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22年10月26日 (IT認証0313)
認証番号	C0315
認証申請者	株式会社 日立製作所
TOEの名称	Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500用制御プログラム
TOEのバージョン	70-02-05-00/00(R7-02-06A)
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	みずほ情報総研株式会社 情報セキュリティ評価室

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23年9月30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 Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500用制御プログラム」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

この認証報告書は、株式会社 日立製作所が開発した「Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 用制御プログラム、バージョン 70-02-05-00/00(R7-02-06A)」（以下「本 TOE」という。）についてみずほ情報総研株式会社 情報セキュリティ評価室（以下「評価機関」という。）が平成 23 年 8 月 31 日に完了した 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 に関心を持つ消費者や調達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、市販される本 TOE を購入する一般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、大型のストレージ装置 Hitachi Virtual Storage Platform（別名 Hitachi Virtual Storage Platform VP9500）を動作させる専用プログラムである。本 TOE は、ホストコンピュータ（以下「ホスト」という。）が Hitachi Virtual Storage Platform（以下「ストレージ装置」という。）へ接続してデータの読み書きを行う時に、そのホストを識別、認証して、そのホストコンピュータから決められた記憶領域への読み書きを制御する機能を有する。本 TOE は、ストレージ装置がデータを暗号化して記憶領域へ保存する時に使用する暗号鍵を安全に管理する機能と、記憶領域からデータを安全に消去する機能を有する。

また TOE は、TOE の利用者（ストレージ管理者、保守員）に対して利用者の識別と認証を実施し、与えられた権限の範囲に沿って、以下のストレージ装置を操作する機能を安全に提供する。ストレージ管理者は、TOE へホストを識別、認証するための各種情報を設定する機能、対応する記憶領域の設定とそこへのアクセスを制御するルールを設定する機能を使用する。保守を行う保守員は、ストレージ装置の

設置時やハードウェアの交換時、障害復旧時の各種設定機能、TOE をネットワークへ接続し、外部認証サーバやリモートデスクトップクライアントを接続するための設定機能を使用する。

これらのセキュリティ機能が悪用されることを防ぐため、TOE は、利用者の識別と認証を実施し、以下の TOE の利用者（セキュリティ管理者、監査ログ管理者）のみへ TOE を管理する機能の使用を許可する。セキュリティ管理者は、利用者のアカウントを管理する機能、利用者のグループや記憶領域などのリソースを管理する機能、ホストやファイバチャネルスイッチの識別・認証機能や暗号化関連機能などのセキュリティ機能の設定機能を使用する。監査ログ管理者は、監査ログを閲覧する機能を使用する。TOE と TOE 外の TOE の動作に必要なプログラムは、相互に識別・認証し、暗号化通信を使用する。

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 が想定する脅威及び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､以下のとおりのセキュリティ機能によりそれぞれの脅威に対抗する。

本 TOE は、接続が許可されていない不正なホストが、ストレージ装置の記憶装置に保存されているストレージ利用者のユーザデータを閲覧したり、改ざんしたりすることを防ぐために、ホストの接続許可、ホスト―TOE 間の安全な通信、ホストのアクセス制御などを実施し、接続が許可されたホストのみへユーザデータへのアクセスを許可する。

本 TOE は、TOE の管理用のインタフェースに接続した攻撃者によって、TOE のセキュリティ機能の設定が変更され、ストレージ装置の記憶装置に保存されているストレージ利用者のユーザデータが不正に閲覧されたり改ざんされたりすることを防ぐために、TOE の利用者（セキュリティ管理者、ストレージ管理者、監査ログ管理者）の識別認証、利用者のアクセス制御、Storage Navigator プログラム―SVP プログラムの間の SSL 通信、セキュリティ機能の管理などを実施し、TOE のセキュリティ機能の設定の不正な変更を防止する。

また、ストレージ装置の記憶装置へ残存するデータの漏えいを防ぐために、記憶装置へ保存するユーザデータの暗号化を支援する暗号鍵の管理機能と、記憶装置の使用領域をダミーデータで上書きして残存データを消去するシュレッディング機能を実施する。TOE は、セキュリティ機能に関係する事象をログへ記録し、不正操作を抑止、軽減する。

1.1.2.2 構成要件と前提条件

評価対象製品は、次のような構成及び前提で運用することを想定する。

本 TOE を含んだストレージ装置、ホスト（ファイバチャネル接続アダプタを含む)、ファイバチャネルスイッチ、他のストレージ装置、外部認証サーバは、許可された者だけが入退室が可能なセキュアなエリアに設置すること。上記の装置の不正な利用が行われないように、セキュリティ管理者は、装置の利用者や構成、セキュリティ対策などについて、適切な運用管理を行うこと。

管理 PC は、不正に利用されないよう、直接監視できる場所へ、外部ネットワークから直接アクセスできないよう制限されたネットワークに接続された状態で設置すること。管理 PC の利用者や管理者の識別認証とアカウント管理、ウイルス対策ソフトウェアの導入、セキュリティパッチの適用、危険なソフトウェアのインストール制限などを行うこと。

本 TOE と外部認証サーバの間は、LDAPS、starttls、RADIUS（CHAP 認証）のいずれかのプロトコルを用いて通信を行うこと。RADIUS プロトコルを使用する場合、外部認証サーバは、CHAP シークレットを用いた CHAP 認証を使用可能な RADIUS プロトコルに対応しており、CHAP シークレットを使用して CHAP 認証を行うこと。

セキュリティ管理者、監査ログ管理者、保守員は不正行為を行わないこと。

1.1.3 免責事項

本 TOE は、以下の脅威に対抗していない。また本 TOE は、以下の TOE の使い方において、情報セキュリティ上の安全を保証できない。

本 TOE は、攻撃者がストレージエリアネットワークまたは TOE へ接続済みのホストを乗っ取り、TOE がホストを識別・認証するための WWN、シークレットを設定または変更し、他のホストになりすまして TOE へ接続する脅威には、対抗できない。TOE へ接続したホストが攻撃者に乗っ取られた場合、保証されない。

保守員は、外部 LAN 側から TOE へログインしてはいけない。

監査ログの Syslog 転送を行った場合、転送先の監査ログのセキュリティは保証されない。

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 セキュリティ認証申請手続等に関する規程」[2]、「IT セキュリティ評価機関承認申請手続等に関する規程」[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 23 年 8 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]、所見報告書、及び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 Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500用 制御プログラム
バージョン：	70-02-05-00/00(R7-02-06A)
開発者：	株式会社 日立製作所

TOE は、以下の 2 つのプログラムから構成される。

TOE名称：	DKCMAINマイクロプログラム
バージョン：	70-02-05-00/00
開発者：	株式会社 日立製作所

TOE名称：	SVPプログラム （Storage Navigatorプログラム含む）
バージョン：	70-02-03/00
開発者：	株式会社 日立製作所

上記のプログラム以外に接続するホストの種類に応じた追加プログラムなどが存在するが、本 TOE は、それらのオプションを含まない。

製品が評価･認証を受けた本 TOE であることを、利用者は以下の方法によって確認することができる。保守員向けのメンテナンスマニュアルに記載された手順に従い、Storage Navigator プログラムまたは SVP（Service Processor）プログラムのメニューから DKCMAIN マイクロプログラム及び SVP プログラムのバージョン番号を表示させ、その名称及びバージョンと利用者向けのユーザーズマニュアルや保守員向けのメンテナンスマニュアルの当該記載を比較することにより、設置された製品が評価を受けた本 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 が脅威に対抗するために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。

TOE は、ストレージ装置に接続したホストからストレージ装置上に格納された保護対象であるユーザデータへのアクセスを制御するプログラムと、その設定を管理する機能を提供するプログラムである。

TOE のセキュリティ機能は、ホストの識別とアクセス制御によるホスト経由のユーザデータの改ざんや漏えいの防止と、ストレージ装置がユーザデータの暗号化処理に使用する暗号鍵の安全な管理とユーザデータの完全消去による取り出したハードディスク上からの漏えいの防止を実現している。

TOE は、TOE の利用者に対して利用者の識別と認証を実施し、利用者の権限の範囲内のストレージ装置を操作する機能と TOE を管理する機能の使用を許可し、誤った機能の使用を防止する。外部 LAN を介した TOE と外部認証サーバ、Storage Navigator プログラムの通信は、相互の識別・認証と暗号化通信を使用し、TOE の利用者へのなりすましを防止する。また TOE は、セキュリティ機能に関係する事象をログへ記録し、不正操作を抑止、軽減する。

TOE は、これらの機能性の実装を保護するメカニズムを持つ。

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、表 3.1-1 に示す脅威を想定し、これに対抗する機能を備える。

表3.1-1　想定する脅威

識別子	脅威
T.ILLEGAL_XCNTL	Storage Navigator利用者および保守員が誤って自身の権限の範囲を越えた機能を使用した結果、ホストがアクセスを許可されていないLDEVへアクセスできてしまい、ユーザデータが漏えいするかもしれない。

識別子	脅威
T.TSF_COMP	外部LANに接続可能な第三者が、Storage Navigatorプログラム－SVP PC間の通信路およびSVP PC－外部認証サーバ間の通信路に不正に機器を接続してStorage Navigator利用者のユーザIDとパスワードなどを含む通信データを入手し、Storage Navigator利用者になりすましてストレージ装置の設定を変更してユーザデータが格納されているLDEVにアクセスできてしまうかもしれない。
T.LP_LEAK	ホスト機器管理者等のホストの使用を許可された第三者が、ホスト上からホストに割り当てられたLDEV以外のLDEVにアクセスして、ユーザデータの漏えい、改ざんを行なうかもしれない。
T.CHG_CONFIG	外部LANに接続可能な第三者が、Storage Navigatorプログラムを悪用してストレージ装置の設定を変更し、アクセスが可能になったLDEVからユーザデータを漏えい、改ざん、削除するかもしれない。
T.HDD_THEFT	保守員がストレージ装置から取り出したハードディスクから、ユーザデータが漏えいするかもしれない。
T.HDD_REUSE	ストレージ管理者が、ストレージ装置またはハードディスクを再使用した場合、ハードディスク内に残っているユーザデータがストレージ利用者に漏えいするかもしれない。

ただし、以下の脅威は、本 TOE は対抗しない。

攻撃者がホストを乗っ取った場合。また、その場合に発生する以下の脅威。

乗っ取ったホスト上からホストに割り当てられている LDEV 上のユーザデータへアクセスし、漏えい、改ざん、削除した場合。

乗っ取ったホストで別のホストに成りすまし､別のホストに割り当てられている LDEV 上のユーザデータへアクセスし、漏えい、改ざん、削除した場合。

ストレージ管理者が、バックアップ先、同期先のストレージ装置から自ストレージ装置へユーザデータをリストア、同期するときに、そのストレージ装置のユーザデータが改ざんされており、自ストレージ装置のユーザデータを改ざんしてしまう恐れ。

3.1.1.2 脅威に対するセキュリティ機能方針

本 TOE は、表 3.1-1 に示す脅威に対し、以下のセキュリティ機能方針で対抗する。

⑴ 脅威「T.ILLEGAL_XCNTL」への対抗

Storage Navigator 利用者および保守員が、自身の権限の範囲を越えた機能を使用して誤った設定を行った場合、ホストが許可されていない LDEV へアクセスして、ユーザデータが漏えいするかもしれない。

本 TOE は、この脅威に対抗するために、Storage Navigator 利用者および保守員を識別・認証し、Storage Navigator 利用者および保守員が操作できる機能を、自身の権限の範囲の機能に制限する。また TOE は、セキュリティに関係する事象をログへ記録するため、不正操作を発見、追跡できる。よって、TOE は上記の脅威に対抗する。

⑵ 脅威「T.TSF_COMP」への対抗

外部 LAN に接続可能な第三者が、Storage Navigator プログラム－SVP PC 間の通信路および SVP PC－外部認証サーバ間の通信路に不正に機器を接続して Storage Navigator 利用者のユーザ ID とパスワードなどを含む通信データを入手し、Storage Navigator 利用者になりすましてストレージ装置の設定を変更してユーザデータが格納されている LDEV にアクセスできてしまうかもしれない。

本 TOE は、Storage Navigator プログラム－SVP PC 間の通信と SVP PC－外部認証サーバ間の通信に暗号化通信を使用して、外部 LAN 上での盗聴の脅威に対抗する。よって、外部 LAN に接続可能な第三者が Storage Navigator 利用者のユーザ ID とパスワードを取得して、Storage Navigator 利用者になりすますことができない。また、外部認証サーバに登録されている Storage Navigator 利用者のユーザ ID とパスワードおよびグループ情報は、適切に管理されるため、外部認証サーバへ不正な Storage Navigator 利用者のユーザ ID とパスワードを登録して、正規の Storage Navigator 利用者になりすまして、ログインすることもできない。

⑶ 脅威「T.LP_LEAK」への対抗

ホスト機器管理者等のホストの使用を許可された第三者が、ホスト上からホストに割り当てられている LDEV 以外の LDEV にアクセスして、ユーザデータの漏えい、改ざんを行なうかもしれない。

TOE は、ホストを識別し、識別されたホストのセキュリティ属性に基づいて、そのホストから許可された LDEV へのアクセスのみを許可する。ストレージ装置、ホスト、ファイバチャネルスイッチは、物理的に保護された入退出が管理されたセキュアなエリアに設置され、適切に管理される。そのため、ホストのファイバチャ

ネル接続アダプタとファイバチャネルスイッチのポートの物理的な接続と、TOE のチャネルアダプタのポートとファイバチャネルスイッチのポートの物理的な接続は、保護されている。さらに、ファイバチャネルスイッチは、ホスト―ファイバチャネルスイッチ間、ファイバチャネルスイッチ―TOE 間、ファイバチャネルスイッチ上でのホストから TOE への通信経路を適切に設定し、維持する。よって、ホストが攻撃者に乗っ取られた場合を除き、脅威に対抗しているとみなす。

(4) 脅威「T.CHG_CONFIG」への対抗

外部 LAN に接続可能な第三者が、Storage Navigator プログラムを悪用してストレージ装置の設定を変更し、アクセスが可能になった LDEV からユーザデータを漏えい、改ざん、削除するかもしれない。

TOE は、Storage Navigator 利用者および保守員を識別・認証し、ログインに連続して 3 回失敗したときに 1 分間ログインを拒否するため、外部 LAN に接続可能な第三者による Storage Navigator プログラムへの不正ログインを軽減する。また TOE は、セキュリティに関係する事象をログへ記録するため、第三者による Storage Navigator プログラムへのログインの試行や不審な TOE の設定変更を発見し、適切な対応によりその脅威を軽減することができる。

(5) 脅威「T.HDD_THEFT」への対抗

保守員がストレージ装置から取り出したハードディスクから、ユーザデータが漏えいするかもしれない。

ストレージ装置は、搭載している暗号化装置（暗号処理用 LSI）を使用してユーザデータを暗号化してハードディスクへ保存したり、復号してホストへ送信したりする。TOE は、その時に使用する暗号鍵を安全に生成、破棄する。ハードディスク上のユーザデータは常に暗号化されており、そのハードディスクが取り出されても、暗号化されたユーザデータを復号できないよう、TOE は、暗号鍵を安全に管理している。よって、TOE は上記の脅威に対抗する。

(6) 脅威「T.HDD_REUSE」への対抗

ストレージ管理者が、ストレージ装置またはハードディスクを再使用した場合、ハードディスク内に残っているユーザデータがストレージ利用者に漏えいするかもしれない。

TOE は、ホストに割り当てたハードディスク上の記憶領域の使用を停止する時やストレージ装置のハードディスクを交換する時に、該当する記憶領域のユーザデータを上書き消去し、取り出したハードディスク上からのユーザデータの漏えいの脅威に対抗する。

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 3.1-2に示す。

表 3.1-2 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.MASQ	ストレージ利用者の要求に従い、ストレージ装置に接続するホストを認証しなければならない。

ストレージ利用者が対価を払ってストレージ装置を利用する顧客の場合など、ストレージ利用者がユーザデータの安全性を向上させるため、ストレージ装置に接続するホストの認証を要求する場合がある。

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 3.1-2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.MASQ」への対応

TOEは、FC-SP(Fibre Channel Security Protocol)を使用し、ホストの認証を行う。そのため、ホストは、FC-SPに準拠したファイバチャネル接続アダプタを搭載し、FC-SPに対応したドライバを設定する。ストレージエリアネットワーク（以下「SAN」という。）は、FC-SPに準拠したファイバチャネルスイッチを用いて構成する。

ファイバチャネルスイッチは、FC-SPを使用してホスト―ファイバチャネルスイッチ間を接続し、ホストを識別・認証する。ファイバチャネルスイッチは、FC-SPを使用してファイバチャネルスイッチ―TOE間を接続し、TOEのチャネルアダプタ(CHA)を識別・認証する。その後、ホストは、ファイバチャネルスイッチを経由してTOEへ接続を要求し、TOEはホストを識別し、ホスト―TOE間の接続が成立する。ホスト―TOE間は、FC-SPではなく、FCP(Fibre Channel Protocol)で接続されるため、TOEはホストを直接、認証することができない。

ただし、ホスト、ファイバチャネルスイッチ、ストレージ装置は、物理的に保護されたセキュアなエリアに設置されて適切に管理されるため、これらの物理的なポート接続の組み合わせは、保護される。攻撃者が、偽装したホストを接続することもできない。また、ファイバチャネルスイッチは、ファイバチャネルスイッチのポートとそのポートに接続されたホストやTOEを識別・認証して、その組み合わせが一意である状態を維持し、ホストのファイバチャネル接続アダプタのポートからファイバチャネルスイッチのポートを経由して、TOEのチャネルアダプタのポー

トまでの接続状態も一意に保証する。よって、このホスト―TOE 間の接続は、TOE がホストを認証した状態と同等とみなすことができる。

したがって、TOE は、組織のセキュリティ方針を満たすとみなす。

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 4.1-1** 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 4.1-1 前提条件

識別子	前提条件
A.NOEVIL	Storage Navigator利用者のうち、セキュリティ管理者、監査ログ管理者は、ストレージ装置全体の管理・運用を行うために十分な能力を持ち、手順書で定められた通りの操作を行い、不正行為を行わないことを前提とする。 ストレージ管理者は、セキュリティ管理者から許可された範囲内においてディスクサブシステムの管理・運用を行うための十分な能力を持ち、手順書で定められた通りの操作を行い、不正行為を行わないことを前提とする。
A.NOEVIL_MNT	保守員は、ホストとTOEのチャネルアダプタのポートの接続作業を含む、ストレージ装置の保守全般を安全に行うために十分な能力をもち、手順書で定められた通りの正しい保守作業を行い、不正行為を行わないことを前提とする。
A.PHYSICAL_SEC	ストレージ装置、ホスト（ファイバチャネル接続アダプタを含む）、ファイバチャネルスイッチ、他のストレージ装置、外部認証サーバは、セキュリティ管理者が責任をもって、許可された者だけが入退室が可能なセキュアなエリアに設置し、不正な利用が行われないように適切に運用管理することを前提とする。
A.MANAGE_SECRET	ホストに設定されているホスト認証用のシークレットは、許可されていない人物に利用されないように、セキュリティ管理者が責任をもって管理することを前提とする。

識別子	前提条件
A.MANAGEMENT_PC	Storage Navigator利用者は、管理PCが不正に利用されないよう、適切に設置、管理することを前提とする。 管理PCに適用する前提条件の例を以下に示す。 ・管理PCは、直接管理できるオフィスエリアなどに設置すること。 ・管理PCは、外部ネットワークから直接アクセスできないこと。 ・管理PCは、利用者の識別、認証を行うこと。 ・管理PCの管理者権限を管理すること。 ・ソフトウェアのインストール制限やウイルス対策ソフトウェアの導入、セキュリティパッチの適用などにより、悪意のあるコードへの対策を行うこと。
A.CONNECT_STORAGE	TOEには、TOEが搭載された他のストレージ装置を接続することを前提とする。
A.EXTERNAL_SERVER	TOEと外部認証サーバの間の通信は、LDAPS、starttls、RADIUS（CHAP認証）のいずれかのプロトコルを利用することを前提とする。 TOE上と外部認証サーバ上のユーザ識別情報およびユーザグループ情報は、適切に登録および管理され、両者の情報は整合の取れた状態であることを前提とする。

上記の前提条件について、詳細な条件などを補足する。

A.EXTERNAL_SERVER

RADIUS プロトコルを使用する場合は、CHAP シークレットを使用して CHP 認証を行うことを前提とする。したがって、外部認証サーバは、RADIUS プロトコルを使用する場合、CHAP シークレットを用いた CHAP 認証を使用可能な RADIUS プロトコルに対応していることを前提とする。

4.2 運用環境と構成

本 TOE が搭載されたストレージ装置、SAN（ファイバチャネルスイッチを含む）、ホスト（ファイバチャネル接続アダプタを含む）、他のストレージ装置、外部認証サーバ、保守員 PC は、物理的に保護された入退出が管理されたセキュアなエリアに設置され、適切に管理される。管理 PC は、セキュリティ管理者が直接管理できるエリアに設置される。TOE が搭載されたストレージ装置、外部認証サーバ、管理 PC は、外部 LAN に接続する。本 TOE の一般的な運用環境を図 4-1 に示す。

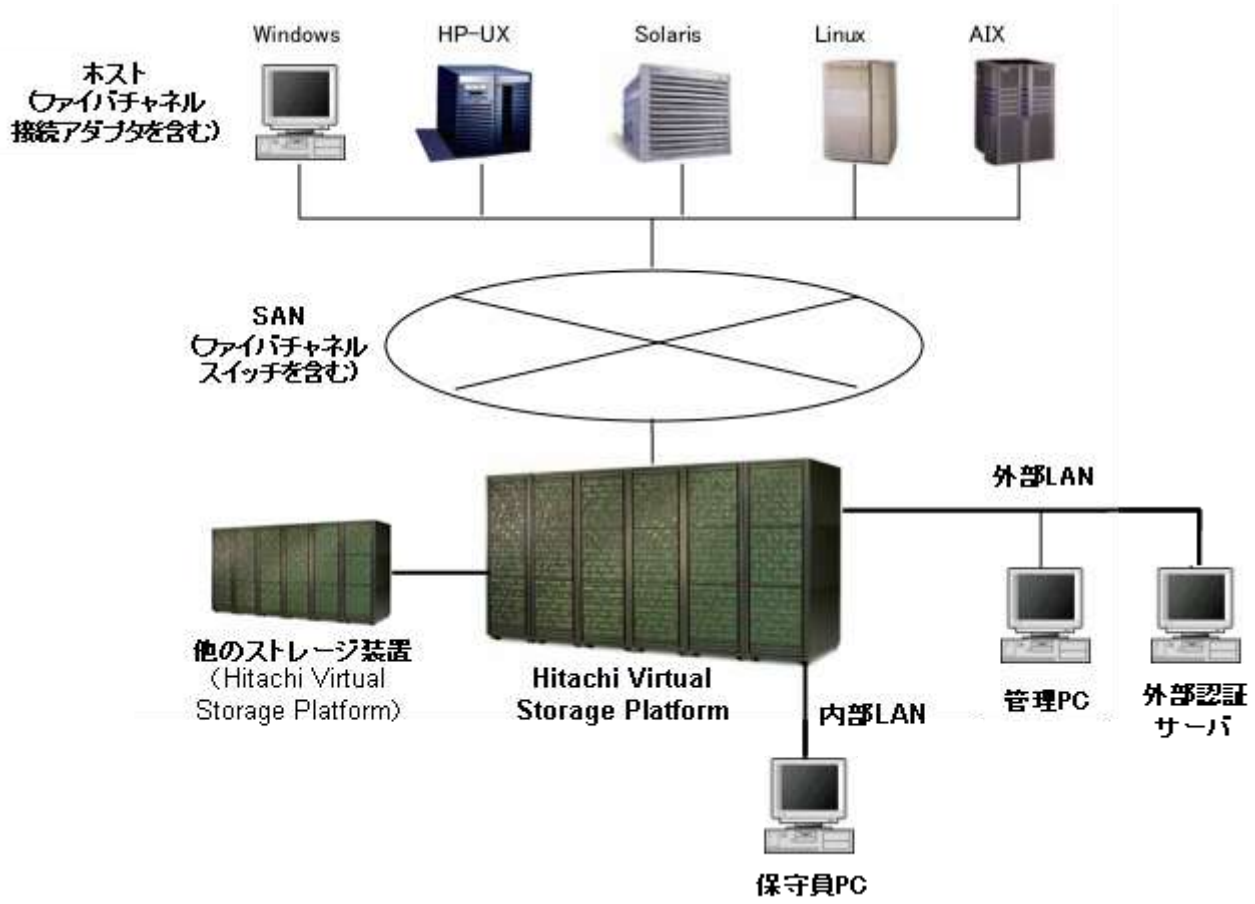

図 4-1 TOEの運用環境

本 TOE が搭載されたストレージ装置とホスト（ファイバチャネル接続アダプタを含む）は、SAN（ファイバチャネルスイッチを含む）に接続し、相互に通信を行う。SAN は、その他のネットワークと接続していないものとする。本 TOE が搭載されたストレージ装置と他のストレージ装置は、SAN を介さずに直接、接続する。外部 LAN は、インターネットなどの外部ネットワークと直接、接続しておらず、外部から管理 PC へ直接アクセスできないこととする。

管理 PC は、セキュリティ管理者が管理 PC の利用者の権限を管理し、利用者の識別・認証を義務付ける。また管理 PC には、ウイルス対策ソフトウェアの導入や

セキュリティパッチの適用、不要なソフトウェアのインストールの制限などのセキュリティ対策を行う。

本 TOE が搭載されたストレージ装置には、ユーザデータを暗号化／復号するための暗号化装置（暗号処理用 LSI）が搭載されている。本構成に示されているストレージ装置やファイバチャネルスイッチ、ファイバチャネル接続アダプタは、本評価の範囲ではないが、十分に信頼できるものとする。

本 TOE は、FC-SP を使用して、市販されている FC-SP に準拠したファイバチャネル接続アダプタを搭載したホスト(Windows, HP-UX, Solaris, Linux, AIX)と接続する仕様である。ただし、開発者は、FC-SP に対応したファイバチャネル接続アダプタ用のドライバの提供を確認できていない。ホストは、ファイバチャネルスイッチのポートを経由して TOE のチャネルアダプタのポートへ接続した場合、ファイバチャネルスイッチ―TOE 間の FC-SP 接続と、SAN やファイバチャネルスイッチの運用と管理の状況から、FC-SP を使用して TOE がホストを識別・認証した状態と同等の安全性が確保されるとみなす。

4.3 運用環境におけるTOE範囲

本 TOE は、TOE に接続するホストを識別・認証し、ホストから LDEV へのアクセスを制御するセキュリティ機能や、TOE の利用者を識別・認証し、TOE の設定を操作する機能を制御するセキュリティ機能を持つ。本 TOE は、TOE の利用者や TOE に接続する機器を信頼することを前提としているため、TOE 範囲や前提条件に含まれていない以下の脅威に対抗していない。

TOE は、TOE が搭載されたストレージ装置へ機種の異なる複数のストレージ装置を接続して使用する基本機能「Hitachi Universal Volume Manager（外部ストレージ管理機能)」を持つ。しかし、TOE が搭載されたストレージ装置へ機種の異なる複数のストレージ装置を接続した構成は、本評価が想定する構成ではない。同構成を使用する場合は、セキュリティ管理者やストレージ管理者の自己責任のもとで行う。

本 TOE は、暗号鍵のバックアップ用ファイル、TOE の設定情報、TOE のユーザ情報を管理 PC などの TOE 外へバックアップする機能を持つ。本 TOE は、TOE の設定情報、TOE のユーザ情報を TOE 外へバックアップした情報の漏えいや改ざんに対抗できない。セキュリティ管理者が責任をもって、IT 環境や運用管理のセキュリティ対策を実施する必要がある。(暗号鍵のバックアップ用ファイルは、暗号化されているため、漏えいや改ざんに対抗する。)

TOE が搭載された他のストレージ装置から TOE が搭載されたストレージ装置へユーザデータをバックアップする接続構成の場合、TOE が搭載されたストレージ装置は、TOE が搭載された他のストレージ装置のストレージ管理者を信頼することができない。したがって、TOE が搭載された他のストレージ装置のスト

レージ管理者がコマンドを実行して、TOE が搭載された他のストレージ装置が TOE が搭載されたストレージ装置のユーザデータを読み書きした場合、ユーザデータの漏えいや改ざんに該当する恐れがある。

以上の機能を使用したり、TOE の運用環境を構成した場合は、評価の範囲外であり、セキュリティ管理者やストレージ管理者の責任となる。

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。ストレージ装置に搭載される TOE は、DKCMAIN マイクロプログラム（OS を含む）と Storage Navigator プログラムを含む SVP プログラムに大きくわかれる。TOE が動作するストレージ装置の本体ハードウェア、SVP プログラムを実行するための SVP PC の OS は、TOE の範囲ではない。

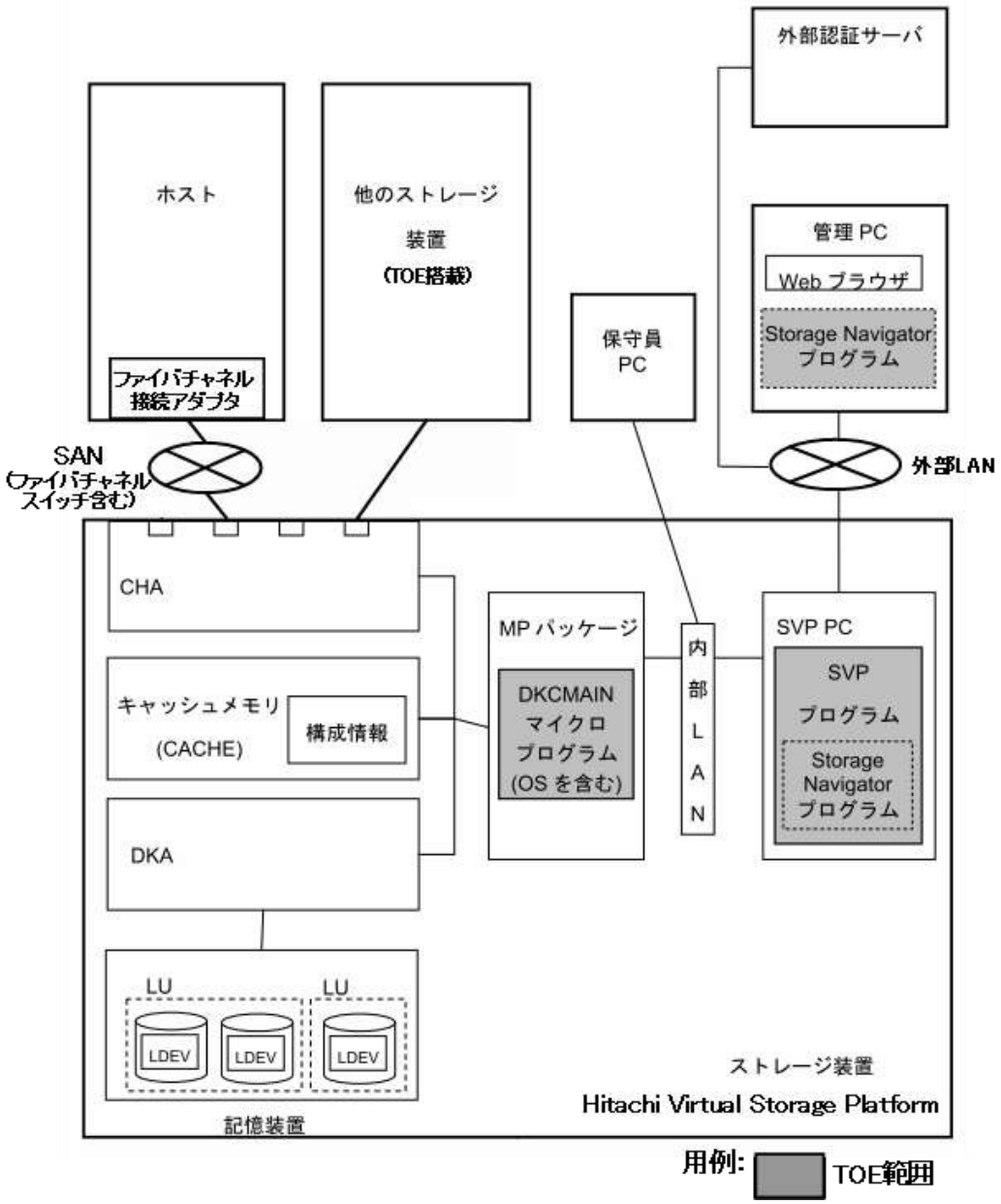

図 5-1 TOE境界

TOE を構成する DKCMAIN マイクロプログラム（OS を含む）と Storage Navigator プログラムを含む SVP プログラムについて、説明する。

(1) DKCMAIN マイクロプログラム

DKCMAIN マイクロプログラムは、ホストの接続やホストとストレージ装置間のデータ転送、記憶装置へのデータ入出力を制御したり、暗号鍵やセキュリティ機能用データを管理したり、シュレッディング機能を提供したりするストレージ装置の制御系プログラムである。ストレージ装置内の MP パッケージと呼ばれる基盤上に搭載され、動作する。DKCMAIN マイクロプログラムの主なセキュリティ機能を以下に示す。

ホスト／ファイバチャネルスイッチの接続制御（FC-SP／FCP 接続）
　ホスト／ファイバチャネルスイッチの識別、認証
　　（DH-CARP 認証（シークレットを含むレスポンス検証））
　ホストの論理ユニット(LU)へのアクセス制御
役割（ロール）ベースのセキュリティ機能用データへのアクセス制御
暗号鍵の管理（生成、削除）
シュレッディング機能
セキュリティ機能の動作／停止設定
　FC-SP 認証機能の設定
　格納データ暗号化機能の設定
セキュリティ機能用データの管理（作成、改変、削除）
　WWN、シークレットの管理
　リソースグループ情報、LU パス情報、LDEV 情報の管理
　利用者の役割情報の管理
　暗号鍵のバックアップ／リストア
　　（保護鍵による暗号鍵の暗号化／復号、暗号鍵のハッシュ検証）

(2) SVP プログラム

SVP プログラムは、Storage Navigator プログラムとリモートデスクトップの接続と TOE の利用者の識別認証を行ったり、TOE を設定するためのインタフェースを提供したり、DKCMAIN マイクロプログラムへ設定を要求したりする、ストレージ装置の運用と保守、および構成情報の管理を行うための管理系ソフトウェアである。SVP プログラムは、SVP PC の OS(Windows Vista Business)上に搭載され、動作する。SVP プログラムの主なセキュリティ機能を以下に示す。

SVP プログラムの利用者の識別認証
　利用者（セキュリティ管理者、ストレージ管理者、監査ログ管理者、保守員）の識別認証

連続認証失敗時のアクセス拒否
内部認証機能、外部認証機能、外部認証サーバとの通信（認証、暗号化）
アカウント、ホスト情報の管理（作成、変更、削除）
ユーザ情報（ユーザ ID／パスワード)、ユーザグループ情報の管理
パスワード、シークレットの品質検証
Storage Navigator プログラムの SSL 接続、リモートデスクトップの接続
SVP プログラムの画面制御機能
DKCMAIN マイクロプログラムへの設定要求の役割別制御
セキュリティ機能の設定要求の制御
セキュリティ機能の動作／停止要求の制御
セキュリティ機能用データの管理要求の制御
セキュリティ機能の設定
内部認証方式／外部認証方式の設定
外部認証サーバの接続設定
設定ファイルの入出力
暗号鍵のバックアップファイルの読み込み、書き出し
構成情報ファイルの読み込み、書き出し（CFL：Configuration File Loader）
構成情報ファイルのフォーマットチェック
監査ログ機能
監査ログの記録、蓄積（ラップアラウンド方式）
監査ログの出力

(3) Storage Navigator プログラム

Storage Navigator プログラムは、SVP プログラムへ接続し、SVP プログラムを操作するためのグラフィカルユーザインタフェースを提供するクライアントプログラムである。Storage Navigator プログラムは、管理 PC の Web ブラウザ上で動作する。Storage Navigator プログラムと SVP プログラムの間は、SSL 通信を使用する。

5.2 IT環境

本 TOE を構成する DKCMAIN マイクロプログラムと SVP プログラムは、分離されたハードウェア上で動作するが、前提条件において保護されている内部 LAN を介して接続され、相互に通信を行う。保守員 PC も内部 LAN に接続され、SVP PC へリモートデスクトップ接続し、SVP プログラムを利用する。

SVP プログラム、Storage Navigator プログラム、外部認証サーバは、外部 LAN を介して接続される。外部 LAN は、前提条件等によって保護されていないため、SVP プログラム―Storage Navigator プログラム間、SVP プログラム―外部認証サーバ間は、認証および暗号化した通信を使用する。また、SVP プログラムと外部

LAN の境界には、ファイアウォールを設置するよう、ガイダンスに記載されている。

DKCMAIN マイクロプログラムとホストは、ファイバチャネルスイッチを用いて構成された SAN を介して接続される。SAN およびファイバチャネルスイッチは、前提条件に基づいて、第三者が SAN の物理構成を変更できないよう物理的に保護され、ファイバチャネルスイッチには安全な設定が施されて不正な利用を防止している。

本ストレージ装置は、Storage Navigator プログラムの SSL 通信やアクセス制御などの TOE のセキュリティ機能と、DKCMAIN マイクロプログラムと SVP プログラムの物理的な分離などにより、外部 LAN に接続した攻撃者からの不正なアクセスから、CHA、CACHE、DKA、記憶装置上の保護対象のユーザデータを保護している。

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。英語版のドキュメントは日本語版を英訳したものであり、内容は一部を除き、日本語版と同じである。「表 5.2-3：ディスクサブシステムの保守マニュアル」と「表 5.2-4：ディスクサブシステムの保守マニュアル(英語版)」は、保守員用のガイダンスである。

表 5.2-1：ユーザーズガイド

No	製品添付ドキュメント名（ユーザーズガイド）	バージョン
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 ISO15408 認証取得機能 取扱説明書	1.6
2	Hitachi Virtual Storage Platform Storage Navigator ユーザーガイド	第 5 版
3	Hitachi Virtual Storage Platform Storage Navigator メッセージ	第 5 版
4	Hitachi Virtual Storage Platform オープンシステム構築ガイド	第 4 版
5	Hitachi Virtual Storage Platform Encryption License Key ユーザガイド	第 3 版
6	Hitachi Virtual Storage Platform Volume Shredder ユーザガイド	第 3 版
7	Hitachi Virtual Storage Platform 監査ログ リファレンスガイド	第 3 版
8	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 利用者ガイダンス	1.2

表 5.2-2：ユーザーズガイド(英語版)

No	製品添付ドキュメント名（ユーザーズガイド）	バージョン
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 Manual for Obtaining ISO15408 Certification	1.6
2	Hitachi Virtual Storage Platform Hitachi Storage Navigator User Guide	MK-90RD7027-02f
3	Hitachi Virtual Storage Platform Hitachi Storage Navigator Messages	MK-90RD7028-03a
4	Hitachi Virtual Storage Platform Provisioning Guide for Open Systems	MK-90RD7022-02e
5	Hitachi Virtual Storage Platform Hitachi Encryption License Key User Guide	MK-90RD7015-02a
6	Hitachi Virtual Storage Platform Hitachi Volume Shredder User Guide	MK-90RD7035-02b
7	Hitachi Virtual Storage Platform Hitachi Audit Log User Guide	MK-90RD7007-02d
8	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 User's Guidance	1.2

表 5.2-3：ディスクサブシステムの保守マニュアル

No	製品添付ドキュメント名（ディスクサブシステムの保守マニュアル）	バージョン
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 ISO15408 認証取得機能 メンテナンスマニュアル	1.4
2	A/H-65AC A-65BC HT-40BC ディスクアレイシステム メンテナンスマニュアル	REV.3
3	検査指導書 RAID700 CTO ユニット	REV.2

表 5.2-4：ディスクサブシステムの保守マニュアル(英語版)

No	英語版ディスクサブシステムの保守マニュアル	バージョン
1	Hitachi Virtual Storage Platform / Hitachi Virtual Storage Platform VP9500 Obtaining ISO15408 Certification Maintenance Manual	1.4
2	DKC710I Maintenance Manual	REV.3

「A/H-65AC」「A-65BC」「HT-40BC」「RAID700」「DKC710I」は、「Hitachi Virtual Storage Platform」の別名である。

国内と海外は、配付方法及びメンテナンス体制の違いがあり、保守マニュアルの No.2 の日本語版と英語版は一部内容が異なる。「DKC710I Maintenance Manual」の「INSTALLATION SECTION」の記述は、日本語版に無い。ただし、同様の内容は、「表 5.2-3：ディスクサブシステムの保守マニュアル」の No.3「検査指導書 RAID700 CTO ユニット」に記載されている。

「表 5.2-3：ディスクサブシステムの保守マニュアル」の No.3「検査指導書 RAID700 CTO ユニット」の英語版は無い。同ガイダンスは、国内の配付時に配付担当者が TOE のインストールに使用するガイダンスである。

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 22 年 10 月に始まり、平成 23 年 8 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 23 年 4 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・配付セキュリティ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 23 年 4 月と 5 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・追加テスト及び脆弱性評定に基づく侵入テストを実行した。

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。

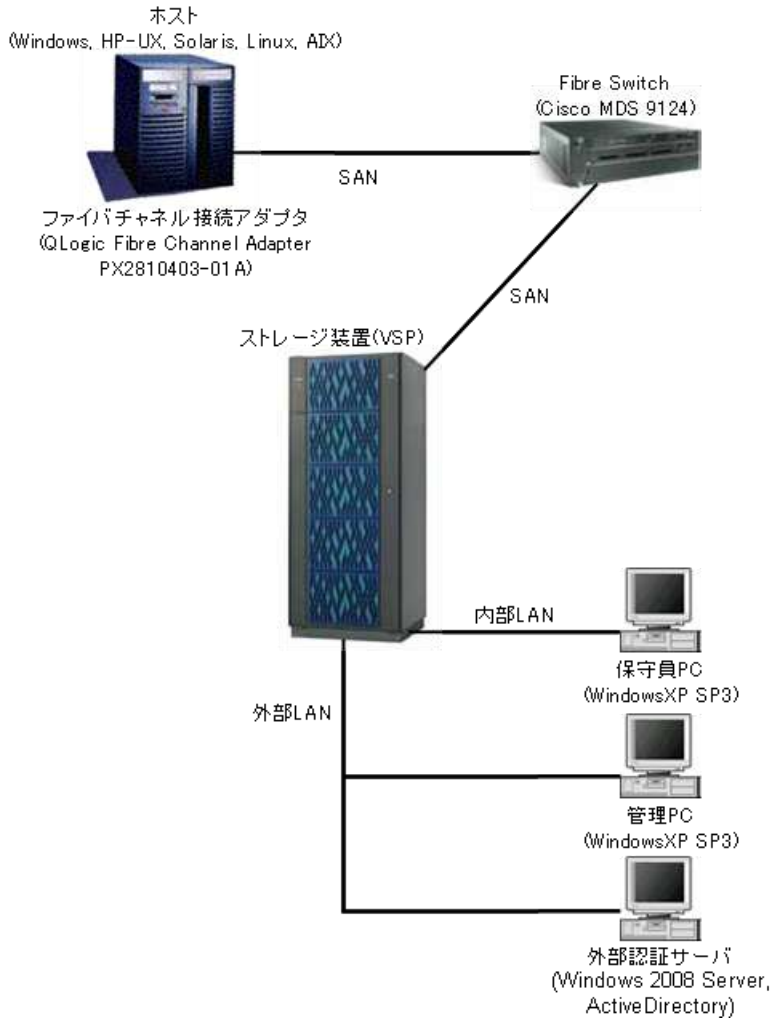

図 7-1 開発者テストの構成図

開発者テストは、「Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500 用制御プログラム バージョン 70-02-00-00/11（DKCMAIN マイクロプログラム バージョン 70-02-00-00/11、SVP プログラム バージョン 70-02-00/10）」を使用した。これは、ST に記載されている TOE のバージョンと異

なる。上記のバージョンの違いは、RAID 機能の改修によるものであり、セキュリティ機能に影響しない。本 TOE には、いくつかのオプションが存在するが、それらは TOE の範囲外であるため、オプションを含まない TOE 単体が評価の対象である。

TOE の運用環境は、評価対象のストレージ装置へ、TOE が搭載された他のストレージ装置が直接、接続された状態を想定している。TOE には、評価対象のストレージ装置へ TOE が搭載された他のストレージ装置が接続された状態を内部的に再現する機能がある。同機能を使用した場合の TOE のふるまいは、物理的に他のストレージ装置を接続した状態と全く同一である。そのため、評価対象のストレージ装置と他のストレージ装置に関係するテストは、この機能を用いて実施した。

表 7.3-1　開発者テストの構成

端末・機器名	製品
ストレージ装置（SVP PC）	OS：Windows Vista Business SP2 Web サーバ：Apache Tomcat 6.0.16
ホスト	OS：Windows Server 2003 SP2, HP-UX、Solaris、Linux、AIX ファイバチャネル接続アダプタ：QLogic Fibre Channel Adapter PX2810403-01A
ファイバチャネルスイッチ	Cisco MDS 9124（4G/2G/1Gbps 24 ポート）
管理 PC	OS：Windows XP SP3 ブラウザ等：Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
保守員 PC	OS：Windows XP SP3 ブラウザ等：Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
外部認証サーバ	OS：Windows 2008 Server 認証サーバ：Active Directory

以上より、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

開発者テストの概説は以下のとおりである。

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＞

Storage Navigator プログラムと保守員 PC から、TOE の外部インタフェースに対して、画面へ入力可能な値の組み合わせをテストし、Storage Navigator プログラムの画面表示やメッセージから、入力に対する TOE の

ふるまいの確認やTOEと外部認証サーバに関係するふるまいの間接的な確認を行った。

ホストを操作してストレージ装置へアクセスし、TOEのログから、そのふるまいを確認した。

＜開発者テストツール＞

図 7-1に示す構成以外、開発者テストで使用したツールは無い。

＜開発者テストの実施内容＞

Storage Navigatorプログラムと保守員PCから利用可能な下記の複数の外部インタフェース(1) (2)について、インタフェースを直接操作して入力を実施し、画面出力と期待されたテスト結果の比較を行った。Storage Navigator利用者や保守員の識別認証や設定データへのアクセス制御などのセキュリティ機能を確認した。

下記(3)のホストとのインタフェースについて、ホストを操作してストレージ装置へアクセスし、TOEのログと期待されたテスト結果の比較を行った。ホストの識別認証や記憶領域のアクセス制御などのセキュリティ機能を確認した。

下記の外部インタフェース(4)については、Storage Navigatorプログラムから TOE へ関連する設定を実施し、Storage Navigatorプログラムへ表示されたメッセージ等と期待されたテスト結果を比較し、間接的にTOEのふるまいを確認した。TOEと外部認証サーバ間の通信の識別認証と暗号化などのセキュリティ機能を確認した。

(1) TOEとStorage Navigator利用者（管理PC）のインタフェース

(2) TOEと保守員PCのインタフェース

(3) TOEとホストのインタフェース

(4) TOEと外部認証サーバのインタフェース

b) 開発者テストの実施範囲

開発者テストは開発者によって119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たすべてのセキュリティ機能と外部インタフェースがテストされたことが検証された。

カバレージ分析によって、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を表 7.3-2、図 7-2 に示す。評価者独立テストでは、Windows Server 2003 が搭載されたホストを使用した構成のみをテストした。開発者テストでは、各ホストの OS（Windows、HP-UX、Solaris、Linux、AIX）とそのファイバチャネル接続アダプタ用ドライバが、WWN を用いて TOE と FCP 接続でき、ストレージ装置を正常に操作できることが確認された。この開発者テストの結果から、評価者は、上記のドライバは FCP に準拠して動作し、違いがないと判断し、評価者独立テストは、Windows Server 2003 が搭載されたホストの構成のみを実施した。

表 7.3-2 評価者独立テストの構成

端末・機器名	製品
ストレージ装置（SVP PC）	OS：Windows Vista Business SP2 Web サーバ：Apache Tomcat 6.0.16
ホスト	OS：Windows Server 2003 SP2 ファイバチャネル接続アダプタ：QLogic Fibre Channel Adapter PX2810403-01A
ファイバチャネルスイッチ	Cisco MDS 9124（4G/2G/1Gbps 24 ポート）
管理 PC	OS：Windows XP SP3 ブラウザ等：Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
保守員 PC	OS：Windows XP SP3 ブラウザ等：Internet Explorer 8, Flash Player 10.1, Java version 1.6.0_20
外部認証サーバ	OS：Windows 2008 Server 認証サーバ：Active Directory

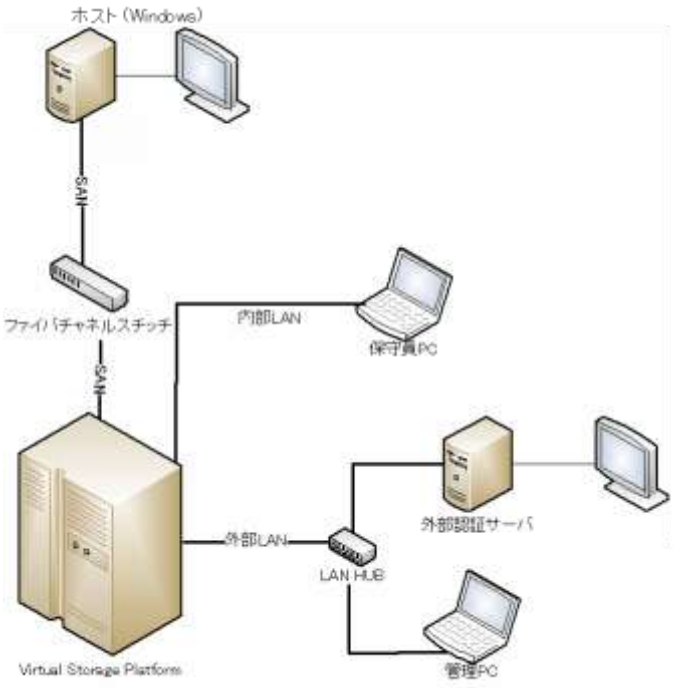

図 7-2　独立テストの構成図

独立テストは、上記のホストの OS の違いと他のストレージ装置の接続以外、本 ST において識別されている TOE の構成と同一の環境で実施された。

⑵ 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。

評価者は、全てのTOEセキュリティ機能のインタフェースについて、少なくとも1つずつのサンプルテストを実施した。評価者は、4種類のTOEセキュリティ機能のインタフェースの区分すべてについて偏りのないテストを実施する方針のもと、追加すべきテスト項目があるインタフェースの独立テストを少なくとも1つずつ実施した。

＜独立テストの観点＞

① 管理 PC 操作、保守員 PC 操作、出力監査ログの確認操作を確認する。

② TOE の運用中に設定を変更した場合の動作を確認する。

③ 外部認証サーバを使用した場合の動作を確認する。

b) **独立テスト概要**

評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点で56項目のサンプリングテストを実施した。評価者は、開発者テスト及び提供された評価証拠資料から、以下の観点で10項目の追加の独立テストを考案した。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＞

開発者テスト手法と同様、インタフェースの直接操作と表示の確認、ホスト操作と TOE のログの確認、TOE と外部認証サーバに関係するふるまいの間接的な確認を実施した。

＜独立テストの実施内容＞

独立テストは、開発者によって 10 項目実施された。

独立テストの観点とそれに対応したテスト内容を表 7.3-3 に示す。

表 7.3-3 実施した独立テスト

No	テスト概要
IND-1	役割別の操作機能へのアクセス制限(1) : ある利用者の役割をストレージ管理者からセキュリティ管理者へ変更した場合、ストレージ管理者の操作メニューへアクセスできなくなることを確認する。
IND-2	役割別の操作機能へのアクセス制限(2) : セキュリティ管理者が、ストレージ管理者の操作メニューへアクセスできないことを確認する。
IND-3	ホストの認証 : セキュリティ管理者でシークレットを変更し、変更したシークレットでホストが認証されることを確認する。
IND-4	削除されたユーザによるログイン : 外部認証サーバに登録されている 1 人のユーザ（ストレージ管理者）を削除して、Storage Navigator プログラムからそのユーザでログインできないことを確認する。
IND-5	リモートデスクトップからのアクセス : セキュリティ管理者、ストレージ管理者、監査ログ管理者は、リモートデスクトップから接続できないことを確認する。
IND-6	保守員の連続認証失敗 : 保守員 ID は、リモートデスクトップで 3 回連続して認証失敗したあと、1 分間ログインできないことを確認する。認証方式は外部認証とする。
IND-7	保守員自身によるパスワード変更 : 保守員自身がパスワードを変更し、変更されたパスワードでログインできることを確認する。パスワードの品質（文字数、文字種）チェック機能を確認する。
IND-8	暗号鍵のリストア : バックアップした暗号鍵が改ざんされた場合、TOE へリストアができないことを確認する。
IND-9	シュレッディング機能の停止 : ストレージ管理者が、シュレッディング機能を停止できること、シュレッディングされていない旨の警告が表示されることを確認する。
IND-10	WWN の変更 : TOE に登録された WWN を変更した場合、TOE がホスト情報を更新した後、ホストはストレージ装置へアクセスできないことを確認する。

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、必要と思われる評価者侵入テスト（以下「侵入テスト」という。）を考案し実施した。評価者が実施した侵入テストを以下に説明する。

(1) 侵入テスト概説

評価者が実施した侵入テストの概説は以下のとおりである。

a) 懸念される脆弱性

評価者は、公知の情報や提供された証拠資料より、潜在的な脆弱性を探索し、侵入テストを必要とする脆弱性を識別した。以下に、識別された脆弱性を5つの観点にまとめたものを示す。

① 不整合操作に対する挙動

不正なパラメタ値、許容範囲外の値（ユーザ名、パスワード等）を入力した場合について、OS コマンド・インジェクション、ディレクトリ・トラバーサルなどの脆弱性が発生する恐れ。ファイバチャネルスイッチのポートへのケーブル誤接続、権限外の操作が行える脆弱性。

② セッションの改竄

SVP PC と管理 PC の間のセッションの維持管理に使用しているセッション ID (Cookie 値)の品質問題、想定外のセッション ID の使用、セッション ID 破損等によるセッション・ハイジャック、クロスサイト・スクリプティングの脆弱性。

③ オープンポートに関係する公知の脆弱性

SVP PC と MP パッケージの外部 LAN、内部 LAN に不要なポートが開いていたり、オープンポートに関係するサービスに公知の脆弱性が存在し、ネットワークからの不正アクセスされる脆弱性。

④ 通信における暗号アルゴリズム

SVP PC と管理 PC 間の SSL 通信、SVP PC と外部認証サーバ間の LDAPS、starttls または RADIUS(CHAP)プロトコルによる通信の脆弱性。

⑤ その他の懸念事項

開発者テストや評価者独立テストで確認されていない LDEV 削除、証明書の期限切れ、排他制御のふるまいに関する脆弱性。

b) **侵入テストの概要**

評価者は、潜在的な脆弱性が悪用される可能性を検出するために、以下の侵入テストを実施した。

＜侵入テスト環境＞

侵入テスト環境を図 7-3 に示す。本環境は、「図 7-2　独立テストの構成図」へ検査 PC と検査ツールを追加している。

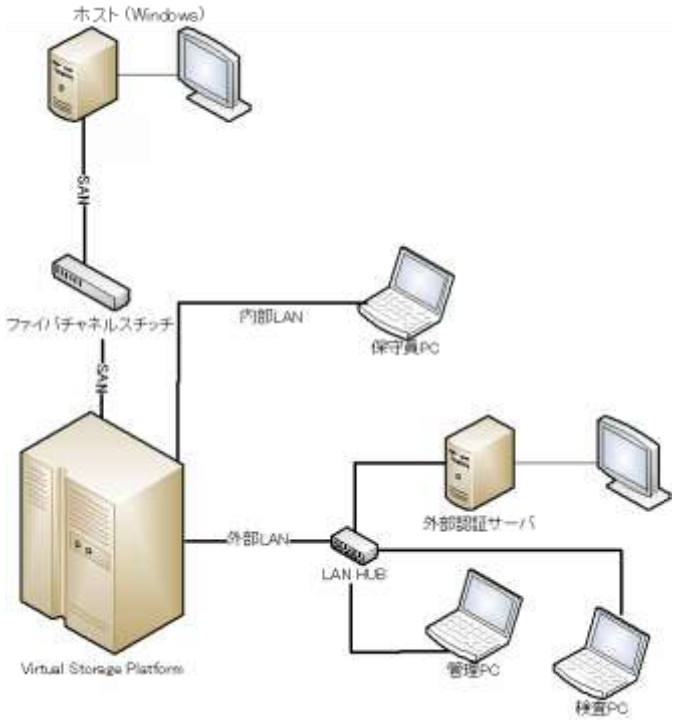

図 7-3　侵入テスト環境

独立テスト環境へ追加した検査 PC 上の検査ツールの詳細を表 7.3-4 に示す。

表 7.3-4　侵入テストで使用したツール

ツール名称	概要・利用目的
Nmap Ver 5.51	調査対象機器がオープンしている IP 通信のポートを検出するツール。 TOE の外部 LAN、内部 LAN 向けにオープンされたポートを調査する。
Nessus Ver 4.4.1 (build 15078)	使用している通信サービスやプロトコルに基づいて、OS、アプリケーション等の公知の脆弱性を検査するツール。プラグインは、2011 年 4 月 19 日のデータを使用。TOE の外部 LAN 向けにオープンされた通信サービスの脆弱性を調査する。
Nikto Ver 2.1.4	Web サーバ専用の脆弱性診断ツール。HTTP プロトコル、CGI 等の公知の脆弱性を検査する。プラグインは、2011 年 4 月 19 日のデータを使用。 TOE の Web サーバを調査する。

ツール名称	概要・利用目的
Fiddler	HTTP パケットをキャプチャして表示したり、その内容を改ざんして送信できるツール。TOE の Web サーバへ不正な値を送信して、脆弱性を調査する。
Wireshark Ver 1.4.4	ネットワークを流れるパケットの分析プログラム。イーサネットワーク上のパケットを収集し、プロトコルを解析する。

＜侵入テスト手法＞

TOE のインタフェースに関する侵入テストは、Storage Navigator プログラムから侵入テスト用の値を入力し、TOE の画面遷移や表示されたメッセージ、ログを確認する。

SVP PC と管理 PC 間の SSL 通信や、SVP PC と外部認証サーバ間の LDAPS、starttls または RADIUS(CHAP)プロトコルによる通信は、その通信の TCP/IP パケットを取得し、プロトコルを使用していること、脆弱性のある通信手順を使用していないこと、暗号化通信であり機密性のあるデータが閲覧できないことを確認する。

＜侵入テストの実施項目＞

懸念される脆弱性と対応する侵入テスト内容を表 7.3-5 に示す。

表 7.3-5　侵入テスト概要

No	テスト名	テスト概要	懸念される脆弱性
VAN-1-1	不正パラメタ	入力値に制限があるパラメタに対して、不正な値を設定し、挙動を確認する。	①
VAN-1-3	ファイバチャネルスイッチポート・ケーブル差し替え	ファイバチャネルスイッチのポートに接続されているケーブルを差し替え、挙動を確認する。	①
VAN-1-4	LDEV 削除	ストレージ管理者により削除された LDEV が再利用できないこと確認する。（※）	⑤
VAN-2	セッション ID のランダム性確認	セッション管理に使用しているセッション ID のランダム性を確認する。	②
VAN-3-1	ポートスキャン(SVP PC)	Nmap を用いて、SVP PC に開いている不要なポートを確認する。	③
VAN-3-2	汎用脆弱性スキャン(SVP PC)	汎用脆弱性スキャンツール Nessus を用いて、SVP PC の公知の脆弱性を確認する。	③
VAN-3-3	Web 系脆弱性スキャン (SVP PC)	Web サーバ専用の脆弱性診断ツール Nikto を用いて、SVP PC の Web サーバ系の脆弱性を確認する。	①
VAN-3-4	ポートスキャン(MP パッケージ)	Nmap を用いて MP パッケージに開いている不要なポートを確認する。	③

No	テスト名	テスト概要	懸念される脆弱性
VAN-4	外部認証確認	SVP PC-外部認証サーバ間が暗号化通信を使用していることを確認する。（※）	④
VAN-5-1	クロスサイトスクリプティング	ユーザ作成画面のユーザ名入力インタフェースへ、悪意のあるスクリプトを混入させることができないことを確認する。	②
VAN-5-2	OS コマンドインジェクション	ユーザ作成画面のユーザ名入力インタフェースへ、悪意のある OS のコマンドを混入させることができないことを確認する。	①
VAN-6	期限切れ証明書	Storage Navigator プログラムから、証明書の有効期限が切れた SVP PC の Web サーバへログインした場合の挙動を確認する。	⑤
VAN-7	クッキー改変	セッション管理に使用している Cookie（セッション ID）を改変し、挙動を確認する。	②
VAN-8	排他制御	異なるストレージ管理者が、同時に同一のリソースグループに属する LDEV を編集できないことを確認する。（※）	⑤
VAN-9	CFL-CLI 不正ファイル	構成情報ファイルの読み込み／書き出し機能に対して、不正な構成情報ファイルを入力した場合の挙動を確認する。	①

※開発者テストや評価者独立テストで実施されている項目だが、懸念される脆弱性が存在するため、侵入テストを追加実施した。

c) **結果**

評価者が実施した侵入テストでは、想定する攻撃能力を持つ攻撃者が悪用可能な脆弱性は確認されなかった。

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 7-2 に示す構成において、評価を行った。評価者は、OS 別の 5 種類のホスト（Windows、HP-UX、Solaris、Linux、AIX）とそのファイバチャネル接続アダプタ用ドライバの組み合わせ、および SVP PC と外部認証サーバ間の 3 種類の通信方式（LDAPS、starttls、RADIUS）について、評価した。TOE と他のストレージ装置との接続は、TOE にある上記状態を内部的に再現する機能を使用した。

本 TOE は、上記の構成要素と大きく異なる構成において、運用される場合はない。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

消費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 は、ホストを識別・認証し、ホストが割り当てられた LDEV 以外へアクセスすることを禁止する機能を持つ。しかし、攻撃者がホストを乗っ取り、ホストに割り当てられた LDEV にアクセスして、その LDEV 内のユーザデータを漏えいしたり、改ざんする場合、TOE は対抗できない。ホストは、ホスト機器管理者が責任を持って、セキュリティ対策を実施する必要がある。

TOE が搭載された他のストレージ装置から TOE が搭載されたストレージ装置へユーザデータをバックアップする場合、TOE が搭載されたストレージ装置は、TOE が搭載された他のストレージ装置のストレージ管理者を信頼することができない。したがって、TOE が搭載された他のストレージ装置のストレージ管理者がコマンドを実行して、TOE が搭載された他のストレージ装置が TOE が搭載されたストレージ装置からユーザデータを読み書きした場合、ユーザデータの漏えいや改ざんに該当する恐れがある。

TOE が搭載されたストレージ装置へ機種の異なるストレージ装置を接続して使用することが可能だが、その場合の TOE のセキュリティ機能の動作は、保証されていない。セキュリティ管理者やストレージ管理者の自己責任のもとで運用する。

セキュリティ管理者は、TOE から管理 PC 上やその他の記録媒体へバックアップした暗号鍵のバックアップ用ファイル、TOE の設定情報ファイル、TOE のユーザ情報を紛失や漏えい、改ざんから保護しなければならない。

前提条件には、TOE が搭載されたストレージ装置と他のストレージ装置を直接接続し、物理的に保護された入退出が管理されたセキュアなエリアに設置することが、記載されている。しかし、一般的にバックアップや同期用の他のストレージ装置は、遠隔地に設置して運用する。TOE と遠隔地の他のストレージ装置間を接続する場合は、セキュリティ管理者やストレージ管理者の自己責任のもとで、TOE と遠隔地の他のストレージ装置間の物理的なセキュリティを確保して運用する必要がある。

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 Virtual Storage Platform セキュリティターゲット バージョン 1.17
2011 年 8 月 19 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 に関する略語を以下に示す。

CFL	Configuration File Loader
CHA	Channel Adapter
CHAP	Challenge Handshake Authentication Protocol
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DKA	Disk Adapter
DKC	Disk Controller
FCP	Fibre Channel Protocol
FC-SP	Fibre Channel Security Protocol
FTP	File Transfer Protocol
JRE	Java Runtime Environment
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over TLS
LDEV	Logical Device
LSI	Large Scale Integration
LU	Logical Unit
PC	Personal Computer
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
SAN	Storage Area Network
SSL	Secure Sockets Layer
SVP	Service Processor
TLS	Transport Layer Security
VSP	Virtual Storage Platform
WWN	World Wide Name

本報告書で使用された用語の定義を以下に示す。

CHAP シークレット	CHAP による認証を相互に行う時に使用する共有パスワード
CHAP 認証	サーバからクライアントに送られた乱数文字列を元に、クライアントがサーバへ暗号化したパスワードを送信して、認証を行う方法
Cookie	Web サーバが、Web ブラウザへ一時的にデータを書き込んで保存させるしくみ。ユーザの識別や認証、セッション管理に利用される。
DKCMAIN マイクロプログラム	ストレージ装置の MP パッケージと呼ばれる基盤上に搭載され、ホストの接続やホストとストレージ装置間のデータ転送、記憶装置へのデータ入出力制御、暗号鍵やセキュリティ機能用データの管理、シュレッディング機能を提供したりするストレージ装置の制御系プログラムである。
FC-SP	ファイバチャネルにおいて、コンピュータとストレージ装置などの周辺機器、ファイバチャネルスイッチが通信するときに、お互いを識別認証し、安全な通信を行うためのプロトコル。認証には、DH-CHAP with NULL DH Group 認証を使用する。
LDEV	論理デバイス(Logical Device)の略。ストレージ装置内のユーザ領域に作成する記憶領域の単位
LU パス情報	ホストと LU 間の経路情報
OS コマンド・インジェクション	外部からサーバへ、そのサーバの OS を操作する命令を送信し、不正に実行すること
starttls	SMTP プロトコルを拡張し、SSL/TLS によって通信を暗号化したもの
Storage Navigator プログラム	ストレージ装置の設定を行う GUI を提供するプログラム。Flex アプリケーションと Java アプレットで構成され、SVP PC および管理 PC で動作する。Storage Navigator 利用者および保守員が使用する。
Storage Navigator 利用者	Storage Navigator プログラムの利用者。セキュリティ管理者とストレージ管理者、監査ログ管理者である。
SVP PC	SVP プログラムを搭載するためのストレージ装置内の PC 基盤
SVP プログラム	ストレージ装置の SVP PC に搭載され、Storage Navigator プログラムとリモートデスクトップの接続、TOE の利用者の識別認証、TOE の設定インタフェースの表示、DKCMAIN マイクロプログラムと通信を行い、ストレージ装置の運用と保守、および構成情報の管理を行うための管理系ソフトウェアである。
Syslog 転送	システムの動作状況やメッセージなどのログを記録する Syslog プログラムが、他のコンピュータとログを送受信する機能
クロスサイト・スクリプティング	動的に Web ページを生成する Web アプリケーションの問題。悪意のあるスクリプトが混入できる脆弱性

シークレット	FC-SP において、DH-CHAP による認証を相互に行う時に使用する共有パスワード
シュレッディング機能	ハードディスクや SSD（Solid State Drive）などの記憶装置をダミーデータで上書きして、残存データを消去する機能
ストレージ・エリア・ネットワーク(SAN)	サーバなどとハードディスク装置などを接続したネットワークシステム。ファイバチャネルやイーサネットを使って通信する。
ストレージ管理者	Storage Navigator プログラムを使用して、割り当てられたストレージ装置のリソースを管理する者
ストレージ利用者	ストレージ装置内に保存されたユーザデータを使用する者。ホストまたはホストを経由してユーザデータを操作する者
セキュリティ管理者	Storage Navigator プログラムを使用して、アカウント、リソースグループ、ユーザグループの管理、TOE へホストやファイバチャネルスイッチの認証設定など、TOE の設定を行う者
セッション・ハイジャック	サーバとクライアント間の通信のセッション（特定利用者間で行われる一連の通信群）を通信当事者以外が乗っ取る攻撃手法。HTTP における Web セッションのハイジャックなど
ディスクサブシステム	ストレージ装置、Hitachi Virtual Storage Platform（別名 Hitachi Virtual Storage Platform VP9500）のこと
ディレクトリ・トラバーサル	アクセス許可の設定ミスや入力されたディレクトリやファイル名のセキュリティ検証が不十分であるため、アクセスの許可を意図していないファイルへアクセスできてしまう攻撃
ファイバチャネル	コンピュータとストレージ装置などの周辺機器間のデータ転送方式。高い性能が必要なサーバとハードディスク装置を接続するときに使用する。
ファイバチャネルスイッチ	ファイバチャネルのインタフェースを持つ各種装置を相互に接続するためのネットワーク装置。ファイバチャネルスイッチを使うことで、複数のホストとストレージ装置を高速接続し、SAN（Storage Area Network）を構築することができる。
ファイバチャネル接続アダプタ	コンピュータに搭載するファイバチャネル用のネットワークインタフェース装置
ホスト機器管理者	ホストのハードウェアおよびソフトウェア構成を管理する管理者。
ユーザグループ	ユーザグループ情報
ラップアラウンド方式	ログのファイルサイズに制限がある場合に、ファイルが満杯になったあと、ファイルの先頭に戻って、ログを上書き記録すること
リソースグループ	リソースグループ情報
レスポンス検証	CHAP 認証において、サーバが、クライアントから送られてきた暗号化されたパスワードをサーバ自身が生成した暗号化されたパスワードと比較検証すること
監査ログ管理者	Storage Navigator プログラムを使用して、監査ログの参照やダウンロードなどの管理、syslog 関連の設定を行う者

管理 PC	Storage Navigator 利用者が、Storage Navigator プログラムを操作するための端末
保守員	ストレージ装置を利用する顧客が保守契約を結んだ保守専門の組織に所属する者。ストレージ装置を設置する際の初期立上げ処理、部品の交換や追加などの保守作業、保守作業に伴う設定変更、異常時の復旧処理などを担当する。
保守員 PC	保守員が、保守作業時に SVP PC へ接続する時に使用する端末
論理ユニット(LU)	論理ユニット。ホストがアクセスする記憶領域の最小単位。1 個または複数の LDEV(論理デバイス)から構成される。
CHAP シークレット	CHAP による認証を相互に行う時に使用する共有パスワード
CHAP 認証	サーバからクライアントに送られた乱数文字列を元に、クライアントがサーバへ暗号化したパスワードを送信して、認証を行う方法

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19年5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

[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, 平成19年5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 Virtual Storage Platform セキュリティターゲット, バージョン 1.17, 2011年8月19日, 株式会社 日立製作所

[13] Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform用制御プログラム評価報告書, 第3版, 2011年8月31日, みずほ情報総研株式会社 情報セキュリティ評価室