運営するITセキュリティ評価･認証プログラムに基づき、公表文書「ITセキュリティ評価及び認証制度の基本規程」[2]、「ITセキュリティ認証申請手続等に関する規程」[3]、「ITセキュリティ評価機関承認申請手続等に関する規程」[4]に規定された内容に従い、評価機関によってTOEに関わる機能及び保証要件の評価が実施された。

本評価の目的は、以下のとおりである。

① 本TOEのセキュリティ設計が適切であること。
② 本TOEのセキュリティ機能が、セキュリティ設計で記述されたセキュリティ機能要件を満たしていること。
③ 本TOEがセキュリティ設計に基づいて開発されていること。
④ 上記①、②、③を、CCパート３及びCEMの規定に従って評価すること。

具体的には、評価機関は、本TOEのセキュリティ機能の基本設計である「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」（以下「ST」という。）[1] 及び本TOE開発に関連する評価用提供物件及び本TOEの開発・製造・出荷の現場を調査し、本TOEがCCパート1 （[5][8][11]のいずれか）附属書B、CCパート2（[6][9][12]のいずれか）の機能要件を満たしていること、また、その根拠として、TOEの開発・製造・出荷環境がCCパート3（[7][10][13]のいずれか）の保証要件を満たしていることを評価した。この評価手順及び結果は、「評価報告書（BES-ETR-0001-02）」（以下「評価報告書」という。）[18]に示されている。なお、評価方法は、CEM（[14][15][16]のいずれか）に準拠する。また、CC及びCEMの各パートは補足[17]の内容を含む。

1.4 評価の認証

認証機関は、評価機関が作成した、評価報告書、所見報告書、及び関連する評価

証拠資料を検証し、本TOE評価が所定の手続きに沿って行われたことを確認した。認証の過程において発見された問題については、認証レビューを作成した。評価は、平成21年6月の評価機関による評価報告書の提出をもって完了し、認証機関が指摘した問題点は、すべて解決され、かつ、本TOE評価がCC及びCEMに照らして適切に実施されていることを確認した。認証機関は同報告書に基づき本認証報告書を作成し、認証作業を終了した。

1.5 報告概要

1.5.1 PP適合

適合するPPはない。

1.5.2 EAL

STが規定するTOEの評価保証レベルは、EAL2適合である。

1.5.3 セキュリティ機能強度

STは、最小機能強度として、”SOF-基本”を主張する。

本TOEは、脅威エージェントのもつ攻撃能力は「低」であることを想定しているため、SOF-基本で十分である。

1.5.4 セキュリティ機能

本TOEのセキュリティ機能については、「1.2.5 TOEの機能」を参照。

1.5.5 脅威

本TOEは、表1-1に示す脅威を想定し、これに対抗する機能を備える。

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。

表1-1　想定する脅威

識別子	脅　威
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。

1.5.6 組織のセキュリティ方針

TOEの利用に当たって要求される組織のセキュリティ方針を表1-2に示す。

表1-2 組織のセキュリティ方針

識別子	組織のセキュリティ方針
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。

1.5.7 構成条件

TOE は、株式会社日立製作所ディスクアレイ装置「Hitachi Adaptable Modular Storage 2300」に含まれる。

1.5.8 操作環境の前提条件

本TOEを使用する環境において有する前提条件を表1-3に示す。

これらの前提条件が満たされない場合、本TOEのセキュリティ機能が有効に動作することは保証されない。

表1-3 TOE使用の前提条件

識別子	前提条件
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 NavigatorModular 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）。 （注：Hitachi Storage Navigator Modular 2以外のツールではアクセスしないこと。） ・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。

	（注：保守作業に必要なWebメンテナンス画面の使用方法と操作手順の提供は保守員に限定すること。） ・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。

1.5.9 製品添付ドキュメント

本TOEに添付されるドキュメントを以下に示す。

- Hitachi Adaptable Modular Storage 2300 ISO/IEC15408 認証取得機能 取扱説明書（管理者編）
- Hitachi Adaptable Modular Storage 2300 ISO/IEC15408 認証取得機能 取扱説明書（利用者編）
- Hitachi Adaptable Modular Storage 2300 ISO/IEC15408 認証取得機能 取扱説明書（保守員編）
- Hitachi Adaptable Modular Storage2100/2300 シリーズ ディスクアレイ ユーザーズ ガイド

2 評価機関による評価実施及び結果

2.1 評価方法

評価は、CCパート3の保証要件について、CEMに規定された評価方法を用いて行われた。評価作業の詳細は、評価報告書において報告されている。評価報告書では、本TOEの概要説明、CEMのワークユニットごとに評価した内容及び判断が記載されている。

2.2 評価実施概要

以下、評価報告書による評価実施の履歴を示す。

評価は、平成20年5月に始まり、平成21年6月評価報告書の完成をもって完了した。評価機関は、開発者から評価に要する評価用提供物件一式の提供を受け、一連の評価における証拠を調査した。また、平成20年9月、平成21年2月、3月の3回、開発・製造現場へ赴き、記録及びスタッフへのヒアリングにより、構成管理・配付と運用の各ワークユニットに関するプロセスの施行状況の調査を行った。また、平成21年2月、3月に開発者サイトで開発者のテスト環境を使用し、開発者が実施したテストのサンプリングチェック及び評価者テストを実施した。

各ワークユニットの評価作業中に発見された問題点は、すべて所見報告書として発行され、開発者に報告された。それらの問題点は、開発者による見直しが行われ、最終的に、すべての問題点が解決されている。

また、評価の過程で認証機関による問題点の指摘として認証レビューが評価機関へ渡された。これらは評価機関及び開発者による検討ののち、評価に反映されている。

2.3 製品テスト

評価者が評価した開発者テスト及び評価者の実施した評価者テストの概要を以下に示す。

2.3.1 開発者テスト

1) 開発者テスト環境

開発者が実施したテストの構成を図2-1に示す。

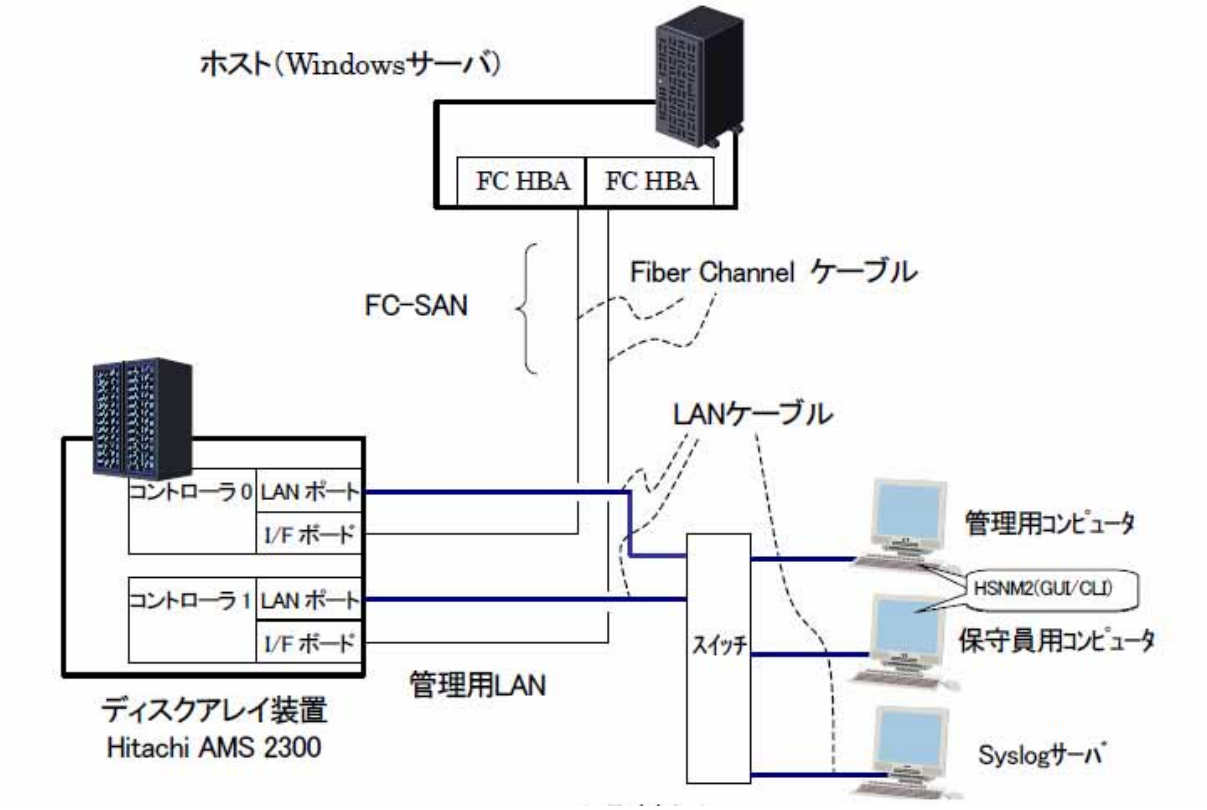

図2-1　開発者テストの構成図

2) 開発者テスト概説

開発者の実施したテストの概要は以下のとおり。

a. テスト構成

開発者が実施したテストの構成を図2-1に示す。開発者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b. テスト手法

テストには、以下の手法が使用された。

①テストツールであるHSNM2上での画面表示

②監査ログ機能による、結果記録

③テストツールであるHSNM2が記録する通信詳細ログ

c. 実施テストの範囲

テストは開発者によって17項目実施されている。

カバレージ分析が実施され、機能仕様に記述されたすべてのセキュリティ機能と外部インタフェースが十分にテストされたことが検証されている。深さ分析が実施され、上位レベル設計に記述されたすべてのサブシステムとサブシステムインタフェースが十分にテストされたことが検証されている。

d. 結果

開発者によるテスト結果は、期待されるテスト結果と実際のテスト結果が一致していることを確認している。評価者は、開発者テストの実施方法、実施項目の正当性を確認し、実施方法及び実施結果がテスト計画書に示されたものと一致することを確認した。

2.3.2 評価者テスト

1) 評価者テスト環境

評価者が実施したテストの構成は、開発者テストと同様の構成に、侵入テストでは侵入テスト用コンピュータ（ネットワーク上を流れるパケットの確認）を追加した。以下に構成を示す。

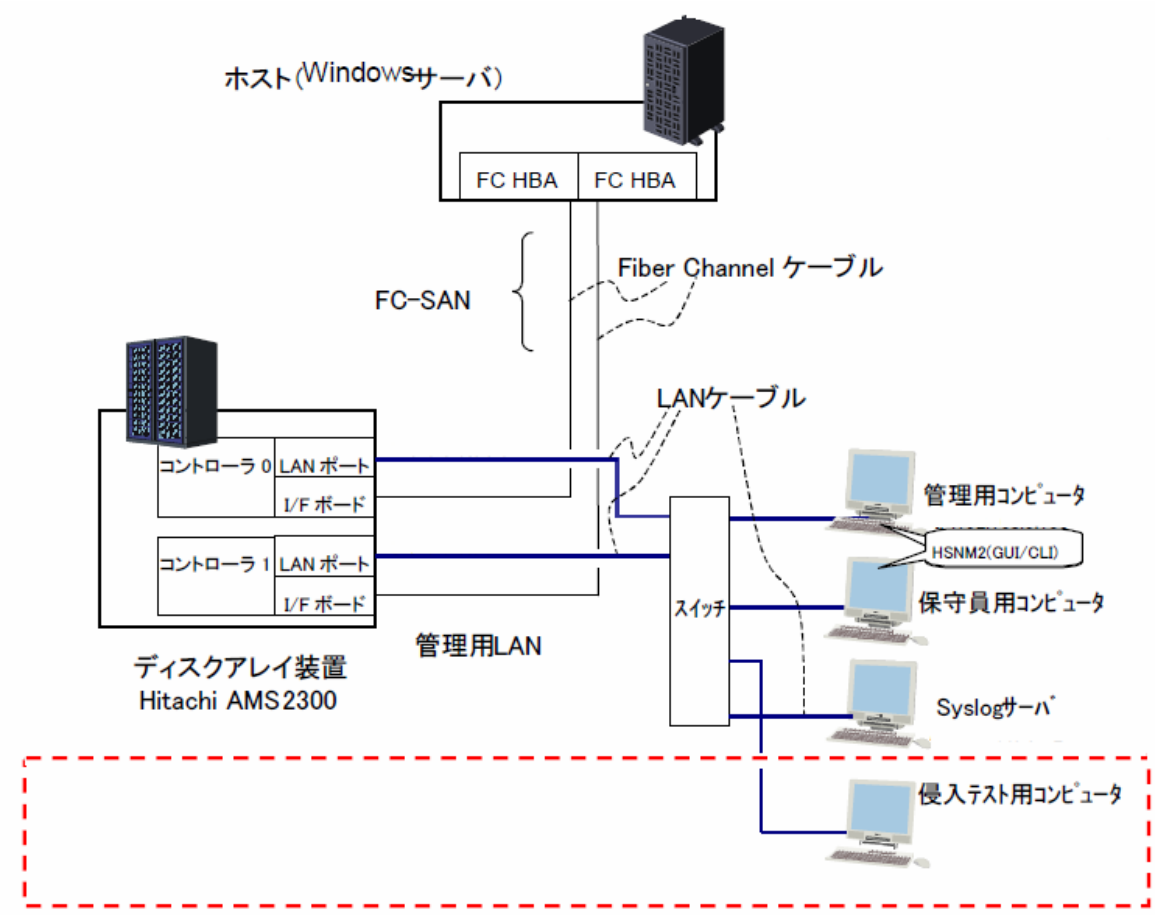

図2-2　評価者テストの構成図

2) 評価者テスト概説

評価者の実施したテストの概要は以下のとおり。

a. テスト構成

評価者が実施したテストの構成を図2-2に示す。評価者テストはSTにおいて識別されているTOE構成と同一のTOEテスト環境で実施されている。

b. テスト手法

テストには、以下の手法が使用された。

① 開発者テストと同じ手法で実施する。

② ネットワーク通信パケットのキャプチャを行い、通信内容の観察を実施する。

c. 実施テストの範囲

評価者が独自に考案した独立テストを9項目、侵入テストを6項目、開発者テストのサンプリングによるテストを13項目、計28項目のテストを実施した。テスト項目の選択基準として、下記を考慮している。

① 開発者テストは、セキュリティ機能の網羅性/重要性を考慮してサンプリングテストを実施する。

② 独立テストは、TSFI パラメータにおいて、組み合わせの網羅性、限界値にかかわる網羅性に関するテストを実施する。

③ 侵入テストは、開発者の脆弱性分析を元にした、通信エラーによるふるまい、設定情報の確認等や類似製品の情報からの不正利用に関するテストを実施する。

d. 結果

実施したすべての評価者テストは正しく完了し、TOEのふるまいを確認することができた。評価者はすべてのテスト結果は期待されるふるまいと一致していることを確認した。

2.4 評価結果

評価報告書をもって、評価者は本TOEがCEMのワークユニットすべてを満たしていると判断した。

3 認証実施

認証機関は、評価の過程で評価機関より提出される各資料をもとに、以下の認証を実施した。

① 当該所見報告書でなされた指摘内容が妥当であること。
② 当該所見報告書でなされた指摘内容が正しく反映されていること。
③ 提出された証拠資料をサンプリングし、その内容を検査し、関連するワークユニットが評価報告書で示されたように評価されていること。
④ 評価報告書に示された評価者の評価判断の根拠が妥当であること。
⑤ 評価報告書に示された評価者の評価方法がCEMに適合していること。

これらの認証において発見された問題事項を、認証レビューとして作成し、評価機関に送付した。

認証機関は、ST及び評価報告書において、所見報告書及び認証レビューで指摘された問題点が解決されていることを確認した。

4 結論

4.1 認証結果

提出された評価報告書、当該所見報告書及び関連する評価証拠資料を検証した結果、認証機関は、本TOEがCCパート3のEAL2に対する保証要件を満たしていることを確認した。

評価機関の実施した各評価者エレメントについての検証結果を表4-1にまとめる。

表4-1 評価者アクションエレメント検証結果

評価者アクションエレメント	検証結果
セキュリティターゲット評価	**適切な評価が実施された。**
ASE_DES.1.1E	評価はワークユニットに沿って行われ、TOE種別、境界の記述が明瞭であることを確認している。
ASE_DES.1.2E	評価はワークユニットに沿って行われ、TOE記述が理路整然とし一貫していることを確認している。
ASE_DES.1.3E	評価はワークユニットに沿って行われ、TOE記述がST全体の内容と一貫していることを確認している。
ASE_ENV.1.1E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が前提条件、脅威、組織のセキュリティ方針を漏れなく識別していることを確認している。
ASE_ENV.1.2E	評価はワークユニットに沿って行われ、TOEのセキュリティ環境の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.1E	評価はワークユニットに沿って行われ、ST概説がST及びTOEの識別、概要及びCC適合が明確に述べられていることを確認している。
ASE_INT.1.2E	評価はワークユニットに沿って行われ、ST概説の記述が理路整然とし一貫していることを確認している。
ASE_INT.1.3E	評価はワークユニットに沿って行われ、ST概説の記述がST全体の内容と一貫していることを確認している。
ASE_OBJ.1.1E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述にTOE及び環境のセキュリティ対策方針が、脅威、組織のセキュリティ方針、前提条件のいずれかへ遡れ、

	その対策方針の正当性をセキュリティ対策方針根拠が示していることを確認している。
ASE_OBJ.1.2E	評価はワークユニットに沿って行われ、セキュリティ対策方針の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_PPC.1.1E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_PPC.1.2E	評価はワークユニットに沿って行われ、PP主張が行われていないため非適用であることを確認している。
ASE_REQ.1.1E	評価はワークユニットに沿って行われ、TOE及びIT環境の要件の記述、操作がCCに準拠していること、要件の依存性、機能強度が適切であること、各要件がそれぞれの対策方針に遡れ、それらを満たす根拠が示されていること、要件のセットが内部的に一貫し、相互サポート可能な構造となっていることを根拠が示していることを確認している。
ASE_REQ.1.2E	評価はワークユニットに沿って行われ、ITセキュリティ要件の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
ASE_SRE.1.1E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_SRE.1.2E	評価はワークユニットに沿って行われ、CCを参照せずに明示された要件はないため非適用であることを確認している。
ASE_TSS.1.1E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が適切なセキュリティ機能及び保証手段を示していること、それらが機能要件や保証要件を満たす根拠が示されていること、ITセキュリティ機能に対する機能強度主張が機能要件に対する機能強度と一貫していることを確認している。
ASE_TSS.1.2E	評価はワークユニットに沿って行われ、TOE要約仕様の記述が完全で、理路整然としていて、かつ一貫していることを確認している。
構成管理	**適切な評価が実施された**

ACM_CAP.2.1E	評価はワークユニットに沿って行われ、TOEとその構成要素が一意に識別され、TOEになされる変更の管理・追跡が可能な手続きが妥当であり正しく適用されていることを確認している。
配付と運用	**適切な評価が実施された**
ADO_DEL.1.1E	評価はワークユニットに沿って行われ、TOE配付についてセキュリティ維持のために必要な手続きが規定され、実施されていることを確認している。
ADO_DEL.1.2D	評価はワークユニットに沿って行われ、実際に配付手続きが使用されていることを、実地検査により確認している。
ADO_IGS.1.1E	評価はワークユニットに沿って行われ、TOEがセキュアにセットアップされるための手順が提供されていることを確認している。
ADO_IGS.1.2E	評価はワークユニットに沿って行われ、ADO_IGS.1.1Eにて提供されたセットアップの手順がセキュアであることを確認している。
開発	**適切な評価が実施された**
ADV_FSP.1.1E	評価はワークユニットに沿って行われ、明確かつ矛盾なく機能仕様が記述され、そこにすべての外部セキュリティ機能インタフェースとそのふるまいが適切に記述されていること、機能仕様にTSFが完全に表現されていること、機能仕様がTSFを完全に表現している論拠を含んでいることを確認している。
ADV_FSP.1.2E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能要件の完全かつ正確な具体化であることを確認している。
ADV_HLD.1.1E	評価はワークユニットに沿って行われ、上位レベル設計が明確で矛盾のないこと、サブシステムを規定しそのセキュリティ機能を記述していること、TSF実現に必要なIT環境としてのハードウェア、ソフトウェアを説明していること、TSFサブシステムの外部とその他のインタフェースが識別され、それらの詳細を記述していることを確認している。

ADV_HLD.1.2E	評価はワークユニットに沿って行われ、上位レベル設計がTOEセキュリティ機能要件の正確かつ完全な具体化であることを確認している。
ADV_RCR.1.1E	評価はワークユニットに沿って行われ、機能仕様がTOEセキュリティ機能の正しく完全な表現であり、上位レベル設計が機能仕様の正しく完全な表現であることを、それらの対応分析により確認している。
ガイダンス文書	**適切な評価が実施された**
AGD_ADM.1.1E	評価はワークユニットに沿って行われ、管理者ガイダンスがTOEのセキュアな運用に必要な管理機能、権限、利用条件とセキュアな状態維持のための適切なセキュリティパラメタ、管理が必要となる事象と対処法を記述してあること、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
AGD_USR.1.1E	評価はワークユニットに沿って行われ、利用者ガイダンスがTOEの管理者でない利用者が利用可能なセキュリティ機能やユーザインタフェース、セキュリティ機能の使用法、対応すべき機能や特権に関する警告、TOEのセキュアな操作に必要なすべての利用者責任が記述してあり、他の証拠資料と一貫しておりIT環境に対するセキュリティ要件を記述してあることを確認している。
テスト	**適切な評価が実施された**
ATE_COV.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料に識別されているテストが機能仕様に正確に対応していることを確認している。
ATE_FUN.1.1E	評価はワークユニットに沿って行われ、テスト証拠資料がテスト計画、手順、期待される結果及び実際の結果を含み、テスト計画が目的を記述しセキュリティ機能を識別し、ST及びテスト手順記述と一貫していること、テスト手順記述がテストするセキュリティ機能のふるまいを識別しており再現可能な記述であること、テスト証拠資料が期待されるテスト結果を含んでおりそれらが実施結果と一致していることを確認し、開発者のテスト成果を報告している。

ATE_IND.2.1E	評価はワークユニットに沿って行われ、テスト構成がSTの記述と一貫し、TOEが正しく設定され、開発者テストと同等の資源が提供されていることを確認している。
ATE_IND.2.2E	評価はワークユニットに沿って行われ、テストサブセットとその証拠資料を作成し実施している。実施したテスト内容を記述し、結果が期待されるべき結果と一貫していることを確認している。また、本評価時に行われたテスト実施方法も適切と判断される。
ATE_IND.2.3E	評価はワークユニットに沿って行われ、サンプリングテストを実施し、結果が期待されるべき結果と一貫していることを確認している。また、本評価のサンプリング方針及びテスト実施方法も適切と判断される。
脆弱性評定	**適切な評価が実施された**
AVA_SOF.1.1E	評価はワークユニットに沿って行われ、STでSOF主張がなされているセキュリティメカニズムに対して、正当なSOF分析が行われ、SOF主張が満たされていることを確認している。
AVA_SOF.1.2E	評価はワークユニットに沿って行われ、すべての確率的または順列的メカニズムがSOF主張を持ち、そのSOF主張が正しいことを確認している。
AVA_VLA.1.1E	評価はワークユニットに沿って行われ、脆弱性分析が脆弱性に関する情報を考慮していること、識別された脆弱性について悪用されない根拠とともに記述していること、脆弱性分析がSTやガイダンスの記述と一貫していることを確認している。
AVA_VLA.1.2E	評価はワークユニットに沿って行われ、侵入テストとそれを再現可能な詳細を持つ侵入テスト証拠資料を作成しテストを実施している。実施したテスト結果とテスト概要について報告がなされている。

4.2 注意事項

本TOEの脅威エージェントは、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を利用した攻撃のみを想定している。

5 用語

本報告書で使用された略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

本報告書で使用されたTOE特有の略語を以下に示す。

HSNM2	Hitachi Storage Navigator Modular 2

本報告書で使用された用語を以下に示す。

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。
LU	Logical Unit の略。論理的に分けたディスクスペースの事。
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。

6 参照

[1] Hitachi Adaptable Modular Storage2300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

[2] ITセキュリティ評価及び認証制度の基本規程　平成19年5月　独立行政法人 情報処理推進機構　CCS-01

[3] ITセキュリティ認証申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-02

[4] ITセキュリティ評価機関承認申請手続等に関する規程　平成19年5月　独立行政法人 情報処理推進機構　CCM-03

[5] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model Version 2.3 August 2005 CCMB-2005-08-001

[6] Common Criteria for Information Technology Security Evaluation Part2: Security functional requirements Version 2.3 August 2005 CCMB-2005-08-002

[7] Common Criteria for Information Technology Security Evaluation Part3: Security assurance requirements Version 2.3 August 2005 CCMB-2005-08-003

[8] 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)

[9] 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)

[10] 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)

[11] ISO/IEC 15408-1:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005 Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements

[14] Common Methodology for Information Technology Security Evaluation : Evaluation Methodology Version 2.3 August 2005 CCMB-2005-08-004

[15] 情報技術セキュリティ評価のための共通方法: 評価方法 バージョン2.3 2005年8月　(平成17年12月翻訳第1.0版)

[16] ISO/IEC 18045:2005 Information technology - Security techniques - Methodology for IT security evaluation

[17] 補足-0512　平成17年12月

[18] 評価報告書(BES-ETR-0001-02) 第1.02版 2009年6月18日
株式会社電子商取引安全技術研究所 評価センター