認 証 報 告 書

独立行政法人情報処理推進機構
理事長 藤江 一正

原紙押印済

評価対象

申請受付日(受付番号)	平成24年8月10日 (IT認証2417)
認証番号	C0420
認証申請者	株式会社 日立製作所
TOEの名称	Hitachi Unified Storage 130用マイクロプログラム
TOEのバージョン	0917/A
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 ECSEC Laboratory 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25年12月12日

技術本部
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 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 バージョン3.1 リリース3
② 情報技術セキュリティ評価のための共通方法 バージョン3.1 リリース3

評価結果：合格

「Hitachi Unified Storage 130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セキュリティ認証等に関する要求事項に従い、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

この認証報告書は、株式会社 日立製作所が開発した「Hitachi Unified Storage 130 用マイクロプログラム 0917/A」(以下「本 TOE」という。)について株式会社 ECSEC Laboratory 評価センター(以下「評価機関」という。)が平成 25 年 10 月に完了した 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とともに、本 TOE に関心を持つ調達者や消費者に対しセキュリティ情報を提供するものである。

本認証報告書の読者は、本書の付属書であるセキュリティターゲット(以下「ST」という。)を併読されたい。特に本 TOE のセキュリティ機能要件、保証要件及びその十分性の根拠は、ST において詳述されている。

本認証報告書は、一般の調達者や消費者を読者と想定している。本認証報告書は、本 TOE が適合する保証要件に基づいた認証結果を示すものであり、個別の IT 製品そのものを保証するものではないことに留意されたい。

1.1 評価対象製品概要

本 TOE の機能、運用条件の概要を以下に示す。詳細は 2 章以降を参照のこと。

1.1.1 保証パッケージ

本 TOE の保証パッケージは、EAL2 である。

1.1.2 TOEとセキュリティ機能性

本 TOE は、株式会社 日立製作所のストレージ製品であるディスクアレイ装置「Hitachi Unified Storage 130」内部で動作する制御プログラム(ソフトウェア)である。

本 TOE は、ディスクアレイ装置に接続されるホストコンピュータがディスクアレイ上の割り当てられた記録領域にアクセスする際の制御を実行する。

本 TOE には、想定する脅威は存在せず、前提とする組織のセキュリティ方針を満たすためのセキュリティ機能を提供する。そのセキュリティ機能として、ホストコンピュータの要求に応じて記録領域へのアクセス制御を行う機能、識別認証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有している。

これらのセキュリティ機能性について、その設計方針の妥当性と実装の正確性について保証パッケージの範囲で評価が行われた。本 TOE が想定する前提については次項のとおりである。

1.1.2.1 脅威とセキュリティ対策方針

本 TOE は、想定される脅威が存在しないので、対抗するセキュリティ対策方針は存在しない。

1.1.2.2 構成要件と前提条件

本 TOE は、次の構成及び前提で運用することを想定する。

◆TOE の管理者は、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こと。

◆TOE の管理者は、TOE の利用に際して、ガイダンス文書通りの利用方法を忠実に守ることが要求されている。また、TOE に対してのガイダンス文書に記載されていない行為は、誤操作を含め一切禁止されている。

※たとえば、TOE の保守ポートへ PC を接続させる行為や、管理用端末に専用ユーティリティプログラムやブラウザ以外の TOE に関係のないソフトウェアをインストールする行為など、ガイダンス文書に記載されていない想定外の行為。

◆本 TOE は、TOE を含むディスクアレイ装置・ホストコンピュータ・ホストコンピュータとディスクアレイ装置を結ぶ専用ネットワーク・管理用端末・管理用端末とディスクアレイ装置を結ぶ LAN、これらすべては、管理者と保守員のみが入退出許可されて、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アクセスできないように設定されているセキュアな環境に設置されること。

◆本 TOE では、Syslog サーバへの監査ログ転送設定を有効にする場合、転送される監査ログは転送時・転送後すべての状況において、監査ログ管理者以外がアクセスできないようセキュアに管理されることが要求されている。また、TOE から取得した監査ログも監査ログ管理者によりセキュアに管理されること。

◆本 TOE は、TOE のセキュリティ機能である監査機能・管理者の識別認証機能・ホストコンピュータのアクセス制御機能の各機能について、製品設置時に各役割の管理者により機能が有効となるよう設定され、運用開始後は設定を無効にすることは許されない。

◆本 TOE のセキュリティ機能の管理機能の操作において、TOE に付随される専用ユーティリティプログラム「Hitachi Storage Navigator Modular 2 (21.70 版)」を利用する以外の操作を禁止されている。

◆TOE のセキュリティ機能の管理機能を操作する管理用端末では、TOE への WEB 操作(保守操作(保証内)及び専用ユーティリティプログラムでの WEB 画面の操作)以外は、一切の WEB アクセスを禁止されている。

◆TOE から取得したすべてのファイル(監査ログ除く)は、取得した管理者本人及び保守員以外がアクセスできないよう適切に管理され、また、保守員以外(取得した管理者本人含む)は取得したファイルを開いて内容を見ることは許されない。

※管理者向けのガイダンス文書にはこれらのファイルの存在は記載されていないため、管理者はファイルの存在を知らないが、障害発生時など保守員の指示によって管理者が管理用端末から識別認証不要の保守操作(保証内)を行い、TOE からディスクアレイ装置のメモリ情報など使用状況を示すトレース情報を取得する場合がある。しかし、ファイルにはセキュリティに係わる情報が含まれる可能性があることから、保守員以外のファイルの解読は許されない。

◆TOE の管理者は、管理用端末の専用ユーティリティプログラムがインストールされたディレクトリ内にあるすべてのファイルに対して、アクセスすることを禁止されている。

1.1.3 免責事項

1) 本 TOE は、ディスクアレイ装置へのホストコンピュータの接続を最大 2 台までの状態で評価がなされたため、ホストコンピュータが 3 台以上接続された状態での利用は、本評価による保証の対象外となる。

2) 本 TOE は、通常モードの状態から、ディスクアレイ装置の保守ポートへの PC 直接接続、または、ディスクアレイ装置上の物理スイッチ入力により、保守モードへ切り替えた時点で、その結果の環境は本評価構成の対象外であるため、保証対象外となる。

主な保守操作(保証外)は、以下の通りである。

・起動時の減設ハードディスク検出機能設定
電源オフ中にディスクアレイ装置から減設されたハードディスクがあった場合に、再起動時に減設されたことを検出し起動を防止する機能の設定

・初期化の実行
TOE 含むディスクアレイ装置を出荷時の状態に戻す機能

・フルダンプ採取機能
保守操作(保証内)で取得できるトレース情報では解析できない難解な障害発生時に、保守員がより詳細な障害解析を行うために使用される機能

3) 本 TOE は、セキュリティ機能である有償オプション「LUN Manager」、「Account Authentication」、「Audit Logging」の 3 種類以外のオプションソフトウェアを導入した場合の評価はなされていないため、上記 3 種類以外のオプションソフトウェアを導入しての運用は保証対象外となる。

4) 本 TOE は、出荷先が日本国内と日本国外の 2 種類あり、日本国内の場合は出荷先を限定していないが、日本国外の場合は出荷先が限定されており「Hitachi Data Systems Corporation」、「Hitachi Computer Products (America), Inc.」、「Hitachi Computer Products (Europe) S.A.S.」の日立グループ 3 社のみとなる。この 3 社から先の出荷に関しては、保証の対象外となる。

1.2 評価の実施

認証機関が運営する IT セキュリティ評価・認証制度に基づき、公表文書「IT セキュリティ評価及び認証制度の基本規程」[1]、「IT セキュリティ認証等に関する要求事項」[2]、「IT セキュリティ評価機関承認等に関する要求事項」[3]に規定された内容に従い、評価機関によって本 TOE に関わる機能要件及び保証要件に基づいて IT セキュリティ評価が実施され、平成 25 年 10 月に完了した。

1.3 評価の認証

認証機関は、評価機関が作成した評価報告書[13]、関連する評価証拠資料を検証し、本 TOE の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。認証機関が指摘した問題点は、すべて解決され、かつ、TOE の評価が CC([4][5][6]または[7][8][9])及び CEM([10][11]のいずれか)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。

2 TOE識別

本 TOE は、以下のとおり識別される。

TOE名称： Hitachi Unified Storage 130用マイクロプログラム
バージョン： 0917/A
開発者： 株式会社 日立製作所

製品が評価･認証を受けた本 TOE であることを、調達者及び消費者は以下の方法によって確認することができる。

本 TOE は、配付形態が日本国内向けと日本国外向けの 2 種類あり、日本国内向けの場合はディスクアレイ装置にインストールされた状態で配付され、日本国外向けの場合はソフトウェアイメージを ZIP ファイル化されて配付される。

確認方法は、日本国内向け・日本国外向けともに共通である。各ガイダンスの名称・版数を ST と同一であるか確認した上で、ディスクアレイ装置に保守ポートで接続された保守用端末の WEB 画面上、または、ディスクアレイ装置に LAN で接続された管理用端末の専用ユーティリティプログラムの画面上に、3 種類の情報が表示され、それらを組み合わせたものをガイダンスと照合することで、TOE の識別情報を認識できる。

これらにより、調達者及び消費者は設置された製品が評価・認証を受けた本 TOE であることを確認できる。

3 セキュリティ方針

本章では、本 TOE が採用したセキュリティ機能方針や組織のセキュリティ方針を説明する。

本 TOE は、ディスクアレイ装置に接続されたホストコンピュータからのアクセス要求に応じて、ディスクアレイ上の記録領域へのアクセスを実施する。

本 TOE は、ホストコンピュータからアクセス要求を受け付けると、要求電文に含まれるホストコンピュータの識別情報を元に、そのホストコンピュータが要求先の記録領域へのアクセスが許可されているかチェックを行い、許可されている場合のみ要求先へのアクセスを可能とする。この機能によって、許可されない記録領域へのアクセスを防止する。

本 TOE は、これらのセキュリティ機能を管理するための機能を提供し、信頼できる許可された管理者のみに管理機能の利用を可能とする。

本 TOE の管理者の役割は、「アカウント管理」、「ディスクアレイ管理」、「監査ログ管理」の 3 つの管理機能ごとに分けられ、さらにその中で、「監査ログ管理」に関しては、Syslog サーバ転送の設定権限を持つ「管理者[設定]」と、監査ログの読出し権限だけを持つ「管理者[読出し]」の 2 つに区分される。合わせて、4 つの管理者役割が存在する(表 3-1 参照)。

表 3-1 TOEの管理者役割

アカウント管理者	全管理者に対するアカウント設定、ログイン中管理者の強制ログアウト処理、無操作時間継続の上限値の設定
ディスクアレイ管理者	ホストコンピュータの記録領域割り当てに係わる管理
監査ログ管理者[設定]	監査ログ読出し、監査ログのSyslogサーバ転送の有効無効の設定
監査ログ管理者[読出し]	監査ログ読出し

本 TOE は、セキュリティに関する操作が行われた際に、その操作結果が監査対象事象であった場合のみ、監査ログが生成される。生成された監査ログは、監査ログ管理者[設定]及び監査ログ管理者[読出し]のみが参照を可能とする。

3.1 セキュリティ機能方針

TOE は、3.1.1 に示す脅威に対抗し、3.1.2 に示す組織のセキュリティ方針を満たすセキュリティ機能を具備する。

3.1.1 脅威とセキュリティ機能方針

3.1.1.1 脅威

本 TOE は、想定される脅威は存在しない。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、想定される脅威は存在しないので、対抗するセキュリティ機能方針は存在しない。

3.1.2 組織のセキュリティ方針とセキュリティ機能方針

3.1.2.1 組織のセキュリティ方針

本 TOE は、表 3-2 に示す組織のセキュリティ方針を要求する組織に限定して、提供を想定している。

表 3-2 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.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なければならない。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なければならない。
P.Audit	管理者による以下の操作事象を監査ログとして記録しなければならない。 ・管理者に対する識別・認証の成功・失敗事象 ・監査ログの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の初期設定・改変・削除のいずれかに該当する操作の

識別子	組織のセキュリティ方針
	成功・失敗事象 監査ログ記録領域が満杯になったとき、先頭の古いデータから順に新しいデータで上書きしなければならない。
P.User_role	TOEは、以下の利用者役割を区別しなければならない。 ・アカウント管理者[設定] 注) ・アカウント管理者[読出し] 注)（一般機能を提供される） ・ディスクアレイ管理者[設定] 注) ・ディスクアレイ管理者[読出し] 注)（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しなければならない。 ・アカウント管理者[設定] 注):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] 注):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] 注):ディスクドライブ記録媒体へのアクセス制御に係わる設定 ・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 注) 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]は、STで使用されている用語であって、本報告書内では定義されていない。これらの用語の意味は、 アカウント管理者[設定]：本報告書のアカウント管理者と同義 アカウント管理者[読出し]：管理者の管理情報を参照できる管理者のこと ディスクアレイ管理者[設定]：本報告書のディスクアレイ管理者と同義 ディスクアレイ管理者[読出し]：ディスクアレイの管理情報を参照できる管理者のこと 本組織のセキュリティ方針は、評価機関により読者が十分理解できるものと判断されているが、製品仕様に特化した

識別子	組織のセキュリティ方針
	利用者役割の詳細な要件を、組織の方針として読者が理解することは困難と判断し、認証機関として上記セキュリティ方針が意図する内容を以下に追記する。 セキュリティに係わる情報について、操作を許可される管理者を、以下の操作ごとに制限しなければならない。 ①ディスクアレイの記録領域に関する設定 ②監査ログに関する設定 ③監査ログの読出し ④管理者に関する設定
P.Session_timeout	管理者によるTOEの操作中に、無操作状態が継続する時間が定められた時間を超えたときに、その管理者のセッションを強制終了しなければならない。

3.1.2.2 組織のセキュリティ方針に対するセキュリティ機能方針

TOE は、表に示す組織のセキュリティ方針を満たす機能を具備する。

(1) 組織のセキュリティ方針「P.Exclusive_assign」への対応

本 TOE は､ホストコンピュータからのアクセス要求時には､ホストコンピュータに付与された識別情報を元にチェックを行い、あらかじめホストコンピュータへ割り当てられた記録領域にのみアクセスを許可する。

これらによって、P.Exclusive_assign を満たす。

(2) 組織のセキュリティ方針「P.Audit」への対応

本 TOE は、P.Audit に示されている事象の発生時には監査ログを生成し、監査ログの記録領域が満杯になった際には先頭のデータから順に新しいデータで上書きし新しい監査ログの損失を防ぐ。

これらによって、P.Audit を満たす。

(3) 組織のセキュリティ方針「P.User_role」への対応

本 TOE は、P.User_role に示されている操作を以下の管理者に制限する。

①ディスクアレイの記録領域に関する設定を、ディスクアレイ管理者のみに制限する
②監査ログに関する設定を、監査ログ管理者[設定]のみに制限する。

③監査ログの読出しを、監査ログ管理者[設定]及び監査ログ管理者[読出し]のみに制限する
④管理者に関する設定を、アカウント管理者のみに制限する

これらによって、P.User_role を満たす。

(4) 組織のセキュリティ方針「P.Session_timeout」への対応

本 TOE は、管理者の無操作継続時間が、あらかじめ管理者に設定された無操作継続時間の上限値を超えた場合は､その管理者のセッションを強制終了する。また、無操作継続時間の上限値設定を行う管理機能を、アカウント管理者のみに制限する。

これらによって、P.Session_timeout を満たす。

4 前提条件と評価範囲の明確化

本章では、想定する読者が本 TOE の利用の判断に有用な情報として、本 TOE を運用するための前提条件及び運用環境について記述する。

4.1 使用及び環境に関する前提条件

本 TOE を運用する際の前提条件を表 4-1 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 4-1 前提条件

識別子	前提条件
A.Environment	TOEは、TOEを含むディスクアレイ装置・ホストコンピュータ・ホストコンピュータとディスクアレイ装置を結ぶ専用ネットワーク・管理用端末・管理用端末とディスクアレイ装置を結ぶLAN、これらすべては、管理者と保守員のみが入退出許可されて、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アクセスできないように設定されているセキュアな環境に設置されること。 Syslogサーバへの監査ログ転送設定を有効にする場合、転送される監査ログは転送時・転送後すべての状況において、監査ログ管理者によりセキュアに管理されること。
A.Administrator	TOE の管理者は、TOE の利用に際して、ガイダンス文書通りの利用方法を忠実に守ることが要求されている。また、TOE に対してのガイダンス文書に記載されていない行為は、誤操作を含め一切禁止されている。 ※たとえば、TOEの保守ポートへPCを接続させる行為や、管理者用端末に専用ユーティリティプログラムやブラウザ以外のTOEに関係のないソフトウェアをインストールする行為など、ガイダンス文書に記載されていない想定外の行為。
A.Configuration	本TOEは、TOEのセキュリティ機能である監査機能・管理者の識別認証機能・ホストコンピュータのアクセス制御機能の各機能について、製品設置時に各役割の管理者により機能が有効となるよう設定され、運用開始後は設定を無効にすることは許されない。

4.2 運用環境と構成

本 TOE は、TOE を含むディスクアレイ装置とともに、ホストコンピュータ・ホストコンピュータとディスクアレイ装置を接続する専用ネットワーク・管理用端末・管理用端末とディスクアレイ装置を接続する LAN を含めて、TOE の管理者と保守員のみが入退出許可されて、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アクセスできないように設定されているセキュアな環境に設置される。もし、Syslog サーバに監査ログを転送する運用を行う場合は、Syslog サーバや Syslog サーバとディスクアレイ装置をつなぐネットワークもセキュアな環境に設置される必要がある。本 TOE の想定される運用環境例を図 4-1 に示す。

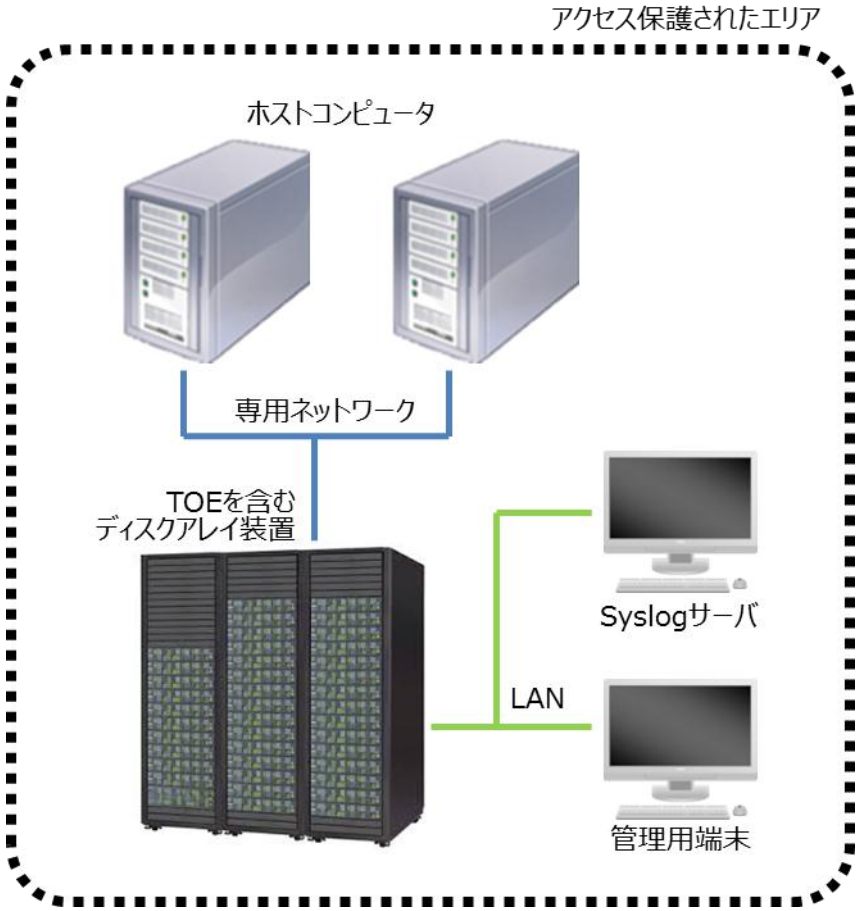

図 4-1 TOEの運用環境例

TOE を含むディスクアレイ装置は､最大 2 台まで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 構造を持つ大容量ストレージサービスを提供する。専用ネットワークには、FC-SAN(Fibre Channel Storage Area Network)と IP-SAN(IP Storage Area Network)の 2 種類を使用できる。また、接続されるホストコンピュー

タについては、特定の機種・種別に限定されず、動作環境も Windows、HP-UX、Solaris など多様な OS に対応している。

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で、TOE を操作するための専用ユーティリティプログラム「Hitachi Storage Navigator Modular 2 (21.70 版)」がインストールされる。このユーティリティプログラムは、TOE のセキュリティ機能の管理機能を利用するために必須のソフトウェアであり、TOE に付随して提供される。

図 4-1 には示されていないが、ディスクアレイ装置には保守員向けの保守用端末が接続されることがある。接続方法は、管理用端末と同様に LAN を介して接続される。

なお、本構成に示されているハードウェア及び連携するソフトウェアの信頼性は本評価の範囲ではない(十分に信頼できるものとする)。

4.3 運用環境におけるTOE範囲

本 TOE は、管理用端末から受信した電文に対して、TOE が受信するより先に管理用端末上の専用ユーティリティプログラム「Hitachi Storage Navigator Modular 2 (21.70 版)」による入力内容のチェックが行われることで、管理者の誤入力の機会を低減する。これにより、前提条件で求められている管理者による誤操作の禁止を現実的範囲内とすることから、管理用端末からの TOE の管理操作には、必ず専用ユーティリティプログラムを利用することが求められる。

5 アーキテクチャに関する情報

本章では、本 TOE の範囲と主要な構成(サブシステム)を説明する。

5.1 TOE境界とコンポーネント構成

TOE の構成を図 5-1 に示す。TOE はディスクアレイ装置内部の制御部ソフトウェアの部分である。TOE は、制御部ハードウェア上で動作する。TOE 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。

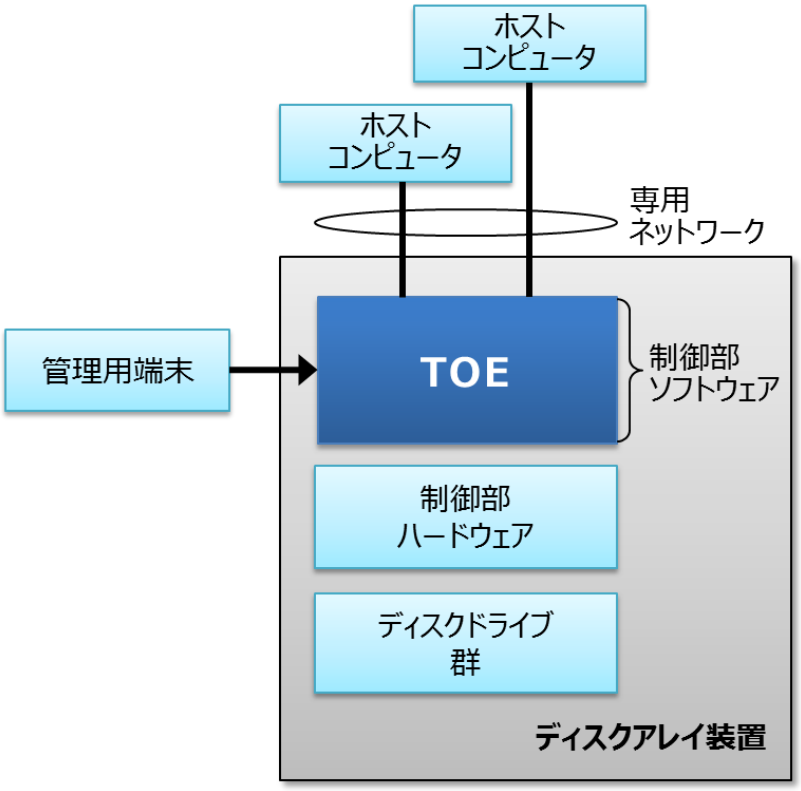

図 5-1 TOE境界

TOE を構成する主なサブシステムとして、記録領域の専有制御、管理者識別認証、監査について説明する。

◆記録領域の専有制御

ホストコンピュータをアクセス制御するサブシステム。ホストコンピュータから操作要求時に、要求電文に含まれるホストコンピュータの識別情報(WWNまたは iSCSI Name)と要求先の記録領域の識別情報を元に、TOE内部の登録情報をチェッ

クし、アクセスが許可されている場合(ホストコンピュータと記録領域がマッピングされている場合)のみ、要求先の記録領域へのアクセスを許可している。

◆管理者識別認証

管理者のログインと、管理者の各機能へのアクセスを制御するサブシステム。管理用端末からログイン要求時に、要求電文に含まれる管理者の識別情報とパスワードを元に、TOE内部の登録情報をチェックし、管理者として登録されている場合のみログインを許可する。許可された場合はセッションIDを発行し、セッションごとにログイン時点の管理者の識別情報・パスワード・管理者役割などの識別認証情報はTOE内部で保持され、ログアウトまでログイン時点の状態が有効となる。ログイン成功後、管理用端末から管理機能の操作要求時に、要求電文に含まれるセッションIDと操作コマンドを元に、TOE内部に登録されたセッションIDをチェックし有効であった場合、かつ、操作コマンドがログイン時点の管理者役割に許可された操作であった場合のみ、管理機能の操作を許可している。

◆監査

監査対象事象の操作に対して監査ログを生成するサブシステム。管理用端末から操作要求時に、アカウント認証制御サブシステムにより操作が許可されて、操作が成功または失敗し、その操作結果が監査対象事象であった場合に監査ログ制御サブシステムが呼ばれて、操作結果の監査ログを生成する。

5.2 IT環境

本 TOE は、ディスクアレイ装置内部の以下のハードウェア上で動作する。

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)

ホストコンピュータからは、要求電文が専用ネットワークを通じてディスクアレイ装置に送信され、ディスクアレイ装置に搭載のプロトコルチップにより要求電文の入力フォーマットチェックが行われ、入力内容が適切であれば要求電文を TOE へ送信し、受信した TOE は要求電文への処理を行う。

管理用端末からは、専用ユーティリティプログラムによって入力内容のチェックが行われ、入力内容が適切であれば専用ユーティリティプログラムによって株式会

社 日立製作所開発の独自プロトコルへ変換され、LAN を通じて TOE に送信されて、受信した TOE は要求電文への処理を行う。

6 製品添付ドキュメント

本 TOE に添付されるドキュメントの識別を以下に示す。TOE の利用者は、前提条件を満たすため下記ドキュメントの十分な理解と遵守が要求される。

本 TOE は、日本国内向け出荷の場合は表 6-1 の 1～12 のガイダンスが添付され、日本国外向け出荷の場合は表 6-1 のすべてのガイダンスが添付される。

表 6-1 ガイダンス文書一覧

種類	日本語版 英語版	
プログラム プロダクト ユーザーズガイド	1	Account Authentication ユーザーズガイド (HUS 100シリーズ) 第6版
		Hitachi Unified Storage 100 Account Authentication User's Guide 5th
	2	Audit Logging ユーザーズガイド (HUS 100シリーズ) 第5版
		Hitachi Unified Storage 100 Audit Logging User's Guide 5th
	3	LUN Manager ユーザーズガイド (HUS 100シリーズ) 第4版
		Hitachi Unified Storage 100 LUN Manager User's Guide 4th
ディスクアレイ ユーザーズガイド (保守あり)	4	HUS 100シリーズ ディスクアレイ ユーザーズガイド 第6版
		Hitachi Unified Storage 100 Series Disk Array System User's Guide 6th
	5	HUS 100シリーズ ディスクアレイ サービスガイド 第6版
		Hitachi Unified Storage 100 Series Disk Array System Service Guide 6th
ディスクアレイ ユーザーズガイド (保守なし)	6	Hitachi Unified Storage 130/150 ディスクアレイ ユーザーズ ガイド 第6版
		Hitachi Unified Storage 130/150 Disk Array System User’s Guide 6th
Hitachi Storage Navigator Modular 2 ユーザーズガイド	7	Hitachi Storage Navigator Modular 2(for GUI) ユーザーズガイド 第54版
		Hitachi Storage Navigator Modular 2(for GUI) User's Guide 54th
	8	Hitachi Storage Navigator Modular 2(for CLI) ユーザーズガイド 第58版
		Hitachi Storage Navigator Modular 2(for CLI) User's Guide 58th

種類	日本語版 英語版	
ホストインストールガイド	9	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 第3版
	10	Hitachi Unified Storage 100 Series Host Installation Guide for Fibre Channel Connection 3rd
	11	Hitachi Unified Storage 100シリーズ iSCSI接続用 ホストインストールガイド 第2版
		Hitachi Unified Storage 100 Series Host Installation Guide for iSCSI Connection 2nd
Hitachi Unified Storage 100 ISO/IEC15408 認証取得機能取扱説明書	12	Hitachi Unified Storage 100 ISO/IEC15408 認証取得機能取扱説明書(管理者/利用者編) 第2版
		Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Administrators/Users) 2nd
	13	Hitachi Unified Storage 100 ISO/IEC15408 認証取得機能取扱説明書(保守員編) 初版
		Hitachi Unified Storage 100 ISO/IEC15408 Certified Functions Guide (for Maintenance) 1st

7 評価機関による評価実施及び結果

7.1 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た。評価報告書では、本 TOE の概要と、CEM のワークユニットごとの評価内容及び判断結果を説明する。

7.2 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 24 年 8 月に始まり、平成 25 年 10 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 24 年 9 月に開発・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 24 年 9 月及び平成 25 年 7 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、認証機関が見つけた評価の問題点は、認証レビューとして記述されて、評価機関へ渡された。これらの指摘は、評価機関及び開発者が検討したのち、評価報告書に反映された。

7.3 製品テスト

評価者は、開発者の実施したテストの正当性を確認し、評価の過程で示された証拠と開発者のテストを検証した結果から、必要と判断された再現・追加テストを実行し、脆弱性評定に基づく侵入テストは不要と判断した。

7.3.1 開発者テスト

評価者は、開発者が実施した開発者テストの完全性と実際のテスト結果の証拠資料を評価した。評価者が評価した開発者テストの内容を以下に説明する。

(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 7-1 に示す。

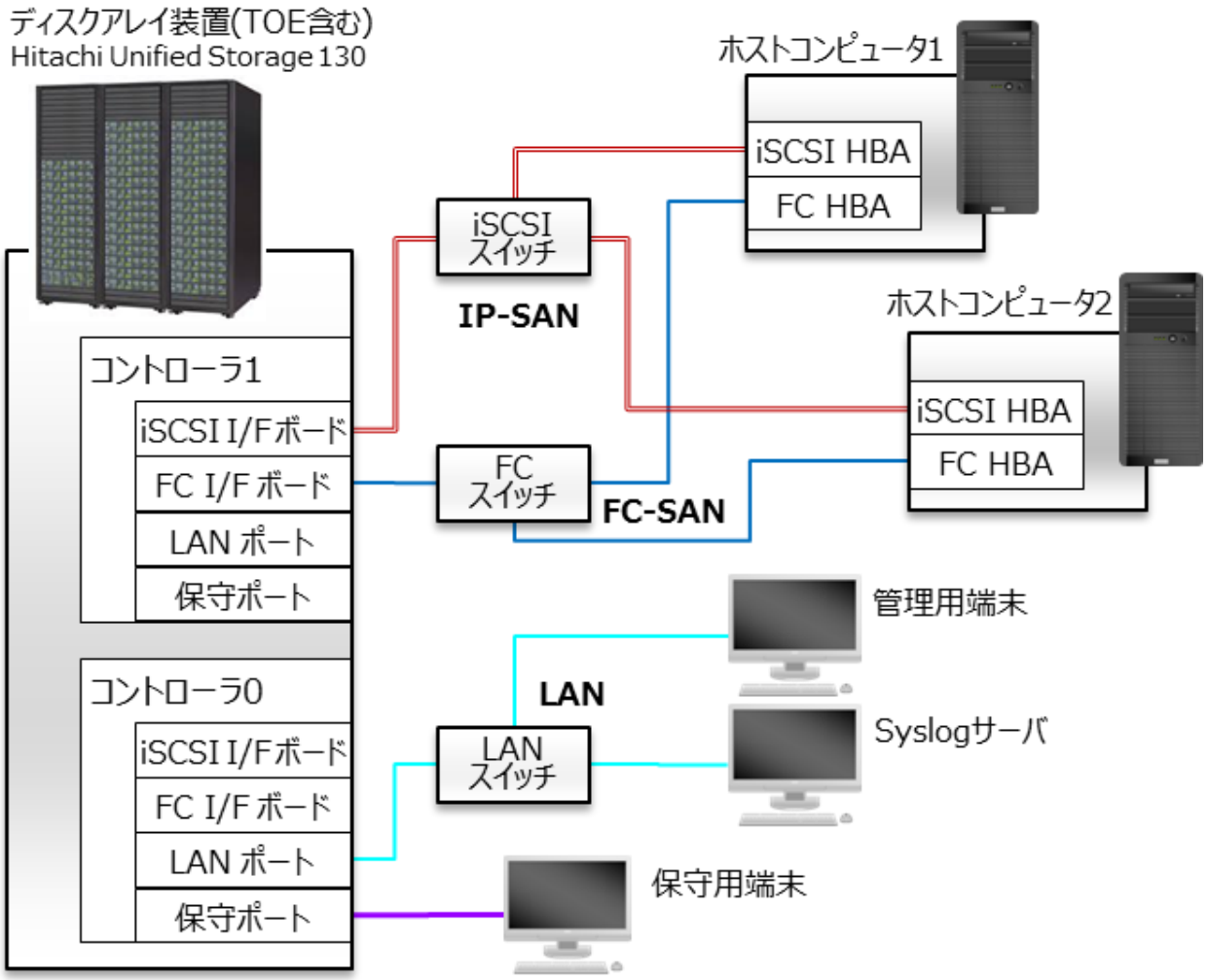

図 7-1 開発者テストの構成図

開発者テストの対象となったTOEは「Hitachi Unified Storage 130用マイクロプログラム 0917/A」である。

開発者テストにおけるTOE以外の構成要素を表7-1に示す。

表 7-1 TOE以外のテスト構成要素

#	名称	概要・利用目的
1	ディスクアレイ装置	TOEがインストールされるディスクアレイ装置「Hitachi Unified Storage 130」である。
2	ホストコンピュータ1	ディスクアレイ装置に専用ネットワークを介して接続する汎用PC。iSCSI用Host Bus Adapter(iSCSI HBA)とFibre Channel用Host Bus Adapter(FC HBA)を装備。 OS：Windows Server 2003 (R2)
3	ホストコンピュータ2	ホストコンピュータ1と同じ。
4	専用ネットワーク	ホストコンピュータとディスクアレイ装置を結ぶSANネットワーク。FC-SANとIP-SANの2種類。
5	FCスイッチ	装置型名：Brocade 300 FC-SANで結ばれているホストコンピュータとディスクアレイ装置間の中継装置。
6	iSCSIスイッチ	装置型名：Brocade 8000 IP-SANで結ばれているホストコンピュータとディスクアレイ装置間の中継装置。
7	LANスイッチ	装置型名：PCi FXG-05MK LANを中継するスイッチングハブ。
8	LAN	管理用端末・保守用端末・Syslogサーバとディスクアレイ装置を結ぶネットワーク。
9	管理用端末	管理用の汎用PC。専用ユーティリティプログラム「Hitachi Storage Navigator Modular 2 (21.70版)」、Javaランタイム「Java6 Update 10 (JRE 1.6.0_10)」をインストールする。 LANに接続する。 OS：Windows XP SP3 ブラウザ：Internet Explorer 8.0

#	名称	概要・利用目的
10	保守用端末	保守用の汎用PC。ディスクアレイ装置の保守ポートに直接接続するか、またはLANに接続する。保守ポートへ接続する構成は製品設置時の起動テストの場合であり、保守操作(保証内)のテストの場合はLANへ接続される。 OS：Windows XP SP3 ブラウザ：Internet Explorer 8.0
11	Syslogサーバ	TOEの監査ログ転送用の汎用PC。LANに接続する。 OS：Windows XP SP3
12	Syslogサーバ用ソフトウェア	ソフトウェア名称：Kiwi Syslog Daemon 8.3.48 監査ログの転送に関するテスト時に、転送先となるSyslogサーバ上で動く監査ログ受信用のソフトウェア。Syslogサーバへインストールされる。
13	SCSIコマンド発行ツール	ツール名称：Testtool.exe V1.3 ホストコンピュータからディスクアレイ装置内部の記録領域に対して、論理アドレスまでを指定したSCSIコマンド(Read/Write)を発行するツール。ホストコンピュータ上に保存されて実行される。
14	テスト用バッチファイル	ファイル名称：監査ログ上書き確認用構成作成スクリプト.bat TOEの監査ログを大量生成させるために監査対象事象を連続で実行するスクリプト。 管理用端末の専用ユーティリティプログラムから実行する。

開発者テストは本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。

(2) 開発者テスト概説

a) テスト概要

開発者テストの概要は、以下のとおりである。

【開発者テスト手法及び実施内容】

ホストコンピュータの記録領域へのアクセスに関しては､ホストコンピュータからTOEに対し､記録領域への操作要求を送信し､そのふるまいが確認され、期待値と結果の照合が行われた。

また、ホストコンピュータのテストの一部については、通常の操作では記録領域の論理アドレスまで指定した任意の領域へアクセスすることが不可能なため、記録領域の論理アドレスを指定した任意の領域へアクセスを行える要求コマンドを生成して送信するテストツールをホストコンピュータ上から実行することによって、そのふるまいが確認され、期待値と結果の照合が行われた。

TOE へのログイン、TOE の管理機能及び監査機能に関しては、管理用端末上の専用ユーティリティプログラムから TOE に対しログイン及び各機能への操作を行い、そのふるまいが確認され、期待値と結果の照合が行われた。

また、TOE の監査ログの領域が上限に達した際の上書き機能に関しては、管理用端末から監査対象事象の操作要求を連続で送信するテスト用バッチファイルを実行し、そのふるまいが確認され、結果と期待値との照合が行われた。

保守操作(保証内)に関しては、図 7-1 の構成図とは異なり保守用端末を LAN へ接続させて TOE への操作を行い、そのふるまいが確認され、期待値と結果の照合が行われた。

【開発者テストツール】

開発者テストにおいて利用したテストツールは表7-1の12～14が該当する。これらは評価者テストの際に評価者により動作確認が行われ、テストツールとしての適切性を確認されている。

b) 開発者テストの実施範囲

開発者テストは106項目実施された。カバレージ分析によって、機能仕様に記述されているセキュリティ機能とインタフェースがすべてテストされているか検証された結果、テストが十分でない機能は独立テストで補われた。

c) 結果

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、テスト計画書に示された実施方法と実際の実施方法が一致することを確認した。評価者は、開発者が期待したテスト結果と開発者によって実施されたテスト結果が一致していることを確認した。

7.3.2 評価者独立テスト

評価者は、開発者テストから抽出したテスト項目を使用して製品のセキュリティ機能が実行されることを再確認するサンプルテストを実施するとともに、評価の過程で示された証拠から、製品のセキュリティ機能が確実に実行されることをより確信するための独立テスト(以下「独立テスト」という。)を考案し実施した。評価者が実施した独立テストを以下に説明する。

(1) 独立テスト環境

評価者が実施した独立テストの構成は、開発者テストと同様の構成(図 7-1、表 7-1)である。ただし、図 7-1 に示されていないが、独立テストでは必要に応じて、LAN スイッチから置き換えたミラーリングハブのミラーポートへ試験用端末(汎用 PC)を接続する。

また、使用されたテストツールについては、開発者テストに用いられたものを利用するとともに、評価者が用意したものを追加で利用する。これらテストツールの仕様確認及び動作試験と校正は評価者によって実施されている。

(2) 独立テスト概説

評価者の実施した独立テストは以下のとおりである。

a) 独立テストの観点

評価者が、開発者テスト及び提供された評価証拠資料から考案した独立テストの観点を以下に示す。

【独立テストの観点】

①サンプリングテストでは、すべての開発者テストの中から、以下の理由で選出されたテスト項目に対してテストを行う。

・セキュリティ機能の実施が多いインタフェースを重点的に選びテストする
・パラメタが異なるだけの類似のテストについては、そのうちの 1 パターンのみをテストする

②すべてのインタフェースについて、最低 1 個のテストをサンプリングテストまたは独立テストのいずれかでカバーする。

③すべてのセキュリティ機能を含むように、開発者テストまたは独立テストでテストされるよう、テストサブセットを抽出する。その結果、開発者テ

ストには抜けているセキュリティ機能のふるまいが存在したため、独立テストでは、開発者テストでカバーされていない機能をテストする。

④開発者テストにおいては、パラメタや確認方法のバリエーションが不足しているため、独立テストでは、パラメタや確認方法を変えたテストを追加する。

⑤開発者テストで行われていなかったログイン中の管理者に対するデータの更新テストを行う。ログイン中の管理者に対して、別の管理者によってそのログイン中の管理者情報に影響を与え得る操作を行い、仕様通りに適切に処理されるか確認するテストを追加する。

b) **独立テスト概要**

評価者が実施した独立テストの概要は以下のとおりである。

【独立テスト手法】

開発者テストと同じ手法で実施された。ただし、必要に応じて、開発者テストの手法に付け加える形で、LAN に接続された試験用端末からテストツールによる通信の観察や記録が行われた。

【独立テストツール】

独立テストにおいて利用したテストツールは表 7-1 の 12～13 が該当する。上記以外に追加で利用されたツールを表 7-2 に示す。追加されたツールは試験用端末にインストールされて利用される。これらは評価者により動作確認が行われ、テストツールとしての適切性を確認されている。

表 7-2 独立テストで使用したツール

ツール名称	概要・利用目的
Wireshark Ver.1.10.0	このツールにより、LANの通信をキャプチャして、テスト中リアルタイムに観察したり、その通信内容を記録したものがテスト結果のエビデンスとして用いられる。

【独立テストの実施内容】

テストは、34 項目のサンプリングテストと、評価者により追加された 78 項目の独立テストが実施された。独立テストの観点とそれに対応したテスト内容を表 7-3 に示す。

表 7-3 実施した独立テスト

観点	テスト概要
①②	開発者が実施したテスト項目(106項目)から、独立テストの観点に基づいて抽出されたテスト項目(34項目)に対してテストを行い、開発者テストと同じ結果が得られることを確認する。
②③	TOEのインストールについて、開発者テストでは行われていなかったため、正常なTOEのインストールを試み、TOEが正しくインストールされることを確認する。
	開発者テストの補足として、監査ログの生成について、TOEの起動時・終了時における監査ログの生成が正しく行われることを確認する。
	開発者テストの補足として、TOEのセキュアな初期化について、破損したTOEのインストールを試み、TOEの自プログラムに対する完全性をチェックする機能によりインストールが失敗して、不完全なTOEがインストールされないことを確認する。
	開発者テストの補足として、記録領域にアクセス中のホストコンピュータについて、TOEに登録されている記録領域の割り当て情報を変更するテストを行い、変更した時点で即座にホストコンピュータのアクセスが拒否されることを確認する。
②④	パスワードの文字種や閾値、未入力など、開発者テストではパラメタのバリエーションが不足している機能のテストについて、パラメタを変更してテストを行う。
	データの整合性維持のために、同じ役割を持つ管理者の同時ログインを不可とする機能について、開発者テストでは不可・可ともに1つの役割に対してのみ確認されたため、すべての役割の確認が行えるよう、役割を変更して不可・可の両方のテストを行う。同時ログインが不可となる役割は、設定操作が可能な役割のみである。
	管理者のアクセス制御について、開発者テストでは各機能においてすべての役割の許可・拒否が確認されていないため、いずれかの機能ですべての役割が最低一度は許可・拒否の確認ができるようテストを行う。 また、役割は1人に対して複数設定が可能なことから、設定可能なすべての役割の組み合わせを確認できるようにテストを行う。

観点	テスト概要
	開発者テストの補足として、監査ログの出力項目に対して、区切り文字やファイル終端文字などの制御コードを混入させて入力を行い、それらの制御コードを空白に置換や除去するなど仕様通り適切に処理されて、監査ログが正しく出力されるか確認を行う。
②⑤	開発者テストの補足として、別々の役割を持つログイン中の管理者A・管理者Bに対して、アカウント管理者Cにより管理者Aの役割を管理者Bと同じ役割へ変更を行い、管理者Aには変更後の役割がログアウト時まで反映されないことで、同じ役割の同時ログイン不可が守られ、整合性のないデータ生成が防止できることを確認する。
	開発者テストの補足として、ログイン中の管理者について、別の管理者によりログイン中の管理者のアカウント削除を行い、削除した時点で該当の管理者のセッションが即無効となることで、削除済の管理者による操作を防止できることを確認する。

c) **結果**

評価者が実施したすべての独立テストは正しく完了し、評価者はTOEのふるまいを確認した。評価者は、すべてのテスト結果と期待されるふるまいが一致していることを確認した。

7.3.3 評価者侵入テスト

評価者は、評価の過程で示された証拠から、想定される使用環境と攻撃レベルにおいて懸念される脆弱性となる可能性があるものについて、評価者侵入テスト(以下「侵入テスト」という。)を実施する必要性の分析を行なった結果、以下の前提条件により懸念される脆弱性は存在せず、侵入テストは不要と判断した。

◆本 TOE では、前提条件により、TOE の運用環境は、管理者と保守員のみが入退出許可されて、外部ネットワークからアクセスできないように設定されているセキュアな環境となっている。

◆本 TOE では、前提条件により、悪意のある管理者が存在しない。

◆本 TOE では、前提条件により、TOE に関してガイダンスにある利用方法以外は一切行なわれない。誤操作も起きない。

よって、評価者は、TOE において懸念される脆弱性が前提条件によって皆無であることを確認し、侵入テストが不要であることを、適切であると判断した。

7.4 評価構成について

本評価では、「7.3.2 評価者独立テスト」及び図 7-1 に示す構成において、評価を行った。

本 TOE は、たとえばディスクアレイ装置へホストコンピュータを 3 台以上接続するなど、上記の評価構成と異なる構成で運用される場合を想定されていない。

よって、評価者は、上記の評価構成は、適切であると判断した。

7.5 評価結果

評価者は、評価報告書をもって本 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。

評価では以下について確認された。

セキュリティ機能要件：コモンクライテリア パート 2 適合

セキュリティ保証要件：コモンクライテリア パート 3 適合

評価の結果として、以下の保証コンポーネントについて「合格」判定がなされた。

EAL2 パッケージのすべての保証コンポーネント

評価の結果は、第 2 章に記述された識別に一致する TOE によって構成されたもののみに適用される。

7.6 評価者コメント/勧告

調達者に喚起すべき評価者勧告は、特にない。

8 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 所見報告書でなされた指摘内容が妥当であること。

② 所見報告書でなされた指摘内容が解決されていること。

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、本 ST 及び評価報告書において、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、本認証報告書を発行した。

8.1 認証結果

提出された評価報告書、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すものと判断する。

8.2 注意事項

本 TOE では、1.1.3 免責事項の行為がなされた場合、それ以降の本 TOE のセキュリティ機能への影響については保証の範囲外となる。よって、1.1.3 免責事項の受入れについては、管理者の責任において判断されたい。

本 TOE は、製品仕様に依存した前提条件や組織のセキュリティ方針を多く想定している。また、保証範囲も非常に限られたものになっている。読者は、それらの要件や保証範囲が自身の組織の運用環境に適応するものであるかを、導入前に十分検討する必要がある。

9 附属書

特になし。

10 セキュリティターゲット

本 TOE のセキュリティターゲット[12]は、本報告書とは別文書として以下のとおり本認証報告書とともに提供される。

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
バージョン 1.2, 2013 年 9 月 25 日, 株式会社 日立製作所

11 用語

本報告書で使用されたCCに関する略語を以下に示す。

CC	Common Criteria for Information Technology Security Evaluation (セキュリティ評価基準)
CEM	Common Methodology for Information Technology Security Evaluation (セキュリティ評価方法)
EAL	Evaluation Assurance Level (評価保証レベル)
PP	Protection Profile (プロテクションプロファイル)
ST	Security Target (セキュリティターゲット)
TOE	Target of Evaluation (評価対象)
TSF	TOE Security Functionality (TOEセキュリティ機能)

本報告書で使用されたTOEに関する用語を以下に示す。

アカウント管理者	TOEの管理者管理を許可された管理者。管理者に対する設定を行う。
オプション ソフトウェア	ディスクアレイ装置の有償オプション機能となるソフトウェア。TOEの一部として、あらかじめディスクアレイ装置にインストール済であるが不活性となっており、各オプションのライセンスキーの入力により初めて活性化される。 TOEのセキュリティ機能である監査機能・管理者の識別認証機能・ホストコンピュータのアクセス制御機能は、製品設置時にオプションソフトウェア「Audit Logging」、「Account Authentication」、「LUN Manager」を活性化することで有効となる。 なお、それらの3種類以外のオプションソフトウェアの活性化はガイダンスによって禁止されている。
ディスクアレイ 管理者	TOEのディスクアレイ管理を許可された管理者。ホストコンピュータのディスクアレイ上の記録領域割当てに関する設定を行う。
ディスクアレイ装置	TOEがインストールされるディスクアレイ装置「Hitachi Unified Storage 130」のこと。
監査ログ管理者 [設定]	TOEの監査ログ読出し、監査ログのSyslogサーバ転送の有無の設定を許可された管理者。

監査ログ管理者 [読出し]	TOEの監査ログ読出しを許可された管理者。
管理者	TOEのセキュリティ機能の管理機能である、ディスクアレイ管理・アカウント管理・監査ログ管理の操作を許可された管理者の総称。
管理用端末	管理者がTOEのセキュリティ機能の管理機能を操作する際に使用される端末のこと。場合により、管理者による保守操作(保証内)にも使用される。 OS：Windows XP SP3、ブラウザ：IE 8.0が動作する汎用製品。
専用ユーティリティプログラム	管理用端末にインストールされる専用のユーティリティプログラム「Hitachi Storage Navigator Modular 2 (21.70版)」のこと。TOEに付属されている。TOEのセキュリティ機能の管理機能を操作する際には、本プログラム使用以外の操作は禁止されている。動作にはJavaランタイム「Java 6 Update 10 (JRE 1.6.0_10)」を必要とする。コマンドラインまたはWEBと、2種類のユーザインタフェースがある。
通常モード	保守モードに切り替わっていない通常の運用状態のこと。
保守ポート	ディスクアレイ装置に装備されている保守用端末を直接接続するポートのこと。
保守モード	保守用端末を保守ポートへ接続するか、またはディスクアレイ装置上の物理スイッチ入力を行うことで、切り替えられる保守の状態のこと。この切り替え操作は保守員のみが行える。これらの手順を踏んでモードを切り替えた時点で保証対象外となる。
保守員	ディスクアレイ装置の保守作業を行う。
保守操作(保証外)	保守モードへ切り替えられた後に、保守ポートまたはLANに接続された保守用端末から、WEB経由で保守画面を表示して行える保証対象外の保守操作のこと。この保守画面の操作には識別認証は不要。この操作は保守員のみが行う。

保守操作(保証内)	通常モード時に、ディスクアレイ装置とLANで接続されたPCからWEB経由で保守画面を表示して行える保守操作のこと。この保守画面の表示には識別認証は不要。ディスクアレイ装置内のメモリ情報など使用状況を示すトレース情報及び構成情報(構成部品の種別・数量・ステータスなど)を取得でき、この操作は保守員または管理者が行える。この保守操作を行っても保証対象外とはならない。
保守用端末	保守員がTOEの保守操作(保証内)及び保守操作(保証外)を行う際に使用される端末のこと。

本報告書で使用された用語の定義を以下に示す。

ホスト コンピュータ	本TOEを含むディスクアレイ装置が提供するストレージサービスを利用するために接続させるPCのこと。本ディスクアレイ装置が提供しているインタフェースは特定のファイルシステムに依存せず、Windows、HP-UX、Solarisなど多様なOSを利用できる。
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。本TOEを含むディスクアレイ装置は、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タイプとなる。
FC-SAN	FC-SAN(Fibre Channel Storage Area Network)とは、光ファイバーを媒体とするネットワークのこと。
IP-SAN	IP-SAN(IP Storage Area Network)とは、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のこと。
WWN	WWN(World Wide Name)とは、FC-SAN経由で接続されるホストコンピュータの場合、ホストコンピュータに搭載のFibre Channel HBA(Host Bus Adaptor)に固有番号として付与される識別情報のこと。
iSCSI Name	iSCSI Nameとは、IP-SAN経由で接続されるホストコンピュータの場合、ホストコンピュータに搭載のiSCSI HBA(Host Bus Adaptor)に固有情報として付与される識別情報のこと。

12 参照

[1] ITセキュリティ評価及び認証制度の基本規程, 平成24年3月, 独立行政法人情報処理推進機構, CCS-01

[2] ITセキュリティ認証等に関する要求事項, 平成25年4月, 独立行政法人情報処理推進機構, CCM-02

[3] ITセキュリティ評価機関承認等に関する要求事項, 平成25年4月, 独立行政法人情報処理推進機構, CCM-03

[4] Common Criteria for Information Technology Security Evaluation Part1: Introduction and general model, Version 3.1 Revision 3, July 2009, CCMB-2009-07-001

[5] Common Criteria for Information Technology Security Evaluation Part2: Security functional components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-002

[6] Common Criteria for Information Technology Security Evaluation Part3: Security assurance components, Version 3.1 Revision 3, July 2009, CCMB-2009-07-003

[7] 情報技術セキュリティ評価のためのコモンクライテリア パート1: 概説と一般モデル, バージョン3.1 改訂第3版, 2009年7月, CCMB-2009-07-001, (平成21年12月, 翻訳第1.0版)

[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, 2009年7月, CCMB-2009-07-002, (平成21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, 2009年7月, CCMB-2009-07-003, (平成21年12月, 翻訳第1.0版)

[10] Common Methodology for Information Technology Security Evaluation : Evaluation methodology, Version 3.1 Revision 3, July 2009, CCMB-2009-07-004

[11] 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3.1 改訂第3版, 2009年7月, CCMB-2009-07-004, (平成21年12月, 翻訳第1.0版)

[12] 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, バージョン 1.2, 2013年9月25日, 株式会社 日立製作所

[13] Hitachi Unified Storage 130用マイクロプログラム 0917/A 評価報告書(ETR), 第2.3版, 2013年10月8日, 株式会社 ECSEC Laboratory 評価センター